



75 Jahre  
Demokratie  
lebendig



Deutscher Bundestag  
Wissenschaftliche Dienste

---

## Sachstand

---

### Deepfakes Straf- und zivilrechtliche Implikationen

**Deepfakes**

## Straf- und zivilrechtliche Implikationen

Aktenzeichen: WD 7 - 3000 - 038/24  
Abschluss der Arbeit: 11.06.2024  
Fachbereich: WD 7: Zivil-, Straf- und Verfahrensrecht, Medienrecht, Bau und Stadtentwicklung

---

Die Wissenschaftlichen Dienste des Deutschen Bundestages unterstützen die Mitglieder des Deutschen Bundestages bei ihrer mandatsbezogenen Tätigkeit. Ihre Arbeiten geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Arbeiten der Wissenschaftlichen Dienste geben nur den zum Zeitpunkt der Erstellung des Textes aktuellen Stand wieder und stellen eine individuelle Auftragsarbeit für einen Abgeordneten des Bundestages dar. Die Arbeiten können der Geheimschutzordnung des Bundestages unterliegende, geschützte oder andere nicht zur Veröffentlichung geeignete Informationen enthalten. Eine beabsichtigte Weitergabe oder Veröffentlichung ist vorab dem jeweiligen Fachbereich anzuzeigen und nur mit Angabe der Quelle zulässig. Der Fachbereich berät über die dabei zu berücksichtigenden Fragen.

**Inhaltsverzeichnis**

<b>1.</b>	<b>Einleitung</b>	<b>4</b>
<b>2.</b>	<b>Strafrechtliche Implikationen</b>	<b>4</b>
<b>3.</b>	<b>Zivilrechtliche Implikationen</b>	<b>6</b>
<b>4.</b>	<b>Rechtsdurchsetzung</b>	<b>6</b>
<b>5.</b>	<b>Fazit</b>	<b>8</b>

## 1. Einleitung

Als Deepfakes werden unter Einsatz von KI-Systemen generierte täuschend echt wirkende Video-, Bild- und Tonaufnahmen menschlicher Gesichter, Körper oder Stimmen bezeichnet.<sup>1</sup> Überwiegend dienen Deepfakes missbräuchlichen Zwecken.<sup>2</sup> Der hierbei in der Praxis wiederum mit Abstand häufigste Fall ist offenbar die Anfertigung von pornographischen Inhalten, bei denen Personen aus Fotoaufnahmen auf die Körper von Darstellern in pornographischen Filmen eingefügt werden.<sup>3</sup>

Fraglich ist, welche straf- und zivilrechtlichen Implikationen entsprechende missbräuchliche Deepfakes grundsätzlich aufweisen können.<sup>4</sup>

## 2. Strafrechtliche Implikationen

Abhängig von der Konstellation im Einzelfall – insbesondere hinsichtlich des beabsichtigten Einsatzzweckes der Deepfakes und ihrer Verbreitung – kommen verschiedene Straftatbestände in Betracht.

So können etwa verschiedene „**Ehrdelikte**“ verwirklicht sein: **Beleidigung** (§ 185 StGB<sup>5</sup>), wenn in dem verbreiteten Deepfake ein beleidigendes Werturteil gegenüber dem Betroffenen oder gegenüber einem Dritten zu erblicken ist<sup>6</sup>, **üble Nachrede** (§ 186 StGB), insoweit mit dem Deepfake in Beziehung auf einen anderen eine Tatsache behauptet oder verbreitet wird, welche denselben verächtlich zu machen oder ihn in der öffentlichen Meinung herabzuwürdigen geeignet ist, sowie **Verleumdung** (§ 187 StGB), wenn mit dem Deepfake wider besseres Wissen in Beziehung auf einen anderen eine unwahre Tatsache behauptet oder verbreitet wird, welche denselben verächtlich zu machen oder in der öffentlichen Meinung herabzuwürdigen geeignet ist. Wegen der bei diesen Tatbeständen erforderlichen Kundgabe gegenüber anderen Personen oder der

---

1 Vgl. Block, Deepfakes und Recht – Einführung in den deutschen Rechtsrahmen für synthetische Medien, 2023, S. 5; Kumkar/Rapp, Deepfakes – Eine Herausforderung für die Rechtsordnung, ZfDR 2022, 199, 227; Lantwin, Strafrechtliche Bekämpfung missbräuchlicher Deep Fakes – Geltendes Recht und möglicher Regelungsbedarf, MMR 2020, 78.

2 Lantwin a.a.O. S. 78. Ein legitimer Zweck kann hingegen etwa in satirischen oder künstlerischen Kontexten gegeben sein, vgl. Kumkar/Rapp a.a.O. S. 200 f.

3 Block a.a.O. S. 8; Lantwin a.a.O. S. 78.

4 Eine verbindliche rechtliche Bewertung einer Handlung ist nur im jeweiligen Einzelfall möglich. Vorliegend werden deshalb nur grundsätzlich im Regelfall naheliegende Implikationen abstrakt dargestellt. Zur weiteren Vertiefung vgl. etwa Block a.a.O.

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

6 Lackner/Kühl/Heger/Heger, StGB, 30. Aufl. 2023, § 185 Rn. 2.

Öffentlichkeit erfüllt das **bloße Erstellen** eines Deepfakes ohne Kenntniserlangung Dritter hiervon gegebenenfalls noch nicht die vorbenannten Tatbestände, sondern erst die **Verbreitung**.<sup>7</sup>

Eine Strafbarkeit kann auch vorliegen nach § 201a StGB wegen **Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen**. So ist es gemäß § 201a Absatz 2 StGB strafbar, „unbefugt von einer anderen Person eine Bildaufnahme, die geeignet ist, dem Ansehen der abgebildeten Person erheblich zu schaden, einer dritten Person zugänglich“ zu machen. Hierbei ist es auch ausreichend, „wenn bloß Teile der Person (insbesondere etwa das Gesicht) abgebildet werden; zudem sind auch Fotomontagen umfasst“<sup>8</sup>. Auch von § 201a StGB nicht erfasst ist damit grundsätzlich das bloße Herstellen eines Deepfakes.<sup>9</sup>

Auch Straftatbestände aus dem **Nebenstrafrecht** – also dem außerhalb des Strafgesetzbuchs normierten Strafrecht – kommen bei missbräuchlichen Deepfakes in Betracht. So ist es gemäß § 33 i.V.m. § 22 KunstUrhG<sup>10</sup> strafbar, **Bildnisse ohne Einwilligung der abgebildeten Person zu verbreiten oder öffentlich zur Schau zu stellen**. Auch insofern wird mithin nicht die Herstellung selbst inkriminiert.<sup>11</sup>

In Betracht kommt des Weiteren auch eine Strafbarkeit wegen der **Verletzung von Urheberrechten**, da bei der Erstellung von Deepfakes – insbesondere auch beim Hauptanwendungsfall der pornographischen Deepfakes – regelmäßig auf urheberrechtlich geschütztes Foto- und Filmmaterial Dritter zurückgegriffen und dieses ohne deren Einverständnis bearbeitet und sodann verbreitet wird.<sup>12</sup> Gemäß § 106 UrhG<sup>13</sup> wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt. § 108 UrhG enthält einen entsprechenden Straftatbestand für verwandte Schutzrechte.<sup>14</sup>

---

7 Vgl. Lackner/Kühl/Heger/Heger, StGB, 30. Aufl. 2023, § 185 Rn. 3.

8 Lantwin a.a.O. S. 79.

9 Kumkar/Rapp a.a.O. S. 208; Lantwin a.a.O. S. 79.

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

11 Lantwin a.a.O. S. 79.

12 Vgl. im Einzelnen Lantwin a.a.O. S. 79 f.

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

14 Vgl. hierzu BeckOK UrhR/Sternberg-Lieben, 42. Ed. 1.5.2024, UrhG § 108 Rn. 1.

Grundsätzlich kann schließlich auch eine Strafbarkeit wegen **Verstoßes gegen Datenschutzrecht** in Betracht kommen. So macht sich nach § 42 Absatz 2 Nr. 1 BDSG<sup>15</sup> strafbar, wer personenbezogene Daten, die nicht allgemein zugänglich sind, „ohne hierzu berechtigt zu sein, verarbeitet (...) und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.“ Eine Verwirklichung dieses Straftatbestands durch Deepfakes kommt deshalb in Betracht, weil die **Gesichtszüge einer Person personenbezogene Daten** im Sinne von Artikel 4 Nr. 1 DSGVO darstellen.<sup>16</sup> Allerdings wird zu § 42 BDSG angemerkt, dass eine Strafbarkeit bei Deepfakes in praxi häufig daran scheitern werde, dass das verwendete Bildmaterial öffentlich zugänglich gewesen sei.<sup>17</sup>

### 3. Zivilrechtliche Implikationen

Das Verbreiten widerrechtlicher Deepfakes verletzt regelmäßig das **allgemeine Persönlichkeitsrecht** der betroffenen Personen.<sup>18</sup> Aufgrund dessen steht den Betroffenen in der Regel ein **Beseitigungsanspruch** gemäß § 1004 Absatz 1 BGB<sup>19</sup> analog i.V.m. Artikel 2 Absatz 1, Artikel 1 Absatz 1 GG<sup>20</sup> zu. In Betracht kommt weiterhin ein **Schadenersatzanspruch** in Gestalt einer Geldentschädigung gemäß § 823 Absatz 1 BGB i.V.m. Artikel 2 Absatz 1, Artikel 1 Absatz 1 GG und § 823 Absatz 2 BGB i.V.m. einem Schutzgesetz<sup>21</sup> bei einer schwerwiegenden Verletzung von Persönlichkeitsrechten. Urheber, deren Werke als Rahmen von Deepfakes widerrechtlich genutzt werden, stehen gegebenenfalls **urheberrechtliche Unterlassungs- und Schadenersatzansprüche** zu (§ 97 UrhG i.V.m. §§ 14, 23 UrhG).<sup>22</sup>

### 4. Rechtsdurchsetzung

In der einschlägigen Literatur wird nicht nur vereinzelt betont, dass sich die **Durchsetzung** der o.g. materiellen Rechtslage bei missbräuchlichen Deepfakes als **problematisch** erweisen kann, da

---

15 Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 7 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist.

16 Lantwin a.a.O. S. 80.

17 Lantwin a.a.O. S. 80.

18 Vgl. hierzu Kumkar/Rapp a.a.O. S. 205 ff. m.w.N. sowie Kraetzig, Deliktsschutz gegen KI-Abbilder – Teil 1: Täuschende Deepfakes, CR 2024, 207.

19 Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das zuletzt durch Artikel 17 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist.

20 Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 19. Dezember 2022 (BGBl. I S. 2478) geändert worden ist.

21 Als solche Schutzgesetze im Sinne von § 823 Absatz 2 BGB kommen insbesondere verwirklichte Straftatbestände in Betracht.

22 Vgl. hierzu Kumkar/Rapp a.a.O. S. 206 f.

die **Ermittlung der Identität** des Anspruchsgegners sowie eine etwaige **Rechtsverfolgung im Ausland** hohe Hürden bereiten können<sup>23</sup>:

„Die Plattformbetreiber können meist nicht in die Pflicht genommen werden, die Identität des Urhebers ist nur schwer zu ermitteln. Entscheidet sich der Geschädigte dennoch für eine zivilprozessuale Anspruchsdurchsetzung, ist dem ein datenschutzrechtliches Gestattungsverfahren gem. § 21 Abs. 2 TTDSG (Telekommunikation-Telemedien-Datenschutz-Gesetz)/§ 14 Abs. 3 TMG (a.F.) vorgelagert, um die Identität des Beklagten herauszufinden. Danach muss ein Diensteanbieter Auskunft erteilen, soweit dies zur Durchsetzung zivilrechtlicher Ansprüche wegen der Verletzung absolut geschützter Rechte aufgrund rechtswidriger Inhalte, die von § 10a Abs. 1 TMG oder § 1 Abs. 3 NetzDG erfasst werden, erforderlich ist. Dies setzt eine gerichtliche Anordnung voraus, für die das Landgericht am Wohnsitz des Verletzten zuständig ist, wobei dieser die Kosten der Anordnung stets zu tragen hat (§ 21 Abs. 3 Satz 3-7 TTDSG/§ 14 Abs. 4 Satz 3-7 TMG a.F.). Zwar dürften die Tatbestandsvoraussetzungen bei deepfakes regelmäßig erfüllt sein, weil eine Strafbarkeit gem. §§ 185 ff., 201a StGB, § 33 KUG, §§ 106, 108 UrhG in Betracht kommt bzw. ‚rechtswidrige audiovisuelle Inhalte‘ im Sinne von § 10a TMG gegeben sind. Der Aufwand für ein datenschutzrechtliches Gestattungsverfahren ist jedoch hoch, zumal der Diensteanbieter den betroffenen Nutzer über das laufende Verfahren unterrichten darf (vgl. § 21 Abs. 4 Satz 2 TTDSG/§ 14 Abs. 5 Satz 2 TMG a.F.). Berücksichtigt man weiterhin, dass sich der handelnde Nutzer in der Anonymität des Internets unter Pseudonym angemeldet hat oder im Ausland lebt, zeigt sich, dass diese Form der privaten Rechtsdurchsetzung im digitalen Raum wenig gangbar ist. Denn selbst wenn trotz der vorgenannten Hürden eine ladungsfähige Anschrift des Handelnden im Rahmen des Gestattungsverfahrens in Erfahrung gebracht werden kann und ein Deliktgerichtsstand für das Hauptverfahren gem. Art. 7 Nr. 2 EuGVVO bzw. § 32 ZPO in Deutschland gegeben sein sollte, wäre eine Vollstreckung im (außereuropäischen) Ausland kostenintensiv und zeitaufwändig.“<sup>24</sup>

Insofern wird mitunter das kritische Fazit gezogen,

„dass mit den klassischen Rechtsschutzmöglichkeiten des Zivil- und Strafrechts, aber auch des Datenschutzrechts letztlich kein geeigneter Schutz vor deepfakes erreicht werden kann, weil die in der Regel zeitlich weit nachgelagerte Rechtsdurchsetzung angesichts der Schnelligkeit digitaler Informationswege und den Schwierigkeiten einer grenzüberschreitenden Rechtsdurchsetzung die Problematik nicht einmal ansatzweise adäquat adressieren kann.“<sup>25</sup>

Als Reaktion wird insofern u.a. empfohlen,

„nach dem Vorbild der ‚false impersonation statutes‘<sup>26</sup> die Zugänglichmachung einer nicht einverständlichen, glaubwürdigen **Nachahmung einer Person gegenüber Dritten** unter Strafe“

---

23 Block a.a.O. S. 19 f.; Kumkar/Rapp a.a.O. S. 207.

24 Kumkar/Rapp a.a.O. S. 207 f.

25 Kumkar/Rapp a.a.O. S. 228.

26 Hierbei handelt sich um das in zahlreichen US-amerikanischen Staaten geltende strafbewehrte Verbot der unberechtigten Nachahmung von Personen, vgl. Lantwin a.a.O. S. 81.

zu stellen, „wenn dies z.B. zur Täuschung im Rechtsverkehr, in Schädigungsabsicht, zur Einschüchterung einer Person, zur Aufstachelung zu Gewalttaten oder zur Provokation von erheblichen Unruhen in der Bevölkerung geschieht und der Täter von der fehlenden Echtheit des Inhalts Kenntnis hat. (...) Vorgelagert sollte auch die **Herstellung** derartiger Inhalte einheitlich pönalisiert werden, wenn deren Herstellung zu den vorgenannten Zwecken erfolgt.“<sup>27</sup>

Von anderer Seite wird hingegen eine **Kennzeichnungspflicht** für Deepfakes angeregt:

„Sinnvoller als absolute Verbote sind strenge Kennzeichnungspflichten für deepfakes, die – ergänzt durch Löschungs- und Sperrpflichten auf Seiten der Plattform- und Netzwerkbetreiber – für mehr Transparenz und Betroffenenenschutz sorgen und gleichzeitig einen rechtssicheren Einsatz von deepfake-Technologien ermöglichen“<sup>28</sup>

## 5. Fazit

Eine Betrachtung von für missbräuchliche Deepfakes einschlägigen straf- und zivilrechtlichen Regelungen ergibt ein **zwiespältiges Bild**: Auf der einen Seite enthält das **geltende Recht** vielfältige straf- und zivilrechtliche Normen, deren Tatbestände bei Deepfakes grundsätzlich einschlägig sind und insofern eine potenziell adäquate rechtliche Handhabung des Phänomens nahelegen.<sup>29</sup> Andererseits wird jedoch mit Blick auf die **Rechtsanwendungspraxis** nicht nur vereinzelt betont, dass dieser geltende Rechtsrahmen nicht vollauf geeignet sei, um dem digitalen Phänomen missbräuchlicher Deepfakes in praxi hinreichend zu begegnen. Während anknüpfend hieran verschiedene **Reformvorschläge**<sup>30</sup> gemacht werden, ist auch **Skepsis** spürbar, ob mit jenen eine spürbare Verbesserung in der Behandlung von Deepfakes erreicht werden würde.<sup>31</sup> Lakonisch wird festgestellt: „Deepfakes werden bleiben.“<sup>32</sup>

\*\*\*

---

27 Lantwin a.a.O. S. 81 (Hervorhebung nicht im Original).

28 Kumkar/Rapp a.a.O. S. 225 f.

29 Kumkar/Rapp sprechen insofern in Bezug auf das Zivilrecht von einem *de lege lata* „gut bestückten Köcher an Rechtsschutzmöglichkeiten bei der Verteidigung gegen widerrechtliche *deepfakes* im digitalen Raum“ (a.a.O. S. 207). Eher positiv in Bezug auf das Deliktsrecht auch Kraetzig a.a.O. S. 212.

30 Vgl. hierzu vorstehenden Gliederungspunkt 4.

31 Vgl. etwa Kumkar/Rapp a.a.O. S. 228: „Deepfakes zeigen damit auch die Grenzen des Rechts im digitalen Raum auf: Diese lassen sich nicht wirksam verhindern und werden – besieht man sich die jüngere Entwicklung in den USA – in ihrer Wirkmächtigkeit tendenziell eher zu- als abnehmen.“

32 Kleemann, Deepfakes – Wenn wir unseren Augen und Ohren nicht mehr trauen können. Medienmanipulationen im Konflikt: Herausforderungen und Bewältigungsstrategien, SWP-Aktuell Nr. 43 Juni 2023, S. 4.