

Strafrechtlicher Persönlichkeitsschutz vor Deepfakes

von RA Dr. Dr. Fabian Teichmann, LL.M.
(London), EMBA (Oxford)*

Abstract

Deepfakes – also mittels Künstlicher Intelligenz manipulierte Video-, Audio- oder Bildaufnahmen – ermöglichen es, Personen täuschend echt Dinge sagen oder tun zu lassen, die sie nie gesagt oder getan haben. Dies birgt erhebliche Gefahren für das allgemeine Persönlichkeitsrecht der Betroffenen. Besonders häufig werden Frauen durch pornografische Deepfakes Opfer schwerwiegender Ruf- und Persönlichkeitsverletzungen. Bislang erfolgt eine Ahndung allenfalls über allgemeine Straftatbestände wie z.B. Beleidigung oder Verleumdung, die den spezifischen Unrechtsgehalt der technisch hochentwickelten Täuschung jedoch nicht vollständig erfassen. Vor diesem Hintergrund wurde im Jahr 2024 ein Gesetzentwurf in den Bundesrat eingebracht, der einen neuen Straftatbestand zum Schutz vor persönlichkeitsrechtsverletzenden Deepfakes schaffen soll. Der Entwurf (§ 201b StGB-E) stellt die Verbreitung wirklichkeitsgetreuer KI-manipulierter Bild- oder Tonaufnahmen unter Strafe, soweit hierdurch das Persönlichkeitsrecht der dargestellten Person verletzt wird. Vorgesehen sind Freiheitsstrafen bis zu zwei Jahren, in schweren Fällen bis zu fünf Jahren. Ausnahmen sollen für berechnete Interessen wie Kunst, Wissenschaft oder Satire gelten. Der Vorstoß hat eine rechtspolitische Debatte ausgelöst, bei der Befürworter die Schutzlücke und den Präventionsbedarf angesichts zunehmender Deepfake-Missbräuche betonen und Kritiker – darunter die Bundesregierung und die Bundesrechtsanwaltskammer – vor Unbestimmtheiten und zu weitem Anwendungsbereich der geplanten Norm warnen und auf bereits bestehende strafrechtliche Sanktionen verweisen. Der Beitrag ordnet den Gesetzentwurf in den bestehenden Rechtsrahmen ein, beleuchtet die aktuellen Diskussionen und weist auf die Herausforderungen bei der strafrechtlichen Regulierung von Deepfakes hin.

Criminal Law Protection of Personality Rights against Deepfakes. Deepfakes – media content manipulated via artificial intelligence – can convincingly depict individuals saying or doing things that never occurred. This poses serious risks to the personality rights of those depicted, for example through highly realistic fake pornography or fabricated statements by public figures. Currently, such

conduct can only be penalized indirectly under general criminal provisions (e.g. defamation), which often fail to capture the specific wrongfulness of the deception involved. In 2024, a legislative proposal was introduced in Germany's Bundesrat to create a new criminal offense aimed at deepfake-related violations of personality rights. The draft (§ 201b of the German Criminal Code) would criminalize making realistic AI-altered images or recordings accessible to others without consent if this violates the person's right of personality. The offense carries up to two years' imprisonment (up to five years in severe cases), with exceptions for socially adequate purposes such as art, science, or satire. This initiative has sparked debate: supporters emphasize the need for better protection and deterrence as deepfake abuse rises, while critics (including the federal government and the national bar association) caution that the proposal is overly broad or vague and point to existing laws that already address parts of the problem. This article examines the proposed law in the context of current German criminal law, discusses the ongoing debate, and highlights challenges in effectively addressing deepfakes through criminal legislation.

I. Einleitung

Manipulierte Medieninhalte mittels Künstlicher Intelligenz – sogenannte *Deepfakes* – haben in den letzten Jahren zunehmend für Aufsehen gesorgt. Darunter versteht man Video-, Bild- oder Audioaufnahmen, die mit Hilfe von Machine-Learning-Techniken so verfälscht oder synthetisch hergestellt werden, dass sie realistisch erscheinen und eine echte Person imitieren. Auf diese Weise können beliebige Äußerungen oder Handlungen einer Person fingiert werden, ohne dass diese tatsächlich stattgefunden haben. Eine eindrucksvolle Illustration bot ein Fall in Spanien, bei dem Mitte 2023 über Chatgruppen täuschend echte Nacktbilder von Schülerinnen – generiert aus harmlosen Social-Media-Fotos – verbreitet wurden.¹ Derartige Deepfake-Szenarien legen nahe, welches Missbrauchspotential diese Technologie birgt. So sind bereits *Fake-Porno-Videos* im Umlauf, in denen Gesichter Prominenter oder Privatpersonen auf Körper in Pornofilmen montiert werden, ebenso wie gefälschte Sprachnachrichten

* RA Dr. Dr. Fabian Teichmann, LL.M. (London), EMBA (Oxford) ist Lehrbeauftragter an den Universitäten Kassel, Trier und zu Köln.

¹ Legal Tribune Online, Streit um Strafbarkeit von Deepfakes, online abrufbar unter: <https://bit.ly/437XyOf> (zuletzt abgerufen am 15.9.2025); Frankfurter Allgemeine, Gefälschte Nacktbilder von Minderjährigen in Spanien im Umlauf, online abrufbar unter: <https://bit.ly/4gUJ3TE> (zuletzt abgerufen am 15.9.2025); Spiegel, Offenbar von KI generierte Nacktbilder zirkulieren an Schulen, online abrufbar unter: <https://bit.ly/4mP93kA> (zuletzt abgerufen am 15.9.2025).

oder Videos von Politiker und Politikerinnen, die skandalöse Aussagen „treffen“.² Für die Betroffenen können die Folgen gravierend sein. Sie sehen sich mit tiefgreifenden Verletzungen ihres allgemeinen Persönlichkeitsrechts konfrontiert, etwa in Form von Rufschädigung, Ehrverletzung, Verletzung der Intimsphäre oder dem Verlust der Kontrolle über das eigene Bild. Nicht selten kommt es zu nachhaltigen psychischen Belastungen der Opfer bis hin zu einem Gefühl der Hilflosigkeit gegenüber der Verbreitung der Fälschungen.³ Angesichts solcher Gefährdungen stellt sich die Frage, wie das geltende Strafrecht auf das Phänomen „Deepfakes“ reagiert und ob neue Straftatbestände erforderlich sind, um effektiven Persönlichkeitsschutz im digitalen Zeitalter zu gewährleisten.

Die Diskussion um eine strafrechtliche Regulierung von Deepfakes erhielt bereits 2024 durch einen entsprechenden Gesetzentwurf des Bundesrates erste Konturen. Nachdem dieser infolge der parlamentarischen Diskontinuität nicht mehr verabschiedet wurde, hat der Bundesrat den Entwurf zu Beginn der neuen Legislaturperiode 2025 erneut eingebracht. Zwar existieren im deutschen Recht schon heute diverse Strafvorschriften, die einschlägige Verhaltensweisen unter Strafe stellen – doch greifen diese in Fällen von Deepfakes oft zu kurz. Insbesondere erfassen allgemeine Tatbestände wie Beleidigung oder Verleumdung regelmäßig nur Teilaspekte des Unrechts, ohne die besondere Täuschungsqualität und Realitätsnähe von KI-Manipulationen abzubilden.⁴ Auch Normen zum Schutz der Intimsphäre durch Bildaufnahmen oder zum Datenschutz lassen Lücken, wenn das kompromittierende Material gar nicht auf realen Vorgängen beruht, sondern künstlich generiert ist.⁵ Vor diesem Hintergrund wurde im Jahr 2024 eine Initiative gestartet, um *Deepfake-basierte Persönlichkeitsrechtsverletzungen* explizit unter Strafe zu stellen. Auf Vorschlag des Freistaats Bayern beschloss der Bundesrat im Juli 2024 einen Gesetzentwurf zum strafrechtlichen Schutz vor Deepfakes, der einen neuen § 201b StGB einführen soll.⁶ Dieser Vorstoß – der sich derzeit im Gesetzgebungsverfahren befindet – hat eine breite rechtspolitische Debatte entfacht über die Notwendigkeit und Ausgestaltung spezieller Strafnormen gegen Deepfakes.⁷

Im Folgenden werden zunächst die Gefahren und Schutzlücken bei persönlichkeitsrechtsverletzenden Deepfakes dargelegt (II.), sodann die bisherige Rechtslage skizziert (III.) und der Inhalt des Gesetzentwurfs erläutert (IV.). Anschließend werden die Argumente der Befürworter und Kritiker diskutiert sowie alternative Lösungsansätze beleuchtet (V.), bevor ein Fazit mit Ausblick erfolgt (VI.).

II. Deepfakes als Herausforderung für den Persönlichkeitsschutz

Deepfakes berühren in besonderem Maße das allgemeine Persönlichkeitsrecht der abgebildeten Personen. Dieses aus Art. 1 Abs. 1 GG (Menschenwürde) und Art. 2 Abs. 1 GG (allgemeine Handlungsfreiheit) hergeleitete Recht schützt die engere persönliche Lebenssphäre, die Selbstbestimmung über die eigene Darstellung und die persönliche Ehre.⁸ Gerade diese Schutzgüter werden durch realistisch wirkende KI-Fälschungen potenziell verletzt. So beeinträchtigen Deepfake-Angriffe die Würde und den sozialen Achtungsanspruch der Opfer, indem sie diese der Lächerlichkeit preisgeben oder in einen entwürdigenden Kontext stellen. Wer ohne Zustimmung in ein täuschend echt simuliertes Geschehen „hineingestellt“ wird – etwa mit Worten, die er nie geäußert hat, oder in Handlungen, die er nie vorgenommen hat – verliert die Kontrolle über sein öffentliches Erscheinungsbild und Identitätsmerkmale.⁹ Die virtuelle *Entfremdung der Identität* durch Fremdbestimmung kann zu einem Gefühl des Ausgeliefertseins führen, da Außenstehende die Fälschung nur schwer von der Realität unterscheiden können.¹⁰ Die bloße Möglichkeit, Deepfakes als solche zu entlarven (etwa mittels technischer Detektionsverfahren), beseitigt die Persönlichkeitsbeeinträchtigung nicht völlig, denn das entwürdigende falsche Bild entfaltet bereits eine Verletzungswirkung, sobald es verbreitet wird.¹¹

In besonderem Maße betroffen von Deepfake-Angriffen sind *Frauen*. Untersuchungen zeigen, dass ein überwiegender Teil (über 90 %) der im Internet kursierenden Deepfake-Inhalte pornographischer Natur ist und praktisch alle Opfer solcher *Deepfake-Pornografie* weiblich

² Kraetzig, Computer und Recht 2024, 207 (208); Vassilaki, Computer und Recht 2024, 701; Buchholz/Kremer, Computer und Recht 2024, 56 (57); Karaboga, in: Jaki/Steiger (Hrsg.), Interdisziplinäre Perspektiven auf Erkennung, Beschreibung und Regulation, 2023, S. 197–199.

³ BT-Drs. 21/1383, online abrufbar unter: <https://bit.ly/4mR8dDf> (zuletzt abgerufen am 15.9.2025); Kraetzig, Computer und Recht 2024, 207 (209); Vassilaki, Computer und Recht 2024, 701 (704); Buchholz/Kremer, Computer und Recht 2024, 56 (57).

⁴ Beck-aktuell, Bayern fordert drastische Strafen für bösartige Deepfakes im Internet, online abrufbar unter: <https://bit.ly/437XyOf> (zuletzt abgerufen am 15.9.2025); Kraetzig, Computer und Recht 2024, 207 (208); Vassilaki, Computer und Recht 2024, 701 (702).

⁵ Legal Tribune Online (Fn 1); Deutschlandfunk, Sexualisierte Gewalt durch KI, online abrufbar unter: <http://bit.ly/46Xxpmn> (zuletzt abgerufen am 15.9.2025); Spiegel, Die Männer hinter den Fake-Pornos, online abrufbar unter: <http://bit.ly/3J6egXw> (zuletzt abgerufen am 15.9.2025).

⁶ BR-Drs. 222/24, online abrufbar unter: <http://bit.ly/4n2LRzI> (zuletzt abgerufen am 15.9.2025); KriPoZ-RR 17/2024; Schilling, Streit um Strafbarkeit von Deepfakes, online abrufbar unter: <http://bit.ly/3J1RNLj> (zuletzt abgerufen am 15.9.2025).

⁷ Vassilaki, Computer und Recht 2024, 701 (704); Kraetzig, Computer und Recht 2024, 207 (212).

⁸ Seiler, in: Dürig/Herzog/Scholz, GG, 107. Aufl. (2025), Art. 2 Abs. 1 Rn. 127–131; Bamberger/Roth, in: BeckOK-BGB, 75. Ed. (Stand: 1.8.2025), § 823 Rn. 1172–1174; Sachs, GG, 10. Aufl. (2024), Art. 1 Rn. 5–7; Huber/Voßkuhle, GG, 8. Aufl. (2024), Art. 2 Rn. 9–10.

⁹ Sachs (Fn. 8), GG, Art. 1 Rn. 38–41; KriPoZ-RR 17/2024; Lennartz, NJW 2023, 3543 (3547); Kraetzig, Computer und Recht 2024, 207 (209); Kumkar/Rapp, ZfDR 2022, 199 (205); Lantwin, MMR 2019, 574 (575); BT-Drs. 21/1383; Deutscher Bundestag, Wissenschaftliche Dienste: Deepfakes Straf- und zivilrechtliche Implikationen, online abrufbar unter: <http://bit.ly/4pYukex> (zuletzt abgerufen am 15.9.2025), S. 6–7.

¹⁰ BT-Drs. 21/1383; Kraetzig, Computer und Recht 2024, 207 (208); Kumkar/Rapp, ZfDR 2022, 199 (220); Deutscher Bundestag (Fn. 9).

¹¹ Determann, KI-Recht, 2025, § 5 Rn. 113; Legal Tribune Online (Fn. 1).

sind.¹² Häufig handelt es sich um *sexualisierte Diffamierungen*: Mit Hilfe frei verfügbarer „Deepfake Apps“ werden Gesichter von Frauen – teils Prominente, teils Frauen aus dem privaten Umfeld – nahtlos in explizite pornografische Bilder oder Videos montiert.¹³ Die Betroffenen erleiden dadurch nicht nur eine Verletzung ihres Rechts am eigenen Bild und ihrer Intimsphäre, sondern auch schwere Rufschäden, weil Außenstehende glauben könnten, es handle sich um reale Aufnahmen. Fälle von sogenannter *Revenge Porn* (Rachepornos) werden durch KI-Technik zusätzlich verschärft, da selbst Frauen, die niemals intime Aufnahmen von sich preisgegeben haben, mittels Deepfake-Technik in solcher Weise bloßgestellt werden können. Das Phänomen ist damit Teil einer breiteren Problematik der bildbasierten sexualisierten Gewalt, vor der zuletzt verstärkt gewarnt wird.¹⁴ Die permanente Verfügbarkeit solcher Fälschungen im Netz kann zu andauernder Viktimisierung führen, da eine effektive Beseitigung aller Kopien kaum gewährleistet werden kann.¹⁵ In der Folge ziehen sich manche Betroffene aus der Öffentlichkeit zurück (*Silencing-Effekt*), was gesamtgesellschaftlich die Meinungsvielfalt beeinträchtigen kann.¹⁶

Doch nicht nur im Bereich pornographischer Inhalte stellen Deepfakes eine Gefahr dar. Auch *politische Persönlichkeitsrechte* und die demokratische Willensbildung können untergraben werden, wenn z.B. täuschend echte Falschaussagen von Politikerinnen und Politikern in Umlauf gebracht werden. Solche Manipulationen dienen oft der gezielten Diskreditierung im Wahlkampf oder der Verbreitung von Desinformation. Prominente Beispiele umfassen gefälschte Video-Reden oder Audio-Mitschnitte, die etwa einem Staatsoberhaupt aggressive Aussagen unterstellen. Die dadurch ausgelösten öffentlichen Reaktionen können den Ruf der betreffenden Person irreparabel beschädigen, bevor die Fälschung aufgeklärt ist. Zwar ließe sich derartige üble Nachrede oder Verleumdung unter Umständen mit den bestehenden Ehrschutzdelikten ahnden – die Besonderheit liegt jedoch in der hohen Glaubwürdigkeit der visuellen oder akustischen Täuschung, die eine neue Qualität der Irreführung darstellt. Darüber hinaus können Deepfakes auch zur Betrugsanbahnung eingesetzt werden, etwa wenn mittels *KI-generierter Stimmen* von Vorgesetzten oder Angehörigen telefonisch Anweisungen oder Notlagen vorgetäuscht werden

(sog. CEO-Fraud bzw. Schockanrufe).¹⁷ Solche Fälle betreffen zwar primär Vermögensdelikte, verdeutlichen aber ebenfalls das breite Gefährdungspotential von Deepfakes.

Zusammenfassend konfrontiert die Deepfake-Technologie den rechtlichen Persönlichkeitsschutz mit neuartigen Herausforderungen: Die *Täuschungsechtheit* und die Geschwindigkeit, mit der manipulierte Inhalte verbreitet werden können, erfordern ein Umdenken bei Schutzkonzepten. Neben präventiven Maßnahmen – etwa Aufklärung und technische Deepfake-Detektion – rückt die Frage in den Fokus, ob das Strafrecht als schärfste Form sozialer Kontrolle hinreichend auf diese Entwicklung vorbereitet ist.

III. Bisherige strafrechtliche Handhabung und Schutzlücken

Mangels ausdrücklicher Regelung mussten Deepfake-Konstellationen bislang unter allgemeine Straftatbestände subsumiert werden. Dies führte jedoch zu dogmatischen Einordnungsproblemen und Lücken im Schutzzumfang. Im Folgenden wird ein Überblick über einschlägige Normen gegeben und deren Anwendbarkeit auf Deepfake-Fälle erörtert.

1. Ehrschutzdelikte (§§ 185 ff. StGB)

Ein naheliegender Ansatz ist die Prüfung von Beleidigungs- oder Verleumdungsdelikten, sofern ein Deepfake dazu dient, die Ehre der betroffenen Person anzugreifen. In Betracht kommt insbesondere Üble Nachrede gem. § 186 StGB¹⁸ oder Verleumdung gem. § 187 StGB¹⁹, wenn durch die Verbreitung eines Deepfake, etwa eines Fake-Pornovideos oder eines manipulierten „Statements“, ehrverletzende Tatsachen über die Person behauptet werden. So könnte das Präsentieren einer Person in pornographischer Handlung implizit die (unwahre) Tatsachenbehauptung enthalten, sie habe an solchen Handlungen teilgenommen – was geeignet ist, ihren Ruf zu schädigen. Tatbestandsmäßig lässt sich dies als Üble Nachrede gem. § 186 StGB qualifizieren, sofern der Täter die Unwahrheit nicht positiv kennt, oder als Verleumdung gem. § 187 StGB, wenn die falsche Tatsache wissentlich verbreitet wird. Allerdings bestehen hier Beweisprobleme²⁰ und Einschränkungen, da die Strafverfolgung der §§ 185 ff.

¹² ZDF heute, Deepfake-Pornos: Gezielte Gewalt gegen Frauen, online abrufbar unter: <http://bit.ly/4q41Tfb> (zuletzt abgerufen am 15.9.2025); Frankfurter Rundschau, Erschreckend viele Frauen werden Opfer von Deepfake-Pornografie, online abrufbar unter: <http://bit.ly/3VZ8R7G> (zuletzt abgerufen am 15.9.2025); Legal Tribune Online (Fn. 1); *Kumkar/Rapp*, ZfDR 2022, 199 (225); *Lantwin*, MMR 2019, 574 (575); Deutscher Bundestag (Fn. 9).

¹³ Beck-aktuell (Fn. 4); NRW LT-Drs. 18/10528, online abrufbar unter: <http://bit.ly/4nNo6gf> (zuletzt abgerufen 15.9.2025), S.3; *Kumkar/Rapp*, ZfDR 2022, 199 (225); *Kraetzig*, Computer und Recht 2024, 207 (209); *Lantwin*, MMR 2019, 574 (575); Deutscher Bundestag (Fn. 9).

¹⁴ *Kumkar/Rapp*, ZfDR 2022, 199 (225); *Kraetzig*, Computer und Recht 2024, 207 (209); *Lantwin*, MMR 2019, 574 (575); Deutscher Bundestag (Fn. 9).

¹⁵ BT-Drs. 21/1383; Deutscher Bundestag (Fn. 9); *Kumkar/Rapp*, ZfDR 2022, 199 (225); *Kraetzig*, Computer und Recht 2024, 207 (209); *Lantwin*, MMR 2019, 574 (576); Deutscher Bundestag (Fn. 9).

¹⁶ *Sittig*, Strafrecht und Regulierung von Deepfake-Pornografie, online abrufbar unter: <http://bit.ly/3L57Ate> (zuletzt abgerufen am 15.9.2025); LT-NRW (Fn. 13); *Kumkar/Rapp*, ZfDR 2022, 199 (217); *Kraetzig*, Computer und Recht 2024, 207 (209); *Lantwin*, MMR 2019, 574 (575).

¹⁷ *Kevekordes*, in: Hoeren/Sieber/Holznapel, MMR-HdB, 62. Aufl. (2024), Teil 29 Rn. 29; *Stern/Sodan/Möstl*, Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverband, 2. Aufl. (2022), § 121 Rn. 67-69; *Hornung/Schallbruch*, IT-Sicherheitsrecht, 2. Aufl. (2024), Rn. 37; Legal Tribune Online (Fn. 1).

¹⁸ *Heinze*, in: NK-MedienStrafR, 2023, § 186 StGB Rn. 44; *Regge/Pegel*, in: MüKo-StGB, 5. Aufl. (2025), § 186 StGB Rn. 14-15; *Eisele/Schittenhelm*, in: TK-StGB, 31. Aufl. (2025), § 186 Rn. 5.

¹⁹ *Kindhäuser/Neumann/Paeffgen/Saliger*, NK-StGB, § 187 Rn. 3-6; *Kindhäuser/Hilgendorf*, LPK-StGB, 10. Aufl. (2025), § 187 Rn. 1-7; *Valerius*, in: BeckOK-StGB, 66. Ed. (Stand: 1.8.2025), 66. Aufl. (2025), § 187 Rn. 2-5.

²⁰ *Regge/Pegel*, in: MüKo-StGB, § 187 Rn. 8; *Dölling/Duttge/König/Rössner*, StGB, 5. Aufl. (2022), § 187 Rn. 3.

StGB in der Regel einen Strafantrag des Opfers gem. § 194 StGB²¹ voraussetzt und bei Verstorbenen die Ehrschutzdelikte nur sehr eingeschränkt greifen. Strafbar ist nach § 189 StGB die Verunglimpfung des Andenkens Verstorbener, was nicht alle Deepfake-Konstellationen erfasst. Überdies schützen die §§ 185 ff. StGB primär die Ehre im sozialen Geltungsanspruch; eine dem Persönlichkeitsrecht im umfassenden Sinne gerecht werdende Würdigung – etwa bei Eingriffen in die Intimsphäre durch Fake-Pornografie – ist damit nicht zwingend verbunden.

Ferner ist nicht jede Deepfake-Montage ohne Weiteres als ehrenrührige Äußerung im Sinne dieser Delikte zu fassen. Beleidigung gem. § 185 StGB erfordert beispielsweise eine Kundgabe von Missachtung oder Nichtachtung gegenüber dem Betroffenen. Die Verbreitung eines pornographischen Deepfake-Images kann zwar als solche eine Demütigung darstellen, doch erfolgt sie oft *ohne direkte kommunikative Äußerung* des Täters dem Opfer gegenüber, was die Subsumtion unter § 185 StGB erschweren mag.²² Der Bundesrat vertritt zudem die Auffassung, ein computergenerierter Inhalt stelle keine „Äußerung“ im Wortsinne dar und könne daher nicht als Beleidigung bewertet werden.²³ Insgesamt greifen die Ehrschutzdelikte punktuell, insbesondere bei rufschädigenden Deepfakes, lassen aber andere Persönlichkeitsverletzungen – z.B. die bloße Entstellung des Erscheinungsbildes oder Entwürdigung ohne ehrenrührige Tatsachenbehauptung – ungehört.

2. Schutz der Privatsphäre und Intimsphäre

Das StGB kennt bereits Normen, die sich dem Bildnis- und Lebensbereichsschutz widmen. Insbesondere stellt § 201a StGB („Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen“) bestimmte unbefugte Aufnahmen und deren Verbreitung unter Strafe. So macht sich gem. § 201a Abs. 1 Nr. 1 und 2 StGB strafbar, wer z.B. von einer anderen Person in deren Wohnung heimlich Fotos macht oder bloßstellende Bildaufnahmen einer hilflosen Person verbreitet und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt.²⁴ Zudem erfasst § 201a Abs. 2 StGB das Verbreiten von Aufnahmen, die durch solche Taten erlangt wurden, sowie – in Nummer 5 – das unbefugte Zugänglichmachen ursprünglich befugt hergestellter Bildaufnahmen aus dem höchstpersönlichen Bereich.²⁵ Denkbar wäre, pornographische Deepfakes unter diese Vorschrift zu fassen, da sie in der Regel intime Handlungen zum Gegenstand haben. Allerdings stößt man

hier auf ein Tatbestandsproblem, da § 201a stets eine *Bildaufnahme* (oder Videoaufnahme) einer realen Person in einer bestimmten Situation verlangt.²⁶ Deepfakes sind aber keine realen Aufnahmen, sondern synthetische Montagen. Selbst wenn das Endergebnis realistisch wirkt, fehlt es am tatsächlichen „Abbild“ eines tatsächlichen Vorgangs. Daher ist umstritten, ob § 201a StGB einschlägig sein kann. Allenfalls könnte man argumentieren, das Zugänglichmachen eines sexualisierten Deepfake-Bildes verletze den höchstpersönlichen Lebensbereich ähnlich wie eine echte Nacktfotografie, doch bewegt man sich damit an den Grenzen des Wortlauts. Bislang ist nicht höchstrichterlich geklärt, ob etwa eine mittels KI erzeugte Nacktaufnahme unter § 201a Abs. 2 StGB fällt.²⁷ Tendenziell lässt sich feststellen, dass der Gesetzgeber bei § 201a an reale Bilder dachte – generierte Fälschungen werden *ausdrücklich (noch) nicht erfasst*.²⁸

Eine neuere Vorschrift, die 2021 ins StGB eingefügt wurde, ist § 184k StGB („Verletzung des Intimbereichs durch Bildaufnahmen“). Diese Norm stellt z.B. das „Upskirting“ (heimliches Fotografieren unter den Rock) unter Strafe. Auch hier fehlt jedoch die Komponente der technischen Manipulation; maßgeblich ist das unbefugte Herstellen oder Übertragen von Bildaufnahmen tatsächlicher Intimbereiche. Deepfake-Pornografie nutzt demgegenüber in der Regel frei zugängliche Fotos, etwa ein Porträt des Gesichts, und generiert daraus ein neues Bild in intimmem Kontext. Da keine tatsächliche intime Körperaufnahme der betroffenen Person stattfindet, dürfte § 184k StGB in diesen Fällen nicht greifen.²⁹

Erwähnenswert ist in diesem Zusammenhang auch das Kunsturhebergesetz (KUG). Nach § 22 KUG dürfen Bildnisse einer Person grundsätzlich nur mit Einwilligung verbreitet oder öffentlich zur Schau gestellt werden.³⁰ Ein Verstoß hiergegen kann nach § 33 KUG als Straftat (mit bis zu einem Jahr Freiheitsstrafe) geahndet werden. Diese seit langem bestehende Regelung betrifft klassischerweise das ungenehmigte Veröffentlichen von Fotos. Sie ist im Prinzip auch auf Deepfake-Bilder anwendbar – denn auch ein mittels KI erzeugtes Porträt ist ein „Bildnis“ der Person, soweit sie erkennbar abgebildet ist. Wer also z.B. ein kompromittierendes Fake-Video mit dem Gesicht einer Person ohne deren Einwilligung ins Internet stellt, verwirklicht tatbestandlich § 33 KUG.³¹ Allerdings stammt das KUG aus dem Jahr 1907 und war nicht auf digital fälschbare Inhalte zugeschnitten. Zudem sind dessen Ausnahmen, z.B. für Bildnisse der Zeitgeschichte, und Begriffe nicht auf die Feinheiten von Deepfakes abgestimmt. Vor allem aber stellt § 33 KUG kein Verbrechen, sondern

²¹ Valerius, in: BeckOK-StGB, § 194 Rn. 2-3; Eisele/Schittenhelm, in: TK-StGB, § 194 Rn. 2.

²² Regge/Pegel, in: MüKo-StGB, § 185 Rn. 8-13; Matt/Renzikowski, StGB, 2. Aufl. (2020), § 185 Rn. 3.

²³ Deutscher Bundestag (Fn. 6), S. 8 Nr. 3a; Legal Tribune Online (Fn. 1).

²⁴ Graf, in: MüKo-StGB, § 201a Rn. 31; Eisele, in: TK-StGB, § 201a Rn. 8; Heuchemer, in: BeckOK-StGB, § 201a Rn. 16-24.

²⁵ Kindhäuser/Neumann/Paeffgen/Saliger, StGB, § 201a Rn. 12-14; Matt/Renzikowski, StGB, § 201a Rn. 9-10; Graf, in: MüKo-StGB, § 201a Rn. 64-68; Kindhäuser/Neumann/Paeffgen/Saliger, StGB, § 201a Rn. 41-44.

²⁶ Graf, in: MüKo-StGB, § 201a Rn. 24-26; Matt/Renzikowski, StGB, § 201a Rn. 5.

²⁷ Sittig (Fn. 16).

²⁸ Graf, in: MüKo-StGB, § 201a Rn. 72-77; Kindhäuser/Neumann/Paeffgen/Saliger, StGB § 201a Rn. 17-19; Legal Tribune Online (Fn. 1).

²⁹ Renzikowski, in: MüKo-StGB, § 184k Rn. 14-16; Sittig (Fn. 16).

³⁰ Dreier/Schulze, UrhG, 8. Aufl. (2025), § 22 KUG Rn. 1-4; Wandtke/Bullinger, UrhR, 6. Aufl. (2022), § 22 KUG Rn. 8-9.

³¹ Valerius, in: BeckOK-StGB, § 33 KUG Rn. 11-15.2; Dreier/Schulze, §§ 33-50 KUG Rn. 3-4; Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 257. Aufl. (2025), § 33 KUG Rn. 9-12; Legal Tribune Online (Fn. 1).

ein relativ mildes Vergehen dar, das in der Praxis kaum abschreckende Wirkung gegen die heutige Deepfake-Problematik entfaltet.

3. Strafvorschriften zum Schutz bestimmter Rechtsgüter

Darüber hinaus können je nach Fallgestaltung weitere Straftatbestände einschlägig sein. Werden jugendpornographische Deepfakes erstellt oder verbreitet – etwa indem das Gesicht eines Kindes in missbräuchlicher Weise in ein Pornovideo montiert wird – so greifen die strengen Strafnormen der §§ 184b, 184c StGB (Kinder- und Jugendpornografie).³² Diese erfassen ausdrücklich auch virtuelles kinderpornographisches Material, sodass KI-generierte Darstellungen Minderjähriger klar strafbar sind. Auch die Verbreitung echter pornographischer Inhalte ohne Altersbeschränkung kann nach § 184 Abs. 1 Nr. 6 StGB strafbar sein; ein Deepfake-Video mit pornographischem Inhalt öffentlich zugänglich zu machen, erfüllt daher unabhängig vom Persönlichkeitsrecht schon den Tatbestand der unzulässigen Pornografieverbreitung, sofern es ungeschützt veröffentlicht wird.³³ Allerdings dient § 184 StGB dem Jugendschutz und Sittlichkeitsschutz³⁴, nicht dem Persönlichkeitsrecht des Dargestellten – eine ahndende Würdigung aus Perspektive des Opferschutzes leistet diese Norm nur indirekt.

In Fällen, in denen Deepfakes zu Droh- oder Erpressungszwecken eingesetzt werden (z.B. Ankündigung, ein Fake-Nacktbild zu verbreiten, falls das Opfer nicht zahlt), kommen die entsprechenden Delikte – *Nötigung/Bedrohung* gem. §§ 240, 241 StGB oder *Erpressung* gem. § 253 StGB – zur Anwendung. Hier steht jedoch ebenfalls nicht die Herstellung oder Verbreitung des Deepfakes selbst unter Strafe, sondern das damit verbundene Druckmittel.³⁵

Schließlich sei auf das Datenschutzstrafrecht hingewiesen. § 42 Abs. 2 BDSG stellt u.a. die unbefugte Weitergabe *nicht allgemein zugänglicher* personenbezogener Daten unter Strafe, wenn dies in der Absicht erfolgt, einen anderen zu schädigen. Ein Personenbildnis gilt als personenbezogenes Datum.³⁶ Greift jemand beispielsweise auf private Fotos zu, z. B. durch Hacking gem. § 202a StGB, und generiert daraus ein Deepfake, um das Opfer zu bloßzustellen, könnte § 42 Abs. 2 BDSG einschlägig sein.³⁷ In der Praxis spielt diese Norm allerdings bislang kaum eine Rolle bei Deepfakes, zumal viele verwendete Ausgangsbilder – z.B. Social-Media-Profilbilder – *bereits öffentlich zugänglich* sind und damit aus dem Anwendungsbereich

des § 42 BDSG herausfallen.³⁸

4. Zwischenfazit

Der aktuelle strafrechtliche Rahmen bietet also durchaus einige Anknüpfungspunkte, um Deepfake-Missbrauch zu sanktionieren. Gerade extreme Fälle wie Kinderpornografie-Deepfakes, Erpressung mit Fake-Material oder öffentliche Pornografieverbreitung sind bereits jetzt klar strafbar. Dennoch bleibt eine Lücke, denn es fehlt ein Tatbestand, der das spezifische Unrecht der *realitätsgetreuen technischen Täuschung über die Identität einer Person* in den Blick nimmt. Bestehende Normen setzen oft an Begleitumständen an wie Beleidigungsgehalt, Intimität echter Aufnahmen oder Jugendschutz und erfassen den Kern des Deepfake-Unrechts – nämlich die täuschende Simulation einer Person und die damit verbundene Verletzung ihres personalen Selbstbestimmungsrechts – allenfalls mittelbar. Diese Feststellung hat in Politik und Rechtswissenschaft vermehrt Rufe nach einer strafrechtlichen Anpassung ausgelöst. So forderten die Justizministerkonferenzen der Länder 2021 und 2023 ein stärkeres Augenmerk auf die Gefahren von Deepfakes und regten gesetzliche Schritte an.³⁹ Auch in der Literatur wurde bereits vor einigen Jahren diskutiert, ob ein neuer Straftatbestand erforderlich sei, um der besonderen Qualität von Deepfake-Delikten gerecht zu werden.⁴⁰

IV. Der Gesetzentwurf des Bundesrates (§ 201b StGB-E)

Vor dem skizzierten Hintergrund hat der Bundesrat – auf Initiative Bayerns – im Jahr 2024 einen Gesetzentwurf für einen neuen Straftatbestand „*Verletzung von Persönlichkeitsrechten durch digitale Fälschung*“ vorgelegt.⁴¹ Ziel ist es, eine Strafbarkeitslücke zu schließen und Opfern von Deepfake-Angriffen einen direkteren Schutz an die Hand zu geben, als dies über die bisherigen Delikte möglich ist. Der vom Bundesrat in seiner 1056. Sitzung am 11. Juli 2025 beschlossene Entwurf eines Gesetzes zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes wurde von der Bundesregierung am 27. August 2025 dem Bundestag übersandt.⁴² Der Entwurf sieht hierzu die Einfügung von § 201b ins Strafgesetzbuch vor, in Anknüpfung an die bestehenden §§ 201, 201a StGB (Geheimnis- und Privatsphärenschutz). Im Folgenden werden die wesentlichen Inhalte des vorgeschlagenen § 201b StGB-E dargestellt.

³² Schmidt, in: MüKo-StGB, § 184b Rn. 29-31; Ziegler, in: BeckOK-StGB, § 184b Rn. 10-11; Kindhäuser/Neumann/Paeffgen/Saliger, StGB, § 184b Rn. 24, § 184c Rn. 11-15, § 184c Rn. 1-3.

³³ Schmidt, in: MüKo-StGB, § 184 Rn. 67-71; Ziegler, in: BeckOK-StGB, § 184 Rn. 19-20; Eisele, in: TK-StGB, § 184 Rn. 51-53; Legal Tribune Online (Fn. 1).

³⁴ Liesching, in: BeckOK-JugendschutzR, 5. Ed. (Stad: 1.6.2025), § 184 StGB Rn. 1-2; Matt/Renzikowski, StGB, § 184 Rn. 2.

³⁵ Matt/Renzikowski, StGB, § 240 Rn. 39-40; Valerius, in: BeckOK-StGB, § 241 Rn. 3-8; Sinn, in: MüKo-StGB, § 241 Rn. 5-8; Kindhäuser/Neumann/Paeffgen/Saliger, StGB, § 253 Rn. 5; Dölling/Duttge/König/Rössner, StGB, § 253 Rn. 8-9.

³⁶ Ehmann/Selmayr, DS-GVO, 3. Aufl. (2024), Art. 4 Rn. 7-21; Paal/Pauß, DS-GVO BDSG, 3. Aufl. (2021), Art. 4 Rn. 3.

³⁷ Gola/Heckmann, DS-GVO BDSG, 3. Aufl. (2022), § 42 Rn. 18-27; Brodowski, in: BeckOK-DatenschutzR, 52. Aufl. (2025), § 42 BDSG Rn. 22-44; Simitis/Hornung/Spiecker (Hrsg.), Datenschutzrecht, 2. Aufl. (2025), Rn. 16-20; Legal Tribune Online (Fn. 1).

³⁸ Kühling/Buchner, DS-GVO BDSG, 4. Aufl. (2024), § 42 Rn. 8; Heghmanns, in: Sydow/Marsch, DS-GVO/BDSG, 3. Aufl. (2022), § 42 Rn. 8.

³⁹ Deutscher Bundestag (Fn. 6), S. 3; Beck-aktuell (Fn. 4).

⁴⁰ Deiß, Deepfakes und Porno-Deepfakes, online abrufbar unter: <http://bit.ly/4nQtXl0> (zuletzt abgerufen am 15.9.2025); djB, Bekämpfung bildbasierter sexualisierter Gewalt, online abrufbar unter: <http://bit.ly/4qbCWyL> (zuletzt abgerufen am 15.9.2025); Sittig (Fn. 16).

⁴¹ Deutscher Bundestag (Fn. 6), Anlage 1; KriPoZ-RR 17/2024; Schilling (Fn. 6).

⁴² BT-Drs. 21/1383; Deutscher Bundestag (Fn. 6).

1. Tathandlung und Grundtatbestand

Nach dem Entwurf macht sich strafbar, wer das Persönlichkeitsrecht einer anderen Person verletzt, indem er *einen mit computertechnischen Mitteln hergestellten oder veränderten Medieninhalt*, der den Anschein einer wirklichkeitsgetreuen Bild- oder Tonaufnahme des äußeren Erscheinungsbildes, des Verhaltens oder mündlicher Äußerungen dieser Person erweckt, *einer dritten Person zugänglich macht*.⁴³ Damit würden Fälle erfasst, in denen jemand ein täuschend echtes KI-Bild oder -Video von einer Person weitergibt, sei es durch Upload ins Internet, Versenden an einzelne Personen oder Vorführen in einer Gruppe, und dadurch das allgemeine Persönlichkeitsrecht der dargestellten Person verletzt wird. Der Strafraum für diese Grundform ist Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe. Bemerkenswert ist, dass neben lebenden Personen ausdrücklich auch Verstorbene vom Schutzbereich erfasst werden. Bezieht sich die Tat auf eine verstorbene Person und wird deren Persönlichkeitsrecht *schwerwiegend* verletzt, so gilt dieselbe Strafordrohung.⁴⁴ Damit reagiert der Entwurf auf Fälle, in denen z.B. das Andenken einer Toten durch ein obszönes oder rufschädigendes Deepfake-Video grob entstellt wird – ein Bereich, der vom geltenden § 189 StGB („Verunglimpfung des Andenkens Verstorbener“) nur begrenzt abgedeckt ist.

Der Tatbestand knüpft zentral an das Kriterium der Persönlichkeitsrechtsverletzung an. Das allgemeine Persönlichkeitsrecht fungiert hier als geschütztes Rechtsgut. Durch die Formulierung „wer das Persönlichkeitsrecht einer anderen Person verletzt, indem...“ wird ein Verletzungserfolg vorausgesetzt – es muss also tatsächlich eine Verletzung des Persönlichkeitsrechts eintreten, nicht nur eine abstrakte Gefährdung. Dieser Erfolgsbezug ist ein Unterschied zu einigen Ehrschutzdelikten wie § 187 StGB, die bereits die Eignung zur Rufschädigung genügen lassen.⁴⁵ Zugleich hat diese Konstruktion Kritik hervorgeufen (dazu unten V.1), da das Persönlichkeitsrecht ein weit offener Begriff ist.

2. Qualifikationen

In § 201b Abs. 2 StGB-E werden erschwerende Umstände definiert, die eine höhere Strafe ermöglichen. Zum einen soll eine Tat mit bis zu fünf Jahren Freiheitsstrafe bedroht sein, wenn der Täter den fraglichen Deepfake-Inhalt *der Öffentlichkeit zugänglich macht oder einen Medieninhalt zugänglich macht, der einen Vorgang des höchstpersönlichen Lebensbereichs zum Gegenstand hat*.⁴⁶ Darunter fällt insbesondere das Hochladen in frei zugängliche Internetplattformen oder das Verbreiten in sozialen Netzwerken,

wodurch potenziell eine unbegrenzte Personenzahl Zugang erhält. Dies trägt dem erhöhten Unrecht Rechnung, das in der breiten Streuung einer Persönlichkeitsrechtsverletzung liegt – die Rufschädigung und Prangerwirkung potenzieren sich, je größer das Publikum ist. Zum anderen erhöht sich der Strafraum ebenfalls auf bis zu fünf Jahre, wenn der verbreitete Inhalt *einen Vorgang des höchstpersönlichen Lebensbereichs* zum Gegenstand hat.⁴⁷ Damit soll klargestellt werden, dass insbesondere intime Deepfakes wie z.B. sexualisierte Darstellungen als schwerwiegende Fälle gelten. Diese zweite Qualifikation stellt eine Parallele zum Schutzzweck des § 201a StGB her, der ja ebenfalls den höchstpersönlichen Lebensbereich fokussiert. Beispielsweise wäre die Verbreitung eines Deepfake-Sexvideos, das eine Person in einer vermeintlich privaten sexuellen Handlung zeigt, ein Fall des § 201b Abs. 2 StGB-E.⁴⁸

3. Ausnahmeregelung

Um eine Überkriminalisierung zu vermeiden und verfassungsrechtlich geschützte Interessen wie Kunstfreiheit, Wissenschaftsfreiheit und Pressefreiheit zu wahren, enthält der Entwurf in § 201b Abs. 3 StGB-E einen ausdrücklichen Ausnahmeverbehalt.⁴⁹ Danach ist der Tatbestand *nicht erfüllt*, wenn die Handlung in Wahrnehmung *überwiegender berechtigter Interessen* erfolgt – namentlich genannt werden die Bereiche Kunst, Wissenschaft, Forschung, Lehre sowie die Berichterstattung über Zeitgeschehen oder Geschichte. Gedacht ist hierbei an Konstellationen, in denen Deepfake-Technik in *sozialadäquater* Weise eingesetzt wird, ohne die Rechte eines Einzelnen zu verletzen. Beispielhaft erwähnt werden in der Begründung satirische oder künstlerische Verfremdungen, die deutlich als solche erkennbar sind.⁵⁰ Ebenso könnte man an den Einsatz von Deepfakes in der Filmindustrie wie das digitale „Verjüngen“ eines Schauspielers oder an wissenschaftliche Experimente denken. Wichtig ist, dass die Interessenabwägung im Einzelfall entscheidet, denn nur wenn das berechnete Interesse *überwiegt* und kein unverhältnismäßiger Eingriff in das Persönlichkeitsrecht vorliegt, greift die Ausnahme. Damit enthält der Entwurf eine *Art geschriebenen Rechtfertigungsgrund*, der verhindern soll, dass z.B. investigative Journalisten oder Satiriker kriminalisiert werden, solange ihr Tun nicht in eine echte Persönlichkeitsverletzung umschlägt.

4. Beschlagnahme und Einziehung

Schließlich sieht § 201b Abs. 4 StGB-E vor, dass die Tatmittel, insbesondere die betreffenden Bild- oder Tonträger, Dateien etc., eingezogen werden können; § 74a StGB

⁴³ BT-Drs. 20/12605, Entwurf eines Gesetzes zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes, online abrufbar unter: <http://bit.ly/47jMyQg> (zuletzt abgerufen 15.9.2025).

⁴⁴ BT-Drs. 21/1383, Anlage 1, § 201b StGB-E; KriPoZ-RR 17/2024.

⁴⁵ Regge/Pegel, in: MüKo-StGB (Fn. 15), § 187 Rn. 6; Kindhäuser/Neumann/Paeffgen/Saliger, § 187 Rn. 3; Deutscher Bundestag (Fn. 6); Scherer, Deepfake: wenn Manipulation straflos bleibt, online abrufbar unter: <http://bit.ly/4n4ABTn> (zuletzt abgerufen am 15.9.2025).

⁴⁶ Vassilaki (Fn. 3); Deutscher Bundestag (Fn. 9); Deutscher Bundestag (Fn. 43); Scherer (Fn. 45).

⁴⁷ Vassilaki (Fn. 3); Deutscher Bundestag (Fn. 9); Deutscher Bundestag (Fn. 43).

⁴⁸ Deutscher Bundestag (Fn. 43).

⁴⁹ Deutscher Bundestag (Fn. 43).

⁵⁰ BT-Drs. 21/1383, Anlage 2, zu § 201b Abs. 3, S. 17; Legal Tribune Online (Fn. 1); Deutscher Bundestag (Fn. 43).

(erweiterte Einziehung) soll anwendbar sein.⁵¹ Dies entspricht der üblichen Regelung bei Delikten, in denen bestimmte Medieninhalte verbreitet werden (z.B. § 201a Abs. 4 StGB enthält eine ähnliche Klausel).⁵² Dadurch soll erreicht werden, dass rechtswidrige Deepfake-Dateien aus dem Verkehr gezogen und nicht weiter verbreitet werden können.

5. Begründung des Entwurfs

In der offiziellen Gesetzesbegründung zum Bundesratsentwurf werden die Motive und Ziele ausführlich dargelegt. Hervorgehoben wird zunächst die *erhebliche Gefahr* von KI-Manipulationen für individuelle Persönlichkeitsrechte, Vermögenswerte und sogar den demokratischen Willensbildungsprozess. Deepfakes werden als eine besonders gefährliche Form der Informationsmanipulation bezeichnet, die Straftäter zunehmend missbräuchlich einsetzen.⁵³ Typische Tätermotive seien Rache oder der Wille, Macht über das Opfer auszuüben; im politischen Bereich gehe es um effektive Diskreditierung von Personen im Meinungswettstreit. Zwar könnten einzelne Deepfake-Fälle durch bestehende Strafvorschriften in *Teilaspekten* erfasst werden, doch werde der eigentliche Unrechtskern – das simulierte Erzeugen einer falschen „Realität“ um eine Person – nicht abgebildet. Die Begründung formuliert pointiert das berechnete Interesse jeder Person, „ohne ihre Zustimmung nicht in eine künstlich erzeugte, aber scheinbar authentische ‘Wirklichkeit’ hineingestellt zu werden mit Äußerungen, die sie selbst nicht getätigt hat, oder mit Handlungen, die sie selbst nicht vorgenommen hat“. Durch Deepfakes verliere der Betroffene die Selbstbestimmung und Kontrolle über das eigene Auftreten nach außen; identitätsprägende Merkmale würden verfälscht oder in falschen Kontext gerückt. Angesichts dieser schwerwiegenden Auswirkungen genüge eine bloße Kennzeichnungspflicht für Deepfakes nicht, so der Gesetzgeber – es bedürfe vielmehr einer Strafandrohung, um effektiv abzuschrecken und das Rechtsgut zu schützen.⁵⁴

Weiter wird begründet, warum die genannten Ausnahmen wie Kunst, Berichterstattung etc., aufgenommen wurden. Man wolle sicherstellen, dass sozialadäquate oder grundrechtlich gedeckte Anwendungen der Technik nicht erfasst werden.⁵⁵ Gleichzeitig – so die Begründung – seien gewisse Grenzen der Ausnahme zu beachten. Handlungen, die zwar unter Kunst- oder Pressefreiheit fallen, aber gleichwohl Persönlichkeitsrechte verletzen, sollen nicht privilegiert werden. Diese Abwägung wird jedoch im Gesetzentwurf selbst durch die Generalklausel „Wahrnehmung berechtigter Interessen“ den Gerichten überlassen.

Der Bundesrat begründete die Notwendigkeit der Neuregelung auch mit dem Hinweis, dass § 201a StGB reale Bildaufnahmen voraussetzt und daher *generierte* Bilder nicht erfasst – eine Lücke, die es zu schließen gelte. Ebenso wenig sei eine täuschend echte KI-Stimme von § 201 StGB (Verletzung der Vertraulichkeit des Wortes) erfasst, da dort eine tatsächliche Äußerung der Person Voraussetzung ist.⁵⁶ Schließlich verweist der Entwurf auf den erheblichen Anteil pornographischer Deepfakes und die besondere Betroffenheit von Frauen, was ein entschlossenes strafrechtliches Einschreiten erfordere.⁵⁷

Der Gesetzentwurf wurde am 11. Juli 2024 vom Bundesrat beschlossen und am 27.8.2025 in den Deutschen Bundestag eingebracht.⁵⁸ Damit war der erste Schritt zu einer gesetzlichen Regelung getan. Im Folgenden ist jedoch zu betrachten, welche Resonanz und Kritik dieser Vorschlag erfahren hat – sowohl seitens der damaligen Bundesregierung als auch aus juristischer Fachsicht.

V. Diskussion: Notwendigkeit, Kritikpunkte und Alternativvorschläge

Die Einführung eines Straftatbestandes für Deepfakes wird kontrovers diskutiert. Einerseits wird die Schaffung einer spezialpräventiven Norm als geboten angesehen, um die erkannte Schutzlücke zu schließen und dem Unrechtsgehalt von Deepfake-Taten gerecht zu werden. Andererseits warnen Kritiker vor möglichen Übermaß- und Bestimmtheitsproblemen der vorgeschlagenen Regelung und halten das bestehende Instrumentarium für im Wesentlichen ausreichend. Im Folgenden werden die wichtigsten Pro- und Contra-Argumente sowie ein alternativer Reformvorschlag der Bundesrechtsanwaltskammer dargestellt.

1. Argumente für den neuen Straftatbestand

Befürworter – zu denen insbesondere die Initiatoren des Entwurfs aus den Ländern zählen – betonen die besondere Gefährlichkeit von Deepfakes und den bisherigen unzureichenden Schutz der Opfer. Exemplarisch heißt es aus der Staatsregierung Bayern: Obwohl es zahlreiche strafrechtliche Regelungen gebe, erfassten diese „jedoch nur Teilaspekte und werden dem besonderen Unrechtsgehalt der Taten nicht gerecht“. Der *technische Täuschungsaspekt* führe zu einer neuen Qualität der Verletzung, die eine eigenständige Strafnorm verlange. Dabei wird auch auf die stark gestiegene Zahl von Vorfällen verwiesen, eine Entwicklung, die sich statistisch zwar mangels spezieller Erfassung schwer belegen lässt, die aber durch vermehrte Medienberichte über Deepfake-Skandale untermauert wird. Insbesondere die Zunahme pornographischer

⁵¹ BT-Drs. 21/1383, Anlage 2, zu § 201b Abs. 4, S. 18; Deutscher Bund (Fn. 43); BRAK, Stellungnahme Nr. 75/2024, online abrufbar unter: <http://bit.ly/3L4DMNp> (zuletzt abgerufen am 15.9.2025).

⁵² Heuchemer, in: BeckOK-StGB, § 74a Rn. 1-4; Heuchemer, in: BeckOK-StGB, § 201a Rn. 1-6.

⁵³ Deutscher Bundestag (Fn. 43); Deutscher Bundestag (Fn. 6); Kraetzig, Computer und Recht 2024, S. (207) 211; Vassilaki, Computer und Recht 2024, S. (701) 704; Karaboga, in: Jaki/Steiger (Hrsg.), Interdisziplinäre Perspektiven auf Erkennung, Beschreibung und Regulation, 2023, S. 197-199.

⁵⁴ BT-Drs. 21/1383, Allgemeiner Teil, I Nr. 1; KriPoZ-RR 17/2024.

⁵⁵ BT-Drs. 21/1383, Allgemeiner Teil, I Nr. 4; Legal Tribune Online (Fn. 1).

⁵⁶ BT-Drs. 21/1383, Allgemeiner Teil, I Nr. 3a; Legal Tribune Online (Fn. 1); Deutscher Bundestag (Fn. 43).

⁵⁷ BT-Drs. 21/1383, Allgemeiner Teil, I Nr. 2c; Beck-aktuell (Fn. 4); Deutscher Bundestag (Fn. 43).

⁵⁸ BT-Drs. 21/1383; Deutscher Bundestag (Fn. 6); KriPoZ-RR 17/2024.

Deepfakes zu Lasten von Frauen und teils Minderjährigen wird als alarmierend dargestellt.⁵⁹ Hier zeige sich, dass Täter mit relativ geringem Aufwand massiven Schaden anrichten könnten, während Opfer mangels klarer Rechtsgrundlage oft *rechtlich kaum Möglichkeiten* sehen, sich zu wehren.⁶⁰ Die Einführung von § 201b StGB soll daher eine Schutzlücke schließen und zugleich eine *abschreckende Wirkung* entfalten. Der Normerlass hätte auch symbolischen Charakter, da er signalisiert, dass der Staat die Persönlichkeitsrechte im digitalen Raum ernst nimmt und neuen Formen digitaler Gewalt entschlossen entgegentritt.

Darüber hinaus wird darauf hingewiesen, dass das Fehlen einer passenden Strafnorm auch Strafbarkeitslücken erzeugt, wo bestehende Tatbestände an Voraussetzungen anknüpfen, die Deepfake-Fälle gerade nicht erfüllen. So bleibt etwa das *postmortale Persönlichkeitsrecht* nach geltendem Recht strafrechtlich weitgehend schutzlos, sofern nicht eine Verunglimpfung (§ 189 StGB) nachweisbar ist – § 201b StGB-E würde hier Abhilfe schaffen, indem schon die schwere Verletzung des Andenkens einer verstorbenen Person durch eine digitale Fälschung erfasst wäre.⁶¹ Ebenso klappt eine Lücke bei täuschenden *Fake-Audioaufnahmen*, da eine gefälschte Sprachnachricht mit beleidigendem Inhalt mangels tatsächlicher Äußerung weder nach § 201 StGB (Verletzung der Vertraulichkeit des Wortes) noch sicher nach § 185 StGB (Beleidigung) geahndet werden könnte.⁶² Solche Konstellationen würden künftig vom neuen Tatbestand abgedeckt.

Befürworter verweisen auch auf die präventive Funktion des Strafrechts. Die Drohung mit Strafe könne zumindest einen Teil potenzieller Täter abschrecken, KI-Technologie für Persönlichkeitsrechtsverletzungen zu missbrauchen. Gerade weil Deepfake-Software immer zugänglicher wird, sei es wichtig, frühzeitig klare Grenzen aufzuzeigen. Schließlich wird argumentiert, die vorgeschlagene Norm sei verhältnismäßig und ausreichend bestimmt formuliert, um nur das wirklich sozialschädliche Verhalten zu erfassen. Die Ausnahmeklausel in Abs. 3 stelle sicher, dass legitime Anwendungsfälle wie Satire, Kunst etc. ausgespart blieben, so dass eine Kriminalisierung von sozialadäquatem Verhalten nicht zu befürchten sei.⁶³ Insgesamt, so die Befürworter, schaffe § 201b StGB ein passgenaues Werkzeug, wo bislang nur *Umwege* über weniger einschlägige Tatbestände möglich waren.

2. Einwände der damaligen Bundesregierung

Der in seiner 1046. Sitzung des Bundesrats am 5. Juli beschlossene Entwurf eines Gesetzes zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes wurde am 21. August 2024 dem Bundestag übersandt⁶⁴, in der

20. Legislaturperiode aber nicht mehr beschlossen. Die damalige Bundesregierung stand der Neuregelung skeptisch gegenüber und hat im Gesetzgebungsverfahren eine ablehnende Stellungnahme abgegeben.⁶⁵ Zunächst wurde betont, dass nach ihrer Auffassung bereits „bestehende Gesetze ausreichende Strafmöglichkeiten“ bieten. In der Stellungnahme der Bundesregierung zum Bundesratsentwurf wurden exemplarisch jene Normen aufgezählt, die auch oben in Teil III beschrieben wurden: So seien kinder- und jugendpornografische Deepfakes durch §§ 184b, 184c StGB abgedeckt; die Verbreitung pornographischer Inhalte sei (unabhängig von Deepfakes) durch § 184 StGB unter Strafe, und für ehrverletzende Deepfakes käme eine Strafbarkeit als Verleumdung (§ 187 StGB) in Betracht. Außerdem wird auf § 33 KUG hingewiesen, der das unbefugte Verbreiten von Bildnissen pönalisiert, sowie auf etwaige Eingriffsmöglichkeiten des Urheberrechts (§§ 106, 108 UrhG), falls urheberrechtlich geschützte Ausgangsfotografien verwendet wurden. Auch § 42 Abs. 2 BDSG (Datenschutzstrafrecht) könne im Einzelfall erfüllt sein.⁶⁶ Nach Ansicht der damaligen Bundesregierung ergab sich daraus ein ausreichendes Netz an Sanktionsmöglichkeiten, ohne dass es eines neuen Straftatbestands bedarf.

Noch gewichtiger sind die verfassungsrechtlichen Bedenken, welche die Regierung vorbrachte. Sie monierte insbesondere die Unbestimmtheit der Formulierung „Wer das Persönlichkeitsrecht einer anderen Person verletzt...“.⁶⁷ Das allgemeine Persönlichkeitsrecht sei ein weit gefasstes, offenes Rechtsgut, das in dieser Allgemeinheit bislang nicht als Tatbestandsmerkmal in einem Strafgesetz verwendet wurde. Art. 103 Abs. 2 GG verlange jedoch ausreichende Bestimmtheit und Vorhersehbarkeit von Strafnormen. Es wird die Frage aufgeworfen, ob das Kriterium der Persönlichkeitsrechtsverletzung hinreichend klar umrissen werden könne, um als Grundlage für eine Strafverfolgung zu dienen. Zweifel ergeben sich z.B. daraus, dass die Schwelle zur „Verletzung“ des Persönlichkeitsrechts nicht näher definiert ist – handelt es sich um jede nicht unerhebliche Beeinträchtigung? Muss eine Ehrkränkung oder eine Rufschädigung eingetreten sein? Gerade weil das Persönlichkeitsrecht in verschiedenen Ausprägungen (Ehre, Privatheit, Selbstdarstellung etc.) geschützt wird, könnten Auslegungsschwierigkeiten entstehen. Hier sah die Bundesregierung ein erhebliches Bestimmtheitsrisiko, das die Norm im Extremfall verfassungswidrig machen könnte.⁶⁸

Darüber hinaus verwies die Regierung darauf, dass § 201b StGB-E in mancher Hinsicht sogar *enger* gefasst sei als bestehende Tatbestände und dadurch paradoxerweise weniger Schutz bieten könnte. So wurde angemerkt, § 201b setze einen tatsächlichen Verletzungserfolg voraus, wo

⁵⁹ BT-Drs. 21/1383, Allgemeiner Teil, S. 6; Beck-aktuell (Fn. 4).

⁶⁰ Deutscher Bundestag (Fn. 6), Besonderer Teil, zu § 201b Abs. 2; BT-Drs. 21/1383, Besonderer Teil zu § 201b Abs. 2.

⁶¹ BT-Drs. 21/1383, § 201b Abs. 1 S. 2 StGB-E; KriPoZ-RR 17/2024.

⁶² Kindhäuser/Neumann/Paeffgen/Saliger, StGB, § 201 Rn. 5; Heuchemer, in: BeckOK-StGB, § 201 Rn. 3; Legal Tribune Online (Fn. 1).

⁶³ BT-Drs. 21/1383, Allgemeiner Teil I. Nr. 4; Legal Tribune Online (Fn. 1).

⁶⁴ Deutscher Bundestag (Fn. 43).

⁶⁵ Deutscher Bundestag (Fn. 43), Anlage 2.

⁶⁶ Deutscher Bundestag (Fn. 43), Anlage 2; Legal Tribune Online (Fn. 1).

⁶⁷ Deutscher Bundestag (Fn. 43), Anlage 2; Legal Tribune Online (Fn. 1).

⁶⁸ Deutscher Bundestag (Fn. 6).

z.B. § 187 StGB bereits die abstrakte Eignung zur Rufschädigung ausreichen lässt.⁶⁹ Es könne schwieriger sein, in der Praxis eine konkrete Persönlichkeitsrechtsverletzung nachzuweisen, etwa psychische Folgen beim Opfer, als die objektive Ehrkränkung durch eine falsche Tatsache. In diesem Sinne könne der Entwurf hinter dem Schutzniveau bestehender Normen zurückbleiben. Die Bundesregierung sah daher keinen überzeugenden Mehrwert in der neuen Vorschrift.

Politisch ist hervorzuheben, dass die ablehnende Haltung der damaligen Bundesregierung im Kontext einer differierenden rechtspolitischen Einschätzung stand. Während einige Bundesländer (insbes. Bayern) starken Handlungsbedarf sehen, verfolgte die damalige Bundesregierung einen zurückhaltenderen Ansatz im Bereich Cybercrime und digitale Gewalt, setzte eher auf punktuelle Anpassungen und effektive Anwendung geltenden Rechts. Gleichwohl war sie durch die Bundesratsinitiative gezwungen, sich mit dem Thema auseinanderzusetzen.

In der Stellungnahme der Bundesregierung, die den Gesetzentwurf des Bundesrats am 29.08.2025 dem Bundestag zur Vorlage gebracht hat, wird auf die o. g. Einwände der damaligen Bundesregierung nicht eingegangen und darauf hingewiesen, dass die Bundesregierung die geschilderten Phänomene sehr ernst nimmt und die Vereinbarung im Koalitionsvertrag für die 21. Legislaturperiode genannt, wonach Strafbarkeitslücken bei bildbasierter sexualisierter Gewalt geschlossen werden sollen. Der Gesetzestext an sich wurde gegenüber der Vorlage vom 21. August 2024 nicht verändert.

3. Stellungnahme der BRAK

Eine wichtige Stimme in der Fachdiskussion ist die BRAK, die im Oktober 2024 eine ausführliche Stellungnahme (Nr. 75/2024) zum Gesetzentwurf veröffentlicht hat. Darin unterstützt die BRAK zwar grundsätzlich die Idee, Deepfake-Missbrauch strafrechtlich zu sanktionieren, übt jedoch Kritik an der Ausgestaltung des Entwurfs und schlägt einen alternativen Lösungsweg vor.⁷⁰

Die BRAK moniert zunächst – in ähnlicher Linie wie die Bundesregierung – die unscharfe Bestimmung des geschützten Rechtsguts. Der Verweis auf das Persönlichkeitsrecht allein sei „zu schwammig formuliert“ und es fehle an der nötigen Präzision.⁷¹ Insbesondere bestehe die Gefahr, dass der geplante § 201b StGB sehr weit greift und theoretisch *jede Verwendung von KI-generierten Bildnissen* unter Strafe stellen könnte, wenn man das Persönlichkeitsrecht großzügig auslegt. Die BRAK führt aus, der Gesetzeswortlaut würde *jegliches Zugänglichmachen an Dritte oder die Öffentlichkeit* bei Vorliegen einer Persönlichkeitsbeeinträchtigung strafbar machen; damit sei unklar, wie z.B. das Teilen eines Deepfake durch einen unwissenden Nutzer zu beurteilen ist, der den Fake für echt hält oder dessen Rechtswidrigkeit nicht erkennt.⁷² Hier würde man u.U. selbst gutgläubige Weiterverbreiter

kriminalisieren. Zwar setzt Strafbarkeit Vorsatz voraus, doch könnten Laien die „Unwahrheit“ eines sehr gut gemachten Deepfakes nicht immer sicher erkennen. Insgesamt, so die BRAK, bedarf die Norm einer klareren Eingrenzung, um nicht über ihr Ziel hinauszuschießen.

Ein weiterer zentraler Kritikpunkt der BRAK betrifft die Ausnahmeregelung in Abs. 3 des Entwurfs. Diese sei in der geplanten Form „zu weitgehend“ und rechtssystematisch problematisch. Die BRAK gibt zu bedenken, dass weder Meinungs- und Pressefreiheit noch Wissenschafts- und Kunstfreiheit einen Freibrief dafür bieten dürften, *unwahre Tatsachenbehauptungen* zu verbreiten – auch nicht in Form schwer erkennbarer Deepfakes. Die vorgeschlagene Ausnahmeformulierung könnte aber genau dies erlauben, sofern sich der Täter auf einen dieser Bereiche beruft. Die Kammer argumentiert, der verfassungsrechtliche Schutz von Satire und Kunst ende dort, wo der durchschnittliche Rezipient eine Darstellung nicht mehr als Satire, sondern als bare Münze auffasse. Wenn also ein vermeintlich satirisches Deepfake-Video von vielen für echt gehalten wird, liege gerade kein schützenswerter Kern mehr vor, sondern eine gefährliche Desinformation. Auch stellt die BRAK infrage, wie das absichtliche Verbreiten falscher Medieninhalte jemals der seriösen Zeitgeschehen-Berichterstattung oder Geschichtsschreibung dienen könne.⁷³ Durch die so weit formulierten Ausnahmen läuft man nach Meinung der BRAK, Gefahr, die Norm *praktisch zu entkernen*, weil sich potenzielle Täter auf Kunst oder Journalismus berufen könnten, um tiefgreifende Persönlichkeitsverletzungen zu rechtfertigen. Hier plädiert die BRAK für eine enger gefasste oder alternative Lösung.

Als solchen alternativen Ansatz schlägt die BRAK vor, anstatt eines völlig neuen § 201b eine Ergänzung des geltenden § 201a StGB vorzunehmen. Dies sei eine „minimalinvasive“ Lösung, welche die vorhandene Struktur nutzt und nur gezielt erweitert. Konkret regt die BRAK an, in § 201a Abs. 2 StGB zwei neue Nummern aufzunehmen, die das unbefugte Verbreiten von ehrschädigenden Bildern und Deepfake-Inhalten erfassen. So solle § 201a Abs. 2 Nr. 1 n.F. jede unbefugte Verbreitung von Bildaufnahmen unter Strafe stellen, die *geeignet ist, dem Ansehen der abgebildeten Person erheblich zu schaden*. Unmittelbar danach – in Nr. 2 – würde das Verbreiten von KI-manipulierten Inhalten (wie in § 201b Abs. 1 beschrieben) erfasst, *sofern diese geeignet sind, dem Ansehen der Person erheblich zu schaden*. Durch die Formulierung „geeignet, erheblich zu schaden“ baut die BRAK also eine Relevanzschwelle ein: Es soll nur strafbar sein, wenn der Deepfake wirklich gravierende Auswirkungen auf das Opfer haben kann (beispielsweise erhebliche Rufschädigung). Triviale oder augenzwinkernde Fälschungen fielen damit heraus. Zugleich würde damit – im Gegensatz zum Entwurf – nicht irgendeine Persönlichkeitsrechtsbeeinträchtigung genügen, sondern konkret eine *erhebliche Ansehensschädigung* erforderlich sein, was dem Bestimmtheitsgebot

⁶⁹ Deutscher Bundestag (Fn. 6).

⁷⁰ BRAK (Fn. 51); Legal Tribune Online (Fn. 1).

⁷¹ BRAK (Fn. 51), zu § 201b Abs. 1; Legal Tribune Online (Fn. 1).

⁷² BRAK (Fn. 51).

⁷³ Legal Tribune Online (Fn. 1).

cher Genüge tun soll. Auch die kritisierte Inhaltsunklarheit („Inhalt“) würde präzisiert, da klar ein reputationsrelevanter Inhalt vorliegen muss.⁷⁴ Im Übrigen schlägt die BRAK vor, die Ausnahmegvorschrift, vergleichbar Abs. 3 des Entwurfs, in angepasster Form ebenfalls zu übernehmen⁷⁵, um Kunst etc. nicht übermäßig zu beschränken. Insgesamt, so die BRAK, lasse sich mit dieser Modifikation ein gezielter Schutz vor Deepfake-Verbreitung erreichen, ohne einen komplett neuen Paragraphen schaffen zu müssen. Gleichzeitig würden die in der Stellungnahme aufgezeigten Probleme (Schwammigkeit, zu weite Ausnahmen) entschärft.⁷⁶ Aus Sicht der BRAK wäre ein solches Vorgehen „minimalinvasiv“ und kompatibel mit den europarechtlichen Vorgaben, die demnächst auf die Mitgliedstaaten zukommen.⁷⁷

Die BRAK-Stellungnahme hat auch in der weiteren Fachöffentlichkeit Diskussionen hervorgerufen. So wurde beispielsweise von Praktikern angemerkt, der BRAK-Vorschlag gehe immer noch zu weit. Es sei ein zusätzliches Eingrenzungsmerkmal nötig, etwa dass die Verbreitung „in der Absicht zu schädigen, zu diffamieren oder politisch zu beeinflussen“ erfolgt oder einen sexualisierten Kontext hat. Andernfalls bestehe weiterhin die Gefahr, „alles Unnötige zu pönalisieren, was unter künstlich generierte Bildnisse fällt“, wie ein IT-Fachanwalt warnte. In drastischen Worten wurde gar von einem möglichen „Tod von Bild-KI in Deutschland“ gesprochen, sollte die Gesetzgebung überziehen.⁷⁸ Diese Stimmen fordern also eine noch engere Fassung, um den Einsatz von KI in Kunst und Kreativität nicht durch allzu strenge Strafanordnungen abzuwürgen. Andererseits betonen Befürworter der Strafbarkeit, dass man dringend effektive Mittel brauche, um *Opfer zu schützen* – und dass man die Abgrenzung zulässiger Parodien von unzulässigen Fälschungen der Rechtsprechung zutrauen könne.

Zusammenfassend lässt sich festhalten, dass die Debatte weniger um das Ob einer Regulierung als um das Wie geht. Einigkeit besteht weitgehend darin, dass nicht-einvernehmliche, persönlichkeitsverletzende Deepfakes ein reales Problem darstellen, dem man begegnen muss. Strittig ist jedoch, ob der Bundesratsentwurf in seiner aktuellen Fassung dafür das richtige Mittel ist, oder ob nachjustiert werden sollte (sei es in Form der BRAK-Anregungen oder durch andere Modifikationen). Dabei spielen sowohl rechtstechnische Überlegungen (Bestimmtheit, Systematik) als auch grundrechtliche Abwägungen (Schutz der Meinungs-/Kunstfreiheit vs. Persönlichkeitsrecht) eine

Rolle.

4. Europäischer und internationaler Kontext

Die Diskussion um Deepfakes beschränkt sich nicht auf Deutschland. Auch auf EU-Ebene und in anderen Staaten wird nach Lösungen gesucht. Die Europäische Union hat jüngst mit der Richtlinie zur *Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt*⁷⁹ erstmals explizite Vorgaben zum Umgang mit bildbasierter digitaler Gewalt gemacht, wonach die Mitgliedstaaten die Rechts- und Verwaltungsvorschriften in Kraft setzen, die erforderlich sind, um dieser Richtlinie bis zum 14. Juni 2027 nachzukommen.⁸⁰ In Art. 7 dieser Richtlinie wird die *nicht einvernehmliche Herstellung oder Weitergabe von intimen Bildern oder manipuliertem Material* unter Strafe gestellt.⁸¹ Darunter fallen auch sexualisierte Deepfakes. Die Richtlinie, die im Juni 2024 politisch verabschiedet wurde, verpflichtet die Mitgliedstaaten, entsprechende Straftatbestände in nationales Recht zu überführen. Deutschland wird diese EU-Vorgabe mit dem am 27. August 2025 dem Bundestag zur Entscheidung vorgelegten Gesetzesentwurf zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes voraussichtlich umsetzen.⁸² Der Bundesratsentwurf antizipiert diese Entwicklung gewissermaßen, wobei dessen Anwendungsbereich (auch nicht-sexuelle Deepfakes, z.B. politische) sogar über die Mindestanforderungen der EU hinausgeht.

In anderen Ländern existieren bereits spezielle Gesetze gegen Deepfakes, vor allem im Bereich Nicht-einvernehmliche Pornografie. Mehrere Bundesstaaten der USA haben Gesetze erlassen, die die Erstellung oder Verbreitung von sog. *deepfake porn* unter Strafe stellen, z.T. eingebettet in die Revenge-Porn-Gesetzgebung.⁸³ Auch Südkorea und einige australische Bundesstaaten haben vergleichbare Straftatbestände geschaffen.⁸⁴ In Großbritannien wird das Problem im Rahmen eines geplanten Gesetzes gegen Cyberflashing und Intimbildmissbrauch aufgegriffen.⁸⁵ Diese internationalen Entwicklungen zeigen einen Trend zur strafrechtlichen Sanktionierung von Deepfake-Missbrauch, wobei der Fokus meist auf eindeutig schädlichen Formen, insb. sexuelle Bloßstellung, liegt. Deutschland reiht sich mit der diskutierten Neuregelung in diesen Trend ein.

Neben dem Strafrecht rücken auch regulatorische Ansätze in den Blick. Der EU-Digital Services Act (DSA) etwa

⁷⁴ BRAK (Fn. 51).

⁷⁵ BRAK (Fn. 51).

⁷⁶ Legal Tribune Online (Fn. 1).

⁷⁷ BRAK (Fn. 51).

⁷⁸ Legal Tribune Online (Fn. 1).

⁷⁹ Richtlinie (EU) 2024/1385 v. 14.5.2024 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt; *Karaboga* (Fn. 2).

⁸⁰ Richtlinie (EU) 2024/1385 (Fn. 80), Art. 49; *Rigotti/McGlynn*, *New Journal of European Criminal Law* 2022, S. (452) 467; *Rigotti*, *German Law Journal*, 25(2); Hate Aid, Deepfakes and dick pics: EU protects women from digital violence, online abrufbar unter: <http://bit.ly/4q30gyz> (zuletzt abgerufen am 15.9.2025).

⁸¹ Richtlinie (EU) 2024/1385 (Fn. 80), Art 7, 10; *Sittig* (Fn. 16).

⁸² BT-Drs. 21/1383; Deutscher Bundestag (Fn. 43).

⁸³ USA, The Take It Down Act: A Federal Law Prohibiting the Non-consensual Publication of Intimate Images of 19.5.2025, Public Law No: 119-12; The White House, ICYMI: President Trump Signs TAKE IT DOWN Act into Law, online abrufbar unter: <http://bit.ly/3VV55MB> (zuletzt abgerufen am 15.9.2025); AP, Pennsylvania Senate passes a bill to outlaw the distribution of deepfake material, online abrufbar unter: <http://bit.ly/4hdhg16> (zuletzt abgerufen am 15.9.2025); NCSL, Deceptive Audio or Visual Media (‘Deepfakes’) 2024 Legislation, online abrufbar unter: <http://bit.ly/46YFRBY> (zuletzt abgerufen am 15.9.2025).

⁸⁴ Lyons, South Korea set to criminalize possessing or watching sexually explicit deepfake videos, online abrufbar unter: <http://bit.ly/3L4E72D> (zuletzt abgerufen am 15.9.2025).

⁸⁵ UK, Online Safety Act v. 26.10.2023; UK, What does the Online Safety Act do?, online abrufbar unter: <http://bit.ly/4mWDVja> (zuletzt abgerufen am 15.9.2025).

zwingt große Plattformen, effektive Melde- und Entferungsverfahren für rechtswidrige Inhalte vorzuhalten.⁸⁶ Dies wird auch Deepfake-Opfern zugutekommen, die Löschung oder Sperrung solcher Inhalte verlangen. Zudem sieht der EU-AI Act bestimmte Transparenzpflichten für KI-Generatoren vor – so müssen generierte Inhalte grundsätzlich als solche gekennzeichnet sein, Ausnahme z.B. bei Satire.⁸⁷ Allerdings stuft der AI Act Deepfake-Software nicht grundsätzlich als Hochrisiko-KI-Systeme, sondern nur als „begrenztes Risiko“ ein, weshalb die Vorgaben relativ mild sind.⁸⁸ In Deutschland befindet sich ferner ein Gesetz gegen digitale Gewalt in Vorbereitung, das durch die vorherige Regierung durch das frühzeitige Aus der Ampelkoalition in der 20. Legislaturperiode allerdings nicht mehr verabschiedet wurde. Das Gesetz soll opferschützende Zivilinstrumente, wie z.B. Auskunftsansprüche gegen Plattformen zur Täteridentifizierung, schnellere gerichtliche Verfügungen zur Löschung, verbessern.⁸⁹ All diese Maßnahmen ergänzen das strafrechtliche Vorgehen, ersetzen es aber nicht.

VI. Fazit und Ausblick

Die Problematik der Deepfakes stellt den Strafrechtsschutz der Persönlichkeit vor neuartige Herausforderungen. Einer fiktiven, aber täuschend echt wirkenden Verletzung der Person – sei es durch pornografische Montage oder durch zugeschriebene falsche Aussagen – sehen sich die bestehenden Straftatbestände nur begrenzt gewachsen. Die Initiative zur Einführung von § 201b StGB macht deutlich, dass der Gesetzgeber gewillt ist, diese Lücke zu schließen und den Opfern moderner digitaler Angriffe gerecht zu werden. Die kontroversen Stellungnahmen haben jedenfalls schon jetzt zu einem Nachschärfen des Problembewusstseins geführt.

Klar ist, dass der Schutz vor Deepfake-basierten Persönlichkeitsverletzungen künftig an Bedeutung gewinnen wird. Je weiter die technische Entwicklung fortschreitet und je leichter entsprechende Tools verfügbar werden, desto dringlicher wird eine klare rechtliche Grenze zwischen erlaubter Nutzung und strafwürdigem Missbrauch von KI-Generierungen. Dabei muss eine Balance gefunden werden, die einerseits wirkungsvollen Opferschutz und Abschreckung gewährleistet, andererseits aber legitime kreative Anwendungen von KI, bspw. in Kunst, Satire oder Bildung nicht über Gebühr behindert. Die aktuelle Debatte zeigt exemplarisch, wie das Strafrecht auf digitale Phänomene reagieren kann, und zwar mit Augenmaß, aber auch mit der notwendigen Entschlossenheit, neue Formen der Verletzung rechtlich zu erfassen.

Schließlich sei angemerkt, dass das Strafrecht allein kein Allheilmittel gegen die „Deepfake-Gefahr“ ist. Parallel sind gesellschaftliche Aufklärung, um die Medienkompetenz zu stärken und Fälschungen schneller zu erkennen sowie technische Lösungen gefragt. Fortschritte bei KI-Detektionssystemen könnten in Zukunft helfen, Deepfakes zuverlässig zu identifizieren. Dies würde zwar die Verbreitung unwahrer Inhalte eindämmen, doch bleibt die potenzielle Persönlichkeitsverletzung durch bereits kursierende Fakes ein Faktum. Daher kommt dem rechtlichen Opferschutz – strafrechtlich wie zivilrechtlich – eine zentrale Rolle zu. Die Initiative für § 201b StGB hat den wichtigen Effekt, eine breite Diskussion über Persönlichkeitsrechte im digitalen Raum angestoßen zu haben. Sie trägt dazu bei, dass Gesetzgeber, Justiz und Gesellschaft sensibilisiert werden für die Herausforderung, die von Deepfakes und vergleichbaren technischen Manipulationen ausgeht. Mit wachsendem Problembewusstsein und einer sorgfältigen Justierung der Rechtsnormen besteht die Hoffnung, dass effektive Schutzmechanismen etabliert werden können, ohne die grundrechtlich verbürgten Freiheiten unangemessen einzuschränken. Die Diskussion ist mit der Vorlage des Gesetzesentwurfs an den Bundestag noch nicht abgeschlossen – sie hat jedoch einen wichtigen Impuls erhalten, dem in Zukunft Taten folgen müssen, um den strafrechtlichen Persönlichkeitsschutz auch im Zeitalter der KI-Generierung effektiv zu gewährleisten.

Über die dogmatische und rechtspolitische Diskussion hinaus ist schließlich zu betonen, dass auch die praktischen Rahmenbedingungen die Effektivität des geplanten § 201b StGB wesentlich bestimmen werden. Die technische Erkennung von Deepfakes stellt derzeit noch eine erhebliche Herausforderung dar. Zwar entwickeln Forschung und IT-Industrie zunehmend Verfahren zur automatisierten Identifikation manipulierter Inhalte, doch sind diese weder flächendeckend verfügbar noch rechtssicher etabliert. Für die Strafverfolgungsbehörden bedeutet dies, dass die Aufklärung entsprechender Taten erhebliche personelle und technische Ressourcen erfordert. Gleiches gilt für die Identifizierung der Täter, die häufig unter Nutzung internationaler Plattformen, Anonymisierungstechniken und Verschleierungsmaßnahmen agieren. Angesichts der ohnehin bestehenden Überlastung der Justiz droht hier eine Diskrepanz zwischen normativem Anspruch und praktischer Durchsetzbarkeit. Ein wirksamer Persönlichkeitsschutz vor Deepfakes erfordert daher nicht nur eine strafrechtliche Neuregelung, sondern auch flankierende Investitionen in die technische Ausstattung und die spezialisierte Ausbildung der Ermittlungsbehörden.

⁸⁶ Verordnung (EU) 2022/2065 v. 19.10.2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG, Art. 6 Abs. 1, Art. 9, Art. 16.

⁸⁷ Verordnung (EU) 2024/1689 v. 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2020/1828 (Verordnung über künstliche Intelligenz), Art. 50.

⁸⁸ Verordnung (EU) 2024/1689 (Fn. 88), Art. 3, Art. 50 Abs. 6, Anhang III i.V.m. Art. 6 Abs. 2.

⁸⁹ BMJ, Entwurf eines Gesetzes zur Stärkung der privaten Rechtsverfolgung im Internet, online abrufbar unter: <http://bit.ly/4ohh2s4> (zuletzt abgerufen am 15.9.2025); BT-Drs. 20/7090, online abrufbar unter: <http://bit.ly/4nGmzZ7> (zuletzt abgerufen am 15.9.2025), Rn. 76; djb (Fn. 40); Sittig (Fn. 16).