Criminal Liability of Deepfake Pornography under Turkish and German Criminal Law

By Prof. Dr. Jörg Eisele, Tübingen, Dr. iur. Irmak Duman, Istanbul*

The EU Directive 2024/1385 on Combating Violence Against Women and Domestic Violence, dated 15.5.2024, introduces new obligations for member states, marking a significant step towards the criminalization of so-called "image-based sexual abuse." Member countries are now expected to implement the directive and introduce criminal sanctions to address this issue. This paper focuses on the most prominent form of image-based sexual abuse: deepfake pornography, a product of rapidly evolving AI technology. The paper examines whether the Turkish and German criminal codes already provide adequate protection for the victims of deepfake pornography or whether the current situation, with the guidance of the new directive, calls for new criminalization.

I. Introduction

Deepfake pornography is a gendered phenomenon.[1] Not surprisingly, just as in sexual crimes in general, the majority of victims of deepfake pornography are women.[2] Being non-consensually featured in a synthetic pornographic image or video is linked to a myriad of consequences, including emotional distress, anxiety, and even suicide, in addition to social and career-related consequences such as job loss, leaving employment or school, or withdrawing from public discourse.[3] The issue is now a focal point of interest for criminal law all over the world, owning to its impact on the violation of an individual's fundamental rights to dignity and privacy and their freedom of sexual expression and autonomy.[4]

This paper explores the phenomenon of deepfake pornography from two distinct perspectives: first, as a product of deep-fake technology (II.), and second, as a specific form of "image-based sexual abuse" (III.). This is followed by the examination of Turkish and German criminal law provisions to assess whether adequate measures are currently in place to address this issue (IV.). The paper concludes with recommendations de lege ferenda for combating deepfake pornography (V.).

II. Exploring deepfake pornography through the lens of deepfake technology

The term deepfake is a portmanteau of "deep learning" and "fake" referring to fake media such as fake photos, videos or recordings created through the employment of deep learning techniques of artificial intelligence.[5] Regulation (EU) 2024/1689 Art. 3 (60) defines the term as 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.

Deepfake technology is powered by Generative Adversarial Networks (GANs), which involve two models: a generator and a discriminator.[6] The generator is trained to generate fake data by incorporating feedbacks from the discriminator which capture the characteristics of the training set and which are indistinguishable from these.[7] The discriminator on the other hand is simply a classifier and tries to distinguish real data[8], meaning real pictures, videos or sounds of real people from the fake data created by the generator.[9] This competitive process continues until the discriminator can no longer distinguish between real and fake data, when the so-called Nash Equilibrium is reached[10]

Pornographers have been early adopters of deepfake technology, since the term first emerged on the online platform Reddit in 2017.[11] Initially targeting female celebrities, the rise of apps like "Fakeapp", "Deepfacelab", and "Reface" has expanded the target range to ordinary individuals.[12] Accord-

* Prof. *Dr. Jörg Eisele* is the Chair of German and European Criminal Law, Criminal Procedure Law, Commercial Criminal Law, and Computer Criminal Law at University of Tübingen. Dr. iur. *Irmak Duman* is a full-time lecturer of Criminal Law and Criminal Procedure at Koç University, Istanbul.

[1] *Chesney/Citron*, California Law Review 107 (2019), 1753 (1773); *McGlynn/Rackley*, Oxford Journal of Legal Studies 37 (2017), 534 (542): "The harm suffered by victim-survivors are deeply gendered."

[2] See Deeptrace, The State of Deepfakes, p. 2, available at https://regmedia.co.uk/2019/10/08/deepfake_report.pdf (18.1.2025); *Hall/Hearn/Lewis*, Encylopedia 3 (2023), 327. Article 2 of EU-Directive 2024/1385 on combatting violence against women and domestic violence defines violence against women as: "All acts of gender-based violence directed against woman or a girl because she is a woman or a girl or that affect women or girls disproportionately." According to this definition, deepfake pornography qualifies as an act of violence against women, as it is a gender-based offense that disproportionately impacts women.

[3] *McGlynn/Rackley*, Oxford Journal of Legal Studies 37 (2017), 534 (543).

[4] *McGlynn/Rackley*, Oxford Journal of Legal Studies 37 (2017), 534 (544).

[5] *Chesney/Citron*, California Law Review 107 (2019), 1753 (1774); *Pascale*, Syracuse Law Review 73 (2023), 335 (337).

[6] *Ahirwar*, Generative Adversarial Networks Projects, 2018, p. 7; *Langr/Bok*, GANs in action, 2019, p. 5.

[7] *Langr/Bok* (fn. 6), p. 5.

[8] *Ahirwar* (fn. 6), p. 7.

[9] *Langr/Bok* (fn. 6), p. 5–6: The *authors* further draw well-known comparisons to clarify the roles of the generator and the discriminator: the generator takes on the role of a forger who prints counterfeit money or an art forger attempting to deceive an art expert, while the discriminator assumes the role of a central bank distinguishing real money from counterfeit or an art expert determining the authenticity of an artwork.

[10] *Ahirwar* (fn. 6), p. 7; *Yavuz*, Deepfake (Derin Sahte), 2022, p. 50.

[11] *Chesney/Citron*, California Law Review 107 (2019), 1753 (1757); *Yavuz* (fn. 10), p. 80.

[12] See also *Delfino*, Fordham Law Review 88 (2019), 887 (893). *Hall/Hearn/Lewis*, Encylopedia 3 (2023), 327 (328):

ing to a study conducted in 2019, pornographic deepfake videos account for the 96 % of all deepfake videos online.[13]

Once the network is trained, the technology can superimpose one person's face onto another person's naked body, resulting in the creation of nude images or videos of that person. For someone to be subjected to a deepfake pornography at the end, they don't have to have nude pictures online – or at all. Creators of the manipulated visual do not have to know the victim personally, they mostly gather images from social media like Facebook or Instagram.[14]

> "Now anyone who has appeared in a digital image may 'star' in pornography against their will."[15]

III. Deepfake pornography as a form of IBSA (Image-based sexual abuse)

Deepfake pornography is also a form of image-based sexual abuse, which is a term that was conceptualized in response to advancements in technology. It is defined as the "non-consensual creation and/or distribution of private sexual images"[16] with the on-purpose description of the acts as sexual abuse.[17] The term is, furthermore, to be interpreted as part of the broader phenomenon of sexual violence and as a strategy in combating violence against women.[18] As per the definition, image-based sexual abuse does not only encompass the dissemination of the images but also their creation.[19] IBSA covers various phenomena such as sextortion, upskirting, downblousing and revenge-porn.[20]

At the crux of the matter lies the lack of consent. Private sexual images that are created or disseminated consensually are excluded from the term IBSA[21], as they are considered part of an individual's sexual expression. Although in some cases determining the lack of consent is straightforward, in other cases, it may require a broader interpretation. For instance, taking a photo of someone without their knowledge is considered as non-consensual, just as sending a nude selfie under pressure is.[22] Even if the creation of a photo is consensual, the subsequent dissemination does not automatically imply the same consent.

> "Consent to one course of action is not consent to another."[23]

IV. Exploring applicable regulations for deepfake pornography in Turkish and German criminal codes

The following will examine whether and to what extent acts regarding deepfake pornography are already criminalized under the current law in Germany and Türkiye.

1. Deepfake Pornography as Part of the Pornography Offense: § 226 TCK and § 184 StGB

The primary rationale behind § 226 (1) (a) and (b) TCK[24] is to safeguard the physical, mental, moral, spiritual, and emotional integrity of children.[25] Additionally, the article aims to prevent adults from being undesirably exposed to obscene materials[26] and to uphold public morals[27]. The latter is clear,

"While the use of technology for sexual purposes is as old as the printing press, what differentiates the modern world is the near-universal availability of sex and sexual materials on the Internet and technological devices for accessing it."

[13] See Deeptrace (fn. 2), p. 1. As of 2019, deep-fake pornographies were viewed 134.364.438 times, and these statistics are pulled from only the top four dedicated deep-fake pornography websites.

[14] See also *Delfino*, Fordham Law Review 88 (2019), 887 (895).

[15] See also *Delfino*, Fordham Law Review 88 (2019), 887 (890).

[16] *McGlynn/Rackley*, Oxford Journal of Legal Studies 37 (2017), 534 (536). In German, the term is referred to as "bildbasierte sexualisierte Gewalt".

[17] *McGlynn/Rackley*, Oxford Journal of Legal Studies 37 (2017), 534 (536): The *authors* claim that catchy names favored by the media such as "celebgate", "peeping tom", and "fappening" when describing the acts downplay the seriousness of these activities. Conversely, using the term "sexual abuse" directly communicates the gravity of the harm caused.

[18] *McGlynn/Rackley*, Oxford Journal of Legal Studies 37 (2017), 534 (536); see also *Hall/Hearn/ Lewis*, Encylopedia 3 (2023), 327 (328): "IBSA can be understood as forms of and part of the broad range and continua of gender-based violence".

[19] *McGlynn/Rackley*, Oxford Journal of Legal Studies 37 (2017), 534 (538): Therefore, voyeurism and the recording of rapes or other sexual assaults, in both cases where the perpetrator is seen as the "creator" of the images, fall within the scope of image-based sexual abuse.

[20] See *Greif*, Strafbarkeit von bildbasierten sexualisierten Belästigungen, 2023.

[21] *McGlynn/Rackley*, Oxford Journal of Legal Studies 37 (2017), 534 (541).

[22] *McGlynn/Rackley*, Oxford Journal of Legal Studies 37 (2017), 534 (542).

[23] *McGlynn/Rackley*, Oxford Journal of Legal Studies 37 (2017), 534 (542).

[24] § 226 (1) TCK (Basic Pornography) reads:
"A person who a) gives a child material containing obscene images, writings or words or shows a child the content of such material, reads such material to a child or makes the child read them or listen to them b) makes the content of such material public in places accessible or visible to a child, or who exhibits such material in a visible manner or who reads or talks about such material, or who induces another to read or talk about such material c) offers such materials for sale or rent in a manner that reveals its content d) offers for sale, sells or rents such materials outside of places designated for the exclusive sale of these, e) gives or distributes such materials along with the sale of other products or services as a free supplement; or f) advertises such products shall be sentenced to imprisonment from six months to two years and a judicial fine."

[25] *Özbek*, Müstehcenlik Suçu, 2009, p. 39.

[26] *Özbek* (fn. 25), p. 40.

as the offense is classified under offenses against public morals, rather than offenses against the sexual integrity or freedom of individuals.[28] With the exception of § 226 (1) (a) and (b) TCK and § 226 (3) TCK,[29] where the protection of children is the primary aim, the victim of the offense is typically considered to be society as a whole, rather than any individual.[30]

At this juncture, it is pertinent to question the position of the performers in pornographic material, who are, in fact, individuals. Does § 226 TCK solely protect consumers and potential consumers of pornographic content and societal morals, or does it also extend to shielding performers from taking part in pornographic visuals against their wills? The answer varies for adult performers and child performers: The protection of the performer[31] is only strived for the child performer, as evident in § 226 (3) TCK. No such regulation exists for the adult performer of pornographic content. Adults are, in the context of pornography offenses, only protected as to their capacities as consumers. This is solidified by the fact that § 226 TCK is structured as a crime of abstract-endangerment (abstraktes Gefährdungsdelikt), that is designed to safeguard the public and public morals rather than a specific victim. These constitute the biggest challenges in invoking § 226 TCK, since the victims of deepfake pornography are specific individuals who suffer firsthand from the actions of the perpetrator.

Invoking § 226 (2) TCK[32] also would not change the end result. Here, the "press or media" encompasses publications disseminated via any form of written, visual, auditory, and electronic mass communication medium according to § 6 (1) (g) TCK. Undoubtedly, the internet falls within the purview of the aforementioned press or media, however, on the condition that it is utilized as a medium of mass communication. But still, taking into account all the information provided, the adequacy of § 226 TCK in safeguarding victims of deepfake pornography, can only be affirmed if the victim is a child. It cannot be claimed that either the sexual freedom or the right to privacy of the adult victim of non-consensual deepfake pornography falls within the protection scope of the provision, which is merely concerned with upholding public morals.

Shifting the focus to German law, at first glance, making such content available can relatively easily be covered by § 184 StGB. According to § 11 (3) StGB, content means that which is contained in writings, on audio or visual media, on data carriers, in images or other materialized content or which is also transmitted independently of any storage using information or communication technologies.[33] It should be noted that § 184 StGB does not only cover real images but also the so-called "realistic portrayals"[34] (wirklichkeitsnahe Geschehen) and "fictional pornography". This is evident from the fact that not only images but also written texts and spoken words are within the scope of the article. Therefore, entirely or partially AI-generated content can also be encompassed by this provision.

However, two central limitations of the offense must be considered. On the one hand, the offense only covers the dissemination, meaning, making such content available, but not its creation. On the other hand, mere nude images and content depicting sexual acts are not covered by § 184 StGB. The key criterion is that the content must be classified as "pornographic", which is not necessarily the case even with sexual acts. According to the prevailing opinion in legal literature, content is only to be classified as pornographic if it foregrounds sexual processes in a grossly intrusive or coarsening manner, to the exclusion of other human references and which, in its overall tendency is exclusively or predominantly intended for sexual stimulation, thereby clearly exceeding the limits drawn in accordance with general social values.[35] This

[27] *Özbek* (fn. 25), p. 40; *Taneri*, Erciyes Üniversitesi Hukuk Fakültesi Dergisi 13 (2018), 561 (586); Yargıtay, decision of 24.3.2015 – 14-306/66.

[28] The current Turkish regulation resembles the early German regulation until 1968, when sexual crimes were thoroughly reformed by the 4. Criminal Law Reform Act. Prior to these reforms, the pornography offense was referred to as the distribution of obscene material (Verbreitung unzüchtiger Schriften). The offense was also classified under offenses against morality (Straftaten gegen Sittlichkeit), similar to its classification in Turkish criminal law today.

[29] § 226 (3) TCK (Child pornography) reads:
"A person who uses children, representations of children, or individuals who appear to be children in the production of materials containing obscene images, writings, or words, shall be punished with imprisonment from five to ten years and a judicial fine of up to five thousand days [...]".

[30] *Özbek* (fn. 25), p. 56; *Taneri*, Erciyes Üniversitesi Hukuk Fakültesi Dergisi 13 (2018), 561 (590), see *Hafızoğulları,* Beşeri Cinsellik ve Yeni Türk Ceza Kanunu, available at http://www.abchukuk.com/cezahukuku/cinsel-suclar.html (20.1.2025) for the view that the obscenity offense is a victimless crime since the victim cannot be specifically identified.

[31] "Darstellerschutz" in German.

[32] § 226 (2) TCK reads:
"Any person who publishes or facilitates the publication of obscene images, writings, or words through the press or media shall be sentenced to imprisonment for a term of six months to three years and a judicial fine of up to five thousand days."

[33] The technical translation of the articles and the terms of the German Penal Code is based on the translation available on the website of German Federal Office of Justice (Bundesministerium für Justiz), available at https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1793 (18.1.2025).

[34] Explicitly mentioned in § 184b (1) sentence 1 no. 3, sentence 2, § 184b (2) and § 184b (3) StGB.

[35] BVerfG BeckRS 2023, 5979; BGHSt 23, 40 (44); BGHSt 37, 55 (60); BGH NStZ-RR 2015, 74; BVerwGE 116, 5 (18); see also 2.2.1. of JuSchRiL; *Eisele*, in: Perron/Sternberg-Lieben/Eisele (eds.), Tübinger Kommentar, Strafgesetzbuch, 31st ed. 2025, § 184 para. 8 (announced for March 2025).

requires an assessment of the entire content,[36] so that simple sexual acts are by no means necessarily pornographic in nature.

In addition to these loopholes, the provision also fails to adequately address the injustice inherent to deepfake pornography. This is because § 184 StGB was legislatively designed to primarily serve to protect minors.[37] § 184 (1) paragraph 6 also deals with protection against unwanted exposure to pornography.[38] However, it is the addressee of the pornographic content that is protected, not the performer whose sexual self-determination is affected. Therefore, for a criminal liability, it does not matter whether the victim is identifiable, as it is only the pornographic nature of the content with regard to the victim that matters.

2. Deepfake Pornography as Sexual Harassment: § 105 TCK and § 184i StGB

§ 105 (1) TCK[39] does not elucidate the term "sexual harassment".[40] Although a consensus on the definition of sexual harassment lacks also within the scholars, a more defendable approach defines sexual harassment as behaviors that 1. occur without the consent of the victim 2. are conducive to violate the victim's sexual freedom and lastly 3. are conducted without physical touch.[41] The distinctive characteristic of the offense of sexual harassment is that physical contact between the victim and the perpetrator is not required.[42] In other words, it is in the Turkish Criminal Code, a hands-off offense. This highlights why § 105 TCK becomes relevant in the search of a norm that establishes criminal liability for creating or sharing of deepfake pornography: By the same token, no physical contact occurs between the perpetrator and the victim of deepfake pornography, yet the act still violates the victim's sexual freedom. And since the offense of sexual harassment is not a crime of specific means (verhaltensgebundenes Delikt), there are no restrictions or specific requirements to the behaviors that can constitute the offense. In this sense, creating or sharing of deepfake pornography is fit to be regarded as one of the various forms the offense of sexual harassment can manifest in.

As the wording makes clear, for the acts of the perpetrator to constitute the sexual harassment offense, the perpetrator needs to act with "sexual purposes".[43] This mens rea gives the offense its character and distinguishes it from other types of offenses such as defamation or the crime of disturbing the peace and tranquility of other people.[44] However, it should be noted that "acting with sexual purposes" does not necessarily need to be interpreted as the perpetrator satisfying their sexual feelings or desires.[45] The perpetrator should act with the knowledge that his actions carry a sexual implication and can hence sexually disturb the victim[46].

It is not plausible to assert that the creators of deepfake pornography consistently operate with sexual intent. Numerous scenarios are conceivable: the perpetrator may be an ex-partner seeking revenge against the victim, a colleague engaging in personal rivalry to discredit them, or someone extorting the victim for personal gain.[47] These examples do not

[36] *Eisele* (fn. 35), § 184 para. 10; *Schumann*, in: Eser/Schittenhelm/Schumann (eds.), Festschrift für Theodor Lenckner zum 70. Geburtstag, 1998, p. 565 (575).

[37] *Erdemir*, MMR 2003, 628 (630); *Heinrich*, in: Rotsch/Brüning/Schady (eds.), Strafrecht, Jugendstrafrecht, Kriminalprävention in Wissenschaft und Praxis, Festschrift für Heribert Ostendorf zum 70. Geburtstag am 7. Dezember 2015, 2015, p. 399 (406); *Hörnle*, Grob anstößiges Verhalten, 2005, p. 441.

[38] BGH NStZ-RR 2005, 309; *Erdemir*, MMR 2003, 628 (630); *Laubenthal*, Sexualstraftaten, 2012, para. 1016.

[39] § 105 (1) TCK (Sexual Harassment) reads:
"A person who harasses a person for sexual purposes shall, upon the complaint of the victim, be sentenced to imprisonment from three months to two years or to a judicial fine, and if the act is committed against a child, to imprisonment from six months to three years."

[40] See *Bayraktar et. al.*, Özel Ceza Hukuku, Cilt II, 2017, p. 559; *Taner*, Cinsel Özgürlüğe Karşı Suçlar, 2013, p. 361 for the critic that this constitutes a violation of the principle of legality.

[41] *Taner* (fn. 40), p. 364; *Ünver*, Ceza Hukuku Dergisi 4 (2009), 101 (122); see *Koca/Üzülmez*, Ceza Hukuku Özel Hükümler, 9th ed. 2023, p. 419 for a similar definition.

[42] *Koca/Üzülmez* (fn. 41), p. 420; *Bayraktar et. al* (fn. 40), p. 561; *Ünver*, Ceza Hukuku Dergisi 4 (2009), 101 (122).

[43] *Koca/Üzülmez* (fn. 41), p. 422; *Taner* (fn. 40), p. 376.

[44] See *Ünver*, Ceza Hukuku Dergisi 4 (2009), 101 (124), that the lack of the specific purpose could give rise to another crime like defamation.

[45] *Baş*, Ankara Üniversitesi Hukuk Fakültesi Dergisi 65 (2016), 1135 (1173); *Koca/Üzülmez* (fn. 41), p. 422; *Tezcan/Erdem/Önok*, Ceza Özel Hukuku, 21st ed. 2023, p. 423; *Ünver*, Ceza Hukuku Dergisi 4 (2009), 101 (124). *Gündel*, Cinsel Saldırı Cinsel İstismar, 2009, p. 161, further concretizes this purpose as "acting on thoughts and aims related to the sexual identity of the opposite party"; but see *Bayraktar et. al.* (fn. 40), p. 567 where the *authors* further require that the perpetrator acts on a feeling of lust towards the victim and that the perpetrator's act offends the sense of shame and honor and creates a discomfort.

[46] *Tezcan/Erdem/Önok* (fn. 45), p. 423.

[47] *Chesney/Citron*, California Law Review 107 (2019), 1753 (1773): "Not all such fakes will be designed primarily, or at all, for the creator's sexual or financial gratification. Some will be nothing less than cruel weapons meant to terrorize and inflict pain"; *McGlynn et. al.*, Female Legal Studies 25 (2017), 25 (31): "The sexual motive requirement precludes those who perpetrate a myriad of other purposes inclu1ding causing distress to the victim, to secure notoriety or bond with a friendship group or for financial gain"; *Salter et. al.*, Current Issues on Criminal Justice 24 (2012–2013), 301 (311): "Perceived injures to masculine pride in the aftermath of a relationship breakdown or generalized aggression towards girls and women can be expressed through the non-consensual circulation of compromising digital imagery of girls and women." For a critique on requiring "sexual gratification" for sexual offenses as a whole see *McGlynn et. al.*,

involve sexual motives, meaning that not all instances of deepfake pornography automatically constitute a sexual harassment in terms of § 105 TCK.[48] § 105 TCK is only applicable to a portion of the cases and does not offer a universally applicable protection.

Unlike in Türkiye, criminal liability for sexual harassment is ruled out for German criminal law from the outset. This is because the offense, being a hands-on crime, always requires that the perpetrator physically touches the victim ("touches another person in a sexually determined manner"), which is not the case with the creation and dissemination of deepfake images.

3. Deepfake Pornography as an Act of Defamation: § 125 TCK and §§ 185 et seq. StGB

§ 125 TCK[49] is a common regulation for both defamation and insult, meaning that the crime can be either committed by attributing a concrete act or fact to a person (defamation) or swearing at someone (insult). The discussion on the relevance of § 125 TCK pertains to whether creating or sharing a deepfake pornography of an individual depicts an "attribution of a concrete act or a fact", since it is evident that such actions clearly do not amount to an act of swearing.

Attributing a concrete act or a fact to a person is not sufficient per se to constitute the crime of defamation. The attributed act or fact must be capable of offending one's honor, dignity or prestige.[50] When determining whether the act is of this nature, the evaluation should be based on the average customary rules and value judgments prevailing in Turkish society at the time the act is committed.[51] A pornographic image – regardless of it being deepfake or authentic – will pass the offensiveness test easily, considering its controversial characteristic among society.

In order to talk about attributing a concrete act or fact, the authenticity of the allegations must be verifiable and provable.[52] The attribution must contain complementary elements about the person, place, subject, time, and manner of the event, distinguishing it from others and showing it is linked to the victim.[53] Based on these criteria, creating a deepfake image of someone and implying their involvement in the pornographic content, should be seen as attributing a concrete act to that person.

If defamation occurs publicly, the imprisonment term increases by one sixth under § 125 (4) TCK. This applies when the defamatory content is disseminated via any medium that enables an indefinite number of people to access it.[54] The element of publicity is satisfied when the offense occurs through press or broadcasting,[55] which includes the internet. Thus, a person who shares a deepfake pornographic image or video, utilizing the internet's broad reach, can indeed be held liable under § 125 (4) TCK.[56] However, this does not necessarily imply that § 125 TCK offers adequate protection for victims of deepfake pornography. § 125 TCK aims to protect the honor, dignity, reputation and prestige of individuals.[57] For the victims of deepfake pornography, the primary concerns are violations of privacy and sexual freedom.

A similar conclusion can be drawn regarding German criminal law. In individual cases, AI-generated images can constitute an offence under §§ 185 et seq. StGB, whereby public disclosure is designed as a qualification with an increased upper limit of the penalty range. It should first be noted that, according to the prevailing opinion in legal literature, § 185 StGB does not have a "gap-filling function" so that the so-called sexual insult is in principle not covered by the article.[58] However, this does not mean that sexually related images cannot fall under § 185 StGB, it is just not "automatically" applicable in cases of "classic" sexual acts involving an act of the perpetrator on the victim.[59] § 185 StGB should not be a catch-all offence (Auffangtatbestand) per se when the requirements of a sexual offence under Section 13 of the StGB have not been met. Such content can indeed be classified as "sexual insult" if it goes beyond a general and unspecific attack on dignity of persons or general personality

Female Legal Studies 25 (2017), 25 (37), that impetus to sexually offend can stem from the motivation for power and control or revenge; anger and punishment; recreation; adventure and sexual entitlement.

[48] See *Retornaz*, Cinsel İçerikli Görüntüleri Rızaya Aykırı Olarak İfşa Etme, Yayma, Erişilebilir Kılmaz ve Üretme Suçu, 2021, p. 83.

[49] § 125 TCK (Defamation) reads:
"A person who offends someone's honor, dignity or prestige by attributing an act or fact to a person or who attacks someone's honor, dignity or prestige by swearing shall be sentenced to imprisonment from three months to two years or with judicial fine."

[50] *Bayraktar et. al.*, Özel Ceza Hukuku, Cilt III, 2018, p. 434; *Centel/Zafer/Çakmut*, Kişilere Karşı İşlenen Suçlar, 5th ed. 2021, p. 249; *Koca/Üzülmez* (fn. 41), p. 534.

[51] *Centel/Zafer/Çakmut* (fn. 50), p. 249; *Koca/Üzülmez* (fn. 41), p. 535. See *Tezcan/Erdem/Önok* (fn. 45), p. 423: The *authors* further employ the principles of a democratic and a secular state that respects human rights as a criterion for the offensiveness evaluation.

[52] *Bayraktar et. al.* (fn. 50), p. 434; *Koca/Üzülmez* (fn. 41), p. 535.

[53] *Bayraktar et. al.* (fn. 50), p. 434; *Koca/Üzülmez* (fn. 41), p. 535.

[54] *Centel/Zafer/Çakmut* (fn. 50), p. 267; *Tezcan/Erdem/Önok* (fn. 45), p. 558.

[55] *Centel/Zafer/Çakmut* (fn. 50), p. 268; *Tezcan/Erdem/Önok* (fn. 45), p. 559.

[56] See also *Babayiğit*, Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi 15 (2021), 655 (671).

[57] *Bayraktar et. al.* (fn. 50), p. 426; *Centel/Zafer/Çakmut* (fn. 50), p. 243; *Koca/Üzülmez* (fn. 41), p. 529; *Tezcan/Erdem/Önok* (fn. 45), p. 536.

[58] See e.g. BGHSt 16, 63.

[59] See also *Eisele/Schittenhelm*, in: Perron/Sternberg-Lieben/Eisele (fn. 35), §§ 185 et seq. para. 4.

rights and additionally expresses an assessment of the victim's inferiority, in the sense of a lack of honor.[60]

An insult under § 185 StGB is understood as an attack on another person's honor through the expression of one's own disrespect or contempt.[61] In cases where the perpetrator makes sexual insinuations – such as, "You want/need it!" – it is recognized that the act constitutes an insult, when the perpetrator implies that they view the victim as someone, "with whom such actions can be done without hesitation", thus evaluating their personality in a derogatory manner and degrading their honor.[62] Nothing different can apply to deepfake images that depict the victim as someone willing to engage in sexual acts. This is to be assessed similarly in the context of §§ 186, 187 StGB, which, according to the dualistic concept of honor, can coincide with § 185 StGB.[63] If a deepfake creates the impression that the victim has engaged in sexual acts when this cannot be proven to be true (§ 186 StGB) or is outright untrue (§ 187 StGB), potential criminal liability arises if the asserted fact is suited to degrading that person or negatively affecting public opinion about that person.

However, the criminal law on defamation does not provide comprehensive protection. Mere AI-generated nude images, such as those of undressing or showering, are not covered by the insult articles, as they constitute an everyday activity and lack a defamatory character. The same applies to content featuring sexual acts, which may only be covered in specific cases – based on the depicted event –, as sexual acts are not considered negative in principle. From the perspective of protecting the honor of a specific person, it is also necessary for that individual to be identifiable in the image/video.

Additionally, it should be noted that the legal interest of "honor" protected in §§ 185 et seq. StGB,[64] does not accurately reflect the injustice inherent in deepfakes. In fact, in the case of deepfake images the general right of personality and, insofar as it concerns content with sexual acts, the right to sexual self-determination are the affected extents of protection. Ultimately, it is about the right to defend oneself against becoming an object of sexual assaults, including unwanted depictions.[65]

4.Deepfake Pornography as an Act of Stalking: § 123A TCK and § 238 StGB

The distinguishing characteristic of the stalking offense[66] is the persistent nature of the actions. Hence a single, non-repetitive act does not give rise to the stalking offense[67], even though it is not clearly established how many repetitions is needed to talk about persistency[68]. Persistence is, however, not a natural component of the acts related to deepfake pornography. Hereby a single instance is just as sufficient to jeopardize the legal interest of the victim.

The only bridge that can be built between stalking and acts related to deepfake pornography lies in the behavior of "attempting to contact the victim by using communication tools or information systems". The wording reveals, however, that the act of using communication tools or information systems should be conducted with the intention to contact the victim.[69] For the creator of a deepfake pornography, it is difficult to argue that the aim is to establish contact with the victim.

Furthermore, the offense of stalking is a result-based offense (Erfolgsdelikt) in Turkish criminal law, where the consequences of the perpetrator's actions are explicitly foreseen.[70] With respect to the stalking offense, these manifest as significant distress or concerns about one's own safety or that of their close ones. In instances involving deepfake pornography, the victim may be unaware of the existence of the material for a really long time, which would exclude the onset of the specified consequences.

In Germany, with the Law to Amend the Criminal Code – More Effective Combating of Stalking and Better Detection of Cyberstalking, as well as Improvement of Criminal Protection Against Forced Prostitution of 10.8.2021, the statutory requirements of § 238 (1) StGB were relaxed, and additional stalking actions were included in section 1 to address the phenomenon of cyberstalking. Since then, deepfake images can be covered by § 238 (1) StGB, points 6 and 7. As outlined in point 6, the dissemination of an image or making an image accessible to the public is punishable. According to the legislator's view, the term image includes not only photographic images but also, inter alia, drawings intended to de-

[60] See e.g. BGHSt 36, 145 (150 et seq.); BGH NStZ 2007, 218; BGH NStZ 2018, 603 (604).
[61] See BGHSt 36, 145 (148); *Eisele*, Strafrecht, Besonderer Teil I, 6th ed. 2021, para. 566.
[62] Cf. BGH NStZ 1992, 34; OLG Hamm NStZ-RR 2008, 108 (109); for more details see *Eisele/Schittenhelm* (fn. 59), §§ 185 et seq. para. 4.
[63] See BGHSt 11, 67 (70 et seq.); *Eisele* (fn. 61), paras. 558, 620.
[64] BGHSt 1, 288 (289); 36, 145 (148); *Heger*, in: Lackner/Kühl/Heger, Strafgesetzbuch, Commentary, 30th ed. 2023, Vorbem. § 185 para. 1.
[65] For more details see *Eisele*, KriPoZ 2023, 230 (231).

[66] § 123A TCK (Stalking) reads:
"The perpetrator who causes significant distress to a person or causes them to have concerns about one's own safety or that of their close ones by persistently following them physically or attempting to contact them using communication tools, information systems, or third parties shall be sentenced to imprisonment from six months to two years."
[67] *Balcı/Çakır*, Hasan Kalyoncu Üniversitesi Hukuk Fakültesi Dergisi 10 (2022), 323 (325); *Bozbayındır/Önok*, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi 1 (2022), 295 (304).
[68] *Özar*, Ankara Üniversitesi Hukuk Fakültesi Dergisi 71 (2022), 1397 (1408); *Taşkın*, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 10 (2023), 91 (111).
[69] *Taşkın*, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 10 (2023), 91 (114).
[70] See *Özar*, Ankara Üniversitesi Hukuk Fakültesi Dergisi 71 (2022), 1397 (1412).

pict the victim.[71] Therefore, the criminal liability does not depend on the authenticity of the image; AI-generated images are also covered. In reference to point 7, the dissemination or making accessible to the public of a content that is suitable to disparage or negatively affect public opinion about that person by feigning that person's authorship, is punishable. However, it should be noted that such images can also be disseminated under someone else's authorship, and disparagement is subject to the provisions of §§ 185 et seq. StGB.[72]

However, criminal liability for stalking will still come into question only in rare cases in German criminal law, where the additional typical characteristics of stalking are present. In this respect, a repeated act is required, so that one-off acts are excluded. Additionally, the action must be suited to not-insignificantly impact the victim's lifestyle. This is particularly problematic in the case of deepfake pornography. Unlike secret shots or recordings, which the victim might be able to avoid in the future by adopting a more cautious lifestyle, changes in the victim's lifestyle have no impact on the actions of the perpetrator of deepfake pornography, as the perpetrator can create deepfake pornography without any involvement from the victim. Thus, only cases remain where the action is likely to cause the victim to withdraw from their social circle or public life due to shame. According to the structure of the offense, it is also important here that the victim is identifiable, as otherwise, the fulfillment of the requirement of the act being suited to not-insignificantly impair the victim's lifestyle must be denied.

5. Deepfake pornography as a Violation of Privacy: §§ 134; 136 TCK and § 201a StGB; § 33 KunstUrhG

Both, § 134 TCK and § 136 TCK are categorized under "Offences against privacy and confidentiality"[73] in the criminal code and hence protecting the same legal interest: right to privacy.[74] § 136 TCK is the lex specialis, regulating the violation of a particular aspect of individuals' privacy: personal data. On the other hand, § 134 TCK serves as the lex generalis, the blanket norm[75] that finds application when an act violating the confidentiality cannot be addressed by a more specific provision.

Committing the offence of violation of privacy[76] requires more than just violating an individual's private life; it necessitates also breaching its confidentiality.[77] Turkish Supreme Court takes a broad approach to interpreting the confidentiality of the private life: The confidential part of the private life does not only mean a person's secluded, undisclosed life behind closed doors, that no one can know of, but all events and information that not everyone knows of or should know of, which can be disclosed only when the person desires.[78]

A more tailored solution seems to be § 134 (2) TCK[79] which is regarded as an independent offense within Turkish academic doctrine.[80] Here, the prohibited act is the disclosure, meaning making the images or sounds accessible to third parties.[81] The sounds or images do not necessarily have to be made public; disclosure to a single person is sufficient.[82] The material unlawfully disclosed may also have been obtained legally. However, even if a person has consented to being photographed or recorded, disclosing these images and sounds without their consent constitutes the of-

[71] BT-Drs. 19/28679, p. 12.

[72] See supra V. 3.

[73] *Akyürek*, Özel Hayatın Gizliliğini İhlal Suçu, 2011, p. 209, states that such a headline hints that the Turkish law is inspired by the three-spheres-theory (Dreisphärentheorie) of German law. The consistent referral to this theory in the criminal law textbooks is supportive of the *author's* argument, see for example *Zafer*, Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması, 2010, p. 13–16.

[74] *Akyürek*, (fn. 73), p. 210, defines the protected legal interest as the right to lead a comfortable and a free life safeguarded by the protection of one's private life and personal space; *Koca/Üzülmez* (fn. 41), p. 600 and 612; *Tezcan/Erdem/Önok* (fn. 45), p. 616.

[75] *Akyürek* (fn. 73), p. 221*; Bayraktar et. al.* (fn. 50), p. 618; *Eker Kazancı*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 9 (2007), 131 (150); *Koca/Üzülmez* (fn. 41), p. 603; *Zafer* (fn. 73), p. 3.

[76] 134 (1) TCK reads:
"A person who violates the confidentiality of the private lives of individuals shall be punished with imprisonment from one to three years. The penalty shall be increased by one-fold if the violation occurs through recording of images or sounds."

[77] *Akyürek* (fn. 73), p. 214; *Eker Kazancı*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 9 (2007), 131 (150). As it was mentioned supra note 74, such a distinction can be interpreted as the distinction between Privatsphäre (private sphere) and Intimsphäre (intimate sphere) in German law.

[78] In Yargıtay, decision of 3.4.2012 – 7345/8936, the supreme court refused to reduce the boundaries of the private life to four walls. See also *Akyürek* (fn. 73), p. 217 and *Bayraktar et. al.* (fn. 50), p. 613 that today the protection of private life is recognized further in public places. But see *Koca/Üzülmez* (fn. 41), p. 603: The *authors* dissent from the Supreme Court's interpretation, which deems photographing a woman's legs during window-shopping a violation of § 134 TCK. They limit the scope of the confidential part of the private life to activities that are kept secret, hidden from the gaze of other or not visible to others.

[79] 134 (2) TCK reads:
"Anyone unlawfully disclosing images and sounds related to the private lives of the individuals shall be punished with imprisonment from two to five years. The same penalty shall apply if the disclosed sounds or images are disclosed through the press or media."

[80] *Akyürek* (fn. 73), p. 230; *Bayraktar et. al.* (fn. 50), p. 617; *Hafızoğulları/Özen*, Ankara Barosu Dergisi 67 (2009), 9 (19); *Koca/Üzülmez* (fn. 41), p. 603; *Tezcan/Erdem/Önok* (fn. 45), p. 616.

[81] *Akyürek* (fn. 73), p. 231; *Bayraktar et. al.* (fn. 50), p. 618; *Eker Kazancı*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 9 (2007), 131 (151); *Tezcan/Erdem/Önok* (fn. 45), p. 600; *Zafer* (fn. 73), p. 196.

[82] See *Zafer* (fn. 73), p. 197.

fense described in § 134 (2) TCK.[83][84] Since the internet is regarded as a medium of press or media, incidents involving the disclosure of deepfake pornography would likely fall within the purview of § 134 (2) sentence 2 TCK.

Understanding what constitutes personal data in terms of § 136 TCK[85] requires weighing the articles of KVKK[86]. § 3 (1) (d) of KVKK defines personal data as any information relating to an identified or identifiable natural person, thereby establishing the two requirements that must be met for information to qualify as personal data. First, the data should be about natural persons, meaning that the term excludes data about legal persons.[87] Second, the data in question should be capable of fully or at least partially identifying the natural person.[88]

The central question yet to be answered concerning deepfake pornography is the following: Which of these two articles is applicable when photos or videos of a person are at stake, § 134 (2) TCK or § 136 TCK? Sharing a person's photos or videos can be considered as a violation of privacy, and no doubt, the photos and videos also constitute personal data.[89]

Decisions from the Turkish Supreme Court indicate that images showing people in their daily, regular, clothed state (meaning not naked) are not considered part of their private spheres and therefore cannot be evaluated under § 134 TCK. In such cases, § 136 TCK is to be invoked.[90] Frequently, creators source the facial photos needed for deepfake pornography from the selfies of the victims (usually found on the victims' public Instagram accounts) that depict the victims' everyday activities and states. Consequently, victims whose faces are superimposed on the deepfake pornography by this method cannot invoke § 134 (2) TCK.

Naked images, on the other hand, are considered part of the private lives of people by the Turkish Supreme Court, falling under the protection of § 134 (2) TCK.[91] Thus, in terms of the confidentiality, the naked images pass the test. But to come to a certain conclusion another question must be answered: Must the image or sound subject to § 134 (2) TCK also be "identifiable" akin to the requirement in § 136 TCK? Opinions vary on this. One opinion states that the person in the images or recording does not have to be identifiable for § 134 TCK to apply.[92] Another perspective regards the act of disclosing images that are not identifiable solely as an attempted violation of privacy.[93] A final opinion draws a distinction between the two paragraphs of § 134 TCK and claims that the recording or image does not have to be identifiable for § 134 (1) TCK; but identifiable for § 134 (2) TCK.[94] Turkish Supreme Court also adopts the last mentioned opinion.[95] As per the Turkish Supreme Court's standpoint, the applicability of § 134 (2) TCK to the person whose body is used, is generally limited, as identification is often hindered by the absence of facial features. Identification will be only occasionally possible if additional indicators, such as distinct birthmarks or tattoos on the body, are present.

As a result, the person, whose naked body is used, is particularly left without protection. § 136 TCK is inapplicable in cases involving naked images, and § 134 TCK is ruled out due to its requirement for identifiability. The protection provided for the victim whose face is used is also not noteworthy: A person whose face is used in deepfake pornography receives the same level of protection under § 136 TCK as someone whose face is shown in a regular photograph that is disseminated.

---

[83] *Akyürek* (fn. 73), p. 230; *Eker Kazancı*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 9 (2007), 131 (151); *Tezcan/Erdem/Önok* (fn. 45), p. 623.

[84] Another relevant provision is § 86 (1) of the Turkish Law on Intellectual and Artistic Works (FSEK): "Pictures and portraits cannot be presented to the public by demonstration or otherwise without the consent of the illustrated person". Violations are punishable under §§ 134, 139 and 140 TCK, as stated in § 86 (3) FSEK.

[85] § 136 TCK (Unlawful Obtaining and Giving Personal Data) reads:
"Any person who unlawfully gives personal data to another person or disseminates or obtains personal data shall be punished with imprisonment from two to four years."

[86] The Turkish Law On Protection of Personal Data.

[87] *Hafızoğulları/Özen*, Ankara Barosu Dergisi 67 (2009), 9 (19); *Kangal*, Kişisel Verilen Ceza ve Kabahatler Hukukunda Korunması, 2019, p. 28; *Koca/Üzülmez* (fn. 41), p. 614.

[88] *Hafızoğulları/Özen*, Ankara Barosu Dergisi 67 (2009), 9 (19); *Kangal* (fn. 87), p. 29; *Koca/Üzülmez* (fn. 41), p. 614.

[89] *Koca/Üzülmez* (fn. 41), p. 627.

[90] See Yargıtay, decision of 12.4.2017 – 13582/3109; Yargıtay, decision of 1.2.2017 – 11112/637; Yargıtay, decision of 22.1.2020 – 13100/3721 that in such cases § 136 TCK finds application.

[91] For the decisions that § 134 TCK applies when nudity is involved see Yargıtay, decision of 11.9.2012 – 17703/18222; Yargıtay, decision of 19.1.2015 – 11530/584 (when the images are naked photos of the victim); Yargıtay, decision of 8.12.2014 – 5239/13911; Yargıtay, decision of 16.6.2010 – 2253/4531 (for recordings of sexual intercourse); Yargıtay, decision of 12.6.2012 – 21801/14797 and Yargıtay, decision of 12.6.2012 – 21801/14797 (for recording naked poses via web-cam); Yargıtay, decision of 17.6.2013 – 20606/16477 (when the perpetrator secretly takes photos of the victim's erogenous areas.)

[92] *Eker Kazancı*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 9 (2007), 131 (149); *Tezcan/Erdem/Önok* (fn. 45), p. 624; *Zafer* (fn. 73), p. 196.

[93] *Bayraktar et. al.* (fn. 50), p. 618.

[94] *Akyürek* (fn. 73), p. 232.

[95] See Yargıtay, decision of 8.6.2022 – 1756/4593; Yargıtay, decision of 28.4.2014 – 25960/10207; Yargıtay, decision of 13.10.2014 – 4283/19486: "In order for the crime in § 134/1 to occur, it is not necessary for the person in the image to be identifiable or for the recorded voice to be clear. Secretly recorded sounds fall within the scope of private life, even if they are incomprehensible [...]. Unlike § 134 (1); in § 134 (2), the person whose private life is violated by the sound or image must be recognized or be recognizable, for the disclosure to be accepted."

In a similar vein, a criminal liability may be considered in German criminal law, under § 201a (2) StGB. According to this provision, whoever, without being authorized to do so, makes available a photograph or other image of another person to a third party, which is of such a nature as to significantly damage the reputation of the person depicted, is subject to punishment. This regulation aims to address the so-called cyberbullying via social media.[96] This offense may also be given in individual cases, but is subject to similar limits as criminal liability under §§ 185 et seq. StGB. The reputation of the depicted person must be significantly impaired in terms of nature, intensity, and duration, taking into account the surrounding circumstances.[97] Nude photographs, for this reason, are not automatically considered to meet the criteria, as indicated by a reverse conclusion of § 201a (3) StGB, which states that only nude images of individuals under 18 are covered. Only in conjunction with further circumstances can significant damage occur, for example, when images of sexual acts between married individuals in public spaces are disseminated.[98] Once again, however, there is the objection that the aim of the article is to protect honor as an aspect of general personal rights[99] and that the right to sexual self-determination is of no significance.

According to § 33 KunstUrhG, anyone who disseminates or publicly displays an image contrary to §§ 22, 23 KunstUrhG is punishable. The scope of the offence is very broad, as it is solely about protecting the right to one's own image[100] and therefore does not have to involve any damage to honor. An image is any representation of a person that depicts their external appearance in a way recognizable to others.[101] In terms of this article deepfakes also constitute an image of a person, as it is recognized that photomontages, drawings and computer animations also fall under the scope.[102] However, only public display is included as a punishable act, meaning that making it accessible to third parties, such as friends of the victim, does not constitute the given offense. Furthermore, the right to sexual self-determination does not gain significance in this context either.

V. Perspective on Legal Reform – What should the future legislation look like?

1. Art. 5 of the EU Directive on Combating Violence Against Women and Domestic Violence

EU has very recently introduced a legal framework addressing this topic: Directive 2024/1385 on Combatting Violence Against Women and Domestic Violence of 15.5.2024. Given that both Germany and Türkiye currently lack adequate protection against the deepfake pornography phenomenon[103], Art. 5 of the EU Directive should be considered, when answering the question of to what extent such deepfakes should be penalized in the future. While the Directive is particularly relevant for Germany as a member state, it provides content-related guidance and points of argumentation for a future regulation in Türkiye as well. The Parliament defines the criminalization of producing and sharing deepfake pornography as one of the goals to be achieved by the member states[104] and further outlines a template for criminalization, as follows:

> Article 5 – Non-consensual sharing of intimate or manipulated material
> 1. Member States shall ensure that the following intentional conduct is punishable as a criminal offence:
> (a) making accessible to the public, by means of information and communication technologies ("ICT"), images, videos or similar material depicting sexually explicit activities or the intimate parts of a person, without that person's consent, where such conduct is likely to cause serious harm to that person;
> (b) producing, manipulating or altering and subsequently making accessible to the public, by means of ICT, images, videos or similar material making it appear as though a person is engaged in sexually explicit activities, without that person's consent, where such conduct is likely to cause serious harm to that person.
> (c) threatening to engage in the conduct referred to in point (a) or (b) in order to coerce a person to do, acquiesce to or refrain from a certain act.[105]
> (2) Paragraph 1, points (a) and (b), of this Article does not affect the obligation to respect the rights, freedoms and principles referred to in Art. 6 TEU and applies without prejudice to fundamental principles related to the freedom of expression and information and the freedom of the arts and sciences, as implemented in Union or national law.

[96] BT-Drs. 18/2601, p. 37.
[97] *Eisele/Sieber*, StV 2015, 312 (315 et seq.).
[98] *Eisele* (fn. 35), § 201a para. 41.
[99] *Eisele* (fn. 35), § 201a para. 37; *Gercke*, CR 2014, 687 (690).
[100] For more details on this specific protective purpose of the article see *Valerius*, in: v. Heintschel-Heinegg/Kudlich (eds.), Beck'scher Online Kommentar, Strafgesetzbuch, as at 1.11.2024, KunstUrhG § 33 para. 1.
[101] See BGH NJW 2000, 2201 (2202); BGH NJW 2018, 2489 (2492).
[102] BGH NJW 2004, 596; LG München ZUM-RD 1998, 18 (19); *Valerius* (fn. 100), KunstUrhG § 33 para. 7.
[103] *Babayiğit*, Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi 15 (2021), 655 (689); *Dülger*, İnternet aracılığıyla işlenen suçlar, p. 26, available at http://dx.doi.org/10.2139/ssrn.3792316 (18.1.2025); *Greif* (fn. 20), p. 312; *Retornaz* (fn. 48), p. 84 and 142.
[104] EU Directive 2024/1385, Preamble 19.
[105] *McGlynn/Rackley*, Oxford Journal of Legal Studies 37 (2017), 534 (552), mentioned back in 2017, prior to the EU draft, that the criminalized acts regarding IBSA should also cover threats to distribute images without consent.

Art. 5 (1) (b) of the EU Directive places deepfakes within the broader context of recordings involving sexual acts or intimate body parts, covered in Art. 5 (1) (a) of the EU Directive. The EU justifies the obligation for member states to impose penalties by stating that, due to the use of ICT, such harmful images, photos, and audio and video clips[106], can now be easily, quickly, and widely disseminated.[107] Regarding deepfakes, the Directive states:[108]

> "Such production, manipulation or altering should include the fabrication of 'deepfakes', where the material appreciably resembles an existing person, objects, places or other entities or events, depicts the sexual activities of a person, and would falsely appear to other persons to be authentic or truthful. In the interest of effectively protecting victims from such conduct, threatening to engage in such conduct should also be covered."

2. The Basic Framework of Art. 5 of the EU Directive

a) Art. 5 (1) (a) of the EU Directive requires Member States to penalize the making accessible of images, videos, or similar material via information and communication technologies (ICT) that depict sexually explicit activities or intimate body parts of a person to the public, without that person's consent. The conduct must be likely to cause serious harm to the person depicted. The subject of the recording is therefore sexual acts and intimate body parts of another person, neither of which is further defined in the Directive. In contrast to § 184 StGB and § 226 TCK, it is not necessary for sexually explicit activities to also be classified as pornographic. The prohibited act of Art. 5 (1) (a) of the EU Directive is limited to the unauthorized making accessible of the relevant material to the public, and does not include its production or making it accessible to a third party, such as friends. Moreover, the Directive only covers making accessible via ICT. The serious harm does not have to materialize as an actual result of the offense; it is sufficient that its occurrence is likely. The Directive does not specify what constitutes "serious harm". Regarding the likelihood of serious harm occurring, it states that consideration should be given to "whether the act would typically cause harm to a victim".[109]

b) The regulation on deepfakes in Art. 5 (1) (b) of the EU Directive represents an extension to Art. 5 (1) (a) of the EU Directive. It criminalizes unauthorized production, manipulation, or alteration of relevant material that makes it appear as though a person is engaged in sexually explicit activities. Furthermore, in this two-act offense, the perpetrator must subsequently make the content publicly accessible, and these conducts must be likely to cause serious harm to the person involved as in Art. 5 (1) (a) of the EU Directive. It is important to note that the content of the recording must involve sexually explicit activities, but not intimate body parts. The reasoning behind this may be that purely AI-generated body parts, which do not depict a real person, cannot cause harm to a specific victim and, therefore, do not infringe upon the protected legal interest.

c) Additionally, Art. 5 (1) (c) of the EU Directive requires that the threat of engaging in conduct referred to in points (a) and (b), with the aim of coercing a person to do, acquiesce to or refrain from a certain act, must also be punishable. This paragraph is intended to cover, among other things, coercion involving the use of deepfakes.

d) Finally, Art. 5 (2) of the EU Directive points out that the rights, freedoms, and principles referred to in Art. 6 of the Treaty on European Union (TEU) must be respected. Therefore, the freedom of expression, freedom of information, and the freedom of arts and sciences may lead to the exclusion of criminal liability. Furthermore, the offense "should not cover the handling of material by authorities, in particular to conduct criminal proceedings or to prevent, detect or investigate crime".[110] The Member States should also have the option to "exempt a person from responsibility under specific circumstances, for example where telephone or internet helplines handle material in order to report an offence to authorities."

3. Fundamental Questions Arising

The directive which is adopted in accordance with general principles and especially Art. 83 (1) of TEU, establishes minimum requirements for the Member States, meaning that any already existing provision that is stricter may remain unaffected, and stricter provisions may also be introduced during implementation. When creating new provisions in Turkish and German criminal law, some fundamental questions must first be raised. First, it is important to discuss which legal interest is to be protected. Two main tendencies can be observed worldwide: protecting the images as part of privacy[111], meaning, in the context of criminalized image recording or as part of an individual's sexual autonomy[112], within the framework of sexual criminal law. Then, there are two paths to choose from when it comes to the issue of punishable acts: a more liberal approach would only punish the sharing of such content, either by making it accessible to the public, or to third parties; a second and a stricter stance, on the other hand, would also punish the creation of such con-

[106] Audio clips are also included, EU Directive 2024/1385, Preamble 19.
[107] EU Directive 2024/1385, Preamble 18.
[108] EU Directive 2024/1385, Preamble 19.
[109] EU Directive 2024/1385, Preamble 22.
[110] EU Directive 2024/1385, Preamble 20.
[111] See Article 226-2-1 of the French Criminal Code, which is classified under offences against privacy within Chapter VI, Section I; Article 197 (7) of the Spanish Criminal Code that is classified under criminal offences against privacy, the right to personal dignity and the inviolability of the dwelling in Title X Chapter I.
[112] See for example Article 162 (1) of the Canadian Criminal Code, titled "Publication, etc., of an intimate image without consent" which is classified under Sexual Offences within Part V; Article 208E of the Maltese Criminal Code, titled "Non-consensual taking or disclosure of private sexual photographs and films" which is classified under sexual offences in Part II, Title VII, Subtitle II.

tent.[113] For instance, § 201a (1) no. 1 StGB penalizes also the creation of photographs or other images of another person in private premises, whereas § 201a (2) StGB penalizes only the making accessible to third parties of regarding the image recordings that are likely to cause significant harm to the reputation of the person depicted. Turkish law, on the other hand, penalizes the creation in § 134 (1) TCK and both making it accessible to public and thirds parties in § 134 (2) TCK.[114] It must also be discussed whether the victim of the offense must be identifiable. In the case of deepfakes that combine the body and face of different individuals, the question arises whether there can be just one victim or possibly multiple victims. Identifiability is, for example, required under § 201a (1) StGB[115]; but not in the case of upskirting under § 184k StGB.[116] It has been explained above, that in line with the Turkish supreme court ruling, the identifiability criterion applies for Türkiye, within the framework of § 134 (2) TCK. Furthermore, the question arises as to which actions or body parts should be the subject of the recordings. Finally, it must be determined whether the offense should be classified as a conduct- or a result-based crime. In any case, for Germany, it should be noted that "serious harm" as defined in Art. 5 (1) of the EU Directive is excluded from constituting the result element of the offense. According to the Directive, it is sufficient that the actions "are likely to cause serious harm to the person concerned". Therefore, only a crime of abstract endangerment, or in accordance with § 238 StGB, a suitability offense should be considered.[117]

The following will address the implementation of the Directive in Germany and the creation of a corresponding criminal offense in Türkiye. The goal of this paper is not to propose identical provisions for both countries, as this is also precluded by the fact that Germany is obligated to implement the Directive and is thus bound by its substantive requirements, while Türkiye is not. Above all, the aim is to create a consistent domestic regulation that fits into each country's national legal framework and takes into account its specific legal principles and values. This will lead to differences, which will be addressed in the discussion of the implementation of the Directive in Germany and the proposal for a regulation in Türkiye.

4. Addressing Deepfake Pornography in Turkish Criminal Code: Establishing a New Provision

The new regulation prohibiting the creation and sharing of deepfake pornography should be included under "Offences against sexual integrity"[118] of the Turkish Criminal Code as § 105/A.

a) Proposal for a new regulation as § 105/A TCK:

> (1) A person who by means of information and communication technologies (ICT) produces, manipulates, alters or shares any form of visual of a person, without that person's consent, which depicts the person as though the person is engaged in sexually explicit activities shall be punished with imprisonment from two to five years, when the aforementioned visual can be assigned to a real person. The same penalty shall apply if the visuals are disclosed through the press or media.
> (2) The penalty shall be increased by one-fold if the offence is committed by a former or current partner or spouse or if any part of the depicted visual belongs to a child in terms of 226 (3).

b) Justification

aa) The new crime has been envisioned as a sexual offense § 105/A TCK to follow § 105 TCK "Sexual Harassment", which regulates sexual behaviors without physical contact.[119] § 105/A envisions the protection of the sexual freedom of individuals.[120]

bb) Regarding the prohibited actions, Turkish law has adopted the stricter approach, envisioning not only the punishment for sharing the deepfake pornographic content, meaning making it accessible to the public or third parties,

[113] See *McGlynn/Rackley*, Oxford Journal of Legal Studies 37 (2017), 534 (556): "Given the diverse forms of image-based sexual abuse, the law must cover the non-consensual creation as well as distribution of private sexual images, including images that have been manipulated".

[114] See *Akyürek* (fn. 73), p. 205–206 where the forbidden act of "disclosing" under § 134 (2) TCK is used to mean sharing, which encompasses both sharing with the public and sharing with third parties.

[115] BGH NStZ 2015, 391; *Eisele*, in: Schönke/Schröder, Strafgesetzbuch, Commentary, 30th ed. 2019, § 201a para. 7; contra *Kargl*, ZStW 117 (2005), 324 (340).

[116] BT-Drs. 19/20668; BT-Drs. 19/15825, p. 16 et seq.; *Eisele* (fn. 35), § 184k para. 8.

[117] As for the types of offenses see *Eisele*, in: Baumann/Weber/Mitsch/Eisele, Strafrecht, Allgemeiner Teil, 13st ed. 2021, § 6 paras. 49 et seq.

[118] See also *McGlynn/Rackley*, Oxford Journal of Legal Studies 37 (2017), 534 (556) for the view that it is vital to see these forms of abuse as sexual offences. *Idem* (fn. 1), p. 557, that this will also encourage integration of preventive measures into broader efforts to tackle violence against women.

[119] See *Dülger* (fn. 104), p. 18–19: "Non-consensual pornography and revenge pornography should be included in criminal laws either as a variant or form of sexual harassment, or as an independent criminal offense, as they represent an attack on sexual integrity."

[120] *Retornaz*, (fn. 48), p. 85 and 142, proposes the only concrete draft of a new offense so far in Turkish literature. Differing from the view advocated here, she calls for the addition of the new provision, § 136/A, under Offenses Against Privacy and Confidentiality, as a continuation of the offense of Unlawfully Obtaining and Disclosing Personal Data in § 136 TCK.

but also for its production.[121] In this sense, a parallel has been established with § 134 TCK, which also penalizes the creation of the non-manipulated visual material ("recording of images or sounds"), ensuring consistency within the criminal code. With particular regard to the nature of conduct involving deepfake pornography, it is often observed that not only the sharing of such content is done without the victim's consent, but also its creation—sometimes even without the victim's awareness. Punishing only the sharing of a deepfake content would, therefore, overlook the aspect of involuntary creation.[122] Mere possession of the material is not punishable.

cc) The crime is a conduct-based crime under Turkish law. The completion of the offense does not require any harm or damage to occur to the victim.[123] The proposed draft under Turkish law deviates from the EU Directive in this regard which seeks to introduce a suitability offense, where the acts should be "likely to cause serious harm" to that victim.

dd) To ensure integrity within the Turkish criminal law system, identifiability of the victim is stated as a statutory element of § 105/A TCK, with respect to the discussions regarding § 134 (2) TCK. Hence, the victim of § 105/A TCK will be the person whose face is used in the first place. If additional markers, such as birthmarks or specific tattoos allow for the identification of a person's identity, the person whose body is used can also be considered a victim.[124]

ee) The commission of a crime by current or former partners is considered an aggravating circumstance under Turkish criminal law. This is especially important given the prevalence of violence, including sexual violence, against women in Turkey, as well as the reduced protection opportunities following the country's withdrawal from the Istanbul Convention. The EU Directive also recommends recognizing offenses committed by current or former partners as an aggravating circumstance.[125]

ff) With the specific aim of child protection, an additional aggravating circumstance is established: the use of the visuals of a child's face or body in the production of deepfake pornography. In this case, the criterion of identifiability will also be waived, meaning that the visuals do not need to be attributable to a specific child.

gg) As repeatedly emphasized in the text, the crime can be committed intentionally, meaning that the perpetrator either directly intends to carry out the conduct or is almost certain of the consequences of their actions. The act does not need to be driven by any specific objective or motive, such as satisfying sexual desires[126], seeking revenge, competition, gaining financial benefits or intending to harm the victim.[127] In offenses aimed at a person's sexual freedom, the inclusion of a motive is unnecessary:

> "Whatever the motivation of the perpetrator, the harm is similar and significant for the victim."[128]

It is sufficient for the perpetrator to be aware of the consequences of their actions[129]. However, the perpetrator must know about the lack of consent in the creation and/or the sharing of the deepfake visual[130], for the mens rea to be established.

hh) A specific provision for justifications related to artistic or scientific purposes is not required under Turkish law. § 26 TCK serves as a general justification clause here, when it can be claimed that pornographic content created using deepfake technology was produced for artistic or scientific purposes.

ii) In accordance with the Directive, the "yes means yes" principle is implemented. Only explicit consent from the victim excludes criminal liability; meaning that it is not sufficient for the act to be performed without the victim's objection. Only explicit consent from the victim on creating or

[121] *Babayiğit*, Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi 15 (2021), 655 (691): "In the production of a pornographic product involving deepfake content, if the consent of the individuals whose appearances are used is lacking, there is no doubt that even merely producing such a content constitutes an injustice."; *McGlynn/Rackley*, Oxford Journal of Legal Studies 37 (2017), 534 (552): "The law must cover the non-consensual creation as well as distribution of private, sexual images, including images that have been manipulated"; *Retornaz* (fn. 48), p. 105; Cf. EU Directive 2024/1385, Preamble 19. Although the new EU-Directive punishes the non-consensual production, this is dependent on the condition that the material subsequently be made accessible to the public.

[122] *McGlynn*, Deepfake porn: why we need to make it a crime to create it, not just share it; available at https://theconversation.com/deepfake-porn-why-we-need-to-make-it-a-crime-to-create-it-not-just-share-it-227177 (21.1.2025).

[123] See also *Retornaz* (fn. 48), p. 105.

[124] See also *Retornaz* (fn. 48), p. 101.

[125] EU Directive 2024/1385, Article 11 point k; *Retornaz* (fn. 48), p. 97 and 142: The *author* also drafts the acts of former or current spouse or partner as an aggravating circumstance.

[126] *McGlynn/Rackley*, Oxford Journal of Legal Studies 37 (2017), 534 (552): "The law should only require the intention to create and/or distribute private sexual images without consent, that is, there should be no additional element of maliciousness."

[127] See *Yavuz* (fn. 10), p. 138.

[128] *McGlynn/Rackley*, Oxford Journal of Legal Studies 37 (2017), 534 (552).

[129] See *Delfino*, Fordham Law Review 88 (2019), 887 (919), further emphasizes that subjective elements such as harm, fear or emotional distress as a result of the acts of perpetrator are hard to prove at trials. The author also highlights that requiring the existence of additional elements gives the message as if "the public display of victims' bodies engaged in revealing or sexually explicit behavior without their consent is insufficient, standing alone, to warrant the law's attention"; *Gieseke*, Vanderbilt Law Review 73 (2020), 1479 (1510).

[130] *Retornaz* (fn. 48), p. 117.

sharing the deepfake pornographic visual can negate the actus reus.[131]

jj) The need to implement Art. 5 (1) (c) of the EU-Draft does not arise for the Turkish provision. Threats, addressed at the sexual integrity of a person are already punishable under § 106 (1) TCK. § 105/A TCK, being envisioned as a sexual crime, falls within the scope of § 106 (1) TCK.

kk) The range of punishment is in accordance with § 134 TCK and complies with the requirements of the EU Directive.

5. Implementing the Directive into the German Criminal Code

a) The protected legal interest

First, the question arises as to which section of the StGB the guidelines should be implemented in. One possibility is implementing them in connection with § 201a StGB – violation of intimate privacy through taking photographs – could be considered, which violates the most intimate personal sphere. The focus of the protection of legal interests would then be on the general right of personality, so that the most intimate personal sphere would be protected.[132] However, a more convincing approach would be to implement the guidelines in connection with sexual offenses, as they explicitly tie to sexually explicit activities, which is further defined in § 184h StGB. Similar to the issue of upskirting under § 184k StGB, this would protect not only the right to one's own image but also the right to sexual self-determination, which includes the right to decide to what extent the depiction of one's intimate areas by others is permissible.[133]

b) Implementing solely the requirements of the directive ("Kleine Lösung")

Looking solely at the requirements of Art. 5 of the EU Directive, these could be regulated in a separate criminal offense, without comprehensively addressing the issue of sexually related recordings in the sense of a "broader solution".[134]

aa) Proposal for an implementation

> (1) Whoever unlawfully disseminates or makes content available to the public that involves sexual acts, bare genitalia or buttocks, or the female breast of another person in a manner that is suited to cause significant harm to that person shall be punished with imprisonment of up to two years or a fine.
> (2) Whoever unlawfully produces, alters, or modifies content that gives the impression that another person is performing sexual acts, and disseminates or makes it available to the public in a manner that it suited to harm that person, incurs the same penalty.
> (3) Whoever threatens another person with actions as described in paragraphs 1 and 2, in order to coerce them into performing, acquiescing or refraining from an action, incurs the same penalty.
> (4) The offense will only be prosecuted upon complaint, unless the prosecuting authority deems it necessary to intervene ex officio due to the special public interest in prosecution.
> (5) Paragraph 1 and paragraph 2 do not apply to acts done by way of exercising overriding legitimate interests, namely those serving the arts or science, research or teaching, to report about current or historical events, or for similar purposes.
> (6) The image media and image recording devices or other technical means used by the offender or participant may be confiscated. § 74a StGB applies.

bb) Justification

(1) In line with the standard terminology of the StGB, disseminating and making available to the public are included as the forbidden acts. However, it would also be justifiable to go beyond what the Directive envisages and penalize the act of production in paragraph 1.[135]

Instead of using the word "image recording" (Bildaufnahmen), the modern term of content is used as terminology, which fills the gaps left by ICT.[136] Another factor is that, the word "content" also covers audio recordings, which is explicitly required by Art. 5 of the EU Directive.[137] The term of "intimate parts" used in the Directive, is specified in accordance with § 184k StGB to include genitals, buttocks or the female breast, to take the principle of certainty enshrined in Art. 103 (2) GG into account. As with § 201a StGB and unlike § 184k StGB[138] – the "other person" must be identifiable, although this does not need to be explicitly regulated. This is already evident for deepfakes, as there would otherwise be no protectable victim in the case of purely AI-generated images. The extent to which intimate body parts can be identified depends on the individual case. This may be the case with specific tattoos. In the case of AI-generated compositions of head and body, the protectable victim would be the person whose face is recognizable.

Instead of requiring a probability of serious harm as an element of the offense, a suitability offense is established in accordance with § 238 StGB[139]. Given the vague concept of serious harm, which refers to professional or private disadvantages caused by the making accessible of the content (such as significant damage to reputation, as in § 201a (2) (d) StGB), it would also be justifiable to give up on a continuing result as in the proposal for Turkish criminal law. Because by

[131] *Retornaz* (fn. 48), p. 123.
[132] See BT-Drs. 19/17795, p. 12 regarding § 201a StGB; BGH NStZ 2015, 391; *Eisele* (fn. 35), § 201a Rn. 3.
[133] BT-Drs. 19/20668, p. 15; Bay VGH BeckRS 2021, 41318; *Eisele/Straub*, KriPoZ 2019, 367 (370); *Eisele* (fn. 35), § 184k Rn. 3.
[134] See also *Eisele/Straub*, KriPoZ 2019, 367 et seq.
[135] Compare it with the proposal infra V. 5. c).
[136] BT-Drs. 19/19859, p. 26 et seq., 62; *Eisele* (fn. 35), § 184 para. 7.
[137] See supra V. 1 and 2.
[138] See supra V. 3.
[139] See supra V. 3.

making the content publicly available, the right to sexual self-determination is already violated, thus fulfilling the result element of the offense. As the directive contains only minimum requirements, this more extensive penalization would be permissible and would also ensure consistency with § 184k StGB. Accordingly, the penalty range is also aligned with § 184k StGB, making it significantly lower than in the proposal for the TCK.

(2) These considerations also apply to paragraph 2, which follows the directive closely. Since, in addition to the act of producing, altering or modifying the subsequent dissemination or making available to the public is required, it could also be justified here to forgo the classification as a suitability offense. In contrast to the proposal for the Turkish Criminal Code, producing deepfakes should not be penalized, as criminalizing this would extend too far into the preliminary stages of the conduct. Unlike real photos or recordings, deepfakes do not directly violate the right to sexual self-determination at that stage yet.

(3) Paragraph 3 merely closes the gaps left by §§ 240, 241 StGB. These are cases where coercion does not materialize as an actual result of the offense under § 240 StGB or when there is no threat of a sexual offense as § 241 (1) StGB describes. In accordance with § 184k StGB, paragraph 4 of the proposal establishes an offense that cannot be prosecuted without a complaint by the victim. In accordance with §§ 184k (3) and (4) StGB, as well as §§ 201a (4) and (5) StGB, paragraph 5 of the proposal introduces a justification for the protection of legitimate interests, and paragraph 6 establishes a provision on confiscation. The regulation in paragraph 5 also complies with the requirements of Art. 5 (2) of the Directive, which explains the difference compared to the proposal for the Turkish Penal Code.

c) Broader reform ("Große Lösung")

In German criminal law, there is a rather fragmented regulation regarding nude images of children (§ 201a (3) StGB), violation of the intimate area through image recordings (§ 184k StGB), which are supplemented by § 33 KunstUrhG. Taking into account Art. 5 of the EU Directive, the following regulation, is proposed, which penalizes deepfakes in paragraph 2, point 4.

aa) Proposal

(1) Anyone who unlawfully creates content will be punished with imprisonment for up to two years or a fine, if the content
1. has sexual acts of another person as its subject,
2. depicts the uncovered genitals, uncovered buttocks, or uncovered female breast of another person,
3. depicts the genitals, buttocks, or female breast of another person covered by underwear, as long as these areas are protected from view.

(2) The same penalty incurs to whomever unlawfully,
1. disseminates or makes accessible to a third party content as described in paragraph 1.
2. disseminates or makes available to the public content that depicts the nudity of another person
3. creates or offers content that depicts the nudity of another person under the age of eighteen, with the intent to provide it to a third party for payment, or acquires it for themselves or a third party for payment.
4. creates, falsifies, or alters content in such a way that it creates the impression that another person is engaging in sexual acts and then distributes or makes this content publicly accessible.

(3) The offense will only be prosecuted upon complaint, unless the prosecuting authority deems it necessary to intervene ex officio due to the special public interest in prosecution.

(4) Paragraph 1 and paragraph 2 do not apply to acts done by way of exercising overriding legitimate interests, namely those serving the arts or science, research or teaching, to report about current or historical events, or for similar purposes.

(5) The image media and image recording devices or other technical means used by the offender or participant may be confiscated. § 74a applies.

bb) Justification

(1) In paragraph 1, numbers 1 and 2, the requirements of Art. 5 (1) of the EU Directive are implemented. Furthermore, the conduct of upskirting is integrated into the provision. For pictures or video recordings of underwear that are not regulated by the Directive, it is still required that these be protected from view, as § 184k (1) StGB stipulates. Due to the significant violation of the right to sexual self-determination, the creation of a photograph should always be punishable in this regard.

(2) Paragraph 2, number 1, extends the offenses in accordance with § 184k (1) no. 2 StGB. According to the newly established number 2, the dissemination and making available to the public of nude images of adults is now also punishable. Mere production is not to be included in this respect, unless the requirements of § 201a StGB are met.[140] In number 3, the previous § 201a (3) StGB has been adopted, which extends protection for nude images of minors. Finally, number 4 regulates deepfakes, for which, unlike in the Directive, no requirement for a "suitable result" is needed. However, the mere creation of such deepfakes should not be penalized in this regard.[141]

(3) For paragraphs 3 to 5, reference can be made to the comments regarding the "kleine Lösung".[142]

[140] For an insight see *Eisele/Straub*, KriPoZ 2019, 367 (373 et seq.).
[141] See supra V. 5. b) bb) point 2.
[142] See supra V. 5. b) aa).