Deepfakes: Eine juristische Einordnung

Inhaltsverzeichnis

1.	**Vorbemerkungen**	**2**
2.	**Rechtliche Einordnung von Deepfakes**	**2**
2.1.	Rechtliche Regelungen auf EU-Ebene	2
2.1.1.	KI-Verordnung	2
2.1.2.	Digital Services Act (DSA)	3
2.1.3.	Datenschutzgrundverordnung (DSGVO)	4
2.2.	Deepfakes im nationalen Zivilrecht	4
2.2.1.	Deepfakes als Eingriff in das Allgemeine Persönlichkeitsrecht	4
2.2.2.	Deepfakes und Namensrecht	5
2.2.3.	Deepfakes und Urheberrecht	6
2.3.	Deepfakes im nationalen Strafrecht	6
2.3.1.	Strafbarkeit nach StGB	6
2.3.2.	Strafbarkeit nach KUG	7
2.3.3.	Strafbarkeit nach dem Urheberrechtsgesetz	7
2.4.	Kennzeichnungspflicht im Medienstaatsvertrag	7
2.5.	Problematik der Durchsetzbarkeit	7
3.	**Zwischenfazit**	**7**
4.	**Aktuelle Entwicklungen**	**8**
4.1.	Grundlegendes zum Entwurf	8
4.2.	Ausgestaltung und Notwendigkeit	9
5.	**Fazit und Ausblick**	**9**
6.	**Quellenverzeichnis**	**10**
	Autoren	**11**
	Kontakt	11

1. Vorbemerkungen

Mit den fortschreitenden Entwicklungen im Bereich der künstlichen Intelligenz (KI) gewinnt die Beschäftigung mit der Thematik Deepfakes an Wichtigkeit. Computersoftware ist mittels KI heute in der Lage Medieninhalte, wie Fotos, Filme und Audioaufnahmen, zu verändern oder auf ihrer Grundlage völlig neu Inhalte zu generieren. Die erstellten oder modifizierten Medieninhalte können sog. „Deepfakes" sein.[1] Der Begriff leitet sich von „deep learning", einer fortgeschrittenen Methode des maschinellen Lernens, und „fake" ab. Deepfakes erreichen durch die neue Leistungsfähigkeit von Künstlicher Intelligenz heute einen völlig neuen Authentizitätsgrad. Gestik, Mimik, Stimme und Tonlagen einer Person können so realistisch imitiert werden, dass für den Laien – und immer häufiger auch den technischen Experten – unmöglich ist, zwischen realer Darstellung oder Deepfake zu unterscheiden.[2]

Deepfakes sind vielseitig einsetzbar. Neben positiven Anwendungsmöglichkeiten im medizinischen Bereich oder im Unterhaltungssektor birgt der Einsatz von Deepfakes nicht nur gesellschaftliche Risiken, sondern auch erhebliche Gefahren für individuelle Persönlichkeitsrechte.[3] Galten Fotos, Videos und Audioaufnahmen einst als verlässliche Tatsachengrundlage, sinkt das diesbezügliche Vertrauen deutlich – spätestens seit die breite Öffentlichkeit die Möglichkeit hat, ohne nennenswerte Hürden Deepfakes zu erstellen. In einer repräsentativen Civey-Befragung im Auftrag des BVDW sagten 72 % der Befragten, dass das Vertrauen in digitale Medien durch die Verbreitung von Deepfakes definitiv oder eher sinkt.[4]

Dieses Papier baut auf dem bereits veröffentlichen Papier des BVDW-Ressorts KI[5] auf und wiederholt daher nicht die Betrachtung der technischen und gesellschaftlichen Diskussion, die bereits geführt wird oder aus Sicht des BVDW zusätzlich geführt werden sollte. Stattdessen wird das Thema Deepfakes im Nachfolgende aus einer juristischen Perspektive betrachtet und die bereits bestehende Gesetzeslage sowie Vorschläge zur Anpassung dieser in den Fokus gerückt.

2. Rechtliche Einordnung von Deepfakes

Deepfakes können falsche Aussagen oder Handlungen simulieren, die tatsächlich nie stattgefunden haben. Das Ansehen von Personen, Unternehmen oder Organisationen kann so erheblich geschädigt werden. So werden beispielsweise Frauen durch Deepfakes in einen zuvor nicht bestehenden und offensichtlich nicht gewollten sexuellen Kontext gesetzt. Aber auch im politischen Kontext können Deepfakes durch bewusste Fehlinformationen Schaden anrichten. Ende 2023 tauchte z.B. ein Deepfake-Video auf, in dem Bundeskanzler Olaf Scholz vermeintlich ankündigte, ein Parteiverbotsverfahren gegen die AfD anstrengen zu wollen.[6]

Angesichts der wachsenden Bedeutung des Phänomens Deepfakes stellt sich die Frage nach der rechtlichen Einordnung jener und insbesondere, inwiefern Rechtsschutzmöglichkeiten für Personen existieren, die ungewollt in Deepfakes „hineineditiert" werden. Spezifische Regelungen gibt es bisher kaum – vorwiegend richtet sich die rechtliche Einordnung nach bestehenden Vorschriften, beispielsweise des Europarechts oder auf nationaler Ebene des Zivil- oder Strafrechts. Die einschlägigen Gesetze dazu werden im Folgenden näher betrachtet und erläutert, wie sie mit dem Thema Deepfake umgehen.

2.1. Rechtliche Regelungen auf EU-Ebene

Mehrere EU-Verordnungen beschäftigen sich bereits mit Deepfakes oder betreffen den Umgang mit Ihnen zumindest indirekt.

2.1.1. KI-Verordnung

Die KI-Verordnung ist eine Revolution und ein Meilenstein im Bereich der Regulierung von künstlicher Intelligenz. Der Unionsgesetzgeber hat in 112 Artikeln und 180 Erwägungsgründen nach langen Verhandlungen ein Gesetz geschaffen, dass die umfassende Regelung von KI weltweit erstmalig darstellt.

1 MMR 2019, 574, beck-online.
2 ZfDR 2022, 199, 202 beck-online.
3 Kumkar/Rapp: Deepfakes (ZfDR 2022, 199), s. 200; (MMR 2019, 574, beck-online).
4 Vgl. dazu das BVDW-Paper „Deepfakes – Eine Einordnung", https://www.bvdw.org/wp-content/uploads/2024/07/2024_BVDW_Deepfakes.pdf?highlight=2024
5 ebd
6 Erdogan, Scholz-Deepfake – bewusste Falschinformation zu politischen Zwecken, MMR 2024, 379.

Allen Beteiligten waren sich von Anfang an einig: Auch Deepfakes müssen bestimmte Anforderungen erfüllen. Um auf Nummer sicher zu gehen, hat der Unionsgesetzgeber in Art. 3 Nr. 60 KI-Verordnung den Begriff des „Deepfakes" sogar definiert. Im Sinne der KI-Verordnung handelt es sich bei einem Deepfake um

> „einen durch KI erzeugten oder manipulierten Bild-, Ton- oder Videoinhalt, der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde."

Betreiber von KI-Systemen, die Deepfakes erzeugen (können), müssen besondere Transparenzpflichten gemäß Art. 50 Abs. 4 KI-Verordnung einhalten. „Betreiber" im Sinne der KI-Verordnung sind natürliche oder juristische Personen (bspw. Unternehmen oder Behörden), die das KI-System in eigener Verantwortung und nicht im privaten Kontext verwenden. Betreiber von KI-Systemen müssen offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert sind. Die Offenlegung muss nach Erwägungsgrund 134 „klar und deutlich" sein. Betreiber müssen die KI-Ergebnisse „entsprechend kennzeichnen und auf ihren künstlichen Ursprung hinweisen". Wer also ein Deepfake zu kommerziellem Nutzen einsetzt, der muss klar kommunizieren, dass es sich um ein Deepfake handelt. Ansonsten drohen hohe Bußgelder. In Art. 50 Abs. 4 KI-Verordnung ist auch festgelegt, wann diese Transparenzpflicht nur eingeschränkt gilt:

> „...,wenn die Verwendung zur Aufdeckung, Verhütung, Ermittlung und Verfolgung von Straftaten gesetzlich zugelassen ist. Ist der Inhalt Teil eines offensichtlich künstlerischen, kreativen, satirischen, fiktionalen analogen Werks oder Programms, so beschränken sich die [...] festgelegten Transparenzpflichten darauf, das Vorhandensein solcher erzeugten oder manipulierten Inhalte in geeigneter Weise offenzulegen, die die Darstellung oder den Genuss des Werks nicht beeinträchtigt."

Die Klarheit und die Deutlichkeit der Kennzeichnung als Deepfake bleiben dabei unberührt. Vielmehr berücksichtigt die KI-Verordnung so nur, dass das Werk nicht durch die Kennzeichnung beeinträchtigt wird.

Die KI-Verordnung macht also Einschränkungen zur Erzeugung und Verbreitung von Deepfakes, verbietet diese aber nicht grundsätzlich durch beispielsweise Art. 5 Abs. 1 lit. a KI-Verordnung. Denn die KI-Verordnung verbietet nur die nicht erkennbaren Reize. Erwägungsgrund 29 nennt dafür die Gehirn-Computer-Schnittstellen oder Virtual Reality als Beispiele. Deepfakes vermitteln keine „nicht erkennbaren" Reize, da diese erkennbar sind. Sie liegen offen zutage.[7]

Auch die Einstufung als Hochrisiko-KI-System scheidet eher aus. Möglich erscheint, dass bestimmte KI-Systeme, die zur Beeinflussung von Wahlen eingesetzt werden als hochriskant eingestuft werden. Das betrifft KI-Systeme, die bestimmungsgemäß zur Beeinflussung der demokratischen Prozesse eingesetzt werden. Wer beispielsweise ein Deepfake zweckentfremdet, der unterfällt demnach nicht zwingend den Pflichten für hochriskante KI-Systeme.

2.1.2 Digital Services Act (DSA)

Der DSA soll zur Schaffung eines sicheren digitalen Raums und Grundrechtsschutz der Nutzer*innen sowie gleichen Wettbewerbsbedingungen beitragen und gilt insbesondere für Online-Vermittler und -Plattformen (z.B. Online-Marktplätze, soziale Netzwerke, Content-Sharing-Plattformen, App-Stores).

In Art. 35 Abs. 1 lit. k DSA enthält er als mögliche Risikominderungsmaßnahme für VLOPs und VLOSEs[8] eine Kennzeichnungspflicht und eine Meldefunktion von Deepfakes, wenn diese fälschlicherweise für echt gehalten werden könnten:

> „(1) Die Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen ergreifen angemessene, verhältnismäßige und wirksame Risikominderungsmaßnahmen (...). Hierzu können unter Umständen gehören:
> (...)
> k) Sicherstellung, dass eine Einzelinformation, unabhängig davon, ob es sich um einen erzeugten oder manipulierten Bild-, Ton- oder Videoinhalt handelt, der bestehenden Personen, Gegenständen, Orten oder anderen Einrichtungen oder Ereignissen merklich ähnelt und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheint, durch eine auffällige Kennzeichnung erkennbar ist, wenn sie auf ihren Online-Schnittstellen angezeigt wird, und darüber hinaus Bereitstellung einer benutzerfreundlichen Funktion, die es den Nutzern des Dienstes ermöglicht, solche Informationen anzuzeigen.(...)"

Dies zeigt, dass Deepfakes grundsätzlich als Risiko angesehen werden. Die Ausgestaltung dieser Regelung lässt aber letztlich den Diensteanbietern ein gewisses Ermessen und funktioniert am Ende nur mit den Regelungen der KI-Verordnung für die Betreiber von KI-Systemen zur Erzeugung von Deepfakes zusammen, wie oben beschrieben.

7 Becker, CR 2024, 353, 364.
8 VLOP= Very Large Online Platform; VLOSE= Very Large Online Search Engine.

2.1.3. Datenschutzgrundverordnung (DSGVO)

Das Erstellen und Verbreiten von Deepfakes wird in der Regel dann vom Datenschutzrecht erfasst, sobald die Video-, Ton- oder Bildaufnahmen auf eine real existierende Person schließen lassen oder eine solche darin erkennbar ist.

Eine Verarbeitung personenbezogener Daten ist nur dann erlaubt, wenn eine Rechtsgrundlage nach Art. 6 DSGVO gegeben ist, wie z.B. eine Einwilligung (Art. 6 Abs. 1 S. 1 lit. a DSGVO), die Erfüllung eines Vertrages (Art. 6 Abs. 1 S. 1 lit. b DSGVO) oder die Wahrung berechtigter Interessen (Art. 6 Abs. 1 S. 1 lit. f DSGVO). Eine mit Einwilligung erfolgte Sprach- oder Videoaufnahme dürfte dann aber beispielsweise nicht automatisch zur Herstellung eines Deepfakes verwendet werden, da die Einwilligung immer nur für den konkreten Fall erteilt werden kann und regelmäßig nicht spätere Bearbeitungsprozesse abgedeckt sind[9]. Zu berücksichtigen sein könnten auch die Voraussetzungen für die Verarbeitung besonderer Kategorien personenbezogener Daten sein (Art. 9 DSGVO).

Von Deepfakes betroffenen Personen kann gegenüber dem Verantwortlichen ein Löschungsanspruch gemäß Art. 17 Abs. 1 lit. d) DSGVO zustehen. Diesem kann der Verantwortliche u.U., z.B. im Fall von Satire und/oder Parodien, sein Recht auf Ausübung freier Meinungsäußerung und Information gemäß Art. 17 Abs. 3 lit. a) DSGVO entgegenhalten – soweit nicht sowieso bereits eine Privilegierung nach Art. 85 DSGVO greift.[10] Daneben kann auch ein Anspruch auf Schadensersatz gem. Art. 82 DSGVO – gerade im Hinblick auf immaterielle Schäden – bestehen.

Anspruchsgegner wäre dann jeweils der datenschutzrechtlich Verantwortliche, also die Person, die über die Zwecke und Mittel der Datenverarbeitung entscheidet (Art. 4 Nr. 7 DSGVO). In Bezug auf über Soziale Medien verbreitete Deepfakes stellt sich hier die Frage nach einer Verantwortlichkeit der Plattformbetreiber. Bei einer werbefinanzierten Plattform tendiert die Literatur dazu, eine gemeinsame Verantwortlichkeit von Plattformbetreiber und der Person, die Deepfakes hochlädt, anzunehmen[11]. Eine unmittelbare Inanspruchnahme des Plattformbetreibers kann aber ausscheiden, da nach Erwägungsgrund Nummer 21 der DSGVO die Regelungen der E-Commerce-Richtlinie fortgelten, wonach Anbieter reiner Vermittlungsdienste dann nicht verantwortlich sein sollen, wenn sie keine Kenntnis von der Rechtsverletzung haben oder unverzüglich nach Kenntniserlangung tätig geworden sind. Gleiches gilt auch nach den neuen entsprechenden Vorschriften des DSA. Eine Störerhaftung des Plattformbetreibers für Datenschutzverstöße durch die Nutzer nach nationalem Recht wird vor diesem Hintergrund ebenfalls überwiegend abgelehnt.[12]

Soweit Deepfakes im Rahmen journalistischer, künstlerischer oder literarischer Zwecke erstellt werden, finden im Rahmen von Art. 85 DSGVO allerdings teilweise nationale Regelungen vorrangig Anwendung.[13] Während für journalistische Zwecke auf die §§ 22, 23 KUG, die nationalen medienrechtlichen Regelungen und das Allgemeine Persönlichkeitsrecht zugegriffen werden kann, ist im Übrigen umstritten, inwieweit dies auch über das Presserecht hinaus gilt.

2.2. Deepfakes im nationalen Zivilrecht

Der zivilrechtliche Schutz gegen Deepfakes ist bereits recht umfangreich. In den meisten Fällen ist eine Verletzung des sog. Allgemeinen Persönlichkeitsrecht (APR) gegeben, wenn eine (erkennbare) Ähnlichkeit zu real existierenden Personen besteht.

Die betroffene Person hat hier häufig einen Anspruch auf Entfernung und künftige Unterlassung. In besonderen Konstellationen können Ansprüche auf Gegendarstellung, Widerruf und Richtigstellung gegeben sein. In einigen Fällen, insbesondere bei Deepfakes, die die betroffene Person in einem bloßstellenden, diskreditierenden oder pornografischen Kontext darstellen, kann auch ein finanzieller Ausgleich durch die Zahlung von Schadensersatz und bei schwerwiegenden und nicht anders auszugleichenden Persönlichkeitsrechtsverletzungen Schmerzensgeld bzw. Geldentschädigung verlangt werden.[14] Gleichwohl bestehen Schwierigkeiten auf der Ebene der praktischen Durchsetzbarkeit.[15] Dabei kommt dem Anspruch auf Auskunft der Identität desjenigen, der einen Deepfake erstellt, veröffentlicht und/oder weiterverbreitet hat, eine besondere Bedeutung zu.[16]

2.2.1. Deepfakes als Eingriff in das Allgemeine Persönlichkeitsrecht

Bei der Verwendung von Deepfakes kommt es vor allem zu Verletzungen des APR. Das APR wird aus Art. 2 Abs. 1 GG (Recht auf freie Entfaltung der Persönlichkeit) und Art. 1 Abs. 1 GG (Menschenwürde) abgeleitet. Grundsätzlich soll jeder selbst

9 Kumkar/Rapp, Deepfakes, ZfDR 2022, 199.
10 Kumkar/Rapp, Deepfakes, ZfDR 2022, 199 (218).
11 Kumkar/Rapp, Deepfakes, ZfDR 2022, 199, 215f.
12 Kumkar/Rapp, Deepfakes, ZfDR 2022, 199, 216.
13 Die Abgrenzung des Datenschutzrechts vom Allgemeinen Persönlichkeitsrecht bzw. der Anwendung des KUG ist ungeklärt und umstritten. Die Gerichte sind derzeit insbesondere bemüht, Wertungswidersprüche zu vermeiden.
14 Vgl. Lantwin, Deep Fakes – Düstere Zeiten für den Persönlichkeitsschutz?, MMR 2019, 574.
15 Kumkar/Rapp, Deepfakes, ZfDR 2022, 199, 207.
16 In Bezug auf Anbieter digitaler Dienste ergibt sich ein solcher aus § 21 Abs. 2 TDDDG (vormals TTDSG).

entscheiden, was über ihn oder sie bekannt wird und wie mit den eigenen Informationen umgegangen wird. Es schützt deshalb vor Eingriffen in das Privatleben, vor falschen oder herabwürdigenden Darstellungen in der Öffentlichkeit und vor ungewollter Veröffentlichung von Bildern oder persönlichen Informationen. Das APR kann durch Deepfakes in verschiedenen Ausprägungen betroffen sein, z.B. als Recht am eigenen Bild (siehe unten), Recht am gesprochenen Wort (schützt u.a. vor Falschzitaten)[17], Recht an der eigenen Stimme, Recht am eigenen Namen (§ 12 BGB), Recht auf informationelle Selbstbestimmung (siehe oben zum Datenschutzrecht) oder als Recht auf sexuelle Selbstbestimmung.[18]

Das APR der betroffenen Personen kann dabei in Widerstreit mit den Interessen/Grundrechten der Hersteller/Verwender von Deepfakes stehen, wie z.B. der Pressefreiheit, Kunstfreiheit, Wissenschaftsfreiheit, Berufsfreiheit oder dem Eigentumsrecht. In solchen Fällen ist eine Abwägung der jeweiligen Interessen erforderlich. Als grobe Faustformel kann man sich merken: Je eindeutiger ein Deepfake als solches erkennbar ist, desto weniger Schutz wird dem APR im Rahmen einer solchen Abwägung zukommen. Je weniger offensichtlich die Manipulation hingegen ist, desto weniger wird sich die Person, die dieses verbreitet, auf eine schutzwürdige Rechtspositionen berufen können.[19] Weiterhin fällt im Rahmen dieser Abwägung ins Gewicht, ob die Darstellung herabsetzend ist und/oder ob ein öffentliches Interesse an ihr besteht. Unter Umständen wiegt dann das Recht des Herstellers/Verwenders und/oder der Öffentlichkeit schwerer, sodass dem Betroffenen keine Ansprüche zustehen. Das kann z. B. der Fall sein, wenn es sich um eine erkennbar satirische, nicht „echte" Darstellung handelt.[20]

Wie sich aus der Rechtsprechung zu Fotomontagen – die auf die Verbreitung und gegebenenfalls auch auf die Herstellung von Deepfakes übertragen werden kann[21] – ergibt, schützt das APR vor der Verbreitung eines technisch manipulierten Bildes, das den Anschein erweckt, ein authentisches Abbild einer Person zu sein. Der Träger des Persönlichkeitsrechts hat danach zwar kein Recht darauf, von Dritten nur so wahrgenommen zu werden, wie er sich selbst gerne sehen möchte, wohl aber ein Recht darauf, dass ein fotografisches Abbild nicht manipulativ entstellt ist, wenn es Dritten ohne Einwilligung des Abgebildeten zugänglich gemacht wird.[22] Das Bundesverfassungsgericht ging dabei von einer Verletzung des APR unabhängig davon aus, ob die Manipulation in guter oder in verletzender Absicht geschah oder ob diese vorteilhaft oder nachteilig wahrgenommen wird. Die Meinungsfreiheit gelte nicht für unrichtige Information, wie manipulierte Bilder.[23]

Keine Verletzung des APR soll dagegen gegeben sein, wenn Person und Leib derart voneinander entkoppelt sind, dass der Zugriff auf Bild oder Stimme keinen unmittelbaren Zugriff auf die Person darstellt, wie es bei der offen fiktiven Verwendung von Körpermerkmalen etwa in Computerspielen der Fall ist. Das ist jedoch nicht der Fall, sobald eine Ähnlichkeit besteht oder Imitation naheliegt.[24]

Für den Bereich des Rechts am eigenen Bild, einen Unterfall des APR, bestehen spezielle Regelungen im Kunsturhebergesetz (KUG). Die Verbreitung oder das Zurschaustellen von Deepfakes kann auch eine Verletzung des dieses Rechts am eigenen Bild darstellen, wenn dabei erkennbar das äußere Erscheinungsbild einer Person wiedergegeben wird. Das Recht am eigenen Bild gem. §§ 22, 23 KUG schützt den Einzelnen vor einer ungewollten Veröffentlichung und Verbreitung des eigenen Bildnisses in dem es dafür grundsätzlich eine Einwilligung verlangt Bildnis ist dabei das äußere Erscheinungsbild einer Person in einer für Dritte erkennbaren Weise. Die umstrittene Frage, ob Deepfakes überhaupt unter diesen Schutz fallen, da sie ja keine echten Aufnahmen sind, wird oft bejaht, weil die Person aufgrund ihrer individuellen Merkmale für Dritte erkennbar ist und der Adressat das Deepfake für echt hält/halten könnte. Mangels Einwilligung wird als einzige Ausnahme ein satirisches und als solches erkennbares Deepfake mit Prominenten im zeitgeschichtlichen Kontext in Betracht kommen.[25]

2.2.2. Deepfakes und Namensrecht

Denkbar ist bei entsprechender Gestaltung eines Deepfakes auch die Verletzung des Namensrechts gem. § 12 BGB des Abgebildeten, was insbesondere von Bedeutung sein kann, wenn das APR nur eingeschränkten Schutz bietet. So habe das LG Berlin II offenbar die Veröffentlichung eines Videos untersagt, dass Bundeskanzler Olaf Scholz bei einer Ansprache zeigt, bei der er ein AfD-Verbotsverfahren ankündigt.[26]

17 MAH UrhR, § 12 (Verfassungs-)Rechtliche Grundlagen der Wort- und Bildberichterstattung Rn. 47, beck-online.
18 Vielfach wird auch das Bestehen eines sog. Unternehmenspersönlichkeitsrechts anerkannt, das z.B. als Instrument zum Schutz der Unternehmensreputation gegen unwahre Tatsachenbehauptungen dienen kann, vgl. Prinz, Fezer/Büscher/Obergfell, Lauterkeitsrecht:UWG, Band 1, Presse im WettbewerbsR, Rn. 87ff., Koreng: Das „Unternehmenspersönlichkeitsrecht" als Element des gewerblichen Reputationsschutzes, GRUR 2010, 1065ff.
19 Vgl. Deutscher Bundestag Wissenschaftliche Dienste, Kurzinformation – Regulierung von Deepfakes, WD-7-015-24.
20 Vgl. Kumkar/Rapp, Deepfakes, ZfDR 2022, 199, 206.
21 Lantwin, Deep Fakes – Düstere Zeiten für den Persönlichkeitsschutz?, MMR 2019, 574.
22 BVerfG, NJW 2005, 3271, 3273.
23 BVerfG, NJW 2005, 3271, 3272.
24 Lennartz, „Digitale Puppenspieler" – die Nachbildung von Körper und Stimme durch KI, NJW 2023, 3543, 3544.
25 Kumkar/Rapp, Deepfakes, ZfDR 2022, 199, 204 f..
26 Vgl. hierzu Erdogan, Scholz-Deepfake – bewusste Falschinformation zu politischen Zwecken, MMR 2024, 379; https://www.lto.de/recht/nachrichten/n/lg-berlin-ii-15o579-23-olaf-scholz-bundeskanzler-deep-fake-afd-verbot-zentrum-politische-schoenheit/.

Eine Verletzung des Namensrechts könne danach auf einer sogenannten Zuordnungsverwirrung beruhen. Entscheidend sei, ob ein durchschnittlicher Betrachter das Video für echt halten könne. Wenn die Gestaltung des Deepfakes darauf angelegt ist, wie eine echte Veröffentlichung zu wirken, wird dies tendenziell zu bejahen sein.[27]

2.2.3. Deepfakes und Urheberrecht

Werden bei der der Erstellung von Deepfakes urheberrechtlich geschützte Werke (z. B. Filme) und/oder Leistungen (z. B. einfache Schnappschüsse) ohne oder gegen den Willen des Urhebers oder Leistungsschutzberechtigten verwendet, kommen urheberrechtliche Ansprüche in Betracht. Dies sind z. B. Ansprüche aufgrund einer Entstellung (§ 14 UrhG), Vervielfältigung (§ 16 UrhG), öffentlichen Zugänglichmachung (§ 19a UrhG) oder Bearbeitung (§ 23 UrhG).[28] Unter Umständen kann aber eine Rechtfertigung für den Eingriff in das Urheberrecht vorliegen: Nach den §§ 51a S. 1, 62 Abs. 4a UrhG ist die Verbreitung und/oder Änderung eines veröffentlichen Werkes zum Zwecke der Parodie zulässig. Die oftmals diffamierend gestalteten Deepfakes dürften indes nicht darunterfallen und unzulässig bleiben.[29]

Die resultierenden Ansprüche stehen allerdings nicht der Person zu, die Gegenstand eines Deepfakes ist, sondern dem Urheber bzw. dem Inhaber der Leistungsschutzrechte.

2.3. Deepfakes im nationalen Strafrecht

Ein explizites strafrechtliches Verbot von Deepfakes gibt es bisher nicht. Es existieren strafrechtliche Regelungen, die bei der Erstellung oder Verwendung von Deepfakes einschlägig sein können. Diese Vorschriften erfassen Deepfakes aber jeweils nur in Teilaspekten, bzw. als Instrument oder Mittel zur Begehung einer Straftat

2.3.1. Strafbarkeit nach StGB

Es kann eine Strafbarkeit wegen Betruges vorliegen (§263 StGB), wenn Deepfakes zur Täuschung von Personen verwendet werden, um diese zu einer Vermögensverfügung zu verleiten. Zu denken ist hier z. B. an Fälle, in denen die Stimmen von Führungskräften mit Deepfakes nachgeahmt werden, um Zahlungen auf fremde Konten zu beauftragen oder zu genehmigen. Ist nicht eine andere Person Adressat der Täuschung, sondern wird versucht, einen technischen Mechanismus mit Hilfe von Deepfakes zu überlisten, kann ein sog. Computerbetrug (§ 263a StGB) vorliegen.

Gem. § 201a Abs. 2 StGB ist zudem das Verbreiten (aber nicht bereits das Erstellen) einer Bildaufnahme unter Strafe gestellt, die geeignet ist, dem Ansehen der abgebildeten Person erheblich zu schaden. Das gilt auch für Bildaufnahmen einer verstorbenen Person (§ 201a Abs. 2 Satz 2 StGB). Auch hier liegt ein Bildnis vor, obwohl die Aufnahme nicht „echt" ist. Ob die Aufnahme geeignet ist, dem Ansehen der abgebildeten Person zu schaden, ist eine Einzelfallentscheidung. Hierbei müssen alle relevanten Tatsachen beachtet werden, etwa die Stellung des Opfers in der Öffentlichkeit und die Art der Darstellung etc.. Eine Faustformel, die dabei helfen kann, lautet: „Je minderwertiger, peinlicher, ekliger oder abstoßender die jeweilige Aufnahme erscheint, umso einfacher dürfte die Eignung zur Ansehensschädigung festzustellen sein."[30]

Auch die Erstellung und Verwendung eines Deepfakes mit kinder- oder jugendpornografischem Inhalt kann strafbar sein (§§ 184b Abs. 1 Nr. 1 lit. a) und Abs. 4, 184c Abs. 1 Nr. 1 lit. a) und Abs. 4 StGB). Die Strafgesetze fordern in diesem Fall gerade nicht, dass es sich um echte Inhalte handeln muss.

Deepfakes können auch eine strafrechtlich relevante Ehrverletzung (§§ 185 ff. StGB) darstellen, sofern die Darstellung geeignet ist, die abgebildete Person verächtlich zu machen oder unwahre Tatsache über den Betroffenen zu verbreiten. Insbesondere kommt eine Verleumdung gemäß § 187 StGB in Betracht, wenn durch das Deepfake eine Lüge über das Opfer behauptet wird und es für Dritte zugänglich ist. Anknüpfungspunkt ist hier meist das „In-den-Mund-legen" politischer Statements und das Erfinden von Vorkommnissen.

Wenn ein Deepfake dazu benutzt wird, um Taten zu „gestehen", die nie passiert sind, kann das eine Strafbarkeit gemäß § 164 StGB – der falschen Verdächtigung – nach sich ziehen.

Deepfakes können auch rassistische und hetzerische Inhalte verbreiten. Hier kommt der Tatbestand der Volksverhetzung nach § 130 StGB in Betracht.

27 Ebd.
28 Lantwin, Deep Fakes – Düstere Zeiten für den Persönlichkeitsschutz?, MMR 2019, 574, 576; Deutscher Bundestag Wissenschaftliche Dienste, Kurzinformation – Regulierung von Deepfakes, WD-7-015-24.
29 Kumkar/Rapp, Deepfakes, ZfDR 2022, 199, 207.
30 https://www.kriminalpolizei.de/downloads/Kripo_4_2019.pdf, S. 9

2.3.2. Strafbarkeit nach KUG

Nach § 33 KUG macht sich strafbar (Freiheitsstrafe bis zu einem Jahr oder Geldstrafe), wer ein Bildnis entgegen §§ 22, 23 KUG verbreitet oder öffentlich zur Schau stellt (siehe dazu bereits oben Ziffer 3.1.).

2.3.3. Strafbarkeit nach dem Urheberrechtsgesetz

Darüber hinaus kommt eine Strafbarkeit nach § 106 UrhG wegen unbefugter Verwertung urheberrechtlich geschützter Werke und nach § 108 UrhG wegen unbefugter Eingriffe in verwandte Schutzrechte in Betracht (Freiheitsstrafe bis zu drei Jahren oder Geldstrafe), wenn Deepfakes ungenehmigt urheberrechtliche geschützte Werke oder Leistungen verwenden.

2.4. Kennzeichnungspflicht im Medienstaatsvertrag

Im § 18 des Medienstaatsvertrag (MStV) ist darüber hinaus eine Kennzeichnungspflicht von mittels Computer automatisiert erstellten Inhalten statuiert, wenn diese zu einer Identitätstäuschung führen können:[31]

„Anbieter von Telemedien in sozialen Netzwerken sind verpflichtet, bei mittels eines Computerprogramms automatisiert erstellten Inhalten oder Mitteilungen den Umstand der Automatisierung kenntlich zu machen, sofern das hierfür verwandte Nutzerkonto seinem äußeren Erscheinungsbild nach für die Nutzung durch natürliche Personen bereitgestellt wurde."

Dies kann insbesondere Social Bots in sozialen Netzwerken betreffen. Da aber alle Imitationen erfasst werden, die auf einem vollständig automatisierten Vorgang beruhen, wie er z. B. von einer künstlichen Intelligenz gesteuert werden kann,[32] kann dies auf für KI generierte Deepfakes relevant sein.

2.5. Problematik der Durchsetzbarkeit

Ein großes Problem bei strafrechtlichen Vergehen durch oder mit Hilfe von Deepfakes ist die Durchsetzung der rechtlichen Ansprüche. Plattformen, auf denen Deepfakes verbreitet werden, sind oft schwer zur Verantwortung zu ziehen, die Identität der Ersteller oder Verbreiter bleibt oft anonym. Da sich Inhalte im Internet außerdem schnell verbreiten können, ist es oft nicht möglich effektiv gegen Deepfakes vorzugehen oder diese aus dem Verkehr zu ziehen.

Dem Anspruch auf Auskunft zur Identität kommt daher eine besondere Bedeutung zu. In Bezug auf Anbieter digitaler Dienste ergibt sich ein solcher aus § 21 Abs. 2 TDDDG (vormals TTDSG), sofern die Auskunftserteilung zur Durchsetzung zivilrechtlicher Ansprüche wegen der Verletzung absolut geschützter Rechte aufgrund rechtswidriger audiovisueller Inhalte oder aufgrund von Inhalten, die bestimmte Tatbestände des StGB erfüllen und nicht gerechtfertigt sind, erforderlich ist. Insbesondere aufgrund des aufwendigen Verfahrens – der Anspruch setzt eine gerichtliche Anordnung voraus – und der vagen Aussicht auf Vollstreckung zivilrechtlicher Ansprüche gegenüber etwa im Ausland ansässige Verletzende, dürften viele Betroffene vor einer Geltendmachung zurückschrecken.

3. Zwischenfazit

Trotz des Fehlens spezifischer gesetzlicher Regelungen zum Verbot oder zur Strafbarkeit von Deepfakes unterliegen die manipulativen Inhalte bereits jetzt verschiedenen rechtlichen Normen. Sowohl auf EU- als auch auf nationaler Ebene existieren zahlreiche Gesetze, die auf Deepfakes anwendbar sein können. Die aktuelle Rechtslage ist dabei einigermaßen komplex und erfordert eine genaue Prüfung des jeweiligen Deepfakes im Einzelfall.

31 BeckOK InfoMedienR/Lent MStV § 18 Rn. 13-22.
32 BeckOK InfoMedienR/Lent MStV § 18 Rn. 13-22.

4. Aktuelle Entwicklungen

Aktuell wird ein gemeinsamer Gesetzentwurf des Bundesrates, der vom Land Bayern (Gesetzesantrag Bayern vom 14.05.24) erarbeitet wurde, diskutiert.[33] Die Bundesregierung bzw. das BMJ weisen auf die relativ weite Fassung und mögliche Probleme hinsichtlich der Bestimmtheit der vorgeschlagenen gesetzlichen Regelung hin. Ebenfalls hat es den Anschein, dass sie neben den bestehenden Regelungen die Schaffung einer Strafvorschrift nicht in jedem Fall für zwingend halten. Allerdings bleibt die weitere Entwicklung hier abzuwarten.[34]

Somit lohnt sich eine Beschäftigung mit dem Gesetzentwurf und den darin angestrengten Maßnahmen.

Laut der Gesetzesbegründung erfassen die bestehenden, über mehrere Regelungswerke verteilten, Regelungen die problematische Nutzung von Deepfakes nur in Teilaspekten und der Unrechtsgehalt von Deepfakes würde bisher nicht erfasst. Geplant ist daher aktuelle die Einführung der folgenden Regelung ins StGB (Hervorhebungen durch Verfasser):

§ 201b – Verletzung von Persönlichkeitsrechten durch digitale Fälschung

(1) 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, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Gleiches gilt, wenn sich die Tat nach Satz 1 auf eine verstorbene Person bezieht und deren Persönlichkeitsrecht dadurch schwerwiegend verletzt wird.

(2) Wer in den Fällen des Absatzes 1 Satz 1 den Medieninhalt der Öffentlichkeit zugänglich macht oder einen Medieninhalt zugänglich macht, der einen Vorgang des höchstpersönlichen Lebensbereichs zum Gegenstand hat, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(3) Absatz 1 Satz 1, auch in Verbindung mit Absatz 2, gilt nicht für Handlungen, die in Wahrnehmung überwiegender berechtigter Interessen erfolgen, namentlich der Kunst oder der Wissenschaft, der Forschung oder der Lehre, der Berichterstattung über Vorgänge des Zeitgeschehens oder der Geschichte oder ähnlichen Zwecken dienen.

(4) Die Bild- oder Tonträger oder andere technische Mittel, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden. § 74a ist anzuwenden.

4.1. Grundlegendes zum Entwurf

Der Gesetzesentwurf sieht in seiner Begründung durch Deepfakes insbesondere das Persönlichkeitsrecht verletzt. Daneben liege in nicht offengelegten Manipulationen eine falsche Tatsachenbehauptung über die betreffende Person.[35]

Der Gesetzentwurf solle primär einen Schutz des Persönlichkeitsrechts im Strafrecht darstellen, der bisher so nicht gegeben sei. Deepfakes würden auch zunehmend durch Straftäter für missbräuchliche Ziele eingesetzt und es wird angenommen, dass Deepfakes in Zukunft noch einfacher und günstiger zu erstellen seien und sich die Anzahl der Angriffe mit Deepfakes erhöhen werde. Auf den Einsatz des Strafrechts könne daher nicht verzichtet werden.[36] Der Unrechtsgehalt von Deepfakes, der insbesondere im Aspekt einer verfälschenden, aber zugleich authentisch wirkenden Darstellung zentraler Persönlichkeitsmerkmale liege[37], würde durch die aktuellen Regelungen nicht erfasst. Die Relevanz für die Persönlichkeitsentfaltung sei ansonsten sonst nur in Teilaspekten, nämlich z. B. in Form der Stimme oder des Abbilds geschützt. Bloße Kennzeichnungspflichten, wie sie im Wesentlichen in der KI-Verordnung enthalten sind, würden für den Schutz nicht genügen.[38]

Die Problemstellung und der Bedarf einer Regelung für Deepfakes sind im Gesetzentwurf umfangreich erläutert. Eine weitergehende Auseinandersetzung mit den bestehenden Ansprüchen aufgrund der Verletzung des APR, sowie ein detailliertes Eingehen darauf, warum dies eine strafrechtliche Regelung in dieser Form sein muss, finden sich in der Begründung hingegen nicht.

33 Gesetzentwurf des Bundesrates: Entwurf eines Gesetzes zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes, Drucksache 224/24, 05.07.24, im Folgenden „Gesetzentwurf".
34 BT-Drucksache 20/12605, Anl.: Stellungnahme der BRg, 21.08.2024.
35 Vgl. Gesetzentwurf S. 2.
36 Ebd.
37 Vgl. Gesetzentwurf Anlage 1 S. 13.
38 Vgl. Gesetzentwurf S. 2.

4.2. Ausgestaltung und Notwendigkeit

Entscheidend ist, nicht zuletzt aufgrund des „ultima ratio"-Prinzips einer Strafbarkeitsregelung, die Form, in der Deepfakes definiert und abgegrenzt werden. Die Formulierung der Regelung legt einen recht weiten Anwendungsbereich nahe:

Der Gesetzentwurf führt die Bezeichnung „Medieninhalt" als Begriff ein. Dieser wird als Bestandteil der Definition von Deepfakes für die Reichweite der Regelung von Bedeutung sein und ist in Abgrenzung mit den ansonsten bestehenden Definitionen von Deepfakes zu sehen. Es leuchtet jedoch nicht auf Anhieb ein, warum neben einer gerade – europaweit – geltenden, neu eingeführten Definition eine weitere, bereichsspezifische Definition vonnöten sein soll. Zudem besteht hier die Gefahr von Uneinheitlichkeit und Unklarheiten.

Ebenso wird der Begriff „Anschein erwecken" als Tatbestandsmerkmal genutzt. In der Gesetzesbegründung wird erläutert, dass es um solche Deepfakes gehen soll, die „Eindruck einer authentischen Aufnahme vermitteln".

Auch dieses Merkmal dürfte, je nach Lesart, etwas über die bestehenden Definitionen hinausgehen. Es wird zu überlegen sein, ob damit ein ausreichend klares Tatbestandsmerkmal gegeben ist, welches die Anforderungen an strafrechtliche Regelungen erfüllt und wodurch sich ein entsprechend weiter Anwendungsbereich begründet. Je nach dem Verständnis der Formulierung mag dies hier sogar weiter gefasst sein als die bisherigen Definitionen (insb. In der KI-Verordnung).

Die Regelung soll eine Persönlichkeitsverletzung voraussetzen. Damit wäre zumindest eine Eingrenzung auf nur rechtsverletzende Deepfakes gegeben und theoretisch ausgeschlossen, dass auch Deepfakes mit keinem oder nur sehr geringem Verletzungspotential für die Rechte von Personen unter Strafe gestellt würden.

Schwierigkeiten scheinen hinsichtlich der Reichweite der Strafbarkeit möglich, da das Vorliegen einer Persönlichkeitsverletzung mitunter eine nicht von vornherein klar abgrenzbarer Frage ist und eine strafrechtliche Regelung eine hinreichend klare Regelung erfordert. Dies spiegelt sich auch in dem bereits von der Bundesregierung thematisierten Bestimmtheitsgebot für Gesetze, dessen Einhaltung wegen der Offenheit des APRs fraglich sein kann.[39]

Sofern dies kritisch gesehen wird, könnten gewisse Konkretisierungen der Tatbestandsmerkmale, wie eine engere Formulierung des „Anschein Erweckens" oder zusätzliche Voraussetzungen neben einer Persönlichkeitsverletzung, etwa durch subjektive Merkmale oder besonders schwere Formen von Verletzungen, erwogen werden.

Zudem wird nicht ganz deutlich, inwieweit genau diese Eingrenzung nicht bereits durch andere Vorschriften, wie oben beschrieben, bereits abgedeckt ist. So könnte sich gegebenenfalls eine „Überregulierung" ergeben, die gerade im strafrechtlichen Bereich rechtsstaatlich fragwürdig wäre.

Zudem dürfte sich die Herausforderung der praktischen Durchsetzbarkeit (siehe dazu oben 2.4) zumindest in Teilen auch im Bereich des Strafrechts fortsetzen. Allein die Schaffung eines neuen Straftatbestands dürfte noch nicht die Herausforderungen im Zusammenhang mit der der Verfolgung und Durchsetzbarkeit erledigen.

5. Fazit und Ausblick

Die aktuell fehlende allgemeine Strafbarkeit von Deepfakes, vor allem in risikoreichen Umfeldern wie der Politik, wird auch in der juristischen Literatur als Argument für einen neuen Straftatbestand gesehen.[40] Die Motivation für eine wirksame Regelung und das Streben nach einer effektiveren Eingrenzung ungewollter und schädigender Nutzungen von Deepfakes kann daher vollständig nachvollzogen werden. Insbesondere mit Blick auf die Bereiche, in denen keine strafrechtliche Regelung besteht und wo zivilrechtliche Ansprüche nur sehr schwer durchsetzbar sind, scheint die Einführung von angemessenen Strafvorschriften für entsprechende Fälle sinnvoll. Für die Frage der Notwendigkeit der Regelung in gegebener Form ist entscheidend, inwieweit die vorhandenen Regelungen bereits als ausreichend angesehen werden können. Hierauf nimmt die Gesetzbegründung umfassend Bezug und stellt insbesondere fehlende oder zu schwache Regelungen für bestimmte Teilbereiche in den Vordergrund (s.o.).

Wesentlich zu berücksichtigen ist dabei, dass bestimmte, wenn auch zivilrechtliche Anspruchsgrundlagen grundsätzlich vorhanden sind, diesbezüglich, aber nicht unerhebliche Probleme bei der Durchsetzung bestehen (s. 2.4). Sofern man davon ausgeht, dass nicht alle Deepfakes strafrechtlich relevant sind oder sein sollten, ist zu fragen, ob der von den bisherigen Regelungen nicht erfasste „Unrechtsgehalt" von Deepfakes allgemein genügt, um eine Strafvorschrift zu fordern, die allgemein alle Arten von Deepfakes erfassen kann. Dagegen spräche, wenn die Strafbarkeit für die speziellen Fälle, für die schon aktuelle Strafvorschriften bestehen und die zivilrechtlichen Ansprüche für die übrigen Fälle genügen würden. Dem

39 BT-Drucksache 20/12605, Anl.: Stellungnahme der BReg, 21.08.2024.
40 Vgl. Erdogan, Scholz-Deepfake – bewusste Falschinformation zu politischen Zwecken, MMR 2024, 379.

scheint der Entwurf zumindest damit zu begegnen, dass eine Strafbarkeit auf Deepfakes mit persönlichkeitsverletzendem Charakter eingegrenzt wird. Dies ist nachvollziehbar.

Im Ergebnis dürfte die vorgeschlagene Regelung so eine weitergehende Strafbarkeit als die bestehenden Regelungen bewirken. Zumindest wenn damit eine erhöhte Durchsetzbarkeit bei klar problematischen Manipulationen erreicht würde, spräche dies dafür. Inwieweit dies im Einzelnen der Fall ist und ob eine strafrechtliche Regelung in dieser Form als notwendig und vertretbar zu sehen oder Anpassungen der Regelung notwendig sind, bleibt der weiteren Abstimmung vorbehalten.

6. Quellenverzeichnis

Becker, C.R., Kommentar zur Cyber-Rights-Entwicklung, CR 2024, 353, 364.
BeckOK DatenschutzR/Bäcker, 48. Ed. 1.8.2023, DS-GVO Art. 2 Rn. 18, beck-online.
Bundesverband Digitale Wirtschaft (BVDW), „Deepfakes – Eine Einordnung", abrufbar unter: https://www.bvdw.org/wp-content/uploads/2024/07/2024_BVDW_Deepfakes.pdf?highlight=2024 (zuletzt abgerufen am [Datum]).
BVerfG, Urteil vom 24. Mai 2005, NJW 2005, 3271, 3272.
BVerfG, Urteil vom 24. Mai 2005, NJW 2005, 3271, 3273.
Deutscher Bundestag Wissenschaftliche Dienste, Kurzinformation – Regulierung von Deepfakes, WD-7-015-24.
Erdogan, Scholz-Deepfake – bewusste Falschinformation zu politischen Zwecken, MMR 2024, 379.
Gesetzentwurf des Bundesrates: Entwurf eines Gesetzes zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes, Drucksache 224/24, 05.07.24.
Kabinettsache 20/07165, Bundesregierung Deutschland, Entwurf eines Gesetzes zur Regelung von Deepfakes, Berlin 2024.
Kumkar, P., Rapp, M., Deepfakes, ZfDR 2022, 199ff.
Lantwin, S., Deep Fakes – Düstere Zeiten für den Persönlichkeitsschutz?, MMR 2019, 574, 576.
Lennartz, A., „Digitale Puppenspieler" – die Nachbildung von Körper und Stimme durch KI, NJW 2023, 3543, 3544.
MAH UrhR, § 12 (Verfassungs-)Rechtliche Grundlagen der Wort- und Bildberichterstattung Rn. 47, beck-online.
Lantwin: Deep Fakes – Düstere Zeiten für den Persönlichkeitsschutz?, MMR 2019, 574 ff., beck-online.
Fezer/Büscher/Obergfell, Lauterkeitsrecht: UWG, Band1, Presse im WettbewerbsR, Rn. 87ff.,
Koreng: Das „Unternehmenspersönlichkeitsrecht" als Element des gewerblichen Reputationsschutzes, GRUR 2010, 1065ff.

Autoren

Dr. Alexander Hogertz
LL.M. (Cardozo), Rechtsanwalt/Partner, Fachanwalt für Urheber- und Medienrecht, Fachanwalt für IT-Recht,
Hogertz Rechtsanwälte PartmbB

Dr. Marian Klingebiel
Rechtsanwalt, Senior Legal Counsel, ePrivacy GmbH

Fritz-Ulli Pieper
LL.M., Rechtsanwalt / Fachanwalt für Informationstechnologierecht, Taylor Wessing Partnerschaftsgesellschaft mbB

Bundesverband Digitale Wirtschaft (BVDW) e.V.

Der Bundesverband Digitale Wirtschaft (BVDW) e.V. ist die Interessenvertretung für Unternehmen, die digitale Geschäftsmodelle betreiben oder deren Wertschöpfung auf dem Einsatz digitaler Technologien beruht. Als Impulsgeber, Wegweiser und Beschleuniger digitaler Geschäftsmodelle vertritt der BVDW die Interessen der Digitalen Wirtschaft gegenüber Politik und Gesellschaft und setzt sich für die Schaffung von Markttransparenz und innovationsfreundlichen Rahmenbedingungen ein. Sein Netzwerk von Experten liefert mit Zahlen, Daten und Fakten Orientierung zu einem zentralen Zukunftsfeld. Neben der DMEXCO und dem Deutschen Digital Award richtet der BVDW eine Vielzahl von Fachveranstaltungen aus. Mit Mitgliedern aus verschiedensten Branchen ist der BVDW die Stimme der Digitalen Wirtschaft.

Ressort Künstliche Intelligenz

Die gewinnbringende und verantwortungsvolle Nutzung von künstlicher Intelligenz (KI) in der deutschen digitalen Wirtschaft steht im Fokus der Ressortarbeit. Ziel ist es, Fragen rund um die Veränderungen der Wertschöpfungskette der digitalen Wirtschaft zu beantworten und Lösungsansätze für die ethischen, sozialen und rechtlichen Herausforderungen durch KI zu bieten, um eine nachhaltige und positive Auswirkung auf die Gesellschaft, Wirtschaft und Umwelt sicherzustellen.

BVDW Kontakte

Katharina Jäger, Leiterin Innovation & Technology, jaeger@bvdw.org
Janek Kuberzig, Public Affairs Manager Data & Technology, kuberzig@bvdw.org

Bundesverband Digitale Wirtschaft (BVDW) e.V.
Schumannstraße 2, 10117 Berlin
www.bvdw.org