Philosophy, Economics and Law Review

Vol. 5. No. 2. 2025
Received: 19.06.2025
Revised: 18.10.2025
Accepted: 27.11.2025

Journal homepage: https://phelr.com.ua/en

UDC 347.78:004.738.5

DOI: 10.63341/2786-491X-2025-2-08

Civil-law aspects of using deepfake content in the context of copyright and personal data protection

Krystyna Rezvorovych*
Doctor of Law, Associate Professor
Dnipro State University of Internal Affairs
49005, 26 Nauky Ave., Dnipro, Ukraine
https://orcid.org/0000-0003-1183-613X

Abstract. The relevance of this study stems from the rapid development of generative technologies that enable the creation of heavily modified or fully synthesised content using artificial intelligence, particularly deepfakes. Such content not only creates an illusion of authenticity but also poses a threat to the protection of intellectual property rights and personal non-property rights, giving rise to significant legal challenges in the digital environment. The aim of the article was to formulate and justify civil-law approaches to the regulation of deepfake content usage in the context of copyright and personal data protection, considering the challenges of society's digital transformation. The study employed methods of systems analysis, legal-logical generalisation, formal legal method, and comparative legal research, considering international norms and doctrinal sources. It was established that current Ukrainian legislation does not define deepfake content as a separate legal category, and existing legal mechanisms are fragmented and do not cover all aspects of responsibility for its creation and distribution. Gaps were identified in the regulation of derivative digital works, the protection of biometric features of individuals, and the procedures for identifying violators in the context of automated content generation. The study proved that without proper regulatory response, deepfake technologies may be used as tools of manipulation, identity forgery, and digital defamation. The research emphasised the need for an interdisciplinary approach that integrates legal, technical, and ethical aspects of deepfake regulation. Special attention was given to legal liability in cases of automated content creation without direct human authorship. The importance of digital transparency and informed consent was highlighted as key principles of legal regulation. The results of the study can be used to improve national legislation and to develop international legal mechanisms in the field of artificial intelligence

Keywords: digital environment; artificial origin; automated creation; digital transformation; synthetic media manipulation

Introduction

The rapid development of artificial intelligence technologies intense learning, has led to the emergence of deepfake – media content created or modified using algorithms that can realistically imitate real people's appearance, voice and behaviour. Using such content raises serious legal challenges in civil law, especially in the context of copyright and personal data protection. On the one hand, deepfake may infringe the copyrights of the creators of the original content used without permission or proper licensing; on the other hand, it raises questions about unacceptable interference with privacy and violation of the right to control one's image, voice or behavioural characteristics, which are protected as personal data. In this regard, there is a need to develop an effective legal mechanism that would ensure a balance between technology innovativeness and individuals' rights. The urgency of the problem is exacerbated by the lack of clearly defined approaches to qualifying violations committed with the help of deepfake technologies, making it difficult to bring to justice and effectively protect subjects' rights. At the same time, international practice demonstrates a variety of models

Suggested Citation:
Rezvorovych, K. (2025). Civil-law aspects of using deepfake content in the context of copyright and personal data protection. *Philosophy, Economics and Law Review*, 5(2), 8-16. doi: 10.63341/2786-491X-2025-2-08.

*Corresponding author

of legal regulation in this area, which creates preconditions for borrowing best practices and adapting them to national legislation. Therefore, the study of the civil law aspects of using deepfake content is of particular importance both in the scientific field and in the context of ensuring legal order in the digital environment.

An analysis of scientific sources on the civil law aspects of using deepfake content in the context of copyright and personal data protection allows to identify four key research areas. The first area covers the issues of digital transformation and cybersecurity. T. Kulchytskyi *et al*. (2024) analysed the legal framework for digital security, focusing on the need to adapt legislation to new digital challenges. A.A. Zavadskyi (2023) emphasised the need to regulate AI and deep synthesis technologies, including deepfake, considering the European experience. Further research should be complemented by the creation of a separate legal regime for artificially generated content, as well as an analysis of Ukrainian case law on diplomatic fakes. The second area focuses on the protection of personal data. For example, V. Ivkova & I. Opirskyi (2024) analysed the risks associated with the unauthorised collection and use of personal information in the OSINT context, which creates the basis for the abuse of deepfake technologies. N. Afshari & A. Mohammadi (2023) considered the violation of privacy due to the use of synthetic media and emphasise the need to expand legal mechanisms for protecting the individual. M.D. Murray (2024) examined the balance between the rights to privacy and publicity, proposing updated approaches to digital consent. In further research, it is advisable to pay attention to creating a unified digital identification mechanism and developing technical standards for verifying the authenticity of images.

The third area concerns copyright challenges. In particular, K. Tyagi (2023) offered an interdisciplinary analysis of the conflicts between copyright, moral rights, and deepfake technologies, paying attention to the limits of the permissible transformation of the original. C. Jasserand (2024) considered misleading headshots a threat to reputational rights, emphasising the legal uncertainty of the category of generated facial images. Aspects that have received insufficient attention include establishing clear criteria for originality in digital creativity and clarifying the user's role in generating synthetic content. The fourth area is international approaches to regulation. B. Van der Sloot & Y. Wagensveld (2022) described the challenges faced by law in the so-called "synthetic society" and justify the need for new norms. A. Wróbel (2024) analysed the Polish model of legal response to deepfake, noting its fragmentation even in the context of the GDPR. Y. Apolo & K. Michael (2024) raised the issue of the reliability of video evidence in court, pointing out the difficulties of examining deepfake content. A.C. Heugas (2021) compared the regulation of image rights in the US and the EU, emphasising the need to harmonise protection mechanisms. I. Aristova *et al*. (2020) substantiated the creation of specialiied courts to protect intellectual and personal rights in the digital environment. Aspects that have received insufficient attention include the unification of international liability standards for the use of deepfakes and the development of ethical codes for AI applications in the media.

Thus, the research analysis showed that the civil law aspects of using deepfake content require a comprehensive approach, including updating copyright laws, strengthening legal protection of privacy, adapting European standards, and developing effective judicial and regulatory mechanisms. Despite the growing interest in deepfake issues, several key aspects remain unresolved. In particular, the legal definition of deepfake content has not been formulated, which makes it impossible to qualify it as an object of copyright or related rights. The limits of transformation under which the created product is considered a derivative work are unclear, and there are no clear criteria for the legitimacy of using someone else's images, voice or stylistic features in digitally generated content. The legal status of such elements often remains outside the scope of current regulation, creating serious gaps in protecting personal non-property rights. The problem of automated content creation without the participation of a specific author has also been insufficiently studied, making it difficult to establish liability. The absence of deepfake labeling mechanisms, imperfect response procedures, and limited integration of international experience leave the field unregulated.

The purpose of the article was to substantiate the civil law approaches to regulating the use of deepfake content in the context of copyright and personal data protection, taking into account the challenges of the digital transformation of society. Objectives of the article were: to determine the technological nature, characteristics and forms of expression of deepfake content as a product of digital generation; to study the legal aspects of creating and using deepfake in the context of copyright and protection of personal non-property rights; to dentify gaps in current legislation and provide practical recommendations for improving legal protection mechanisms in the digital environment.

Materials and Methods

This research used a mixed methodological approach that combined traditional legal analysis with elements of interdisciplinary study. The main goal was to understand how deepfake technologies affect civil law, especially in the fields of copyright and personal data protection. The doctrinal legal method was used to study laws, legal concepts, and academic opinions. This method helped to analyse how current legal norms work and where there are gaps in regulating deepfakes. It also allowed for the identification of legal definitions that are still unclear or missing in national and international law.

A comparative legal method was also important. It was used to study how different countries respond to deepfake technologies. To identify existing gaps in the legal framework, a comparative analysis was conducted between current Ukrainian legislation (Civil Code of Ukraine, 2003; Law of Ukraine No. 2811-IX, 2022) and relevant international standards and doctrines.This approach enabled the systematic detection of discrepancies between existing legal regulations and the evolving requirements of the digital environment. By comparing laws from the EU, Germany, France and Ukraine, the research identified both common trends and differences. This helped to find possible legal solutions that could be adapted to the Ukrainian context. The content analysis method was used to study specific legal texts, such as international regulations (e.g., Regulation of the European Parliament and of the Council No. 2016/679, 2016 (GDPR); Regulation of the European Parliament and of the Council No. 2022/2065, 2022), draft laws (like the U.S. Congress Act No. H.R.5586, 2023), court decisions, and expert reports. Special attention was paid to documents that discussed image rights, biometric data, and the use of AI in media.

In addition, the systemic-structural approach helped to understand how different parts of the legal system (civil, media, digital, and data protection law) are connected when dealing with deepfake-related issues. It showed how legal problems often require solutions not from one area of law, but from several at once. The research materials were collected through academic databases like Scopus, HeinOnline, and Google Scholar, along with official publications from the European Commission, World Intellectual Property Organisation (WIPO), and Council of Europe. The study focused on legal and ethical risks related to the unauthorised use of personal images, voices, and behaviour in AI-generated content. The analysis included practical examples from court cases, legal commentaries, and national digital strategies. Altogether, this methodological framework allowed the research to build a clear picture of how legal systems respond to deepfake technologies and where improvements are needed to better protect intellectual and personal rights in the digital era.

Results and Discussion

Deepfake content is one of the most sophisticated manifestations of modern artificial intelligence technologies based on deep learning, in particular, generative adversarial networks (GANs), to create or modify images, video, and audio with high realism. Its technological nature is based on the automatic training of computer models on a large amount of data, which makes it possible to imitate facial expressions, intonations, movements, and other features of real people or objects. As a result, a new digital product may look identical to the real thing, although it is essentially a synthesised artificial object. Such content is actively used in various fields, from mass culture and advertising to educational programmes and cyber threats (Jasserand, 2024). Its functionality constantly expands: modern deepfake systems can adapt to voice samples, reproduce body language, synchronise lips with artificially generated speech, and automatically create a video sequence based on a text script. This provides flexibility in creating media products and, at the same time, raises concerns about its use in contexts of deception, manipulation, or invasion of personal space (Table 1).

Table 1. General characteristics, forms and functionalities of deepfake content

Feature	Contents	Application examples
Technological basis	Generative deep learning algorithms, including GANs, autoencoders, neural networks	Using GANs to create videos with new faces based on samples
Types of content	Video, audio, images, combined multimodal content	Voice replacement in audio, face overlay in real video
Forms of expression	Full generation (creation from scratch), partial modification (replacement of individual elements), motion simulation	Animation of historical figures, synthesis of famous people's addresses
Functional features	Lip synchronisation, intonation imitation, emotion generation, speech adaptation	Automatic dubbing of videos with other voices, creation of deep narratives
Purposes of use	Entertainment, advertising, art, education, disinformation, cyberattacks	Social apps for creating video memes, fake political appeals

Source: compiled by the author on the basis of A. Lee & P. Woo (2022), A.A. Zavadskyi (2023), N. Afshari & A. Mohammadi (2023), M.D. Murray (2024)

In practice, deepfake content is actively used in the open media space and specialised services. In the entertainment industry, mobile applications that allow users to interactively change their faces in photos or videos or duplicate the voices of celebrities have become popular. In digital art, deepfake creates immersive installations and visual content that would be impossible to realise using traditional means. For example, Lucasfilm, in the movie Star Wars: The Rise of Skywalker, used deepfake technologies to "restore" actress Carrie Fisher, who died before the end of filming (Screen Rant, 2019). Another striking example is the Reface (n.d.) platform, developed by Ukrainian experts, which allows users to change faces in videos using neural networks and has become globally

popular due to the simplicity and high quality of content generation. At the same time, along with the positive developments, there has been a sharp increase in the number of fake appeals by public figures, manipulative videos in information campaigns, and commercials created without the parties' consent. For example, in 2022, a video was circulated in which the President of Ukraine, Volodymyr Zelenskyy, allegedly called for surrender; this deepfake was quickly exposed, but the fact of its appearance became an example of an information attack in wartime (Allyn, 2022). As a result, deepfake content appears as a technologically advanced but legally ambiguous digital product that combines the potential for innovation with a high risk of violating ethical and legal norms.

The legal use of other people's works when creating deepfake content requires a clear distinction between primary and derivative copyrighted works. Since most deepfake products are based on existing audio, video, or visual materials, the key question is whether the result of the generation is a new work subject to legal protection or a derivative work requiring the permission of the copyright holder (Lee & Woo, 2022). The degree of transformation, the level of creative contribution, the nature of use, and the purpose of creation play a crucial role in determining the legal status. Particularly difficult are cases where content is created automatically, without clear authorship, which gives rise to legal conflicts in the field of intellectual property. To summarise approaches to the classification of such objects, it is advisable to analyse the types of deepfake content in terms of source, form of processing, and legal consequences (Table 2).

Table 2. Legal classification of deepfake content in relation to primary and derivative works

Type of material used	Signs of the legal status of the created content	Terms of legitimate use	Application examples
Copyrighted work (video, music, images)	Derivative work, provided that the structure or image of the work is preserved in a modified form	Requires permission of the copyright holder; may be licensed or quoted in accordance with the law	Replacing an actor's face in a movie clip or re-arranging a music video
Fragments from the public domain or works whose protection period has expired	New or derivative work, depending on the scope of the transformation	Free use is allowed in the absence of restrictions	Creating a video based on works of the nineteenth century or historical documents
Individual elements of the work (image, style, voice, facial expressions)	Mixed status: can be recognised as either a new work or an infringing interpretation	Depends on the level of originality, transformation and commercial use	Generate a promotional video using the style or visual code of a famous movie
Full generation of new content without direct copying	May be considered a primary work if it is the original result of creative activity	Does not require consent unless related or personal rights of third parties are violated	Creating a video based on a text description using generative AI
Combined use of several sources	Mostly classified as a derivative work; the level of modification is important	May require permissions for each element used	Mix audio and video fragments from different sources into a new video

Source: compiled by the author on the basis of A. Lee & P. Woo (2022), K. Tyagi (2023), C. Jasserand (2024), A. Wróbel (2024)

In practice, the legal status of deepfake products remains ambiguous, as each case requires an individual assessment, considering the content sources used, the nature of the transformation, and the presence of a commercial purpose. As part of the legal regulation in Ukraine, there are currently no special rules directly related to deepfake content. However, the general provisions of the Law of Ukraine No. 2811-IX (2022), as well as articles of the Civil Code of Ukraine (2003) regulating the right to work and the procedure for using derivative works, apply. In particular, Article 433 of the Civil Code of Ukraine stipulates that the object of copyright is works expressed in an objective form, including audiovisual, computer and other products created by creative labor. Suppose deepfake content is created by modifying an existing protected work. In that case, it is classified as a derivative and requires the right holder's consent by Article 440 of the Civil Code of Ukraine.

At the international level, no separate regulatory act is dedicated to the legal status of deepfake content. At the same time, the provisions of the Berne Convention for the Protection of Literary and Artistic Works (1979) apply, according to which the author has the exclusive right to authorise adaptations, translations, and other modifications of his or her work. Within the framework of WIPO, there are Treaties on Copyright (WIPO Copyright Treaty, 1996) and Performances of Phonograms (WIPO Performances and Phonograms Treaty, 1996), which recognise digital forms of use of works and cover protection in the digital environment. The European Union, although not directly regulating deepfake, introduced the Regulation of the European Parliament and of the Council No. 2022/2065 (2022) and the Regulation of the European Parliament and of the Council No. 2021/0106 (2021), which set requirements for transparency of digital content, including that created using generative models,

and provide for liability for infringement of intellectual property rights in the digital space (Tyagi, 2023). Thus, the legal framework is gradually adapting to new challenges. However, legal uncertainty remains, which requires further development at both the national and international levels, with a clear distinction between primary and derivative digital works generated with the participation of artificial intelligence. In the context of the proliferation of deepfake content, the effectiveness of legal protection mechanisms in reproducing a person's appearance, voice or behavioural traits without their consent becomes particularly relevant. Such actions may violate personal non-property rights, including the right to image, voice, privacy and dignity. Different jurisdictions develop their approaches to responding to these judicial and administrative violations. For a scientific assessment, it is appropriate to compare Ukrainian and European law enforcement experience (Table 3).

Table 3. Protection of personal non-property rights in the context of deepfake: Ukrainian and European experience

Jurisdiction	Types of violations	Protection mechanisms
Ukraine	1. Unauthorised use of a person's image in deepfake content. 2. Imitation of voice for commercial purposes	1. Claim for protection of the right to the image, demanding a ban on distribution. 2. Appeal to the court or regulator regarding the violation of the individualisation of a person
France	Voice imitation for commercial use without consent	Administrative response, removal of content, notification of the subject
Germany	Using the appearance of a public figure without participation in the project	Court ban on video distribution, compensation for non-pecuniary damage
EU	Processing of personalised deepfake content by without the person's consent	Filing a complaint with the national regulator, exercising the "right to be forgotten"

Source: compiled by the author on the basis of German Civil Code (2002), Civil Code of Ukraine (2003), CNIL (2022), N. Afshari & A. Mohammadi (2023), A. Wróbel (2024), Code of Relations Between the Public and the Administration (2024), EU Data Protection Authorities (DPA) (2024)

In the European Union, in addition to the Regulation of the European Parliament and of the Council No. 2016/679 (2016), case law and the practice of national regulators are relevant (Van der Sloot & Wagensveld, 2022). In France, for example, in 2022, the National Commission for Informatics and Liberties considered a case of using a deepfake voice to fraudulently use online advertising, ordering the company to remove the content and notify the victims of the fake (CNIL, 2022; Code of Relations Between…, 2024). In Germany, a court ordered an online platform to remove a deepfake video featuring a well-known TV presenter, although she had never participated in the project (German Civil Code, 2002). Both examples demonstrated the real-world application of judicial and administrative protection mechanisms, even in complex digital environments. In Ukraine, the Law of Ukraine No. 2297-VI (2010) defines the basic principles of processing, storage, and use of personal information, including biometric data such as facial images and voice samples. However, it does not explicitly regulate the use of synthetically generated representations created by AI systems. This creates a legal vacuum where the protection of personal data in deepfake contexts is limited to general norms and does not ensure direct liability for algorithmic misuse of identity features (Law of Ukraine No. 2297-VI, 2010). Consequently, Ukrainian regulators and courts still rely on broad interpretations of privacy and image rights to address cases of AI-generated content infringement.

At the international level, a key initiative is the U.S. Congress Act No. H.R.5586 (2023), which proposed mandatory digital watermarks and disclosure requirements for synthetically created visual and audio content. The Act introduced obligations for content producers and platforms to label AI-generated materials and establishes civil liability for intentional distribution of unlabeled deepfakes that may cause harm to an individual's reputation or privacy. Although still under consideration, this approach reflects a trend towards the global institutionalisation of transparency standards in AI media governance. Thus, the practice of Ukraine and EU countries indicates the growing importance of the non-property component of digital identity and the need to develop specialised procedures for rapid response to violations by deepfake content.

Despite the existence of general legal norms in the field of intellectual property, personal data and non-property rights protection, the current legislation of Ukraine does not ensure proper regulation of the specifics of the use and distribution of deepfake content. The absence of a legal definition of this phenomenon makes it impossible to unambiguously qualify it as an object of an offense or legal relationship, complicating the application of existing rules in practice (Petrovskyi *et al*., 2025). Comparative legal studies confirm that a similar gap exists even in advanced jurisdictions, where regulatory fragmentation and the absence of unified standards hinder effective accountability for synthetic media dissemination. J. Meskys *et al*. (2020) highlighted the challenges posed by dispersed regulatory frameworks, while A. Fabuyi *et al*. (2024) emphasised the limitations of current standards in ensuring compliance.

Determining the legal status of persons who initiate the creation of deepfakes remains problematic, especially in the case of automated generative systems, when the issue of authorship and liability becomes legally blurred. According to A. Busacca & M.A. Monaca (2023), this ambiguity also extends to determining intent and purpose in the creation of AI-generated materials, which complicates distinguishing artistic innovation from manipulative or defamatory use. Also, current legislation does not set limits on the permissible transformation of primary works in the digital environment, which creates risks for both the copyright and moral rights of third parties (Wróbel, 2024).

A significant gap was observed in the mechanisms for identifying the source of deepfake content, which is critical for proving the fact of infringement in court which correlates with the conclusions made by N. Afshari & A. Mohammadi (2023). Empirical evidence has shown that the lack of transparent labeling mechanisms substantially reduces victims' ability to prove identity misuse, particularly in cases of non-consensual intimate content or political disinformation (Mania, 2024; Romero Moreno, 2024). In addition, there are no regulatory requirements to label or disclose the artificial origin of visual or audio content, which limits the transparency of the digital environment (Murray, 2024). Public perception research indicates that societies without explicit labeling rules are more tolerant of synthetic representations, underestimating their manipulative potential as stated by M.B. Kugler & C. Pace (2021).

An additional threat is the low level of public awareness of the technological characteristics and potential risks of deepfake, which increases vulnerability to manipulation and disinformation (Ivkova & Opirskyi, 2024). Therefore, as A. Fabuyi *et al*. (2024) emphasised, public education and awareness-raising campaigns play a decisive role in preventing harmful use of deepfakes in media and entertainment ecosystems. As a result, law enforcement practice is forced to rely on general rules that do not take into account the technological complexity, speed of dissemination, and social danger of deeply generated content, which requires the development of specialised legislative provisions.

To ensure effective protection of intellectual and personal rights in the context of the spread of deepfake technologies, it is advisable to initiate the development of a comprehensive legal category of deepfake content as a separate object of digital legal relations. At the legislative level, a clear definition of such content should be introduced, taking into account the method of its creation, the purpose of its use, and the level of transformation of primary works or personal characteristics. It is necessary to provide for mandatory labeling of artificially generated content containing a reproduction of a person's image or voice, as well as liability for its distribution without informed consent. In the field of copyright, it is advisable to regulate the legal status of derivative works created using deep learning algorithms, with requirements for obtaining permission from the copyright holder or the person whose identity elements are used. It is also recommended that a procedurally simplified procedure be provided for responding to violations, including the possibility of filing applications with digital platforms and relevant data protection authorities to promptly block or remove content. In addition, at the level of international cooperation, it is advisable to initiate the unification of approaches to the legal regulation of deepfake, taking into account EU standards and Council of Europe practice, which will contribute to legal certainty and strengthen interstate responsibility in the digital environment.

Conclusions

In the course of this research, thr appropriate conclusion would be that deepfake content is not just a technological novelty, but a serious legal challenge that current civil law systems are not yet ready for. As deep learning algorithms continue to develop, they give rise to complex digital products that can reproduce human appearance, voice, and behaviour with impressive accuracy. At the same time, this progress brings with it significant legal risks – particularly in the areas of copyright and the protection of personal non-property rights. Based on the analysis, it was found that Ukrainian legislation does not yet provide a clear legal definition of deepfake content, which complicates its qualification in legal disputes. This makes it difficult to clearly separate what is a derivative work from what could be considered a violation of moral or copyright rights. Moreover, there are no detailed rules for how consent should be obtained when someone's face or voice is used in AI-generated content.

The absence of labeling requirements (such as an obligation to indicate when a video or voice recording was generated by AI) only deepens the problem. Without such transparency, it is almost impossible for ordinary users or even courts to distinguish real content from synthetic. In Ukraine's current legal context, where many digital challenges are still unregulated, this creates space for potential abuses – especially in times of war, when information security plays a key role. In comparison with European practice, Ukraine could benefit from adapting certain tools, such as simplified takedown procedures, the "right to be forgotten" in relation to deepfakes, and rules from the upcoming EU Artificial Intelligence Act. It is also worth considering the creation of specialised judicial or administrative procedures to quickly respond to violations caused by the use of synthetic content.

To summarise, it was recommend developing a full-fledged legal category of deepfake content within civil law, which would regulate its definition, the degree of permissible transformation, and requirements for consent. The issue of authorship in AI-generated works also needs

attention, especially in cases where content is produced automatically and without direct human input. Further research should focus on real case studies, technical tools for verifying content authenticity, and possible cooperation with digital platforms that host user-generated media. Only through a combination of legal, technical, and ethical approaches can the society build an effective system to protect people's rights in the digital environment.

Acknowledgements
None.

Funding
None.

Conflict of Interest
None.

References
[1] Afshari, N., & Mohammadi, A. (2023). The legal implications of deepfake technology: Privacy, defamation, and the challenge of regulating synthetic media. *Legal Studies in Digital Age*, 2(2), 13-23.
[2] Allyn, B. (2022). *Deepfake video of Zelenskyy could be "tip of the iceberg" in info war, experts warn*. Retrieved from https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia.
[3] Apolo, Y., & Michael, K. (2024). Beyond a reasonable doubt? Audiovisual evidence, AI manipulation, deepfakes, and the law. *IEEE Transactions on Technology and Society*, 5(2), 156-168. doi: 10.1109/TTS.2024.3427816.
[4] Aristova, I., Rezvorovich, K., Sydorova, E., Nesterchuk, L., & Kislitsyna, I. (2020). Creation of an intellectual property court in Ukraine: Protection of intellectual property rights in a system of economic security of a country. *Journal of Security and Sustainability Issues*, 9, 362-380. doi: 10.9770/jssi.2020.9.m(29).
[5] Berne Convention for the Protection of Literary and Artistic Works. (1979, September). Retrieved from https://www.wipo.int/treaties/en/ip/berne/.
[6] Busacca, A., & Monaca, M.A. (2023). Deepfake: Creation, purpose, risks. In D. Marino & M.A. Monaca (Eds.), *Innovations and economic and social changes due to artificial intelligence: The state of the art* (pp. 55-68). Cham: Springer. doi: 10.1007/978-3-031-33461-0_6.
[7] Civil Code of Ukraine. (2003, January). Retrieved from https://zakon.rada.gov.ua/laws/show/435-15#Text.
[8] CNIL. (2022). Retrieved from https://www.cnil.fr/fr.
[9] Code of Relations Between the Public and the Administration. (2024, July). Retrieved from https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000031366350/.
[10] EU Data Protection Authorities (DPA). (2024). Retrieved from https://www.enforcementtracker.com/.
[11] Fabuyi, J., Olaniyi, O.O., Olateju, O., Aideyan, N.T., Selesi-Aina, O., & Olaniyi, F.G. (2024). Deepfake regulations and their impact on content creation in the entertainment industry. *Archives of Current Research International*, 24(12), 52-74. doi: 10.9734/acri/2024/v24i12997.
[12] German Civil Code. (2002, January). Retrieved from https://surl.li/zqggxo.
[13] Heugas, A.C. (2021). Protecting image rights in the face of digitalisation: A United States and European analysis. *The Journal of World Intellectual Property*, 24(5-6), 344-367. doi: 10.1111/jwip.12194.
[14] Ivkova, V., & Opirskyi, I. (2024). Research on the problem of ensuring personal data and confidential information security in the context of OSINT counteraction. *Cybersecurity: Education, Science, Technology*, 26(2), 189-199. doi: 10.28925/2663-4023.2024.26.682.
[15] Jasserand, C. (2024). Deceptive deepfakes: Is the law coping with AI-altered representations of ourselves? In *2024 international conference of the Biometrics Special Interest Group (BIOSIG)* (pp. 1-4). Darmstadt: IEEE. doi: 10.1109/BIOSIG61931.2024.10786729.
[16] Kugler, M.B., & Pace, C. (2021). Deepfake privacy: Attitudes and regulation. *Northwestern University Law Review*, 116(3), 611-652. doi: 10.2139/ssrn.3781968.
[17] Kulchytskyi, T., Rezvorovych, K., Povalena, M., Dutchak, S., & Kramar, R. (2024). Legal regulation of cybersecurity in the context of the digital transformation of Ukrainian society. *Lex Humana*, 16(1), 443-460.
[18] Law of Ukraine No. 2297-VI "On Personal Data Protection". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text.
[19] Law of Ukraine No. 2811-IX "On Copyright and Related Rights". (2022, December). Retrieved from https://zakon.rada.gov.ua/laws/show/2811-20#Text.
[20] Lee, A., & Woo, P. (2022). Copyright law should stay true to itself in the age of artificial intelligence. In R. Abbot (Ed.), *Research handbook on intellectual property and artificial intelligence* (pp. 179-197). Cheltenham: Edward Elgar Publishing. doi: 10.4337/9781800881907.00015.
[21] Mania, K. (2024). Legal protection of revenge and deepfake porn victims in the European Union: Findings from a comparative legal study. *Trauma, Violence, & Abuse*, 25(1), 117-129. doi: 10.1177/15248380221143772.
[22] Meskys, E., Kalpokienė, J., Jurcys, P., & Liaudanskas, A. (2020). Regulating deep fakes: Legal and ethical considerations. *Journal of Intellectual Property Law & Practice*, 15(1), 24-31. doi: 10.1093/jiplp/jpz167.

[23] Murray, M.D. (2024). Deceptive exploitation: Deepfakes, the rights of publicity and privacy, and trademark law. *IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property*, 65(2), 124-210. doi: 10.2139/ssrn.4981531.
[24] Petrovskyi, A., Kyrdan, B., & Kutsyk, K. (2025). Implementation of artificial intelligence in civil proceedings: Experience of EU countries. *Scientific Journal of the National Academy of Internal Affairs*, 30(1), 45-59. doi: 10.63341/naia-herald/1.2025.45.
[25] Reface. (n.d.). Retrieved from https://reface.ai/.
[26] Regulation of the European Parliament and of the Council No. 2016/679 "On the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)". (2016, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[27] Regulation of the European Parliament and of the Council No. 2021/0106 "On Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts". (2021, April). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.
[28] Regulation of the European Parliament and of the Council No. 2022/2065 "On a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act)". (2022, October). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/2065/oj.
[29] Romero Moreno, F. (2024). Generative AI and deepfakes: A human rights approach to tackling harmful content. *International Review of Law, Computers & Technology*, 38(3), 297-326. doi: 10.1080/13600869.2024.2324540.
[30] Screen Rant. (2019). Retrieved from https://screenrant.com/star-wars-9-carrie-fisher-footage/.
[31] Tyagi, K. (2023). Deepfakes, copyright and personality rights: An inter-disciplinary perspective. In *Law and economics of the digital transformation. ILEC 2023. Economic analysis of law in European legal scholarship* (pp. 191-210). Cham: Springer. doi: 10.1007/978-3-031-25059-0_9.
[32] U.S. Congress Act No. H.R.5586 "Deepfakes Accountability Act". (2023, September). Retrieved from https://www.congress.gov/bill/118th-congress/house-bill/5586.
[33] Van der Sloot, B., & Wagensveld, Y. (2022). Deepfakes: Regulatory challenges for the synthetic society. *Computer Law & Security Review*, 46, article number 105716. doi: 10.1016/j.clsr.2022.105716.
[34] WIPO Copyright Treaty. (1996, December). Retrieved from https://www.wipo.int/treaties/en/ip/wct/.
[35] WIPO Performances and Phonograms Treaty. (1996, December). Retrieved from https://www.wipo.int/treaties/en/ip/wppt/.
[36] Wróbel, A. (2024). Can GDPR and copyright law stop deepfake? A comprehensive legal analysis of the deepfake phenomenon and liability for the deepfake in the Polish legal system. *Młody Jurysta*, 1, 22-39. doi: 10.21697/mj.14572.
[37] Zavadskyi, A.A. (2023). On the legal regulation of artificial intelligence for deep content synthesis and deepfakes: European experience and prospects for its application in Ukraine. In *Integration of higher education of Ukraine into the European educational space in the conditions of martial law* (pp. 69-72). Lomza-Kharkiv: MANS.

Цивільно-правові аспекти використання deepfake-контенту в контексті авторського права й захисту персональних даних

Кристина Резворович
Доктор юридичних наук, доцент
Дніпровський державний університет внутрішніх справ
49005, просп. Науки, 26, м. Дніпро, Україна
https://orcid.org/0000-0003-1183-613X

Анотація. Актуальність дослідження зумовлена нестримним розвитком генеративних технологій, що дають змогу створювати глибоко змінений або повністю синтезований контент за допомогою штучного інтелекту, зокрема deepfake. Такий контент не лише створює ілюзію достовірності, а й ставить під загрозу дотримання прав інтелектуальної власності й особистих немайнових прав, викликаючи суттєві правові виклики в цифровому середовищі. Мета статті полягала у формулюванні й обґрунтуванні цивільно-правових підходів до врегулювання використання deepfake-контенту в контексті авторського права та захисту персональних даних з урахуванням викликів цифрової трансформації суспільства. У межах дослідження використано методи системного аналізу, логіко-юридичного узагальнення, формально-юридичний метод, а також метод порівняльного правознавства з урахуванням міжнародних норм і доктринальних джерел. Установлено, що чинне українське законодавство не містить окремого поняття deepfake-контенту, а наявні правові механізми є фрагментарними й не охоплюють усіх аспектів відповідальності за його створення та поширення. Виявлено прогалини в регулюванні статусу похідних цифрових творів, захисту біометричних ознак особи, а також у процедурі встановлення правопорушника в умовах автоматизованої генерації контенту. Доведено, що без належного нормативного реагування deepfake-технології можуть використовуватися як інструмент маніпуляцій, підміни ідентичності й цифрової дискредитації. Дослідження підкреслило необхідність міждисциплінарного підходу, що поєднує юридичні, технічні й етичні аспекти регулювання deepfake. Особливу увагу приділено проблематиці юридичної відповідальності в разі автоматизованого створення контенту без безпосередньої участі автора. Акцент зроблено також на важливості цифрової прозорості й інформованої згоди як ключових принципів правового врегулювання. Результати дослідження можуть бути використані для вдосконалення національного законодавства та розроблення міжнародних правових механізмів у сфері штучного інтелекту

Ключові слова: цифрове середовище; штучне походження; автоматизоване створення; цифрова трансформація; синтетична маніпуляція медіа