



Soni Rathore

Deepfakes

Datenschutz- und strafrechtliche Betrachtung

JURA

Academic *Plus* 

BEI GRIN MACHT SICH IHR WISSEN BEZAHLT



- Wir veröffentlichen Ihre Hausarbeit, Bachelor- und Masterarbeit
- Ihr eigenes eBook und Buch - weltweit in allen wichtigen Shops
- Verdienen Sie an jedem Verkauf

Jetzt bei www.GRIN.com hochladen
und kostenlos publizieren



Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de/> abrufbar.

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlanges. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Impressum:

Copyright © 2026 GRIN Verlag
ISBN: 9783389197875

GRIN Publishing GmbH
Waltherstr. 23
80337 München

Dieses Buch bei GRIN:

<https://www.grin.com/document/1742132>

Soni Rathore

Deepfakes. Datenschutz- und strafrechtliche Betrachtung

GRIN - Your knowledge has value

Der GRIN Verlag publiziert seit 1998 wissenschaftliche Arbeiten von Studenten, Hochschullehrern und anderen Akademikern als eBook und gedrucktes Buch. Die Verlagswebsite www.grin.com ist die ideale Plattform zur Veröffentlichung von Hausarbeiten, Abschlussarbeiten, wissenschaftlichen Aufsätzen, Dissertationen und Fachbüchern.

Besuchen Sie uns im Internet:

<http://www.grin.com/>

<http://www.facebook.com/grincom>

http://www.twitter.com/grin_com

Academic Plus – Aktuell, relevant, hochwertig

Mit Academic Plus bietet GRIN ein eigenes Imprint für herausragende Abschlussarbeiten aus verschiedenen Fachbereichen. Alle Titel werden von der GRIN-Redaktion geprüft und ausgewählt.

Unsere Autor:innen greifen in ihren Publikationen aktuelle Themen und Fragestellungen auf, die im Mittelpunkt gesellschaftlicher Diskussionen stehen. Sie liefern fundierte Informationen, präzise Analysen und konkrete Lösungsvorschläge für Wissenschaft und Forschung.



Hochschule Darmstadt

Fachbereich Gesellschaftswissenschaften

Studiengang: Internationales Lizenzrecht

Deepfakes – Datenschutz- und strafrechtliche Betrachtung

Abschlussarbeit zur Erlangung des akademischen Grades

Master of Laws (LL. M.)

Wintersemester 2025/26

Gender-Erklärung

Für die folgende formulierte Ausarbeitung wird ausdrücklich eine männliche Schreibweise verwendet. Dadurch sollen eine bessere sprachliche Lesbarkeit und ein höheres Textverständnis gewahrt bleiben. Sämtliche Personen und Bezeichnungen beziehen sich gleichermaßen auf alle Geschlechter.

A. Literaturverzeichnis	VII
B. Abkürzungsverzeichnis	XXIV
C. Ausarbeitung.....	1
I. Einleitung.....	1
1. Fragestellung und Zielsetzung der Arbeit	1
2. Gang der Untersuchung	2
II. Begriffsbestimmung	3
1. Künstlichen Intelligenz und (Audio-) Deepfakes	3
a) Maschinelles Lernen	4
b) Deep Learning.....	4
2. Verfahren zur Erstellung von Audio-Deepfakes	4
III. Schutz der eigenen Stimme durch Datenschutz- und Persönlichkeitsrecht	6
1. Sachlicher Anwendungsbereich der DSGVO	6
a) Personenbezogenes Datum	7
b) Biometrisches Datum.....	7
c) Stimme als Datum besonderer Kategorien gem. Art. 9 DSGVO.....	8
d) Verarbeitung	11
aa) Erstellung der Audio-Deepfakes	11
bb) Nutzung der Audio-Deepfakes	11
2. Persönlicher Anwendungsbereich	12
3. Zwischenergebnis.....	12
4. Anwendbarkeit des KUG	12
a) Journalistische Tätigkeit	13
b) Lerninhalte als journalistische Tätigkeit	13
5. Deepfake als Bildnis	14
6. Stimme als Bildnis	14
7. Abgrenzung eigene Stimme und gesprochenes Wort.....	16
8. Zwischenergebnis.....	16
9. Grundsätze der Datenverarbeitung, Art. 5 DSGVO.....	16
a) Rechtmäßigkeit und Transparenz.....	16
b) Zweckbindung.....	17
c) Datenminimierung	17
d) Richtigkeit.....	18
e) Speicherbegrenzung (Datenaufbewahrung).....	19

f)	Integrität und Vertraulichkeit	19
g)	Rechenschaftspflicht	20
10.	Rechtmäßigkeit der Datenverarbeitung	20
a)	Berechtigtes Interesse, Art. 6 I UAbs. I lit. f DSGVO	20
b)	Verarbeitung zur Erfüllung eines Vertrags (Art. 6 I UAbs. I lit. b)	21
aa)	Model-Release-Vertrag (MRV)	21
bb)	Einwilligung, Art. 6 I UAbs. I lit. a i. V. m. Art. 9 II lit. a DSGVO	22
(1)	Wirtschaftlicher Vorteil durch MRV	23
(2)	Festlegung einer Vergütung	24
cc)	Weitere Anforderungen der Einwilligung	25
dd)	Form	28
ee)	Widerruf	29
(1)	Persönlichkeitsrechtliche Einwilligung	29
(2)	Form	30
ff)	Nutzungsarten und Bearbeitungsrecht	30
gg)	Sonstiges	31
11.	Ergebnis und Gesamtwürdigung	31
IV.	Weitere datenschutzrechtliche Anforderungen	32
1.	Auftragsverarbeitungsvertrag mit KI-Anbieter	32
2.	Drittlandübermittlung	33
3.	Technische und Organisatorische Maßnahmen	34
a)	Technische Maßnahmen	35
b)	Organisatorische Maßnahmen	36
4.	Datenschutzfolgenabschätzung	37
5.	Betroffenenrechte	38
V.	Rechtsfolgen, Haftung und Sanktion bei Verstößen	39
VI.	Schutz der eigenen Stimme durch das KI-Recht (KI-VO)	41
1.	Anwendungsbereich der KI-VO	41
a)	Sachlicher Anwendungsbereich	41
aa)	Deepfake-Generator als KI-System	41
bb)	Deepfakes i. S. d. KI-VO	42
(1)	Inhalte	43
(2)	Ähnlichkeit zu realweltlichen Bezugsobjekten	43
(3)	Eindruck als echt oder wahrheitsgemäß	44

b) Persönlicher Anwendungsbereich	45
aa) K als Anbieter.....	45
bb) K als Betreiber	45
2. Zwischenergebnis.....	46
3. Pflichten nach der KI-VO	46
a) Offenlegungspflicht des Betreibers.....	46
b) Kennzeichnungspflicht des Anbieters	47
aa) Wasserzeichen	48
bb) Mögliche Herausforderungen	49
c) Sonstige Pflichten nach Art. 50 KI-VO	50
d) Freiwillige Verhaltenskodizes	51
4. Rechtsfolgen bei Pflichtverletzungen oder sonstigen Verstößen	51
VII. Schutz der eigenen Stimme im Strafrecht.....	52
1. Anwendbarkeit deutschen Strafrechts und bestehender Strafnormen.....	52
2. Vermögensdelikte: Betrug, § 263 StGB.....	53
a) Täuschungshandlung.....	53
b) Irrtumserregung	54
aa) Identitätsmissbrauch des M.....	54
bb) Irrtum trotz Zweifeln?.....	55
c) Vermögensverfügung	56
d) Vermögensschaden.....	57
e) Zwischenergebnis	57
f) Qualifikation: Bandenbetrug nach § 263 V StGB.....	57
3. Rechtfolge und Anmerkung	58
4. Computerbetrug, § 263a StGB.....	58
5. Delikte gegen den persönlichen Lebens- und Geheimnisbereich: Verletzung der Vertraulichkeit des Wortes, § 201 StGB	59
6. Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen, § 201a II 1 StGB.....	60
7. Zwischenergebnis.....	60
8. § 201b StGB-E.....	60
a) Kritik des § 201b-E StGB	62
aa) Tatobjekt.....	62
bb) Tathandlung	62
cc) Unklarheit über Schutzgut.....	63

dd) Geeignetheit bestehender Regelungen.....	64
b) Notwendigkeit und Alternativvorschläge	65
9. Datenbezogene Delikte: Ausspähen von Daten, § 202a StGB.....	66
a) Daten	66
b) Nicht für den Täter bestimmt.....	67
c) Gegen unberechtigten Zugang besonders gesichert.....	68
d) Verschaffen des Zugangs unter Überwindung der Zugangssicherung.....	69
e) Ergebnis und Rechtsfolge	70
10. Abfangen von Daten, § 202b StGB	70
11. Vorbereiten des Ausspähens und Abfangens von Daten, § 202c StGB	70
a) Computerprogramme	71
b) Herstellen	71
c) Ergebnis und Rechtsfolge	72
12. Datenveränderung, § 303a StGB	72
VIII. Strafrechtlicher Schutz der Authentizität von Medieninhalten	73
VII. Strafrechtliche Nebengesetze	74
1. Zivilrechtliche Ansprüche	74
2. KUG	75
3. BDSG	75
4. Durchsetzungsschwierigkeiten.....	75
IX. Abschließende Handlungsempfehlungen.....	76
1. Alternative Regulierungsansätze.....	76
2. Beteiligung des Betriebsrats.....	77
3. Ethische Aspekte	77
4. Generelle Empfehlungen.....	78
a) Prävention	78
b) Detektion.....	78
c) Komplementäres	79
X. Fazit.....	80