Täuschend echt, strafrechtlich relevant? Zur Regulierung von Deepfakes vor dem Hintergrund des § 201b StGB-E

*von Johannes Härtlein**

Abstract
Der Beitrag analysiert den Entwurf des § 201b StGB-E vor dem Hintergrund neuartiger Erscheinungsformen von Deepfakes, die in der bisherigen Literatur noch weitgehend unbeachtet geblieben sind. Neben Deepfake-Pornografie werden gefälschte Werbeinhalte, Identitätsdiebstahl in Videokonferenzen und der Einsatz von Echtzeit-Deepfakes in Gerichtsverhandlungen untersucht. Auf dieser Grundlage wird geprüft, inwieweit das geltende Strafrecht solche Konstellationen bereits erfasst und wo Strafbarkeitslücken verbleiben. Unter Einbeziehung der KI-Verordnung und der Gewaltschutzrichtlinie bewertet der Beitrag den § 201b StGB-E als unionsrechtskonform, jedoch in seiner Reichweite partiell unzureichend. Die Beschränkung auf täuschungsbasierte Sachverhalte lässt zentrale Missbrauchsformen, insbesondere im höchstpersönlichen Lebensbereich, unberücksichtigt. Vorgeschlagen wird eine erweiterte Ausgestaltung nach französischem Vorbild sowie die Einführung einer besonderen Irrtumsregelung.

The article analyzes the draft of Section 201b of the German Criminal Code against the backdrop of novel forms of deepfakes that have so far received little attention in the academic literature. In addition to deepfake pornography, the study examines falsified advertising content, identity theft in video conferences, and the use of real-time deepfakes in court proceedings. On this basis, it assesses the extent to which existing criminal law already covers such scenarios and where gaps in criminal liability remain. Taking into account the EU Artificial Intelligence Act and the Victims' Rights Directive, the article concludes that Section 201b StGB-E is consistent with Union law, but its scope is partially insufficient. The restriction to deception-based cases fails to address key forms of abuse, particularly in highly personal spheres of life. The paper therefore proposes an expanded design following the French model and the introduction of a specific rule on mistake.

I. Einleitung

Künstliche Intelligenz spielt in der Gesellschaft eine immer größer werdende Rolle. Neben dem Einsatz in Medizin und Wirtschaft wird KI auch verstärkt zur Generierung von Medien genutzt. So können Bilder, Videos und Audioinhalte durch KI-Anwendungen täuschend echt erzeugt werden.[1] Diese Entwicklung wird kritisch beobachtet. Es befindet sich derzeit eine Petition im Bundestag, die ein Verbot von Deepfakes fordert.[2] Durch die Einfügung eines neuen Straftatbestandes in Italien, der den Umgang mit Deepfakes in bestimmten Fällen unter Strafe stellt,[3] ist das Thema generativer KI auch in Deutschland weiter in den Fokus geraten. Der Bundesrat hat mit dem Vorschlag einer neuen Strafnorm auch hierzulande einen Gesetzgebungsprozess angestoßen, der den Umgang mit Deepfakes regulieren soll.[4]

Dieser Beitrag hat zum Ziel, ausgewählte Problemstellungen im Zusammenhang mit Deepfakes zu beleuchten und davon ausgehend eine Bewertung des aktuellen Gesetzgebungsvorhabens vorzunehmen. Hierzu soll zunächst der Begriff „Deepfake" näher erläutert werden. Anschließend erfolgt eine Darstellung der verschiedenen Anwendungsbereiche generativer KI. Davon ausgehend wird geprüft, inwieweit die aktuell geltenden Strafnormen dazu in der Lage sind, bestimmten negativen Nutzungen dieser Systeme zu begegnen. Nach einer Auseinandersetzung mit den europarechtlichen Vorgaben schließt der Beitrag mit einer Prüfung, ob der vorgeschlagene § 201b StGB-E sowohl die ausgemachten Schwachstellen schließen als auch die an ihn gestellten Anforderungen erfüllen würde.

II. Begriffsdefinitionen

Der vorliegende Beitrag widmet sich der rechtlichen Behandlung von Deepfakes. Hiervon sind Cheapfakes und synthetische Medien abzugrenzen. KI-Systemen kommt dabei ebenfalls Bedeutung zu.

„Deepfake" ist ein Kofferwort aus den Begriffen „Deep Learning" und „Fake". Hiervon werden Inhalte erfasst, die durch künstliche Intelligenz erstellt oder verändert wurden und eine gewisse Qualität aufweisen. Die europäische KI-Verordnung definiert einen Deepfake als „*einen durch KI erzeugten oder manipulierten Bild-, Ton- oder Videoinhalt, der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt und einer Per-*

* *Johannes* Härtlein ist Wissenschaftlicher Mitarbeiter am Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtstheorie, Informationsrecht und Rechtsinformatik von Herrn *Prof. Dr. Dr. Eric Hilgendorf* in Würzburg. Der Beitrag beruht auf Teilen seiner Dissertation, die 2026 erscheinen wird.

1 Eine gute Möglichkeit, seine eigenen diesbezüglichen Fähigkeiten zu testen, findet sich auf der Website https://www.whichfaceisreal.com/. Dort muss man generierte Inhalte von echten Fotos unterscheiden.
2 Petition 179446, abrufbar unter: https://epetitionen.bundestag.de/petitionen/_2025/_03/_19/Petition_179446.nc.html.
3 Dort gilt seit dem 10.10.2025 der Art. 612-quater Codice Penale.
4 BT-Drs. 21/1383.

son fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde.“[5] Diese Definition ist jedoch nur eine von vielen.[6] Die Begriffsverständnisse variieren dabei in Abbildungsgegenstand und Qualität der Darstellung.[7] Nachfolgend werden Deepfakes als Video-, Bild- oder Audioinhalte verstanden, die mithilfe von Deep Learning erzeugt werden und zumindest realitätsnahe Darstellungen *von Personen* zeigen. Deepfakes und generierte Inhalte, die diese Voraussetzungen nicht erfüllen, werden oberbegrifflich als synthetische Medien bezeichnet.[8] Cheapfakes sind dagegen künstlich erzeugte oder veränderte Inhalte, die ohne den Einsatz von KI hergestellt wurden.[9] Wann eine Anwendung als KI-System zu qualifizieren ist, ist im Einzelnen umstritten und v.a. im Kontext europarechtlicher Regulierung noch nicht eindeutig geklärt.[10] Für die vorliegenden Ausführungen soll es genügen, dass eine Softwareanwendung dann *kein* KI-System ist, wenn die wesentlichen Arbeitsschritte durch einen Menschen vorgenommen werden. Klassische Bildbearbeitungsprogramme oder auch die digitale Manipulation von Tonspuren gelten somit nicht als Anwendungen künstlicher Intelligenz.

III. Anwendungsbereiche

1. Allgemeine Einsatzgebiete

Im Rahmen einer strafrechtlichen Betrachtung liegt der Fokus naturgemäß auf den schädlichen Nutzungsmöglichkeiten. Es soll jedoch nicht außen vor gelassen werden, dass Deepfakes in vielen Bereichen einen wertvollen Beitrag leisten können. Hierzu gehören etwa Kultur und Lehre. Durch den Einsatz von generativer KI werden beispielsweise Museen in die Lage versetzt, ihre Besucher in den unmittelbaren Austausch mit historischen Personen zu bringen.[11] Daneben könnte Deep Learning bei der Aussage von gefährdeten Zeugen oder auch bei Ermittlungsmaßnahmen der Strafverfolgungsbehörden zukünftig eine tragende Rolle spielen.[12] Den nachfolgenden Ausführungen sollte daher zu Grunde gelegt werden, dass nicht die Verfügbarkeit generativer Software an sich, sondern deren Fehlgebrauch zur Gefährdung von Rechtsgütern führt. Die Möglichkeit, jede Person digital abbilden und steuern zu können, eröffnet hierzu einige Optionen. Grundsätzlich kann hierbei die Schädigung von Individuen und die Schädigung von Kollektiven unterschieden werden.

Verhaltensweisen, die den Einzelnen betreffen, sind Betrug,[13] Erpressung,[14] Persönlichkeitsrechtsverletzungen und die Übernahme fremder Identitäten. Von allen Deepfakes machen Persönlichkeitsverletzungen in Form von Deepfake-Pornografie den Löwenanteil aus.[15] Frauen werden in pornografische Inhalte animiert oder es werden direkt neue, gewillkürte Inhalte erstellt.[16]

Die gemeinschädliche Nutzung von KI zeigt sich dagegen in allgemeiner,[17] marktmanipulativer[18] oder demokratiebezogener Desinformation. Hinsichtlich der Beeinflussung von Wahlen ereignete sich 2023 in der Slowakei eine eindrückliche Begebenheit: Zwei Tage vor der Stimmabgabe wurde ein Audio-Mitschnitt veröffentlicht, aus dem hervorgeht, dass der Vorsitzende einer Partei mit einer Journalistin über die Manipulation der Wahl telefoniert.[19] Außerdem ist in einer weiteren Sequenz zu hören, wie er über eine geplante Erhöhung der Bierpreise spricht.[20] Weder die Aussage noch das Telefonat haben jemals stattgefunden.[21]

Damit kann man festhalten: Generative KI-Systeme verändern nicht nur die Gesellschaft allgemein, sondern auch die Kriminalität. Teils werden neue Verhaltensweisen erst ermöglicht, teils bekannte Verhaltensweisen um eine KI-Komponente erweitert. Es kann dabei beobachtet werden, dass Täter nicht mehr auf die Mitwirkung ihrer Opfer oder Dritter angewiesen sind. Der Taterfolg wird durch KI weitgehend vom Opferverhalten entkoppelt.

---

5 Art. 3 Nr. 60 Verordnung (EU) 2014/1689.

6 Einen Überblick über die verschiedenen Begriffsverständnisse bietet *Whittaker et al.*, Mapping the deepfake landscape for innovation, Technovation 125 (2023), S. 10.

7 Zu der Schwierigkeit einer Definition im rechtlichen Kontext s. *Pölle*, RDi 2025, 452 (453).

8 So auch *Pawelec/Bieß*, Deepfakes, 2021, S. 23.

9 *Lossau*, Deep Fake: Gefahren, Herausforderungen und Lösungswege, Analysen & Argumente, Konrad-Adenauer-Stiftung, 2020, S. 5.

10 *Hilgendorf/Härtlein*, HK-KI-VO, 2025, Vorb. Art. 1 Rn. 5 ff.

11 Diese Technik nutzt ein Museum in den USA, um *Salvador Dalí* für die Besucher wieder zum Leben zu erwecken. Auch die ZDF-Serie „Deepfake Diaries“ macht sich das Prinzip zu Nutze, https://www.zdf.de/dokus/deepfake-diaries-100 (zuletzt abgerufen am 5.11.2025).

12 *Margerie/Hartmann*, EuDIR 2025, 84.

13 Hierbei wird der „Enkeltrick“ um Audiodeepfakes erweitert, Polizeiliche Kriminalprävention der Länder und des Bundes, 4.9.2025, abrufbar unter: https://www.polizei-beratung.de/aktuelles/detailansicht/betrug-mit-hilfe-von-kuenstlicher-intelligenz/ (zuletzt abgerufen am 5.11.2025).

14 Dabei werden zunächst explizite Inhalte einer Person erstellt. Anschließend wird mit der Veröffentlichung gedroht, sollte eine bestimmte Geldsumme nicht bezahlt werden, FBI, 5.6.2023, abrufbar unter: https://www.ic3.gov/PSA/2023/psa230605 (zuletzt abgerufen am 5.11.2025).

15 Eine Studie aus dem Jahr 2023 geht davon aus, dass es sich dabei um 98 % aller Deepfakes handelt, Home Security Heroes, 2023 State of Deepfakes, abrufbar unter: https://www.securityhero.io/state-of-deepfakes/#key-findings (zuletzt abgerufen am 5.11.2025).

16 Vgl. hierzu ausführlich *Diedrich/Lippitz*, Kriminalität und Künstliche Intelligenz, 2024, S. 38 ff.

17 Zu Beginn des Krieges in der Ukraine wurde ein KI-Video ausgestrahlt, auf dem zu sehen ist, wie *Zelensky* seine Truppen zur Kapitulation aufruft, Die Zeit, 17.3.2022, abrufbar unter: https://www.zeit.de/news/2022-03/17/meta-loescht-gefaelschtes-selenskyj-video (zuletzt abgerufen am 5.11.2025).

18 Nachdem 2024 das Bild eines Angriffs auf das Pentagon publik wurde, beeinflusste dies den Aktienmarkt unmittelbar, vgl. hierzu *Tilson/Eichinger*, BKR 2024, 648.

19 Bloomberg, 4.10.2023, abrufbar unter: https://www.bloomberg.com/news/newsletters/2023-10-04/deepfakes-in-slovakia-preview-how-ai-will-change-the-face-of-elections (zuletzt abgerufen am 5.11.2025).

20 CNN, 1.2.2024, abrufbar unter: https://edition.cnn.com/2024/02/01/politics/election-deepfake-threats-invs/index.html (zuletzt abgerufen am 5.11.2025).

21 AfP, 28.9.2023, abrufbar unter: https://fakty.afp.com/doc.afp.com.33WY9LF (zuletzt abgerufen am 5.11.2025).

2. Einzelne Erscheinungsformen

Neben den allgemeinen Missbrauchsoptionen eröffnet die Verfügbarkeit von generativer KI auch Verhaltensweisen, die bisher nur wenig Aufmerksamkeit erfahren haben, da sie nur vereinzelt oder noch gar nicht zu beobachten sind. Hierzu gehört gefakte Werbung mit Prominenten ohne deren Zustimmung. Diese lässt sich in zwei Gruppen unterteilen. Zum einen werden Werbeclips mit Personen des öffentlichen Lebens kommerziell für echte Firmen angeboten.[22] Das zu bewerbende Unternehmen kann individuelle Vorgaben zur Werbeperson und Werbeaussage machen, welche dann von einem kommerziellen Dienstleister umgesetzt werden.[23] Daneben machen auch Kriminelle Gebrauch von dieser Möglichkeit, indem sie Prominente für dubiose Anlageprodukte oder falsche Gewinnspiele werben lassen.[24]

Des Weiteren können mittels Deepfakes sensible Informationen in Erfahrung gebracht werden.[25] Die voranschreitende Digitalisierung hat zur Folge, dass auch vertrauliche Informationen in Videocalls ausgetauscht werden. Hierzu gehört etwa die vermehrte Nutzung von Onlinevernehmungen durch die Polizei oder auch das Angebot ärztlicher und therapeutischer Leistungen via Onlinesprechstunde. Auch wenn auf diese Weise eine Kommunikation „*von Angesicht zu Angesicht*"[26] simuliert wird, ist nicht mehr mit Sicherheit festzustellen, wem man sich gegenübersieht. Echtzeit-Deepfakesoftware führt hier zu großer Täuschungsgefahr.[27]

Neben dem unbefugten Abgreifen von Informationen ist es auch möglich, unbefugt Informationen in den Verkehr zu bringen. Im Rahmen der Desinformation geschieht dies, indem etwa Politikern Aussagen in den Mund gelegt werden. Ein besonders sensibles Thema im Zusammenhang mit Identitätsdiebstahl, das materiellrechtlich bisher noch wenig Aufmerksamkeit erfahren hat, besteht in Videoverhandlungen vor Gericht. Durch Deepfake-Software ist es möglich, das Erscheinungsbild eines Zeugen ohne wesentliche zeitliche Verzögerungen zu übernehmen und so glaubhaft eine eigene Aussage unter der Identität eines Zeugen zu tätigen.[28]

IV. Erfassung durch aktuelle Rechtslage

Sofern bereits bekannte Verhaltensweisen lediglich angepasst oder optimiert werden, bestehen bei deren strafrechtlicher Erfassung meist keine Schwierigkeiten. Dies gilt etwa für die technikoffenen Vermögensdelikte. Wird eine Person durch eine KI-generierte Stimme getäuscht und überträgt daraufhin irrtümlich Vermögenswerte, macht sich der Täter nach § 263 StGB strafbar. Wird einer Person die Veröffentlichung KI-generierter pornografischer Inhalte von ihr in Aussicht gestellt, sofern die Person einen bestimmten Geldbetrag nicht überweist, so liegt eine Erpressung nach § 253 StGB vor. Auch die gezielte Manipulation von Aktienmärkten kann über § 119 Abs. 1 Nr. 1 WpHG und § 263 StGB angemessen abgebildet werden. Allgemein wird die Verbreitung von Deepfakes auch von § 33 KUG erfasst.[29] Entgegen einer in der Literatur vermehrt vertretenen Auffassung ist § 201a StGB auf synthetische Inhalte aber weder im Rahmen des Abs. 1 noch des Abs. 2 anwendbar.[30] Probleme ergeben sich v.a. bei Sachverhalten, die bisher nicht oder nicht in nun möglicher Qualität denkbar waren. Im Folgenden wird anhand der aufgezeigten Problempunkte dargestellt, dass generative KI das geltende Strafrecht punktuell an seine Grenzen bringt.

1. Deepfake-Pornografie und das Beleidigungsstrafrecht

Wird KI dazu eingesetzt, um Menschen ohne deren Zustimmung zum Gegenstand pornografischer Inhalte zu machen, so könnte man hierin ein nach §§ 185 ff. StGB relevantes Verhalten erblicken. Eine Beleidigung gem. § 185 StGB ist die Kundgabe der Miss- oder Nichtachtung.[31] Eine üble Nachrede nach § 186 Abs. 1 StGB liegt dagegen vor, wenn eine unwahre und ehrrührige Tatsache in Beziehung auf einen anderen behauptet oder verbreitet wird. Maßgebliches Abgrenzungskriterium ist die Qualifikation einer Äußerung als Tatsache oder Werturteil. Als

22 So wurde bspw. *Eckart von Hirschhausen* unfreiwilligerweise zur Werbefigur für Diätmittel, Tagesspiegel, 27.1.2025, abrufbar unter: https://www.tagesspiegel.de/gesellschaft/betrug-mit-deepfakes-hirschhausen-will-mehr-uber-ki-reden-13090987.html (zuletzt abgerufen am 5.11.2025).
Zum nachfolgenden Rechtsstreit s. *OLG Frankfurt a.M.*, GRUR-RS 2025, 3551.

23 Bekannt wurde hiermit vor einigen Jahren das Unternehmen Rephrase AI, das mittlerweile von Adobe übernommen wurde, https://www.faz.net/pro/digitalwirtschaft/ki-revolution-in-der-werbung-19102120.html (zuletzt abgerufen am 5.11.2025). Rephrase AI handelte allerdings nicht ohne die Zustimmung der Werbefiguren.

24 Vgl. hierzu näher Verbraucherzentrale Thüringen, 9.7.2025, abrufbar unter: https://www.vzth.de/pressemeldungen/vertraege-reklamation/verbraucherzentrale-warnt-vor-deepfakewerbung-mit-promis-108987 (zuletzt abgerufen am 5.11.2025).

25 Seit dem Jahr 2022 kommt es wiederholt vor, dass europäische Politiker in Videocalls über die Identität ihres Gegenübers getäuscht werden. So etwa bei *Franziska Giffey*, Deutschlandfunk, 27.6.2022 abrufbar unter: https://www.deutschlandfunk.de/mediasres-fakes-in-der-politik-100.html (zuletzt abgerufen am 5.11.2025) oder *David Cameron,* The Guardian, 8.6.2024, abrufbar unter: https://www.theguardian.com/politics/article/2024/jun/08/david-cameron-victim-hoax-call-former-ukraine-president (zuletzt abgerufen am 5.11.2025).

26 So beschrieb die BaFin ein Verifikationsverfahren, in dem Kunden sich in einem Videocall mit dem Personalausweis identifizieren, Rundschreiben 3/2017 (GW) – Videoidentifizierungsverfahren, Bundesanstalt für Finanzdienstleistungsaufsicht, Ziffer A.

27 Vgl. zur Möglichkeit von Echtzeit-Deepfakes *Steinebach*, in: Pfeffer (Hrsg.), Smart Big Data Policing – Chancen, Risiken und regulative Herausforderungen, 2023, S. 29-38.

28 *Steffes/Zichler*, DuD 2024, 158.

29 *Valerius*, in: BeckOK-StGB, 66. Ed. (2025), § 33 KUG Rn. 8.1.

30 So auch *Elsner/Meinen/Rückert*, KriPoZ 2025, 269 (274); *Valerius*, CyberStR 2025, 1 (2); a.A. *Lantwin*, MMR 2019, 574 (578); *Thiel*, ZRP 2021, 202 (204); *Akay/Schiemann*, KriPoZ 2024, 76 (84); *Greif,* Strafbarkeit von bildbasierten sexualisierten Belästigungen, 2023, S. 235 ff.

31 *Kindhäuser/Hilgendorf*, in: LPK-StGB, 10. Aufl. (2024), § 185 Rn. 4.

Tathandlung kommt nicht die Erstellung, sondern lediglich die Verbreitung eines solchen Inhalts in Betracht.

Ob es sich bei der Verbreitung von Deepfakes um Tatsachenaussagen oder um Werturteile handelt, kann nicht pauschal beurteilt werden, sondern ist in hohem Maße von den individuellen Gegebenheiten des Sachverhalts abhängig.[32] Wird ein Deepfake-Porno eines internationalen Prominenten auf einer einschlägigen Website hochgeladen,[33] so kann nicht ernsthaft davon ausgegangen werden, dass der Urheber damit zum Ausdruck bringt, das dargestellte Geschehen habe sich so ereignet.[34] Umso mehr gilt das, wenn es als KI-generiert gekennzeichnet ist. Sofern ein solcher Inhalt jedoch keinen Star, sondern eine durchschnittliche Person zeigt und die Aufnahme an deren Arbeitsplatz verbreitet wird, so könnte sich durchaus der Eindruck einer Tatsachenbehauptung ergeben.

Die Äußerung müsste außerdem auch ehrrührig sein. Ehrrührig ist eine Tatsache, wenn sie nach den gesamten Umständen geeignet ist, den Betroffenen in der Meinung eines größeren Teils der Bevölkerung als verachtenswert erscheinen zu lassen.[35] Erstreckt sich der Aussagegehalt auf die bloße Vornahme sexueller Handlungen ist dies zwar unwahr; ehrrührig ist es allerdings nicht.[36] Der Aussagegehalt ist keine Basis für ein Unwerturteil der Mehrheitsgesellschaft, in der Sexualität und auch kurzfristige Beziehungen im Grundsatz akzeptiert sind. An dieser Stelle wird deutlich, dass nicht die vermittelte Aussage die Rechtsgutsverletzung verursacht, sondern die Art und Weise ihrer Übermittlung. Das Störgefühl, das diese Ausführungen möglicherweise begleitet, rührt nicht aus dem Informationsgehalt der Aussage, sondern aus deren visueller Einkleidung. Die §§ 185 ff. StGB schützen aber nicht das allgemeine Persönlichkeitsrecht und die Intimsphäre, sondern lediglich die Ehre.[37] Als Rahmenrecht genießt das allgemeine Persönlichkeitsrecht nur dort strafrechtlichen Schutz, wo der Gesetzgeber es gesondert anordnet.[38] Die Existenz besonderer Strafnormen unterstreicht, dass der Gesetzgeber nicht jegliche Verletzung als vom Beleidigungsstrafrecht umfasst ansieht. Es darf daher nicht ohne Weiteres subsidiär auf §§ 185 ff. StGB zurückgegriffen werden.[39]

Das bedeutet zwar nicht, dass die §§ 185 ff. StGB nicht auch durch die Verbreitung von Deepfakes verwirklicht werden könnten. Allerdings ergeben sich an den Stellen Schutzlücken, an denen die Rechtsgutsverletzung nicht aus dem Aussageinhalt eines Mediums herrührt, sondern aus der realistischen und realitätsnahen Darstellung eines intimen Lebensvorgangs.[40] Es handelt sich weniger um einen Angriff auf die Ehre als um eine Tat gegen die Privatsphäre. Diese wird zwar von § 33 KUG geschützt, der vorliegend auch einschlägig ist. Hier ist die Strafgewalt allerdings sehr gering. Eine Qualifikation, etwa aufgrund des Darstellungsgegenstandes, ist nicht vorgesehen.

2. Gefälschte Werbung

Wird eine Person ohne ihre Zustimmung Akteur in einer Werbung, so kommen verschiedene Straftatbestände in Frage. Dabei kann man drei unterschiedliche Perspektiven einnehmen: Die des Abgebildeten, die der Kunden und die der Mitbewerber.

Hinsichtlich des Schutzes des Abgebildeten ist zunächst auch hier § 33 KUG anzudenken. Diese Strafnorm greift, sofern ein Bildnis genutzt wird, ohne dass der Abgebildete dem zugestimmt hat oder ein Ausnahmetatbestand nach § 23 KUG vorliegt.[41] Wird hingegen lediglich die Stimme einer Person genutzt, um beispielsweise einen Slogan einzusprechen, ist dies bisher jedenfalls strafrechtlich nicht erfasst.[42] Eine dem § 33 KUG nachgebildete Norm fehlt für die Verbreitung von Stimmaufnahmen. Zwar wird zivilrechtlich diskutiert, ob eine analoge Anwendung der Regelungen geboten ist.[43] Strafrechtlich ist dies aber aufgrund des Bestimmtheitsgebots aus Art. 103 Abs. 2 GG nicht möglich. Auch § 201 StGB ist nicht anwendbar, da von dieser Norm lediglich das *von der betroffenen Person* gesprochene Wort erfasst ist. Bei Audio-Deepfakes hat die Zielperson *diese Worte* gerade nicht gesprochen.

---

32 Vgl. hierzu die Ausführungen des *AG Bamberg* in dem vielbeachteten Fall der Bildmanipulation i.Z.m. einer ehemaligen Bundesministerin, *AG Bamberg*, Urt. v. 8.4.2025 – 27 Cs 1108 Js 11315/24 (2) Rn. 6 = BeckRS 2025, 6554.

33 Dies ist mehrfach geschehen und wird regelmäßig wiederholt, vgl. *Ajder et al*., The state of deepfakes. Landscape, threats and impact, Deeptrace, 2019, S. 3.

34 Es kommt bei der Bestimmung des Aussageinhalts zwar nicht auf die Intention des Äußernden an, sondern auf die Auslegung durch einen objektiven Dritten, *BGH*, NJW 2000, 3421 (3422)*; Kargl*, in: NK-StGB, 6. Aufl. (2023), § 185 Rn. 6. Allerdings würde auch ein objektiver Dritter dies wohl nicht als Aussage über den Prominenten auffassen.

35 *BGH*, NJW 1956, 312 (312); *Gaede*, in: Matt/Renzikowski, StGB, 2. Aufl. (2020), § 186 Rn. 6; *Eisele/Schittenhelm*, in: TK-StGB, 31. Aufl. (2025), § 186 Rn. 5; *Fischer,* StGB, 72. Aufl. (2025), § 186 Rn. 4; Es ist jedoch anzumerken, dass sich hiergegen eine im Vordringen befindliche Gegenmeinung entwickelt. Diese möchte die Ehrrührigkeit anhand eines faktischen Maßstabs bestimmen, um so die tatsächlichen Umstände, denen der Betroffene aufgrund der Äußerungen ausgesetzt sein kann, angemessen zu berücksichtigen, *Hoven*, ZStW 2017, 718 (722); *Schreiber*, Strafbarkeit politischer Fake News, 2022, S. 176.

36 Das gilt jedenfalls für Inhalte, die nicht den §§ 184a ff. StGB unterfallen oder aus anderen Gründen eine Abwertung der Person bewirken.

37 *Hilgendorf*, in: LK-StGB, 13. Aufl. (2023), Vorb. § 185 Rn. 1.

38 § 201 StGB für das Recht am eigenen Wort, § 33 KUG für das Recht am eigenen Bild, usw. Zu den einzelnen Ausprägungen des APR s. *Barczak*, in: Dreier, GG, 4. Aufl. (2023), Art. 2 Abs. 1 Rn. 78 ff.

39 Dies sorgte lange Zeit für einen Streit über die Anwendbarkeit des Beleidigungsstrafrechts i.Z.m. sexuellen Übergriffen. Der *BGH* nimmt mittlerweile nur dann eine Beleidigung an, wenn über die Tatbegehung hinaus eine Abwertung des Opfers vorliegt, *BGH*, NJW 1989, 3028 (3028 f.); *BGH*, NStZ 1993, 182 (182). Dieser Rechtsgedanke ist auf den Umgang mit persönlichkeitsrechtsverletzenden Deepfakes übertragbar.

40 Auch dieses Phänomen ist nicht neu, vgl. hierzu die BVerfGE 119, 1 (34) „Esra“. Allerdings wiegt die Verletzung durch einen von der Realität nicht zu unterscheidenden Film deutlich schwerer als die schriftlichen Darstellungen in einem Roman.

41 In Ausnahmefällen kann auch bei Werbung ein Bildnis der Zeitgeschichte vorliegen, wenn sie etwa in eine satirische Darstellung eingekleidet ist, vgl. *BGH*, NJW 2007, 689.

42 Zivilrechtlich können dagegen auch bei einer KI-generierten Stimme fiktive Lizenzgebühren eingeklagt werden, s. hierzu *LG Berlin II*, *2. Zivilkammer*, Urt. v. 20.8.2025 – 2 O 202/24.

43 *Gomille*, ZUM 2025, 500 (506).

Es kommen darüber hinaus auch die Beleidigungsdelikte in Betracht. Nach § 186 Abs. 1 StGB ist es verboten, eine ehrrührige Tatsache wahrheitswidrig zu verbreiten oder zu behaupten. In der Generierung und Publikation eines Werbespots kann jedenfalls die konkludente Aussage enthalten sein, das dargestellte Geschehen habe sich in dieser Form ereignet. Die Tatsache müsste aber auch ehrrührig sein. Sie müsste also dazu geeignet sein, den Betroffenen bei einem erheblichen Teil der Bevölkerung herabzuwürdigen.[44] Möglich erscheint dies, wenn Werbung für besonders verwerfliche oder anrüchige Dinge gemacht wird. Sofern aber Ed Sheeran Werbung für einen kleinen Laden um die Ecke macht, mag das für Verwunderung sorgen. Den Sänger wertet es aber nicht ab. Ebenso wenig wird hierdurch eine Missachtung gegenüber dem Betroffenen ausgedrückt. Man wird im Gegenteil eher davon ausgehen müssen, dass der Werbetreibende den Abgebildeten für populär hält.

Nimmt man dagegen die Perspektive der Kunden ein, die sich möglicherweise aufgrund der Werbung zu einem Kauf entschieden haben, könnte man einen Betrug gem. § 263 StGB annehmen. Sofern der Werbeclip keine Hinweise auf seinen Ursprung enthält, wird man in der Mitwirkung des Prominenten eine falsche Tatsache erkennen können, die auch durch den Werbetreibenden vorgespiegelt wird. Es ist jedoch bereits fraglich, ob zwischen dieser Täuschung und einem späteren Kaufentschluss überhaupt Kausalität besteht. Diesen Beweis wird die Staatsanwaltschaft nur selten führen können. Jedenfalls liegt in Fällen, in denen für tatsächlich bestehende Unternehmen geworben wird, kein Vermögensschaden beim Kunden vor. In dem Erhalt der Ware bzw. einer Dienstleistung besteht regelmäßig ein angemessenes Äquivalent für den gezahlten Preis.[45]

Auch aus dem Blickwinkel der Mitbewerber könnte dieses Verhalten für Unmut sorgen. Es kommt ein Verstoß gegen § 16 Abs. 1 UWG in Betracht. Demnach wird bestraft, wer in der Absicht, den Anschein eines besonders günstigen Angebots hervorzurufen, in öffentlichen Bekanntmachungen oder in Mitteilungen, die für einen größeren Kreis von Personen bestimmt sind, durch unwahre Angaben irreführend wirbt. Es ist allerdings zweifelhaft, ob die Mitwirkung eines Prominenten (oder auch einer sonstigen Person) ein Angebot „besonders günstig" macht. Zwar ist hiermit nicht allein der Preis gemeint.[46] Allerdings wird nur in seltenen Konstellationen die Verknüpfung eines Produkts mit einer Person das Angebot als solches besonders attraktiv gestalten. In den meisten Fällen ist damit zu rechnen, dass der Prominente hauptsächlich zur Generierung von Aufmerksamkeit dient. Das Wettbewerbsstrafrecht ist dann nicht einschlägig.

In Fällen gefakter Werbung kommt so zumeist nur der allgemeine § 33 KUG in Frage. Weder die dargestellte Person noch die Kunden sind besonders geschützt.

3. Informationsbeschaffung

Gibt sich jemand in einem Videocall mittels Deepfake für einen anderen aus, um so an Informationen zu gelangen, ist erneut an § 33 KUG zu denken. Zur Begründung einer Strafbarkeit muss der Täter hierzu das Bildnis einer anderen Person verbreiten oder öffentlich zur Schau stellen. Wird lediglich vorübergehend das äußere Erscheinungsbild angenommen und nicht als gespeicherte Datei übersendet, so liegt mangels Verfügungsmacht des Empfängers über das Bildnis kein Verbreiten vor.[47] Sofern nur ein abgrenzbarer Personenkreis am Call teilnimmt, was in den meisten Fällen anzunehmen sein wird, ist das Bildnis auch nicht der Öffentlichkeit zur Schau gestellt.[48] Damit scheidet die Anwendung von § 33 KUG aus.

Wird ein Geheimnis- oder/und Amtsträger durch eine Täuschung dazu gebracht, vertrauliche Informationen herauszugeben, so könnten die §§ 203, 353b StGB einschlägig sein. Regelmäßig wird sich der Täter dabei für eine Person ausgeben, gegenüber der das Geheimnis offenbart werden darf (das könnte ein Mitarbeiter, Vorgesetzter oder auch der vom Geheimnis Betroffene selbst sein). Wird der Geheimnisträger auf diese Weise erfolgreich getäuscht, so liegt ein Tatbestandsirrtum nach § 16 Abs. 1 StGB vor und er macht sich durch das Offenbaren nicht strafbar. Man könnte nun andenken, dem Täuschenden das Verhalten im Rahmen einer mittelbaren Täterschaft nach § 25 Abs. 1 Var. 2 StGB zuzurechnen. Allerdings sind sowohl § 203 als auch § 353b StGB sowie § 23 Abs. 1 Nr. 3 GeschGehG echte Sonderdelikte, die nur von dem umschriebenen Personenkreis begangen werden können.[49] Eine Strafbarkeit scheidet demnach von vornherein aus. Möglich erscheint die Verwirklichung einer Straftat nur unter der Voraussetzung, dass der Täter durch die Täuschung eine inhaltlich falsche Erklärung in einer öffentlichen Urkunde durch den Getäuschten bewirkt. In diesem Fall ist § 271 StGB einschlägig.

Damit ist eine derartige Informationsbeschaffung praktisch straflos, wenn der Täter hierbei weder falsche Urkunden nutzt noch öffentliche Urkunden erstellen lässt.

4. Identitätsdiebstahl vor Gericht

Sofern eine Person einen Echtzeit-Deepfake nutzt, um anstatt eines Zeugen bei einer Videoverhandlung nach § 128a ZPO teilzunehmen, könnte eine Strafbarkeit nach § 153 StGB gegeben sein. Spätestens bei der Frage nach den Personalien gem. § 395 Abs. 2 ZPO muss der Täter

---

44 *BGH*, NJW 1956, 312 (312); *Gaede*, in: Matt/Renzikowski, StGB, § 186 Rn. 6; *Eisele/Schittenhelm*, in: TK-StGB, § 186 Rn. 5; *Fischer,* StGB, § 186 Rn. 4.

45 *Kindhäuser/Hilgendorf*, LPK-StGB, § 263 Rn. 24, 161 ff.

46 *Rengier*, in: Fezer/Büscher/Obergfell, UWG, 3. Aufl. (2016), § 16 Rn. 96; *Fritzsche/Knapp*, in: BeckOK-UWG, 29. Ed. (2025), § 16 Rn. 48.

47 *Specht-Riemenschneider*, in: Dreier/Schulze, UrhG, 8. Aufl. (2025), § 22 KUG Rn. 9; *Valerius*, in: BeckOK-StGB, § 33 KUG Rn. 11.

48 *Götting*, in: Schricker/Loewenheim, UrhR, 6. Aufl. (2020), § 22 KUG Rn. 37; *Valerius*, in: BeckOK-StGB, § 33 KUG Rn. 13.

49 *Kargl*, in: NK-StGB, § 203 Rn. 139; *Perron/Hecker*, in: TK-StGB, § 353b Rn. 23; *O. Hohmann*, in: MüKo-StGB, 4. Aufl. (2023), § 23 GeschGehG Rn. 135.

lügen, damit die Täuschung nicht auffällt. Fraglich ist, ob er hierbei auch „als Zeuge“ handelt, wie es § 153 StGB voraussetzt. Das StGB kennt keinen eigenen Zeugenbegriff, weshalb sich die Zeugeneigenschaft nach dem Prozessrecht bestimmt.[50] Die §§ 373 ff. ZPO legen fest, dass dies mittels Benennung durch eine Partei und Ladung durch das Gericht geschieht.[51] Der Täter ist aber weder benannt noch geladen. Nach dem Prozessrecht ist er demnach kein Zeuge. Man könnte jedoch erwägen, den Täter dennoch als Zeugen zu behandeln, da er sich als solcher geriert.

Dem widerspricht allerdings die Deliktsnatur der Aussagedelikte. Die §§ 153 ff. StGB sind eigenhändige Delikte.[52] Sie können nicht in mittelbarer oder Mittäterschaft begangen werden. Während man sich im Ergebnis hierüber einig ist, ist die Ursache umstritten.[53] *Müller* leitet die dogmatische Begründung aus der folgenden Prämisse ab:[54] Der Zeugenbeweis stellt eine Einheit aus Aussageinhalt und Aussageperson dar. Eine Aussage ist isoliert irrelevant. Erst dadurch, dass sie mit einer Person verbunden wird, kommt ihr Geltung zu.[55] Das zeigt sich auch daran, dass im Prozessrecht nicht die Aussage eines Zeugen, sondern der Zeuge selbst das Beweismittel darstellt.[56] Wollte man nun etwa eine Aussage in mittelbarer Täterschaft annehmen, so müsste man dem Hintermann die Tat zurechnen. Während dies für den eigentlichen Sprechakt noch möglich erscheint,[57] ist die Zurechnung der Identität des Zeugen nicht logisch denkbar. Dem Hintermann geht es nicht darum, überhaupt eine bestimmte Aussage in den Prozess einfließen zu lassen; es kommt ihm darauf an, dass auch der Anschein der Urheberschaft einer bestimmten Person entsteht.[58]

Legt man diese Maßstäbe zu Grunde, so kommt man bei der Beurteilung der obigen Fallgestaltung zu folgendem Ergebnis: Das notwendige Zusammenfallen von Aussageinhalt und Aussageperson ist auch hier nicht gegeben. Als Beweismittel geht weiterhin der ursprünglich benannte Zeuge in den Prozess ein. Der Aussageinhalt kommt allerdings vom Täter. Wollte man nun die Prozessrechtsakzessorietät an dieser Stelle durchbrechen, um den Täter dennoch als Zeugen zu werten, so müsste ihm damit auch die Identität des eigentlichen Zeugen zugerechnet werden. Dass dies aufgrund des Erfordernisses der Beweiseinheit nicht möglich ist, wurde eben dargelegt.[59] Ob der Täter den echten Zeugen als Werkzeug benutzt oder die Aussage unter dessen Erscheinung gleich selbst tätigt, kann keinen Unterschied machen.[60] Das bedeutet, dass der Täter nicht in zeugenschaftlicher Vernehmung im Sinne des § 153 StGB handelt und nach dieser Norm auch nicht bestraft werden kann. Führt man sich vor Augen, dass sich ein „echter“ Zeuge bereits dann strafbar macht, wenn er ein falsches Alter nennt, führt dies zu erheblichen Wertungswidersprüchen und zu einer offenen Flanke bei Videoverhandlungen.

V. Europarechtliche Vorgaben

Deutschland steht dabei nicht allein vor der Herausforderung, den negativen Begleiterscheinungen künstlicher Intelligenz begegnen zu müssen. Die EU ist bereits aktiv geworden und hat zwei Rechtsakte erlassen, die Deepfakes unmittelbar betreffen: Die KI-Verordnung und die Richtlinie zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt.

1. Die KI-Verordnung

Die KI-Verordnung verfolgt den Ansatz, die von Deepfakes ausgehende Gefahr durch Transparenzvorgaben zu reduzieren. Hierzu nimmt sie sowohl die Anbieter als auch die Betreiber von generativen KI-Systemen in die Pflicht. Anbieter müssen gem. Art. 50 Abs. 2 KI-VO dafür sorgen, dass die Ausgaben ihrer Systeme durch ein maschinenlesbares Format gekennzeichnet und als künstlich erzeugt oder manipuliert erkennbar sind. Dies gilt nicht nur für Deepfakes, sondern für alle synthetischen Medien.[61]

Sofern Betreiber generative KI-Systeme nutzen, um Deepfakes zu generieren, müssen diese gem. Art. 50 Abs. 4 KI-VO den künstlichen Ursprung der Inhalte offenlegen. Für sonstige synthetische Inhalte gilt das nicht.

Im Grunde sind diese Regelungen nachvollziehbar. Wenn Deepfakes als solche erkennbar sind, ist ihre Gefahr gebannt. Dies soll sowohl durch diejenigen sichergestellt werden, die die hierzu benötigte Software zur Verfügung stellen, als auch durch deren Anwender. Gefahren, die sich nicht aus dem Täuschungspotenzial, sondern aus der Visualisierung intimer Lebensvorgänge ergeben, sollen

---

50 *OLG Karlsruhe*, NStZ 1996, 282 (283); *Müller*, in: MüKo-StGB, 5. Aufl. (2025) § 153 Rn. 4; *Zöller*, in: SK-StGB, 9. Aufl. (2019), § 153 Rn. 38.

51 Auch wenn eine andere Prozessordnung anzuwenden wäre, würde sich im Ergebnis nichts ändern. In allen anderen Verfahrensordnungen wird auf die Vorgaben der ZPO verwiesen, vgl. § 98 VwGO, § 118 SGG, § 46 Abs. 2 S. 1 ArbGG. In der StPO ist derzeit keine Videoverhandlung vorgesehen.

52 Ganz h.M. *Wolters/Ruß,* in: LK-StGB, Vorb. § 153 Rn. 7; *Heger,* in: Lackner/Kühl/Heger, StGB, 31. Aufl. (2025), Vorb. § 153 Rn. 7; a.A. *Puppe,* ZStW 2008, 504 (516).

53 Zu Herleitung und Streitstand s. *Müller*, in: Hilgendorf/Kudlich/Valerius, StrafR-HdB IV, 2019, § 21 Rn. 41 ff.

54 *Müller*, Falsche Zeugenaussage und Beteiligungslehre, 2000, S. 144 ff.

55 So ist die Aussage „X war der Täter“ per se nichtssagend. Sofern man diese aber dem Y zuordnen kann, der nachweislich zur Tatzeit am Tatort war, kommt ihr ein hohes Gewicht zu.

56 *Müller*, Falsche Zeugenaussage und Beteiligungslehre, S. 147; *Fischer*, in: KK-StPO, 9. Aufl. (2023), Einl. Rn. 270 f.; *Kudlich*, in: MüKo-StPO, 2. Aufl. (2023), Einl. Rn. 417.

57 So ist bspw. die Zurechnung bei Beleidigungsdelikten grundsätzlich möglich, vgl. *Kargl*, in: NK-StGB, § 185 Rn. 56; *Fischer,* StGB, § 185 Rn. 13; *Eisele/Schittenhelm*, in: TK-StGB, § 185 Rn. 17.

58 Ansonsten könnte er sich auch selbst als Zeuge melden und eine dahingehende Aussage machen, *Müller*, Falsche Zeugenaussage und Beteiligungslehre, S. 149.

59 Dass der *BGH* § 153 StGB nicht als Sonderdelikt ansieht, widerspricht diesem Ergebnis nicht, vgl. *BGH*, NJW 2024, 2268 (2269). Das Ergebnis stützt sich nicht auf eine Sonderpflicht des Zeugen, sondern darauf, dass der Täter nicht zeugenschaftlich vernommen wird.

60 Daran kann auch ein Verweis auf die mangelnde Schutzwürdigkeit des Täters nichts ändern. Auch der mittelbare Täter einer Falschaussage ist nicht schutzwürdig, würde sich aber ohne § 160 StGB ebenfalls nicht strafbar machen.

61 Zur begrifflichen Unterscheidung s. oben.

eigens durch besondere Normen reguliert werden.[62] Bei der gesetzgeberischen Umsetzung verbleibt jedoch noch Potenzial zur Nachjustierung. Dies ergibt sich v.a. durch unklare Norminhalte.

Der Normadressat muss wissen, was der Gesetzgeber von ihm verlangt. Dies lässt Art. 50 KI-VO an einigen Stellen vermissen. So ist seit Veröffentlichung der KI-VO umstritten, wie die Kennzeichnung nach Art. 50 Abs. 2 KI-VO gestaltet sein muss. Einerseits könnte man dies so verstehen, dass Menschen die Inhalte als KI-generiert erkennen müssen.[63] Andererseits könnte man die Vorgabe auch so begreifen, dass die Kennzeichnung lediglich von einer anderen Maschine erkannt werden muss.[64] Bisher hat die EU noch keine Leitlinien zur Klärung dieser Frage veröffentlicht. Diese wären für Gerichte allerdings auch nicht bindend. Für Entwickler bedeutet diese Unklarheit auch rechtliche Unsicherheit.

Daneben ist nicht klar, wer überhaupt Betreiber einer KI-Anwendung ist. Nach Art. 3 Nr. 4 KI-VO ist Betreiber, wer ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet. Die meisten Deepfakes werden jedoch im privaten Kontext und im Zusammenhang mit Persönlichkeitsrechtsverletzung erstellt. Dass der Gesetzgeber mit Art. 50 Abs. 4 KI-VO nur eine Spartenregelung für den beruflichen Einsatz treffen wollte, darf aber bezweifelt werden. Zur Bestimmung der konkreten Reichweite der Betreiberdefinition hätte man aber Hinweise im Gesetzestext oder zumindest in den Erwägungsgründen hinterlassen können.[65]

Man kann vor diesem Hintergrund nicht annehmen, dass durch die KI-Verordnung eine ausreichende Reglementierung generativer KI erfolgt ist. Das war allerdings auch nicht die Intention der Verordnung. Der eigene Anspruch war es, das allgemeine Informationsökosystem und das ihm entgegengebrachte Vertrauen zu schützen, nicht kriminelle Handlungen mittels generativer KI zu unterbinden.[66]

2. Gewaltschutzrichtlinie

Um eine wirksame Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt zu bewerkstelligen, legt die EU-RL 2024/1385 unter anderem Mindestvorschriften für bestimmte Arten der Computerkriminalität fest. Sie verpflichtet die Mitgliedsstaaten bis zum Jahr 2027 die „*Herstellung, Manipulation oder Veränderung von Bildern, Videos oder vergleichbarem Material, die den Anschein erwecken, dass eine Person eindeutig sexuelle Handlungen vornimmt, und deren anschließende Zugänglichmachung für die Öffentlichkeit mittels IKT, ohne Einverständnis der betreffenden Person, sofern diese Handlungen wahrscheinlich dazu führen, dass der genannten Person schwerer Schaden zugefügt wird*“ zu verbieten, Art. 5 lit. b. Aus Erwägungsgrund 19 geht hervor, dass hiermit nicht nur, aber vor allem auch Deepfakes gemeint sind.

Wie bereits die KI-VO wird auch die Gewaltschutzrichtlinie von Unklarheiten über den konkreten Regelungsgegenstand begleitet. Dabei ist vor allem fraglich, was genau verboten werden muss. Man könnte den Wortlaut dahingehend interpretieren, dass bereits die Herstellung unter Strafe gestellt werden muss.[67] Dagegen könnte man den Normtext auch so verstehen, dass nur die Zugänglichmachung der auf diese Weise erzeugten Inhalte strafbar sein muss. Für letzteres sprechen sowohl die Erwägungsgründe als auch die Intention der Richtlinie als Mindestharmonisierung.[68]

VI. Zwischenergebnis

Die bisherigen Ausführungen haben gezeigt, dass die Verfügbarkeit von hochqualitativer generativer KI neue Kriminalitätsfelder erschließt und Problemstellungen aufwirft, auf die das bestehende Strafrecht keine adäquaten Antworten liefern kann. Regelmäßig ist nur § 33 KUG einschlägig, der weder in seinem Strafmaß noch nach seiner allgemeinen Konzeption dazu in der Lage ist, das verwirklichte Unrecht abzubilden. In der Praxis stellt Deepfake-Pornografie den mit Abstand größten Anwendungsbereich dar. Dies wurde von der europäischen Politik wahrgenommen und muss auch nach deutschem Recht unter Strafe gestellt werden. In der Frage, wie der Gesetzgeber diese Verpflichtung konkret ausgestaltet und ob er in diesem Zug ggf. auch weitere Verhaltensweisen pönalisiert, ist er jedoch frei. Die Notwendigkeit und Sinnigkeit einer eigenständigen Regelung wurde bereits diskutiert.[69] Dieser Beitrag soll dagegen überprüfen, ob der aktuelle Vorschlag des § 201b StGB-E die ausgemachten Lücken schließen und die europäischen Vorgaben erfüllen würde.

VII. Lösung: § 201b StGB-E?

Der Bundesrat hat eine Initiative zur Schaffung einer Strafnorm in den Bundestag eingebracht.[70] Der § 201b Abs. 1 StGB-E soll es unter Strafe stellen, mit computertechnischen Mitteln hergestellte oder veränderte Medieninhalte, die den Anschein einer wirklichkeitsgetreuen Bild- oder Tonaufnahme einer Person erwecken, anderen zugänglich zu machen. § 201b Abs. 2 StGB-E enthält eine Qualifikation für den Fall, dass es sich um Darstellungen des höchstpersönlichen Lebensbereichs handelt oder die Inhalte öffentlich zugänglich gemacht werden. Bei § 201b

---

62 S. hierzu sogleich die Ausführungen im Rahmen der Gewaltschutz-RL.

63 *Hilgendorf/Härtlein*, HK-KI-VO, Art. 50 Rn. 10; *Merkle*, in: Bomhard/Pieper/Wende, KI-VO, 2025, Art. 50 Rn. 71 ff.

64 *Lauber-Rönsberg*, in: BeckOK-KI-Recht, 3. Ed. (2025), Art. 50 Rn. 34.

65 Näher zum Begriff des Betreibers *Hilgendorf/Härtlein*, HK-KI-VO, Art. 2 Rn. 4.

66 Vgl. Erwgr. 133 KI-VO.

67 So wohl der Ausschuss für Frauen und Jugend, BR-Drs. 222/1/24, S. 4.

68 *Elsner/Meinen/Rückert*, KriPoZ 2025, 269 (275); Erwgr. 19 Richtlinie (EU) 2024/1385.

69 Zum Streitstand und den verschiedenen Ansätzen s. *Teichmann*, KriPoZ 2025, 382 ff.

70 Zum bisherigen Gesetzgebungsprozess s. *Teichmann*, KriPoZ 2025, 380 ff.; *Elsner/Meinen/Rückert*, KriPoZ 2025, 269 (274 f.).

Abs. 3 StGB-E handelt es sich um eine dem § 201a Abs. 4 StGB nachgebildete Ausnahme für sozialadäquates Verhalten.

1. Erfüllung europäischer Vorgaben

Der § 201b StGB-E erfüllt die Vorgaben der Gewaltschutzrichtlinie. Wenn man überzeugenderweise davon ausgeht, dass nicht bereits das Herstellen, sondern erst das Zugänglichmachen besagter Inhalte bestraft werden muss, wird dies mit § 201b StGB-E auch ohne die Verwendung von IKT[71] erfüllt. Sofern vorgebracht wird, durch das Erfordernis der Wahrscheinlichkeit eines Schadenseintritts sei die Ausgestaltung als Gefährdungsdelikt gefordert, so ist dem zu widersprechen.[72] Mit diesem Passus wird den Mitgliedsstaaten lediglich der Spielraum eingeräumt, ein zusätzliches Kriterium verlangen zu *können*.[73] Eine Persönlichkeitsrechtsverletzung ist damit nicht mit dem Eintritt eines Schadens gleichzusetzen, da das Erfordernis ansonsten keine eigenständige Bedeutung aufweisen würde.

2. Individuelle Bestimmung des Tatgegenstandes

Allgemein kann man die Gefahren, die von Deepfakes ausgehen, in Gefahren aufgrund des Täuschungspotenzials und Gefahren aufgrund der Möglichkeit zur Visualisierung bestimmter Lebensvorgänge unterteilen, wobei erstere den praktischen Großteil ausmachen. Der § 201b StGB-E begegnet allerdings ausschließlich dem Täuschungspotenzial, indem er zur Tatbestandsmäßigkeit den Anschein einer wirklichkeitsgetreuen Bild- oder Tonaufnahme einer Person voraussetzt. Sofern Inhalte gekennzeichnet sind oder sich aus den Umständen der Darbietung ergibt, dass nicht die Wirklichkeit wiedergegeben wird, liegt kein taugliches Tatobjekt vor und § 201b StGB-E ist nicht anwendbar.[74] Für die Betroffenen ist es aber nur ein schwacher Trost, wenn pornografische Inhalte als KI-generiert gekennzeichnet werden, in denen sie die Hauptrolle spielen. An dieser Stelle sollte eine Orientierung an der französischen Gesetzgebung erfolgen:

Frankreich hat bereits 2024 seine Strafgesetze angepasst und die Verbreitung von Deepfakes unter Strafe gestellt.[75] Hierbei ist interessant, dass der Tatgegenstand je nach dargestelltem Geschehen variiert. Sofern der Inhalt allgemeine Darstellungen zeigt, führt eine Kennzeichnung als KI-Produkt zur Straflosigkeit. Dies entspricht auch dem deutschen Entwurf. Werden dagegen Inhalte „*sexueller Natur*“[76] zugänglich gemacht, spielt eine mögliche Kennzeichnung keine Rolle. Frankreich legt seiner Regelung damit zutreffend die erwähnte Zweiteilung der bestehenden Gefahren zu Grunde. Auch der deutsche Gesetzgeber sollte das Erfordernis einer Täuschungsgefahr in § 201b Abs. 2 Alt. 2 StGB-E streichen.

3. Ergänzung einer besonderen Irrtumsregel

An anderer Stelle berücksichtigt der Entwurf das Täuschungspotenzial noch nicht ausreichend. Treffend geht er zwar davon aus, dass Rezipienten die generierten Inhalte für echt halten könnten. Dass sich jedoch auch Täter über die Inhalte irren könnten, wird in dem Entwurf nicht aufgegriffen. Teilt beispielsweise eine Person einen Deepfake, in dem Glauben, es handle sich um ein echtes Foto, so liegt gem. § 16 Abs. 1 StGB ein Tatbestandsirrtum vor. Dies führt grundsätzlich auch zu billigen Ergebnissen. Handelt es sich jedoch um einen Inhalt, der als Bildaufnahme den § 201a Abs. 2 StGB verwirklichen würde, so führt dies zu einem Widerspruch. Eine Strafbarkeit aufgrund eines Versuchs scheidet aus, da der Versuch des § 201a StGB nicht strafbar ist. Dem Täter kommt so zugute, dass er sich über das Tatobjekt irrt, obwohl der Gesetzgeber das Zugänglichmachen beider Tatobjekte unter Strafe stellt. Als Schutzbehauptung wäre dies auch nicht ohne Weiteres von der Hand zu weisen, da eine Täuschung durchaus plausibel ist. Dies könnte durch die Einfügung des folgenden Absatzes vermieden werden: „*Nimmt der Täter bei Begehung der Tat an, der Medieninhalt bilde ein reales Geschehen ab, so bestimmt sich seine Verantwortung nach den hierfür geltenden Vorschriften. Die Strafe darf nicht schwerer sein als die, die in diesem Paragrafen vorgesehen ist.*“

4. Verschiedene Tatbestände für verschiedene Rechtsgüter

Zuletzt unternimmt der Entwurf den Versuch, ganz unterschiedliche Belange in einer einzigen Norm zu regeln. Namentlich sollen Desinformation, die Manipulation des demokratischen Willensbildungsprozesses, die Verfolgung eigennütziger Vermögensinteressen und Persönlichkeitsrechtsverletzungen durch die Norm unterbunden werden.[77] Als kleinsten gemeinsamen Nenner all dieser Anwendungsfelder erkennt die Initiative die Verletzung des Persönlichkeitsrechts des Dargestellten und möchte implizit die anderen Felder miterfassen. Auf diese Weise werden jedoch Interessen miteinander verbunden, die nicht zwangsläufig zusammenhängen. So entfällt die Strafbarkeit, sofern der Abgebildete der Zugänglichmachung zustimmt.[78] Im o.g. Fall, in dem eine Person die Identität eines Zeugen vor Gericht übernimmt, sollte aber die Zustimmung des benannten Zeugen keine Auswirkungen auf die Strafbarkeit des Verhaltens haben. Dasselbe gilt, wenn es um die Manipulation demokratischer Prozesse geht. Umgekehrt wäre im Zusammenhang mit dem Schutz von Wahlen auch eine temporäre Begrenzung der Strafbarkeit

71 Informations- und Kommunikationstechnologien.
72 a.A. *Elsner/Meinen/Rückert*, KriPoZ 2025, 269 (276).
73 Vgl. hierzu den Wortlaut von Erwgr. 18: „Um nicht mehr als Mindestvorschriften für die schwersten Formen von Cybergewalt festzulegen, sind die in dieser Richtlinie definierten Straftaten auf Handlungen beschränkt, die dem Opfer wahrscheinlich schweren Schaden oder schweren psychischen Schaden zufügen (…).“.
74 BT-Drs. 20/12605, S. 16.
75 Art. 226-8 f. Code pénal.
76 Im Original: „caractère sexuel“.
77 BT-Drs. 20/12605, S. 9 f.
78 BT-Drs. 20/12605, S. 13, 17.

sowie erhöhte Anforderung an den Tatgegenstand angebracht.[79] Präziser wäre es deshalb, diese Belange nicht gemeinsam über § 201b StGB-E zu regeln, sondern stattdessen passgenau eine Erweiterung in § 108a und § 153 StGB einzufügen.

VIII. Fazit

Die Verfügbarkeit generativer KI revolutioniert neben vielen Lebensbereichen auch die Kriminalität. Bekannte Deliktsformen werden adaptiert, neue Kriminalitätsfelder entstehen. Zugleich eröffnet KI erhebliche Chancen für Bildung, Kultur und Strafverfolgung. Der Gesetzgeber steht damit vor einem Zwiespalt: Einerseits soll das Potenzial künstlicher Intelligenz umfassend genutzt werden, andererseits muss der Staat seiner Schutzpflicht gegenüber neuen Bedrohungen gerecht werden. Bei der Schaffung einer Strafnorm im Zusammenhang mit generativer KI ist daher ein angemessener Ausgleich zwischen Innovationsförderung und dem Schutz verschiedener Rechtsgüter zu finden. Die aktuelle Initiative zur Einführung des § 201b StGB-E weist dabei in die richtige Richtung, schließt einige Straflücken und erfüllt die europarechtlichen Vorgaben. Es verbleibt aber noch Raum zu weiteren Präzisierungen, um diesen Ausgleich zu gewährleisten.

[79] Dies entspricht dem Vorbild der meisten US-Bundesstaaten, vgl. Minnesota House Bill 1370, Sec. 2, Subdivision 2, 5.13. Meist gilt ein Zeitraum von 60-90 Tagen. Die erhöhten Anforderungen an den Tatbestand sollen dagegen den Eintritt eines sog. chilling effects vermeiden, bei dem sich Personen aus Angst aus dem öffentlichen Diskurs heraushalten, vgl. *Gärditz,* in: Stern/Sodan/Möstl, StaatsR, 2. Aufl. (2022), § 22 Rn. 67.