

„Junges Publizieren“

Seminararbeit von

Lisa-Marie Möller

**Wie kann das Strafrecht Persönlichkeitsrechte vor Deepfakes schützen –
braucht es spezifische Normen gegen digitale Bildmanipulation im Netz?**

Universität zu Köln

Fachbereich: Rechtswissenschaft

Gutachter: Frau Prof. Dr. Anja Schiemann

Abgabedatum: 6.10.2025

Inhaltsverzeichnis

I. Einleitung.....	3
II. Der Begriff „Deepfake“ und sein Verhältnis zum Persönlichkeitsrecht.....	4
1. Technische Einordnung von Deepfakes.....	4
a) Funktionsweise von Deepfakes.....	4
b) Typische Erscheinungsformen von Deepfakes	4
2. Verletzung des Persönlichkeitsrechts durch Deepfakes	5
III. Bestehende strafrechtliche Schutzmöglichkeiten	6
1. Kernstrafrecht.....	6
a) §§ 185 ff. StGB	6
aa) § 185 StGB.....	6
bb) §§ 186, 187 StGB.....	6
cc) § 188 StGB	7
b) § 201a StGB.....	7
c) §§ 184 b, 184 c StGB	8
2. Nebenstrafrecht	8
a) § 33 KunstUrhG	9
b) §§ 106, 108 UrhG.....	9
c) § 42 Abs. 2 Nr. 1 BDSG.....	10
3. Schutzlücken und Reichweite.....	11
IV. Strafrechtliche Bewertung und Herausforderungen.....	12
1. Herausforderungen.....	12
a) Ungleichmäßigkeiten der strafrechtlichen Bewertung.....	12
b) Spannungsfeld zwischen Meinungs- und Kunstfreiheit (Art. 5 GG) und Persönlichkeitsrechtsschutz	12
c) Unzureichende Erfassung des Unrechtskerns	12
d) Schwierigkeiten bei der Strafverfolgung	13
2. Handlungsbedarf – neue Strafnorm erforderlich?	14
a) Argumente gegen eine Reform	14
b) Argumente für eine Reform	14
c) Zwischenergebnis Reformbedarf.....	15
V. Reform.....	15
1. Überblick über die aktuelle Reformdiskussion.....	15
2. Mögliche Reformmodelle.....	16
a) Grundsätzliches Verbot von Deepfakes.....	16
b) Strafbarkeit der „nichteinvernehmlichen, glaubwürdigen Nachahmung einer Person“	16
aa) Darstellung.....	16
bb) Kritik.....	16
c) Orientierung an Urkundendelikten, §§ 267 ff. StGB	17
d) § 201 b StGB-E.....	18
aa) Zielsetzung.....	18
bb) Tatbestand	18

cc) Kritik	19
e) Erweiterung des § 201a StGB	20
3. Beurteilung und eigener Reformvorschlag.....	21
VI. Fazit.....	22

I. Einleitung

Die rasanten Entwicklungen im Bereich der Künstlichen Intelligenz (KI) prägen zunehmend unseren Alltag und werfen zugleich neue rechtliche Fragen auf. Besonders eindrücklich zeigt sich dies im Phänomen der sogenannten *Deepfakes* – täuschend echt wirkender Bild-, Video oder Tonaufnahmen, die mit Hilfe von KI-Technologien erstellt oder modifiziert werden können.¹ Was einst harmlos begann, hat sich längst zu einer gesellschaftlichen Herausforderung entwickelt: Von politischer Desinformation bis hin zu pornografischen Fälschungen reichen die Einsatzmöglichkeiten, die das Vertrauen in die Echtheit digitaler Inhalte erschüttern und eine Gefahr für die Persönlichkeitsrechte darstellen.²

Für das deutsche Recht stellt sich damit eine drängende Frage: Wie können die Persönlichkeitsrechte Betroffener effektiv vor Eingriffen geschützt werden? Zwar bietet das geltende Strafrecht bereits verschiedene Anknüpfungspunkte – etwa über Normen zum Schutz der Ehre oder des Rechts am eigenen Bild.³ Doch durch die spezifischen Dynamiken digitaler Bildmanipulation – unter anderem die schnelle Verbreitung in sozialen Netzwerken, die Anonymität⁴ der Täter⁵ im Netz und dem besonderen Schadenspotenzial – wird das Strafrecht vor neue Herausforderungen gestellt.⁶ Ein Beispiel hierfür ist der Fall der italienischen Premierministerin Giorgia Meloni: Ihr Gesicht wurde in Deepfake-Pornografie verwendet, die online veröffentlicht worden ist. Meloni klagt gegen die Ersteller und Verbreiter dieser Inhalte und fordert Schadensersatz in Höhe von 100.000 Euro – ein Fall, der verdeutlicht, wie Persönlichkeitsrechte durch Deepfakes verletzt werden können, lange bevor eine wirksame rechtliche Intervention erfolgt.⁷

Vor diesem Hintergrund untersucht diese Arbeit die Möglichkeiten und Grenzen des strafrechtlichen Schutzes von Persönlichkeitsrechten im Umgang mit Deepfakes. Im Fokus steht dabei die Frage, ob die bestehenden Vorschriften genügen oder spezifische Normen gegen digitale Bildmanipulation erforderlich sind und, wenn ja, welcher Reformvorschlag am besten geeignet ist, um einen effektiven Persönlichkeitsrechtsschutz zu gewährleisten. Damit soll ein Beitrag zu der grundlegenden Diskussion geleistet werden, wie das Strafrecht in Zeiten technischer Umbrüche seine Schutzfunktion für das Persönlichkeitsrecht bewahren und weiterentwickeln kann.

¹ Stosz, Policy Options for Fighting Deepfakes, Georgetown Security Studies Review, 3.02.2019; online abrufbar unter: <https://georgetown-securitystudiesreview.org/2019/02/03/policy-options-for-fighting-deepfakes/> (6.10.2025).

² Lantwin, MMR 2020, 78 (78 f.).

³ Lantwin, MMR 2020, 78 (79 ff.).

⁴ Kumkar/Rapp, ZfDR 2022, 199 (212).

⁵ Im Interesse einer besseren Lesbarkeit wird in dieser Arbeit auf eine geschlechterdifferenzierte Sprachform verzichtet. Die im Folgenden willkürlich gewählte weibliche oder männliche Form schließt alle Geschlechter gleichberechtigt ein.

⁶ Lantwin, MMR 2019, 574.

⁷ ka, Deepfake: Gefälschte Pornovideos mit Melonis Gesicht online gestellt, Südtirol News, 26.10.2023; online abrufbar unter: <https://www.suedtirolnews.it/italien/deepfake-gefaelschte-pornovideos-mit-melonis-gesicht-online-gestellt> (zuletzt abgerufen am 6.10.2025).

II. Der Begriff „Deepfake“ und sein Verhältnis zum Persönlichkeitsrecht

1. Technische Einordnung von Deepfakes

a) Funktionsweise von Deepfakes

Das *Deepfake* wird in Art. 3 Nr. 60 der EU-Verordnung zur Künstlichen Intelligenz legal definiert.⁸ Demnach handelt es sich bei einem Deepfake um „einen durch KI erzeugten oder manipulierten Bild- Ton- oder Videoinhalt, der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde“⁹. Nicht erfasst sind also Inhalte, die erkennbar nicht real sind.¹⁰

Die Erstellung von Deepfakes basiert auf dem sogenannten *Deep Learning*.¹¹ Hierbei handelt es sich um maschinelles Lernen durch ein mehrschichtiges Lernen.¹² Dabei wird eine Künstliche Intelligenz anhand von einer sehr großen Anzahl an Datensätzen „trainiert“, menschliche Gesichtszüge und Bewegungen, Mimik und Gestik, sowie Stimmen erfassen und reproduzieren zu können.¹³ Dies ermöglicht unter anderem, die in einer Aufnahme erkennbaren Gesichter von Personen in täuschend echter Weise durch die Gesichter anderer Personen auszutauschen (sog. *Face Swap*). Außerdem können durch die KI gesprochene Worte in einer Videoaufnahme durch völlig neue Worte ersetzt werden, wobei die Stimme, Lippenbewegung und Mimik der Person angeglichen werden (sog. *Lip Sync*). Darüber hinaus kann mit Hilfe der KI das Erscheinungsbild einer Person durch einen Darsteller vor der Kamera bewegt werden (sog. *Puppet Master*).¹⁴

Aufgrund des rasanten technischen Fortschritts ist es der KI heutzutage möglich, komplexe Zusammenhänge von Mimik und Gestik, sei es ein Augenblinzeln oder ein Schattenwurf, zu erfassen und detailgetreu zu übertragen.¹⁵ Deepfakes verfügen daher bereits über ein so hohes Niveau an Authentizität, dass die Täuschung in den meisten Fällen mit dem bloßen Auge nicht mehr erkennbar ist, insbesondere bei schnellen Wahrnehmungsprozessen, wie über Social Media auf dem Handybildschirm.¹⁶

b) Typische Erscheinungsformen von Deepfakes

Heutzutage gibt es eine Vielzahl öffentlich zugänglicher Apps und Websites, mithilfe derer Deepfakes erstellt werden können, weshalb das Phänomen im Internet mittlerweile weit verbreitet ist.¹⁷ Laut einer Studie aus dem Jahr 2023 ist die Anzahl von Deepfakes im Internet im Zeitraum von 2019-2023 um 550% gestiegen.¹⁸ Teilweise handelt es sich um harmlose und sogar sinnvolle Erscheinungsformen, zum Beispiel in der Medizin oder in Kunst

⁸ Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz, ABl. L v. 12.7.2024.

⁹ VO (EU) 2024/1689.

¹⁰ Lauber-Rönsberg, in: BeckOK KI-Recht, 3. Ed. (2025), KI-VO, Art. 50 Rn. 62.

¹¹ Söbbing, MMR 2021, 111 (112).

¹² Söbbing, MMR 2021, 111 (112).

¹³ Thiel, ZRP 2021, 202 (203).

¹⁴ Farid/Schindler, Deepfakes. Eine Bedrohung für Demokratie und Gesellschaft, 2020, S. 16.

¹⁵ Meinicke, DSRITB 2020, 981 (982).

¹⁶ Meinicke, DSRITB 2020, 981 (982).

¹⁷ Paris/Donovan, Deepfakes and Cheap Fakes, 2019, S. 15.

¹⁸ Home Security Heroes, 2023 State of Deepfakes, 2023; online abrufbar unter: <https://www.securityhero.io/state-of-deepfakes/> (zuletzt abgerufen am 6.10.2025).

und Kultur.¹⁹

Darüber hinaus verfügen Deepfakes jedoch über ein enormes Missbrauchspotential.²⁰ Laut einer im September 2019 veröffentlichten Studie zum Thema Deepfakes verfolgen nicht alle, aber die meisten Deepfakes missbräuchliche Zwecke.²¹ Im Jahr 2023 handelte es sich bei 98% aller Deepfakes um sog. Deepfake-Pornographie.²² Hierbei werden künstliche Nacktbilder und Sexvideos, welche täuschend echt aussehen, durch KI erstellt.²³

Ein weiterer relevanter Anwendungsbereich von Deepfakes sind sog. politische Deepfakes. Hierbei wird die Wahrnehmung von Politikern sowie anderen Entscheidungsträgern manipuliert.²⁴ Oft werden einer im politischen Leben stehenden Person politische Äußerungen „in den Mund gelegt“. ²⁵ Durch den Einsatz politischer Deepfakes besteht neben Persönlichkeitsrechtsverletzungen auch die Gefahr der Manipulation demokratischer Prozesse.²⁶ Darüber hinaus kommen Deepfakes auch in Gestalt von Stimmimitationen im Rahmen von KI-gestützten Cyber-Betrugsfällen zur Anwendung.²⁷

2. Verletzung des Persönlichkeitsrechts durch Deepfakes

Das allgemeine Persönlichkeitsrecht ist in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verankert.²⁸ Davon erfasst ist zum einen der Schutz der Privatsphäre.²⁹ Außerdem werden die Selbstdarstellung des Einzelnen in der Öffentlichkeit, sowie das Recht auf informationelle³⁰ sowie sexuelle³¹ Selbstbestimmung geschützt. Darüber hinaus wird das Recht auf die Vertraulichkeit und Integrität informationstechnischer Systeme erfasst.³² Das allgemeine Persönlichkeitsrecht schützt den Betroffenen auch vor der Verbreitung eines täuschend echt wirkenden künstlich hergestellten oder manipulierten Medieninhalts.³³

Die missbräuchliche Verwendung personenbezogener Deepfakes führt zu immensen Persönlichkeitsrechtsverletzungen.³⁴ Besonders einschneidend sind die Verletzungen durch Deepfake-Pornographie, aber auch andere Manipulationen, die geeignet sind, dem sozialen oder beruflichen Ansehen einer Person zu schaden, sind relevant.³⁵ So stellen Deepfakes auch eine Gefahr für den Ehrschutz der betroffenen Personen dar.³⁶

¹⁹ Lantwin, MMR 2019, 574 (574 f.).

²⁰ Lantwin, MMR 2019, 574 (575).

²¹ Aider/Patrini/Cavalli/Cullen, The State of Deepfakes: Landscape, Threats, And Impact, 2019, S. 1.

²² Home Security Heroes, 2023 State of Deepfakes, 2023; online abrufbar unter: <https://www.securityhero.io/state-of-deepfakes/> (zuletzt abgerufen am 6.10.2025).

²³ Völzmann, ZUM 2025, 493.

²⁴ Lantwin, MMR 2020, 78 (79).

²⁵ Meinicke, DSRITB 2020, 981 (990).

²⁶ Lantwin, MMR 2019, 574 (575).

²⁷ ZD-Aktuell 2019, 06776.

²⁸ BVerfG, Ur. v. 15.12.1999 – 1 BvR 653/96.

²⁹ Eichberger, in: Huber/Voßkuhle, GG, 8. Aufl. (2024), Art. 2 Rn. 152.

³⁰ Eichberger, in: Huber/Voßkuhle, GG, Art. 2 Rn. 152.

³¹ BVerfG, Ur. v. 3.3.2004 – 1 BvR 2378/98, 1 BvR 1084/99; Völzmann, ZUM 2025, 493 (493 f.).

³² Eichberger, in: Huber/Voßkuhle, GG, Art. 2 Rn. 152.

³³ BVerfG, Ur. v. 14.2.2005 – 1 BvR 240/04.

³⁴ Blocher, KIR 2025, 225 (226).

³⁵ Lantwin, MMR 2019, 574 (575).

³⁶ Meinicke, DSRITB 2020, 981 (990).

III. Bestehende strafrechtliche Schutzmöglichkeiten

Im deutschen Strafrecht existieren bereits einige Normen, die geeignet sein könnten, die Persönlichkeitsrechte einer Person vor digitaler Bildmanipulation im Netz zu schützen.

1. Kernstrafrecht

a) §§ 185 ff. StGB

Im Rahmen des strafrechtlichen Schutzes von Persönlichkeitsrechten vor Deepfakes kommen zunächst die in den §§ 185 ff. StGB normierten Ehrdelikte in Betracht.³⁷ Das geschützte Rechtsgut der §§ 185 ff. StGB ist die Ehre der betroffenen Person.³⁸ Von der „Verbreitung“ im Sinne der §§ 185 ff. StGB ist auch das Teilen von Medieninhalten im Netz erfasst. Dies ergibt sich aus §§ 185 ff. i.V.m. § 11 Abs. 3 StGB.³⁹ § 11 Abs. 3 StGB nennt explizit auch solche Inhalte, die „unabhängig von einer Speicherung mittels Informations- oder Kommunikationstechnik übertragen werden“.

aa) § 185 StGB

Von § 185 StGB (Beleidigung) werden Äußerungen von Tatsachen und Werturteilen gegenüber dem Betroffenen sowie Äußerungen von Werturteilen gegenüber Dritten erfasst.⁴⁰

bb) §§ 186, 187 StGB

Die §§ 186, 187 StGB sanktionieren jeweils ehrverletzende Tatsachenäußerungen über den Betroffenen gegenüber Dritten.⁴¹ Bei Deepfakes handelt es sich in den meisten Fällen um Tatsachenäußerungen gegenüber Dritten, weshalb diese Straftatbestände häufiger einschlägig sind.⁴² Wenn der Täter in Bezug auf die Falschheit der Tatsachenäußerung vorsätzlich handelt, kommt eine Strafbarkeit wegen Verleumdung im Sinne des § 187 StGB in Betracht (vgl. den Wortlaut: „wider besseres Wissen“), während bei fehlendem Vorsatz hinsichtlich der Falschheit § 186 StGB (Üble Nachrede) einschlägig sein kann.⁴³

Die Tatsache muss dafür jedoch geeignet sein, den Betroffenen „verächtlich zu machen oder [ihn] in der öffentlichen Meinung herabzuwürdigen“ (vgl. den Wortlaut von § 186 und § 187 StGB). Wann ein (politisches) Deepfake ehrverletzend ist, ist teilweise schwierig zu beurteilen.⁴⁴ Grundsätzlich lässt sich sagen, dass eine Ehrverletzung auf jeden Fall dann zu bejahen ist, wenn durch das Deepfake fälschlicherweise behauptet wird, die betroffene Person habe eine Straftat begangen.⁴⁵ Auf der anderen Seite ist eine Ehrverletzung abzulehnen, wenn es sich offensichtlich um Behauptungen handelt, die den Wertungen der Verfassung beziehungsweise des geltenden Rechts

³⁷ Haag, in: Hoeren/Sieber/Holznagel, MMR-HdB, 62. EL (Juni 2024), Teil 29 Rn. 28.

³⁸ Regge/Pegel, in: MüKo-StGB, 5. Aufl. (2025), § 185 Rn. 1.

³⁹ Valerius, in: BeckOK-StGB, 66. Ed. (2025), § 11 Rn. 70 f.

⁴⁰ Regge/Pegel, in: MüKo-StGB, § 185 Rn. 3.

⁴¹ Regge/Pegel, in: MüKo-StGB, § 185 Rn. 3.

⁴² Meinicke, DSRITB 2020, 981 (990).

⁴³ Meinicke, DSRITB 2020, 981 (990).

⁴⁴ Meinicke, DSRITB 2020, 981 (990).

⁴⁵ Hoven/Krause, JuS 2017, 1167 (1168).

entsprechen.⁴⁶

Um eine Strafbarkeit gem. § 186 oder § 187 StGB bejahen zu können, muss zudem ein Drittbezug vorliegen.⁴⁷ Dieser liegt bei (politischen) Deepfakes immer vor, da die Verbreitung des Deepfakes (beispielsweise über die sozialen Medien) gegenüber anderen Personen als dem Betroffenen erfolgt.⁴⁸

Eine weitere Tatbestandsvoraussetzung von § 186 StGB ist, dass die behauptete oder verbreitete Tatsache nicht erweislich wahr ist und der Täter hinsichtlich der Unwahrheit wenigsten sorgfaltswidrig handelt.⁴⁹ Im Zusammenhang damit kann es allerdings zu Schwierigkeiten hinsichtlich der Nachweisbarkeit kommen, wenn der Täter geltend macht, er habe das Deepfake für wahr gehalten.⁵⁰

cc) § 188 StGB

Darüber hinaus gewährt § 188 StGB „im politischen Leben des Volkes stehenden“ Personen Schutz, wenn die Tat aus Beweggründen erfolgt, „die mit der Stellung des Beleidigten im öffentlichen Leben zusammenhängen“ und die Tat geeignet ist, „sein öffentliches Wirken erheblich zu erschweren“.

b) § 201a StGB

§ 201a StGB dient dem Schutz des höchstpersönlichen Lebensbereichs einer Person. Erfasst ist der Kerngehalt des allgemeinen Persönlichkeitsrechts, namentlich die Intimsphäre, Sexualsphäre sowie die Bereiche Krankheit und Tod.⁵¹

Gem. § 201a Abs. 2 StGB wird die Zugänglichmachung einer Bildaufnahme von einer Person bestraft, die geeignet ist, dem Ansehen dieser abgebildeten Person erheblich zu schaden. Die Veränderung einer bereits existierenden Bildaufnahme ist hiervon erfasst.⁵²

Ob allerdings auch vollständig neue, künstlich generierte Bilder vom Anwendungsbereich des § 201a Abs. 2 StGB erfasst sind, ist umstritten.⁵³ Es ist nicht klar, ob der Gesetzgeber durch § 201a Abs. 2 StGB auch digitale Bildmanipulationen oder nur reale Bildaufnahmen pönalisieren wollte.⁵⁴ Unter Berücksichtigung des in der Verfassung verankerten Bestimmtheitsgebots gem. Art. 103 Abs. 2 GG könnte man zu dem Schluss kommen, dass digitale Bildmanipulationen nicht unter § 201a Abs. 2 StGB subsumiert werden können.⁵⁵ Dafür spricht zudem, dass auch Computeranimationen nicht von § 201a Abs. 1 StGB erfasst werden.⁵⁶

Eine andere, von dem Großteil der Lehre vertretene Ansicht bejaht die Subsumtion von Deepfakes unter § 201a

⁴⁶ Hoven/Krause, JuS 2017, 1167 (1168).

⁴⁷ Regge/Pegel, in: MüKo-StGB, § 186 Rn. 20.

⁴⁸ Meinicke, DSRITB 2020, 981 (991).

⁴⁹ Regge/Pegel, in: MüKo-StGB, § 186 Rn. 24; AG Göttingen, Urt. v. 27.9.2022 – 63 Cs 300 Js 41237/21 (119/22).

⁵⁰ Meinicke, DSRITB 2020, 981 (991).

⁵¹ Heuchemer, in: MüKo-StGB, 5. Aufl. (2025), § 201a Rn. 1.

⁵² Kumkar/Rapp, ZfDR 2022, 199 (209).

⁵³ Kumkar/Rapp, ZfDR 2022, 199 (209).

⁵⁴ Kumkar/Rapp, ZfDR 2022, 199 (209).

⁵⁵ Kumkar/Rapp, ZfDR 2022, 199 (209).

⁵⁶ Graf, in: MüKo-StGB, 5. Aufl. (2025), § 201a Rn. 26.

StGB.⁵⁷ Grund dafür ist, dass der BGH schon die Identifizierbarkeit einer Person auf dem Bildnis ausreichen lässt, um den Tatbestand des § 201a StGB zu eröffnen.⁵⁸

Wenn man die Anwendbarkeit von § 201a StGB bejaht, muss die Bildaufnahme gem. § 201a Abs. 2 StGB geeignet sein, dem Ansehen der abgebildeten Person erheblich zu schaden. Bei pornografischen Deepfakes, die nicht konsensual erstellt worden sind, sowie anderen in hohem Maße persönlichkeitsrechtsverletzenden Deepfakes liegt dies in der Regel zweifelslos vor.⁵⁹ Allgemein kann man sagen, dass „je minderwertiger, peinlicher, ekliger oder abstoßender“⁶⁰ die jeweilige Bildaufnahme erscheint, desto eher der § 201a Abs. 2 StGB zu bejahen ist.

Im Gegensatz zu § 201a Abs. 1 StGB, sanktioniert der Abs. 2 allerdings nur die Verbreitung, aber nicht schon die Herstellung einer solchen Bildaufnahme.⁶¹ Die Herstellung eines Deepfakes lässt sich nicht unter § 201a Abs. 1 StGB subsumieren, da nachträgliche Bearbeitungen einer Aufnahme nicht von dem Herstellungsbegriff des § 201a StGB umfasst sind.⁶² In den meisten Fällen nutzen Täter allerdings ohnehin keine eigens erstellten, sondern öffentlich zugängliche Bildaufnahmen.⁶³

§ 201a StGB sanktioniert also durchaus die Verbreitung von (pornografischen oder anderen massiv persönlichkeitsrechtsverletzenden) Deepfakes, aber nicht deren Herstellung.⁶⁴

c) §§ 184b, 184 c StGB

Im Fall von kinder- und jugendpornographischen Deepfakes können zusätzlich die §§ 184b und 184c StGB einschlägig sein.⁶⁵ Gem. § 184b Abs. 1 S. 1 Nr. 2 und § 184c Abs. 1 S. 1 Nr. 2 StGB ist die Zugänglichmachung oder Besitzverschaffung eines kinder- bzw. jugendpornographischen Inhalts, der ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergibt, zu bestrafen. Deepfakes, die ein solches Geschehen authentisch vortäuschen, sind als „wirklichkeitsnahes Geschehen“ hiervon erfasst.⁶⁶ Dies ist nur dann abzulehnen, wenn ein durchschnittlicher Beobachter äußerlich erkennen kann, dass es sich um eine Fiktion handelt.⁶⁷ Gem. § 184b Abs. 3 StGB ist zudem der Abruf und Besitz kinderpornografischer Inhalte, die ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergeben, also unter anderem auch kinderpornografische Deepfakes, strafbar. Im Gegensatz dazu wird der Besitz und Abruf jugendpornografischer Deepfakes nicht sanktioniert, da § 184c Abs. 3 StGB nur von „tatsächlichen Geschehen“ spricht.⁶⁸

2. Nebenstrafrecht

Auch im Nebenstrafrecht finden sich Vorschriften, durch die Persönlichkeitsrechte vor digitaler Bildmanipulation

⁵⁷ Kumkar/Rapp, ZfDR 2022, 199 (209).

⁵⁸ BGH, Beschl. v. 26.2.2015 – 4 StR 328/14.

⁵⁹ Lantwin, MMR 2020, 78 (79).

⁶⁰ Graf, in: MüKo-StGB, § 201a Rn. 77.

⁶¹ Kumkar/Rapp, ZfDR 2022, 199 (209).

⁶² Graf, in: MüKo-StGB, § 201a Rn. 33.

⁶³ Lantwin, MMR 2020, 78 (79).

⁶⁴ Lantwin, MMR 2020, 78 (79).

⁶⁵ Lantwin, MMR 2020, 78 (80).

⁶⁶ Schmidt, in: MüKo-StGB, § 184b Rn. 34.

⁶⁷ Eisele, in: TK-StGB, 31. Aufl. (2025), § 184b Rn. 27 f.

⁶⁸ Eisele, in: TK-StGB, § 184c Rn. 17.

geschützt werden können.

a) § 33 KunstUrhG

Zunächst kann eine Strafbarkeit von Deepfakes im Rahmen des KunstUrhG in Betracht kommen.⁶⁹ Gem. § 22 KunstUrhG dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Das Schutzgut des § 22 ist das Selbstbestimmungsrecht der abgebildeten Person.⁷⁰ Wenn Aufnahmen einer Person der Allgemeinheit vorgeführt werden, stellt dies einen Eingriff in die Privatsphäre und damit auch in das Persönlichkeitsrecht der betroffenen Person dar.⁷¹

Gem. § 33 Abs. 1 KunstUrhG wird die Verbreitung oder die öffentliche Zurschaustellung eines Bildnisses entgegen der §§ 22, 23 KunstUrhG bestraft. Wie § 201a Abs. 2 StGB (s.o.) sanktioniert § 33 KunstUrhG zwar die Verbreitung beziehungsweise die öffentliche Zurschaustellung, nicht aber die Herstellung von Bildnissen.⁷² Eine Ausweitung des Tatbestandes auf das Herstellen geht aufgrund des strafrechtlichen Analogieverbotes zulasten des Täters nicht.⁷³

Ein „Bildnis“ im Sinne des § 22 KunstUrhG liegt vor, wenn das äußere Erscheinungsbild der abgebildeten Person erkennbar wiedergegeben wird.⁷⁴ Daher kommen auch Deepfakes in Betracht, solange die Person identifizierbar und das Deepfake authentisch ist.⁷⁵ Dies ist bei den meisten Deepfakes der Fall, oftmals sogar das Ziel desjenigen, der das Deepfake erstellt.⁷⁶ Darüber hinaus handelt es sich bei dem Veröffentlichen solcher Deepfakes in den sozialen Medien um ein öffentliches Zurschaustellen im Sinne des § 33 Abs. 1 KunstUrhG.⁷⁷

Ist die auf dem Deepfake abgebildete Person erkennbar und hat sie in die Verbreitung – etwa in sozialen Medien – nicht eingewilligt, so wird diese also gem. § 33 KunstUrhG sanktioniert.⁷⁸

Zweifelhaft erscheint hingegen, dass das KunstUrhG den besonderen Unrechtsgehalt des Verbreitens eines Deepfakes überhaupt vollständig erfassen kann.⁷⁹ Bei einem Deepfake wird anders als bei anderen Verletzungen des KunstUrhG nicht etwas tatsächlich Geschehenes in die Öffentlichkeit gezogen. Stattdessen wird eine neue „Realität“ erstellt, indem ein reales Bild manipuliert und ein völlig neues, erfundenes generiert wird.⁸⁰ Der Unrechtsgehalt der Verbreitung von Deepfakes geht daher stark über den Schutzzweck des § 22 KunstUrhG hinaus.⁸¹

b) §§ 106, 108 UrhG

Darüber hinaus kommt eine Strafbarkeit gem. §§ 106, 108 UrhG in Betracht, wenn für die Erstellung des

⁶⁹ Völzmann, ZUM 2025, 493 (498).

⁷⁰ BGH, Urt. v. 14.4.1992 – VI ZR 285/91.

⁷¹ BGH, Urt. v. 16.9.1966 – VI ZR 268/64.

⁷² Valerius, in: BeckOK-StGB, 66. Ed. (2025), KunstUrhG § 33 Rn. 3.

⁷³ Valerius, in: BeckOK-StGB, KunstUrhG § 33 Rn. 3; OLG Hamburg, Beschl. v. 14.4.1972 – 1 Ws 84/72.

⁷⁴ BGH, Urt. v. 10.11.1961 – I ZR 78/60.

⁷⁵ Lantwin, MMR 2020, 78 (79); BVerfG, Beschl. v. 14.2.2005 – 1 BvR 240/04.

⁷⁶ Lantwin, MMR 2020, 78 (Fn. 25).

⁷⁷ Völzmann, ZUM 2025, 493 (498).

⁷⁸ Lantwin, MMR 2020, 78 (79).

⁷⁹ Völzmann, ZUM 2025, 493 (498).

⁸⁰ Völzmann, ZUM 2025, 493 (498).

⁸¹ Völzmann, ZUM 2025, 493 (498).

Deepfakes auf fremdes Bild- oder Videomaterial zurückgegriffen wird, welches entweder ein Lichtbild oder Filmwerk i.S.d. § 2 Abs. 1 Nr. 5, 6 UrhG ist oder zumindest unter den Begriff des Licht- oder Laufbildes i.S.v. §§ 72 Abs. 1, 95 UrhG fällt.⁸² Dies ist bei der Erstellung von Deepfakes prinzipiell der Fall.⁸³ Die §§ 106 Abs. 1, 108 Abs. 1 Nr. 3, 7 UrhG sanktionieren die widerrechtliche Vervielfältigung, Verbreitung, öffentliche Wiedergabe oder die Bearbeitung eines Werkes oder verwandten Schutzgegenstandes ohne die Einwilligung des Berechtigten.⁸⁴ Hinsichtlich der Strafbarkeit von Deepfakes nach dem UrhG ergeben sich also mehrere Anknüpfungspunkte.⁸⁵

Bei der Erstellung eines Deepfakes unter Rückgriff auf fremdes Bild- oder Videomaterial handelt es sich regelmäßig um eine Bearbeitung i.S.d. §§ 3, 23 UrhG oder eine Vervielfältigung.⁸⁶ Darüber hinaus stellt das Hochladen oder das Versenden von Deepfakes in sozialen Medien eine Vervielfältigung oder eine öffentliche Wiedergabe der Bearbeitung gem. §§ 15 Abs. 1 Nr. 1 und Abs. 2 S. 1, 2 Nr. 2, 16 Abs. 1, 19a UrhG dar.⁸⁷ Außerdem ist auch schon die Speicherung des zur Erstellung des Deepfakes verwendeten Bild- oder Filmmaterials eine Vervielfältigung.⁸⁸

Eine Strafbarkeit von Deepfakes scheidet jedoch aus, wenn eine Einwilligung des Berechtigten vorliegt oder eine der in den §§ 44a ff. UrhG verankerten Schranken einschlägig ist. In diesem Kontext kann die Privatkopieschranke gem. § 53 Abs. 1 S. 1 UrhG relevant sein.⁸⁹ Demnach sind einzelne Vervielfältigungen eines Werkes durch eine natürliche Person zum privaten Gebrauch zulässig, solange sie nicht Erwerbszwecken dienen und zur Herstellung des Deepfakes keine offensichtlich rechtswidrig hergestellte beziehungsweise öffentlich zugänglich gemachte Vorlage verwendet wird. Das bedeutet, dass jemand, der ein Deepfake erstellt, aber nicht an Dritte weitergibt, sich durch die Speicherung des Ausgangsmaterials zur Herstellung des Deepfakes nicht i.S.d. UrhG strafbar macht.⁹⁰ Abgesehen davon sanktioniert das UrhG jedoch – wie erläutert – sowohl die widerrechtliche Vervielfältigung, Verbreitung, öffentliche Wiedergabe als auch die Bearbeitung des Werkes.⁹¹ Handelt es sich bei dem Urheber (beispielsweise dem Fotografen) allerdings nicht um die auf dem Deepfake abgebildete Person, wird dieser in den meisten Fällen wohl nur ein begrenztes Verfolgungsinteresse haben.⁹²

c) § 42 Abs. 2 Nr. 1 BDSG

Ferner wäre eine Strafbarkeit gem. § 42 Abs. 2 Nr. 1 BDSG möglich.⁹³ Gem. § 42 Abs. 2 Nr. 1 BDSG wird bestraft, wer ohne Berechtigung personenbezogene Daten, die nicht allgemein zugänglich sind, verarbeitet, und dies gegen Entgelt oder in der Absicht, sich oder einen Dritten zu bereichern, oder einen Dritten dadurch zu schädigen, tut. Bei den Gesichtszügen einer Person, die auf einem Deepfake abgebildet ist, handelt es sich um „personenbezogene Daten“ i.S.d. Art. 4 Nr. 1 DSGVO.⁹⁴ „Verarbeitung“ i.S.d. § 42 Abs. 2 Nr. 1 BDSG ist weit zu

⁸² Lantwin, MMR 2020, 78 (80).

⁸³ Meinicke, DSRITB 2020, 981 (988).

⁸⁴ Lantwin, MMR 2020, 78 (80).

⁸⁵ Lantwin, MMR 2020, 78 (80).

⁸⁶ Lantwin, MMR 2020, 78 (80).

⁸⁷ Heerma, in: Wandtke/Bullinger, UrhR, 6. Aufl. (2022), UrhG § 16 Rn. 19; Bullinger, in: Wandtke/Bullinger, UrhR, UrhG § 19a Rn. 22 f.

⁸⁸ Lantwin, MMR 2020, 78 (80).

⁸⁹ Lantwin, MMR 2020, 78 (80).

⁹⁰ Lantwin, MMR 2020, 78 (80).

⁹¹ Lantwin, MMR 2020, 78 (80).

⁹² Kumkar/Rapp, ZfDR 2022, 199 (210).

⁹³ Kumkar/Rapp, ZfDR 2022, 199 (211).

⁹⁴ Kumkar/Rapp, ZfDR 2022, 199 (211).

verstehen: sowohl die Speicherung des Bildmaterials, welches zur Erstellung eines Deepfakes verwendet wird, als auch die Herstellung des Deepfakes und dessen Verbreitung werden erfasst.⁹⁵

Der Verbreiter des Deepfakes macht sich gem. § 42 Abs. 2 Nr. 1 BDSG allerdings nur strafbar, wenn zur Erstellung des Deepfakes Bilder verwendet wurden, die nicht öffentlich zugänglich sind. Als nicht öffentlich zugänglich gelten beispielsweise auch Fotos, die in den sozialen Medien gepostet wurden, aber nicht im öffentlichen Bereich des Netzwerkes einsehbar sind.⁹⁶ Bei den meisten – insbesondere politischen – Deepfakes dürfte dies jedoch in der Regel zu verneinen sein, weshalb § 42 Abs. 2 Nr. 1 BDSG in der Praxis eher selten in Betracht kommt.⁹⁷

3. Schutzlücken und Reichweite

Wie dargestellt, gibt es bereits einige Straftatbestände, durch die der missbräuchliche Umgang mit Deepfakes sanktioniert werden kann. Dieser Schutz ist allerdings nicht allumfassend und hinsichtlich seiner praktischen Reichweite begrenzt.⁹⁸

Die Verbreitung missbräuchlicher Deepfakes – insbesondere von pornografischen oder anderen massiv persönlichkeitsrechtsverletzenden Deepfakes – wird durch eine Vielzahl von Normen erfasst.⁹⁹ Im Gegensatz dazu wird die Herstellung von Deepfakes von den Normen des Kernstrafrechts, namentlich §§ 185 ff. StGB sowie § 201a Abs. 2 StGB, nicht sanktioniert (s.o.). Die Herstellung von Deepfakes ist nur in bestimmten Konstellationen und unter erhöhten Voraussetzungen strafbar.¹⁰⁰ Davon ausgenommen sind kinder- und jugendpornografische Deepfakes, dessen Herstellung, Verbreitung, sowie Abruf und Besitz durch §§ 184b f. StGB umfassend sanktioniert werden.¹⁰¹

Ungleichmäßigkeiten hinsichtlich der Strafbarkeit von persönlichkeitsrechtsverletzenden Deepfakes ergeben sich außerdem durch die Überschneidungen der verschiedenen Straftatbestände.¹⁰² So ist abhängig davon, welchen Inhalt das Deepfake hat und woher das für die Erstellung verwendete Bild- oder Videomaterial stammt, teilweise nur die Verbreitung, manchmal aber auch die Herstellung strafbar, und das ohne, dass sich aus dem jeweiligen Inhalt des Deepfakes herleiten ließe, warum es zu dieser Ungleichbehandlung kommt.¹⁰³ Dies hat zur Folge, dass bei – inhaltlich sehr ähnlichen – Deepfakes ein unterschiedlich hohes Strafmaß einschlägig sein kann, je nachdem, welche Norm zur Anwendung kommt.¹⁰⁴ So sanktioniert § 33 KunstUrhG die Verbreitung oder öffentliche Zurschaustellung eines Bildnisses mit Geldstrafe oder mit Freiheitsstrafe bis zu einem Jahr, während bei einer Strafbarkeit gem. § 201a Abs. 2 StGB eine Freiheitsstrafe bis zu zwei Jahren in Betracht kommt. Auch § 42 Abs. 2 Nr. 1 BDSG und §§ 106, 108 UrhG sanktionieren die Erstellung und Verbreitung missbräuchlicher Deepfakes mit einer bis zu zwei- beziehungsweise dreijährigen Freiheitsstrafe.

⁹⁵ Lantwin, MMR 2020, 78 (80).

⁹⁶ Bergt, in: Kühling/Buchner, DS-GVI/BDSG, 4. Aufl. (2024), BDSG § 42 Rn. 10.

⁹⁷ Lantwin, MMR 2020, 78 (80).

⁹⁸ Beispielsweise: Lantwin, MMR 2020, 78 (81); Völzmann, ZUM 2025, 493 (499).

⁹⁹ Lantwin, MMR 2020, 78 (81).

¹⁰⁰ Lantwin, MMR 2020, 78 (81).

¹⁰¹ Blocher, KIR 2025, 225 (227).

¹⁰² Lantwin, MMR 2020, 78 (81).

¹⁰³ Lantwin, MMR 2020, 78 (81).

¹⁰⁴ Lantwin, MMR 2020, 78 (81).

Darüber hinaus ist die Reichweite dieser nationalen Strafnormen territorial begrenzt.¹⁰⁵ Grund dafür ist, dass es sich bei der Herstellung und Verbreitung von Deepfakes – insbesondere im Zusammenhang mit sozialen Medien – um ein globales Phänomen handelt. Server und Täter befinden sich oft im Ausland, was eine Durchsetzung des deutschen nationalen Strafrechts erschwert.¹⁰⁶

IV. Strafrechtliche Bewertung und Herausforderungen

Nun sollen die gewonnen Erkenntnisse zum strafrechtlichen Umgang mit Deepfakes kritisch reflektiert werden.

1. Herausforderungen

a) Ungleichmäßigkeiten der strafrechtlichen Bewertung

Wie bereits erläutert, ergeben sich Ungleichmäßigkeiten hinsichtlich der strafrechtlichen Bewertung, je nachdem welche Straftatbestände einschlägig sind, und das auch in Fällen, in denen die jeweiligen Deepfakes inhaltlich keine Veranlassung für eine solche Ungleichbehandlung bieten.¹⁰⁷ Das System bisheriger strafrechtlicher Regelungen, welche im Rahmen der Strafbarkeit von Deepfakes einschlägig sein können, wirkt unübersichtlich.¹⁰⁸

b) Spannungsfeld zwischen Meinungs- und Kunstfreiheit (Art. 5 GG) und Persönlichkeitsrechtsschutz

Auch das Spannungsfeld zwischen der verfassungsrechtlich geschützten Meinungsfreiheit gem. Art. 5 Abs. 1 S. 1 GG und der Kunstfreiheit gem. Art. 5 Abs. 3 GG auf der einen Seite und dem Schutz der Persönlichkeitsrechte auf der anderen Seite stellt eine Herausforderung für den strafrechtlichen Umgang mit Deepfakes dar.¹⁰⁹ Dies ist besonders bei politischen Deepfakes von großer Bedeutung.¹¹⁰ Die strafrechtliche Sanktionierung solcher Deepfakes stellt eine Zäsur der Kunst und einen Eingriff in die Grundrechte des Erstellers beziehungsweise Verbreiters des Deepfakes dar.¹¹¹ Die Vielfalt von Meinungen und deren kritische Darstellung – auch beispielsweise in Form von Satire – sind elementarer Bestandteil unserer Demokratie.¹¹² Im Rahmen des strafrechtlichen Umgangs mit (persönlichkeitsrechtsverletzenden) Deepfakes sind also auch die Grundrechte (Art. 5 Abs. 1 S. 1, Abs. 3 GG) der Ersteller beziehungsweise der Verbreiter der Deepfakes zu berücksichtigen, um eine „Überpönalisierung“ zu verhindern.¹¹³

c) Unzureichende Erfassung des Unrechtskerns

Ferner ist fraglich, ob die bestehenden strafrechtlichen Vorschriften den speziellen Unrechtskern von Deepfakes abschließend erfassen können.¹¹⁴ So schützt § 201a StGB in erster Linie die Intimsphäre des Betroffenen in Form

¹⁰⁵ Lantwin, MMR 2020, 78 (81).

¹⁰⁶ Kumkar/Rapp, ZfDR 2022, 199 (212).

¹⁰⁷ Lantwin, MMR 2020, 78 (81).

¹⁰⁸ Blocher, KIR 2025, 225 (227).

¹⁰⁹ Lantwin, MMR 2020, 78 (81).

¹¹⁰ Lantwin, MMR 2020, 78 (81).

¹¹¹ Erdogan, MMR 2024, 379 (383).

¹¹² Erdogan, MMR 2024, 379 (383).

¹¹³ Erdogan, MMR 2024, 379 (383).

¹¹⁴ Völzmann, ZUM 2025, 493 (499).

eines räumlich geschützten Raumes und die missbräuchliche Verbreitung sowie Herstellung (Abs. 2) realer Bildaufnahmen.¹¹⁵ Der persönlichkeitsrechtsverletzende Charakter missbräuchlicher Deepfakes entspringt jedoch in der Regel der Manipulation bereits bestehender, für sich nicht den höchstpersönlichen Lebensbereich der Person verletzender Aufnahmen, die häufig sogar veröffentlicht worden sind.¹¹⁶ Die Bildaufnahme, welche als Ausgangsmaterial verwendet wird, stellt für sich also oftmals keine Verletzung des höchstpersönlichen Lebensbereichs der betroffenen Person dar.¹¹⁷ Damit weichen Deepfakes von dem eigentlichen Unrechtskern des § 201a StGB ab.¹¹⁸ Dasselbe gilt auch hinsichtlich der Strafbarkeit von Deepfakes gem. des KunstUrhG: bei der Verbreitung missbräuchlicher Deepfakes geht es im Grunde nicht darum, etwas tatsächlich Privates, Intimes der Öffentlichkeit zur Schau zu stellen, sondern um die „Generierung einer neuen Realität“¹¹⁹, die mit dem tatsächlichen Bildmaterial nichts zu tun hat.¹²⁰ Damit geht der Unrechtsgehalt von – insbesondere pornografischen – Deepfakes stark über den Schutzzweck des § 22 KunstUrhG hinaus.¹²¹ Das Strafrecht kann dem Phänomen der Deepfakes somit nur zum Teil, allerdings nicht hinsichtlich seines spezifischen Unrechtskerns, begegnen.¹²²

d) Schwierigkeiten bei der Strafverfolgung

Darüber hinaus stellen Deepfakes eine Herausforderung für die Strafverfolgung dar.¹²³ Probleme sind beispielsweise die Anonymität der Täter im Internet sowie der Auslandsbezug vieler Taten in Bezug auf die Herstellung sowie Verbreitung.¹²⁴ Nicht selten haben die Täter ihren Sitz im Ausland, sodass das deutsche nationale Strafrecht an seine Grenzen stößt.¹²⁵ Zudem ist die Ermittlungsarbeit der Strafverfolgungsbehörden in diesem Bereich sehr aufwändig, und die Taten sind teilweise aufgrund des Auslandsbezugs praktisch kaum verfolgbar.¹²⁶

Außerdem verbreiten sich missbräuchliche Deepfakes über die sozialen Medien sehr schnell, was nur schwierig zu unterbinden ist.¹²⁷ Daher kann eine – zeitlich viel spätere – strafrechtliche Sanktionierung die zu dem Zeitpunkt längst eingetretene Persönlichkeitsrechtsverletzung nur unzureichend kompensieren.¹²⁸ Grundsätzlich ist die Rechtsdurchsetzung im digitalen Raum bisher nur begrenzt effektiv.¹²⁹ Des Weiteren ist es aufgrund der Authentizität von Deepfakes technisch schwierig, diese von realen Aufnahmen zu unterscheiden und Verstöße zu erkennen.¹³⁰ Aufgrund dieser Durchsetzungsdefizite kann man annehmen, dass eine strafrechtliche Aufarbeitung von Deepfakes wahrscheinlich auch in der Zukunft keine große Relevanz erfahren wird.¹³¹

¹¹⁵ Völzmann, ZUM 2025, 493 (499).

¹¹⁶ Völzmann, ZUM 2025, 493 (499).

¹¹⁷ Völzmann, ZUM 2025, 493 (499).

¹¹⁸ Völzmann, ZUM 2025, 493 (499).

¹¹⁹ Völzmann, ZUM 2025, 493 (498).

¹²⁰ Völzmann, ZUM 2025, 493 (498).

¹²¹ Völzmann, ZUM 2025, 493 (498).

¹²² Völzmann, ZUM 2025, 493 (499 f.).

¹²³ Kumkar/Rapp, ZfDR 2022, 199 (212).

¹²⁴ Kumkar/Rapp, ZfDR 2022, 199 (212).

¹²⁵ Kumkar/Rapp, ZfDR 2022, 199 (212).

¹²⁶ Kumkar/Rapp, ZfDR 2022, 199 (212).

¹²⁷ Lantwin, MMR 2020, 78 (81).

¹²⁸ Kumkar/Rapp, ZfDR 2022, 199 (212).

¹²⁹ Pölle, RD 2025, 452 (458) Rn. 35.

¹³⁰ Pölle, RD 2025, 452 (458) Rn. 33.

¹³¹ Kumkar/Rapp, ZfDR 2022, 199 (212).

2. Handlungsbedarf – neue Strafnorm erforderlich?

Mit Blick auf diese Herausforderungen, mit denen das deutsche Strafrecht derzeit im Rahmen der Sanktionierung persönlichkeitsrechtsverletzender Deepfakes zu kämpfen hat, stellt sich die Frage, ob es einer Reform hinsichtlich der Sanktionierung von persönlichkeitsrechtsverletzenden Deepfakes bedarf.

a) Argumente gegen eine Reform

Teilweise wird die Auffassung vertreten, dass es keiner Reform bedarf, da das Phänomen Deepfakes bereits hinreichend strafrechtlich sanktioniert werde.¹³² Die Ungleichmäßigkeiten im Zusammenhang mit den Voraussetzungen der Strafbarkeit und der Höhe der Strafandrohung seien unter Berücksichtigung des jeweiligen Ausmaßes des Schadens sowie des von der jeweiligen Strafnorm geschützten Rechtsgutes gerechtfertigt.¹³³

Für diese Ansicht spreche zudem, dass es sich bei der Annahme fremder Identitäten um einen elementaren Bestandteil der Selbstdarstellung im virtuellen Raum handle, welcher nicht nur im Rahmen von Kunst und Satire, sondern auch darüber hinaus noch ein sozialadäquates Verhalten darstellen könne.¹³⁴ Im Zusammenhang damit wird auch vor einer Überpönalisierung, besonders im Bereich Kunst und Satire, gewarnt.¹³⁵

Gegner einer strafrechtlichen Reform zum Thema Deepfakes bezweifeln außerdem die Effektivität eines solchen Straftatbestandes hinsichtlich der Abschreckung von potenziellen Tätern, sowie der Durchsetzbarkeit.¹³⁶ Wie bereits geschildert, erweist sich die Strafverfolgung im digitalen Raum als schwierig, weshalb vermutet wird, dass ein neu eingeführter Straftatbestand praktisch ohnehin kaum relevant wäre.¹³⁷ Wichtiger und effizienter als eine strafrechtliche Sanktionierung seien gesellschaftliche Maßnahmen, wie eine bessere Aufklärungsarbeit sowie die Förderung von Medienkompetenz.¹³⁸

b) Argumente für eine Reform

Im Gegensatz dazu wird ein Reformbedarf jedoch von vielen Stimmen mit Verweis auf die derzeitigen Ungleichmäßigkeiten der strafrechtlichen Bewertung (s.o.) bejaht.¹³⁹ Befürworter einer Reform sind der Auffassung, dass das Phänomen Deepfakes bisher eben nicht ausreichend sanktioniert werden könne.¹⁴⁰ Dafür sprechen die bereits erläuterten Herausforderungen des deutschen Strafrechts im Umgang mit Deepfakes, unter anderem Strafbarkeitslücken im Zusammenhang mit der Pönalisierung der Herstellung von Deepfakes sowie eine nur teilweise Erfassung des spezifischen Unrechtskerns missbräuchlicher Deepfakes (s.o.). So sehen es nicht nur verschiedene Stimmen aus der Literatur¹⁴¹, sondern auch der Bundesrat und die Bundesrechtsanwaltskammer (BRAK).¹⁴² Des

¹³² Beispielsweise: *Meinicke*, DSRITB 2020, 981 (996); *Kumkar/Rapp*, ZfDR 2022, 199 (211).

¹³³ *Meinicke*, DSRITB 2020, 981 (996).

¹³⁴ *Golla*, Fake-Strafrecht in Wahlkampfzeiten, Verfassungsblog on Matters Constitutional, 7.9.2021; online abrufbar unter: <https://verfassungsblog.de/fake-strafrecht-in-wahlkampfzeiten/> (zuletzt abgerufen am 6.10.2025).

¹³⁵ *Golla*, Fake-Strafrecht in Wahlkampfzeiten, Verfassungsblog on Matters Constitutional, 07.09.2021; online abrufbar unter: <https://verfassungsblog.de/fake-strafrecht-in-wahlkampfzeiten/> (zuletzt abgerufen am 6.10.2025).

¹³⁶ *Kumkar/Rapp*, ZfDR 2022, 199 (211 f.).

¹³⁷ *Kumkar/Rapp*, ZfDR 2022, 199 (212).

¹³⁸ *Meinicke*, DSRITB 2020, 981 (998).

¹³⁹ *Lantwin*, MMR 2020, 78 (81).

¹⁴⁰ Beispielsweise: *Lantwin*, MMR 2020, 78 (81); *Völzmann*, ZUM 2025, 493 (499).

¹⁴¹ Beispielsweise: *Lantwin*, MMR 2020, 78 (81 ff.); *Blocher*, KIR 2025, 225 (228 ff.); *Klass*, ZUM 2025, 485 (491).

¹⁴² BT-Drs. 21/1383, 2; BRAK, Stellungnahme Nr. 75/2024, S. 7 f.

Weiteren enthält Art. 5 Abs. 1 lit. b der EU-Richtlinie zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt eine Kriminalisierungsanweisung hinsichtlich der Herstellung, Manipulation oder Veränderung sowie der öffentlichen Zugänglichmachung von Bildern oder Videos, die den Anschein erwecken, dass eine Person eindeutig sexuelle Handlungen vornimmt.¹⁴³ Zumindest in Bezug auf Deepfake-Pornografie wird also auch von der EU eine strafrechtliche Regelung der Mitgliedstaaten gefordert.¹⁴⁴

c) *Zwischenergebnis Reformbedarf*

Im Ergebnis erscheinen die Argumente für ein Reformfordernis im Zusammenhang mit der strafrechtlichen Sanktionierung missbräuchlicher Deepfakes überzeugend. Die Herstellung und Verbreitung solcher Deepfakes können massive Persönlichkeitsrechtsverletzungen implizieren,¹⁴⁵ weshalb eine umfassende strafrechtliche Pönalisierung dieses Phänomens möglich sein muss. Strafbarkeitslücken oder eine nur teilweise Erfassung des Unrechtsgehalts von Deepfakes müssen ausgeschlossen werden.¹⁴⁶ Vor diesem Hintergrund ist eine spezifische Norm gegen Bildmanipulationen im Netz meines Erachtens erforderlich. Hinsichtlich der Ausgestaltung einer solchen Reform spalten sich jedoch die Meinungen.

V. Reform

1. *Überblick über die aktuelle Reformdiskussion*

In anderen Ländern sind Gesetzesänderungen zu dieser Problematik bereits umgesetzt worden. So etwa gibt es in vielen US-Bundesstaaten mittlerweile sog. „false impersonation statutes“¹⁴⁷, welche unter bestimmten Voraussetzungen die „wissentliche, glaubwürdige Nachahmung einer Person über das Internet“¹⁴⁸ unter Strafe stellen. Als erstes EU-Land beschloss Italien am 23. September 2025 die Einführung eines Straftatbestandes, welcher die Verbreitung von Deepfakes mit einer Freiheitsstrafe von bis zu fünf Jahren sanktioniert, wenn einer Person dadurch ein Schaden zugefügt wird und die Verbreitung ohne Zustimmung der betroffenen Person erfolgt.¹⁴⁹

Am 5. Juli 2024 wurde auch in Deutschland durch den Bundesrat ein, durch den Freistaat Bayern eingebrachter, Gesetzesentwurf für einen § 201b StGB zur Sanktionierung von Deepfakes beschlossen.¹⁵⁰ Dieser hatte allerdings aufgrund von Diskontinuität keinen Erfolg.¹⁵¹ Nun ist der, mit dem vom letzten Jahr identische, Gesetzesentwurf durch den Bundesrat erneut in den Bundestag eingebracht worden.¹⁵² Ziel des § 201b StGB-E ist der Schutz von Persönlichkeitsrechten vor Deepfakes.¹⁵³ Eine diesbezügliche Entscheidung des Bundestages steht zum gegenwärtigen Zeitpunkt noch aus.

¹⁴³ Richtlinie (EU) 2024/1385; Zimmermann, KriPoZ 2025, 50.

¹⁴⁴ Zimmermann, KriPoZ 2025, 50.

¹⁴⁵ Blocher, KIR 2025, 225 (226).

¹⁴⁶ BT-Drs. 21/1383, S. 2.

¹⁴⁷ Beispielsweise: Cal. Penal Code § 528.5.

¹⁴⁸ Lantwin, MMR 2020, 78 (81).

¹⁴⁹ Art. 612-quater c.p. (Italien); Wykretowicz, Italien beschließt als erstes EU-Land Haftstrafe für Deepfakes, 23.9.2025; online abrufbar unter: <https://mueller.legal/de/aktuelles/italien-beschliesst-als-erstes-eu-land-haftstrafe-fuer-deepfakes-auch-deutschland-plant-strafrechtliche-regelungen> (zuletzt abgerufen am 6.10.2025).

¹⁵⁰ BR-Drs. 222/24; Woerlein, MMR-Aktuell 2024, 01624.

¹⁵¹ Beukelmann, NJW-Spezial 2025, 504.

¹⁵² BT-Drs. 21/1383.

¹⁵³ BT-Drs. 21/1383, S. 1.

2. Mögliche Reformmodelle

Es gibt bereits einige Reformvorschläge bezüglich der strafrechtlichen Sanktionierung von Deepfakes.

a) Grundsätzliches Verbot von Deepfakes

Ein generelles Verbot von Deepfakes würde eine Verletzung der Meinungs- und Kunstfreiheit gem. Art. 5 Abs. 1 S. 1, Abs. 3 GG darstellen.¹⁵⁴ Darüber hinaus verfolgen nicht alle Deepfakes missbräuchliche Zwecke.¹⁵⁵ Ein grundsätzliches Verbot ist daher abzulehnen.¹⁵⁶

b) Strafbarkeit der „nichteinvernehmlichen, glaubwürdigen Nachahmung einer Person“

aa) Darstellung

Teilweise wird – in Anlehnung an die „false impersonation statutes“ aus den USA – die Einführung eines Straftatbestandes zur Strafbarkeit der „nichteinvernehmlichen, glaubwürdigen Nachahmung einer Person“¹⁵⁷ vorgeschlagen. Dadurch würde das Zugänglichmachen einer unberechtigten, glaubwürdigen Nachahmung einer Person gegenüber Dritten sanktioniert werden, solange diese entweder eine Täuschung im Rechtsverkehr bezweckt oder in der Absicht erfolgt, die abgebildete Person zu schädigen, einzuschüchtern, zu Gewalttaten aufzustacheln oder erhebliche Unruhen in der Bevölkerung zu provozieren.¹⁵⁸ Strafbar wäre dieses Verhalten, wenn der Täter weiß, dass es sich bei dem Inhalt um eine manipulierte und keine reale Aufnahme handelt.¹⁵⁹ Argumentiert wird, dass ein solcher Straftatbestand technologieoffen formuliert sei und nicht an eine bestimmte Form der Herstellung manipulierter Aufnahmen anknüpfe, sodass die Vorschrift auch auf zukünftige neu entwickelte Technologien angewendet werden könne.¹⁶⁰ Darüber hinaus enthalte dieser Straftatbestand Elemente der überschießenden Innentendenz, wie beispielsweise die Schädigungsabsicht, wodurch gewährleistet werden könne, dass der Tatbestand nicht ausufert, sondern sich auf tatsächlich missbräuchliches Verhalten beschränkt.¹⁶¹ Dadurch werde verhindert, dass die Grundrechte der betroffenen Person in unzulässiger Weise beschränkt werden.¹⁶² Um auch die Herstellung persönlichkeitsrechtsverletzender Deepfakes erfassen zu können, wird vorgeschlagen, das Tatbestandsmerkmal der Eignung zur erheblichen Ansehensschädigung gem. § 201a Abs. 2 StGB als weitere Tatbestandsalternative aufzunehmen.¹⁶³

bb) Kritik

An einem solchen Straftatbestand der unberechtigten Nachahmung einer Person wird jedoch kritisiert, dass dieser mit dem im deutschen Strafrecht verankerten Grundsatz des Tatstrafrechts unvereinbar sei.¹⁶⁴ Darüber hinaus sei

¹⁵⁴ Lantwin, MMR 2019, 574 (577).

¹⁵⁵ Lantwin, MMR 2019, 574 (574 f.).

¹⁵⁶ Lantwin, MMR 2020, 78 (81).

¹⁵⁷ Lantwin, MMR 2020, 78 (81).

¹⁵⁸ Lantwin, MMR 2020, 78 (81).

¹⁵⁹ Lantwin, MMR 2020, 78 (81).

¹⁶⁰ Lantwin, MMR 2020, 78 (81).

¹⁶¹ Lantwin, MMR 2020, 78 (81).

¹⁶² Lantwin, MMR 2020, 78 (81).

¹⁶³ Lantwin, MMR 2020, 78 (81).

¹⁶⁴ Eisele, in: TK-StGB, Vorb. § 13 Rn. 3.

die Pönalisierung der Herstellung von Deepfakes problematisch.¹⁶⁵ Dies wird damit begründet, dass die reine Herstellung missbräuchlicher Deepfakes – anders als die Verbreitung – für sich genommen zumindest keine schwerwiegende Verletzung der Persönlichkeitsrechte der abgebildeten Person mit sich bringe.¹⁶⁶ Bei der Herstellung handele es sich vielmehr um eine in der Regel straflose Vorbereitungshandlung.¹⁶⁷ Anders sei dies allenfalls bei der Herstellung von pornografischen Deepfakes, wobei auch in diesen Fällen fraglich sei, ob das Ausmaß der Persönlichkeitsverletzung so gravierend ist, dass es eine strafrechtliche Pönalisierung verlangt.¹⁶⁸ Laut Kritikern sei einer derartigen Ausdehnung der Strafbarkeit mit Vorsicht zu begegnen.¹⁶⁹ Eine „Vorverlagerung der Strafbarkeit in den Bereich der Vorbereitungshandlung“¹⁷⁰ sei abzulehnen.

c) *Orientierung an Urkundendelikten, §§ 267 ff. StGB*

Ein weiterer Lösungsvorschlag ist die Orientierung an den Urkundendelikten gem. §§ 267 ff. StGB.¹⁷¹ Eine direkte Anwendung der Urkundendelikte auf Deepfakes scheidet aus, da diese weder Urkundenqualität besitzen noch unter den Begriff der „technischen Aufzeichnung“ i.S.d. § 268 StGB subsumiert werden können.¹⁷² Laut Vertretern dieses Reformvorschlags käme jedoch eine Erweiterung der §§ 267 ff. StGB in Betracht.¹⁷³

Der Schutzzweck der §§ 267 ff. StGB ist der „Schutz der Sicherheit und Zuverlässigkeit des Rechts- und Beweisverkehrs“¹⁷⁴. Digitale Medieninhalte gewinnen in der Gesellschaft zunehmend an Bedeutung für die Kommunikation.¹⁷⁵ Daher spielt selbstverständlich auch das Vertrauen in die Echtheit dieser Inhalte eine große Rolle.¹⁷⁶ Das Schutzbedürfnis der Authentizität solcher digitalen Inhalte sei deshalb mit dem Schutzbedürfnis von Urkunden und technischen Aufzeichnungen vergleichbar.¹⁷⁷

Damit eine Erweiterung der Urkundendelikte in Betracht kommt, müssten Deepfakes darüber hinaus für die Rechtsposition einer am Rechtsverkehr teilnehmenden Person von Bedeutung sein.¹⁷⁸ Dies ist bei Deepfakes, die eine andere Person abbilden, in der Regel gegeben, da sie die geschützten Rechtspositionen der betroffenen Person tangieren.¹⁷⁹

In subjektiver Hinsicht müsste die Tat zudem eine unmittelbare Einwirkung auf das Rechtsleben der betroffenen Person darstellen, indem sie diese zu einem rechtserheblichen Verhalten veranlasst.¹⁸⁰ Dies kann bei Persönlichkeitsrechtsverletzenden Deepfakes allerdings problematisch sein, da der Täter häufig lediglich beabsichtigt, die

¹⁶⁵ Meinicke, DSRITB 2020, 981 (996 f.).

¹⁶⁶ Meinicke, DSRITB 2020, 981 (997).

¹⁶⁷ Meinicke, DSRITB 2020, 981 (997).

¹⁶⁸ Meinicke, DSRITB 2020, 981 (997).

¹⁶⁹ Meinicke, DSRITB 2020, 981 (997).

¹⁷⁰ Meinicke, DSRITB 2020, 981 (997).

¹⁷¹ Wörner/Gmelin, RIDP 2024, 367 (373 f.).

¹⁷² Wörner/Gmelin, RIDP 2024, 367 (373 f.).

¹⁷³ Blocher, KIR 2025, 225 (228).

¹⁷⁴ Blocher, KIR 2025, 225 (229).

¹⁷⁵ Blocher, KIR 2025, 225 (229).

¹⁷⁶ Blocher, KIR 2025, 225 (229).

¹⁷⁷ Blocher, KIR 2025, 225 (229).

¹⁷⁸ Erb, in: MüKo-StGB, § 267 Rn. 70 ff.

¹⁷⁹ Blocher, KIR 2025, 225 (229).

¹⁸⁰ Schuster, in: TK-StGB, § 267 Rn. 87b.

abgebildete Person schlecht darzustellen und sich oder andere zu unterhalten.¹⁸¹ Dagegen spricht, dass die rechtserheblichen Interaktionen einer Person durchaus durch die Darstellung dieser Person im virtuellen Raum beeinflusst werden können.¹⁸² So kann eine negative Selbst- oder Fremddarstellung im Netz beispielsweise negative Auswirkungen auf das Berufsleben des Betroffenen haben.¹⁸³ Aus diesem Grund sei die Verbreitung von Deepfakes durchaus zu der Veranlassung rechtserheblichen Verhaltens geeignet.¹⁸⁴ Diesen möglichen negativen Folgen für die abgebildete Person ist sich der Täter in der Regel auch bewusst.¹⁸⁵

Darüber hinaus wird argumentiert, dass das strafwürdige Verhalten bei der Herstellung und Verbreitung von Deepfakes mit den Tathandlungen der §§ 267 ff. StGB vergleichbar sei.¹⁸⁶ Zudem würde ein Tatbestand zum Schutz der Authentizität von Medieninhalten systematisch gut in den 23. Abschnitt des StGB passen und den Unrechtskern missbräuchlicher Deepfakes sachgerecht erfassen.¹⁸⁷

d) § 201 b StGB-E

aa) Zielsetzung

Der aktuelle, durch den Freistaat Bayern initiierte und vom Bundesrat beschlossene Reformvorschlag befasst sich mit der Einführung eines § 201b StGB.¹⁸⁸ Wie bereits erwähnt, liegt er derzeit dem Bundestag vor. Ziel dieses Gesetzesentwurfes ist die Sanktionierung von Persönlichkeitsrechtsverletzungen durch digitale Fälschung.¹⁸⁹ Es handele sich um einen Entwurf zu einer „spezifisch auf Deepfakes und vergleichbare technische Manipulationen“¹⁹⁰ ausgerichteten Norm. In der Gesetzesbegründung des Antrags wird auf die bisher unzureichenden strafrechtlichen Sanktionierungsmöglichkeiten missbräuchlicher Deepfakes verwiesen.¹⁹¹

bb) Tatbestand

§ 201b Abs. 1 StGB-E sanktioniert das Zugänglichmachen eines mit computertechnischen Mitteln hergestellten oder veränderten Medieninhalts, welcher den Anschein einer wirklichkeitsgetreuen Bild- oder Tonaufnahme des äußeren Erscheinungsbildes, Verhaltens oder mündlicher Äußerungen einer Person erweckt und dadurch deren Persönlichkeitsrecht verletzt, mit einer Freiheitsstrafe bis zu zwei Jahren oder einer Geldstrafe.¹⁹²

In Fällen, in denen der Medieninhalt der Öffentlichkeit zugänglich gemacht wird oder einen Vorgang des höchstpersönlichen Lebensbereichs darstellt, wird dies gem. § 201b Abs. 2 StGB-E mit einer Freiheitsstrafe von bis zu fünf Jahren oder mit Geldstrafe bestraft.¹⁹³ Davon erfasst wäre unter anderem Deepfake-Pornografie.¹⁹⁴

¹⁸¹ Henry et. al., Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery, 2021, S. 3.

¹⁸² Blocher, KIR 2025, 225 (230).

¹⁸³ Chesney/Citron, Calif. L. Rev. 2019, 1753 (1775).

¹⁸⁴ Blocher, KIR 2025, 225 (230).

¹⁸⁵ Blocher, KIR 2025, 225 (230).

¹⁸⁶ Wörner/Gmelin, RIDP 2024, 367 (374).

¹⁸⁷ Blocher, KIR 2025, 225 (230).

¹⁸⁸ BT-Drs. 21/1383.

¹⁸⁹ BT-Drs. 21/1383, S. 1.

¹⁹⁰ BT-Drs. 21/1383, S. 3.

¹⁹¹ BT-Drs. 21/1383, S. 2 ff.

¹⁹² BT-Drs. 21/1383, S. 6.

¹⁹³ BT-Drs. 21/1383, S. 6 f.

¹⁹⁴ Völzmann, ZUM 2025, 493 (500); BT-Drs. 21/1383, S. 9 ff.

§ 201b Abs. 3 StGB-E nimmt Handlungen i.S.d. Abs. 1 und 2, die in Wahrnehmung überwiegender berechtigter Interessen erfolgen, namentlich der Kunst, Wissenschaft, Forschung, Lehre, der Berichterstattung über Vorgänge des Zeitgeschehens oder der Geschichte oder ähnlichen Zwecken dienen, von der Strafbarkeit aus.¹⁹⁵

Gem. § 201b Abs. 4 StGB-E können durch den Täter oder Teilnehmer verwendete Tonträger oder andere technische Mittel eingezogen werden.¹⁹⁶

cc) Kritik

Die BRAK äußerte sich im Oktober 2024 kritisch zu dem Gesetzesentwurf aus dem letzten Jahr, welcher inhaltlich mit dem aus diesem Jahr identisch ist.¹⁹⁷ In ihrer Stellungnahme kritisiert die BRAK zunächst, dass in der Gesetzesbegründung mehrfach von „Deepfakes“, „KI“ oder „künstlichen neuronalen Netzwerken“ gesprochen wird, während der Wortlaut des Tatbestandes gem. § 201b Abs. 1 S. 1 StGB-E „mit computertechnischen Mitteln“ hergestellte oder veränderte Medieninhalte, lautet. Die Unterscheidung zwischen KI-generierten und manuell erzeugten Manipulationen sei nicht sinnvoll.¹⁹⁸

Darüber hinaus sei das Rechtsgut unklar. Einerseits werde der Schutz des allgemeinen Persönlichkeitsrechts betont, andererseits werde in der Gesetzesbegründung der „Einsatz von Deepfake-Technologie zu Desinformationszwecken, namentlich zur Manipulation des demokratischen Willensbildungsprozesses“¹⁹⁹ als erster Anwendungsbereich genannt.²⁰⁰ Handlungen, die den demokratischen Willensbildungsprozess manipulieren, können sich jedoch stark von denen unterscheiden, die das Persönlichkeitsrecht des Betroffenen verletzen. Für einen solch weitgehenden Schutzzweck fehle die Legitimation.²⁰¹ Kritisch sei außerdem, dass der Wortlaut der Norm sehr weit sei, wodurch jegliches Zugänglichmachen eines missbräuchlichen Deepfakes an einen Dritten oder die Öffentlichkeit zu einer Strafbarkeit führen könne.²⁰² So könnte beispielsweise schon eine mithilfe von Photoshop bearbeitete Datei ein taugliches Tatobjekt sein.²⁰³ Darüber hinaus würde durch den Begriff „Medieninhalt“ ein neuer Rechtsbegriff geschaffen werden, welchen das Strafrecht bisher nicht kennt, was zur Erzeugung neuer Auslegungsprobleme führen würde.²⁰⁴

Auch die Rechtfertigungsgründe des § 201b Abs. 3 StGB-E seien problematisch.²⁰⁵ Das Verbreiten bewusst unwahrer Inhalte ist laut der allgemein anerkannten Rechtsprechung von dem Schutzbereich der Meinungs- und Kunstfreiheit gem. Art. 5 Abs. 1 und Abs. 3 GG ohnehin nicht erfasst.²⁰⁶ Das Verbreiten nicht als fiktiv gekennzeichneten Deepfakes für gerechtfertigt zu halten, wenn dies beispielsweise der Meinungs- oder Kunstfreiheit

¹⁹⁵ BT-Drs. 21/1383, S. 7.

¹⁹⁶ BT-Drs. 21/1383, S. 7.

¹⁹⁷ BRAK, Stellungnahme Nr. 75/2024.

¹⁹⁸ BRAK, Stellungnahme Nr. 75/2024, S. 4; BT-Drs. 21/1383, S. 1 ff.

¹⁹⁹ BT-Drs. 21/1383, S. 10.

²⁰⁰ BRAK, Stellungnahme Nr. 75/2024, S. 4.

²⁰¹ BRAK, Stellungnahme Nr. 75/2024, S. 4.

²⁰² BRAK, Stellungnahme Nr. 75/2024, S. 4.

²⁰³ Woerlein, MMR-Aktuell 2024, 01624.

²⁰⁴ BRAK, Stellungnahme Nr. 75/2024, S. 6.

²⁰⁵ BRAK, Stellungnahme Nr. 75/2024, S. 4.

²⁰⁶ BVerfG, Urt. v. 9.10.1991 – 1 BvR 1555/88; BGH, Urt. v. 27.9.2016 – VI ZR 250/13.

dient, würde dieser Rechtsprechung folglich widersprechen.²⁰⁷ Darüber hinaus sei nicht nachzuvollziehen, in welchen Konstellationen der Rechtfertigungsgrund der „Berichterstattung über Vorgänge des Zeitgeschehens oder der Geschichte“ gem. § 201b Abs. 3 StGB-E einschlägig sein könnte.²⁰⁸

Dass in § 201b Abs. 4 StGB-E explizit auch der Teilnehmer genannt wird, könne außerdem zu einer „Selbstzensur verunsicherter Nutzer“²⁰⁹ führen, da bereits Personen, welche ein Deepfake lediglich auf Social Media Plattformen geteilt haben, eine strafrechtliche Verfolgung und gem. Abs. 4 eine Einziehung ihrer Tonträger oder anderer technischer Mittel befürchten müssten.²¹⁰

Darüber hinaus empfiehlt die BRAK, zwischen den Handlungsformen klarer zu unterscheiden und die Strafbarkeit des Gehilfen durch das Erfordernis des Direktvorsatzes einzugrenzen.²¹¹

Auch in der Literatur wird der Gesetzesentwurf zu § 201b StGB-E kritisch gesehen, wobei überwiegend auf die Kritik der BRAK verwiesen wird.²¹² Darüber hinaus wird kritisiert, dass in der Gesetzesbegründung erläutert wird, dass der „Anschein einer wirklichkeitsgetreuen Bild- oder Tonaufnahme“ i.S.d. § 201b Abs. 1 StGB-E entfalle, wenn es sich um eine „klar erkennbare Manipulation oder eine klar erkennbare künstliche Herstellung“²¹³ handelt, jedoch nicht definiert wird, was genau darunter zu verstehen ist.²¹⁴ Des Weiteren sei auch der subjektive Tatbestand nicht optimal ausgestaltet, da für eine Strafbarkeit bei dem Täter mindestens der Eventualvorsatz vorliegen muss, welcher in der Praxis allerdings schwierig nachzuweisen sei.²¹⁵

e) Erweiterung des § 201a StGB

Anstelle der Schaffung einer völlig neuen Strafnorm kommt auch die Ergänzung des bereits geltenden § 201a StGB in Betracht. Die BRAK empfiehlt in ihrer Stellungnahme vom Oktober 2024 die Ergänzung des § 201a Abs. 2 StGB um einen S. 2, welcher das Zugänglichmachen eines „mit computertechnischen Mitteln hergestellten oder veränderten Inhalt[s] (§ 11 Abs. 3), der den Anschein einer wirklichkeitsgetreuen Bild- oder Tonaufnahme des äußeren Erscheinungsbildes, des Verhaltens oder mündlicher Äußerungen dieser Person erweckt“²¹⁶ sanktioniert, wenn durch den Inhalt dem Ansehen der betroffenen Person erheblich geschadet werden kann.²¹⁷ Vorteil dieses Reformvorschlages sei die Umgehung der Beteiligten- und Rechtfertigungsprobleme des § 201b StGB-E.²¹⁸ Durch den Verweis auf § 11 Abs. 3 StGB werden zudem die Schaffung des neuen Rechtsbegriffs „Medieninhalt“ und damit einhergehende Auslegungsprobleme vermieden.²¹⁹

²⁰⁷ BRAK, Stellungnahme Nr. 75/2024, S. 5.

²⁰⁸ BRAK, Stellungnahme Nr. 75/2024, S. 5.

²⁰⁹ BRAK, Stellungnahme Nr. 75/2024, S. 5.

²¹⁰ BRAK, Stellungnahme Nr. 75/2024, S. 5.

²¹¹ BRAK, Stellungnahme Nr. 75/2024, S. 6.

²¹² Beispielsweise: Blocher, KIR 2025, 225 (228); Woerlein, MMR-Aktuell 2024, 01624; Beukelmann, NJW-Spezial 2025, 504.

²¹³ BT-Drs. 21/1383, S. 22.

²¹⁴ Woerlein, MMR-Aktuell 2024, 01624.

²¹⁵ Woerlein, MMR-Aktuell 2024, 01624.

²¹⁶ BRAK, Stellungnahme Nr. 75/2024, S. 7.

²¹⁷ BRAK, Stellungnahme Nr. 75/2024, S. 7 f.

²¹⁸ BRAK, Stellungnahme Nr. 75/2024, S. 8.

²¹⁹ BRAK, Stellungnahme Nr. 75/2024, S. 6, 8.

3. Beurteilung und eigener Reformvorschlag

Hinsichtlich der strafrechtlichen Sanktionierung missbräuchlicher Deepfakes liegen also bereits verschiedene Reformvorschläge vor, von denen einige erheblich divergieren, andere hingegen aufeinander aufbauen.

Im Ergebnis erscheint die Schaffung eines neuen Straftatbestandes in Anlehnung an den vorgeschlagenen § 201b StGB-E überzeugend. Die Kritik der BRAK sowie von Teilen der Literatur ist jedoch berechtigt und sollte bei der Gestaltung einer neuen Strafnorm berücksichtigt werden. Unter Einbeziehung dieser Einwände und zur weiteren Präzisierung schlage ich folgende geänderte Fassung des § 201b StGB-E vor:

§ 201b Verletzung von Persönlichkeitsrechten durch digitale Fälschung²²⁰

- (1) Wer mit computertechnischen Mitteln einen Inhalt (§ 11 Abs. 3 StGB), der den Anschein einer wirklichkeitsgetreuen Bild- oder Tonaufnahme des äußeren Erscheinungsbildes, des Verhaltens oder mündlicher Äußerungen dieser Person erweckt und einen Vorgang des höchstpersönlichen Lebensbereichs zum Gegenstand hat, herstellt oder verändert, um das Persönlichkeitsrecht einer anderen Person zu verletzen, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. Gleiches gilt, wenn sich die Tat nach Satz 1 auf eine verstorbene Person bezieht und deren Persönlichkeitsrecht dadurch schwerwiegend verletzt wird.*
- (2) Wer einen mit computertechnischen Mitteln hergestellten oder veränderten Inhalt (§ 11 Abs. 3 StGB), der den Anschein einer wirklichkeitsgetreuen Bild- oder Tonaufnahme des äußeren Erscheinungsbildes, des Verhaltens oder mündlicher Äußerungen dieser Person erweckt, einer dritten Person zugänglich macht, um das Persönlichkeitsrecht einer anderen Person zu verletzen, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Absatz 1 Satz 2 findet entsprechend Anwendung.*
- (3) Wer in den Fällen des Absatzes 2 Satz 1 den Inhalt der Öffentlichkeit zugänglich macht oder einen Inhalt zugänglich macht, der einen Vorgang des höchstpersönlichen Lebensbereichs zum Gegenstand hat, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.*
- (4) Auf die in den Absätzen 1, 2 und 3 genannten Taten findet § 193 StGB entsprechend Anwendung.*
- (5) Die Bild- oder Tonträger oder andere technische Mittel, die der Täter verwendet hat, können eingezogen werden. § 74a StGB ist anzuwenden.*

Im Gegensatz zu dem Gesetzesentwurf des Bundesrates enthält dieser Formulierungsvorschlag fünf statt vier Absätze. Dadurch, dass durch Abs. 1 die Herstellung und Veränderung eines Inhalts gesondert sanktioniert werden, wird der Empfehlung der BRAK nachgegangen, klarer zwischen den Handlungsformen zu unterscheiden.²²¹ Der Strafraum wird dementsprechend angepasst, sodass gem. Abs. 1 die Herstellung oder Veränderung mit Frei-

²²⁰ Stark angelehnt an: BT-Drs. 21/1383, S. 6 f.; BRAK, Stellungnahme Nr. 75/2024.

²²¹ BRAK, Stellungnahme Nr. 75/2024, S. 6.

heitsstrafe bis zu einem Jahr oder Geldstrafe sanktioniert wird, während die Zugänglichmachung (Abs. 2) weiterhin mit einer Freiheitsstrafe von bis zu zwei Jahren oder Geldstrafe geahndet wird. Auch die Kritik aus der Literatur, dass hinsichtlich der strafrechtlichen Sanktionierung der Herstellung von Deepfakes Vorsicht geboten sei,²²² wird berücksichtigt, indem diese nur in den Fällen, in denen das Deepfake einen Vorgang des höchstpersönlichen Lebensbereichs zum Gegenstand hat, unter Strafe gestellt wird. Dem Einwand, die Herstellung eines Deepfakes solle nicht strafbar sein, da es sich hierbei bloß um eine straflose Vorbereitungshandlung handele²²³, ist im Falle von massiv persönlichkeitsrechtsverletzenden Deepfakes nicht zuzustimmen. Meines Erachtens sollten insbesondere die Persönlichkeitsrechte von Opfern pornografischer Deepfakes bereits geschützt werden können, bevor es zu einer etwaigen Verbreitung kommt.

Um eine Überdehnung des Straftatbestandes zu verhindern, wird dieser auf subjektiver Seite so formuliert, dass der Täter oder Teilnehmer mit Direktvorsatz handeln muss (s. Wortlaut: „um zu“), was auch auf der Empfehlung der BRAK beruht.²²⁴ Zwar erschwert das Vorsatzelement eine Verurteilung aufgrund von Schwierigkeiten hinsichtlich der Nachweisbarkeit²²⁵, jedoch würde eine Ausweitung der Strafbarkeit auf fahrlässiges Verhalten zu einer Überdehnung des Straftatbestandes führen,²²⁶ welche meines Erachtens zu weit ginge. Des Weiteren wird die Kritik der BRAK hinsichtlich der Rechtfertigungsgründe berücksichtigt und diese daher in Abs. 4 durch einen Verweis auf § 193 StGB ersetzt.²²⁷ Um eine von der BRAK befürchtete, „Selbstzensur verunsicherter Nutzer“²²⁸ zu vermeiden, wurde außerdem der letzte Absatz so angepasst, dass sich die Einziehung verwendeter Tonträger oder anderer technischer Mittel nur noch auf den Täter und nicht mehr auf den Teilnehmer bezieht. Des Weiteren wurde auf Empfehlung der BRAK der neue Rechtsbegriff „Medieninhalt“ durch „Inhalt“ mit Verweis auf § 11 Abs. 3 StGB ersetzt, um Auslegungsprobleme zu vermeiden.²²⁹

Ein derartig formulierter § 201b StGB würde die verschiedenen Handlungsformen umfassend sanktionieren, jedoch ohne die Strafbarkeit zu weit auszudehnen und der ultima ratio Funktion des Strafrechts zu widersprechen.²³⁰ Der spezifische Unrechtsgehalt von Deepfakes wird vollumfänglich erfasst und insbesondere die Herstellung missbräuchlicher Deepfakes könnte regelmäßiger strafrechtlich sanktioniert werden. Mit Blick auf die zunehmende Bedeutung von KI und das damit einhergehende Missbrauchspotential erscheint dies angemessen.

VI. Fazit

Die Auseinandersetzung mit Deepfakes erhellte, dass es sich hierbei um ein Phänomen handelt, das das Strafrecht und den Schutz von Persönlichkeitsrechten vor erhebliche Herausforderungen stellt. Während Deepfakes einerseits für harmlose oder sogar nützliche Zwecke eingesetzt werden können, birgt ihre missbräuchliche Erstellung oder Verbreitung erhebliche Gefahren für die Integrität des Einzelnen. Die vorangehende Analyse hat gezeigt, dass bestehende strafrechtliche Normen nur unzureichend auf die spezifischen Gefahren reagieren können, die von Deepfakes ausgehen. Insbesondere die Tatbestände der §§ 185 ff. StGB sowie des § 201a StGB stoßen an ihre

²²² Meinicke, DSRITB 2020, 981 (997).

²²³ Meinicke, DSRITB 2020, 981 (997).

²²⁴ BRAK, Stellungnahme Nr. 75/2024, S. 6.

²²⁵ Woerlein, MMR-Aktuell 2024, 01624.

²²⁶ BRAK, Stellungnahme Nr. 75/2024, S. 6.

²²⁷ BRAK, Stellungnahme Nr. 75/2024, S. 5.

²²⁸ BRAK, Stellungnahme Nr. 75/2024, S. 5.

²²⁹ BRAK, Stellungnahme Nr. 75/2024, S. 6.

²³⁰ BRAK, Stellungnahme Nr. 75/2024, S. 6.

Grenzen, da sie den Missbrauch digitaler Bild-, Video- und Tonmanipulationen nicht systematisch und umfassend erfassen.

Vor diesem Hintergrund ist die Einführung eines speziellen Straftatbestandes gegen digitale Bildmanipulation im Netz in Anlehnung an den derzeit im Bundestag vorliegenden Gesetzesentwurf des § 201b StGB-E²³¹ grundsätzlich zu begrüßen. Dieser Reformvorschlag zeigt, dass der Gesetzgeber die nur teilweise Erfassung des Unrechtsgehalts von Deepfakes erkannt hat und auf die neuartigen, mit KI einhergehenden Gefahren reagieren möchte. Nichtsdestotrotz wurde deutlich, dass der Entwurf in seiner jetzigen Form nicht frei von Schwächen ist. Die Kritik der BRAK sowie Stimmen in der Literatur sind insoweit berechtigt, als der Gesetzeswortlaut Unklarheiten aufweist, etwa hinsichtlich des neuen Rechtsbegriffs „Medieninhalt“, der erfassten Handlungsformen oder der Rechtfertigungsgründe.²³²

Um diesen Bedenken Rechnung zu tragen und den Schutz der Persönlichkeitsrechte effektiv auszugestalten, habe ich im Rahmen dieser Arbeit eine modifizierte Fassung des § 201b StGB-E vorgeschlagen. Dieser Reformvorschlag unterscheidet deutlich zwischen Herstellung und Veränderung, sowie Zugänglichmachung von Deepfakes und entspricht damit dem Erfordernis einer differenzierten Erfassung der Handlungsformen. Ferner wird dem gesteigerten Unrechtsgehalt der Zugänglichmachung an Dritte im Vergleich zur bloßen Herstellung oder Veränderung durch eine entsprechende Staffelung der Strafraumen berücksichtigt. Ergänzt wird der Entwurf durch den Verweis auf § 193 StGB, wodurch Rechtfertigungsmöglichkeiten systematisch eingebunden werden.

Im Ergebnis lässt sich festhalten, dass die Einführung eines neuen Straftatbestandes notwendig und angemessen erscheint, um den spezifischen Gefahren von Deepfakes wirksam zu begegnen. Der vorgeschlagene § 201b StGB-E in der in dieser Arbeit entwickelten Fassung gewährleistet einen präzise abgrenzbaren und dogmatisch stimmigen Schutz des Persönlichkeitsrechts, ohne eine Überdehnung des Strafrechts oder verfassungsrechtlich problematische Unklarheiten zu riskieren. Damit leistet er einen Beitrag zur Modernisierung des Strafrechts und zur Anpassung an technische Entwicklungen im digitalen Zeitalter. Zugleich bleibt der Gesetzgeber gefordert, die praktische Umsetzung und Effektivität eines solchen Straftatbestandes fortlaufend zu prüfen. Angesichts der rasanten technischen Entwicklung ist nicht auszuschließen, dass sich in Zukunft neue Missbrauchsformen herausbilden, die heute noch nicht absehbar sind. Diese Arbeit versteht sich insofern als Anstoß, den strafrechtlichen Schutz kontinuierlich an die digitale Realität anzupassen. Dabei darf jedoch nicht verkannt werden, dass das Strafrecht das Problem rund um missbräuchliche Deepfakes allein nicht bewältigen kann; erforderlich sind zusätzliche Maßnahmen wie verstärkte Aufklärungsarbeit, Sensibilisierung der Öffentlichkeit und präventive technische Lösungen.²³³

Die Kriminalpolitische Zeitschrift (KriPoZ) darf dieses Werk unter den Bedingungen der Digital Peer Publishing Lizenz (DPPL) elektronisch übermitteln und zum Download bereitstellen. Der Lizenztext ist im Internet abrufbar unter der Adresse <http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-de0>.

²³¹ BT-Drs. 21/1383.

²³² BRAK, Stellungnahme Nr. 75/2024, S. 4 ff.

²³³ Lantwin, MMR 2020, 78 (82).