Teka Komisji Prawniczej PAN Oddział w Lublinie
vol. XVIII, 2025, no. 2, pp. 35–49
https://doi.org/10.32084/tkp.10243

DEEPFAKE AND SELECTED CRIMES IN POLISH AND GERMAN CRIMINAL LAW

Dr. Iwona Bień-Węgłowska

The John Paul II Catholic University of Lublin, Poland
e-mail: iweglowska@kul.pl; https://orcid.org/0000-0002-8575-8085

Dr. habil. Ewa Tuora-Schwierskott, University Professor

Jan Długosz University in Częstochowa, Poland
e-mail: e.tuora-schwierskott@ujd.edu.pl; https://orcid.org/0000-0003-0926-2173

Abstract. This study examines the issue of deepfake technology, with particular emphasis on its mechanisms, applications, and the potential threats it poses in various areas of social life. It outlines the elements of prohibited acts that may be committed by individuals who create or distribute deepfake content. The aim of the article is to analyse the deepfake phenomenon in the context of selected provisions of the Polish Penal Code, as well as in light of the relevant provisions of German criminal law. In addition, the article discusses the provisions contained in the Artificial Intelligence Act, which establish a system of protection against the malicious use of deepfake technology based on transparency obligations. The study provides an assessment of the applicable provisions of Polish and German criminal law with regard to the protection of persons who may be harmed by the dissemination of deepfake content, and also evaluates the regulatory framework adopted at the EU level.

Keywords: Polish Penal Code; German Penal Code; Artificial Intelligence Act; deepfake; manipulation.

INTRODUCTION

Accelerated technological progress gives rise to completely new, previously unknown threats related to the creation of a false image of reality. Manipulation of information has now taken on a particularly dangerous form; content, such as videos, images and sounds generated by artificial intelligence, known as deepfakes, has become a tool for spreading misinformation, while it is not always possible to verify the authenticity of content. Deepfakes are not a uniform phenomenon – their harmfulness depends on the context of the content created. Deepfake technology is used in applications ranging from the entertainment industry to education, but is most often used to produce

ISSN 1899-7694
e-ISSN 2719-7379

fake pornographic films; deepfake recordings are also used as an instrument of blackmail and fraud. Rising concerns over deepfakes are prompting calls for legislative action at both national and EU levels.

The aim of the present article is to analyse the phenomenon of deepfakes in the context of selected provisions of the Polish Penal Code[1] (Articles 190a(2), 191a, 212 and 216) and to highlight the risk that this technology may be used to commit other crimes, such as fraud (Article 286 PC) or coercion (Article 191(1) PC). Issues associated with deepfakes are also analysed in the light of German criminal law, especially with regard to such crimes as insult, defamation, slander, violation of the protection of private life and infringement of personal rights by taking photos. A proposal to introduce a new legal regulation on combating deepfakes into the German Penal Code is also presented.[2]

Moreover, the article discusses the provisions of the EU Regulation – the Artificial Intelligence Act (AI Act)[3] regarding deepfake content, a legal definition of deepfakes, and provisions creating a system of protection against harmful uses of deepfakes based on transparency obligations.

The present paper assesses the applicable provisions of Polish and German criminal law concerning the protection of persons potentially harmed by the dissemination of deepfake content, as well as evaluating the regulations adopted at the EU level.

1. THE ESSENCE OF THE DEEPFAKE PHENOMENON

Deepfake is a technology that uses artificial intelligence systems to generate or modify images, sounds or video recordings so that they ultimately depict something that did not actually happen. In practice, deepfake technology is most often used to publish videos online that are intentionally fake but appear authentic. The term deepfake is a combination of two English words: "deep" – profound and "fake" – false. The first element of the name "deep" comes from the term deep learning, which denotes a machine learning method (an artificial intelligence technology) that uses multi-layer neural networks to independently analyse and recognise data in order to effectively solve complex tasks such as image recognition, natural language processing, speech analysis or content

[1] Act of 6 June 1997, the Penal Code, Journal of Laws of 2025, item 383 [hereinafter: PC].

[2] Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322).

[3] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (hereinafter referred to as the Artificial Intelligence Act). OJ EU.L.2024.1689 of 2024.07.12, LEX/el. 2025 [hereinafter: Artificial Intelligence Act or AI Act].

generation. A deepfake is a highly realistic falsification created with advanced technology that is difficult for recipients to recognise as false.

Deepfake technology uses an algorithm called GAN – generative adversarial networks – to replace a real image or video of a person with a fake image or video. One of the advantages of GANs is that they can learn from a given dataset [Almars 2021, 24-25]. GANs consist of two main AI systems – the first is called a generator, the second is a discriminator [Dąbrowska 2020, 90]. The generator creates fake images, videos, or sounds in an attempt to imitate real-life data. The discriminator determines whether the generated content comes from the generator and is real. The entire process iteratively improves both networks, resulting in the generator becoming better at creating realistic images and the discriminator becoming better at detecting them. This leads to the creation of images and videos that look very realistic, and are produced entirely by artificial intelligence [Rajtar 2025, 194].

The growing use of deepfake technology in a wide range of sectors is facilitated by widespread access to tools and software capable of sophisticated visual and audio manipulation. Deepfakes can now be easily created using applications that change a person's face and voice, synchronise facial expressions and lip movements with a selected audio track, generate voices that imitate specific individuals, or create character animations based on photographs.

Currently, there are three basic types of deepfake creations: Face Swapping, Voice Swapping and Body Puppetry. In recent years, several AI-based methods have been developed to manipulate faces in videos. They are used to replace faces in a film, control a person's lip movements, facial expressions and head or synthesise new (pseudo) identities in order to in order to seamlessly integrate an actor's face into existing footage. This method, called Face Swapping, allows one to create fake videos in which a person makes statements they have never made in real life. This effect is achieved by reconstructing a three-dimensional face model based on a video stream. The manipulator can then freely control the footage based on subsequent video frames and create deceptively realistic facial expressions in the target individual.

Deepfake software can also be used to reconstruct a person's voice (Voice Swapping). For example, politicians can be digitally manipulated to appear to say words they have never spoken. This technology can also become a problem in business; in certain circumstances, fraudsters can create audio recordings with the voices of key employees to order a money transfer over the phone, etc. It is also possible to transfer individual movements or even entire movement sequences from filmed material onto another person. This form of deepfake is called body puppetry [Gradek-Lewandowska 2020].

Due to the fact that deepfake technology was designed as a falsification instrument, it is inherently associated with destructive potential [Kiełpiński 2023, 97]. This technology contributes to numerous abuses,

including attempts at electoral manipulation, discrediting politicians, creating pornographic content (so-called deep porn), and catalysing financial fraud schemes. The list of harmful uses of deepfakes is long and growing. Deepfakes are considered a powerful instrument of misinformation, and their appearance in public space reduces trust in the media, increases the feeling of insecurity among citizens and threatens the functioning of democratic societies. On the other hand, deepfakes can also have positive applications, e.g. in education, entertainment or tourism [Łabuz 2024, 784].

Due to the widespread and ever-increasing use of deepfake technology, which poses a threat in many areas of social and economic life, both researchers and practitioners have initiated a debate on the rules for creating and using deepfake content. Attempts to define this phenomenon have resulted in scientific studies focusing primarily on audio and visual forms of deepfakes, omitting textual forms. This understanding of deepfakes is also related to the belief, firmly established in the public consciousness, that this technology is primarily a tool that enables the impersonation of another person's identity using generated images and sounds [ibid., 787].

2. EU LEGAL FRAMEWORK FOR DEEPFAKE TECHNOLOGY

EU legislators have also recognised the threat posed by the widespread use of deepfake technology and have introduced procedures to protect citizens from manipulation and misinformation. These procedures are provided for in the Artificial Intelligence (AI) Act, which officially entered into force on 1 August 2024. The AI Act is the first legal solution in the world to establish a comprehensive legal framework specifying harmonised rules for the creation, use and dissemination of AI systems. In principle, the AI Act takes effect on 2 August 2026, although the application of individual provisions is deferred and will follow the timetable set by the EU legislator (Article 113 AI Act).

The AI Act introduces a legal definition of deepfake, which plays a key role in regulating the creation of synthetic content and is also important for conducting in-depth scientific research and legal analysis. According to Section 3(60) AI Act, "'deep fake' means AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful." Importantly, the definition of deepfake focuses mainly on audio and visual forms. And although it is not limited to a specific medium, it does not apply to textual forms. The legislator's position in this respect is consistent with the views of the doctrine, in which the belief dominates that focusing solely on audio and visual content more accurately reflects the essence of the a deepfake [Łabuz 2024, 787].

The EU legislator has classified deepfake technology as a limited-risk system, making it necessary to implement transparency obligations under Article 50(2) and (4) AI Act. The AI Act establishes a transparency obligation on two levels. First, it requires AI system providers to mark AI-generated and manipulated content in a machine-readable format (Article 50(2) AI Act), secondly, it requires entities using AI systems to disclose only deepfake content and texts published for the purpose of informing the public about matters of public interest (Article 50(4) AI Act). Recital 133 AI Act provides an open catalogue of technical solutions for tracing the origin of information, including the use of watermarks, metadata identification, watermarks, metadata identifications, cryptographic methods for proving provenance and authenticity of content, logging methods,, digital fingerprints and other effective techniques for identifying synthetic content. It can be assumed with a high degree of certainty that transparency obligations will be fulfilled through disclosure of information and the use of watermarks [Łabuz 2023, 23]. The provisions of Article 50(2) and (4) AI Act also introduce exceptions to the obligation to mark deepfake content by AI system providers and entities using a specific AI system. Failure to comply with the transparency obligations imposed by the AI Act is subject to administrative fines as defined in Article 99 AI Act.

It should be emphasised that the provisions of the AI Act require providers of AI systems to mark content generated and manipulated by AI and provide for the obligation for entities using AI systems to disclose deepfake content, but do not provide for the obligation to remove such content from virtual space. Certainly, the use of technical solutions, such as watermarks, and the inclusion of relevant information can help identify deepfake content, but it will not solve the problem of malicious intent behind the creation and dissemination of deepfakes. Even when watermarked, falsified content can still be distributed to mislead recipients, hoping that many will miss or misunderstand the watermark [Lisińska and Castro 2024]. Moreover, the principle of transparency does not provide protection for individual victims of deepfake technology, because the AI Act only provides legal protection to recipients of content created or manipulated by AI, and does not refer in this respect to persons to whom deepfake technology may have caused serious harm.

The AI Act is not the only EU act regulating the issue of deepfakes. Article 35(3)(k) of the Digital Services Act imposes an obligation on providers of very large online platforms and very large online search engines to identify and mitigate the risks associated with the dissemination of artificially generated or manipulated content, such as deepfakes.[4] However, as far

[4] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the single market for digital services and amending Directive 2000/31/EC (Digital Services Act), OJ EU.L.2022.277.1 of 2022.10.27. Lex/el. 2025 [hereinafter: Digital Services Act or DSA].

as personal data and their misuse for deepfakes are concerned, the limitations and requirements apply concerning the right to respect for private and family life contained in Article 8 of the European Convention on Human Rights (ECHR)[5] and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (GDPR).[6]

3. DEEPFAKE AND SELECTED CRIMES IN POLISH CRIMINAL LAW

Polish criminal law does not directly address the problem of deepfake; the terms deepfake or deep porn do not feature in Polish criminal legislation at all. It should be noted, however, that deepfake technology is a tool for creating and disseminating false content, which inherently implies the intentional falseness of the effects of its action (the intention to mislead) [Szpyt 2019, 79], and as such is punishable by Polish criminal law for falsification of reality. It is therefore necessary to pay attention to the purpose for which deepfakes are used, in what context they occur, and what consequences they bring about [Mamak 2020]. Taking the above into account, it should be stated that the use of deepfake technology may constitute a crime, and the legal problems arising in this context may be resolved under criminal law in terms of the criminal liability of their creators and those who disseminate them.

In the context of deepfake technology, identity theft constitutes one of the primary offences of concern. It is now firmly embedded in public discourse that deepfakes function predominantly as tools for impersonating another person's identity through the generation or manipulation of visual and audio content. The Penal Code penalises identity theft in Article 190a(2).[7] This act involves impersonating another person, using their image, other personal data or other data by which they are publicly identified in order to cause property or personal damage to them. Due to the fact that the legislator used the words "person" and "personal data" in the provision, it must be assumed that only the identity of a natural person is at stake, and the perpetrator must impersonate another, actually existing person, not a fictitious one (e.g. a literary character)

---

[5] Journal of Laws 1993, No. 61, item 284, Lex/el. 2025.

[6] OJ EU.L.2016.119.1, Lex/el. 2025.

[7] Article 190a PC states: "§ 1. Whoever, by persistently harassing another person or their closest relative, causes in that person a sense of threat, humiliation or torment that is justified by the circumstances, or significantly violates that person's privacy, shall be subject to the penalty of deprivation of liberty for a term of between 6 months and 8 years. § 2. The same penalty shall apply to anyone who, impersonating another person, uses his or her image, other personal data or other data by means of which he or she is publicly identified, thereby causing property or personal damage to that person."

and only a living person [Mozgawa 2025a]. As for the definition of the term "image", the Dictionary of the Polish Language provides two meanings: "someone's likeness in a drawing, painting, photograph, etc." and "the way in which a person or thing is perceived and represented."[8] Mozgawa emphasises that under Article 190a(2) PC, both meanings of the word "image" will be taken into account, and the use by the legislator of the term "image or other personal data" means that the image is part of personal data [ibid.].

The conduct consisting in the perpetrator taking actions as another person meets the criteria of the crime under Article 190a(2) PC [Zoll 2017, 592]. The doctrine emphasises that impersonation is pretending to be another person, misleading others about one's identity, and presenting oneself as someone else [Lachowski 2023a, 1020]. It can therefore be stated that impersonation is directly linked to the perpetrator and requires them to adopt someone else's identity, whereas in the case of deep porn production we are dealing with a "combination of images" of two different people without the perpetrator adopting their personality. In this situation, due to the lack of the element of impersonation, a perpetrator who creates false pornography (deep porn) cannot be held criminally liable under Article 190a(2) PC [Ziobroń 2021, 229].

Another deepfake-related crime is recording the image of a naked person or a person engaged in sexual activity by using violence, unlawful threat or deception against them, or disseminating the image of a naked person or a person engaged in sexual activity without their consent – Article 191a PC.[9] This provision mainly protects human intimacy, which is closely related to the right to privacy. Therefore, human sexual freedom is protected as the freedom to decide on the recording or dissemination of one's naked image or one's image during sexual activity – this aspect of freedom is related to human dignity, due to the intimate sphere to which it refers [Wala 2025, 467]. Lachowski emphasizes that a crime can only occur when the injured party is a participant in the sexual act and has not consented to its dissemination. The concept of an image should be understood as a likeness of a person that allows for their identification, while a naked person is one whose intimate parts of the body are exposed and who is at least half naked. In the case of men, intimate body parts will be the buttocks and genitals, and in the case of women – breasts, buttocks and genitals [Lachowski 2023b, 1027-1028]. Mozgawa specifies that the legislator, when speaking about sexual activity (during which a person is recorded) means both sexual intercourse and other sexual activity [Mozgawa 2025b].

---

[8] See https://sjp.pwn.pl/slowniki/wizerunek.html [accessed: 01.09.2025].

[9] Article 191a PC reads: "§ 1. Whoever records the image of a naked person or a person during a sexual act, using violence, unlawful threat or deceit against that person, or disseminates the image of a naked person or a person during a sexual act without their consent, shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years. § 2. Prosecution takes place at the request of the injured party."

Ziobroń notes that in the case of fake pornography, two images are disseminated: the image of the person whose face was used and the image of the naked person whose body was recorded in the film. Therefore, it cannot be claimed that a participant in a sexual act is a person whose face has only been pasted on using deepfake technology, because he or she is neither the subject of the sexual act nor is naked, while images of naked bodies in deep porn productions belong to pornographic film actresses who, in principle, consent to their recording [Ziobroń 2021, 230]. The above statements lead to the conclusion that under Article 191a PC there is no legal basis for assigning criminal liability to a person who creates and distributes deep porn content.

Crimes of particular relevance to the analysis of deepfake technology include defamation[10] – Article 212 PC and insult[11] – Article 216 PC. The essence of the crime of defamation is the negative consequences that a specific entity may suffer due to the content of the slander, which may contribute to the loss of trust necessary for a given position, profession or type of activity. The subject of protection under Article 212 PC is the external part, perceived as the "good name" of the entity to which it applies [Błachnio 2024, 1080]. The crime of defamation, in the absence of normative restrictions, may be committed in any form that enables the transmission of information to another person. It can occur using various means of transmitting information, not only orally, but also in writing, print, image, caricature or through an artistic work [Raglewski 2017, 32]. By presenting a specific person or institution in a bad light, deepfakes can even destroy their life or, in the case of an institution, negatively affect its functioning and social perception [Mamak 2020]. Deepfake authors who disseminate content that

---

[10] Article 212 PC states: "§ 1. Whoever accuses another person, group of persons, institution, legal person or organizational unit without legal personality of such conduct or characteristics that may humiliate them in public opinion or expose them to the loss of confidence necessary for a given position, profession or type of activity, shall be subject to a fine or restriction of liberty. § 2. If the perpetrator commits the act specified in § 1 through the mass media, he or she shall be subject to a fine, restriction of liberty or imprisonment for up to one year. § 3. In the event of conviction for the offence specified in § 1 or 2, the court may order compensation to be paid to the injured party, the Polish Red Cross or another social cause indicated by the injured party. § 4. The offence specified in § 1 or 2 shall be prosecuted on private accusation."

[11] Article 216 PC states: "§ 1. Whoever insults another person in his presence, or even in his absence but in public, or with the intention that the insult shall reach such a person, shall be subject to a fine or the penalty of restriction of liberty. § 2. Whoever insults another person using the mass media shall be subject to a fine, restriction of liberty or imprisonment for up to one year. § 3. If the insult was caused by the offended party's provocative conduct or if the offended party responded by violating the personal inviolability or by a reciprocal insult, the court may refrain from imposing a penalty. § 4. In the event of conviction for the offence specified in § 2, the court may order compensation to be paid to the injured party, the Polish Red Cross or another social purpose indicated by the injured party. § 5. The prosecution takes place on private accusation."

attributes negative behaviour or characteristics to the injured party, e.g., related to their character, health, or sexual preferences, which expose them to loss of trust or humiliation in public opinion, may be held liable under Article 212 PC. The crime of defamation can cover various types of deepfakes concerning not only individuals but also institutions.

Deepfake technology can play a particular role in cases of insult. The protected legal interest in the offence under Article 216 PC is dignity, perceived as the inner part of a person. Insults refer to the perpetrator's behaviour that expresses contempt for another person, in particular by humiliating them, degrading their dignity and making them feel offended. This applies to all behaviours of the perpetrator, regardless of their form [Zgoliński 2023, 1147-148]. Insults can therefore be made, for example, through gestures, writing, as well as verbally and by means of images. If the victim's face is pasted onto the silhouette of another character who behaves in a way that is incompatible with the dignity of the person, then we are dealing with an insult. Such a photomontage featuring the victim's face can be used in pornographic production (deep porn), where the victim is involved in an act that will be perceived as degrading in the eyes of the public [Mamak 2020]. With the use of deepfake technology, a person can therefore be insulted by being humiliated or ridiculed in a generated video.

It should be noted that for certain persons the Penal Code provides for a separate category of crime, e.g. Article 135(2) PC concerns insulting the President of the Republic of Poland.[12] A separate crime is insulting the nation or the Republic of Poland, as defined in Article 133 PC,[13] as well as a group of people or an individual because of their national, ethnic, racial or religious affiliation.[14]

Deepfake technology can also be used to commit other crimes such as fraud – Article 286 of the Penal Code or coercion – Article 191(1) PC. In the context of the production and distribution of deep porn, coercion would consist in an unlawful threat to distribute a given recording in the absence of the required behaviour by the perpetrator, e.g. payment of a certain sum of money [Ziobroń 2021, 233]. Fraud, on the other hand, means that the perpetrator, through his deceitful actions, leads another person to a false impression of the actual state of affairs, e.g. as to the characteristics of the

[12] Article 135(2) PC states: "Whoever publicly insults the President of the Republic of Poland shall be subject to the penalty of imprisonment for up to 3 years."

[13] Article 133 PC: "Whoever publicly insults the Nation or the Republic of Poland shall be subject to the penalty of imprisonment for up to 3 years."

[14] Article 257 PC states: "Whoever publicly insults a group within the population or an individual because of his or her national, ethnic, racial or religious affiliation or because of his or her lack of religious beliefs or for these reasons breaches the personal inviolability of another individual, shall be subject to the penalty of imprisonment for up to 3 years."

goods sold or the circumstances of the transaction, as a result of which the injured party disposes of his property in an unfavourable manner [Guzik-Makaruk and Pływaczewski 2016, 1522]. Another means of misleading may be deepfake technology by means of which the perpetrator generates a video in which, for example, well-known public figures (celebrities, politicians, entrepreneurs) advertise fictitious investments or cryptocurrencies, and the misled victims invest funds, believing in the authenticity of the recording.

Despite identifying selected examples of crimes whose elements would correspond to the use of deepfake technology, it must be noted that Polish criminal law does not fully take this issue into account. In view of the harmful nature of this phenomenon, it should be stated that the applicable regulations are fragmentary and do not fully address the specific nature of the threats arising from deepfake technology; they are inadequate to the character of the threat, and the legal protection afforded to victims is insufficient.

4. DEEPFAKE AND REGULATIONS IN GERMAN CRIMINAL LAW

German law does not yet contain specific legal regulations regarding deepfakes. Depending on the circumstances of the specific case within the scope of criminal law – particularly with regard to the intended purpose of deepfakes and their dissemination – it is necessary to rely primarily on the existing regulations governing individual criminal offences. It should be noted that such punishable acts will include crimes against honour and physical integrity[15]: insult (para. 185 StGB), if the deepfake being distributed is to be perceived as an offensive value judgement towards the person concerned or towards a third party [Kumkar and Rap. 2022, 199 and 226; Heckmann and Paschke 2022], defamation (para. 186 StGB), insofar as the deepfake is used to state or disseminate a fact about another person that is likely to make them contemptible or humiliate them in public opinion, and slander (para. 187 StGB), if the deepfake is used to state or disseminate a false fact about another person that is likely to make them contemptible or humiliate them in public opinion [Tuora-Schwierskott 2018, 270].

Criminal liability may also arise under Section 201a of the German Penal Code (StGB) for violating the protection of private life and infringing personal rights through photographing. Pursuant to para. 201a(2)[16] of the German Penal Code, it is a crime to provide a third party with photos of another person, which infringes upon the personal sphere of life of the person being photographed,

---

[15] Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 12 des Gesetzes vom 27. März 2024 (BGBl. 2024 I Nr. 109) geändert worden ist.

[16] Ibid., p. 276

as well as to make available to a third party an image taken by another person without permission, which may seriously damage the reputation of the person being photographed. Also in this case it is sufficient "if only parts of a person are depicted" (in particular, for example, the face); the crime may be committed by the fact of making a photomontage [Lantwin 2020, 78-79].

Offences under other criminal laws – i.e. laws other than the Penal Code – may also be taken into account in the case of deepfake abusers. Therefore, in accordance with para. 33 in conjunction with para. 22 of the Art and Photographic Copyright Act (KunstUrhG),[17] dissemination or public display of an image without the consent of the person depicted in it is punishable. The penalty for such an offence is up to one year of imprisonment or a fine.[18]

Furthermore, criminal liability for copyright infringement may also be taken into account, as when creating deepfakes – especially pornographic deepfakes – the photo and video materials taken by the author and used by third parties, edited and then distributed without the author's consent are protected by copyright [Haag 2023]. Pursuant to para. 106 of the Intellectual Property and Copyright Act (UrheberGesetz UrhG)[19] for such crimes, a prison sentence of up to three years or a fine is stipulated, and the provision reads: "Whoever reproduces, distributes or makes publicly available a work or adapts or processes the work without the rightholder's consent in cases other than those permitted by law, shall be subject to the penalty of imprisonment for up to three years or a fine."

In turn, the provision of para. 108 UrhG contains a description of further punishable acts, namely, the following: a third party, without the author's consent, reproduces, distributes or publicly makes available a scientific edition or an adaptation of such an edition, uses a posthumous work or an adaptation or transformation of such a work, reproduces, distributes or publicly makes available a photograph or an adaptation or transformation of a photograph, uses a performance of a work by an artist, uses a phonogram, uses a radio broadcast, uses an image carrier or an image and sound carrier, uses a database [Heckmann and Paschke 2022]. It should therefore be stated that the scope of the described acts of using the work contrary to the author's will is quite wide.

Since the fight against deepfakes has been recognised as an issue of exceptional importance, a draft amendment to the Criminal Code concerning the

---

[17] Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie in der im Bundesgesetzblatt Teil III, Gliederungsnummer 440-3, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 3 § 31 des Gesetzes vom 16. Februar 2001 (BGBl. I S. 266) geändert worden ist.

[18] Para. 33 of the of the Art and Photographic Copyright Act (KunstUrhG).

[19] Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), das zuletzt durch Artikel 25 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858) geändert worden ist.

protection of privacy – providing detailed regulation of deepfakes – has been submitted to the Bundestag.[20]

The new paragrap. 201b of the German Penal Code proposes prison sentences of up to two years or a fine for violating personal rights through digital forgery. In serious cases, such as the dissemination of pornographic deepfakes online, the expected range of penalties includes up to five years of imprisonment. Deepfakes that are shared "to pursue primarily legitimate interests," for example in the fields of art, science, or journalism, will not be covered by this new provision [Sittig 2024].

The proposed legal regulation is as follows: "§ Whoever infringes the personal rights of another person by making available to a third party media content generated or modified by computer technology, giving the appearance of a realistic image or sound recording of the physical appearance, behaviour or oral statements of that person, shall be subject to the penalty of imprisonment for up to two years or a fine. The same applies if the offence referred to in sentence 1 concerns a deceased person and as a result his or her right to personal protection is seriously impaired.

In the cases referred to in section 1 sentence 1, anyone who makes media content publicly available or makes available media content the subject of which is a process concerning the most personal sphere of life shall be punished with imprisonment of up to five years or a fine."

However, the above provisions do not apply to acts undertaken for the purpose of pursuing overriding legitimate interests, namely art or science, research or teaching, reporting on current events or history, or for similar purposes. The legislative initiative also provides that image or sound carriers, or other technical means used by the perpetrator or participant, may be subject to forfeiture.

Further initiatives result from the provisions of EU law. The legislator establishes some of the risk mitigation measures referred to in Article 35 of the Digital Services Act as mandatory requirements. Article 35(1)(2)(k) DSA[21] still leaves the requirement to label deepfake content at the discretion of service providers. The German legislator has not yet addressed this issue, although it will undoubtedly have to do so in the near future.

[20] Entwurf eines Gesetzes zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes, Drucksache 20/12605, (Drucksache 20/12605).

[21] OJ EU.L.2022.277.1, Lex/el. 2025.

CONCLUSION

A new category of socially dangerous behaviour is related to the harmful use of deepfake technology, and the applicable legal regulations do not guarantee citizens a sufficient level of legal protection in this regard. Consequently, the introduction of new criminal-law solutions appears necessary, particularly in light of the entry into force of the Artificial Intelligence Act, which is becoming a point of reference for the creation of more effective protective mechanisms.

The EU AI Act introduces a legal definition of deepfake that focuses on audio and visual forms and does not apply to text-based forms. Moreover, the legislator classifies deepfake technology within the category of limited-risk systems, which entails the fulfilment of transparency obligations, but does not establish provisions requiring the removal of deepfake content from the digital space. The provisions of the AI Act designate only the recipients of deepfake content as subjects of legal protection, while they do not provide legal protection to the individual victims of this technology. In this situation, it is necessary to introduce regulations at the national level that will ensure such legal protection.

The analysis of the current legal status in Poland allows us to conclude that the provisions of the Penal Code do not meet the contemporary challenges resulting from the development of deepfake technology. Although deepfakes may be subject to criminalisation under the above-mentioned provisions, the applicable regulations are fragmentary, inadequate to the nature of the threat, and provide insufficient legal protection for victims. This situation justifies undertaking a legislative initiative aimed either at updating the applicable provisions of the Penal Code or introducing new ones which, inter alia, would establish criminal liability for failure to comply with the rules governing the creation of deepfake content, and would extend the scope of criminalisation relating to the dissemination of the image of a naked person to include artificially generated images, where such images misleadingly suggest that they depict the person in question [Mamak 2020].

The foregoing considerations relating to the current provisions of German criminal law indicate that the German Penal Code does not contain specific legal regulations concerning deepfakes. Criminal liability for the dissemination of deepfake content is likewise fragmentary and is based on the provisions governing individual prohibited acts. Additional conclusions also arise from the analysis of the current German legal framework, namely that the fight against deepfakes, given the specific nature of the phenomenon, cannot be limited solely to provisions of criminal law itself. It is necessary to extend criminal provisions to copyright law and to undertake legislative initiatives covering new aspects of crime. Therefore, it seems reasonable to penalise

actions involving the infringement of another person's personal rights by making available to a third party media content generated or modified by computer technology, giving the appearance of a realistic image or sound recording, appearance, behaviour or oral statements of that person.

REFERENCES

Almars, Abdulqader. 2021. "Deepfakes Detection Techniques Using Deep Learning: A Survey." *Journal of Computer and Communications* 9:20-35.

Błachnio, Adam. 2024. "Komentarz do art. 212." In *Kodeks karny. Komentarz*, edited by Jarosław Majewski, 1079-1082. Warszawa: Wolters Kluwer.

Dąbrowska, Ilona. 2020. "Deepfake – nowy wymiar internetowej manipulacji." *Zarządzanie Mediami* 20, no. 8:89-101.

Gradek-Lewandowska, Małgorzata. 2020. "Część 1 – Czy deepfake – face swap i face reenactment mieszczą się w prawach własności intelektualnej?" https://lgl-iplaw.pl/2020/09/czesc-1-czy-deepfake-face-swap-i-face-reenactment-mieszcza-sie-w-prawach-wlasnosci-intelektualnej/ [accessed: 01.08.2025].

Guzik-Makaruk, Ewa, and Emil Pływaczewski. 2016. "Komentarz do art. 286." In *Kodeks karny. Komentarz*, edited by Marian Filar, 1521-525. Warszawa: Wolters Kluwer.

Haag, Markus. 2023. "KI im Strafrecht und Strafprozessrecht." In *Handbuch Multimedia-Recht*, edited by Thomas Hoeren, Ulrich Sieber, and Bernd Holznagel, Rn. 28, 60, München: C.H. Beck.

Heckmann, Dirk, an Anne Paschke. 2022. "§ 121 Digitalisierung und Grundrechte." In *Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund*, Rn 82, edited by Klaus Stern, Helge Sodan, and Markus Möstl. München: C.H. Beck.

Kiełpiński, Krzysztof. 2023. "Deepfake jako narzędzie do przekazywania informacji fałszywej i domniemanej. Analiza prawnokarna i cybernetyczna." *Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury* 51, no. 3:83-99.

Kumkar, Lea, and Julian Rapp. 2022. *Deepfakes. Eine Herausforderung für die Rechtsordnung*. Zeitschrift für Digitalisierung und Recht (ZfDR).

Lachowski, Jerzy. 2023a. "Komentarz do art. 190a." In *Kodeks karny. Komentarz*, edited by Violetta Konarska-Wrzosek, 1016-1021. Warszawa: Wolters Kluwer.

Lachowski, Jerzy. 2023b. "Komentarz do art. 191a." In *Kodeks karny. Komentarz*, edited by Violetta Konarska-Wrzosek, 1021-1030. Warszawa: Wolters Kluwer.

Lantwin, Tobias. 2020. "Strafrechtliche Bekämpfung missbräuchlicher Deep Fakes – Geltendes Recht und möglicher Regelungsbedarf." *Multimedia und Recht* 2:78-82.

Lisińska, Justyna, and Daniel Castro. 2024. "Why AI- Generated content labeling mandates fall short." https://www2.datainnovation.org/2024-ai-watermarking.pdf. [accessed: 01.08.2025].

Łabuz. Mateusz. 2023. "Regulating deep fakes in the Artificial Intelligence Act." *Applied Cybersecurity & Internet Governance* 2, no. 1:1-42.

Łabuz. Mateusz. 2024. "Deep fakes and the Artificial Intelligence Act – An important signal or a missed opportunity?" *Policy & Internet* 16, no. 4:783-800.

Mamak, Kamil. 2020. "Prawnokarne sposoby walki z fake newsami. Raport projektu SpołTech." https://centrumcyfrowe.pl/wp-content/uploads/sites/16/2020/06/Raport_walka-z-fake-newsami.pdf. [accessed: 01.08.2025].

Mozgawa, Marek. 2025a. "Komentarz do art. 190a." In *Kodeks karny. Komentarz aktualizowany*, edited by Marek Mozgawa. Lex el.

Mozgawa, Marek. 2025b. "Komentarz do art. 191a." In *Kodeks karny. Komentarz aktualizowany*, edited by Marek Mozgawa. Lex el.

Raglewski, Janusz. 2017. "Komentarz do art. 212." In *Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. 212-277d*, edited by Włodzimierz Wróbel, and Andrzej Zoll, 27-53. Warszawa: Wolters Kluwer.

Rajtar, Oliwia. 2025. "Technologie deepfake w zakresie danych osobowych." *Rocznik Administracji Publicznej* 11, no. 1:193-210.

Sittig, Jacqueline. 2024. "Strafrecht und Regulierung von Deepfake-Pornografie." https://www.bpb.de/lernen/bewegtbild-und-politische-bildung/556843/strafrecht-und-regulierung-von-deepfake-pornografie/ [accessed: 17.03.2025].

Szpyt, Kamil. 2019. "Sztuczna inteligencja i nowe technologie (nie zawsze) w służbie ludzkości, czyli cywilnoprawna problematyka rozwoju i popularyzacji technologii *deepfake*." In *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, edited by Kinga Flaga-Gieruszyńska, Jacek Gołaczyński, and Dariusz Szostek, 75-94. Warszawa: C.H. Beck.

Tuora-Schwierskott, Ewa. 2018. *Deutsches Strafgesetzbuch, Niemiecki Kodeks karny w tłumaczeniu na język polski*. Berlin: Verlag de-iure-pl.

Wala, Krzysztof. 2025. "Komentarz do art. 191a." In *Kodeks karny. Komentarz*, edited by Jan Kulesza, 467-71. Warszawa: Wolters Kluwer.

Zgoliński, Igor. 2023. "Komentarz do art. 216." In *Kodeks karny. Komentarz*, edited by Violetta Konarska-Wrzosek, 1130-138. Warszawa: Wolters Kluwer.

Ziobroń, Agata. 2021. "Deepfake a prawo karne. Uwagi de lege lata i de lege ferenda dotyczące fałszywej pornografii." *Studenckie Prace Prawnicze, Administratywistyczne i Ekonomiczne* 37:225-38.

Zoll, Andrzej. 2017. "Komentarz do art. 190a." In *Kodeks karny. Część szczególna. Komentarz do art. 117-211a*, edited by Włodzimierz Wróbel, and Andrzej Zoll, 589-96. Warszawa: Wolters Kluwer.