Deepfakes im VideoIdent-Verfahren: (fehlende) Straf- und zivilrechtliche Konsequenzen für Täter

Simone Salemi[1], Bianca Steffes[2]

Abstract: Der Einsatz des sogenannten VideoIdent-Verfahrens zur Authentifzierung im Videochat erfreut sich wachsender Beliebtheit bei Banken und Versicherungen. Nach erfolgter Legitimation wird der Zugang zu neu eröffneten Bankkonten freigeschaltet. Gleichzeitig führen Fortschritte im Bereich des Deep Learnings dazu, dass Manipulationen von Videos mittels sogenannter Deepfakes kaum mehr erkennbar sind. Dieser Beitrag widmet sich der Frage, ob Deepfakes eine reale Gefahr für die Sicherheit des VideoIdent-Verfahrens darstellen und wie der Einsatz rechtlich zu bewerten ist.[3]

Keywords: Deepfakes; Authentifizierung; VideoIdent

1 Problemstellung

Die Manipulation von Videos stellt mit heute gängigen technischen Mitteln selbst für Laien keine große Herausforderung mehr dar. Mittels sogenannter *Deepfakes* können täuschend echte Fälschungen erstellt werden, die mit dem bloßen Auge kaum mehr erkennbar sind. Dem Einsatz von Deepfakes sind indes nur wenige Grenzen gesetzt. Zu denken wäre an den Einsatz im VideoIdent-Verfahren, welches inzwischen von mehreren Banken (vgl. [Co], [IN]) zur Authentifizierung mittels Videochat genutzt wird. Nach erfolgter Legitimation kann bspw. ein Girokonto eröffnet werden. Betrachtet man dieses Verfahren nun unter Berücksichtigung der Manipulationsmöglichkeiten durch den Deepfake-Einsatz, erscheint es alles andere als sicher. Dass sich eine Person etwa der Identität einer anderen bedient, um ein Konto auf deren Namen zu eröffnen, ist durchaus vorstellbar. Überzieht diese Person nun besagtes Konto, bleibt der Bank als Ansprechpartner nur die Person, als die sich der Täter ausgegeben hat. In diesem beispielhaften Szenario werden also gleich mehrere Beteiligte geschädigt, da sowohl die Person, deren Identität sich der Täter angeeignet hat, als auch die Bank betroffen sind. Aus technischer Sicht ist zu klären, ob der Deepfake-Einsatz im VideoIdent-Verfahren realistisch umsetzbar ist. Rechtliche Regelungen, die speziell auf den Einsatz von Deepfakes zugeschnitten sind, existieren derweil nicht. Zu prüfen ist daher, inwieweit die existierenden Regelungen sich auf den beschriebenen Fall anwenden lassen.

[1] Saarbrücker Zentrum für Recht und Digitalisierung, Campus C3.1, 66123 Saarbrücken, Deutschland, simone.salemi@zrd-saar.de

[2] Universität des Saarlandes, Lehrstuhl für Rechtsinformatik, Saarland Informatics Campus, 66123 Saarbrücken, Deutschland, bianca.steffes@uni-saarland.de

[3] Dieser Beitrag wurde durch das Projekt „Digitale Präsenz bei Gericht“ (BMJ) inspiriert.

doi:10.18420/inf2022_53

2 Technische Grundlagen

In einem ersten Schritt soll nun erläutert werden, was genau Deepfakes aus technischer Sicht sind und auf welchen technischen Methoden sie basieren. Im weiteren Verlauf soll bewertet werden, ob das einleitend beschriebene Szenario in Betracht des heutigen Stands der Technik als realistisch einzustufen ist. Der Ursprung des Begriffs „Deepfake“ ist im Jahr 2017 zu verordnen, in dem auf der Plattform reddit.com ein Nutzer mit dem Namen „deepfakes“ begann, mehrere Deepfake-Videos zu posten (bspw. bei [Sa17]). In diesen Videos wurden die Gesichter der Darsteller durch die von bekannten Persönlichkeiten ausgetauscht. Dies beschreibt eine der möglichen Ausprägungen von Deepfakes: das *Face Swapping*. Neben dem reinen Austauschen eines Gesichts in einem Bild oder Video können Deepfakes aber auch Sprachartefakte sein, die eine Person nie gesprochen hat, oder auch komplett neue Videos, in denen Mimik und Kopfbewegungen von Personen vollkommen nach Belieben gesteuert werden können (*Face Reenactment*). Zhang [Zh22] fasst die Menge an möglichen Deepfakes aus dem Englischen übersetzt als „realistisch wirkende aber unechte Bild-, Audio-, Video- und weitere digitale Medien, die durch KI-Methoden und insbesondere deep learning erstellt wurden“ zusammen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet auf seiner Webseite [22b] detaillierte Informationen zu den verschiedenen Arten von Deepfakes an. Für den Anwendungsfall von Deepfakes im VideoIdent-Verfahren ist es theoretisch ausreichend, mittels Deepfakes ein Face Reenactment zu erreichen.

2.1 Zugrundeliegende Technologien

Die Erstellung von Deepfake-Videos ist ein Resultat der intensiven Forschung im Bereich der Computergrafik. Entgegen des ursprünglichen Vorgehens in der Computergrafik, die das konkrete Modellieren von Szenen umfasst, wird hier ein statistisches Lernen aus realem Bildmaterial durch Verfahren des maschinellen Lernens umgesetzt. Wie auch schon vom Begriff „Deepfake“ angedeutet, kommen hier Techniken aus dem Bereich des *deep learnings* zum Einsatz. Dabei handelt es sich um eine Unterklasse des maschinellen Lernens, die auf mehrschichtigen neuronalen Netzen basiert (im Detail bei LeCun et al. [LBH15]). Diese neuronalen Netze imitieren die Funktionsweise des Gehirns und bestehen dementsprechend aus einer Menge an untereinander verknüpften Neuronen, die in aufeinander folgenden Schichten oder auch *layers* angeordnet sind. Schichten, welche die Eingaben des Algorithmus' erhalten, werden *input layers* genannt, Schichten, welche das Ergebnis liefern, sind *output layers*. Dazwischenliegende Schichten, die nicht von außen ersichtlich sind, heißen *hidden layers*. Die Neuronen in den layers führen dabei die Berechnungen aus und geben ihre Ergebnisse an die mit ihnen verbundenen Neuronen weiter. Die Parameter der Berechnungen lernen sie dabei ohne das Zutun von Menschen (dazu ausführlich LeCun et al. [LBH15]). Im Bereich der Computergrafik haben sich neuronale Netze vor allem aufgrund der Fortschritte um *Convolutional Neural Networks (CNNs)* und *Generative Adversarial Networks (GANs)* durchgesetzt (näheres bei Tewari et al. [Te20]). CNNs ermöglichen es, mehrere zusammenhängende Datenpunkte (etwa

nebeneinanderliegende Pixel) gemeinsam zu betrachten und somit Kontextinformationen zu erfassen. So können Linien oder auch komplexe Objekte erkannt werden. Ursprünglich waren CNNs jedoch nur auf Klassifikationen ausgelegt und konnten keine neuen Inhalte generieren. Daher werden sie in der Computergrafik zumeist in der Kombination mit den von Vaswani et al. [Va17] vorgeschlagenen *Transformers* und GANs verwendet. GANs beschreiben ein Vorgehen für einen insgesamten Lernprozess. Sie wurden erstmals von Goodfellow et al. [Go14] vorgestellt und beschreiben eine Art und Weise, wie (content-) generierende neuronale Netze erstellt werden können. Das Vorgehen umfasst dabei einen Generator, der den neuen Content (wie bspw. ein Deepfake-Video) erstellt und einen Diskriminator, der versucht, zwischen echtem und generiertem Content zu unterscheiden. Durch stufenweises abwechselndes Verbessern der Parameter versucht der Diskriminator einerseits, immer besser zwischen echten und unechten Daten zu unterscheiden, und der Generator andererseits, den Diskriminator bestmöglich zu überlisten.

2.2 Deepfake-Videos im VideoIdent-Verfahren

Dass Deepfake-Videos von hoher Qualität auch außerhalb der Forschung weit verbreitet sind, haben Pu et al. [Pu21] in ihrer Studie belegt. Dort überprüfen sie auch die Performance von State-of-the-Art-Methoden zum Erkennen von Deepfakes auf von Laien erstellten Videos. Sie stellen fest, dass diese Methoden nur mäßig erfolgreich sind. Hinzu sollte hier bedacht werden, dass in dieser Studie nur Deepfake-Videos betrachtet wurden, die offensichtlich als solche gekennzeichnet waren. Damit ist nicht auszuschließen, dass eine Reihe von Videos von noch höherer Qualität unerkannt blieb, da diese Videos nicht ausgezeichnet waren und vielleicht auch nicht als Deepfake erkennbar waren. Ihre Studie beweist jedoch, dass theoretisch die Möglichkeit für Laien besteht, echt wirkende Deepfake-Videos ohne großen Aufwand zu erstellen und zu nutzen. Bekannte Beispiele sind das Open-Source-Projekt DeepFaceLab [22a], welches aufgrund seiner Bandbreite an Möglichkeiten recht komplex ist, und Zao [22d] als mobile Anwendung, die recht einfach zu benutzen ist. Wichtig ist anzumerken, dass diese Anwendungen noch keine Deepfakes in Echtzeit produzieren können. Nichtsdestotrotz zeigt ihre weite Verbreitung, dass derartige Software von Personen ohne detailliertes Wissen über die Erstellung von Deepfakes genutzt werden kann und die Möglichkeit des Erstellen von Deepfake-Videos in Echtzeit lediglich davon abhängt, wann eine derartige Anwendung der breiten Masse zur Verfügung gestellt wird. Als Lernmaterial und somit Voraussetzung für die Erstellung von Deepfake-Videos benötigen diese Verfahren teilweise nur ein kurzes Video, wie bei Kim et al. [Ki18] oder auch Thies et al. [Th18]. Andere Verfahren schaffen es sogar, nur anhand von ein paar oder auch nur eines einzigen Fotos realistische Videos zu erstellen wie bspw. bei Zakharov et al. [Za19] und Averbuch-Elor et al. [Av17] zu sehen. Zudem wird für diese Ergebnisse keine besonders teure oder seltene Hardware benötigt, wie Thies et al. ([Th16], [Th18]) zeigt. Dort wird auch bewiesen, dass Verfahren zur Erstellung von qualitativ hochwertigen Deepfakes mit handelsüblicher Hardware in Echtzeit möglich ist. Kim et al. [Ki18] zeigen zudem, dass nicht nur der Kopf, sondern bspw. auch der komplette Oberkörper manipuliert werden kann.

Deepfake-Videos von Personen und vor allem deren Köpfen haben jedoch auch Grenzen in ihrer Realitätsnähe. Während die hier vorgestellten Verfahren die ursprünglichen Probleme der korrekten Darstellung der Blickrichtung (bspw. bei Kim et al. [Ki18]) und des Mundes (z. Bsp. bei Thies et al. [Th16]) lösen, bleiben immer noch einige Aspekte der Ungenauigkeit in den erstellten Videos. Unter anderem seltene oder außergewöhnliche Körperhaltungen führen zu unrealistischen Ergebnissen und die Darstellung von Hautfalten bspw. an den Mundwinkeln erfolgt oftmals noch nicht vollkommen korrekt (bspw. bei [Th18] zu sehen). Andererseits können auch (Bart-) Haare zu einer Verschlechterung der Ergebnisse führen (exemplarisch bei [Th16] gezeigt). Zudem kann die erzeugte Auflösung der Videos auch von der Trainingszeit und der zur Verfügung stehenden Rechenleistung beschränkt werden, wie bei Kim et al. [Ki18] zu sehen. In Anbetracht des dauerhaften Fortschritts der Technik ist jedoch nicht auszuschließen, dass diese kleineren Probleme ebenfalls bald gelöst werden können. Bei der Nutzung von Deepfakes im VideoIdent-Verfahren kann aber auch eine Zielperson gewählt werden, die für diese Dinge weniger anfällig ist (bspw. kurze Haare oder kein Bart). Zudem könnte eine verminderte Videoqualität im Kontext eines Videoanrufs sowie weitere Kleinigkeiten (bspw. ungenaue Darstellung von Hautfalten) auch mit einer schlechten Internetverbindung begründet werden. Weiterhin ist wohl davon auszugehen, dass Videoanrufe im VideoIdent-Verfahren größtenteils ohne technische Unterstützung zur Erkennung von Deepfakes durchgeführt werden und es somit alleine den Mitarbeitern der VideoIdent-Anbieter obliegt, Deepfake-Videos zu erkennen. Betrachten diese die Videos nicht ausgiebig oder detailliert genug, auf einem zu kleinen Fenster oder wissen nicht, welche Anzeichen auf ein Deepfake-Video hinweisen, ist nicht zu erwarten, dass effektiv Fälschungen dieser Art erkannt werden. Die Tatsache, dass Deepfake-Videoanrufe auf dem heutigen Stand der Technik tatsächlich Personen täuschen können, hat u.a. das BSI [21] betont, indem es bestätigt, dass im Berichtszeitraum mehrere europäische Politiker einer Täuschung durch Deepfakes in einem Videoanruf zum Opfer gefallen sind, und auch die Agentur der Europäischen Union für Cybersicherheit (ENISA) [22c] sieht die Gefahr von Deepfakes in der Videoidentifikation als realistisch an. Anzumerken ist hier, dass für die Authentifizierung im VideoIdent-Verfahren ordnungsgemäß ebenfalls der Personalausweis vor der Kamera gezeigt werden muss. Der ENISA [22c] zufolge ist jedoch auch das digitale Fälschen des Personalausweises mitsamt der Lichtspiegelungen und Muster, die das Fälschen des physischen Personalausweis verhindern sollen, durch Deepfakes möglich.

3 Rechtliche Einordnung

Wie gesehen, handelt es sich bei der Nutzung von Deepfakes bei der Authentifizierung um ein realistisches Szenario. Fraglich sind jedoch die rechtlichen Konsequenzen.

3.1 Verletzung des allgemeinen Persönlichkeitsrechts

In Betracht kommt eine Verletzung des allgemeinen Persönlichkeitsrechts (APR). Dieses findet im Rahmen mittelbarer Drittwirkung bei Streitigkeiten zwischen Privatpersonen

über zivilrechtliche Generalklauseln Anwendung ([Gs22], *Hermann*, § 823 BGB Rn. 1659). Das APR steht nicht explizit im Grundgesetz der Bundesrepublik Deutschland, sondern wird aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG hergeleitet ([He21], *Di Fabio*, Art. 2 GG Rn. 128). Gewährleistet und geschützt wird durch das APR die engere persönliche Lebenssphäre ([JK20], *Jarass*, Art. 2 GG, Rn. 36a). Der Schutzbereich des APRs als von der Rechtsprechung entwickeltes Recht ergibt sich aus der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) ([MPS22], *Schmidt*, Art. 2 GG Rn. 34). Laut dem BVerfG ist der Schutzbereich nicht abschließend umschrieben, sondern es werden Fallgruppen entwickelt ([Bu86], 1860). Eine der Fallgruppen stellt das Recht am eigenen Bild dar; so hat jeder das Recht, selbst darüber zu entscheiden, wie er in der Öffentlichkeit dargestellt werden will ([Bu05], 3272). Der Einzelne erhält Einfluss- sowie Entscheidungsmöglichkeiten hinsichtlich der Erstellung und Verbreitung von Fotografien durch andere Personen ([Bu00], 1022), wobei auch der Schutz vor der Verbreitung von technisch manipulierten Bildern, die den Anschein eines authentischen Abbildes einer Person erwecken, umfasst ist ([Bu05], 3272). Die Herstellung von Deepfakes berührt daher den Schutzbereich des APRs. Dieser ist verletzt, soweit (wie im vorliegenden Fall) der Eingriff nicht gerechtfertigt werden kann. Das Recht am eigenen Bild ist auch einfachgesetzlich in den §§ 22, 23 KUG geregelt (vgl. hierzu: Abschnitt 3.2.4). Eine weitere Fallgruppe des APRs ist das Namensrecht. Da der Name einer Person Ausdruck ihrer Individualität und Identität ist, kann sie verlangen, dass er durch die Rechtsordnung geschützt wird ([Bu07], 671). Das Namensrecht besitzt ebenfalls eine zivilrechtliche Anspruchsgrundlage: § 12 BGB ([St21], *Mansel*, § 12 BGB Rn. 1,vgl. hierzu Abschnitt 3.2.1). Neben dem Recht am eigenen Bild sowie dem Namensrecht ist an dieser Stelle noch auf das Recht auf informationelle Selbstbestimmung zu verweisen, wonach auch das Recht darauf, selbst über die Preisgabe und Verwendung personenbezogener Daten zu entscheiden, vom APR geschützt wird ([Bu84], 422).

3.2 Zivilrechtliche Ansprüche

Im Folgenden werden die zivilrechtlichen Ansprüche geprüft, die die Person, deren Aussehen imitiert wurde, gegenüber dem Täter geltend machen kann.

3.2.1 Anspruch aus der Verletzung des Namensrechts, § 12 BGB

Die erste Rechtsgrundlage, aus der sich ein Unterlassungs- oder Beseitigungsanspruch ergeben könnte, ist § 12 BGB (Namensrecht). Verletzt ist das Namensrecht gemäß § 12 BGB dann, wenn die Rechte des Berechtigten durch unbefugten Gebrauch seines Namens durch einen anderen verletzt werden, § 12 S. 1 BGB (unbefugte Namensanmaßung). Da sich der Verwender des Deepfakes hier der Identität einer anderen Person ohne Nutzungsrecht bedient, ist der Anspruch gemäß § 12 BGB gegeben.

3.2.2 Unterlassungsanspruch aus § 1004 BGB in Verbindung mit dem APR

Auch § 1004 BGB gewährt als quasi-negatorischer Abwehranspruch Beseitigungs- und Unterlassungsansprüche für die Beeinträchtigung absoluter Rechte ([SS19], *Volkmann*, § 1004 BGB Rn. 1). Zu den *absoluten Rechten* in diesem Sinne gehört insbesondere auch das oben beschriebene APR und damit auch das Recht am eigenen Bild ([Bu06], 208). Die Verletzung des Rechts am eigenen Bild führt bei Vorliegen der sonstigen Voraussetzungen des § 1004 BGB zu einem Unterlassungs- bzw. Beseitigungsanspruch ([Ga20], *Raff*, § 1004 BGB Rn. 37 f.).

3.2.3 Schadensersatzanspruch aus § 823 Abs. 1 BGB

§ 823 Abs. 1 BGB ist ein deliktischer Anspruch und gewährt Schadensersatz für Rechtsgutsverletzungen, die durch eine unerlaubte Handlung eingetreten sind. Aus dem Wortlaut des § 823 Abs. 1 GG geht hervor, dass für widerrechtliche Verletzungen der in Abs. 1 explizit aufgezählten Rechtsgüter oder von sonstigen Rechten Schadensersatz zu zahlen ist. Zu den *sonstigen Rechten* gehören u.a. einzelne Persönlichkeitsrechte ([St21], *Teichmann*, § 823 BGB, Rn. 12), wozu das Recht am eigenen Bild (§ 22 KUG) sowie das Namensrecht (§ 12 BGB) zählen ([St21], *Teichmann*, § 823 BGB, Rn. 13; [Ha20], *Wagner*, § 823 BGB, Rn. 416; [HP22], *Förster*, § 823 BGB, Rn. 159). Um einen Anspruch aus § 823 Abs. 1 BGB zu begründen, bedarf es einer rechtswidrigen Verletzung eines dieser Rechte durch eine vorsätzliche oder fahrlässige Verletzungshandlung ([Gs22], *Spindler*, § 823 BGB, Rn. 70 ff.). Im Falle der Nutzung von Deepfakes bei der Authentifizierung im VideoIdent-Verfahren liegt eine vorsätzliche Verletzung des Rechts am eigenen Bild sowie des Namensrechts vor. Einzig fraglich ist hier die *Rechtswidrigkeit* der Verletzungshandlung. Anders als bei der Verletzung der in § 823 Abs. 1 BGB ausdrücklich genannten Rechte, wird bei der Verletzung des APRs die Rechtswidrigkeit nicht durch die Tatbestandsmäßigkeit indiziert ([Gs22], *Specht-Riemenschneider*, § 823 BGB, Rn. 1461). Der Eingriff in den Schutzbereich des APRs ist nur dann rechtswidrig, wenn die schutzwürdigen Interessen des Verletzten überwiegen ([Bu14], 696 Rn. 22) (positive Feststellung der Rechtswidrigkeit, ([Gs22], *Specht-Riemenschneider*, § 823 BGB, Rn. 1461 f.)). In dem hier betrachteten Fall fällt diese Abwägung eindeutig zugunsten des Verletzten aus: Dessen Recht am eigenen Bild bzw. Namensrecht wurde aus verwerflichen Motiven verletzt. Die Interessen des Deepfakes-Verwenders sind indes schon gar nicht schutzwürdig, weshalb dem Verletzten hier ein Anspruch auf Schadensersatz zusteht.

3.2.4 Schadensersatzanspruch aus einer Schutzgesetzverletzung, § 823 Abs. 2 BGB

Ein Schadensersatzanspruch könnte sich auch aus § 823 Abs. 2 BGB ergeben. § 823 Abs. 2 BGB fordert die zurechenbare Verletzung eines sogenannten Schutzgesetzes

([Gs22], *Spindler*, § 823 BGB, Rn. 255). Ein Schutzgesetz ist gemäß § 823 Abs. 2 S. 1 BGB ein Gesetz, welches den Schutz eines anderen bezweckt. Als Schutzgesetz kommen hier sowohl § 22 KUG, als auch möglicherweise verwirklichte Straftatbestände in Frage. Da die Verwirklichung der Straftatbestände unter Abschnitt 3.3 geprüft wird, soll der Fokus dieses Abschnitts auf § 22 KUG liegen. Das KUG wird vorliegend aufgrund der Öffnungsklausel aus Art. 85 Abs. 1 DSGVO als anwendbar betrachtet, obwohl das Verhältnis von DSGVO und KUG sich weiterhin im Diskurs befindet (Vgl. hierzu:[KW19]). § 22 KUG ist als Schutzgesetz in diesem Sinne anerkannt ([HP22], *Förster*, § 823 BGB, Rn. 291 m.w.N.). Laut § 22 KUG dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Bildnisse sind Darstellungen von Personen, die deren äußere Erscheinung in einer für Dritte erkennbaren Weise wiedergeben ([LLO20], *Götting*, § 22 KUG Rn. 14). Im vorliegenden Fall bestehen keine Zweifel daran, dass ein Bildnis verwendet wird: Der Täter will den Eindruck erwecken, dass die abgebildete Person handelt. Deren Darstellung ist also das ausgemachte Ziel des Täters. Problematisch erscheint jedoch die erforderliche Handlung, um § 22 KUG zu erfüllen. § 22 KUG verbietet nämlich nur die Verbreitung sowie die öffentliche Zurschaustellung des Bildnisses; die schlichte Herstellung fällt nicht unter § 22 KUG. Zwar wird vom „Verbreiten“ jegliche Art der Verbreitung erfasst. Jedoch ist erforderlich, dass der Verbreitende die Kontrolle darüber verliert, inwieweit das Bildnis an die Öffentlichkeit gelangt ([LLO20], *Götting*, § 22 KUG, Rn. 36). Die öffentliche Zurschaustellung ist die Sichtbarmachung des Bildnisses im weitesten Sinne ([LLO20], *Götting*, § 22 KUG Rn. 37), das Bildnis muss der Öffentlichkeit zur Verfügung gestellt werden. Beide Varianten erscheinen hier nicht erfüllt. Wird das Foto lediglich gegenüber dem Angestellten einer Bank zur Authentifizierung verwendet, handelt es sich zwar durchaus um eine Verletzung des APRs — § 22 KUG ist hingegen nicht verletzt. Damit einher geht auch, dass eine Strafbarkeit nach § 33 KUG nicht in Betracht kommt.

3.3 Strafrechtliche Aspekte

Bei der strafrechtliche Bewertung ist zwischen Straftaten, die an die Nutzung des Deepfakes im VideoIdent-Verfahren als Tathandlung anknüpfen, und denen, die anschließendes Verhalten unter Strafe stellen, zu unterscheiden.

3.3.1 Betrug, § 263 StGB

In Betracht käme vorliegend die Verwirklichung eines Betrugs gemäß § 263 Abs. 1 StGB. Der Betrug könnte hier sowohl *gegenüber* einem Bankangestellten und *zulasten* einer dritten Person (deren Identität verwendet wurde) als auch *gegenüber* eines Bankangestellten und *zulasten* der Bank verwirklicht worden sein. Ein Betrug liegt vor, wenn durch die Vorspiegelung falscher Tatsachen oder die Entstellung oder Unterdrückung wahrer Tatsachen bei einer anderen Person ein Irrtum erregt oder unterhalten wird und dadurch das Vermögen eines anderen beschädigt wird. Dabei muss der Täter in der Absicht handeln, sich oder

einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen. Mit einer Täuschung über Tatsachen möchte der Täter auf die Vorstellungskraft des Gegenübers einwirken und ihn dadurch in die Irre führen, wobei die Täuschung sowohl durch positives Tun (auch durch schlüssiges Verhalten) als auch durch Unterlassen verwirklicht werden kann ([LHK18], *Kühl*, § 263 StGB Rn. 6 ff.). Zu *Tatsachen* im Sinne des § 263 StGB gehören alle Zustände und Geschehnisse der Vergangenheit und der Gegenwart, die dem Beweis zugänglich sind ([KNP17], *Kindhäuser*, § 263 StGB Rn. 73), auch die Identität einer Person ([He22a], *Hefendehl*, § 263 StGB, Rn. 99). Setzt eine Person also im VideoIdent-Verfahren Deepfakes ein, um über ihre Identität zu täuschen, ist jedenfalls eine tatbestandliche Täuschung gegeben. Soweit das Gegenüber von der Richtigkeit der vorgetäuschten Identität ausgeht, erliegt es auch dem erforderlichen Irrtum, also einer Fehlvorstellung über Tatsachen ([Sc19], *Perron*, § 263 StGB Rn. 32a). Problematisch könnte vorliegend jedoch das ungeschriebene Tatbestandsmerkmal der Vermögensverfügung sein. Eine Vermögensverfügung wird als jedes Tun, Dulden oder Unterlassen des Getäuschten definiert, welches sich *unmittelbar* vermögensmindernd beim Getäuschten oder einem Dritten auswirkt ([Bu60], 1069). Dabei ist zwingend erforderlich, dass Getäuschter und Verfügender identisch sind. („Dreiecksbetrug“ ([He22b], *Beukelmann*, § 263 Rn. 34)). Hier ist jedoch fraglich, ob überhaupt eine Vermögensverfügung vorliegt. Selbst wenn nach erfolgter Authentifizierung der Zugriff auf ein Bankkonto ermöglicht würde, wird hiermit noch keine Vermögensminderung ausgelöst. Zu einer Minderung des Vermögens käme es erst durch ein weiteres Verhalten des Täters — wenn dieser bspw. den Dispokredit überzieht — *und* der Bank - wenn diese sich an den vermeintlichen Kontoinhaber wegen etwaiger Ansprüche wendet. Der Betrug ist ein *Selbstschädigungsdelikt*, was bedeutet, dass die Vermögensschädigung unmittelbar durch ein Handeln des Opfers ([He22b], *Beukelmann*, § 263 StGB, Rn. 32) erfolgt. Die Unmittelbarkeit ist zu verneinen, wenn durch die Handlung des Getäuschten lediglich Zugriffsmöglichkeiten des Täters erhöht werden und dieser damit die Möglichkeit erhält, durch eigenständige Schritte eine Vermögensverschiebung auszulösen ([He22b], *Beukelmann*, § 263 StGB Rn. 32). Zwar können auch mehraktige Geschehen zu einem Betrug führen, essentiell ist jedoch, dass die Handlung, durch die die Vermögensverschiebung ausgelöst wird, auch vom Getäuschten vollzogen wird ([KNP17], *Kindhäuser*, § 263 StGB, Rn. 202). Dies ist hier jedoch nicht der Fall. Erforderlich sind weitere Handlungen des Täters selbst, was schon dem Selbstschädigungscharakter des Betruges widerspricht. Ein Betrug und damit auch ein Schadensersatzanspruch aus § 823 Abs. 2 BGB i.V.m. § 263 StGB sind mithin nicht verwirklicht.

3.3.2 Geldwäsche, § 261 StGB

Ferner könnte hier der Straftatbestand der Geldwäsche verwirklicht worden sein. Gemäß § 261 Abs. 1 StGB macht sich strafbar, wer einen Gegenstand, der aus einer in § 261 Abs. 1 S. 2 StGB näher bezeichneten rechtswidrigen Tat herrührt, verbirgt, dessen Herkunft verschleiert oder die Ermittlung der Herkunft, das Auffinden, die Einziehung oder die Sicherstellung eines solchen Gegenstandes vereitelt oder gefährdet. Es bedarf mithin

eines *Gegenstandes*, der aus einer rechtswidrigen Tat herrührt. Unter einem Gegenstand in diesem Sinne ist jeder Vermögensgegenstand, der seinem Inhalt nach bewegliche oder unbewegliche Sachen oder Rechte umfasst, zu verstehen ([Bu15], 3254 Rn. 4). Ausgangspunkt des Gegenstandsbegriff ist § 90 BGB, wonach Sachen nur körperliche Gegenstände sind ([Sa21], *Neuheuser*,§ 261 StGB Rn. 35). Durch den Deepfake-Einsatz im VideoIdent-Verfahren kann zwar ein Konto eröffnet werden, einen vermögenswerten Gegenstand erhält der Täter dadurch jedoch wohl nicht. Selbst wenn man den Erhalt eines vermögenswerten Gegenstandes aufgrund des Erhalts von Zugangsdaten zu einem Konto bejahen wollte, so mangelt es an der Katalogstraftat gemäß § 261 Abs. 1 S. 2 StGB, aus der dieser „Gegenstand" herrührt. Der Täter macht sich hier also nicht der Geldwäsche gemäß § 261 Abs. 1 StGB schuldig.

3.3.3 Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen, § 201a StGB

Im Rahmen der rechtlichen Bewertung der Verwendung von Deepfakes wird häufig auf die Strafnorm des § 201a StGB verwiesen ([La19], 576; [Th21], 204; [La20], 79), welche die Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen unter Strafe stellt. Die Herstellung des Deepfakes ist von § 201a StGB indes nicht erfasst: Die Nachbearbeitung von Bildern bzw. computergenerierte Bilder fallen nicht unter den Begriff der „Bildaufnahme" in diesem Sinne ([Sc19], *Eisele*, § 201a StGB, Rn. 6; [La20], 79), womit eine Strafbarkeit nach § 201a Abs. 1 StGB ausscheidet. Jedoch ist § 201a Abs. 2 StGB regelmäßig bei der Verbreitung pornographischer Deepfakes erfüllt ([La20], 79). Dieser Fall unterscheidet sich jedoch vom hier betrachteten Szenario: Hier werden keine Fotos verbreitet, die dazu geeignet sind, das Ansehen des Abgebildeten erheblich zu beeinträchtigen. Dies ist bei einem pornographischen Deepfakes naturgemäß anders zu bewerten. Werden Deepfakes jedoch zur Authentifizierung im VideoIdent-Verfahren genutzt, kommt keine Strafbarkeit nach § 201a Abs. 2 StGB in Betracht.

3.3.4 Datenschutzrechtliche Strafvorschrift, § 42 Abs. 2 BDSG

Neben den angeprüften und abgelehnten Delikten kommt für die Handlung des Täters ferner die Verletzung datenschutzrechtlicher Vorschriften und damit einhergehend die Erfüllung der datenschutzspezifischen Strafnorm des § 42 BDSG in Betracht. Zu beachten ist, dass es sich gemäß § 42 Abs. 3 S. 1 BDSG um ein absolutes Antragsdelikt handelt ([KB20], *Bergt*, § 42 BDSG Rn. 56). Eine Tat im Sinne des § 42 Abs. 1 oder Abs. 2 BDSG wird also stets nur auf Antrag der betroffenen Person, des Verantwortlichen, des Bundesbeauftragten oder der Aufsichtsbehörde verfolgt. Erfüllt sein könnte hier der § 42 Abs. 2 Nr. 1 BDSG. § 42 Abs. 1 BDSG ist indes nicht gegeben, da die verwendeten Daten weder einer großen Anzahl an Personen zugänglich gemacht werden, noch ohne Weiteres von einem gewerbsmäßigen Handeln des Täters auszugehen ist. § 42 Abs. 2 Nr. 1 BDSG stellt die unrechtmäßige

Verarbeitung nicht allgemein zugänglicher personenbezogener Daten gegen ein Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, unter Strafe. Personenbezogene Daten sind, im Einklang mit Art. 4 Nr 1 DSGVO ([BW22], *Brodowski/Nowak*, § 42 BDSG Rn. 22), alle Informationen, die sich auf identifizierte oder identifizierbare Personen beziehen. Hierzu zählen bspw. auch die Gesichtszüge einer Person ([La20], 80). Der Begriff der Datenverarbeitung nach Art. 4 Nr. 2 DSGVO geht indes sehr weit: So ist jegliches datenschutzrelevantes Verhalten hiervon erfasst ([KB20], *Bergt*, § 42 BDSG Rn. 32). Daher fällt hierunter sowohl die Speicherung des Ausgangsmaterials als auch die Deepfake-Herstellung und auch -Verwendung ([La20], 80). Da im vorliegenden Fall auch von der erforderlichen Bereicherungsabsicht zu eigenen Gunsten auszugehen ist, erscheint die Verwirklichung von § 42 Abs. 2 Nr. 1 BDSG hier durchaus denkbar. Insbesondere ist nicht erforderlich, dass sich der Vermögensvorteil unmittelbar aus der Tathandlung ergibt ([KB20], *Bergt*, § 42 BDSG, Rn. 49). Einzig problematisch erscheint das Tatbestandsmerkmal der Zugänglichkeit. Daten sind im Sinne des § 42 Abs. 2 Nr. 1 BDSG öffentlich zugänglich, wenn sie von jedermann wahrgenommen werden können, ohne dass es rechtliche Beschränkungen gibt ([KB20], *Bergt*, § 42 BDSG Rn. 8). Nicht öffentlich zugänglich sind beispielsweise Fotos, die auf dem privaten Social-Media-Profil geteilt werden ([La20], 80). Anders ist dies jedoch zu bewerten, wenn das Social-Media-Profil ohne Anmeldung öffentlich abrufbar ist ([KB20], *Bergt*, § 42 BDSG Rn. 9). Nimmt der Täter daher Fotos und den Namen, die auf einer technisch nicht besonders geschützten Webseite ([KB20], *Bergt*, § 42 BDSG Rn. 9) veröffentlicht sind, entzieht er sich der Strafbarkeit. Hinweise auf der Webseite, dass die Fotos nicht verwendet werden dürfen oder dass der Zugriff bestimmten Personen vorbehalten ist, sind dabei unbeachtlich ([KB20], *Bergt*, § 42 BDSG Rn. 9; [BW22], *Brodowski/Nowak*, § 42 BDSG Rn. 26). Betrachtet man die Fülle an teils hochwertigen Fotos auf öffentlich und ohne Anmeldung verfügbaren *Instagram*-Profilen, dürfte es ein leichtes Unterfangen sein, öffentlich zugängliche Fotos zu verwenden. Werden hingegen private Fotos und Informationen genutzt, ist eine Strafbarkeit gemäß § 42 Abs. 2 Nr. 1 BDSG gegeben, wodurch auch ein Anspruch auf Schadensersatz in Verbindung mit § 823 Abs. 2 BGB entsteht.

3.3.5 Urkundenfälschung, § 267 StGB, Datenveränderung, § 303a StGB und Vorbereiten des Ausspähens und Abfangens von Daten, § 202c StGB

Da ein Personalausweis als Urkunde anzusehen ist ([Sc19], *Heine/Schuster*, § 267 StGB Rn. 44), könnte eine Urkundenfälschung, § 267 StGB, in der Veränderung von Name und Lichtbild auf dem im VideoIdent-Verfahren vorgezeigten Ausweis liegen. Es ist jedoch zu beachten, dass durch die vorübergehende Bearbeitung des Personalausweises kein physisches Dokument hergestellt wird, somit zu keinem Zeitpunkt eine unechte Urkunde vorliegt und mithin auch keine Urkundenfälschung (siehe hierzu: [Bu11], 214). Einer Datenveränderung nach § 303a StGB macht sich schuldig, wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert. Unter der *Veränderung* wird in diesem Sinne jede inhaltliche Umgestaltung von gespeicherten Daten, die mit einer

Funktionsbeeinträchtigung verbunden ist ([HH19], *Wieck-Noodt*, § 303a StGB Rn. 15), verstanden. Damit erscheint das Handeln des Täters im hier beschriebenen Szenario bereits nicht tatbestandsmäßig: So werden hier keine *gespeicherten* Daten verändert. Auch bei Nutzung eines bereits existierenden Bildes des Opfers wird der Informationsgehalt der Daten nicht abgeändert. Eine Datenveränderung nach § 303a Abs. 1 StGB liegt daher nicht vor. § 202a StGB stellt das Ausspähen von Daten, § 202c StGB entsprechende Vorbereitungshandlungen unter Strafe. Da der Täter im Erfolgsfall ein Passwort erhalten könnte, welches auf den Namen einer anderen Person läuft, könnte § 202c Abs. 1 Nr 1 StGB verwirklicht sein. Jedoch bleibt zu beachten, dass der Täter selbst wenn er ein Passwort oder Online-Banking-Zugangsdaten erhalten sollte, keinen Zugang zu Daten einer anderen Person erhält, womit auch diese Straftatbestände ausscheiden.

3.3.6 Strafbarkeit anschließender Handlungen des Täters

Betrachtet man als Tathandlung nicht die Verwendung der Deepfakes im VideoIdent-Verfahren, sondern anschließende Handlungen des Täters, so kommt eine Strafbarkeit wegen Betruges, § 263 StGB oder wegen Computerbetruges, § 263a StGB in Betracht. Die 3. Variante des § 263a StGB (die unbefugte Verwendung von Daten) könnte der Verwender dann verwirklichen, wenn er das eröffnete Konto bspw. durch Einkäufe in Onlineshops unter Nutzung von Online-Banking-Daten überzieht. Um einen Computerbetrug zu realisieren, müsste er durch die unbefugte Verwendung von Daten einen Datenverarbeitungsvorgang beeinflussen und dadurch das Vermögen einer anderen Person schädigen ([He22a], *Hefendehl/Noll*, § 263a StGB Rn. 20). Die unbefugte Verwendung von Daten liegt nach der herrschenden betrugsnahen Auslegung des § 263a Abs. 1 Var. 3 StGB vor, wenn der Berechtigte oder ein Dritter getäuscht würden, wenn der Täter jene Daten ihm gegenüber verwenden würde ([MR20], *Altenhain*, § 263a StGB Rn. 12). Da der Täter sich als andere Person ausgibt und damit über seine Identität täuscht, kann man von einer Täuschung ausgehen. Die Überziehung eines fremden Kontos durch Online-Bestellungen ist auch einer der anerkannten Fälle des Computerbetrugs ([MR20], *Altenhain*, § 263a StGB Rn. 16). Geschädigt ist in diesen Fällen dann regelmäßig der Berechtigte. Einen Betrug könnte der Täter realisieren, wenn er eine erhaltene Bankkarte verwendet, um Geld abzuheben oder um eine Zahlung zu tätigen. Im vorliegenden Fall besteht jedoch ein Unterschied zu sonst gängigen Fällen: Zwischen der Bank und dem „Berechtigten“, also der Person, deren Identität verwendet wurde, gab es nie Kontakt. Mangels wirksamer Stellvertretung durch den Täter kann man hier auch nicht davon ausgehen, dass eine Vertragsbeziehung zustande gekommen ist. Da für eine Bank der Name und die Identität des Gegenübers von Relevanz ist, ist auch kein Vertrag mit dem Täter selbst zustande gekommen. Ein Schaden des Berechtigten liegt mithin gar nicht vor: Da sein eigenes Konto nicht überzogen wurde und auch keine vertragliche Beziehung zwischen ihm und der Bank zustande kam, treffen ihn keine Ansprüche und sein Vermögen ist nicht gemindert. In Frage kommt also nur ein Betrug zulasten der Bank, die hier wohl mangels Ansprechpartner den erlittenen Schaden nicht ausgleichen kann. Ein Computerbetrug gemäß § 263a Abs. 1 Var. 3 StGB

könnte hier also ebenso wie ein Betrug nach § 263 StGB erfüllt sein und mit ihm auch ein Schadensersatzanspruch gemäß § 823 Abs. 2 BGB i.V.m. dem jeweiligen Straftatbestand.

4 Fazit

Im Verlaufe dieses Beitrags wurde aufgezeigt, dass Deepfakes Ergebnisse des deep learning sind und auf neuronalen Netzen basieren und ihre Produktion auch unter Laien weit verbreitet und leicht zugänglich ist. Zudem ist es technisch möglich, qualitativ hochwertige Deepfake-Videos in Echtzeit mithilfe weniger Fotos oder eines kurzen Videos zu erstellen, wobei keine besonders teure oder aufwändige Hardware benötigt wird. In Bezug auf die Anwendbarkeit im VideoIdent-Verfahren bedeutet dies, dass eine Nutzung von Deepfake-Videos zu unlauteren Zwecken ein durchaus realistisches Szenario darstellt. Rechtlich gesehen würde der Einsatz eines Deepfake-Videos im VideoIdent-Verfahren eine Verletzung des Allgemeinen Persönlichkeitsrechts der imitierten Person bedeuten, woraus Beseitigungs- und Unterlassungsansprüche sowie Schadensersatzansprüche resultieren. Es hat sich jedoch auch gezeigt, dass die strafrechtliche Einordnung des beschriebenen Szenarios deutlich komplexer ist: So scheitern mehrere Straftatbestände an einzelnen Tatbestandsmerkmalen, insbesondere ist mangels Vermögensverfügung kein Betrug gemäß § 263 StGB gegeben. Einzig der § 42 BDSG erscheint zumindest in Einzelfällen anwendbar, kann aber auch leicht umgangen werden. Es zeigt sich, dass der beim Deepfakes-Einsatz im VideoIdent-Verfahren vorgenommene „Identitätsdiebstahl“ als solcher keine strafrechtlichen Konsequenzen nach sich zieht, was als durchaus problematisch anzusehen ist. Bereits die Eröffnung eines Girokontos kann beispielsweise Auswirkungen auf die persönliche Schufa-Auskunft haben. Daran ändert auch die Tatsache, dass durch spätere Handlungen des Täters ein Computerbetrug verwirklicht werden könnte, nichts.

Dazu bleibt die Problematik des reinen Erkennens von Deepfake-Videos. Die technischen Methoden zur Erkennung von Deepfakes sind noch nicht sehr zuverlässig oder auf die breite Masse anwendbar, da sie stark von dem Erstellungsalgorithmus abhängen (im Detail bei Pu et al. [Pu21]). Auch eine breit angelegte *Deepfake Detection Challenge* [Do20] hat nur einen mäßigen Erfolg der teilnehmenden Algorithmen gezeigt. Dementsprechend bleibt die zuverlässige Erkennung von Deepfakes trotz ihrer weiten Verbreitung ein offenes Problem, welches durch den fehlenden rechtlichen Rahmen bei der Nutzung im VideoIdent-Verfahren nur noch unterstrichen wird und gemeinsam einen akuten Handlungsbedarf auf rechtlicher wie auch auf technischer Seite offenbart.

Literatur

[21] Die Lage der IT-Sicherheit in Deutschland 2021. Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2021.

[22a] DeepFaceLab, 2022, URL: https://github.com/iperov/DeepFaceLab.

[22b] Deepfakes - Gefahren und Gegenmaßnahmen, 2022, URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html.

[22c] Remote Identity Proofing - Attacks and Countermeasures, 2022, URL: https://www.enisa.europa.eu/publications/remote-identity-proofing-attacks-countermeasures.

[22d] ZAO, 2022, URL: https://www.zaoapp.net/.

[Av17] Averbuch-Elor, H.; Cohen-Or, D.; Kopf, J.; Cohen, M. F.: Bringing Portraits to Life. ACM Trans. Graph. 36/6, Nov. 2017, ISSN: 0730-0301, URL: https://doi.org/10.1145/3130800.3130818.

[Bu00] Bundesverfassungsgericht. Neue Juristische Wochenschrift/14, S. 1021–1026, 2000.

[Bu05] Bundesverfassungsgericht. Neue Juristische Wochenschrift/45, S. 3271–3273, 2005.

[Bu06] Bundesverfassungsgericht. Neue Juristische Wochenschrift/4, S. 207–211, 2006.

[Bu07] Bundesverfassungsgericht. Neue Juristische Wochenschrift/10, S. 671–672, 2007.

[Bu11] Bundesgerichtshof. Neue Zeitschrift für Strafrecht/7, S. 213–214, 2011.

[Bu14] Bundesgerichtshof. Gewerblicher Rechtsschutz und Urheberrecht/7, S. 693–702, 2014.

[Bu15] Bundesgerichtshof. Neue Juristische Wochenschrift/44, S. 3254–3255, 2015.

[Bu60] Bundesgerichtshof. Neue Juristische Wochenschrift/23, S. 1068–1069, 1960.

[Bu84] Bundesverfassungsgericht. Neue Juristische Wochenschrift/8, S. 419–428, 1984.

[Bu86] Bundesverfassungsgericht. Neue Juristische Wochenschrift/30, S. 1859–1861, 1986.

[BW22] Brink, S.; Wolff, H. A.: BeckOK Datenschutzrecht. C.H.Beck Verlag, München, 2022.

[Co] Commerzbank: Online-Legitimation, URL: https://www.commerzbank.de/portal/de/privatkunden/hilfe-kontakt/services/online-legitimation/online-legitimation.html, Stand: 19. 04. 2022.

[Do20] Dolhansky, B.; Bitton, J.; Pflaum, B.; Lu, J.; Howes, R.; Wang, M.; Ferrer, C. C.: The DeepFake Detection Challenge (DFDC) Dataset, 2020, URL: https://arxiv.org/abs/2006.07397.

[Ga20] Gaier, R.: Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 8, Sachenrecht §§ 854 - 1296, WEG - ErbbauRG. C.H.Beck Verlag, München, 2020.

[Go14] Goodfellow, I. J.; Pouget-Abadie, J.; Mirza, M.; Xu, B.; Warde-Farley, D.; Ozair, S.; Courville, A.; Bengio, Y.: Generative Adversarial Nets. In: Proceedings of the 27th International Conference on Neural Information Processing Systems - Volume 2. NIPS'14, MIT Press, Montreal, Canada, S. 2672–2680, 2014.

[Gs22] Gsell, B.; Krüger, W.; Lorenz, S.; Reymann Christoph (Gesamthrsg. Zivilrecht); Artz, M.; Ball, W.; Benecke, M.; Geibel, S.; Gsell, B.; Hager, J.; Harke, J. D.; Kessen, M.; Köndgen, J.; Krafka, A.; Krüger, W.; Lobinger, T.; Looschelders, D.; Lorenz, S.; Maurer, H.-U.; Müller-Engels, G.; Reymann, C.; Schindler, W.; Schmidt, H.; Segna, U.; Sprickhoff, A.; Wellenhofer, M.: beck-online.Grosskommentar BGB. C.H.Beck Verlag, München, 2022.

[Ha20] Habersack, M.: Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 7, Schuldrecht - Besonderer Teil IV, §§ 705 - 853. C.H.Beck Verlag, München, 2020.

[He21] Herzog, R.; Scholz, R.; Herdegen, M.; Klein, H.: Grundgesetz Kommentar, Band I, Texte und Art. 1-5. C.H.Beck Verlag, München, 2021.

[He22a] Hefendehl, R.: Münchener Kommentar zum Strafgesetzbuch, Band 5 §§ 263 - 297 StGB. C.H.Beck Verlag, München, 2022.

[He22b] von Heintschel-Heinegg, B.: BeckOK StGB. C.H.Beck Verlag, München, 2022.

[HH19] Hefendehl, R.; Hohmann, O.: Münchener Kommentar zum Strafgesetzbuch, Band 5 §§ 263 - 358 StGB. C.H.Beck Verlag, München, 2019.

[HP22] Hau, W.; Poseck, R.: BeckOK BGB. C.H.Beck Verlag, München, 2022.

[IN] ING: Girokonto, URL: https://www.ing.de/girokonto/konto-eroeffnen/, Stand: 19. 04. 2022.

[JK20] Jarass, H.; Kment, M.: Grundgesetz für die Bundesrepublik Deutschland Kommentar. C.H.Beck Verlag, München, 2020.

[KB20] Kühling, J.; Buchner, B.: Datenschutz-Grundverordnung BDSG - Kommentar. C.H.Beck Verlag, München, 2020.

[Ki18] Kim, H.; Garrido, P.; Tewari, A.; Xu, W.; Thies, J.; Niessner, M.; Pérez, P.; Richardt, C.; Zollhöfer, M.; Theobalt, C.: Deep Video Portraits. ACM Trans. Graph. 37/4, Juli 2018, ISSN: 0730-0301, URL: https://doi.org/10.1145/3197517.3201283.

[KNP17] Kindhäuser, U.; Neumann, U.; Paeffgen, H.-U.: NomosKommentar Strafgesetzbuch. Nomos Verlag, Baden-Baden, 2017.

[KW19] Krüger, S.; Wiencke, J.: Bitte recht freundlich – Verhältnis zwischen KUG und DS-GVO Herstellung und Veröffentlichung von Personenbildnissen nach Inkrafttreten der DS-GVO. Multimedia und Recht/2, S. 76–80, 2019.

[La19] Lantwin, T.: Deep Fakes - Düstere Zeiten für den Persönlichkeitsschutz? Multimedia und Recht/9, S. 574–578, 2019.

[La20] Lantwin, T.: Strafrechtliche Bekämpfung missbräuchlicher Deepfakes - Geltendes Recht und möglicher Regelungsbedarf. Multimedia und Recht/2, S. 78–82, 2020.

[LBH15] LeCun, Y.; Bengio, Y.; Hinton, G.: Deep learning. Nature 521/, S. 436–444, 2015, URL: https://doi.org/10.1038/nature14539.

[LHK18] Lackner, K.; Heger, M.; Kühl, K.: Strafgesetzbuch Kommentar. C.H.Beck Verlag, München, 2018.

[LLO20] Loewenheim, U.; Leistner, M.; Ohly, A.: Urheberrecht Kommentar UrhG - KUG - VGG. C.H.Beck Verlag, München, 2020.

[MPS22] Müller-Glöge, R.; Preis, U.; Schmidt, I.: Erfurter Kommentar zum Arbeitsrecht, Band 51. C.H.Beck Verlag, München, 2022.

[MR20] Matt, H.; Renzikowski, J.: Strafgesetzbuch Kommentar. Verlag Franz Vahlen München, München, 2020.

[Pu21] Pu, J.; Mangaokar, N.; Kelly, L.; Bhattacharya, P.; Sundaram, K.; Javed, M.; Wang, B.; Viswanath, B.: Deepfake Videos in the Wild: Analysis and Detection. In: Proceedings of the Web Conference 2021. WWW '21, Association for Computing Machinery, Ljubljana, Slovenia, S. 981–992, 2021, ISBN: 9781450383127, URL: https://doi.org/10.1145/3442381.3449978.

[Sa17] Samantha Cole, Vice.com: AI-Assisted Fake Porn Is Here and We're All Fucked, 2017, URL: https://www.vice.com/en_us/article/gydydm/gal-gadot-fake-ai-porn, Stand: 29. 03. 2022.

[Sa21] Sander, G. M.: Münchener Kommentar zum Strafgesetzbuch, Band 4 §§ 185 - 262 StGB. C.H.Beck Verlag, München, 2021.

[Sc19] Schönke, A.; Schröder, H.; Eser, A.; Perron, W.; Sternberg-Lieben, D.; Eisele, J.; Hecker, B.; Kinzig, J.; Bosch, N.; Schuster, F.; Weißer, B.; Schittenhelm, U.: Schönke/Schröder Strafgesetzbuch Kommentar. C.H.Beck Verlag, München, 2019.

[SS19] Spindler, G.; Schuster, F.: Recht der elektronischen Medien Kommentar. C.H.Beck Verlag, München, 2019.

[St21] Stürner, R.: Jauernig Bürgerliches Gesetzbuch. C.H.Beck Verlag, München, 2021.

[Te20] Tewari, A.; Fried, O.; Thies, J.; Sitzmann, V.; Lombardi, S.; Sunkavalli, K.; Martin-Brualla, R.; Simon, T.; Saragih, J. M.; Nießner, M.; Pandey, R.; Fanello, S. R.; Wetzstein, G.; Zhu, J.; Theobalt, C.; Agrawala, M.; Shechtman, E.; Goldman, D. B.; Zollhöfer, M.: State of the Art on Neural Rendering. CoRR abs/2004.03805/, 2020, arXiv: 2004.03805, URL: https://arxiv.org/abs/2004.03805.

[Th16] Thies, J.; Zollhöfer, M.; Stamminger, M.; Theobalt, C.; Nießner, M.: Face2Face: Real-Time Face Capture and Reenactment of RGB Videos. In: 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). S. 2387–2395, 2016.

[Th18] Thies, J.; Zollhöfer, M.; Theobalt, C.; Stamminger, M.; Nießner, M.: Headon: Real-Time Reenactment of Human Portrait Videos. ACM Trans. Graph. 37/4, Juli 2018, ISSN: 0730-0301, URL: https://doi.org/10.1145/3197517.3201350.

[Th21] Thiel, M.: „Deepfakes“ - Sehen heißt glauben? - Gefahren, gesetzgeberischer Handlungsbedarf, Konsequenzen für die biometrische Gesichtserkennung. Zeitschrift für Rechtspolitik/7, S. 202–205, 2021.

[Va17] Vaswani, A.; Shazeer, N.; Parmar, N.; Uszkoreit, J.; Jones, L.; Gomez, A. N.; Kaiser, Ł.; Polosukhin, I.: Attention is All You Need. In: Proceedings of the 31st International Conference on Neural Information Processing Systems. NIPS'17, Curran Associates Inc., Long Beach, California, USA, S. 6000–6010, 2017, ISBN: 9781510860964.

[Za19] Zakharov, E.; Shysheya, A.; Burkov, E.; Lempitsky, V.: Few-Shot Adversarial Learning of Realistic Neural Talking Head Models, 2019, arXiv: 1905.08233.

[Zh22] Zhang, T.: Deepfake generation and detection, a survey. Multimedia Tools and Applications 81/, S. 6259–6276, 2022.