Verwendung computergenerierter Kinderpornografie zu Ermittlungszwecken im Darknet[1]

Sandra Wittmer[2] und Martin Steinebach[3]

Abstract: Die Möglichkeiten für Cyberkriminelle, Straftaten mit Hilfe des Internets weitestgehend anonym zu begehen, wachsen mit der Entwicklung neuer Technologien stetig. Ein bekanntes Beispiel hierfür ist das Verbreiten von Kinderpornografie über geschützte Peer-to-Peer Netzwerke wie Tor und Freenet. Seit dem Bekanntwerden der Hintergründe des Amoklaufs vor dem Olympia-Einkaufszentrum in München ist das Darknet als Synonym für solche Netze in den Fokus der öffentlichen Wahrnehmung gerückt. Zuletzt wurde im Rahmen der 89. Konferenz der Justizministerinnen und Justizminister der Länder sogar die Zulassung von computergeneriertem kinderpornografischem Material zur Täterermittlung im Darknet angeregt. Der folgende Beitrag greift den Beschluss der Justizministerkonferenz auf und widmet sich der aktuellen Diskussion, indem auf rechtliche Rahmenbedingungen und technische Möglichkeiten zur Umsetzung eines solchen Vorhabens eingegangen wird.

Keywords: Darknet, Kinderpornografie, Strafverfolgung, Keuschheitsprobe, Computergrafik, Vektorgrafiken.

1 Einleitung

Was die Verbreitung, sowie den Erwerb und Besitz kinderpornografischer Schriften[4] i.S.d. §§ 184b ff. StGB angeht, handelt es sich um einen Kriminalitätsbereich, der in den letzten Jahrzehnten einen grundlegenden Wandel erfahren hat. Während in den Siebzigern vor allem Zeitschriften kursierten und in den Achtzigern Videokassetten ausgetauscht wurden, spielen Trägermedien mit kinderpornografischen Material heute praktisch keine Rolle mehr, da sich die Szene seit den 1990er Jahren zunehmend ins Internet – und schließlich auch ins Darknet – verlagert hat. Für Schlagzeilen sorgte zuletzt die Verurteilung der Betreiber der Kinderpornoplattform „Elysium“, die seit 2016 im Tor-Darknet existierte und zuletzt über 111.000 Mitglieder zählte. Zuvor war es den Ermittlern der Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT) in Gießen gelungen, den Serverstandort der „Elysium“-Seite aufgrund eines Programmfehlers zu lokalisieren. Anders als im Fall von „Elysium“ bleiben die Bemühungen der

[1] Das dieser Veröffentlichung zugrundeliegende Verbundprojekt „Parallelstrukturen, Aktivitätsformen und Nutzerverhalten im Darknet“ (PANDA) wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter den Förderkennzeichen 13N14355 und 13N14356 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autor*innen.
[2] Fraunhofer SIT/TU Darmstadt, Rheinstraße 75, 64295 Darmstadt, sandra.wittmer@sit.fraunhofer.de
[3] Fraunhofer SIT, Rheinstraße 75, 64295 Darmstadt, martin.steinebach@sit.fraunhofer.de
[4] Kinderpornografischen Schriften stehen gem. § 11 Abs. 3 StGB „Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen“ gleich.

doi:10.18420/inf2019_56

Strafverfolger, Serverstandorte von versteckten Diensten im Tor-Netzwerk zu ermitteln, aufgrund der im Darknet gewährleisteten technischen Anonymität von Nutzern und Diensteanbietern jedoch häufig erfolglos. Was Ermittlungen im Bereich der §§ 184b ff. StGB angeht, wird der Einsatz von verdeckt agierenden Beamten daher häufig als einzige Möglichkeit angesehen, in die pädokriminelle Szene vorzudringen. Vor diesem Hintergrund thematisiert der folgende Beitrag die Verwendung von computergenerierter Kinderpornografie zu Ermittlungszwecken im Darknet. Begonnen wird mit einer Einführung in den Phänomenbereich der sogenannten „Keuschheitsproben". Anschließend werden die rechtlichen Rahmenbedingungen für Ermittlungen im Bereich der §§ 184b ff. StGB thematisiert und auf die technischen Möglichkeiten zur Erstellung entsprechenden Materials eingegangen. Schließlich folgt ein Diskussionsteil mit Blick auf mögliche Folgeprobleme, welche die Verwendung von digitalen Missbrauchsabbildungen zu Ermittlungszwecken mit sich bringen könnte.

2 Problem: „Keuschheitsproben" auf Darknet-Plattformen mit kinderpornografischen Inhalten

Um Ermittlungsbeamten den Zugang zu Darknet-Plattformen mit kinderpornografischen Inhalten zu erschweren, wird auf einigen Seiten das Bestehen einer sogenannten „Keuschheitsprobe" gefordert.[5] Wer sich als Nutzer registrieren und am Austausch über die Plattform teilnehmen will, muss zunächst selbst strafbares kinderpornografisches Material zur Verfügung stellen. Dies kann entweder durch einen Upload der Bild- oder Videodateien in ein geschlossenes Forum oder aber durch den Versand an einen Moderator, der den User dann freischaltet, geschehen.[6] Dieser Vorgehensweise auf den Plattformen liegt die Annahme zugrunde, dass Ermittlungsbeamte zur Aufklärung von Straftaten selbst keine Straftatbestände verwirklichen dürfen. Durch das Ablegen von derartigen „Integritätsprüfungen" soll also die Strafverfolgung auf den einschlägigen Plattformen behindert werden. Um für Ermittlungen im Bereich der §§ 184b ff. StGB Abhilfe zu schaffen, wurde im Rahmen der 89. Konferenz der Justizministerinnen und Justizminister der Länder daher die Verwendung von computergeneriertem kinderpornografischem Material zur effektiven Strafverfolgung im Darknet angeregt.[7] Dies sei eine wirksame und zugleich Individualrechtsgüter schonende Methode, die eine erneute Viktimisierung der Opfer durch die Verwendung echten Materials für das Bestehen der „Keuschheitsprobe" vermeiden könnte.[8] Da in der Folgezeit vertreten wurde, dass Ermittlungsbeamte bereits nach geltendem Recht berechtigt sind, virtuelle kinderpornografische Inhalte in

[5] Fiebig, DRiZ 2019, 50 (51).
[6] Gercke, CR 2018, 480 (482, Rn. 13).
[7] Beschluss der 89. Konferenz der Justizministerinnen und Justizminister (TOP II.9), S. 2.
[8] Es gibt in jüngster Zeit Angebote von Opfern, die ihr bereits im Umlauf befindliches Material zu Ermittlungszwecken zur Verfügung stellen würden, wie Eva Kühne-Hörmann etwa in einem Interview mit dem SPIEGEL preisgab, https://www.spiegel.de/panorama/justiz/hessen-justizministerin-fordert-tabubruch-bei-kinderporno-ermittlungen-a-1211011.html. (18.06.2019)

geschlossene Foren im Darknet hochzuladen[9], sollen zunächst die rechtlichen Rahmenbedingungen für Ermittlungen im Bereich der §§ 184b ff. StGB untersucht werden.

3 Rechtliche Rahmenbedingungen für Ermittlungen im Bereich der §§ 184b ff. StGB

In Deutschland gilt – unabhängig davon, ob ein Verdeckter Ermittler i.S.v. § 110a StPO zum Einsatz kommt oder reguläre Ermittlungen i.S.d. §§ 161, 163 StPO stattfinden[10] – der Grundsatz, dass Beamte im Rahmen ihrer Ermittlungstätigkeit nicht berechtigt sind, selbst Straftaten zu begehen. Als Grund werden das Legalitätsprinzip und die andernfalls drohende Erschütterung des Vertrauens der Bevölkerung in die Integrität der Strafverfolgungsbehörden genannt.[11] In anderen Ländern – zum Beispiel in den Niederlanden – liegen die Dinge anders.[12] In der dortigen Strafprozessordnung gilt etwa das Opportunitätsprinzip, sodass von der Verfolgung von Straftaten abgesehen werden kann, wenn dies im öffentlichen Interesse ist.[13] Zudem ist es verdeckt ermittelnden Polizeibeamten in den Niederlanden unter bestimmten Umständen erlaubt, Straftaten zu begehen.[14] Obwohl diese erweiterten Ermittlungsbefugnisse bereits erfolgreich in multinationalen Ermittlungsverfahren mit deutscher Beteiligung eingesetzt wurden[15], lässt die Strafprozessrechtstradition hierzulande eine vollständige Abkehr vom Legalitätsprinzip für den Bereich der verdeckten Ermittlungen wohl nicht zu.[16] Allerdings kennt auch die deutsche Rechtsordnung Ausnahmen von Straftatbeständen für staatliche Behörden. So ist beispielsweise der Umgang mit Betäubungsmitteln nach § 4 Abs. 2 BtMG für diese erlaubnisfrei und nach § 202d Abs. 3 Nr. 1 StGB dürfen Steuer- und Strafverfolgungsbehörden zur Erfüllung ihrer Dienstpflichten mit Daten hehlen.[17] Auch für Ermittlungen im Bereich der Kinderpornografie hat der Gesetzgeber in den letzten Jahren weitgehende tatbestandliche Ausnahmeregelungen geschaffen. So wurde durch das 27. Strafrechtsänderungsgesetz schon 1993 klargestellt, dass sich Ermittlungsbeamte, die im Rahmen ihrer rechtmäßigen Pflichten handeln, weder wegen Besitzes von Kinderpornografie noch dadurch strafbar machen, dass sie einer anderen Person den Besitz verschaffen.[18] Diese gesetzliche Berechtigung zum Besitz und zur Besitzverschaffung wurde bis heute beibehalten und findet sich in § 184b Abs. 5 StGB wieder.[19] Allerdings bezieht sich die Aus-

[9] So etwa Gercke, CR 2018, 480 (484, Rn. 26).
[10] Gercke, CR 2018, 480 (482, Rn. 11.); Für Verdeckte Ermittler ist dies in RiStBV Anl.D II 2.2 ausdrücklich geregelt.
[11] Safferling, DRiZ 2019, 206 (207).
[12] Safferling, DRiZ 2019, 206 (207).
[13] Safferling, DRiZ 2019, 206 (207).
[14] Safferling, DRiZ 2019, 206 (207).
[15] So zum Beispiel bei der Übernahme und dem Weiterbetrieb des Darknet-Drogenmarktplatzes „Hansa Market“ durch die niederländischen Behörden, vgl. Safferling, DRiZ 2019, 206 (207).
[16] Safferling, DRiZ 2019, 206 (207).
[17] Safferling, DRiZ 2019, 206 (207).
[18] Gercke, CR 2018, 480 (482, Rn. 12).
[19] Gercke, CR 2018, 480 (482, Rn. 12).

nahmeregelung ausweislich ihres eindeutigen Wortlauts nicht auf § 184b Abs. 1 Nr. 1 StGB, welcher das Verbreiten (Nr. 1 Var. 1) und öffentliche Zugänglichmachen (Nr. 1 Var. 2) kinderpornografischer Schriften normiert. Dahinter steht die Überlegung, dass der Markt für entsprechende Bilder und Videos als solcher „ausgetrocknet" werden soll, um als Reflex den Missbrauch von Kindern zur Herstellung der Bilder zu bekämpfen.[20] Zwar bestehen zu Recht Zweifel daran, ob die Bereitstellung von kinderpornografischen Inhalten in rigoros abgeschirmten Foren im Darknet überhaupt ein „öffentliches Zugänglichmachen" i.S.v. § 184b Abs. 1 Nr. Var. 2 StGB darstellen kann, da es letztlich an einer Wahrnehmbarkeit der Missbrauchsabbildungen durch eine unbestimmte Anzahl an Personen fehlt.[21] Nichtsdestotrotz wird durch das Hochladen solcher Darstellungen die Tatbestandsalternative des Verbreitens aus § 184b Abs. 1 Nr. 1 Var. 1 StGB erfüllt. Auch wenn hierfür ursprünglich eine körperliche Weitergabe der strafbaren Inhalte erforderlich war, hat der BGH aufgrund der Möglichkeit, digitalisierte Daten via Internet auch „unkörperlich" weitergeben zu können, in der Zwischenzeit einen spezifischen Verbreitungsbegriff entwickelt.[22] Ein Verbreiten von Dateien im Internet liegt demnach bereits vor, „wenn die [übertragene] Datei auf dem Rechner des Internetnutzers (…) angekommen ist."[23] Dabei sei unerheblich, ob dieser die Möglichkeit des Zugriffs auf die Datei genutzt habe oder die übertragene Datei auf einem Speichermedium persistiert wird.[24] Da die Tatbestandsalternative des § 184b Abs. 1 Nr. 1 StGB sowohl real- als auch fiktivpornografische Darstellungen umfasst[25], sind computergenerierte Darstellungen vom Verbreitungsverbot ebenso betroffen wie echte Aufnahmen. Es bleibt somit festzuhalten, dass sich Ermittlungsbeamte nach geltender Rechtslage durch das Hochladen von kinderpornografischen Inhalten auf Darknet-Plattformen gem. § 184b Abs. 1 Nr. 1 Var. 1 StGB strafbar machen würden, ohne dass die Ausnahmeregelung des § 184b Abs. 5 StGB greift. Strafverfolgungsbehörden verfügen de lege lata folglich nicht über das erforderliche rechtliche Handwerkszeug, um Zugriff auf abgeschirmte Kinderporno-Tauschbörsen im Darknet zu erhalten.[26]

4 Möglichkeiten der technischen Umsetzung

Sollte de lege ferenda die Verwendung von computergeneriertem kinderpornografischem Material zur Täterermittlung im Darknet ermöglicht werden, stellt sich unweigerlich die Frage nach der Umsetzbarkeit eines solchen Vorhabens. Diese hat in den bisherigen Diskussionen um die Zulassung der „Keuschheitsprobe" jedoch keinerlei Beachtung gefunden. Aus technischer Sicht sind verschiedene Möglichkeiten zur Umsetzung denk-

[20] Safferling, DRiZ 2019, 206 (207).
[21] Gercke, CR 2018, 480 (483, Rn. 12).
[22] Palm, Kinder- und Jugendpornographie im Internet, S. 122.
[23] *BGH*St 47, 55 (58 f.).
[24] Palm, Kinder- und Jugendpornographie im Internet, S. 122.
[25] Palm, Kinder- und Jugendpornographie im Internet, S. 120.
[26] Ebenso Safferling, DRiZ 2019, 206 (207) und Krause, NJW 2018, 679 (680); zu einem anderen Ergebnis kommt Gercke, CR 2018, 480 (484, Rn. 26).

bar, die allesamt auf der Nutzung moderner Ausprägungen der Computergrafik basieren. Die grundlegende Annahme dabei ist, dass bereits heute in Computerspielen und Filmen lebensechte Nachahmungen von Geschehnissen und Personen enthalten sind, die vom Betrachter nicht oder zumindest nicht als störend wahrgenommen werden, obwohl die Inhalte in einer sehr hohen Wiedergabequalität (also mit hoher Auflösung, niedriger Kompressionsstufe und hohen Anzahl an Bildern pro Sekunde) wiedergegeben werden. Was computergenerierte „Keuschheitsproben" angeht, könnte eine niedrigere Qualität (beispielsweise durch Vortäuschen einer Videoverbindung mit niedriger Datenrate, einer Kamera minderer Qualität oder schlechter Lichtverhältnisse) sogar dazu führen, dass dem Betrachter ein Erkennen der künstlichen Natur des Bildmaterials noch schwerer fällt. Einen Beleg hierfür liefert der Fall „Sweetie" aus dem Jahr 2013, im Rahmen dessen ein computergeneriertes Kind erfolgreich als Lockvogel in Videochats mit insgesamt 20.000 Nutzern eingesetzt wurde.[27] Während der Lockvogel betrieben wurde, brachte er insgesamt 1000 Personen dazu, dem vermeintlich zehnjährigen Mädchen aus den Philippinen Geld für sexuelle Handlungen anzubieten. Technisch umgesetzt wurde „Sweetie" durch eine Kombination aus Computergrafik und dem Erfassen von Bewegungen eines menschlichen Darstellers anhand eines Motion Capture-Verfahrens, wodurch eine äußerst realitätsnahe Darstellung erzielt werden konnte. Da in der Zwischenzeit jedoch die Befürchtung geäußert wurde, dass künstlich erzeugte Bild- und Videodateien für Täter relativ leicht als Fälschungen zu erkennen seien[28], soll im folgenden Abschnitt auf die verschiedenen denkbaren Ansätze zur Erzeugung solchen Materials eingegangen werden.

4.1 Vektorgrafiken

Die einfachste Variante wäre es, analog zu Computerspielen ein Modell eines Kindes zu erstellen. Solche werden üblicherweise durch ein Drahtgittermodell in Kombination mit Texturen realisiert. Eine Unterstützung zum Erreichen eines höheren Realismus wird in Computerspielen durch Photogrammetrie[29] ermöglicht. Hier wird aus einer Vielzahl von Fotografien ein 3D Modell eines Objektes, einer Landschaft oder einer Person erstellt. Um dem Modell natürliche Bewegungen zu ermöglichen, werden menschliche Bewegungen mit Sensoren erfasst[30] oder aus Bilddaten abgeleitet.[31] Gebräuchliche Bezeichnung hierfür ist der englische Begriff Motion Capture. Im engeren Sinn handelt es sich

[27] https://www.bbc.com/news/uk-24818769, Computer-generated 'Sweetie' catches online predators, Angus Crawford, BBC News

[28] So etwa der Vorsitzende des Bunds Deutscher Kriminalbeamter Sebastian Fiedler, http://www.spiegel.de/panorama/justiz/kinderporno-ermittler-sollen-computergenerierte-bilder-nutzen-duerfen-a-1211706.html (08.04.2019).

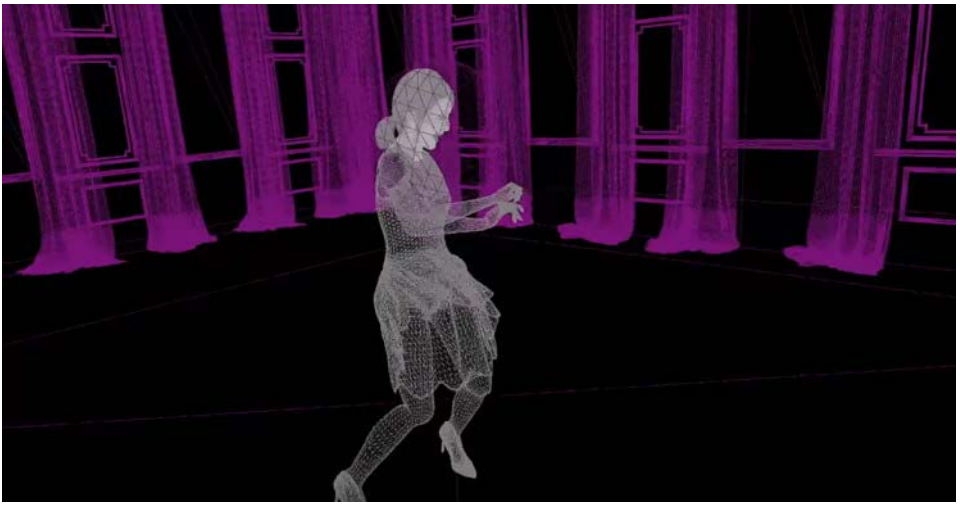
[29] Kraus, K. (2012). Photogrammetrie: Geometrische Informationen aus Photographien und Laserscanneraufnahmen. Walter de Gruyter.

[30] Vlasic, D., Adelsberger, R., Vannucci, G., Barnwell, J., Gross, M., Matusik, W., & Popović, J. (2007, August). Practical motion capture in everyday surroundings. In ACM transactions on graphics (TOG) (Vol. 26, No. 3, p. 35). Acm.

[31] Moeslund, T. B., & Granum, E. (2001). A survey of computer vision-based human motion capture. Computer vision and image understanding, 81(3), 231-268.

hierbei aber nur um das Erfassen von Bewegungen des Körpers. Die detaillierte Erfassung von Gesichtsausdrücken wird unter dem Begriff Performance Capture[32] beschrieben. Aktuelle SDKs für Computerspiele erlauben hierbei bereits fotorealistische Darstellungen von Personen, wenn die Bewegungen von Schauspielern mittels Motion Capture gesteuert werden. Die künstliche Person „Siren“, die als Demonstration für die Unreal 4 Engine eingesetzt wird, zeigt dies deutlich.

Abb. 1: Standbild der künstlichen Person „Siren“ aus dem Unreal YouTube Channel[33]



[32] Cao, C., Bradley, D., Zhou, K., & Beeler, T. (2015). Real-time high-fidelity facial performance capture. ACM Transactions on Graphics (ToG), 34(4), 46.
[33] https://www.youtube.com/watch?v=9owTAISsvwk

Abb. 2: Gitterstruktur von „Siren“, aus dem CubicMotion YouTube Channel[34]

4.2 Austausch von Gesichtern

Alternativ zu synthetisch erzeugten Inhalten könnten auch reale Bild- und Videoaufnahmen als Grundlage für das Material verwendet werden. Notwendig hierzu sind erwachsene Darsteller und Darstellerinnen, deren Körper kindlich wirken. Die Gesichter werden dann durch Methoden auf Basis maschinellen Lernens durch das von Kindern ausgetauscht. Ein bekanntes Beispiel hierfür sind die sogenannten DeepFakes, mit denen anhand eines Deep Learning-Verfahrens unter anderem die Gesichter Prominenter auf die Körper von Pornodarstellern und -darstellerinnen montiert wurden.[35] Um bei diesem Ansatz keine Gesichter von realen Kindern verwenden zu müssen, ist der Einsatz von Methoden des maschinellen Lernens denkbar[36], bei welchen Gesichter echter Kinder als Grundlage für die Erzeugung eines künstlichen Gesichts verwendet werden. Wie realitätsnah auf diese Weise künstlich erzeugte Gesichter sind, veranschaulicht die Webseite „thispersondoesnotexist“.[37] Hier werden zufällig von einem Algorithmus mittels maschinellen Lernens erzeugte Portraits gezeigt, die nur schwer von einem echten Menschen unterscheidbar sind. Erkannt werden die künstlichen Personen nur dadurch, dass der Algorithmus derzeit noch Fehler in Details macht, beispielsweise bei Haaransatz oder Augenpaaren. Fehlerhafte Bilder könnten von den Ermittlern allerdings ohne größeren Aufwand aussortiert werden.

[34] https://www.youtube.com/watch?v=zjfAPkAu2zw
[35] Harris, D. (2019). Deepfakes: False Pornography Is Here and the Law Cannot Protect You. Duke Law & Technology Review, 17(1), 99-127.
[36] Huang, R., Zhang, S., Li, T., & He, R. (2017). Beyond face rotation: Global and local perception gan for photorealistic and identity preserving frontal view synthesis. In Proceedings of the IEEE International Conference on Computer Vision (pp. 2439-2448).
[37] https://thispersondoesnotexist.com/

Abb. 3: Beispiel eines künstlichen Portraits erzeugt auf „thispersondoesnotexist.com“

4.3 Vergleich der verschiedenen Ansätze

Die oben aufgeführten Ansätze sind in der Lage, künstliches Bildmaterial zu erzeugen, welches ein Mensch zumindest bei einer flüchtigen Prüfung als „echt“ ansehen oder für eine Fotografie halten würde. Der Aufwand für die Erstellung von Videomaterial ist dabei deutlich höher als für Einzelbilder, da hier neben einer natürlich wirkenden Grafik auch noch eine ebenso natürliche Bewegung erzeugt werden muss. Bei den synthetischen Ansätzen liegt der große Vorteil darin, dass theoretisch beliebig viele künstliche Personen erzeugt werden können. Dies kann potentiell sogar sehr effizient geschehen, da das Aussehen der Personen durch einfache Parameter variiert werden kann. Im Falle von DeepFake-Ansätzen werden allerdings geeignete Körper-Double benötigt, von denen mit hoher Wahrscheinlichkeit nur eine überschaubare Anzahl existiert.

4.4 Forensische Erkennung

Aus Sicht der Multimedia-Forensik[38] sind die genannten Ansätze derzeit als erkennbar einzustufen, da synthetische Bilder von echten Fotografien unterschieden werden können. In Fotografien existieren unvermeidbar verschiedene Typen von Rauschen, die durch die Kameraelektronik verursacht werden und bei synthetisch erzeugtem Material nicht vorhanden sind. DeepFakes basieren wiederum auf Montagen, die Bilder unterschiedlicher Historie zusammenfügen und auch auf Skalierungen der Bildelemente angewiesen sind. Beide Ansätze hinterlassen also Spuren, die erkannt werden können. Die Methoden der Multimedia-Forensik stoßen allerdings schnell an ihre Grenzen, wenn ihnen mit Gegenmaßnahmen begegnet wird. Rauschen von echten Fotos lässt sich bis in hohe Details simulieren oder nachträglich von anderen Fotos übertragen[39] und Spuren, die auf Montagen hinweisen, lassen sich durch Weichzeichner oder das leichte Beschneiden des Bildes mit erneuter Kompression verwischen, da hier sowohl Hinweise auf Interpolation als auch die Historie der Kompressionsvorgänge der einzelnen Bildelemente entfernt oder stark geschwächt werden.

5 Diskussion

Obwohl die künstliche Erzeugung von virtuellen Missbrauchsabbildungen aus technischer Sicht also möglich wäre, wirft die Verwendung solchen Materials zu Ermittlungszwecken im Darknet eine Reihe von Folgeproblemen auf, welche im folgenden Abschnitt thematisiert werden sollen.

5.1 Persönlichkeitsrechte der Darsteller

Was künstlich erzeugte Bild- und Videodateien angeht, ist an die Verbindung des computergenerierten Materials zu echten Personen zu denken. Denn lediglich Einzelbilder, die aus Vektorgrafiken erstellt wurden, sind als völlig frei von personenbezogenen Daten einzustufen. Bereits die Animation solcher Vektorgrafiken in einem Video führt jedoch dazu, dass Bewegungsdaten echter Personen hinzugefügt werden. Diese Bewegungsdaten können wiederum biometrisch verwertbare Informationen beinhalten[40], die auf die echten Personen zurückgeführt werden könnten. Sobald Bilder und Videos mittels maschinellem Lernen erzeugt werden, besteht außerdem die Gefahr, dass die neu erzeugten Bilder zu nah an den Vorlagen bleiben und somit erkannt werden können. In der Praxis ist dies allerdings nur bei einer geringen Menge von Trainingsdaten zu erwarten. Das inzwischen bekannte Risiko, dass im Falle von Bildern aus trainierten Netzen die Trai-

[38] Farid, H. (2016). Photo forensics. MIT Press.

[39] Steinebach, M., El Ouariachi, M., Liu, H., & Katzenbeisser, S. (2009, September). On the reliability of cell phone camera fingerprint recognition. In International Conference on Digital Forensics and Cyber Crime (pp. 69-76). Springer, Berlin, Heidelberg.

[40] Balazia, M., & Plataniotis, K. N. (2017). Human gait recognition from motion capture data in signature poses. IET Biometrics, 6(2), 129-137.

ningsbilder wieder in hoher Qualität erstellt werden können, dürfte für das Szenario nicht kritisch sein: Ein System zum Erzeugen künstlicher Kinderpornografie wird nur in einem geschlossenen Kreis von Anwendern verbleiben dürfen, ein Verbreiten der Netze ist dementsprechend unwahrscheinlich. Im Falle von DeepFakes können jedoch auch die Körper der Darsteller und Darstellerinnen erkannt werden. Davon ausgehend, dass es sich hier um volljährige Personen handelt, die professionell Erotikdarstellungen produzieren, ist hier jedoch kein zusätzlicher Verlust an Privatheit zu befürchten.

5.2 Umsetzungsaufwand

Neben den rechtlichen Fragestellungen gilt es hinsichtlich der praktischen Umsetzbarkeit zu erörtern, ob die Erzeugung computergenerierter Kinderpornografie zu Ermittlungszwecken mit einem vertretbaren Aufwand möglich ist. Aus technischer Sicht ist dies zu bejahen – insbesondere in Anbetracht der möglichen Alternativen. Davon ausgehend, dass die „Keuschheitsprobe" nicht umgangen werden kann, ist ein erfolgreiches Bestehen nur mit Bildmaterial möglich, welches den Anforderungen der Gegenseite genügt. Da heute die Computertechnik fortgeschritten genug ist, um entsprechendes Material auf Standardrechnern zu erstellen und mit Motion Capture zu steuern, ist der Aufwand bei der Erstellung vertretbar. Von höherem Aufwand ist hier nur das Erstellen der initialen Modelle, welche gegebenenfalls auch das Mitwirken von Künstlern oder Grafikspezialisten erfordern. Da eine „Keuschheitsprobe" nach unserem Verständnis nicht in Echtzeit abgelegt werden muss, sondern auf gespeichertem Bildmaterial basiert, kann entsprechendes Material an einer zentralen Stelle produziert und den Ermittlern zur Verfügung gestellt werden. Die Anzahl von Fachleuten ist also zeitlich und räumlich begrenzt.

5.3 Befürchteter „Nachahmungseffekt"

Allerdings darf das Thema „Keuschheitsproben" nicht ohne Hinweis auf die Befürchtung diskutiert werden, dass die Verwendung von virtuellen Missbrauchsabbildungen möglicherweise den Schutzzweck des § 184b StGB konterkarieren könnte. Denn dieser beruht auf der Annahme, dass erst der durch die Verbreitung ermöglichte Konsum kinderpornografischer Materialien den Anreiz zu neuen Produktionen liefert – und damit auch den Anreiz zu immer neuem Missbrauch schafft.[41] Obwohl dieser vom Gesetzgeber unterstellte Wirkungszusammenhang bislang nicht empirisch untersucht wurde, kann nicht ausgeschlossen werden, dass der Konsum des von den Ermittlungsbeamten hochgeladenen Materials bei den Betrachtern falsche Normalität suggeriert, eigene Hemmschwellen herabsetzt und diese im schlimmsten Fall darin bestärken könnte, selbst Kinder zu missbrauchen.[42]

[41] Kuhnen, Kinderpornographie im Internet, S. 11.
[42] Kuhnen, Kinderpornographie im Internet, S. 12.

6 Fazit

Die Verwendung von computergenerierter Kinderpornografie zu Ermittlungszwecken im Darknet ist folglich eine zweischneidige Angelegenheit. Einerseits wird sich davon zwar erhofft, dem Markt für Kinderpornografie schaden zu können, indem Teilnehmer der Plattformen aus dem Verkehr gezogen werden und gleichzeitig mit dem vermehrten Auftreten von verdeckten Ermittlern in den bislang als relativ „sicher" geltenden Darknet-Tauschforen gerechnet werden muss.[43] Andererseits kann nicht ausgeschlossen werden, dass das künstlich erzeugte Material einen „Nachahmungseffekt" bei den Konsumenten hervorruft. Hinzu kommt, dass eine empirische Untersuchung, in wie vielen Fällen Ermittlungen im Bereich der §§ 184b ff. StGB de facto an einer „Keuschheitsprobe" scheitern, bislang fehlt.[44] Bevor wissenschaftlich fundierte Erkenntnisse dazu vorliegen, fällt es entsprechend schwer, sich für oder gegen die Verwendung von computergenerierten Missbrauchsabbildungen zu Ermittlungszwecken auszusprechen. Ziel dieser Ausarbeitung kann es dementsprechend nicht sein, sich diesbezüglich eindeutig zu positionieren. Vielmehr soll dieser Beitrag als Grundlage für die Diskussion eines etwaigen Reformvorhabens dienen. Erkenntnisse aus anderen Disziplinen wie beispielsweise der Kriminalpsychologie könnten in Zukunft einen wichtigen Beitrag für die abschließende Klärung der Fragestellung leisten. Feststeht, dass die Erzeugung authentisch wirkender kinderpornografischer Bild- und Videodateien aus technischer Sicht mit einem vertretbaren Aufwand möglich wäre. Dennoch sollte die erhoffte Effektivitätssteigerung der Ermittlungen gewissenhaft mit den möglichen negativen Folgen einer Ausweitung der Ermittlungsbefugnisse abgewogen werden. Wie sich das Spannungsverhältnis zwischen dem materiell-rechtlichen Verbot des § 184b StGB und der staatlichen Verpflichtung zur Aufklärung und Verfolgung von Straftaten im Falle der Einbringung einer entsprechenden Gesetzesinitiative am sinnvollsten auflösen lässt, wird letzten Endes der Gesetzgeber zu entscheiden haben.

Literaturverzeichnis

[BP17] Balazia, M., Plataniotis, K. N. (2017). Human gait recognition from motion capture data in signature poses. IET Biometrics, 6 (2), 129-137.

[Be18] Beschluss der 89. Konferenz der Justizministerinnen und Justizminister (TOP II.9), https://www.justiz.nrw.de/WebPortal_Relaunch/JM/jumiko/beschluesse/2018/Fruehjahrskonferenz_2018/II-9-BY---Effektive-Verfolgung-und-Verhinderung-von-Kinderpornografie-und-Kindesmissbrauch-im-Darknet.pdf

[Ca15] Cao, C., Bradley, D., Zhou, K., Beeler, T. (2015). Real-time high-fidelity facial performance capture. ACM Transactions on Graphics (ToG), 34(4), 46.

[43] Safferling, DRiZ 2019, 206 (207).
[44] Gercke, CR 2018, 480 (481, Rn. 7).

[Cr13] Crawford, A.: Computer-generated 'Sweetie' catches online predators, https://www.bbc.com/news/uk-24818769 (23.04.2019)

[Fa16] Farid, H. (2016). Photo forensics. MIT Press.

[Fi19] Fiebig, P.: Verbrecherjagd im Darknet, Deutsche Richterzeitung (DRiZ) 2019, S. 50-51.

[Ge18] Gercke, M.: Brauchen Ermittlungsbehörden zur Bekämpfung von Kinderpornographie im sog. „Darknet“ weitergehende Befugnisse?, Computer und Recht (CR) 2018, S. 480-484, 2018.

[Ha19] Harris, D. (2019). Deepfakes: False Pornography Is Here and the Law Cannot Protect You. Duke Law & Technology Review, 17(1), 99-127.

[Hu17] Huang, R., Zhang, S., Li, T., & He, R. (2017). Beyond face rotation: Global and local perception gan for photorealistic and identity preserving frontal view synthesis. In Proceedings of the IEEE International Conference on Computer Vision (pp. 2439-2448).

[Kr12] Kraus, K. (2012). Photogrammetrie: Geometrische Informationen aus Photographien und Laserscanneraufnahmen. Walter de Gruyter.

[Ku07] Kuhnen, K.: Kinderpornographie und Internet. Hogrefe Verlag, Göttingen, 2007.

[MG01] Moeslund, T. B., Granum, E. (2001). A survey of computer vision-based human motion capture. Computer vision and image understanding, 81(3), 231-268.

[Pa12] Palm, J.: Kinder- und Jugendpornographie im Internet. Eine materiell-rechtliche Untersuchung der Rechtslage in Deutschland. Verlag Peter Lang, Frankfurt am Main, 2012.

[Sa18] Safferling, C.: Keuschheitsproben und Verdeckte Ermittler im Darknet, Deutsche Richterzeitung (DRiZ) 2018, S. 206-207.

[Si18] Siren Real-Time Performance, https://www.youtube.com/watch?v=9owTAISsvwk (23.04.2019)

[St09] Steinebach, M., El Ouariachi, M., Liu, H., & Katzenbeisser, S. (2009, September). On the reliability of cell phone camera fingerprint recognition. In International Conference on Digital Forensics and Cyber Crime (pp. 69-76). Springer, Berlin, Heidelberg.

[Th19] This person does not exist, https://thispersondoesnotexist.com/ (23.04.2019).

[Vl07] Vlasic, D., Adelsberger, R., Vannucci, G., Barnwell, J., Gross, M., Matusik, W., & Popović, J. (2007, August). Practical motion capture in everyday surroundings. In ACM transactions on graphics (TOG) (Vol. 26, No. 3, p. 35). Acm.