

Hans-Christian Gräfe (Hrsg.) | Telemedicus e.V. (Hrsg.)

§ Telemedicus
Sommerkonferenz

Über den Tellerrand

Am 28. und 29. Juni 2019 in Berlin



Tagungsband zur Konferenz

weizenbaum
institut



HÄRTING

Bird & Bird

game

Verband der deutschen
Games-Branche

SKW
Schwarz

Tagungsband zur Sommerkonferenz 2019:
Über den Tellerrand

Hans-Christian Gräfe (Hrsg.)
Telemedicus e. V. (Hrsg.)

**Tagungsband zur Sommerkonferenz 2019:
Über den Tellerrand**

Telemedicus – Recht der Informationsgesellschaft

Telemedicus-Schriftenreihe

Band 5

**Alle Fundstellen, soweit sie ins Internet verweisen, wurden zuletzt
überprüft am 27.09.2020 – soweit nicht anders angegeben.**

Bibliografische Information Der Deutschen Nationalbibliothek

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

I S B N 9 7 8 – 3 – 8 0 0 5 – 1 7 8 0 – 8

dfv' Mediengruppe

© 2020 Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft, Frankfurt am Main

Dieses Werk ist lizenziert unter der Lizenz „Creative Commons Namensnennung – Nicht-kommerziell – Weitergabe unter gleichen Bedingungen 3.0 Deutschland“ (CC BY-NC-SA 3.0 DE). Eine vollständige Version des Lizenztextes ist abrufbar unter <http://creativecommons.org/licenses/by-nc-sa/3.0/de/>.

Druck: WIRMachenDRUCK GmbH, Backnang

Printed in Germany

Vorworte der Herausgeber

Über den Tellerrand – unter diesem **Motto** stand die Telemedicus Sommerkonferenz 2019 (Soko19). Mit dem Thema wollten wir uns fachübergreifend der Komplexität der realen Welt im Digitalbereich widmen. Dabei haben wir aktuelle Entwicklungen und Zukunftstrends interdisziplinär betrachtet, zum Beispiel Möglichkeiten von Chatbots, Music Data Mining oder den Wert digitaler Güter. Diese und viele andere Themen durften wir bei der Soko19 mit hochqualifizierten und namhaften Speaker*innen und Teilnehmenden diskutieren. Die wesentlichen Themen der Konferenz dokumentieren wir in diesem Tagungsband. Wie in den vorherigen Bänden haben wir uns dazu entschieden, die Inhalte unter einer Creative Commons Lizenz und neben einer Druckversion auch digital zu veröffentlichen. Wir sind der Überzeugung, dass wissenschaftliche Diskurse am sinnvollsten geführt werden, wenn sie möglichst vielen Menschen zugänglich sind. Wir hoffen deshalb, mit diesem Band weitere Diskussionen anstoßen und bereichern zu können.

Die Soko19 und der Tagungsband wären ohne das ganze **Telemedicus-Team** und ein Netzwerk von Sponsoren und Partnern nicht möglich gewesen. Wir bedanken uns herzlich bei allen **Speaker*innen** und **Teilnehmenden** der Telemedicus Sommerkonferenz 2019 für spannende Diskussionen und wertvolle Impulse und ganz besonders bei den **Autor*innen**, die uns für diesen Tagungsband ihre Beiträge zur Verfügung stellen! Außerdem danken wir unseren **Mitveranstaltern**, dem Bayreuther Arbeitskreis für Informationstechnologie – Neue Medien – Recht e.V. (AKIT) und dem Weizenbaum-Institut für die vernetzte Gesellschaft, unseren **Partnern**, der Humboldt Law Clinic Internetrecht (HLCI), dem Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG), der Zeitschrift Kommunikation & Recht (K&R), unserem Gastgeber Microsoft Deutschland sowie unseren **Sponsoren**, namentlich der Kanzlei Bird&Bird, dem Game – Verband der deutschen Games-Branche, Härtling Rechtsanwälten und der Kanzlei SKW Schwarz. Ohne Sie und Euch gäbe es keine Telemedicus Sokos!

*Hans-Christian Gräfe,
Weizenbaum-Institut für die vernetzte Gesellschaft/Telemedicus*

*Adrian Schneider,
Vorstand Telemedicus e. V.*

Inhaltsverzeichnis

Vorworte der Herausgeber	V
1 KONFERENZBERICHT: DAS WAR DIE SOKO19.	1
1.1 Spannungsfelder: Demokratie, Digitalisierung und Pressearbeit	1
1.2 Recht und Praxis: Jazz, Informatik und Visualisierung . .	2
1.3 Recht und Pflichten: Umgang mit Datenleaks und digitale Barrierefreiheit.	4
1.4 Digital im Unternehmen: Digitale Güter und Chatbots . .	4
1.5 Vom Ende der Memes: EU-Urheberrechtsreform.	5
1.6 Online-Werbung, Blockchain und Bodycams.	5
1.7 Algorithmen als Entscheider und sichere Kommunikation	6
1.8 Datenschutz- und Kartellrecht	7
2 KEIN LIKE FÜR DIE PRESSEFREIHEIT	8
2.1 Der Präsident und die (sozialen) Medien	8
2.2 Von Washington nach Berlin: Zum Umgang der Bundes- regierung mit den Medien.	11
2.3 Pressefreiheit in den USA – Yay or Nay?	19
3 MUSIC DATA MINING	27
3.1 Anwendungsfelder	27
3.2 Mining und Recht	30
3.3 Schritte des Minings im Einzelnen	33
3.4 Fazit.	45
4 DATA LEAKS	47
4.1 Einleitung	47
4.2 Effektive Information nach digitalem Identitätsdaten- diebstahl	49
4.3 Daten und Informationsfluss.	50
4.4 Technisches Konzept und Umsetzung.	51
4.5 Datenschutz.	54
4.6 Risiken der Verarbeitung.	59
4.7 Fazit.	62
5 DER WERT DIGITALER GÜTER – STEUERRECHTLICHE EINORDNUNG. .	63
5.1 Überblick über das internationale Steuerrecht heute	64
5.2 Steuerliche Werterfassung von digitalen Gütern und Daten.	68

5.3	Steuerbare Wertschöpfung durch Daten?!.	75
5.4	Fazit und Ausblick	80
6	DER WERT DIGITALER GÜTER – ÖKONOMISCHE BETRACHTUNG	82
6.1	Einleitung	82
6.2	Eigenschaften von Daten.	83
6.3	Der Wert datenbasierter Dienste für Verbraucher*innen. .	84
6.4	Der Wert von Daten für Unternehmen	87
6.5	Zusammenfassung.	91
7	BLOCKCHAIN-BEWEIS	92
7.1	Nachweis von Rechten	92
7.2	Schutz von Geheimnissen	94
7.3	Akzeptanz von Blockchain-Beweisen vor Gericht	96
8	ZUR NUTZUNG VON DASHCAMS UND BODYCAMS IM ÖFFENTLICHEN INTERESSE ZUR VERHINDERUNG VON STRAFTATEN UND ORDNUNGS- WIDRIGKEITEN AUS SICHT DES RUSSISCHEN GESETZGEBERS.	99
8.1	Einleitung	99
8.2	Deutsche Rechtspraxis zur Verwendung von Body- und Dashcams	101
8.3	Russische Rechtspraxis zur Verwendung von Body- und Dashcams	102
8.4	Zusammenfassung und Fazit.	105
	Autor*innenhinweise	107

1 KONFERENZBERICHT: DAS WAR DIE SOKO19

Jonas Kunze und Hans-Christian Gräfe¹

*Die Telemedicus Sommerkonferenz im Jahr 2019 (#Soko19) stand unter dem Motto „Über den Tellerrand“. Wir haben verstärkt Expert*innen nichtjuristischer Fachrichtungen einbezogen. Die Soko19 beschäftigte sich mit der fachübergreifenden Komplexität der realen Welt im Digitalbereich und knüpfte an die Soko18 an, die sich mit der zunehmenden Komplexität entsprechender Rechtsfragen befasst hatte.*

So fanden die meisten Vorträge in juristisch-nichtjuristischen Tandems statt. Das machte die Vorträge anschaulich, abwechslungsreicher und sorgte dafür, dass sie nicht mit Paragraphen überfrachtet waren. Wie immer auf den Sokos waren die Vorträge mit einer ungezwungenen Diskussion mit dem Publikum verknüpft. Die typische Soko-Atmosphäre ohne formelle Kleidung tat ihr übriges und sorgte für eine kommunikative Atmosphäre.²

1.1 Spannungsfelder: Demokratie, Digitalisierung und Pressearbeit

Die Keynote hielt **Prof. Dr. Jeanette Hofmann** zur mediatisierten Demokratie. Sie sprach sich für einen Sichtwechsel auf das Zusammenwirken von Digitalisierung und Demokratie aus. Der digitale Wandel führe zu einem langfristigen Strukturwandel statt zu einem stetigen Kampf zwischen Neuerung und politischer Regulierung.³

Dem Zusammenspiel von Politik und Öffentlichkeit widmeten sich auch **Anna K. Bernzen** und **Verena Reiter** in ihrem Vortrag „Kein Like für die Pressefreiheit“.⁴ Sie stellten dar, welche Entwicklungen in der amerikanischen Presseöffentlichkeit seit der Wahl von Donald Trump zu be-

1 Mehr über die Autoren erfahren Sie im Autor*innenhinweis auf S. 109, 108.

2 Die Ursprungsversion des Beitrages ist am 19. August 2019 erschienen unter: <https://www.telemedicus.info/article/3432-Konferenzbericht-und-Folien-zur-Soko19.html> [Anm. d. Hrsg.].

3 S. Gedanken zur Keynote von Soko-Teilnehmerin *Christofori*, abrufbar unter <https://www.socialmediatagebuch.de/2019/07/03/digitalisierung-und-demokratie-wer-treibt-wen/>.

4 Die Präsentationsfolien sind abrufbar unter <https://www.telemedicus.info/uploads/AnnaBernzenundVerenaReiterPressefreiheit.pdf>.

obachten sind. Dabei erörterten sie den Stellenwert der Presse als vierte Gewalt in den USA und zeigten die gesamtgesellschaftlichen Folgen von Trumps Verhalten auf. Denn werde der traditionellen Presse und ihren Vertreter*innen von höchster Stelle des Staates jegliche Legitimität und Glaubwürdigkeit entzogen, wirke sich dies schließlich auch auf die Meinungsbildungsprozesse der Amerikaner*innen als Nation aus.

Anhand ausgewählter Situationen, in denen US-Präsident Trump auf unkonventionelle Art und Weise mit den Medien interagierte, prüften die Referentinnen, ob auch deutsche Regierungsmitglieder einzelne Medien derart in ihrem Interesse an Informationen beschränken könnten.⁵

Zum Abschluss des Freitagvormittages präsentierte **Daniel Moßbrucker** seine gemeinsam mit **Prof. Dr. Tobias Gostomzyk** (TU Dortmund) verfasste Studie zu präventiven Anwaltsstrategien gegenüber Medien: „Wenn Sie das schreiben, verklage ich Sie!“ Dazu befragten sie Presserechts-Anwält*innen und Redaktionen zu ihren Erfahrungen mit Versuchen, vermeintliche Betroffenenrechte anwaltlich oder gerichtlich durchzusetzen.⁶ Sie kamen dabei zu dem Ergebnis, dass es Anwält*innen (noch) nicht gelinge, Berichterstattung im Vorfeld durch Drohschreiben unmittelbar zu unterbinden. Die Bemühung kritische Berichterstattungen vor Veröffentlichung zu unterbinden, bleibt aber keinesfalls folgenlos. Positiv könne sie sogar zu einer gesteigerten Sorgfalt und mithin gesteigertem Selbstbewusstsein der (großen) Redaktionen führen.

1.2 Recht und Praxis: Jazz, Informatik und Visualisierung

2019 gingen bei Telemedicus besonders viele Themenvorschläge auf den Call for Proposals ein. Deshalb startete ab der Mittagspause des ersten Tages ein Sidetrack. So konnten wir gleichzeitig zwei Themen eine Bühne bieten.

⁵ Vgl. den Beitrag von *Bernzen/Reiter* auf S. 8 ff. [Anm. d. Hrsg.].

⁶ Die Präsentationsfolien sind abrufbar unter: https://www.telemedicus.info/uploads/Tobias_GostomzykUndDanielMossbruckerPraventiveAnwaltsstrategien.pdf; Die Studie ist abrufbar unter https://www.otto-brenner-stiftung.de/fileadmin/user_data/stiftung/02_Wissenschaftsportaal/03_Publikationen/AH99_Journalisten_Juristen.pdf.

Im Lichthof gaben **Fabian Rack** und **Dr. Klaus Frieler** einen Einblick in die Jazz-Forschung.⁷ Frieler entwickelte u. A. an der Musikhochschule Weimar ein Programm zur computergestützten Analyse von Jazz. Da im Jazz intensiv improvisiert wird, stellten sich hier besondere Anforderungen an eine leicht verständliche Datenaufbereitung. Telemedicus Kernteammitglied Fabian Rack beleuchtete anschließend die Forschung von Frieler aus urheberrechtlicher Perspektive. Er machte deutlich, welchen Herausforderungen sich Wissenschaftler*innen bei einer Bearbeitung von Musikdateien mit vielfältigen Schutzrechten stellen würden.

Insbesondere juristische Aufsätze können schwer verständlich sein. Diesem Problem widmeten sich die Juristin **Daniella Domokos** und die PR-Beraterin **Stephanie Kowalski**. Primär liege diese Unverständlichkeit an mangelnder visueller Aufbereitung. Lange Blocktexte ließen Sinnzusammenhänge nicht sehr deutlich werden. Abhilfe schaffen könne die gezielte Visualisierung – z. B. durch allgemeinverständliche Icons.⁸ Zur Verdeutlichung ließen die Referentinnen ihr Publikum den Stift selbst in die Hand nehmen.⁹

Im Meetingraum bekamen die Soko Teilnehmer*innen währenddessen eine praktische Einführung in die Informatik. Jurist und Informatiker **Maximilian Kroker** führte die Anwesenden auf interaktive und kreative Weise in sein zweites Fachgebiet ein. Im Rahmen von Quizfragen und Abstimmungen konnten Jurist*innen die technischen Grundlagen lernen, z. B. wie ein Algorithmus funktioniert und arbeitet.¹⁰ Für viele Teilnehmende eine gute Gelegenheit, um etwa IT-Mandate besser nachvollziehen zu können.

⁷ Vgl. den Beitrag von *Frieler/Rack* auf S. 27 ff. [Anm. d. Hrsg.].

⁸ S. Tweet von *Assion*, 28.06.2019, abrufbar unter https://twitter.com/sas_assion/status/1144580306609102850.

⁹ Die Präsentationsfolien sind abrufbar unter <https://www.telemedicus.info/uploads/StephanieKowalskiundDaniellaDomokosVisualisierung.pdf>.

¹⁰ S. Tweet von *Gräfe*, 28.06.2019, abrufbar unter <https://twitter.com/haensselbert/status/1144570866812018690>.

1.3 Recht und Pflichten: Umgang mit Datenleaks und digitale Barrierefreiheit

Betroffene über einen Datenleak zu informieren kann eine unangenehme Aufgabe sein. Wie man es richtig angeht, berichteten **Susan Gonscherowski** und **Matthias Wübbeling** in ihrem Vortrag.¹¹ Die Politikwissenschaftlerin und der IT-Berater zeigten auf, welche Betroffenenrechte zur Verfügung stehen und welche Hürden sich bei den Informationspflichten stellen können.¹² Dabei gingen sie besonders darauf ein, wie Warnsysteme gestaltet sein könnten. Die Workshopteilnehmer*innen konnten anschließend überprüfen, ob ihre eigenen Daten online kompromittiert worden sind.

Johannes Nehlsen und **Wolfgang Wiese** berichteten über die Pflicht öffentlicher Stellen, ihre Onlineangebote demnächst barrierefrei bereitzustellen. Den Ausgangspunkt bildet die EU-Richtlinie 2016/2102,¹³ die einen klaren Zeitplan aufstellt, bis wann digitale Anwendungen barrierefrei zugänglich sein müssen. Der Aufwand, barrierefreie PDFs zu erstellen, könne einen Mehrwert bieten und das Publikationsverfahren sowie die Art der Öffentlichkeitsarbeit ändern. In den Fokus rückten die Referenten dabei die technischen Voraussetzungen sowie den rechtlichen Rahmen. Außerdem stellten sie einen Leitfaden zur Barrierefreiheit vor.¹⁴

1.4 Digital im Unternehmen: Digitale Güter und Chatbots

Gleichzeitig stellten **Aline Blankertz** und **Julia Sinnig** Forschungsergebnisse zum Wert digitaler Güter vor.¹⁵ Blankertz zeigte auf, wie unterschiedlich Menschen einem digitalen Gut einen Wert auf dem Markt

11 Die Präsentationsfolien sind abrufbar unter <https://www.telemedicus.info/uploads/SusanGonscherowskiundMatthiasWuebbelingDataLeaks.pdf>.

12 Vgl. den Beitrag von *Gonscherowski/Wübbeling* auf S. 47 ff. [Anm. d. Hrsg.].

13 Richtlinie (EU) 2016/2102 des Europäischen Parlaments und des Rates vom 26. Oktober 2016 über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen.

14 Die Verwaltung erfolgt über ein öffentliches GitHub Repository, abrufbar unter <https://github.com/RZ-BY/Leitfaden-Barrierefreiheit/>.

15 Die Präsentationsfolien von Blankertz sind abrufbar unter <https://www.telemedicus.info/uploads/AlineBlankertzWertdigitalerGueter.pdf>.

zuschrieben.¹⁶ Steuerrechtlich knüpfte Sinnig an und legte dar, wie komplex eine Besteuerung digitaler Güter in globalen Schöpfungsketten sein kann.¹⁷

Einen Chatbot in die unternehmenseigenen Abläufe zu integrieren, ist kein leichtes Unterfangen.¹⁸ Davon berichtete **Sarah Honne**. Sie stellte in einem Versicherungskonzern den Mitarbeiter*innen im Kundenservice einen Chatbot bereit. Dieser unterstütze die Mitarbeiter*innen etwa bei der Auswahl neuer Angebote. Justiziar **Markus Schröder** umriss die regulatorischen Herausforderungen. Zwar könne man andiskutieren, ob Chatbots eine werbliche Ansprache i. S. d. ePrivacy-RL oder des UWG seien, aber es handele sich hier immer noch nur um einfache Pop-Ups auf den Unternehmenswebseiten.

1.5 Vom Ende der Memes: EU-Urheberrechtsreform

Bevor der Tag im Sonnenuntergang auf der Dachterrasse der GAMES Academy endete, präsentierte **Prof. Dr. Christoph Fiedler** seine Gedanken zur EU-Urheberrechtsreform. Auf Einladung des Mitveranstalters @KIT informierte er über seine Ansichten zur Regulierung von Äußerungen im Netz. Er plädierte dafür, bereits vorhandene Instrumente der Rechtsordnung zu nutzen, anstatt unklare neue Möglichkeiten zu schaffen. Instrumente, die rechtmäßige Äußerungen filtern würden, lehnte er ab.¹⁹

1.6 Online-Werbung, Blockchain und Bodycams

Den zweiten Konferenztag begann **Tilman Herbrich** mit einer Einleitung zum Datenschutz in der Online-Werbung und warnte vor möglichen Bußgeldern in beachtlicher Höhe. Er erklärte die technisch komplexe Anzeige von Werbung, insbesondere das sogenannte Real-Time-Bid-

¹⁶ Vgl. den Beitrag von *Blankertz* auf S. 82 ff. [Anm. d. Hrsg.].

¹⁷ Vgl. den Beitrag von *Sinnig* auf S. 63 ff. [Anm. d. Hrsg.].

¹⁸ Die Präsentationsfolien sind abrufbar unter <https://www.telemedicus.info/uploads/Markus-SchroederundSarahHonneChatbots.pdf>.

¹⁹ S. Tweet von *Moenikes*, 28.06.2019, abrufbar unter <https://twitter.com/jmoenikes/status/1144633771167244293>.

ding. Hierbei zeigte er auf, welche Herausforderungen sich bei der Einholung einer wirksamen Einwilligung ergeben würden. Da der Co-Referent von Herbrich leider ausgefallen war, stellte sich spontan Soko-Teilnehmer **Christian Pfeiffer** als technischer Referent zur Verfügung.

Der Implementierung von digitalen Möglichkeiten in unser Rechtssystem widmeten sich **Yvonne Schäfer** und **Jean-Maxime Riviere**. Sie erläuterten rechtlich und technisch, wie die Blockchain-Technologie etwa zur Beweisführung vor Gericht eingesetzt werden könnte. So bestehe die Möglichkeit, Schutzrechte wie Marken oder Urheberrechte auf der Blockchain abzubilden, Betriebsgeheimnisse zu sichern oder den Stand der Technik zu etablieren. Zwar bestehen derzeit Hürden bei Beweisführungen, aber sichere und vertrauenswürdige Zertifikate, wie sie mittels Timestamps oder kryptographischen Fingerprints auf Blockchain-Basis erstellt werden können, könnten die Beweisführung erleichtern.²⁰

Beweissicherung war zeitgleich auch bei **Hermann Jakobi** und **Bodo Pfalzgraf** das Thema. Wie Bodycams von Sicherheitsbehörden in Deutschland und Russland genutzt werden, stellte Jurist Jakobi vor.²¹ Während in Russland Kameras zu Beweis Zwecken kaum reguliert seien, gebe es in Europa eine Vielzahl von Normen, die den Einsatz solcher Technologien regeln.²² Pfalzgraf gab als Vorsitzender der Polizeigewerkschaft Berlin Einblicke in die Arbeit seiner Kolleg*innen, die bereits Bodycams nutzten. Er berichtete von den ersten Testläufen in einzelnen Bundesländern und den daraus resultierenden Maßnahmen, die es in technischer und organisatorischer Weise für Bodycams und für Polizist*innen zu bewältigen gebe.²³

1.7 Algorithmen als Entscheider und sichere Kommunikation

Wenn Entscheidungen von Algorithmen vorbereitet oder getroffen werden, dann ist eine mögliche Diskriminierung oft nicht direkt sichtbar. Wie hier bei der Programmierung eingegriffen werden kann und

20 Vgl. den Beitrag von *Schäfer* auf S. 92 ff. [Anm. d. Hrsg.].

21 Die Präsentationsfolien sind abrufbar <https://www.telemedicus.info/uploads/HermannJakobiDash-undBodycams.pdf>.

22 Vgl. den Beitrag von *Jakobi* auf S. 99 ff. [Anm. d. Hrsg.].

23 S. Tweet von *Domokos*, 29.06.2019, abrufbar unter <https://twitter.com/Akoneira/status/1144901142037585920>.

ob rechtliche Bedingungen zum Greifen kommen können, erläuterten **Amadeus Peters** und **Prof. Dr. Claudia Müller-Birn**. Dabei müsse abgegrenzt werden, wie Diskriminierung im allgemeinen Sprachgebrauch verstanden wird und was eine Diskriminierung im Rechtssinne ist. Das größte Problem stellten dabei mittelbare Diskriminierungen dar, die nicht offensichtlich sind. Dann sei es schwierig bis unmöglich zu bestimmen, ob die Ergebnisse eines Algorithmus mittelbar diskriminierend sind, wenn es an einer objektiven Referenz fehle, um die mittelbare Diskriminierung zu messen.

Parallel gab **Daniel Moßbrucker** Nachhilfe zur digitalen Selbstverteidigung. Die Tools, die Journalist*innen zur sicheren Kommunikation mit Informant*innen nutzen, könnten für Jurist*innen ebenso nützlich sein. Moßbrucker gab Tipps, wie tägliche digitale Abläufe besser zu schützen seien und warb für einen sensiblen Umgang mit digitalen Technologien.²⁴

1.8 Datenschutz- und Kartellrecht

Der Abschluss der Soko19 stand im Zeichen eines aktuellen kartellrechtlichen Verfahrens. Das Bundeskartellamt wagte sich mit einem Beschluss gegen Facebook in neue Rechtsbereiche vor, in dem es dem Unternehmen untersagte, Daten von anderen Plattformen auf Facebook ohne ausreichende Einwilligung der Nutzer*innen zusammenzuführen.²⁵ Die entstandene Verknüpfung von Kartell- und Datenschutzrecht irritiert und fasziniert die Fachjurist*innen zugleich. **Sebastian Louven** stellte die Entscheidung aus kartellrechtlicher Sicht vor.²⁶ **Dr. Carlo Piltz** machte deutlich, warum der Beschluss des Bundeskartellamtes ihn als Datenschutzrechtler irritierte.²⁷

24 Die Präsentationsfolien sind abrufbar unter https://www.telemedicus.info/uploads/Daniel_MobruckerDigitaleSicherheit.pdf.

25 Zur Pressemitteilung des Bundeskartellamtes vom 07.02.2019, abrufbar unter https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2019/07_02_2019_Facebook.html.

26 Die Präsentationsfolien sind abrufbar https://www.telemedicus.info/uploads/Sebastian_LouvenDatenschutz-undWettbewerbsrecht.pdf.

27 Die Präsentationsfolien sind abrufbar https://www.telemedicus.info/uploads/CarloPiltz_Datenschutz-undWettbewerbsrecht.pdf.

2 KEIN LIKE FÜR DIE PRESSEFREIHEIT

*Dr. Anna K. Bernzen/Verena Reiter*²⁸

Am liebsten würde er die klassische Öffentlichkeitsarbeit ganz bleiben lassen: Den Eindruck gewinnt man, wenn man die Aussagen von Donald Trump auf Twitter und ähnlichen Plattformen verfolgt. Wo er nur kann, entzieht der US-Präsident sich dem Zugriff der traditionellen Presse. Das bedeutet nicht nur, dass er seine Botschaften lieber direkt über Social Media als klassisch per Pressemitteilung an die Öffentlichkeit übermittelt und traditionelle Mittel der Öffentlichkeitsarbeit wie etwa Pressekonzferenzen, wo möglich, meidet. Missfällt ihm die Berichterstattung eines Journalisten, entzieht er diesem auch gerne einmal die Akkreditierung für das Weiße Haus.

*Der Beitrag ordnet dieses Verhalten des US-Präsidenten aus amerikanistischer und rechtlicher Sicht ein. Er erörtert den Stellenwert der Presse als vierte Gewalt in den USA und wie sich diese Rolle seit dem Antritt Präsident Trumps verändert hat. Dies hat gesamtgesellschaftliche Folgen. Wird der traditionellen Presse und ihren Vertreter*innen von höchster Stelle Legitimität und Glaubwürdigkeit entzogen, wirkt sich dies schließlich auch auf die Meinungsbildungsprozesse der Nation aus. Schließlich bleibt zu fragen, inwiefern ein derartiges Verhalten in Deutschland rechtlich zulässig wäre.*

2.1 Der Präsident und die (sozialen) Medien

2.1.1 Die „Fake News“ als „Enemy of the people“

“The FAKE NEWS media (failing @nytimes, @NBCNews, @ABC, @CBS, @CNN) is not my enemy, it is the enemy of the American people!”²⁹

Dies twitterte der US-amerikanische Präsident Donald Trump nur wenige Wochen nach seiner Amtseinführung im Januar 2017 und äußerte

²⁸ Mehr über die Autorinnen erfahren Sie im Autor*innenhinweis auf S. 107 und S. 109.

²⁹ Twitter-Account @realDonaldTrump v. 27.02.2017, abrufbar unter <<https://twitter.com/realdonaldtrump/status/832708293516632065?lang=de>> (Stand: 21.09.2020).

sich damit in einem Tonfall, den er bereits während seines Wahlkampfes angeschlagen hatte. Statt Journalist*innen für Interviews zu seiner Kampagne zur Verfügung zu stehen, hatte er schon damals lieber ungefiltert über seinen Twitter-Account mit seinen Wähler*innen kommuniziert. Seine Einstellung gegenüber den Medien sollte sich auch im zweiten Jahr seiner Präsidentschaft nicht ändern:

“There is great anger in our Country caused in part by inaccurate, and even fraudulent, reporting of the news. The Fake News Media, the True Enemy of the People, must stop the open & obvious hostility & report the news accurately & fairly. That will do much to put out the flame...”³⁰

Nicht zuletzt mit solchen Aussagen auf Twitter hatte Trump insbesondere den liberalen Medien einen Kampf angesagt, der bis heute andauert. Dabei greift er Journalist*innen und Medienhäuser verbal an und behindert diese gezielt bei ihrer Arbeit. Im ersten Teil dieses Beitrags werden zwei Beispiele geschildert, die einen Eindruck davon vermitteln, wie es in der Praxis um die Pressefreiheit in den USA unter der Regierung von Präsident Trump steht. Anschließend wird aus juristischer Sicht untersucht, wie ähnliche Situationen nach deutschem Recht zu beurteilen wären. Die deutsche Sach- und Rechtslage wird in einem dritten Schritt aus amerikanistischer Sicht mit den jüngeren Entwicklungen in den USA verglichen.

2.1.2 Der Fall Jim Acosta

7. November 2018, Pressekonferenz im Weißen Haus: Der White House-Korrespondent für den Fernsehsender CNN, Jim Acosta, stellte Präsident Trump eine unangenehme Frage zur Situation an der amerikanisch-mexikanischen Grenze sowie zu dessen Äußerungen, dass es sich bei der derzeitigen Migrationsbewegung um eine „Invasion“³¹ handle. Weil Trump darauf nur ausweichend antwortete und keine weitere Frage gestattete, weigerte sich Acosta, das Mikrofon abzugeben. Dabei streifte er unabsichtlich den Arm einer Praktikantin, die ihm das Mikrofon ab-

30 Twitter-Account @realDonaldTrump v. 29.10.2018, abrufbar unter <<https://twitter.com/realdonaldtrump/status/1056879122348195841?lang=de>> (Stand: 21.09.2020).

31 Siehe die Aufzeichnung der Pressekonferenz durch *syracuse.com*, President Trump – Jim Acosta press conference, www.youtube.com v. 08.11.2018, abrufbar unter <<https://www.youtube.com/watch?v=MvfqUMg10uM>> (Stand: 21.09.2020).

nehmen sollte. Acosta entschuldigte sich sofort. Daraufhin stellte er eine weitere brisante Frage zu den Ermittlungen im Hinblick auf den russischen Einfluss auf die Präsidentschaftswahl 2016. Trump jedoch nahm die unabsichtliche Berührung zum Anlass, um zum Gegenschlag gegen seinen Rivalen CNN auszuholen, indem er Acosta eine schreckliche Person nannte und CNN als „the enemy of the people“³² bezeichnete, da sie „fake news“³³ verbreiten würden.

Was dann folgte, erregte weltweites Aufsehen: Jim Acosta wurde die Akkreditierung für das Weiße Haus bis auf Weiteres entzogen, weil er die Praktikantin absichtlich unangemessen berührt habe, so die offizielle Begründung³⁴, obwohl eine Videoaufnahme des Zwischenfalles das Gegenteil zeigt³⁵. Trump stand in der Kritik, da der Entzug der Akkreditierung international überwiegend als Akt reiner Willkür sowie als Angriff auf die Pressefreiheit bewertet wurde.³⁶ Der Fall Acosta steht beispielhaft für ein neues Zeitalter, in welchem die uneingeschränkte Arbeit von Journalist*innen und anderen Medienvertreter*innen bedroht ist und damit auch die amerikanische Demokratie.

2.1.3 Ein Dinner in Hanoi

27. Februar 2019, Präsident Trump traf Nordkoreas Machthaber Kim Jong Un in Hanoi: Bei einer dem Abendessen vorausgehenden Begegnung der Staatschefs an diesem Tag hatten Journalist*innen den US-Präsidenten nach einer Reaktion auf die Vorwürfe gefragt, die Trumps früherer Anwalt Michael Cohen vor einem Ausschuss des US-Repräsentantenhauses erhoben hatte. Trump hatte daraufhin nur den Kopf geschüttelt und die Frage ignoriert.³⁷ Zahlreiche Reporter*innen wurden

32 *Syracuse.com* (Fn. 31).

33 *Syracuse.com* (Fn. 31).

34 *Guardian staff and agencies*, CNN's Jim Acosta has White House pass revoked after Trump confrontation, [www.theguardian.com](https://www.theguardian.com/us-news/2018/nov/07/cnn-jim-acosta-reporter-credentials-revoked) v. 08.11.2018, abrufbar unter <<https://www.theguardian.com/us-news/2018/nov/07/cnn-jim-acosta-reporter-credentials-revoked>> (Stand: 21.09.2020).

35 Siehe dazu *Syracuse.com* (Fn. 31).

36 Siehe die Zusammenstellung kritischer Stimmen bei *Stelter*, Reporters condemn White House decision to bar CNN's Acosta, [edition.cnn.com](https://edition.cnn.com/2018/11/08/media/trump-acosta-press-pass-reaction/index.html) v. 08.11.2018, abrufbar unter <<https://edition.cnn.com/2018/11/08/media/trump-acosta-press-pass-reaction/index.html>> (Stand: 26.07.2019).

37 *Tagesschau*, USA schließen Reporter aus, www.tagesschau.de v. 27.02.2019, abrufbar unter <<http://www.tagesschau.de/ausland/reporter-trump-kim-101.html>> (Stand: 21.09.2020).

in Folge dieser kritischen Nachfrage von der Berichterstattung über ein Abendessen von Trump und Kim Jong Un ausgeschlossen.

Kurz vor Beginn des Abendessens informierte die Pressesprecherin des Weißen Hauses die mit Trump reisenden Journalist*innen, dass nur Fotograf*innen und Kameralleute zugelassen sein würden. In Folge des Protests einiger Fotojournalist*innen, die sich daraufhin weigerten, ihrer Arbeit bei dem Dinner nachzugehen, wurde einer einzigen Printjournalistin Zugang gewährt.³⁸ Dies war Vivian Salama, die Korrespondentin des Wall Street Journal.³⁹ Von diesem Ausschluss waren unter anderem Journalist*innen der Los Angeles Times sowie der Nachrichtenagenturen Reuters, The Associated Press und Bloomberg betroffen.⁴⁰

Bis zu diesem Zeitpunkt hätte wohl niemand damit gerechnet, dass Trump sich zu so einem radikalen Schritt hinreißen lassen würde, nur da er sich durch unangenehme Fragen der Reporter*innen angegriffen fühlte. Seine Vorgänger hatten insbesondere bei Treffen mit Vertreter*innen autoritärer Regimes stets großen Wert darauf gelegt, die Vereinigten Staaten durch eine vorbildliche Handhabung der Pressefreiheit als beispielhafte Demokratie zu präsentieren.⁴¹

2.2 Von Washington nach Berlin: Zum Umgang der Bundesregierung mit den Medien

2.2.1 Die Akkreditierung von Medienvertreter*innen

Wie wäre es, wenn sich statt Donald Trump Bundeskanzlerin Angela Merkel mit Kim Jong Un getroffen hätte – und wenn statt der Washington Post die Welt am Sonntag davon ausgeschlossen worden wäre? Im zweiten Teil dieses Beitrags wird der rechtliche Rahmen dargestellt, in

38 Grynbaum/Rogers, White House Bars 4 U.S. Journalists From Trump's Dinner With Kim in Hanoi, www.nytimes.com v. 27.02.2019, abrufbar unter <<https://www.nytimes.com/2019/02/27/business/media/reporters-banned-trump-hanoi.html>> (Stand: 21.09.2020).

39 Tagesschau (Fn. 37).

40 Grynbaum/Rogers (Fn. 38).

41 Vergleiche Restuccia/Galiot, White House boots media after Trump faced Cohen question in front of Kim, www.politico.com v. 27.02.2019, abrufbar unter <<https://www.politico.com/story/2019/02/27/trump-kim-summit-2019-journalists-1190214>> (Stand: 21.09.2020).

dem sich die deutsche Bundesregierung in derartigen Situationen bewegt.

Wollen Medienvertreter*innen über Veranstaltungen der Regierung berichten, können sie sich dafür auf zwei Arten akkreditieren: Journalist*innen, die regelmäßig und hauptberuflich aus Berlin oder Bonn über bundespolitische Themen berichten, können beim Presse- und Informationsamt der Bundesregierung eine Jahresakkreditierung beantragen. Sie gilt zum Beispiel für Staatsbesuche oder internationale Konferenzen, an denen die Bundeskanzlerin teilnimmt.⁴² Damit ähnelt sie der Dauerakkreditierung, die Acosta durch das Weiße Haus entzogen wurde. Daneben können alle Journalist*innen sich für einzelne Veranstaltungen der Bundesregierung über das Akkreditierungsbüro des Presse- und Informationsamtes anmelden.⁴³

Medienvertreter*innen, die eine Akkreditierung bei der Bundesregierung beantragen, haben bei deren Entscheidung über ihren Antrag einen Anspruch auf Gleichbehandlung im publizistischen Wettbewerb. Dieser folgt aus der jeweiligen Medienfreiheit nach Art. 5 Abs. 1 S. 2 GG i. V. m. dem allgemeinen Gleichheitssatz gemäß Art. 3 Abs. 1 GG.⁴⁴ Veranstatet die Bundesregierung zum Beispiel eine Pressekonferenz oder organisiert sie eine Pressereise, um Einblicke in ihre Arbeit zu geben, muss sie den Zugang hierzu infolgedessen allen Medienvertreter*innen nach allgemeinen, sachgerechten Kriterien ermöglichen.⁴⁵

Die Anforderungen an eine Versagung der Akkreditierung sind dabei hoch, führt sie doch mit Blick auf die jeweilige Veranstaltung dazu, dass den betroffenen Journalist*innen jene Informationsbeschaffung unmöglich gemacht wird, die durch die Medienfreiheiten geschützt wird.⁴⁶

42 *Presse- und Informationsamt der Bundesregierung*, Pressemitteilung Nr. 403 v. 10.11.2014, abrufbar unter <<http://www.bundesregierung.de/breg-de/aktuelles/jahresakkreditierung-2015-jetzt-beantragen-750186>> (Stand: 21.09.2020).

43 *Presse- und Informationsamt der Bundesregierung*, Das Akkreditierungsteam des BPA, abrufbar unter <<https://www.akkreditierung.bundesregierung.de/onlineakkredi/team.jsp>> (Stand: 21.09.2020).

44 OVG NRW, Beschl. v. 07.10.2008 – Az. 5 A 1602/05, juris Rn. 29. In diese Richtung schon BVerwG, Urt. v. 03.12.1974 – Az. I C 30.71, NJW 1975, 891, 892.

45 OVG NRW (Fn. 44), Rn. 32; OVG Berlin, Urt. v. 22.06.2011 – Az. OVG 10 B 1.11, juris Rn. 41/48; VG Hamburg, Beschl. v. 26.05.2010 – Az. 15 E 1351/10, juris Rn. 11.

46 OVG Berlin (Fn. 45), Rn. 42. Zum Schutz der Informationsbeschaffung durch die Medienfreiheiten siehe nur BVerfG, Beschl. v. 06.10.1959 – Az. 1 BvL 118/53, BVerfGE 10, 118, 121; Beschl. v. 14.07.1994 – Az. 1 BvR 1595/92 u. a., BVerfGE 91, 125, 135; Urt. v. 27.02.2007 – Az. 1 BvR 538/06 u. a., BVerfGE 117, 244, 259.

Praktisch relevant sind zwei Versagensgründe: Die Bundesregierung darf die Akkreditierung, erstens, verweigern, wenn hinreichende Anhaltspunkte dafür vorliegen, dass der antragstellende Journalist durch sein Verhalten die Veranstaltung, für die er sich anmelden möchte, stören oder gar Leib und Leben ihrer Teilnehmer*innen gefährden wird.⁴⁷ Bei der Prüfung dieser Anhaltspunkte muss die Bundesregierung allerdings der Bedeutung der Medienfreiheiten in einer freiheitlichen Demokratie Rechnung tragen.⁴⁸ Ein beliebiges störendes Verhalten des Antragstellers in der Vergangenheit reicht deshalb für die Versagung der Akkreditierung nicht aus; es muss vielmehr speziell mit Blick auf die jeweilige Veranstaltung eine Störung drohen.

Zweitens kann die Bundesregierung eine Akkreditierung aus Kapazitätsgründen ablehnen. Wollen Medienvertreter*innen zum Beispiel an einer Pressereise teilnehmen, bei der aus Platzgründen jedoch nur ein beschränkter Personenkreis mitreisen kann, darf die Regierung eine Auswahl unter den Antragstellenden treffen.⁴⁹ Sie kann die Akkreditierung zum Beispiel bevorzugt an solche Medienvertreter*innen vergeben, die sich regelmäßig mit den Themen befassen, die Gegenstand der Reise sind.⁵⁰ Wird beispielsweise ein Feldlager der Bundeswehr besucht, kann die Akkreditierung für den Besuch bevorzugt an Journalist*innen vergeben werden, die regelmäßig über Verteidigungspolitik berichten.⁵¹

Nicht gestattet ist es der Bundesregierung dagegen, Medienvertreter*innen die Akkreditierung zu verweigern oder zu entziehen, weil ihnen deren bisherige oder zu erwartende Berichterstattung nicht genehm ist.⁵² Ein deutscher Kollege Jim Acostas könnte gegen einen Entzug seiner Akkreditierung daher sein Recht auf Gleichbehandlung im publizistischen Wettbewerb in Stellung bringen. Könnte die Bundesregierung keinen Grund für den Entzug nachweisen, der nicht mit seiner Berichterstattung zusammenhängt, wäre der Journalist in seinem Gleichbehandlungsrecht verletzt.

47 OVG Berlin (Fn. 45), Rn. 48; VG Berlin, Beschl. v. 06.06.2007 – Az. 27 A 146.07, juris Rn. 16; VG Hamburg (Fn. 45), Rn. 12.

48 OVG Berlin (Fn. 45), Rn. 53; OVG NRW (Fn. 44), Rn. 37.

49 OVG NRW (Fn. 44), Rn. 32.

50 Vergleiche BVerwG (Fn. 44), 893.

51 Siehe den Sachverhalt, welcher der Entscheidung des OVG NRW (Fn. 44) zugrunde lag.

52 BVerwG (Fn. 44), 892; VG Hamburg (Fn. 45), Rn. 14.

Grundsätzlich gibt dieses Recht den Medienvertreter*innen zwar nur einen Anspruch darauf, dass die Bundesregierung ermessensfehlerfrei über ihren Antrag auf die Akkreditierung entscheidet. Liegen aber keine der beschriebenen persönlichen Versagensgründe vor und reicht die Kapazität der Veranstaltung aus, um alle interessierten Medienvertreter*innen zuzulassen, verdichtet sich der Anspruch auf Gleichbehandlung zu einem Recht auf Erteilung der Akkreditierung.⁵³

Um dieses Recht durchzusetzen, ist der einstweilige Rechtsschutz nach § 123 VwGO in der Praxis das maßgebliche Mittel. Wird Journalist*innen die Akkreditierung für eine Veranstaltung der Bundesregierung versagt, verlieren sie schließlich faktisch die Möglichkeit, hierüber zu berichten. Die Verpflichtungsklage vor den Verwaltungsgerichten, die in der Hauptsache statthaft wäre, käme regelmäßig zu spät, um ihnen diese Möglichkeit wieder zu eröffnen. Um wesentliche Nachteile für die berufliche Tätigkeit der Medienvertreter*innen zu vermeiden, haben Verwaltungsgerichte die Bundesregierung in der Vergangenheit daher im Wege des einstweiligen Rechtsschutzes sowohl zur Erteilung der Akkreditierung für einzelne Veranstaltungen als auch (jedenfalls vorläufig) zur Erteilung der Jahresakkreditierung verpflichtet.⁵⁴

2.2.2 Die Pflicht zur Öffentlichkeitsarbeit auf Social Media

Anstelle sich der Fragen von Medienvertreter*innen wie Jim Acosta zu stellen, kommuniziert US-Präsident Trump mit den Bürger*innen bevorzugt direkt über seinen Twitter-Account. Ob auch die Bundesregierung sich für ihren Außenauftritt völlig auf ihre Profile in den sozialen Medien verlassen könnte, ist aus Sicht des deutschen Verfassungsrechts eine vielschichtige Frage. Um sie zu beantworten, muss im ersten Schritt die Zulässigkeit der Social-Media-Nutzung in den Blick genommen werden.

Seit der Öffentlichkeitsarbeit-Entscheidung des Bundesverfassungsgerichts (BVerfG) aus dem Jahr 1977 ist höchstrichterlich anerkannt, dass die Öffentlichkeitsarbeit der Bundesregierung nicht nur verfassungsrechtlich – innerhalb bestimmter Grenzen –⁵⁵ zulässig ist, sondern dass

53 Vergleiche VG Berlin (Fn.47), Rn. 20; VG Hamburg (Fn.45), Rn. 17.

54 VG Berlin, Beschl. v. 28.04.2004 – Az. 27 A 102.04, juris Rn. 10; (Fn. 47), Rn. 15.

55 Zu diesen Grenzen allgemein *Gröpl/Zembruski*, Äußerungsbefugnisse oberster Staatsorgane und Amtsträger, JURA 2016, 268, 274 ff. sowie speziell mit Blick auf die sozialen Medien

diese Öffentlichkeitsarbeit in einer freiheitlichen Demokratie darüber hinaus notwendig ist.⁵⁶ Zur Begründung führte das Verfassungsgericht damals im Wesentlichen vier Argumente an: Die Öffentlichkeitsarbeit der Bundesregierung soll helfen, den Grundkonsens des Staatsvolkes mit der vom Grundgesetz geschaffenen Staatsordnung lebendig zu halten. Sie soll der Regierung die Möglichkeit geben, der Öffentlichkeit ihre Arbeit zu erläutern, um sie dadurch in die Lage zu versetzen, an dem politischen Willensbildungsprozess hierüber teilzunehmen. Daneben soll sie es der Bundesregierung ermöglichen, den Bürger*innen auch unpopuläre Maßnahmen zu erklären und damit Verständnis und Akzeptanz dafür zu schaffen. Zuletzt soll die Regierung den Bürger*innen ihre Rechte und Pflichten auf diesem Weg so erläutern, dass sie hiervon auch praktisch Gebrauch machen können.⁵⁷

Diese Gründe, die das BVerfG in den 1970er Jahren für eine verfassungsrechtliche Pflicht der Bundesregierung zur Öffentlichkeitsarbeit anführte, sind heute noch ebenso tragfähig wie damals. Allerdings stellte das Verfassungsgericht bereits 2002 in seinen sogenannten Osho- und Glykol-Entscheidungen zum staatlichen Informationshandeln fest: „*Die staatliche Teilhabe an öffentlicher Kommunikation hat sich im Laufe der Zeit grundlegend gewandelt und verändert sich unter den gegenwärtigen Bedingungen fortlaufend weiter.*“⁵⁸ Statt Fernsehen, gucken Bürger*innen heute YouTube, statt der Tageszeitung lesen sie ihren Twitter-Feed. Diesen veränderten Kommunikationsgewohnheiten des Staatsvolkes muss sich auch die Bundesregierung anpassen, will sie dieses Volk mit ihrer Öffentlichkeitsarbeit erreichen. Sie muss deshalb dort über ihre Arbeit informieren, wo eine immer größere Gruppe von Bürger*innen diese Informationen auch tatsächlich wahrnimmt: im Internet.⁵⁹ Die verfassungsrechtliche Pflicht der Bundesregierung zur Öff-

Friehe, Facebook, Twitter und Regierung, in: Uhle (Hrsg.), Information und Einflussnahmen, Berlin 2018, S. 81, S. 105 ff.

56 BVerfG, Urt. v. 02.03.1977 – Az. 2 BvE 1/76, BVerfGE 44, 125, 147.

57 BVerfG (Fn. 56), 147 f.

58 BVerfG, Beschl. v. 26.06.2002 – Az. 1 BvR 558/91 u. a., BVerfGE 105, 252, 268; Beschl. v. 26.06.2002 – Az. 1 BvR 670/91, BVerfGE 105, 279, 301.

59 In diese Richtung allgemein für die staatliche Öffentlichkeitsarbeit auch Milker, Äußerungen von Hoheitsträgern im Wahlkampf und darüber hinaus, JA 2017, 647, 654; ders., Die Polizei auf Twitter – Brauchen wir ein Social-Media-Gesetz für staatliche Stellen?, NVwZ 2018, 1751, 1753; Müller-Franken, Unzulässige Staatsmedien oder zulässige Informationstätigkeit?, AfP 2016, 301, 306/308.

fentlichkeitsarbeit umfasst damit heutzutage die Verpflichtung, (auch) in den sozialen Medien präsent zu sein.⁶⁰

2.2.3 Das Blockieren von Medienvertreter*innen auf Social Media

Gibt die Bundesregierung den Bürger*innen auf ihren Social-Media-Profilen Einblicke in ihre Arbeit, eröffnet sie damit auch eine neue Informationsquelle für Medienvertreter*innen, die über die Bundespolitik berichten. Aus deren bereits im Zusammenhang mit Akkreditierungen angeführten Recht auf Gleichbehandlung im publizistischen Wettbewerb (Art. 5 Abs. 1 S. 2 i. V. m. Art. 3 Abs. 1 GG) folgt ein Anspruch darauf, der Bundesregierung in den sozialen Medien unter gleichen Bedingungen folgen zu können. In Anbetracht der Bedeutung, die der regierungsamtlichen Kommunikation über die sozialen Medien heutzutage zukommt, müssen Journalist*innen hierzu ebenso gleichberechtigten „Zutritt“ erhalten wie zu klassischen Pressekonferenzen.

Die Bundesregierung muss Medienvertreter*innen den Zugriff auf ihre Social-Media-Profile, also nach allgemeinen, sachgerechten Kriterien ermöglichen. Die Voraussetzungen für ihren Ausschluss von diesen Profilen sind hoch, weil ein Teil der grundrechtlich geschützten Informationsbeschaffung der Journalist*innen damit vereitelt wird. Aus Kapazitätsgründen kann die Regierung die Medienvertreter*innen – anders als zum Beispiel von Pressereisen – nicht ausschließen, existieren doch keine Grenzen für die Anzahl der Fans und Follower in den sozialen Medien. Möglich ist ein Ausschluss aber – ebenso wie etwa bei Pressereisen –, wenn hinreichende Anhaltspunkte für ein störendes Verhalten der betroffenen Medienvertreter*innen vorliegen. Übt ein Journalist auf dem Social-Media-Profil der Bundesregierung etwa Schmähkritik und verletzt er dadurch das allgemeine Persönlichkeitsrecht Dritter, kann hiergegen vorgegangen werden.

Ebenso wenig wie die Bundesregierung den Medienvertreter*innen allerdings die Akkreditierung zu analogen Veranstaltungen aufgrund ihrer bisherigen oder zukünftigen Berichterstattung versagen darf, kann sie

⁶⁰ Anders aber *Frevert/Wagner*, Rechtliche Rahmenbedingungen behördlicher Internetauftritte, NVwZ 2011, 76, 81, die der Ansicht sind, die Nutzung sozialer Netzwerke gehe über den gebotenen Minimalstandard an staatlicher Öffentlichkeitsarbeit hinaus.

solche Berichte zum Anlass nehmen, Journalist*innen von ihren Auftritten in den sozialen Medien auszuschließen.⁶¹

Selbst wenn ein Grund für einen Ausschluss einmal vorliegt, wäre es zudem oft unverhältnismäßig, dem betroffenen Medienvertreter den Zugriff auf das Profil der Bundesregierung endgültig zu versperren.⁶² Meist dürfte es nicht erforderlich sein, ihn langfristig zu blockieren, weil stattdessen ein abgestuftes Vorgehen gewählt werden kann: Milder und ebenso effektiv dürfte es häufig sein, erst einmal den konkreten rechtsverletzenden Beitrag zu löschen. Im nächsten Schritt könnte ein Journalist, der sich regelmäßig auf diese Weise äußert, temporär gesperrt werden. Erst als Ultima Ratio, nämlich wenn die anderen Maßnahmen nicht dazu geführt haben, dass er sich rechtsverletzender Beiträge enthält, dürfte der Zugriff des Journalisten auf das Profil der Regierung endgültig beendet werden.

Das Recht auf eine ermessensfehlerfreie Entscheidung über diesen Zugriff, das aus dem Recht auf Gleichbehandlung im publizistischen Wettbewerb folgt, verdichtet sich immer dann zu einem Anspruch auf Zugriff auf das Social-Media-Profil, wenn in der Person des Journalisten keiner der beschriebenen Gründe für einen Ausschluss vorliegt. Auch diesbezüglich besteht eine Parallele zur Entscheidung der Bundesregierung über die Akkreditierung von Medienvertreter*innen. Blockiert die Regierung Journalist*innen auf ihren Profilen in den sozialen Medien, können sie ihren Anspruch im Wege der allgemeinen Leistungsklage – womöglich verbunden mit einem Antrag auf Erlass einer einstweiligen Anordnung nach § 123 VwGO – vor den Verwaltungsgerichten durchsetzen.

2.2.4 Die Pflicht zur Pressearbeit

Die Verpflichtung der Bundesregierung, die Allgemeinheit – und damit als Reflex auch die Medienvertreter*innen – auf Social Media über ihre

61 So allgemein für das Blockieren der Nutzer*innen aufgrund von Meinungsäußerungen, die öffentlichen Stellen nicht genehm sind, auch die Wissenschaftlichen Dienste des Deutschen Bundestages, WD 3 – 3000 – 044/18, S. 4; *Kalscheuer/Jacobsen*, Das digitale Hausrecht von Hoheitsträgern, NJW 2018, 2358, 2362.

62 Vergleiche die Wissenschaftlichen Dienste des Deutschen Bundestages (Fn. 61), S. 4f.; *Kalscheuer/Jacobsen* (Fn. 61), 2362; *Milker*, Die Polizei auf Twitter (Fn. 59), 1756.

Arbeit zu informieren, bedeutet nicht, dass sie sich ganz auf diese Kanäle verlassen darf. Vielmehr ist sie aus grundrechtlicher Sicht gehalten, zusätzlich zur Öffentlichkeitsarbeit in den sozialen Medien auch klassische Pressearbeit zu betreiben.⁶³

Die Medienfreiheiten gemäß Art. 5 Abs. 1 S. 2 GG sind schließlich nicht nur subjektive Abwehrrechte der Medienvertreter*innen gegen den Staat, die ihn daran hindern sollen, in ihre Arbeit einzugreifen. Sie enthalten zudem in objektiv-rechtlicher Hinsicht den Auftrag an den Staat, die Voraussetzungen dafür zu schaffen, dass von den Medienfreiheiten tatsächlich Gebrauch gemacht werden kann.⁶⁴ Die Medien sind schließlich schlechthin konstituierend für die freiheitliche demokratische Grundordnung.⁶⁵ Daraus folgt für die Bundesregierung, dass sie ihr Ermessen bei der Entscheidung über das Ob und Wie der Öffentlichkeits- und der Pressearbeit im Lichte der Medienfreiheiten ausüben muss.

Politischen Medien, die über die Arbeit der Regierung berichten wollen, wird ihre funktionsgemäße Betätigung erst dadurch ermöglicht, dass diese sich umfassend bei jener Arbeit beobachten lässt, Auskunft hierüber gibt und, wo nötig, Rückfragen ermöglicht. Über ihre Profile in den sozialen Medien gibt die Bundesregierung zwar Einblicke in ihre Arbeit – jedoch nicht in einer Weise, welche die Vertreter*innen der politischen Medien umfassend informiert. So verläuft die Kommunikation zum Beispiel im Grundsatz einseitig von der Regierung hin zu den Bürger*innen. Wirkliche, womöglich auch kritische Rückfragen sind nicht möglich. Auch entscheidet die Regierung selbst, welche Ereignisse sie auf Instagram oder Facebook präsentiert und welche Aspekte ihrer Arbeit der Öffentlichkeit vorenthalten werden. Eine umfassende und kritische Berichterstattung über die Regierungsarbeit, die gerade Aufgabe der politischen Medien ist, wird dadurch nicht ermöglicht.

Die objektiv-rechtliche Komponente der Medienfreiheiten fordert von der Bundesregierung deshalb, über ihre Präsenz in den sozialen Medien hinaus auch weiterhin klassische Pressearbeit zu betreiben. Teils kön-

⁶³ So auch schon *Friehe* (Fn.55), S.14.

⁶⁴ *Bethge*, in: Sachs (Hrsg.), Grundgesetz, 8. Aufl., München 2018, Art. 5 Rn. 73; *Grabenwarter*, in: Maunz/Dürig (Begr.), Grundgesetz, 86. EL, München Januar 2019, Art. 5 Abs. 1 Rn. 353; *Schulze-Fielitz*, in: Dreier (Hrsg.), Grundgesetz, 3. Aufl., Tübingen 2013, Art. 5 I, II Rn. 213.

⁶⁵ Ständige Rechtsprechung, siehe nur BVerfG (Fn. 46); 121; Beschl. v. 24.05.2005 – Az. 1 BvR 1072/01, BVerfGE 113, 63, 82; Urt. v. 27.02.2007 – Az. 1 BvR 538/06 u. a., BVerfGE 117, 244, 258.

nen Medienvertreter*innen auf die Einhaltung dieser Pflicht hinwirken, indem sie ihren verfassungsunmittelbaren Auskunftsanspruch, der aus den Medienfreiheiten folgt, gegenüber der Regierung geltend machen.⁶⁶ Diesen Anspruch können sie im Wege der allgemeinen Leistungsklage vor den Verwaltungsgerichten durchsetzen.⁶⁷ Der Auskunftsanspruch gewährt den Journalist*innen allerdings nur einen Minimalstandard an Auskünften zu einzelnen Fragen.⁶⁸ Ein einklagbares Recht darauf, dass die Bundesregierung darüber hinaus Pressekonferenzen und Pressereisen veranstaltet oder dass Angela Merkel für einzelne Medieninterviews zur Verfügung steht, folgt hieraus dagegen nicht.

2.3 Pressefreiheit in den USA – Yay or Nay?

2.3.1 CNN v. Trump

In Anbetracht der verfassungsrechtlichen Rahmenbedingungen in Deutschland, die den Journalist*innen bei ihrer Arbeit einen umfassenden Schutz gewähren, ist im dritten Teil dieses Beitrags aus amerikanistischer Sicht zu fragen, weshalb in den USA die eingangs beschriebenen Angriffe auf die Medien möglich sein können.

Bezeichnend ist hier erneut der Fall Jim Acostas: Nachdem ihm seine Dauerakkreditierung entzogen worden war, beschloss der Fernsehsender CNN, über diese Behandlung seines Mitarbeiters nicht hinwegzusehen, da das Weiße Haus seiner Ansicht nach Acostas „First Amendment Rights“ („Freedom of Speech“/„Freedom of Press“) verletzt hätte. Acosta hatte zwischenzeitlich zwar versucht, eine vorläufige Akkreditierung für das Weiße Haus zu erhalten, diese war ihm jedoch verweigert worden.⁶⁹ Am 13. November 2018 reichten CNN und Acosta daher Klage beim U. S. District Court for the District of Columbia ein. Das Gerichts-

66 Siehe zu diesem Anspruch nur BVerwG, Urt. v. 20.02.2013 – Az. 6 A 2/12, BVerwGE 146, 56, 64; Urt. v. 25.03.2015 – Az. 6 C 12/14, BVerwGE 151, 348, 355; Urt. v. 16.03.2016 – Az. 6 C 65/14, BVerwGE 154, 222, 225.

67 Siehe zur Diskussion um die statthafte Klageart nur Bernzen, „Lachst Du noch oder klagst Du schon?“, VBIBW 2017, 434, 435.

68 BVerwG (Fn. 66), 64; (Fn. 66), 355.

69 *Nover*, The Looming Legal Battle Over Jim Acostas Press Pass, www.theatlantic.com v. 13.11.2018, abrufbar unter <<https://www.theatlantic.com/politics/archive/2018/11/cnn-sues-trump-revoking-jim-acostas-credentials/575788/>> (Stand: 21.09.2020).

verfahren CNN v. Trump⁷⁰ sollte klarstellen, dass die Pressefreiheit eine besonders schutzwürdige verfassungsrechtliche Position ist, die auch der Präsident zu beachten hat.⁷¹ Der Nachrichtensender erhielt hierbei Unterstützung durch Amicus Curiae-Schriftsätze aus dem rechtswissenschaftlichen wie dem journalistischen Bereich⁷² – selbst von dem Nachrichtensender Fox News,⁷³ der eher der Trump-Regierung nahesteht und ein erbitterter Gegner CNNs ist.

Zuständig für den Fall CNN v. Trump war Timothy Kelly, ein von Präsident Trump eingesetzter Richter.⁷⁴ Er entschied, dass Acosta seine Akkreditierung vorläufig zurückerhalten müsse, da ihr plötzlicher Entzug ohne eine vorherige Verwarnung oder Anhörung des betroffenen Journalisten dessen Recht auf ein ordnungsgemäßes Verfahren gemäß des fünften Verfassungszusatzes („Due Process“) verletzt habe.⁷⁵ Presseberichten nach hätte das Weiße Haus nicht hinreichend darlegen können, weshalb man Acosta die Akkreditierung ohne Vorwarnung entzogen hätte, und sich zudem im Rahmen von Erklärungsversuchen in widersprüchliche Aussagen verstrickt.⁷⁶

Diese Entscheidung war ein Etappensieg für Acosta und den Nachrichtensender CNN sowie ein Schlag gegen Trumps Willkür. Dennoch darf nicht außer Acht gelassen werden, dass Acosta seine Akkreditierung

70 Az. 1:18-cv-02610-TJK.

71 Siehe für die Details der Argumentation den klägerseitigen Schriftsatz, abrufbar unter <<https://edition.cnn.com/2018/11/13/media/cnn-sues-trump-full-complaint/index.html>> (Stand: 21.09.2020).

72 Siehe nur die Amicus Curiae-Schriftsätze des *Georgetown Law's Institute for Constitutional Advocacy and Protection* und des *Reporters Committee for Freedom of the Press*, abrufbar unter <https://www.rcfp.org/wp-content/uploads/imported/20181113_103841_20181113cnvdonaldjtrump.pdf> sowie der *White House Correspondents' Association*, abrufbar unter <<https://www.politico.com/f/?id=00000167-186d-def8-a56f-98ef20150002>> (Stand beider: 21.09.2020).

73 *Anapol*, Fox News, other outlets back CNN's lawsuit against Trump administration, *www.thehill.com* v. 14.11.2018, abrufbar unter <<https://thehill.com/homenews/media/416630-fox-news-backs-cnns-lawsuit-against-trump-administration>> (Stand: 21.09.2020).

74 Vergleiche *Kellys* Profil auf der Website des U.S. District Court for the District of Columbia, abrufbar unter <<https://www.dcd.uscourts.gov/content/district-judge-timothy-j-kelly>> (Stand: 21.09.2020).

75 Protokoll der gerichtlichen Verhandlung vom 16.11.2018, S.6 ff., abrufbar unter <https://upload.wikimedia.org/wikipedia/commons/9/99/CNN_v._Trump_transcript_2018-11-16.pdf> (Stand: 21.09.2020).

76 *Schwartz*, Judge orders White House to return press credentials to CNN's Acosta, *www.politico.com* v. 16.11.2018, abrufbar unter <<https://www.politico.com/story/2018/11/16/judge-orders-white-house-to-return-press-credentials-to-cnns-acosta-995512>> (Stand: 21.09.2020).

vorläufig auf der Grundlage des fünften Verfassungszusatzes („Due Process“) zurückkehrte und nicht auf der Grundlage des ersten Verfassungszusatzes. Der zuständige Richter betonte, dass dies damit zu begründen sei, dass die Reichweite dieses sehr schnellen Urteils begrenzt sei und die Berufung auf den fünften Verfassungszusatz ausschlaggebend für eine Entscheidung zugunsten Acostas gewesen sei.⁷⁷ Reporter*innen gegenüber stimmte er jedoch der Regierung darin zu, dass der erste Verfassungszusatz nicht bedeute, dass Journalist*innen generell der Zugang zum Weißen Haus gewährt werden müsse. Sobald sie allerdings zugelassen worden seien, schütze das Recht auf Pressefreiheit gemäß des „First Amendment“ ihre Arbeit.⁷⁸

Wie sich der Fall CNN v. Trump vor Gericht weiterentwickelt hätte, bleibt offen, da sich das Weiße Haus nach der Eilentscheidung dazu entschloss, Acosta seine Dauerkreditierung zurückzugeben.⁷⁹ Im Zusammenhang mit dieser Rückgabe erließ Trump jedoch eine Reihe von „Verhaltensregeln“ für künftige Pressekonferenzen, die ihm einen großen Spielraum bei der Gestaltung solcher Veranstaltungen gewähren.⁸⁰ Der durchaus gefährdeten Pressefreiheit in den USA hätte es jedoch sicherlich nicht geschadet, wenn der Prozess bis zu Ende geführt und in diesem Zuge auch die Pressefreiheit, die im ersten Verfassungszusatz verankert ist, thematisiert worden wäre.

2.3.2 Presse- und Medienfreiheit in den USA und in Deutschland: Ein Vergleich aus amerikanistischer Sicht

Das Beispiel Jim Acostas zeigt, wie unterschiedlich das Recht auf Pressefreiheit in den USA im Vergleich mit den Medienfreiheiten in Deutschland gehandhabt wird. In Deutschland sind die Medienfreiheiten gemäß Art. 5 Abs. 1 S. 2 GG – wie erörtert – nicht nur subjektive Abwehrrechte gegen den Staat. Aus ihrer Garantie erwächst auch die Pflicht des Staa-

⁷⁷ Protokoll (Fn. 75), S. 20.

⁷⁸ Schwartz (Fn. 76).

⁷⁹ Siehe die „Notice of Voluntary Dismissal Without Prejudice“ v. 19.11.2018, abrufbar unter <<https://justlawfulblog.files.wordpress.com/2018/11/cnn-v-trump-voluntary-dismissal.pdf>> (Stand: 21.09.2020).

⁸⁰ Choi, White House issues rules for the media after it reinstates CNN correspondent Jim Acosta's press pass, *www.businessinsider.de* v. 20.11.2018, abrufbar unter <<https://www.businessinsider.de/white-house-press-rules-cnn-jim-acosta-2018-11?r=US&IR=T>> (Stand: 21.09.2020).

tes, die Betätigung der Freiheiten zu ermöglichen. In den Vereinigten Staaten wird das Recht auf Pressefreiheit meist anders verstanden. Es enthält hier, wie im Fall *Acostas* zu sehen ist, vor allem ein subjektives Abwehrrecht gegen den Staat.⁸¹

Das Recht auf Pressefreiheit ist in der amerikanischen Verfassung nicht detailliert geregelt, sondern wird stark durch die Interpretation des zuständigen Richters beeinflusst. Oft besteht keine Einigkeit darüber, was genau durch den ersten Verfassungszusatz geschützt wird und aus welchen Gründen.⁸² Die „Amendments to the U.S. Constitution“ sind sehr allgemein formuliert, sodass bei ihrer Anwendung ein enormer Auslegungsspielraum bleibt. Dies ist insbesondere der Fall, wenn es um Konzepte wie „Freedom“, „Liberty“ oder „Equality“ geht, da deren Interpretation stark vom persönlichen Verständnis des jeweils zuständigen Richters abhängig ist.⁸³ Ein Teil dieses Phänomens liegt auch in der Grundstruktur der amerikanischen Rechtsordnung begründet, in der Gesetze aufgrund des Systems des Fallrechts („Case Law“) nicht die primäre Rechtsquelle darstellen.⁸⁴ Der Einfluss der Richter*innen auf die Auslegung der oft sehr vage formulierten Konzepte in den Verfassungszusätzen ist daher sehr groß.

Dieses Problem prägte beispielsweise auch die sogenannte „Marriage Equality“-Debatte, in der gleichgeschlechtliche Paare und ihre Unterstützer*innen um die Ehe für alle in den USA kämpften. Sie stützten ihre Forderungen, wie die Bezeichnung „Marriage Equality“ bereits verrät, auf den Grundsatz der Gleichheit aller Amerikaner*innen, wie im „Equal Protection Clause“ des vierzehnten Verfassungszusatzes beschrieben.⁸⁵ Hierbei bestand jedoch das gleiche Problem wie bei der Pressefreiheit, die im ersten Verfassungszusatz garantiert wird: Der Staat darf die Rechte der Bürger*innen im Hinblick auf die Ehe nicht beschneiden. Dies bedeutet jedoch nicht automatisch, dass der Staat auch, in einem ersten Schritt, ein gleiches Recht für alle schaffen muss. Im Fall *Obergefell v. Hodges*⁸⁶ legte eine Mehrheit von 5–4 Richter*innen

81 Vergleiche *Neuborne*, in: Morrison (Hrsg.), *Fundamentals of American Law*, New York 1996, S. 100 f.

82 Vergleiche *Neuborne* (Fn. 81), S. 22.

83 Vergleiche *Neuborne* (Fn. 81), S. 22.

84 Vergleiche *Neuborne* (Fn. 81), S. 22.

85 *Franklin*, *Marrying Liberty and Equality: The New Jurisprudence of Gay Rights*, *Va. L. Rev.* 100 (2015) 817, 820.

86 US Supreme Court, Urt. v. 26.06.2015 – Az. 576 U.S. (2015).

den vierzehnten Verfassungszusatz zu Gunsten homosexueller Paare aus und entschied, dass alle Staaten die Ehe für gleichgeschlechtliche Partner*innen erlauben müssen und kein rechtlicher Unterschied zur Ehe von heterosexuellen Paaren bestehen darf.⁸⁷ Diese Auslegung des vierzehnten Verfassungszusatzes im Fall Obergefell v. Hodges hätte jedoch bei einer anderen Konstellation der Richter*innen am Obersten Gericht der USA auch anders ausfallen können.

2.3.3 Die amerikanische Pressefreiheit in Zahlen

Wie schlecht es derzeit um die Pressefreiheit in den USA steht, lässt sich nicht nur anlässlich von Vorfällen wie den eingangs beschriebenen Situationen erahnen, sondern auch an konkreten Zahlen festmachen. Die international tätige Nichtregierungsorganisation Reporter ohne Grenzen veröffentlicht jedes Jahr die „Rangliste der Pressefreiheit“. Während Deutschland einen soliden 13. Platz aus 180 Ländern belegt und sich somit mit anderen westlichen Ländern im Spitzenfeld bewegt, sind die Vereinigten Staaten weit abgeschlagen.⁸⁸ Derzeit belegen die USA den 48. Platz der Rangliste und liegen damit noch hinter einigen afrikanischen Ländern, die Präsident Trump auch schon als „Shithole Countries“⁸⁹ bezeichnete.⁹⁰

Der U.S. Press Freedom Tracker, eine Initiative der Freedom of the Press Foundation und des Committee to Protect Journalists in Kollaboration mit weiteren Partner*innen, kommt zu ähnlichen beunruhigenden Ergebnissen. Journalist*innen erleben in den USA einen hohen Grad an Feindseligkeit, sowohl von Regierungsseite auf Bundes- und Lokalebene als auch von Seiten der Bevölkerung. Im ersten Halbjahr des Jahres 2019 waren der Organisation bereits acht Festnahmen von Journalist*innen in den USA bekannt sowie zwanzig Angriffe und acht

87 „They ask for equal dignity in the eyes of the law. The Constitution grants them that right“, so die Mehrheit der Richter*innen in ihrer Entscheidung, siehe (Fn. 86), S. 22.

88 *Reporter ohne Grenzen*, Rangliste der Pressefreiheit 2019, abrufbar unter <https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Downloads/Ranglisten/Rangliste_2019/Rangliste_der_Pressefreiheit_2019.pdf> (Stand: 21.09.2020).

89 *Vitali/Hunt/Thorp*, Trump referred to Haiti and African nations as “shithole” countries, *www.nbcnews.com* v. 11.01.2018, abrufbar unter <<https://www.nbcnews.com/politics/white-house/trump-referred-haiti-african-countries-shithole-nations-n836946>> (Stand: 21.09.2020).

90 *Reporter ohne Grenzen* (Fn. 88).

Fälle, in denen Journalist*innen an der Grenze festgehalten wurden.⁹¹ Im Juni 2018 kam es zu einer Schießerei in der Redaktion der Capital Gazette in Annapolis, Maryland, bei der fünf Journalist*innen zu Tode kamen. Die örtlichen Behörden bestätigten, dass der Angriff der Zeitung als Ganzes galt und der Schütze bereits aus einem Rechtsstreit gegen die Capital Gazette bekannt war.⁹²

Eine 2018 durchgeführte Umfrage des führenden Meinungsforschungsinstituts Gallup bestätigt die Vermutung, dass die amerikanische Bevölkerung immer weniger von der Glaubwürdigkeit der Nachrichtenmedien überzeugt ist. 94 % der Republikaner*innen, 66 % der Moderaten und 42 % der Demokrat*innen sagen, dass sie das Vertrauen in die Medien verloren haben. Dabei finden sich in dieser Gruppe mehr Männer als Frauen, mehr Weiße als Nicht-Weiße und mehr Personen ohne Collegeabschluss als Collegeabsolvent*innen.⁹³

Auch wenn dies sicherlich eine schleichende Entwicklung war, trägt Trumps Verhalten offenbar zu einer rapiden Verschlechterung der Situation bei. Zahlen wie die soeben genannten sind besorgniserregend, da sie zeigen, dass die Medien als die vierte Gewalt im Staat enorm an Einfluss und Glaubwürdigkeit verloren haben. Insbesondere die Tatsache, dass neun von zehn Republikaner*innen das Vertrauen in die Arbeit von Journalist*innen verloren haben, zeigt, wie erfolgreich Trump bei seiner Wählerschaft mit seinen Anschuldigungen von „Fake News“ und den „Enemy of the People“ ist.

2.3.4 Gesellschaftliche Konsequenzen einer bedrohten Pressefreiheit

Die Pressefreiheit gilt auch in den USA als eine der tragenden Säulen der Demokratie. Nur mit ihrer Hilfe können sich Bürger*innen umfas-

91 U.S. Press Freedom Tracker, ständig aktualisiert und abrufbar unter <<https://pressfreedomtracker.us/>> (Stand: 21.09.2020).

92 Romo/Hernandez/Brown/Neumann, Maryland Newsroom Shooting That Left 5 Dead Was “Targeted Attack”, www.npr.org v. 28.06.2018, abrufbar unter <<https://www.npr.org/2018/06/28/624392089/active-shooter-at-maryland-newspaper?t=1564067622960>> (Stand: 21.09.2020).

93 Knight Foundation, Indicators of News Media Trust, www.knightfoundation.org v. 11.09.2018, abrufbar unter <<https://www.knightfoundation.org/reports/indicators-of-news-media-trust>> (Stand: 21.09.2020).

send informieren und dadurch ihr Recht auf aktive politische und gesellschaftliche Teilhabe bestmöglich ausüben. Nur mit ihrer Hilfe kann das Handeln von Entscheidungsträger*innen kritisch beleuchtet und können Missstände aufgedeckt werden. Die Demokratie und die freie Presse müssen untrennbar miteinander verbunden sein, um einen wirkungsvollen Schutz vor autoritären Herrschaftsformen zu garantieren, wie der Journalist Marvin Kalb in seiner Monographie „Enemy of the People: Trump’s War on the Press, the New McCarthyism, and the Threat to American Democracy“ betont:

“A free press guarantees a free society, a functioning and, one hopes, flourishing democracy. Therefore, when a president attacks the press as an ‘enemy of the people’, he is doing more than delegitimizing, demeaning, and trivializing the so-called fourth branch of government. He is also attacking the very foundation of American democracy – and he must be challenged and either stopped or somehow persuaded to change his ways”⁹⁴.

Der amerikanische Präsident hat erkannt, dass der Journalismus am leichtesten bei seiner Glaubwürdigkeit anzugreifen ist, denn damit trifft er ihn im Kern seines Daseins. Wenn die Bevölkerung das Vertrauen in die Glaubwürdigkeit des Journalismus verliert, wird dieser gleichzeitig seiner Existenzberechtigung entledigt. Trump verfolgt im Hinblick auf die Presse eine perfide Strategie, wie er selbst gegenüber der CBS-Korrespondentin Lesley Stahl bestätigte. Sie hatte ihn auf seine konstanten Attacken auf Medienvertreter*innen angesprochen, woraufhin er laut Stahl geantwortet haben soll: *“You know why I do it? I do it to discredit you all and demean you all so when you write negative stories about me, no one will believe you.”⁹⁵*

Wenn Donald Trump die Presse als Lügenpresse bezeichnet, ist dies offenbar Teil seiner langfristigen Strategie, die eigenen Lügen zu vertuschen und diejenigen zu entmachten, die ihm ernsthaft gefährlich werden könnten. Durch seine gleichbleibende Rhetorik in diesem Kontext und die beinahe zwanghafte Wiederholung von Phrasen wie „Fake News“ oder „Enemy of the People“ brennen sich diese Zuschreibungen in den

94 Kalb, Enemy of the People: Trump’s War on the Press, the New McCarthyism, and the Threat to American Democracy, Washington, D.C. 2018, S. 7.

95 CBS News, Lesley Stahl: Trump admitted mission to “discredit” press, [www.cbsnews.com v. 23.05.2018](https://www.cbsnews.com/news/lesley-stahl-donald-trump-said-attacking-press-to-discredit-negative-stories/), abrufbar unter <<https://www.cbsnews.com/news/lesley-stahl-donald-trump-said-attacking-press-to-discredit-negative-stories/>> (Stand: 21.09.2020).

Köpfen der Bürger*innen ein. Trump bagatellisiert und normalisiert Angriffe auf die Medien bis zu einem Punkt, an dem Attacken auf das „First Amendment Right“ von Journalist*innen gemeinhin als tolerierbar oder gar gerechtfertigt erachtet werden.

„*Democracy Dies in Darkness*.“ So lautet der derzeitige Slogan der Washington Post, mit dem die Zeitung versucht, auf die gesellschaftlichen Konsequenzen eines postfaktischen Zeitalters aufmerksam zu machen und damit den Gegner*innen journalistischer Arbeit den Kampf anzusagen.⁹⁶ Medienvertreter*innen können den Kampf jedoch nur gewinnen, wenn sie sich auf ihr höchstes Gut besinnen: die journalistische Glaubwürdigkeit. Daher sind sie in der Pflicht, noch genauer zu arbeiten und noch genauer zu recherchieren, um ihren Gegner*innen keine Angriffsfläche zu bieten. In Zeiten, in denen die Pressefreiheit in den USA kaum Schutz bietet, da der erste Verfassungszusatz plötzlich verhandelbar geworden scheint, sind Journalist*innen dort gefordert, sich stärker denn je selbst zu schützen. Dabei schützen sie nicht nur ihre Profession, sondern auch die Demokratie.

Nur solange die Pressefreiheit und deren Schutz eines der höchsten Güter in einer Demokratie sind, sind Wahlen und andere Entscheidungsprozesse auch wirklich demokratisch. Die Pressefreiheit wird im ersten Zusatzartikel zur amerikanischen Verfassung in einem Atemzug mit weiteren fundamentalen Grundrechten wie der Meinungs-, der Religions- und der Versammlungsfreiheit genannt. Alleine dies sollte den Bürger*innen verdeutlichen, dass es sich auch bei der Pressefreiheit um eine besonders schutzwürdige Rechtsposition handeln muss.

⁹⁶ Siehe zur Entstehungsgeschichte des Slogans *Farhi*, The Washington Post's new slogan turns out to be an old saying, [www.washingtonpost.com v. 24.04.2017](https://www.washingtonpost.com/lifestyle/style/the-washington-posts-new-slogan-turns-out-to-be-an-old-saying/2017/02/23/cb199cda-fa02-11e6-be05-1a3817ac21a5_story.html?utm_term=.e1d4fddd416b), abrufbar unter <https://www.washingtonpost.com/lifestyle/style/the-washington-posts-new-slogan-turns-out-to-be-an-old-saying/2017/02/23/cb199cda-fa02-11e6-be05-1a3817ac21a5_story.html?utm_term=.e1d4fddd416b> (Stand: 21.09.2020).

3 MUSIC DATA MINING

Fabian Rack/Dr. Klaus Frieler⁹⁷

Was macht erfolgreiche Musik aus? Haben sich Genreumbrüche und musikalische Revolutionen angebahnt? Gibt es unentdeckte Muster der Improvisation im Jazz? Welche Zusammenhänge bestehen zwischen Harmonie, Tongeschlecht, Sound und Textduktus? Die Musikwissenschaft sucht Antworten auf diese Fragen zunehmend mit automatisierter Analyse. Man spricht von Music Data Mining (MDM). Die Anwendungsfelder sind weit, sowohl in der (musik-)wissenschaftlichen Forschung als auch bei der Entwicklung kommerzieller Anwendungen.

Music Data Mining kann man als eine Spielart des Text-und-Data-Minings begreifen. Dabei werden Datensätze aus der Musik ausgewertet, um daraus Gesetzmäßigkeiten, Muster, Abweichungen zu destillieren. Letztlich geht es dabei um digitale, automatisierte Analyse von allen Arten von Daten (also nicht nur mit Fokus auf Texten), um daraus mit Hilfe eines Algorithmus Information über Muster, Trends und Korrelationen usw. zu extrahieren. Dies macht es in der Musik möglich, computergestützt Wissen aus Zehntausenden von Kompositionen, Lyrics und Aufnahmen zu gewinnen.

3.1 Anwendungsfelder

Was wird nun genau beim Mining mit der Musik gemacht? Ganz allgemein lässt sich der Vorgang wie folgt beschreiben: Die Musik, die zum Beispiel als Audioaufnahme oder in Notenform vorliegt, wird durch “Features” beschrieben. Das sind einzelne Parameter wie beispielsweise die Tonhöhe, Intensität (Lautstärke), Klangfarbe, das Tempo, die Instrumentierung, die Akustik der Aufnahmen, der Rhythmus, Melodien als horizontale, Harmonien als vertikale Tonfolgen⁹⁸ und viele mehr. Das Entnehmen dieser Features ist der Zwischenschritt, der dann in der Datenanalyse zu einer bestimmten Erkenntnis führen kann; sie wiederum mündet in einer Anwendung oder hilft dabei, eine musikwissenschaftli-

⁹⁷ Mehr über die Autoren erfahren Sie im Autor*innenhinweis auf S. 109 und S. 107.

⁹⁸ *L/Li*. Music Data Mining: An Introduction. In *Li, Tao/Ogihara, Mitsunori/Tzanetakis, George* (Hrsg.), *Music Data Mining*. Florida: CRC Press (2011), S. 6.

che Forschungsfrage zu beantworten. Mit Hören oder Notenlesen durch Menschen wäre dies kaum zu bewältigen – Music Data Mining hebt die Erkenntnissuche auf ein neues Niveau.

Folgende Anwendungen machen sich das Music Data Mining zunutze:

- **Musiksuche.** Musikbestände werden computergestützt verarbeitet, indem Features extrahiert werden, um damit Musik auffindbar zu machen und so beispielsweise Musikredaktionen zu unterstützen. So lässt etwa der SWR seinen Musikbestand von zwei Millionen Audiodateien analysieren. Dabei soll ein Hochleistungscomputer ähnlich klingende Musiktitel erkennen, um etwa die Suche nach passender Hintergrundmusik für die Beiträge des Senders zu erleichtern. 700 Features sollen dabei benutzt werden.⁹⁹
- **Automatische Transkription** von Audioaufnahmen als Standardaufgabe des MIR (Music Information Retrieval). Hier erfolgt die Umschrift in Notenform, die dann als Beschreibung eines Werkes dienen kann. In moderneren Ansätzen werden allerdings diese Features oft nicht mehr im Voraus definiert, sondern von künstlichen neuronalen Netzen implizit mitgelernt, was direkte Zuordnungen von Audioaufnahmen auf komplexen Eigenschaften erlaubt, z. B. Genre und Stil oder Stimmung und Emotionalität. Diese Zuordnung ist dann allerdings eine Black Box, d. h. man kann nicht mehr ablesen, warum ein Element in dieser oder jener Klasse gelandet ist.
- **Automatische Playlisterstellung**, die viele Streamingdienste anbieten. Sie beruht meistens auf einer Kombination von intrinsischen und extrinsischen Beschreibungen von Musik. Erstere sind die automatisch (oder auch wie bei Pandora händisch) extrahierten Features. Extrinsische Features wiederum sind Daten über das User-Verhalten auf dem Dienst. Anhand dieser Eigenschaften und des Musiknutzungsverhaltens¹⁰⁰ kann dann ein Algorithmus versuchen, automatisch eine Playlist mit ähnlichen, der Nutzerin ggf. noch unbekannten Musikstücken zu generieren.

99 S. die Pressemitteilung des High-Performance Computing Centers in Stuttgart, <https://www.hlrs.de/news/detail-view/2019-10-24/>, zuletzt abgerufen am 15. Januar 2020.

100 Die Untersuchung des Nutzungsverhaltens mit seinen u. a. datenschutzrechtlichen Implikationen ist nicht Gegenstand dieses Beitrags.

- **Audiofingerprinting** erlaubt es, Titel und Interpret eines Musikstücks direkt aus einem kurzen Ausschnitt zu ermitteln. So können Nutzer*innen kurze Ausschnitte mit ihrem Smartphone aufnehmen und an den Dienstleister senden. Beispiele sind Dienste wie Shazam und Soundhound. Audiofingerprinting wird auch von Musikverwertungsgesellschaften wie der GEMA eingesetzt, um automatisch Radiostationen oder Clubs abzuhören, um die Vergütung zu gewährleisten.¹⁰¹
- **Automatische Generierung von Musik.** Unternehmen wie JukeDeck (mittlerweile von der Social-Media-Plattform TikTok gekauft) generieren Musik automatisch mit Hilfe Künstlicher Intelligenz (KI),¹⁰² die wiederum auf MDM basiert. Generell fußt der ganze Bereich künstlicher Musikkompositionen mit neuronalen Netzen auf MDM.
- **Hit Song Science** ist ein Feld der Musikwissenschaft. Dabei wird anhand von Eigenschaften eines Songs dessen kommerzieller Erfolg vorhergesagt bzw. zu erklären versucht¹⁰³ – bislang oft aber nur mit geringem Erfolg.¹⁰⁴
- Die **Erforschung der Jazzimprovisation** ist ein weiteres Anwendungsgebiet. Dabei will die Forschung den Geheimnissen der Improvisation auf die Spur kommen.¹⁰⁵ Es kommt ein breites Feld an MDM- und MIR-Methoden zum Einsatz, etwa bei der DTL Pattern Similarity Search¹⁰⁶, die es erlaubt, nach melodischen Mustern in einer Menge von über 1.700 Jazzsolotranskriptionen zu suchen, die

101 <https://www.gema.de/en/news/press/advertising-monitoring-next-steps-towards-digitisation-launched/>, zuletzt abgerufen am 15. Januar 2020.

102 Ein besserer Begriff ist Machine Learning (ML), der das statistische Lernen von Algorithmen anhand großer Datenmenge beschreibt, da es dies ist, was künstliche neuronale Netze eigentlich tun, und was noch sehr wenig mit Intelligenz im eigentlichen Sinne zu tun hat (allerhöchstens eine Vorstufe dazu darstellt).

103 *Frieler/Jakubowski/Müllensiefen*, Is it the Song and Not the Singer? Hit Song Prediction Using Structural Features of Melodies. In *Musikpsychologie* Bd.25, Göttingen: Hogrefe Verlag (2015), S.41–54.

104 Es liegt die Vermutung nahe, dass extrinsische Faktoren (z. B. Airplay, PR-Aufwand, Vorbekanntheit) wichtiger sind als die musikalischen Eigenschaften per se. Denn sie werden in klassischen Verwertungsstrukturen von den Beteiligten (Musiker, Komponisten, Produzenten, A&R Manager) streng in Hinsicht auf kommerzielles Potential selektiert, bevor es überhaupt zu einer Veröffentlichung kommt.

105 *Pfleiderer, M., Frieler, K., Abeßer, J., Zaddach, W.-G., & Burkhard, B.* (Eds.) (2017). *Inside the Jazzomat. New Perspectives for Jazz Research*.

106 <https://dig-that-lick.hfm-weimar.de/>, zuletzt abgerufen am 15. Januar 2020.

(zum größten Teil automatisch) aus Audioaufnahmen extrahiert wurden.¹⁰⁷

3.2 Mining und Recht

Zunächst einmal ist klar, dass Musik¹⁰⁸, die gemined wird, urheberrechtlichen Schutz genießen kann: sei es als Komposition und Text (also als Werke),¹⁰⁹ als Aufnahme mit Rechten der Tonträgerhersteller*innen¹¹⁰ bzw. der ausübenden Künstler*innen,¹¹¹ oder – etwas spezieller – in Form von Noten klassischer Musik, die als wissenschaftliche Ausgabe¹¹² geschützt sind. Je nach Anwendung und Epoche handelt es sich um zeitgenössische (Pop)Musik, die noch geschützt ist, oder um klassische Musik, bei der etwa nur Aufnahmen geschützt sind.

Doch ist Mining überhaupt urheberrechtlich relevant? So ganz pauschal lässt sich das nicht beantworten. Nähern kann man sich dieser Frage mit einem Petitum aus der Wissenschaft: *The Right to Read is the Right to Mine* – es dürfe keinen Unterschied machen, ob nun ein Mensch oder eine Maschine urheberrechtlich geschütztem Material Informationen entnimmt. Menschen dürfen Texte lesen, Musik hören oder Filme und Kunstwerke betrachten – verbotsfrei. Das nennt sich Werkgenuss.¹¹³ Zumindest dürfe Mining nicht vertraglich untersagt werden.

Dass allerdings der reine Werkgenuss urheberrechtlich stets unbedenklich ist, stimmt tendenziell nur für den analogen Bereich, etwa beim Lesen eines Buchs. Keine Neuigkeit hingegen ist es, dass beim digitalen

107 Frieler/Başaran/Höger/Crayencour/Peeters, Don't hide in the frames: Note- and pattern-based evaluation of automated melody extraction algorithms. In: Proceedings of the 6th International Conference on Digital Libraries for Musicology (DLfM '19), November 9, 2019, The Hague, Netherlands.

108 Wenn im Folgenden von „Musik“ die Rede ist, so ist damit musikalisches Material im weiten Sinne gemeint, also in Form von Kompositionen, Texten und geschützten Leistungen (Aufnahmen, Darbietungen etc.) auf allen denkbaren Trägern. Die derzeitige TDM-Schranke § 60d UrhG – sie wird spätestens zum 7. Juni 2021 abgelöst werden – bezeichnet Material, das der Analyse später zugeführt wird, als „Ursprungsmaterial“. Sie versteht darunter eine „Vielzahl von Werken“.

109 Schutz als persönliche geistige Schöpfung nach § 2 UrhG.

110 § 85 UrhG.

111 §§ 73 ff. UrhG.

112 § 70 UrhG.

113 Dreier in Dreier/Schulze UrhG 6. Aufl. 2018, § 15 Rn. 20 mwN.

Werkgenuss an vielen Stellen Kopien angefertigt werden. Die Verwertungsrechte sind so weit gefasst, dass fast alles eine urheberrechtlich relevante Kopie ist. Dann ist es auch egal, dass die Features, die man der Musik entnimmt (welche Tonart etc.), häufig ungeschützte, gemeinfreie Information sind – denn die gemeinfreie Information steckt oft in einer urheberrechtlich geschützten Hülle.¹¹⁴ Wer also Musikwerke in den Computer einspeist, sammelt, in andere Formate umwandelt oder archiviert, um sie dann zu analysieren, erstellt digitale Vervielfältigungen und greift zunächst einmal in Verwertungsrechte ein. Der Wissenschaft und den Kulturinstitutionen, die diese Techniken einsetzen wollen, machen die sehr weit gehenden Verwertungsrechte zu schaffen; sie waren fürs Digitale ursprünglich nicht konzipiert.¹¹⁵

Und dennoch ist eine forschungsgetriebene Analyse von Musik keine „klassische“ Musikverwertung: Es geht ja weder darum, ein Stück aufzuführen, digital zu verbreiten oder in einem Film zu verwenden. Es wird kaum weniger Musik verkauft oder gestreamt werden, nur weil ein Computer sie analysiert. Oftmals leisten Forschungseinrichtungen ja für den erstmaligen Zugang zur Musik bereits einen Beitrag (Kauf von Noten, MP3s etc.).

Weil aber die urheberrechtlichen Verwertungsrechte so unflexibel sind („Alles ist Kopie“), bestand Bedarf für eine gesetzliche Erlaubnis. Die Gesetzgeber haben auf nationaler und zuletzt auf EU-Ebene den Bedarf an erleichterten Bedingungen der Datenanalyse erkannt. Der Nutzen, insbesondere für die Wissenschaft, sei groß; der Schaden für Rechteinhaber*innen gering.¹¹⁶ Zunächst trat im Jahr 2018 in Deutschland erstmals eine Schranke spezifisch für TDM in Kraft (§ 60d UrhG).¹¹⁷ Sie erlaubt den Umgang mit urheberrechtlich geschütztem Material, darunter vor allem die Vervielfältigung und das beschränkte Zugänglichmachen für wissenschaftliche Reviews.

Im Sommer 2019 schließlich trat die Urheberrechtsrichtlinie für den Digitalen Binnenmarkt (RL (EU) 2019/790, im Folgenden kurz DSM)¹¹⁸.

¹¹⁴ So formuliert es *Raue* in ZUM 2019, 684, 685.

¹¹⁵ Vgl. *de la Durantaye/Raue*, RuZ 2020, 83, 84.

¹¹⁶ So wurde früher schon argumentiert, dass die Verwertungsrechte kaum betroffen seien, vgl. statt vieler *de la Durantaye*, Allgemeine Bildungs- und Wissenschaftsschranke, 2014, S. 240.

¹¹⁷ Zuvor hatte die EU-Kommission bereits eine TDM-Schranke in ihrem Richtlinienentwurf vorgeschlagen, siehe COM(2016) 593 final.

¹¹⁸ DSM steht für *digital single market*.

RL) in Kraft. Sie enthält zwei Erlaubnisse für TDM. Die eine zielt auf die nicht-kommerzielle Wissenschaft in öffentlichen Forschungsorganisationen¹¹⁹ sowie in Gedächtnisinstitutionen (Institutionen des kulturellen Erbes – also Museen, Bibliotheken, Archive und im Bereich des Film- oder Tonerbes tätige Einrichtungen, Art. 3 DSM-RL) ab; die andere auf kommerzielle Forschung und alle sonstigen Bereiche (Art. 4 DSM-RL). Art. 3 DSM-RL knüpft zusätzlich an die Eigenschaft der Institution an, die die Forschung betreibt bzw. der die Forschenden angehören, die minen. Nicht mehr im Rahmen von Art. 3 DSM-RL liegen die Institutionen, sobald sie etwa unter dem Einfluss gewerblicher Unternehmen stehen und diese Unternehmen Exklusivzugang zu Forschungsergebnissen erhalten sollen.¹²⁰ Institutionen dürfen sich aber der Hilfe Privater bedienen,¹²¹ womit sie z. B. Digitalisierungs- und Aufbereitungshandlungen in Auftrag geben können.

Ein wesentlicher Unterschied zwischen den Vorschriften besteht darin, dass bei der allgemeinen Mining-Schranke **Rechtevorbehalte** der Rechteinhaber*innen beachtet werden müssen. Das bedeutet, dass Rechteinhaber*innen die Datenanalyse untersagen und etwa von gesonderten Lizenzzahlungen abhängig machen können. Dies kann aber nur soweit gelten, wie überhaupt urheberrechtlich geschütztes Material gemined werden soll; gemeinfreies Material kann von solchen Verboten nicht erfasst sein. Bei Inhalten im Netz muss der Rechtevorbehalt zudem maschinenlesbar sein, damit er für automatisierte Mining-Prozesse überhaupt erkennbar ist;¹²² ein maschinenlesbarer Rechtevorbehalt kann technisch zum Beispiel über Robots.txt-Dateien verwirklicht werden. Wissenschaft und Gedächtnisinstitutionen, die unter Art. 3 DSM-RL fallen, dürfen solche Vorbehalte aber ignorieren.

Der zweite Unterschied zwischen beiden Vorschriften liegt darin, dass die Organisationen, die unter Art. 3 DSM-RL fallen, die Kopien der Korpora aufbewahren dürfen.

119 Darunter fallen Hochschulen und ihre Bibliotheken, Forschungsinstitute oder sonstige Einrichtungen, die entweder nicht gewinnorientiert arbeiten oder im öffentlichen Interesse tätig sind (Art. 2 Nr. 1 DSM-RL).

120 ErwGr. 13.

121 ErwGr. 11.

122 ErwGr. 18 Abs. 2. Klarstellung in der gesetzlichen Umsetzung fordert *Steinbrecher*, MMR 2019, 639, 640.

Die Gesetzgeber der EU-Mitgliedstaaten müssen die Richtlinie bis zum 7. Juni 2021 in nationales Recht umsetzen.¹²³ Es liegt ein Diskussionsentwurf des BMJV aus Januar 2020 vor, der einen neuen § 44b UrhG-E einführt (allgemeine Mining-Schranke), sowie einen überarbeiteten § 60d UrhG-E für die Wissenschaft.¹²⁴

3.3 Schritte des Minings im Einzelnen

Nach Art. 2 Nr. 2 DSM-RL bezeichnet Text und Data Mining „eine Technik für die automatisierte Analyse von Texten und Daten in digitaler Form, mit deren Hilfe Informationen unter anderem – aber nicht ausschließlich – über Muster, Trends und Korrelationen gewonnen werden können“. Es kann durchaus Schwierigkeiten bereiten, sämtliche oben dargestellten Anwendungen ohne Weiteres unter diese Definition fallen zu lassen. Teilweise handelt es sich nur um Formatumwandlungen, die mit keiner tieferen Analyse einhergehen (so etwa das Fingerprinting). Einen Grenzbereich könnte auch die Konstellation darstellen, dass das Mining betrieben wird, um die o. g. Anwendungsfelder wie Playlisterstellung etc. zu verbessern, wenn es also gar nicht um die Erforschung der Musik selbst geht. Allerdings müssen auch solche Handlungen erfasst sein, da es nur um irgendeine Art von Erkenntnisgewinn gehen muss und insoweit der Zweck der TDM-Erlaubnisse weit zu verstehen ist.

Unser Beitrag setzt im Folgenden einen Schwerpunkt bei der wissenschaftlichen Forschung, die überwiegend institutionell angebunden ist. Dafür durchlaufen wir ein Music-Mining-Schema, das an den Zyklus von Forschungsdaten¹²⁵ angelehnt ist. In diesem Zyklus wird musikalisches Material zunächst in seinen verschiedenen Erscheinungsformen

¹²³ Art. 29 UA 1 DSM-RL.

¹²⁴ Die Communia Association hat eine ausführliche Übersicht zu TDM in der DSM-RL und den Umsetzungsspielräumen für die Mitgliedstaaten erstellt, abrufbar unter <https://www.notion.so/Articles-3-4-Text-and-data-mining-9be17090ebc545b88ed9ac7d39e4e25a>.

¹²⁵ *de la Durantaye/Raue* beschreiben für die Digital Humanities in RuZ 2020, 83, 91 ff. – wenn auch nicht als Zyklus, sondern als Phasen bezeichnend – „Recherche- und Materialsammelphase/Aufbereitungsphase/Erkenntnisgewinnung/Ergebnispräsentation/Nachnutzungsphase“. Weitere Darstellungen finden sich etwa bei dem Research-Data-Management-Serviceteam des KIT („Plan & Fund/Collect & Analyze/Preserve & Store/Publish & Share/Discover & Reuse“) unter https://www.rdm.kit.edu/fodaten_zyklus.php.

gesammelt (1.) und aufbereitet (2.). Die aufbereitete Musik wird dann der Analyse zugeführt (3.). Die gewonnenen Erkenntnisse werden online präsentiert oder anderweitig verwertet (4.). Schließlich wird das aufbereitete Material zur Nachvollziehbarkeit oder für die Anschlussforschung aufbewahrt und für Fachkreise verfügbar gemacht (5.).

3.3.1 Zugang und Sammlung

Oftmals ist für die spätere Analyse eine lokale Kopie der Musik nötig. Diese Vervielfältigungen sind im Rahmen der TDM-Erlaubnisse nun **erlaubt**. „Texte und Daten“ als Untersuchungsgegenstand ist weit zu verstehen. Art. 3 DSM-RL spricht von „Werken und sonstigen Schutzgegenständen“, weshalb im Musikbereich auch das gesamte Spektrum an Werkarten und Leistungsschutzrechten erfasst ist.

3.3.1.1 Zugänge zur Musik

Die Mining-Erlaubnisse setzen bei den privilegierten Institutionen rechtmäßigen Zugang zur Musik voraus.¹²⁶ Dazu zählt etwa der Zugang zu Inhalten auf der Grundlage von Open-Access-Strategien, was vermutlich nur im Bereich gemeinfreier Musik relevant werden wird. Weiter erwähnt die DSM-RL vertragliche Vereinbarungen zwischen Rechteinhaber*innen und Forschungsorganisationen bzw. Einrichtungen des Kulturerbes. Im Internet „frei verfügbare“ Inhalte fallen gemäß der DSM-RL ebenfalls unter den rechtmäßigen Zugang.¹²⁷

Unproblematisch ist es, wenn der Umgang mit Musik weder vertraglich noch technisch eingeschränkt ist: CD oder Vinyl und in MP3-Shops erworbene Musikfiles ohne Kopierschutz, Leihgaben aus Musik- oder Tonträgerarchiven sowie Institutsbestände können kopiert und aufbereitet werden. Die Digitalisierung von analogem Material ist ebenfalls von den Erlaubnissen umfasst. Vielfach werden analoge Quellen digitalisiert, etwa beim Scan von Noten, dem digitalen Aufzeichnen von Schallplatten oder auch der Aufzeichnung von Konzerten. Die Digitalisierung von analogen Quellen sprechen die TDM-Schranken zwar nicht explizit

¹²⁶ Explizit in Art. 3 I DSM-RL.

¹²⁷ ErwGr. 14.

an.¹²⁸ Dem Zweck der TDM-Erlaubnis wird man allerdings nur gerecht, wenn man es auf Beschaffenheit und Trägerform der Musik nicht ankommen lässt.

Schwieriger wird es bei Streamingdiensten wie Spotify, Apple Music, Tidal usw. Denn dort werden Kopierschutzmaßnahmen eingesetzt, die nicht umgangen werden dürfen (vgl. § 95a UrhG). Ein Recht, den Kopierschutz selbst zu knacken, gibt es nicht – auch, wenn die Nutzung dann von der Schranke gedeckt wäre. Zwar existiert mit § 95b UrhG eine Regelung, die u. a. Forschenden einen Anspruch gegenüber Rechteinhabern gibt, ihnen die „notwendigen Mittel zur Verfügung zu stellen“, um von den Schrankenbestimmungen Gebrauch zu machen. Die Regelung gilt allerdings nicht bei Inhalten, die zum Online-Abruf bereitstehen (§ 95b Abs. 3 UrhG). Dies wäre bei Spotify und Co. der Fall. An dieser Stelle wird die TDM-Schranke also durchsetzungsschwach sein. Versiegen dann noch die Quellen von MP3-Download-Stores mit DRM-freier Musik und unterbinden Plattformen wie YouTube ihre aktuell noch einfache Downloadmöglichkeit technisch, könnte es schlecht um den gesetzgeberisch vorgesehenen Interessenausgleich stehen.

3.3.1.2 Musik-Scraping von Plattformen aus dem Netz

Downloads dürfen künftig auch automatisiert von Plattformen erfolgen. Denkbar ist aber, dass Plattformanbieter dies über Scraping-Verbote einschränken. Solche Verbote sind aber nur denkbar, soweit überhaupt Nutzungsverträge geschlossen werden. Bei YouTube beispielsweise ist es gemäß dem AGB-Abschnitt „Berechtigungen und Einschränkungen“ allgemein nicht zulässig, mit „automatisierten Verfahren (z. B. Robotern, Botnets oder Scrapern) auf den Dienst zuzugreifen“. YouTube macht hiervon wiederum Ausnahmen, so u. a. „soweit durch anwendbares Recht gestattet“.¹²⁹ Hierdurch signalisiert YouTube, die urheberrechtlichen Schranken nicht aushebeln zu wollen; und auch ein Mining-Vorbehalt – er wäre ja auch nur bei der allgemeinen TDM-Schranke nach Art. 4 DSM-RL wirksam – ist hier nicht herauszulesen. Die Rechteinhaber*innen dürfen allerdings für solche Vorgänge Zugriffsmöglichkeiten einschränken, damit ihre technische Infrastruktur

¹²⁸ Vgl. die Begriffsdefinition von TDM (Art. 2 Nr. 2 DSM-RL).

¹²⁹ <https://www.youtube.com/t/terms>, abgerufen am 3. Februar 2020.

nicht in die Knie geht. Sie dürfen die „Sicherheit und Integrität ihrer Netze und Datenbanken“ wahren, dabei aber nicht über das Notwendige hinausgehen.¹³⁰

3.3.1.3 Digitalisieren von Noten zu Mining-Zwecken

Noten haben urheberrechtlich gesehen einen gewissen Sonderstatus: Auch wenn die Musik schon gemeinfrei ist, muss der Schutz wissenschaftlicher Ausgaben (§ 70 UrhG) beachtet werden, und weiter ist selbst die Privatkopie nur unter sehr engen Voraussetzungen erlaubt. Das strenge Notenkopieverbot gilt aber für Mining-Zwecke nicht – Noten dürfen digitalisiert und in digitalisierter Form weiter kopiert werden.

3.3.1.4 Rechtmäßigkeit des Zugangs

Eine bemerkenswerte Konstellation erscheint uns Musikmaterial, das selbst urheberrechtlich inkriminiert ist. Zu denken ist hier an Remix- und Mashup-Inhalte, die – oft erkennbar – ohne Erlaubnis der Rechteinhaber*innen hochgeladen worden sind.

Es darf der Anwendung der Schranke jedenfalls nicht entgegenstehen, wenn einzelnes Ursprungsmaterial ohne Zustimmung der Rechteinhaber*innen zugänglich gemacht wurde. Denn das ist von außen oft schon gar nicht sichtbar.¹³¹ Zumindest bei etablierten Zugangswegen muss also ein gewisser Gutglaubensschutz an die Rechtmäßigkeit des Zugangs greifen. Allerdings kann die Analyse auch von vornherein auf „inkriminierte Musik“ angelegt sein. Oft handelt es sich dabei um Material an der Grenze zur unfreien Bearbeitung. Kann hier der Zugang noch rechtmäßig sein?

Zunächst ist den Rechtsinhaber*innen der Ausgangswerke zuzugestehen, dass ihr Kontrollinteresse beeinträchtigt ist: Sie sollen den Zugang grundsätzlich von einer Vergütung abhängig machen können, die originäre Verwertung von Werken soll geschützt bleiben.¹³² Auf der anderen Seite fußt eine Erforschung auch dieses Contents für die Wissenschaft

¹³⁰ Art. 3 III DSM-RL.

¹³¹ *Stieper*, in *Schricker/Loewenheim*, UrhG 6. Aufl. 2020, § 60d Rn. 10 mwN. Fn. 44.

¹³² *Raue* ZUM 2019, 684, 686.

auf einem legitimen Interesse. Daher sollte der „rechtmäßige Zugang“ grundrechtskonform ausgelegt werden (Art. 5 Abs. 3 GG, Art. 13 Grundrechte-Charta) und das Mining auch bei illegalem Material möglich sein.¹³³ Sonst müsste MDM überall dort unterbleiben, wo es keinen originär – zumal unzweifelhaft – rechtmäßigen Zugang zu diesen Inhalten gibt.

Entsprechend zu lösen sind rechtswidrig aufgezeichnete Konzerte (Bootlegs) als Quellen, für die es gar keine rechtmäßigen Zugänge gibt. Sofern ihre Nutzung nicht durch rechtmäßige Quellen ersetzt werden kann, streitet auch hier die Wissenschaftsfreiheit für ein weites Verständnis des „rechtmäßigen Zugangs“. Eine konkrete Forschungsfrage kann beispielsweise sein, die fein ziselierten Unterschiede in der Improvisation in möglichst vielen unterschiedlichen Interpretationen desselben Stücks zu untersuchen, für die oftmals keine offiziellen Aufnahmen zur Verfügung stehen. Dasselbe sollte für die Sammlung bereits digitalisierter analoger Quellen gelten, deren Ursprung sich nicht mehr klären lässt.

3.3.2 Aufbereitung

Musik wird vor der Analyse häufig kategorisiert, umgewandelt, zugeschnitten, normalisiert und angereichert. Dabei werden veränderte Versionen des Ausgangsmaterials **gespeichert**: Sei es, dass Audioaufnahmen in Wellenformen überführt oder in Noten transkribiert werden, oder dass eine Software Texte aus Aufnahmen erkennt. Auch dies sind Vervielfältigungen:¹³⁴ solange nämlich die körperlichen Festlegungen des Musikwerks geeignet sind, das Werk den menschlichen Sinnen auf irgendeine Weise unmittelbar oder mittelbar wahrnehmbar zu machen¹³⁵. Mittelbar wahrnehmbar ist eine Wellenform-Grafik zum Beispiel dann, wenn eine Software sie wieder als Audiodatei abspielen kann.

133 Die grundrechtskonforme Auslegung zu Gunsten des Minings von nicht rechtfreien Leaks fordert *Raue* ZUM 2019, 684, 690.

134 Nach der Klarstellung in § 23 S.3 UrhG sind solche „ausschließlich technisch bedingten Änderungen“ keine Bearbeitung.

135 Vgl. die Begründung des Regierungsentwurfs zum Urheberrechtsgesetz aus dem Jahr 1962, BT-Drs. IV/270, S.47; unkörperlich ist zum Beispiel das Abspielen vom Notenblatt. Das Vervielfältigungsrecht hat vor allem Kontrollfunktion für Rechteinhaber und ist deshalb so streng: Mit steigender Zahl von Kopien vergrößert sich der Kreis von Personen, die Werke wahrnehmen können, Dreier/Schulze/*Schulze* § 16 Rn. 1.

3.3.2.1 Formatumwandlungen

Sollen Features aus Kompositionen extrahiert werden (z.B. Intervalle und Patterns in Melodien) und liegen Audioaufnahmen vor, so darf dieses Material transkribiert werden – manuell oder automatisch. Ein hierbei oft verwendetes Format ist MusicXML. Es enthält Steuerinformationen, das derzeit von über 200 Programmen verstanden wird.¹³⁶ Im MusicXML-Format vorliegende Musik kann in Standardnotation angezeigt oder etwa in Digital-Audio-Workstations im- oder exportiert werden. Erlaubt ist jede Aufbereitung, die zum Zweck der späteren Analyse erfolgt.

3.3.2.2 Von der geschützten Musik zum freien Schnipsel oder Feature

Wenn eine Aufbereitung geschützte Musik in ihre ungeschützten Bestandteile übergehen lässt, ist jeder weitere Umgang mit der extrahierten Information frei erlaubt. Bei einer Formatumwandlung eines geschützten Werks ist das zunächst einmal sehr unwahrscheinlich. Denkbar wiederum ist es beim Kürzen, indem Ausschnitte aus Kompositionen gewählt werden. Ein Musikwerk muss Schöpfungshöhe erreichen, die nach der individuellen ästhetischen Ausdruckskraft bemessen wird.¹³⁷ Die Nutzung von Fragmenten ist nur dann urheberrechtlich relevant, wenn die Fragmente überhaupt noch die geistige Schöpfung der Urheberin zum Ausdruck bringen.¹³⁸ Wann ist also ein Fragment so individuell, dass es Werkschutz genießt? Hier kann es keine pauschale Aussage zu einer allgemeinen Mindestlänge geben. Da jedenfalls in der Hit Song Science gerade das ästhetisch besonders Prägende der Musik untersucht wird (etwa Hooklines in einem Refrain), wird man schon aus Pragmatismus von der Schutzfähigkeit dieser prägenden Segmente ausgehen müssen. Differenzieren kann man bei Melodiepattern, also Sequenzen, die etwa in einem Stück mehr als einmal auftauchen. Melodiepattern können durchaus auch „nicht prägend“ und damit gemeinfrei sein. Sie sind musikalische Standardsprache.

¹³⁶ Siehe <https://www.musicxml.com/de/software/> (zugegriffen: 15. Januar 2020).

¹³⁷ BGH MMR 2015, S. 824, 826 – *Goldrapper*.

¹³⁸ Vgl. EuGH GRUR 2009, 1041 – *Infopaq*, Rz. 38 f.

Differenzieren muss man weiter, wenn Musik gänzlich ohne Melodie und ohne schutzfähigen Rhythmus (bei elektronischer Musik oft relevant) transkribiert wird. Lässt sich durch eine Transkription das Werk nicht mehr rekonstruieren, so spricht auch dies dafür, dass die Aufbereitung in ungeschützte Bestandteile gemündet ist. In den Digital Humanities wird bereits diskutiert, wie geschützte Inhalte aufbereitet werden können, um sie in gemeinfreie – und damit frei nachnutzbare – Forschungsdaten zu transformieren.¹³⁹

3.3.2.3 Entstehen eigener Rechte

Bei der Digitalisierung und Aufbereitung von bestehendem Material sollte auch das Entstehen eigener Rechte berücksichtigt werden: Wird beispielsweise in einem Forschungsprojekt gemeinfreies Liedmaterial aufwendig aufbereitet und in Forschungsdatenkorpora gesammelt und möchte man die Korpora später frei zugänglich machen, so müssen auch entstandene Rechte geklärt werden. Zu denken ist hier vor allem an Datenbankschutz: Eine Datenbank ist eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet werden und deren Beschaffung, Überprüfung oder Darstellung eine wesentliche Investition erfordert (§ 87a UrhG). Bei Korpora-Datenbanken ist dies durchaus denkbar. Entscheidend ist, dass die Daten auf eine systematische oder methodische Art und Weise so aufbereitet sind, dass sie sinnvoll abgefragt werden können.¹⁴⁰ Wenn Noten zum Beispiel aus Audiodateien mit Jazzsoli transkribiert werden, müssen die Transkriptionen oft nachgebessert werden. Denn die Ergebnisse sind oft nicht exakt, fehlerhaft oder bilden das exakte Timing („Mikrotiming“) nicht ab. Bei der Aufbereitung dieser Datenbanken kann also ein Datenbankschutz entstehen. Denkbar ist aber auch das Anreichern durch Metainformation, die im Musikwerk selbst nicht enthalten ist, etwa mit Strukturdaten, Volltexterfassungen und Verlinkungen.

Sollen solche Datenbanken frei zugänglich gemacht werden oder wesentliche Teile daraus entnommen werden, muss derjenige zustimmen,

¹³⁹ Erler, DFG-Expertenworkshop: Strategien für die Nutzarmachung urheberrechtlich geschützter Textbestände für die Forschung durch Dritte, in RuZ 2020, 108; OA-publiziert unter der DOI 10.5771/2699-1284-2020-1-108.

¹⁴⁰ Dreier in Dreier/Schulze UrhR, 6. Aufl. 2018, § 87a Rn. 7.

der die Investition in die Aufbereitung geleistet hat („Datenbankhersteller“, § 87a Abs. 2 UrhG).

3.3.2.4 Zwischenergebnis

In der Aufbereitungs- und Anreicherungsphase dürfen für die Forschung Kopien von urheberrechtlich geschütztem Material angefertigt werden. Die Kopien verlieren ihren Schutz oft nicht, auch wenn die Bestandteile nicht mehr zum Werkgenuss taugen mögen. Geht es um das Mining im Individuell-Prägenden, verlieren Werkfragmente durch Kürzung ihren Schutz tendenziell nicht.

3.3.3 Analyse

Der technische Vorgang der eigentlichen Analyse wird von den Gesetzgebern als urheberrechtlich nicht relevant angesehen¹⁴¹. Sollte es dennoch zu Vervielfältigungen kommen, seien dies oft flüchtige Kopien, die lediglich im Arbeitsspeicher erstellt werden. Diese können schon nach bisherigem Recht über § 44a UrhG¹⁴² erlaubt sein.

3.3.4 Veröffentlichung und Verwertung

Eine uneingeschränkte Erlaubnis zur Veröffentlichung von TDM-Korpora enthalten die TDM-Schranken nicht.

3.3.4.1 Teilen von TDM-Korpora

Für die Präsentation von Forschungsergebnissen bei MDM bieten sich Tonaufnahmen oder im Browser eingebettete MIDI-Player an, zum Beispiel mit variablen Wiedergabegeschwindigkeiten und zumindest kurzen Notationen oder Textzeilen. Das Online-Stellen ist eine öffentliche Zugänglichmachung, die nicht von den TDM-Schranken abgedeckt ist.

¹⁴¹ Für § 60d UrhG siehe BT-Drs. 18/12329, S. 41.

¹⁴² Basierend auf Art. 5 I InfoSoc-RL. ErwGr. 9 der DSM-RL stellt ebenfalls klar, dass diese Vorschrift bei der eigentlichen Analyse anwendbar sein kann.

Forschung kann sich nicht darauf berufen, dass sich online zugängliche Korpora mit ihren Kompositionen, Texten, Aufnahmen oder Noten gar nicht mehr für einen (vollwertigen) Werkgenuss eignen. Das ist misslich, zumal diese Aufbereitungen vielfach gar nicht mehr den Genuss der Musik ersetzen können und Rechteinhaber*innen damit auch keine Einbußen befürchten müssen. Vor diesem Hintergrund wäre es gesetzgeberisch möglich (gewesen), eine Erlaubnis zum unbeschränkten Bereitstellen von Korpora zu schaffen.

3.3.4.2 Wissenschaftliche Publikation

Bei einer inhaltlichen Auseinandersetzung kann aber die Zitierfreiheit greifen. Im Rahmen des Zitatrechts (§ 51 UrhG) dürfen auch geschützte Bestandteile wiedergegeben werden, etwa durch Abdruck von Noten, Wellenformen, Textteilen in einer Forschungspublikation, die die Analyseergebnisse und deren Interpretation vorstellt. Damit das Zitatrecht greift, muss das zitierende Werk dem Beleg einer Aussage dienen und der Umfang geboten sein. Es muss jedenfalls eine innere Verbindung¹⁴³ zum zitierten Werk hergestellt werden. Die Gedankenführung sollte also auch Bezug auf das konkret zitierte Werk nehmen. Dann darf umfangmäßig so viel angezeigt werden, wie fürs Erläutern des Gedankens nötig ist. Ein Online-Stellen ganzer Werke ohne technische Zugangsbeschränkungen kann im Internet unzulässig sein¹⁴⁴, sodass möglicherweise technischer Schutz ergriffen werden muss – sofern möglich. Zudem muss die Pflicht zur Quellenangabe berücksichtigt werden (§ 63 UrhG).

Aus unserer Sicht ist es zulässig, trotz Änderungsverbot (§ 62 UrhG) kleinere Abweichungen am Werk vorzunehmen, sei es durch die eigene Notation, die bei einem Solo oder einer Improvisation Details weglässt, oder durch die Hervorhebung bestimmter Audiomerkmale, etwa durch einen Equalizer etc.¹⁴⁵

143 *Schulz* in BeckOK Urheberrecht, 26. Edition 2019, § 51 Rn. 13 mwN.

144 LG München I GRUR-RR 2006, 7 – *Karl Valentin*.

145 Vgl. *Schulz* in BeckOK Urheberrecht, 26. Edition § 51 Rn. 4 mwN., wonach bei Zitaten aus Sprachwerken z. B. die Umstellung des Satzbaus zulässig ist.

3.3.4.3 Einbetten von Fremdinhalten

Abseits des Zitatrechts gibt es noch eine durchaus bedenkenswerte Gestaltungsmöglichkeit. So ist es möglich, legal bereits veröffentlichten Content auf der Online-Präsentation einzubinden. Denn dabei wird, sofern der fremde Content technisch nur eingebunden und nicht erneut hochgeladen wird, keine neue öffentliche Wiedergabe vorgenommen.¹⁴⁶ Damit liegt schon keine Nutzungshandlung vor und es muss nicht geprüft werden, ob eine Schranke die Nutzung erlaubt. Bei offensichtlich rechtswidrig hochgeladener Musik sollte aber auch von dieser Möglichkeit kein Gebrauch gemacht werden. Für den Bereich der Forschung sind die Kriterien noch nicht festgezurr. Das Einbinden von YouTube-Videos, SoundCloud-Streams etc. ist also eine durchaus denkbare Option. Dabei dürfen aber keinesfalls Paywalls umgangen werden; Player sollten nicht über ihre Funktion hinaus manipuliert werden.

3.3.4.4 Neue Musik

Das Nutzen der gewonnen Erkenntnisse als Grundlage neuer Musik ist grundsätzlich ein freier Vorgang: Die aus der Forschung gewonnenen Konzepte und Ideen dürfen in neue Werke einfließen. Diskutiert wird dies u. a. beim Trainieren Künstlicher Intelligenz, die dann Werke schafft.¹⁴⁷ Problematisch wird es erst, wenn geschützte Bestandteile fremder Werke in neue Werke Einzug finden. Hier gilt im Hinblick auf Kompositionen und Texte: Längere Melodie- oder Textpassagen sollten jedenfalls nicht übernommen werden. Solange geschützte Bestandteile fremder Werke nicht verblassen, sondern das Ausgangswerk in wesentlichen Zügen erhalten bleibt, liegt darin eine unfreie Bearbeitung (§ 23 UrhG).

¹⁴⁶ Ausführlich hierzu *Raue* ZGE 2017, 514. EuGH-Rechtsprechung zur öffentlichen Wiedergabe: EuGH, Urt. v. 13.02.2014, Az. C-466/12 – *Svensson*; EuGH, Urt. v. 21.10.2014, Az. C-348/13 – *BestWater International*; EuGH, Urt. v. 08.09.2016, Az. C-160/15 – *GS Media*; EuGH, Urt. v. 26.04.2017, Az. C-527/15 – *Filmpeleer*; EuGH, Urt. v. 07.08.2018, Az. C-161/17 – *Renckhoff*.

¹⁴⁷ Hierzu *Rosati*, Copyright as an Obstacle or an Enabler? A European Perspective on Text and Data Mining and Its Role in the Development of AI Creativity, *Asia Pacific Law Review*, 2019. Abrufbar unter <https://ssrn.com/abstract=3452376>, zuletzt abgerufen am 3. Februar 2020.

Die Abgrenzung von gemeinfreien Features und geschützten Werkbestandteilen ist schwierig. Tendenziell ist die Übernahme nicht kompositorischer, eher stilistischer Mittel frei. Die per MDM geschürften Features enthalten einerseits oft formale Gestaltungselemente, die auf Lehren von Harmonik, Rhythmik und Melodie beruhen und sind freies Musikvokabular.¹⁴⁸ Dazu zählen einfache Akkordfolgen wie ein Bluesschema oder die klassische Kadenz. Werden die gemeinfreien Standardharmonien aus einer Komposition extrahiert (zum Beispiel die Akkordabfolge A/D/A/E, eine Quintfallsequenz etc.), kann in diesem Extrakt auch kein schutzfähiger Teil liegen. Das Urheberrecht weist den Urheber*innen weder ihre wirtschaftliche Verwertung zu noch ihre exklusive Kontrolle darüber.

Wo liegt aber die Grenze zur geschützten Form? Zu kurz greift es jedenfalls, nur Melodien¹⁴⁹ als schutzfähigen Teil einer Komposition zu sehen. Auch Arrangement, Zusammenspiel von Instrumentierung, Melodik, Rhythmik, Tempo, Harmonik und Klangeffekten können Schutz begründen,¹⁵⁰ es kommt auf den ästhetischen Gesamteindruck an.¹⁵¹ Diese Abgrenzung von freier Idee und freiem Stilmittel zu geschützter Form ist vor allem angesichts der jüngeren Plagiatsprozesse in den USA in die Diskussion geraten.

Heikel ist auch das Einbinden fremder Soundschnipsel. Hier gilt: Sind die Audiofragmente erkennbar und unverändert, etwa weil prägende Teile geloopt sind, ohne dass künstlerisch damit interagiert wird, ist dies tendenziell eine Rechtsverletzung. Sind die Schnipsel verändert/manipuliert, verblasst also die Wiedererkennbarkeit, kann dies zulässig sein (quasi verwandt mit der freien Benutzung). Eine zulässige künstlerische Auseinandersetzung ist denkbar. Klar unzulässig ist es aber, extrahierte und sortierte Fragmente zu verwenden, etwa um Kosten und Mühen für

148 Zur Freiheit dieser Merkmale u. a. BGH GRUR 1991, S. 533 – *Brown Girl II*.

149 Eine Melodie kann verstanden werden als eine relative Tonfolge (oder eine Folge von Intervallen), die in sich abgeschlossen rhythmisiert und wiedererkennbar ist und die dem Werk eine charakteristische Prägung verleiht. So *Canaris* in einer ausführlichen Untersuchung 2012, S. 71 m. w. N.

150 Vgl. etwa LG München I ZUM-RD 2009, S. 101 ff. – *Still Got The Blues*.

151 Ausführlich hierzu etwa *Döhl*, Substantially Similar? – Das Plagiat aus Sicht des Verhältnisses von Musik und Recht. In *Plagiate. Fälschungen, Imitate und andere Strategien aus zweiter Hand* (= Beiträge zur Rechts-, Gesellschafts- und Kulturkritik Bd. 10), Bung, Jochen/Gruber, Malte-Christian/Kühn, Sebastian (Hrsg.), Berlin: trafo, S. 201–215; <http://www.pop-zeitschrift.de/2013/05/27/substantially-similardas-plagiat-aus-sicht-des-verhaeltnisses-von-musik-und-rechtvon-frederic-dohl27-5-2013/>, zuletzt abgerufen am 15. Januar 2020.

Sampling-Datenbanken und Rechteklärung zu sparen.¹⁵² Vom Schaffen von Sounddatenbanken, die durch das Mining sortiert werden, ist also derzeit abzuraten.

3.3.5 Verfügbarmachen und -halten für die Forschung

Wiederum Teil der TDM-Schranken ist das Verfügbarmachen der entstandenen Korpora. Es kann ein wissenschaftliches Interesse bestehen, etwa für Reviewzwecke oder zur Reproduktion von Forschungsergebnissen bzw. deren Nachvollziehbarkeit. Hier sind zwei Verwertungsarten betroffen: die Vervielfältigung durch die Speicherung und die öffentliche Zugänglichmachung.

3.3.5.1 Verfügbarmachen unter Forschenden

Womöglich auch schon früher bzw. als Teil iterativer Prozesse wird das Bedürfnis bestehen, in größeren Teams aus Forschenden gegenseitig Korpora oder Ursprungsmaterial zu teilen. Im geschlossenen, abgrenzbaren Forschendenkreis ist der Tausch von Forschungsdaten oft nicht als urheberrechtlich relevante Handlung einzustufen. Dort wird nämlich in der Regel keine Öffentlichkeit im Sinne des § 15 Abs. 3 UrhG vorliegen. Tut sie dies doch, trifft für die Zusammenarbeit unter Forschenden § 60d Abs. 1 S. 1 Nr. 2 UrhG eine Erlaubnis. Institutionsweites Zugänglichmachen ist jedenfalls nicht erlaubt.

3.3.5.2 Archivieren, Publizieren

Nach dem aktuellen § 60d UrhG müssen Korpora und Ursprungsmaterial nach Abschluss der Forschungstätigkeit gemäß § 60d Abs. 2 UrhG gelöscht werden,¹⁵³ dürfen allerdings in Archiven eingelagert werden. Die privilegierten Institutionen haben künftig die Möglichkeit, die Korpora

¹⁵² Wenn es nicht eigenständiges Schaffen ist, sondern nur Aufwand und Kosten gespart werden sollen, so zum Sampling-Urteil des EuGH *Schulze* in seiner Anmerkung zu EuGH NJW 2019, 2913.

¹⁵³ Kritisch zur Rechtsnatur der Löschpflicht und zur Unklarheit des „Abschlusses“ von Forschungsdaten *Hoeren*, IWRZ 2018, 120, 124.

zum Beispiel in einem Forschungsdaten-Repository zu speichern. Für die Publikation von Korpora werden fremde Rechte in den Korpora in aller Regel entgegenstehen. Auch Open-Access-Policies oder Förderbedingungen können die Publikation der Korpora nicht legalisieren. Sofern die Ausgangsmusik gemeinfrei war, ist die Publikation erlaubt. Beim kommerziellen Mining sind die Aufbewahrungsvorschriften strenger, weil hier wiederum Kopien nur so lange aufbewahrt werden dürfen, wie dies für TDM-Zwecke erforderlich ist (Art. 4 Abs. 2 DSM-RL). Damit wollen Rechtsinhaber sogenannte Schattendatenbanken verhindern.

3.4 Fazit

Das Petitum The Right to Read is Right to Mine konnte sich zwar nicht für den gesamten Forschungszyklus durchsetzen. Für die Musikwissenschaft sind die Phasen der Aufbereitung, Analyse und Aufbewahrung aber weitgehend abgesichert. Dass Auslegungsspielräume wie der rechtmäßige Zugang bei fehlender rechtmäßiger Alternative zu Gunsten der Forschung ausgefüllt werden, ist zu hoffen. Sehr zu bedauern wäre jedenfalls, wenn von den neuen Freiheiten aus Sorge vor Rechtsverfolgung nur zurückhaltend Gebrauch gemacht würde.

Verbleibende Unsicherheit, etwa über die Zugänglichmachung von Korpora, muss vertraglich geregelt werden. Da dies oft nicht möglich ist, sollte der Gesetzgeber weiter austarieren, wann – außerhalb des Zitatrechts – das Allgemeininteresse an der Präsentation der Forschungsergebnisse höher wiegt und der Eingriff in das Urheberrecht gering ist.

Für die kommerziellen Anwendungsbereiche bzw. Musikschaffende wird in aller Regel der durchsetzungsschwächere Art. 4 DSM-RL einschlägig sein. Im kommerziellen Kontext hat der Gesetzgeber jedenfalls bewusst die Entscheidung getroffen, die Privilegierung des Minings nicht so weit zu ziehen. Folglich sind nicht alle gesellschaftlichen Akteure für Mining gleich privilegiert.¹⁵⁴ Langfristig sollte eine generelle

154 Kritisch die Allianz der Wissenschaftsorganisationen in ihrer Stellungnahme zur Umsetzung der DSM-RL, S. 2, https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2019/Downloads/090519_Stellungnahme_Allianz_EU-Richtlinien_Urheberrecht.pdf?jsessionid=4F141F6FC848ABDE4C817B35A144572E.1_cid297?__blob=publicationFile&v=2, zuletzt abgerufen am 2. Februar 2020.

Data-Mining-Ausnahme geschaffen werden, mit der Möglichkeit zum Teilen von TDM-Korpora.

Schließlich: Da eine starke Tendenz hin zu Subskriptionsdiensten wie Spotify geht und Big-Data-Forschung von den technischen Gegebenheiten abhängig ist, sollte künftig darauf Acht gegeben werden, dass den eigentlich nach Schrankenregelung privilegierten Nutzenden nicht stets die Last aufgebürdet wird, ihre gesetzlichen Erlaubnisse durchzusetzen.¹⁵⁵

¹⁵⁵ Kritisch zur „Aktionslast“ von Nutzenden, die sich auf eine Schrankenbestimmung berufen können, aber durch Technik gehindert sind *Specht* in GRUR 2019, 253, 259.

4 DATA LEAKS

Susan Gonscherowski/Dr. Matthias Wübbeling¹⁵⁶

*Um Identitätsdiebstahl im Internet zu verhindern, können öffentlich verfügbare Identitätsdaten datenschutzfreundlich genutzt werden. Das sind häufig genau die Daten, die auch von Kriminellen für betrügerische Zwecke missbraucht werden. Das vom Bundesministerium für Bildung und Forschung geförderte Projekt Effektive Information nach Digitalem Identitätsdiebstahl (EIDI) betrachtet neben psychologischen Auswirkungen von Identitätsdiebstahl insbesondere die technische und datenschutzrechtliche Komponente einer Umsetzung zum Schutz betroffener Bürger*innen. Dafür werden die gesammelten Identitätsdaten ganz besonders geschützt und die Umsetzung datenschutzrechtlich bewertet, um nicht selbst zu einem attraktiven Ziel für Kriminelle zu werden.*

4.1 Einleitung

Das Internet bietet für Cyberkriminelle eine Vielzahl an Möglichkeiten, sich zu bereichern. Identitätsdaten, Konto- oder Kreditkarteninformationen sowie E-Mail-Adressen und Passwörter werden von kriminellen Banden in großen Mengen gesammelt. Auch das Jahr 2019 begann mit einem besonderen Datenskandal. Der unter dem Titel „Politiker-Doxxing“¹⁵⁷ bekannt gewordene Hackerangriff ist jedoch kein Einzelfall. Im Internet finden sich viele Milliarden Datensätze, die teilweise hochvertrauliche Informationen, wie beispielsweise Passwörter, enthalten. Die Betroffenen bemerken davon meist nichts. Erst, wenn die öffentlich verfügbaren personenbezogenen Daten für Kreditkarten- oder Warenbetrug genutzt werden und plötzlich unerwartet Rechnungen eintreffen, wird klar, dass Kriminelle an ihre Daten gelangt sind. Dabei stehen sowohl die einzelnen Endgeräte der Opfer selbst als auch Webseiten und Benutzerdatenbanken der Dienstleister im Fokus gezielter Angriffe. Phishing-E-Mails, Botnetze und Trojanische Pferde sind typische Werkzeuge, die von Cyberkriminellen verwendet werden. Sie hel-

156 Mehr über die Autor*innen erfahren Sie im Autor*innenhinweis auf S. 108 und S. 110.

157 FAZ.net, Was ist Doxing?, <https://www.faz.net/aktuell/wirtschaft/diginomics/hacker-angriff-auf-politiker-was-ist-doxxing-15972248.html> (Stand 04. Januar 2019).

fen ihnen Endgeräte unter ihre Kontrolle zu bringen und erlauben so den Zugriff auf lokale persönliche Daten und Korrespondenzen der Opfer sowie auf deren Zugangsdaten zu unterschiedlichen Online-Diensten. Diese Werkzeuge sind dabei gezielt darauf ausgelegt, möglichst lange unentdeckt zu bleiben. Ein erfolgreicher Angriff liefert einem Kriminellen zumeist tausende oder hunderttausende Datensätze. Cyberkriminelle geben auch dann die Kontrolle über ein Gerät nicht auf, wenn alle Daten eines Opfers bereits kopiert wurden. Gekaperte Maschinen verrichten dann als „Zombies“ ihren Dienst und unterstützen die Täter*innen bei der Infektion weiterer Endgeräte, beim Versand von Phishing-E-Mails oder bei gezielten Angriffen auf Teile der Internet-Infrastruktur (DDoS).

Nur selten lässt sich durch die Opfer nachträglich feststellen, welche Daten tatsächlich von einem Vertraulichkeitsverlust¹⁵⁸ betroffen sind. In den meisten Fällen sind sich die Personen, deren Daten von einem derartigen Vertraulichkeitsverlust betroffen sind, nicht bewusst, dass sie Opfer einer Straftat geworden sind. Je nach krimineller Aktivität erfahren sie möglicherweise erst sehr viel später davon, dass sich die Täter*innen durch die Verwendung ihrer persönlichen Daten bereichert haben.

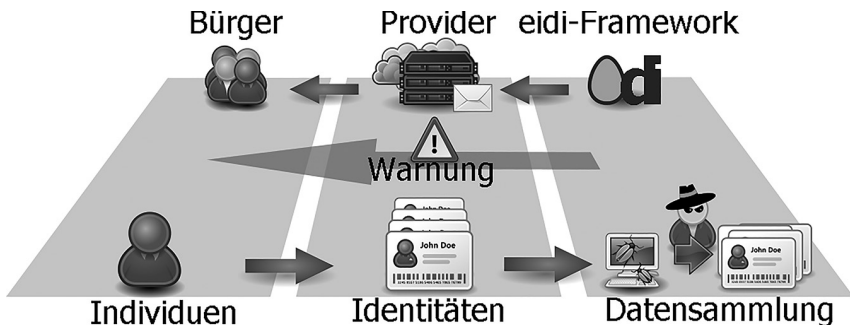
Das hier vorgestellte Verfahren beschreibt einen Ansatz der zukünftig mehr Transparenz für die Betroffenen herstellen und diese somit in die Lage versetzen soll, Risiken und Folgeschäden zu antizipieren sowie präventiv Maßnahmen zu ergreifen. Der Beitrag ist wie folgt strukturiert: Zunächst wird der technische Ansatz zur Verarbeitung öffentlich verfügbarer Identitätsdaten vorgestellt und das Konzept zur Information von Betroffenen diskutiert. Anschließend werden rechtliche, insbesondere datenschutzrechtliche Aspekte im Detail erläutert und ein möglicher Einsatz des Frameworks im Lichte der Datenschutz-Grundverordnung betrachtet.

158 *Wolf/Pfitzmann*, Charakteristika von Schutzzielen und Konsequenzen für Benutzungsschnittstellen, Informatik Spektrum, Juni 2000.

4.2 Effektive Information nach digitalem Identitätsdatendiebstahl¹⁵⁹

Strafverfolgungsbehörden und IT-Sicherheitsforscher gelangen bei der Aufklärung von IT-Sicherheitsvorfällen und der Analyse von Schadsoftware oder Botnetz-Kommunikation regelmäßig in den Besitz umfangreicher Sammlungen von Identitätsdaten, die Kriminelle über diese Wege sammeln und austauschen. Es gibt bisher keine erprobte oder standardisierte Methode, Opfer zuverlässig und präventiv über ihre Betroffenheit zu informieren. Um betroffene Individuen präventiv über einen Missbrauch ihrer Identität oder den Verlust der Vertraulichkeit ihrer persönlichen Daten zu informieren und so vor möglichen weiteren Aktionen von Kriminellen zu schützen, müssen verfügbare Identitätsdaten-Sammlungen kontinuierlich analysiert, betroffene Personen identifiziert und angemessen informiert und gewarnt werden. Eine effektive Dissemination der Untersuchungsergebnisse trägt nicht nur zur umfassenden Aufklärung von IT-Sicherheitsvorfällen bei, sondern stärkt auch berechtigte Interessen betroffener Personen.

Um dieses Ziel zu erreichen wurden die Grundlagen für eine Umsetzung in Deutschland erarbeitet. Dabei wurden eng miteinander verbundene Ziele verfolgt, die von dem Erhalt von Datensätzen über die Bewertung der Qualität der Daten und die Identifikation der Opfer bis hin zur rechtssicheren und gezielten Information der Betroffenen reichen.



159 Förderhinweis: Das diesem Beitrag zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16KIS0697 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren. Weitere Informationen zum Projekt EIDI über: <https://itsec.cs.uni-bonn.de/eidi/>.

4.3 Daten und Informationsfluss

Um eine Vorstellung vom Fluss der Daten und Informationen zu erhalten, werden in diesem Abschnitt die unterschiedlichen Schritte sowie die relevanten Begriffe erläutert. Abbildung 1 zeigt dabei einen entsprechenden Überblick.

4.3.1 Erstellung von Identitätsdaten

Ausgehend von Bürger*innen, die als Identitätsinhaber*innen mehrere Identitäten im Internet, beispielsweise bei verschiedenen Inhalte- und Diensteanbietern, besitzen, gelangen die eigenen persönlichen Daten in Umlauf. Die Inhalte- und Diensteanbieter sind also als Verantwortliche diejenige Stelle, bei der die Identitätsdaten von Kunden*innen legitim in der Datenbank liegen. Kriminelle erbeuten solche Kundendatenbanken und verfolgen damit unterschiedliche Ziele: die Nutzung der Identitätsdaten für eigene betrügerische Zwecke oder die Anreicherung der Daten zum Weiterverkauf an entsprechende Betrüger. Solche kriminellen Datensammlungen kursieren dann etwa in Botnetzen, vor allem zum Versand von SPAM-E-Mails an die enthaltenen E-Mail-Adressen, oder in spezialisierten Foren von Kriminellen.

4.3.2 Datensenkern

Viele Kriminelle teilen etwa interessierten Käufer*innen bereits im Vorfeld Teile ihrer Datensammlungen zur Qualitätskontrolle mit. Dafür verwenden sie häufig öffentliche Dienste zum Datenaustausch, sogenannte Paste-Sites. Diese Dienste können auch von unbeteiligten genutzt und die Identitätsdaten eingesehen werden. Gehandelt und getauscht werden Identitätsdaten darüber hinaus in speziellen Foren im sogenannten Darknet. Das nur mit bestimmten Zugangsprogrammen erreichbare Netzwerk erlaubt die anonyme Benutzung des Darknets ebenso wie des normalen Internets. Als öffentlich verfügbare Identitätsdaten gelten in unserer Betrachtung solche Daten, die entweder auf Paste-Sites oder in Darknet-Foren ohne weitere Hürden zugänglich sind. Gemeinsam mit den im Forschungsumfeld anfallenden Daten bilden diese Datensenkern die Basis unserer Datensammlung.

4.3.3 EIDI-Framework

Die Identitätsdaten liegen in unterschiedlichen Dateiformaten und Formatierungen vor. In einem ersten Schritt müssen diese unterschiedlichen Repräsentationen erkannt und die enthaltenen Identitätsdaten herausgefiltert werden. Dabei ist vordergründig wichtig, nur solche Inhalte weiter zu verarbeiten, die bei der Identifikation des Bürgers und zur Einschätzung der Kritikalität und Aktualität der Datensammlung hilfreich sind. Informationen gemäß Art. 9 DSGVO werden nicht weiter verarbeitet. Die eingelesenen Informationen werden dabei gehasht und verschlüsselt in der Datenbank abgelegt. Wichtig ist dabei, nicht selbst zum Ziel potentieller Angreifer zu werden und die Hürden für einen Angriff höher zu legen als den Aufwand, die (im Grunde bereits öffentlichen) Daten selbst zu sammeln.

4.3.4 Provider

Unter dem Begriff Provider werden Dienstanbieter im Internet subsumiert, bei denen sich Bürger*innen Online-Konten erstellen und an die sie Identitätsdaten übermitteln. Provider eignen sich dazu, ihre Kund*innen zweifelsfrei zu identifizieren und bei Bedarf entsprechend mit diesen in Kontakt zu treten und diese über ihre Betroffenheit zu informieren. Es gilt also, die im EIDI-Framework aus den Datensammlungen extrahierten Daten an die unterschiedlichen teilnehmenden Provider zu übermitteln. Dabei wird durch Hashes sichergestellt, dass ein Provider nur solche Daten zur Identifikation weiterverarbeiten kann, die einem Kunden eindeutig zugeordnet werden können. Identitätsdaten von Bürger*innen, die nicht Kunde eines Providers sind, sind für den Provider nicht zu entschlüsseln.

4.4 Technisches Konzept und Umsetzung

Um die datenschutzrechtliche Bewertung des resultierenden Prozesses durchführen zu können, müssen weitere Details über technische Konzepte und die konkrete Umsetzung bekannt sein. In den folgenden Absätzen werden diese in dem notwendigen Umfang dargestellt.

4.4.1 Einlesen der Datensammlungen

Die wichtigsten Faktoren beim Einlesen von Identitätsdaten, die in einem unbekannten Format vorliegen, ist die Erkennung der verwendeten Trennzeichen zwischen einzelnen Identitäten und innerhalb einer Identität zwischen den einzelnen Informationen. Ausgehend von textbasierten Formaten, wird zunächst davon ausgegangen, dass eine Identität in genau einer Zeile der Textdatei steht. Somit müssen nur noch die in den einzelnen Zeilen verwendeten Trennzeichen ermittelt werden. Die verwendeten Trennzeichen unterscheiden sich häufig auch innerhalb derselben Datensammlung und sogar in denselben Dateien. Mittels statistischer und dynamischer Analyse werden die Trennzeichen erkannt und die jeweiligen Spalten extrahiert.

Die meisten Leaks enthalten keine semantischen Informationen. Es ist also nicht automatisch klar, welche Inhalte tatsächlich in einer Spalte stehen. Da eine einzelne Betrachtung hier nicht zielführend ist, viele Vornamen werden beispielsweise auch als Passwort genutzt, erfolgt eine semantische Gruppierung in Blöcken von Identitäten. Je nach Konfiguration werden etwa 10.000 Zeilen eingelesen und anschließend die in einer Spalte maßgeblich enthaltenen Informationen bestimmt. So funktioniert eine Einordnung in unterschiedliche Typen von Identitätsdaten. Insgesamt werden die folgenden Typen erkannt und weiterverarbeitet: E-Mail-Adresse, Passwort, Hash (z. B. Passwort-Hashes), Benutzername, Vorname, Nachname, Postleitzahl, Adresse, IBAN, Kreditkartennummern, Telefonnummern. Das sind auch die bei einem Provider üblicherweise hinterlegten Informationen, so dass damit eine Identifikation möglich sein sollte.

4.4.2 Bewertung

Um die Kritikalität der eingelesenen Datensammlungen zu bemessen, müssen unterschiedliche Faktoren berücksichtigt werden. Niemand soll unnötig informiert werden, etwa wenn die gefundene Datensammlung bereits (in Teilen) bekannt ist oder die Kundendaten mehrere Jahre alt und nicht mehr aktuell sind. Für die Bewertung der Kritikalität spielen also, soweit bekannt, das Alter der Datensammlung, die Herkunft, das Missbrauchspotential der beinhalteten Datentypen und die Aktualität

enthaltener Passwörter eine große Rolle. Nur, wenn ein Identitätsbetrug als tatsächliche Bedrohung durch die bearbeiteten Informationen möglich ist, ist eine Warnung der Betroffenen unerlässlich.

4.4.3 Hashes und Verschlüsselung

Um nicht versehentlich die Identitätsdaten von Nicht-Kund*innen an einen Provider zu senden, werden die Daten gehasht bzw. verschlüsselt übertragen. Anhand der Typen E-Mail-Adresse und Passwort soll dies im Folgenden kurz erläutert werden. Die E-Mail-Adresse gilt in diesem Fall als identifizierender Datentyp (jedem Konto wird eindeutig eine E-Mail-Adresse zugeordnet), das Passwort als zusätzliche Information (mehrere Kund*innen können dasselbe Passwort wählen). Um nun die Verarbeitung durch fremde Provider zu verhindern, wird das Passwort mit der E-Mail-Adresse als Verschlüsselungskennwort verschlüsselt. Das bedeutet, dass eine Entschlüsselung des Passworts nur möglich ist, wenn dem Provider die E-Mail-Adresse bekannt ist.

Es ist klar, dass die E-Mail-Adresse selbst nun nicht unverschlüsselt übertragen werden darf, sonst könnten auch Dritte einfach das Passwort entschlüsseln. Daher soll die E-Mail-Adresse gehasht werden. Hashing ist eine Einwegfunktion, die beliebige Eingabewerte mit möglichst wenigen Kollisionen auf ein definiertes Alphabet abbildet. Ein Provider muss so nur noch für die vorhandenen Kund*innen einen Hashwerts berechnen und mit diesem anschließend abgleichen. Handelt es sich um einen Kund*innendatensatz, lässt sich der Hash von der Klartext-E-Mail-Adresse berechnen und die dem Provider vorliegende E-Mail-Adresse des Kunden zum Entschlüsseln des Passworts verwenden.

4.4.4 Information

Die tatsächliche Information an die Betroffenen durch die Provider soll nicht vorgegeben werden. Insbesondere können die Provider zusätzliche Dienste, etwa eine Kund*innenhotline oder E-Mail-Support, anbieten. Auch der Kommunikationsweg, den ein Provider wählt, ist diesem überlassen. Je nachdem, wie ein Provider üblicherweise wichtige Informationen an seine Kund*innen übermittelt, etwa per Post, E-Mail oder aber

beim täglichen Login des Kunden, sollten auch die Informationen entsprechend übermittelt werden. Wichtig ist, dass diese Information vom Kunden ernstgenommen und umfassend verstanden wird.

4.5 Datenschutz

Der Umstand, dass personenbezogene Daten ohne den Willen oder das Wissen der Betroffenen veröffentlicht wurden, zieht einen Kontrollverlust nach sich, der für die Betroffenen nicht hinnehmbar ist. Das vorliegende Konzept ist daher auch vom Standpunkt des Datenschutzes sinnvoll. Ziel ist es, die Risiken und mögliche Folgeschäden zu minimieren und das Bewusstsein für die Problematik grundsätzlich zu erhöhen. Um einen rechtssicheren Einsatz der Verfahren und Prozesse zu ermöglichen, wurden diese auf ihre Vereinbarkeit mit den rechtlichen Rahmenbedingungen der Bundesrepublik Deutschland analysiert. Dabei gilt es zu klären, wer eine solche Stelle zur Opfer-Warnung betreiben kann und darf oder wessen öffentlicher Auftrag diese Zuständigkeit möglicherweise sogar impliziert. Zusätzlich werden die Rahmenbedingungen im haftungsrechtlichen Umfeld analysiert, z. B. darauf hin, ob es eine Pflicht zur Warnung gibt oder ob eine unterlassene oder fehlerhafte Information und Warnung zu weiteren Konsequenzen führen kann. Da es im Rahmen des Projektes zur Verarbeitung personenbezogener bzw. personenbeziehbarer Daten kommt, werden bereits die Entwicklung des Prozesses und die technische Umsetzung auf ihre Konformität mit den strengen Vorgaben des deutschen Datenschutzrechts überprüft.

4.5.1 Schutzlücken

Der Artikel 34 Abs. 1 DSGVO legt fest, unter welchen Umständen von einem Datenschutzvorfall betroffene Personen zu benachrichtigen sind: sofern ein hohes Risiko besteht. Damit es überhaupt zu dieser Feststellung kommen kann, müssen folgende Voraussetzungen erfüllt sein:

1. Der Verantwortliche muss den Datenschutzvorfall als solchen erkannt haben.
2. Der Verantwortliche muss eine korrekte Einschätzung des daraus resultierenden Risikos für die Betroffenen vornehmen.

3. Der Verantwortliche muss die Betroffenen identifizieren und benachrichtigen können.
4. Die Betroffenen müssen auf Basis der Benachrichtigung handeln.

Anhand dieser Zusammenfassung wird bereits deutlich, dass dem Verantwortlichen eine zentrale Rolle zukommt. Die Forderung des Gesetzgebers, dass die Stelle, die personenbezogene Daten verarbeitet, tätig werden muss, wenn sie die Vertraulichkeit, Verfügbarkeit und/oder Integrität dieser Daten nicht mehr gewährleisten kann, ist absolut angemessen und bleibt vom beschriebenen System unberührt. Die Notwendigkeit eines Benachrichtigungssystems ergibt sich vor allem daraus, dass die Datenschutz-Grundverordnung (DSGVO) Verletzungen des Schutzes personenbezogener Daten (Datenschutzvorfälle) nur in Bezug auf die Pflichten der Verantwortlichen reguliert.

Es kann jedoch nicht in jedem Fall ein Verantwortlicher benannt werden. So richten sich Angriffe mit Phishing-Mails häufig direkt gegen die Betroffenen. Gleiches gilt für Daten, die Täter durch infizierte Endgeräte erlangen. Es kann zudem vorkommen, dass ein Datenschutzvorfall vom Verantwortlichen (noch) nicht entdeckt wurde, die erbeuteten Daten aber bereits auf dem Schwarzmarkt gehandelt werden. Schließlich bleibt noch die Möglichkeit, dass die verantwortliche Organisation nicht mehr existiert, z.B. aufgrund einer Insolvenz, und mithin auch keine Stelle mehr für die Benachrichtigung zuständig ist. In all den genannten Fällen bleibt die Benachrichtigung der Betroffenen aus.

Der zweite kritische Punkt des Artikels 34 ist die Risikobeurteilung. Hier ist die zeitliche Komponente in Bezug auf die Risikobeurteilung eines Datenschutzvorfalls von hoher Relevanz. Wird ein Datenschutzvorfall vom Verantwortlichen bemerkt und dann einer Beurteilung unterzogen, so fordert der Gesetzgeber eine Risikobewertung anhand objektiver Maßstäbe. Hierzu sollen gemäß Erwägungsgrund (ErwGr) 76 Art, Umfang, Umstände und Zwecke der Verarbeitung einbezogen werden. Der Einfluss zukünftiger technischer Entwicklungen wird in diesem Zusammenhang nicht erwähnt, sondern findet sich lediglich in ErwGr 26. Die Risikobestimmung im Fall einer Datenschutzverletzung ist jedoch maßgeblich von kurz-, mittel und langfristigen Entwicklungen abhängig. Insofern ist auf die Anforderung aus ErwGr 26 in Bezug auf das Bestehen eines Personenbezugs zu verweisen, wenn es dort heißt:

„Bei der Feststellung ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.“

Aus dieser Überlegung folgt, dass ein Datenschutzvorfall, der heute nur mit einem geringen Risiko behaftet ist, in zehn Jahren aufgrund der veränderten äußeren Umstände durchaus zu einem hohen Risiko für die Betroffenen werden kann. Es anschauliches Beispiel hierfür ist der Einsatz von Verschlüsselung. Die Vorhersage über die zukünftige Sicherheit kryptographischer Verfahren ist – wenn überhaupt – nur begrenzt möglich. Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) geht davon aus, dass Vorhersagen über 2025 hinaus nicht möglich sind.¹⁶⁰ Ein Datenschutzvorfall von dem vertrauliche personenbezogene Daten betroffen sind, die nach Stand der Technik durch als sicher geltende Verschlüsselung gegen die Kenntnisnahme Unberechtigter geschützt sind, kann in zehn Jahren zu einem Risiko für die Betroffenen werden. Es ist jedoch nicht davon auszugehen, dass der Verantwortliche in zehn Jahren die Risikobewertung für diesen Vorfall wiederholen wird, da dies in der DSGVO nicht vorgesehen ist. Im Ergebnis führt dies dazu, dass Betroffene auch in diesem Fall nicht informiert werden, zumal Art. 34 Abs. 3 a) DSGVO eine Ausnahme von der Benachrichtigungspflicht vorzieht, wenn der Verantwortliche Maßnahmen zum Schutz vor einer unberechtigten Kenntnisnahme auf die betroffenen Daten angewandt hat.

Eine Ausnahme von der persönlichen Benachrichtigung besteht zusätzlich in den Fällen in denen diese einen unverhältnismäßigen Aufwand für den Verantwortlichen bedeuten würde (Art. 34 Abs. 3 c) DSGVO). Dieser Punkt steht hingegen in engem Zusammenhang mit der Handlungsfähigkeit der Betroffenen. Eine persönliche Ansprache stellt sicher, dass Betroffene einen Datenschutzvorfall tatsächlich zur Kenntnis nehmen. Allgemeine Bekanntmachungen bergen in der Regel die Gefahr, dass sie nicht alle Betroffenen erreichen. Dies gilt insbesondere für

¹⁶⁰ BSI – TR-02102-1 Kryptographische Verfahren. Empfehlungen und Schlüssellängen (Stand Februar 2019), über: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=10, S. 16 (Stand 02.07.2019).

Dienste mit sehr diverser Nutzer*innenklientel. Hier ist die Wahrscheinlichkeit, dass nur ein Teil der Zielgruppe erreicht wird besonders hoch. Vorausgesetzt die Nutzer*innen fühlen sich tatsächlich angesprochen, besteht eine weitere Hürde in Bezug auf den Inhalt der Nachricht. Allgemeine Benachrichtigungen können nur in den Fällen hilfreich sein, in denen dieselben Maßnahmen für alle Betroffenen vorgeschlagen werden können. Auf individuelle Besonderheiten kann in diesen Fällen nicht eingegangen werden.

4.5.2 Datenschutzkonzeption

Ein Warnsystem sollte nicht nur die Schwächen der bestehenden Benachrichtigungspflichten minimieren, sondern auch keine zusätzlichen Risiken für die Betroffenen kreieren. Die Verarbeitung personenbezogener Daten birgt jedoch grundsätzlich Risiken für die von der Verarbeitung Betroffenen. Hierbei ist es unerheblich, dass die entsprechenden Daten aus freizugänglichen Quellen stammen. Die Risikobeurteilung einer Datenverarbeitung beurteilt sich grundsätzlich anhand des Verfahrens an sich. Äußere Umstände, wie im vorliegenden Fall, sollten einbezogen werden, können jedoch weder Legitimationsgrundlage noch Rechtfertigung für etwaige Mängel der Verarbeitung darstellen. Das heißt, bei der Konzeption eines derartigen Warnsystems müssen dieselben Maßstäbe angesetzt werden, wie bei anderen Verfahren des gleichen Risikotyps. Dies gilt in vorliegenden Fall insbesondere für konkrete technische und organisatorische Maßnahmen, die die Vertraulichkeit der personenbezogenen Daten sicherstellen sollen.

Grundvoraussetzung für jede Datenverarbeitung ist hierbei die Rechtmäßigkeit. Da für das vorliegende Verfahren auf keine Grundlage zurückgegriffen werden kann, die eine Aktion oder Reaktion der Betroffenen erfordern, kommen die Artikel 6 Abs. 1 a) und b) DSGVO nicht in Frage. Auch eine lebensbedrohliche Situation für Betroffene oder Dritte liegt nicht vor, demnach scheidet auch Art. 6 Abs. 1 d) DSGVO als Rechtsgrundlage aus. Ein präventives Warnsystem kann demnach auf Grundlage eines Gesetzes (Art. 6 Abs. 1 e) DSGVO) bzw. in Ausübung öffentlicher Gewalt betrieben werden. Alternativ kommt eine Verarbeitung auf Grundlage einer rechtlichen Verpflichtung (Art. 6 Abs. 1 c) DSGVO) oder eines berechtigten Interesses in Frage (Art. 6 Abs. 1 f) DSGVO).

Die Verarbeitung durch eine öffentliche Stelle kann vor dem Hintergrund staatlicher Schutzpflichten gesehen werden. Grundsätzlich ist jedoch zu hinterfragen, ob dies eine generelle Verarbeitungspflicht für alle potentiell geleakten Daten begründet. Naheliegender ist, dass sich die Verarbeitung in diesem Fall nur auf einige wenige langlebige und/oder besonders sensible personenbezogene Daten beschränken würde, die nur von öffentlichen Stellen vergeben werden, z. B. Reisepass- oder Rentenversicherungsnummern. Die ausschließlich privat genutzte, aber zentrale Kombination aus E-Mail-Adresse und Passwort fällt aus diesen Anwendungen jedoch heraus. Art. 6 Abs. 1 e) wäre nach dieser Lesart nur sehr begrenzt als Rechtsgrundlage anwendbar und würde die meisten Vorfälle nicht abdecken. Das eigentliche Ziel des präventiven Warnens würde verfehlt.

Die Verarbeitung aus einer rechtlichen Verpflichtung herzuleiten, ist ebenfalls nur begrenzt möglich. Zwar fordert Art. 32 DSGVO unter anderem, dass der Verantwortliche die Datensicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) auf Dauer zu gewährleisten hat. Die bezieht sich jedoch nur auf die eigene Verarbeitung und nicht auf zufällig übereinstimmende personenbezogene Daten von anderen Verantwortlichen. Grundsätzlich steht es dem Gesetzgeber weiterhin offen, eine Konkretisierung oder Erweiterung, beispielsweise des Art. 34 DSGVO, vorzunehmen und ein präventives Benachrichtigungssystem zu etablieren.

Es bleibt Artikel 6 Abs. 1 f) DSGVO als letzte Variante zur Auswahl. Die Verarbeitung auf Grund eines berechtigten Interesses des Verantwortlichen ist grundsätzlich möglich. Abhängig davon, welche Stellen die Verarbeitung übernehmen, stellt sich jedoch die Frage, inwieweit das Interesse der Betroffenen daran, dass die bereits geleakten Daten von diesen nicht verarbeitet werden ggf. überwiegt. Unter der Annahme, dass eine neutrale bzw. vertrauenswürdige Stelle als Treuhänder die Erhebung und Aufbereitung der Daten übernimmt, sollten die Interessen der Betroffenen dem nicht entgegenstehen. Die Vertrauenswürdigkeit der erhebenden Stelle (Datenanalyst) wird unter anderem dadurch sichergestellt, dass diese keine Informationen darüber erhält mit welchen Kooperationspartner*innen Betroffene in Beziehung stehen. Die Stelle erhält nur Informationen, die öffentlich verfügbar sind und stellt diese für die Kooperationspartner*innen zum Abruf bereit, erhält jedoch keine Rückmeldung darüber, welche Informationen bei welchen Stellen zu einer Warnung führen.

Die Kooperationspartner*innen (Provider) stehen bereits mit den potentiell Betroffenen in Kontakt. Es ist ihnen daher im Gegensatz zum Datenanalysten möglich die Verarbeitung aus dem Warnsystem auf eine Einwilligung der Betroffenen zu stützen, diese in die Allgemeinen Geschäftsbedingungen (Vertragsbedingungen) aufzunehmen oder ebenfalls im Sinne eines berechtigten Interesses Daten für den Zweck einer frühzeitigen Warnung zu verarbeiten.

4.6 Risiken der Verarbeitung

Neben der Rechtmäßigkeit des Verfahrens und der Zweckbindung der Daten sind vor der Inbetriebnahme die Risiken für die Rechte und Freiheiten der Betroffenen zu bewerten, die durch das Verfahren entstehen können. Eine ausführliche Risikoanalyse, wie sie für ein solches Verfahren erforderlich ist, würde den Umfang dieses Beitrags übersteigen, daher soll im Folgenden nur auf einige zentrale Verarbeitungsrisiken eingegangen werden, die besonders kritisch für das hier erörterte Verfahren sind.

4.6.1 Datenminimierung

Die geplante Verarbeitung basiert auf der Erhebung öffentlich zugänglicher Daten aus dem Internet. In diesem Zusammenhang ist bei der Gestaltung des Systems darauf zu achten, dass nicht wahllos Daten gesammelt und gespeichert werden. Die Erforderlichkeit der Daten ergibt sich aus dem Zweck der Verarbeitung und den beteiligten Kooperationspartner*innen. Im vorliegenden Fall sollen die Betroffenen immer dann benachrichtigt werden, wenn ein Datensatz sich potentiell dazu eignet deren Identität zu übernehmen oder deren personenbezogene Daten anderweitig in betrügerischer Absicht zu missbrauchen. Da die Benachrichtigung von den Kooperationspartner*innen übernommen wird, richtet sich die Erforderlichkeit nach den auf deren Seite vorhandenen identifizierenden Merkmalen.

Viele Online-Dienste verwenden E-Mail-Adressen sowohl als Identifikatoren als auch als Kommunikationsmittel. Daher sind E-Mail-Adressen für den vorgesehenen Zweck gut geeignet. Informationen die

grundsätzlich weder der (eindeutigen) Identifizierung bei Kooperationspartner*innen dienen noch zur Kommunikation geeignet sind, werden nicht vorgehalten. Dies betrifft insbesondere sensible Daten, wie sie z. B. in Art. 9, 10 und 11 DSGVO aufgeführt sind.

Das Pendant zur Erhebung stellt die Löschung dar. Da täglich Daten aus neuen Quellen verarbeitet werden, sind Kriterien für die Löschung festzulegen. Grundsätzlich müssen bereits erfasste Leaks nicht noch einmal verarbeitet werden. Dies gilt umso mehr, wenn es sich hierbei um alte, allgemein bekannte Veröffentlichungen handelt, die lediglich erneut in Umlauf gebracht wurden.¹⁶¹ Darüber hinaus sind auch einmalige Veröffentlichungen zu löschen, wenn diese ein bestimmtes Alter erreicht haben. Es ist davon auszugehen, dass die Durchsetzung (zivil-)rechtlicher Ansprüche nach 36 Monaten verjährt und die Verarbeitung der Daten über diesen Zeitpunkt hinaus für die Betroffenen keinen erkennbaren Vorteil mehr hat, wohl aber ein Datenschutzrisiko darstellt, weil nicht erforderliche personenbezogene Daten weiterhin verarbeitet werden.

4.6.2 Vertraulichkeit, Verfügbarkeit und Integrität

Datensicherheit mit den drei Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität ist für jede Form der Verarbeitung ein essentieller Baustein im Datenschutzkonzept. Die Tatsache, dass Datenkategorien, wie Passworte, Kreditkartennummer oder Bankverbindungen verarbeitet werden, erfordert, dass diese so vertraulich behandelt werden, als wären sie nicht öffentlich verfügbar.

Die Integrität der Daten darf zudem nicht beeinträchtigt werden, damit sowohl die Identifizierung als auch die Benachrichtigung des jeweiligen Betroffenen fehlerfrei gewährleistet werden kann. Diese Gewährleistung setzt jedoch voraus, dass die Daten entsprechend der erarbeiteten Spezifikationen für die Kooperationspartner*innen zur Verfügung stehen. Hierdurch soll auch der Versand von Falschmeldungen vermieden werden.

¹⁶¹ Zum Beispiel der Leak von Yahoo.

4.6.3 Transparenz

Erreicht die Benachrichtigung schließlich die Betroffenen muss diese ebenfalls bestimmten Anforderungen genügen. Einerseits sollte die Botschaft der Warnung in klarer und einfacher Sprache formuliert sein, damit das beabsichtigte Ziel erreicht werden kann. Dies betrifft zum einen Informationen über den jeweiligen Datenschutzvorfall und das damit verbundene Risiko für die Betroffenen, zum anderen aber auch Hinweise zum weiteren Vorgehen.

Des Weiteren erfordert dieser Erstkontakt mit Betroffenen, dass Informationspflichten (Art. 14 DSGVO) erfüllt werden, die sich auf die Verarbeitung durch den Verantwortlichen beziehen. Dies schließt auch die Belehrung über Betroffenenrechte und Widerspruchsmöglichkeiten (Art. 15–22 DSGVO) gegen die Verarbeitung ein. Da von Seiten der Verantwortlichen keine Möglichkeit besteht zu überprüfen, ob alle Betroffenen informiert wurden, sollten diese auch selbstständig überprüfen können, ob sie gegebenenfalls betroffen sind. Hierfür ist ein Auskunftssystem vorgesehen, dass anhand der eingegebenen E-Mail-Adresse den zugehörigen Datensatz ermittelt und eine Benachrichtigung direkt an das entsprechende E-Mail-Konto versendet.

4.6.4 Nichtverkettung und Intervenierbarkeit

Die Betroffenen sind nicht nur über ihre Rechte aufzuklären, sondern es muss auch die Möglichkeit bestehen diese Rechte ohne Hürden gegenüber dem Verantwortlichen durchzusetzen. Dies umfasst vor allem Löschansprüche der Betroffenen, die in zwei Varianten zur Verfügung stehen. Betroffene können die vorhandenen Daten löschen lassen oder sie können die Daten löschen lassen und einer weiteren Benachrichtigung widersprechen. Im zweiten Fall wird ein Hashwert der E-Mail-Adresse hinterlegt, der automatisch die Erhebung neuer Datensätze zur gleichen E-Mail-Adresse bzw. zum gleichen Hashwert unterbindet.

4.6.5 Risikobeurteilung

Zusammenfassend ist festzuhalten, dass die neben der großen Anzahl der potentiell Betroffenen, der verarbeiteten Datenkategorien, der Einbeziehung der Betroffenen zu einem relativ späten Zeitpunkt sowie der Neuartigkeit des Verfahrens von einem hohen Risiko auszugehen ist.

4.7 Fazit

Der Ansatz eines präventiven Warnsystems bietet Betroffenen erstmals die Möglichkeit Identitätsbetrügern einen Schritt voraus zu sein. Ein erhöhtes Bewusstsein für die Problematik öffentlich verfügbarer, vertraulicher Informationen gepaart mit entsprechender Aufklärung und Hilfestellung kann den Betroffenen die Kontrolle zumindest in Teilen zurückgeben und die möglichen Folgen mindern. Das Verfahren trägt jedoch auch Risiken in sich. Ein solides und durchdachtes Datenschutzkonzept trägt dazu bei, dass das Verfahren nicht selbst zum Datenleck wird und stellt sicher, dass Betroffene keinen zusätzlichen Schaden erleiden.

5 DER WERT DIGITALER GÜTER – STEUERRECHTLICHE EINORDNUNG

*Julia Sinnig*¹⁶²

Was sind eigentlich digitale Güter und Daten wert? Insbesondere im Steuerrecht stellt sich diese Frage zwangsläufig, da das Erwirtschaften von Gewinnen bzw. die Schaffung eines Mehrwerts durch Erbringung digitaler Dienstleistungen möglicherweise ein steuerbares Ereignis darstellen. Ziel dieses Beitrags ist es, die steuerrechtlichen Instrumente zur Bewertung digitaler Güter und Daten vorzustellen und somit einen Überblick zu verschaffen, wie deren Wert in der Praxis beziffert wird. Darüber hinaus sollen die Schwierigkeiten der internationalen Steuerrechtsordnung zu diesem Thema dargelegt werden.

Nach einer kurzen Einführung, die einen Überblick über den heutigen Stand des internationalen Steuerrechts und die Herausforderungen im Themengebiet der Besteuerung der digitalisierten Welt bietet, werden im Hauptteil zwei Fragen erörtert. Zunächst stellt sich die Frage der steuerlichen Wertermittlung digitaler Güter. Diese betrifft die konkrete „Mikroperspektive“ des Steuerzahlers: Wie spiegelt sich der Wert von digitalen Gütern und Daten in der Buchhaltung und letztlich dem Steuerbescheid eines Unternehmens wider? Im zweiten Kapitel des Hauptteils wird aus Sicht der Staaten, also einer globalen „Makroperspektive“, eruiert, ob Daten Grundlage für eine Wertschöpfung im Ertragsteuerrecht sind, die eine Besteuerung ermöglichen sollte. Frage ist also, wo diese Erträge zu lokalisieren sind und welcher Staat somit ein Besteuerungsrecht ausüben dürfen sollte. Es stellen sich hierzu systemische Fragen der internationalen Steuerrechtsordnung, die derzeit aufgearbeitet werden. Der Beitrag schließt mit einem Fazit und Ausblick auf künftige Entwicklungen ab.

¹⁶² Mehr über die Autorin erfahren Sie im Autor*innenhinweis auf S. 110.

5.1 Überblick über das internationale Steuerrecht heute

Der nachfolgende Beitrag behandelt ertrag- und umsatzsteuerrechtliche Aspekte bei der Bewertung digitaler Güter und Daten. Der ertragsteuerrechtliche Teil konzentriert sich lediglich auf die Unternehmens-, nicht jedoch die Einkommenbesteuerung natürlicher Personen.

5.1.1 Ertragsteuerrecht

Die erste Frage, die sich für ein Unternehmen im Ertragsteuerrecht stellt, ist, wo und wie Einkünfte besteuert werden. Im internationalen Ertragsteuerrecht wird bei der Aufteilung von Besteuerungsrechten grundsätzlich zwischen Ansässigkeits- und Quellenstaat unterschieden. Um Doppelbesteuerung zu vermeiden, stimmen Staaten in (zumeist) bilateralen Doppelbesteuerungsabkommen (DBA) ab, welcher der beiden Staaten (Ansässigkeits- oder Quellenstaat) welche Art der Einkünfte unter welchen Bedingungen besteuert. Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) hat ein Musterabkommen (MA) ausgearbeitet,¹⁶³ auf dessen Grundlage viele Staaten ihre bilateralen DBA abschließen, um ihre komplexen nationalen Steuerrechtsordnungen zu koordinieren.

Ansässigkeitsstaat ist der Staat, in dem der Steuerzahler (juristische oder natürliche Person) gemäß Artikel 4 des OECD MA ansässig ist. Quellenstaat ist der andere Staat, in dessen Hoheitsgebiet die Einkünfte ihren Ursprung finden.¹⁶⁴

Im Fall von Unternehmensgewinnen regelt Artikel 7 (1) des OECD MA eine ausschließliche Besteuerung im Ansässigkeitsstaat, mit Ausnahme von Situationen, in denen die Geschäftstätigkeit durch eine im anderen

163 Erstmalig veröffentlichte die OECD ein solches MA sowie Kommentare zu den einzelnen Vorschriften im Jahr 1963. Seither wird das MA regelmäßig überarbeitet; zuletzt wurde eine aktualisierte Version 2017 veröffentlicht. Da die meisten DBA dem MA der OECD ähneln, ist es sinnvoll, sich bei einer allgemeinen Diskussion auf die Vorschriften des MA zu beziehen. Das MA und Kommentare zu den einzelnen Vorschriften sind verfügbar unter: <https://www.oecd.org/tax/treaties/model-tax-convention-on-income-and-on-capital-condensed-version-20745419.htm> (alle Webseiten wurden zuletzt am 29. Juli 2019 aufgerufen). Zitate des OECD MA in diesem Beitrag beruhen auf der aktuellen Fassung (2017).

164 S. hierzu auch: *Lehner*, Grundlagen des Abkommensrechts, in: Vogel/Lehner (Hrsg.), DBA, Beck 2015 (6. Aufl.), insb. Rn. 7, 11 und 23.

Staat, also dem Quellenstaat, bestehende Betriebsstätte ausgeübt wird. Artikel 5 (1) des OECD MA definiert die Betriebsstätte als „feste Geschäftseinrichtung, durch die die Geschäftstätigkeit eines Unternehmens ganz oder teilweise ausgeübt wird“. Wichtiges Merkmal der Betriebsstätte ist das Vorliegen einer physischen Präsenz im Quellenstaat („feste Geschäftseinrichtung“). Dieser enge Betriebsstättenbegriff soll sicherstellen, dass weit gefasste nationale außensteuerrechtliche Vorschriften begrenzt werden, um die Unternehmensbesteuerung zu vereinfachen und den grenzüberschreitenden Wirtschaftsverkehr zu liberalisieren.¹⁶⁵

Für Unternehmen, die ihre Erträge durch die Erbringung digitaler Dienstleistungen oder den Vertrieb digitaler Güter erwirtschaften, bedeutet dies meist eine ausschließliche Besteuerung im Ansässigkeitsstaat, da die Ausübung der Geschäftsaktivität als solche zunächst keine feste Geschäftseinrichtung in Kundennähe erfordert.¹⁶⁶ Während das Betriebsstättenkonzept ursprünglich u. a. auch darauf abzielte, eine Besteuerung am Ort der eigentlichen Geschäftstätigkeit dann zuzulassen, wenn eine „intensive[n] geschäftliche[n] Bindung“ zum Quellenstaat vorliegt,¹⁶⁷ kann heutzutage eine solche intensive geschäftliche Bindung im Quellenstaat auch ohne physische Präsenz gegeben sein, was durch den engen Betriebsstättenbegriff, der auf die feste Geschäftseinrichtung abstellt, jedoch zu keiner Besteuerung führt. Durch den Wandel der wirtschaftlichen Realität im Rahmen der Digitalisierung stimmen somit Ziel und Wortlaut der Norm nicht mehr vollumfänglich überein.¹⁶⁸ Da sich die Ansässigkeit eines Unternehmens gemäß Artikel 4 (1) des OECD MA durch den Sitz des Unternehmens bzw. den Ort seiner Geschäftsleitung relativ leicht vom Steuerzahler selbst bestimmen lässt, liegt somit auch die Wahl der ertragsteuerlichen Rahmenbedingungen in den Händen des Steuerzahlers.

165 Görl, Artikel 5 – Betriebsstätte, in: Vogel/Lehner (Hrsg.), DBA, Beck 2015 (6. Aufl.), Rn. 3.

166 Dank der globalen Vernetzung durch das Internet können neue Märkte wesentlich einfacher erschlossen werden als noch vor fünfzig Jahren, als Unternehmen sich oft zwangsläufig in der physischen Nähe ihrer Märkte ansiedeln mussten, um ihre Kund*innen zu erreichen.

167 Görl, Artikel 5 – Betriebsstätte, in: Vogel/Lehner (Hrsg.), DBA, Rn. 2. S. auch OECD, Kommentar zu Artikel 7 (engl. Originalfassung), Rn. 11.

168 Zum Ziel der Norm, s. OECD, Kommentar zu Artikel 7 (engl. Originalfassung), Rn. 11. S. auch: OECD, Programme of Work to Develop a Consensus Solution to the Tax Challenges Arising from the Digitalisation of the Economy, 29. Mai 2019, abrufbar unter: <https://www.oecd.org/tax/beps/programme-of-work-to-develop-a-consensus-solution-to-the-tax-challenges-arising-from-the-digitalisation-of-the-economy.pdf>, Rn. 24; Eilers/Oppel, IStR 2018, 361 (362, 370).

Artikel 7 (1) des OECD MA findet nur Anwendung, wenn die Einkünfte nicht in den Anwendungsbereich einer der spezifischeren Vorschriften fallen. Bestimmte Erträge, die auf Grundlage der Nutzung oder Bereitstellung digitaler Güter und Daten erwirtschaftet werden, können jedoch ggf. als Lizenzgebühren eingeordnet werden. Lizenzgebühren sind gemäß Artikel 12 (2) des OECD MA „Vergütungen jeder Art, die für die Benutzung oder für das Recht auf Benutzung von Urheberrechten an literarischen, künstlerischen oder wissenschaftlichen Werken, einschließlich kinematographischer Filme, von Patenten, Marken, Mustern oder Modellen, Plänen, geheimen Formeln oder Verfahren oder für die Mitteilung gewerblicher, kaufmännischer oder wissenschaftlicher Erfahrungen gezahlt werden“. Lizenzgebühren werden gemäß Artikel 12 (1) des OECD MA im Ansässigkeitsstaat des Zahlungsempfängers besteuert.¹⁶⁹

Zusammenfassend werden Unternehmensgewinne, die durch die Nutzung bzw. den Vertrieb digitaler Güter und Daten erwirtschaftet werden, also in den meisten Fällen im Ansässigkeitsstaat des Unternehmens besteuert. Für den Wert digitaler Güter und Daten stellt sich hier also insbesondere die Frage der Wertermittlung, die bei konzerninternen Transaktionen im Rahmen der Verrechnungspreisermittlung problematisch sein kann (siehe hierzu Abschnitt 5.2). Darüber hinaus ist fraglich, ob und wie das Betriebsstättenkonzept abgeändert werden sollte, um auf die Tätigkeit digitaler Geschäftsmodelle Anwendung zu finden (siehe hierzu Abschnitt 5.3).

5.1.2 Umsatzsteuerrecht

Die Umsatzsteuer (USt) ist eine mehrstufige Besteuerung der jeweiligen Wertschöpfung auf jeder Stufe der Erzeugung und des Vertriebs.¹⁷⁰ Hierzu werden die eingenommene und ausgegebene USt des Unterneh-

169 Es ist anzumerken, dass Artikel 12 (2) des MA der Vereinten Nationen das Besteuerungsrecht bzgl. Lizenzgebühren zwischen Ansässigkeits- und Quellenstaat aufteilt. Dieses MA wird vor allem von weniger entwickelten Staaten bevorzugt als DBA-Grundlage genutzt, da es dem Quellenstaat mehr Besteuerungsrechte zuteilt.

170 Art. 1 (2) S. 1 der Richtlinie 2006/112/EG des Rates über das gemeinsame Mehrwertsteuersystem vom 28. November 2006, ABl. EU Nr. L 347, S. 11 ff., berichtigt 2007 Nr. L 335, S. 60 ff. (MwStSystRL); Klenk, Wesen der Umsatzsteuer, Verhältnis von nationalem Recht zu Unionsrecht, in: Sölch/Ringleb (Hrsg.), UStG, Beck 2019 (85. Aufl.), Rn. 9; Robisch, Einleitende Hinweise zum Umsatzsteuerrecht, in: Bunjes (Hrsg.), UStG, Beck 2018 (17. Aufl.), Rn. 19.

mens verrechnet, um den Mehrwert, den das jeweilige Unternehmen beigetragen hat, zu besteuern.¹⁷¹ Die Kosten der Umsatzsteuer trägt der Verbraucher.¹⁷² Kohärenterweise sollte eine Verbrauchssteuer am Ort des Verbrauchs erhoben werden, was bedeutet, dass der Ort der Besteuerung im europäischen Umsatzsteuerrecht i. d. R. das Bestimmungsland ist.¹⁷³ Insbesondere in Hinblick auf sonstige Leistungen, die gegenüber Verbrauchern auf elektronischem Wege erbracht werden, ist der Bestimmungsort oft schwierig zu bestimmen. Bestimmungsort ist hier der Ort, „an dem der Leistungsempfänger seinen Wohnsitz, seinen gewöhnlichen Aufenthaltsort oder seinen Sitz hat“.¹⁷⁴

Steuerbar sind gemäß § 1(1) UStG Umsätze, die ein Unternehmen durch „Lieferungen und sonstige[n] Leistungen, die ein Unternehmer gegen Entgelt im Rahmen seines Unternehmens ausführt“, erwirtschaftet. Bemessungsgrundlage für die USt ist also das Entgelt, das gemäß § 10 (1) S. 2 UStG alles ist, was der Leistungsempfänger aufwendet, um die Leistung zu erhalten (abzgl. der USt).¹⁷⁵ Grundsätzlich sollten, im Einklang mit dem Neutralitäts- und Gleichheitsgrundsatz, auch Tauschgeschäfte der USt obliegen.¹⁷⁶ Insbesondere vor dem Hintergrund der „Lieferung“ digitaler Güter (wie z. B. auch Content) oder Nutzerdaten ist diese Frage berechtigter denn je, da heute viele Geschäftsmodelle unentgeltlich

171 Art. 1 (2) S. 2 MwStSystRL; s. auch: *Robisch*, Einleitende Hinweise zum Umsatzsteuerrecht, in: Bunjes (Hrsg.), UStG, Rn. 13 u. 19–21.

172 *Klenk*, Wesen der Umsatzsteuer, Verhältnis von nationalem Recht zu Unionsrecht, in: Sölch/Ringleb (Hrsg.), UStG, Rn. 4 u. 9; *Robisch*, Einleitende Hinweise zum Umsatzsteuerrecht, in: Bunjes (Hrsg.), UStG, Rn. 13 f. u. 19 f.

173 *Robisch*, Einleitende Hinweise zum Umsatzsteuerrecht, in: Bunjes (Hrsg.), UStG, Rn. 7 u. 26 f.; *Robisch*, § 1a Innergemeinschaftlicher Erwerb, in: Bunjes (Hrsg.), UStG, Rn. 1.

174 § 3a (5) S. 1 Hs. 2 UStG. In der Praxis kann dieser Ort durch verschiedene Indizien und Vermutungsregelungen bestimmt werden, die tw. jedoch widersprüchlich sein können. S. auch: *Wäger*, § 3a Ort der sonstigen Leistung, in: Sölch/Ringleb, UStG, Rn. 337 ff.

175 Der genaue Wortlaut lautet: „Entgelt ist alles, was den Wert der Gegenleistung bildet, die der leistende Unternehmer vom Leistungsempfänger oder von einem anderen als dem Leistungsempfänger für die Leistung erhält oder erhalten soll, einschließlich der unmittelbar mit dem Preis dieser Umsätze zusammenhängenden Subventionen, jedoch abzüglich der für diese Leistung gesetzlich geschuldeten Umsatzsteuer.“ S. auch: *Oelmaier*, § 1 Steuerbare Umsätze, in: Sölch/Ringleb (Hrsg.), UStG, Rn. 36 ff.

176 Ist es gerechtfertigt, dass Facebook keine USt erheben muss, wenn es seine Dienstleistungen „kostenlos“ im Tausch gegen Datenverwertungsrechte anbietet, auf Grundlage derer Werbeflächen (an andere u. U. gem. § 15 (1) (1.) UStG vorsteuerabzugsberechtigte Unternehmen) entgeltlich angeboten werden; anstatt wenn es seine Dienstleistungen gegen eine vom Nutzer getragene Gebühr anbietet? S. u. Abschnitt 5.2.2. Zum Neutralitätsgrundsatz, s. auch: *Klenk*, Wesen der Umsatzsteuer, Verhältnis von nationalem Recht zu Unionsrecht, in: Sölch/Ringleb (Hrsg.), UStG, Rn. 10.

funktionieren, da der Nutzer seine Datenverwertungsrechte gegen eine auf den ersten Blick „kostenlose“ Dienstleistung „tauscht“. Die Steuerbarkeit im Rahmen der USt ist jedoch strittig.¹⁷⁷

Im Ergebnis konzentrieren sich die Probleme im Rahmen der USt also auf die Ermittlung des Leistungsorts und die umsatzsteuerliche Behandlung von Tauschgeschäften.

5.2 Steuerliche Werterfassung von digitalen Gütern und Daten

5.2.1 Ertragsteuerliche Werterfassung

Wie während der Sommerkonferenz von Aline Blankertz ausgeführt, ist der Wert digitaler Güter für die Nutzer*innen ebendieser deutlich spürbar. Wie jedoch spiegelt sich dieser Wert in der Besteuerung der Unternehmen wider?

5.2.1.1 Digitale Güter

Wenn ein Unternehmen Gewinne aus dem Vertrieb digitaler Güter erwirtschaftet, stellen sich diese im Umsatz des Unternehmens dar. Der steuerrechtliche Wert digitaler Güter definiert sich also i. d. R. über den Preis, den Kund*innen bereit sind, zu zahlen. Schwierigkeiten bei der Ermittlung des Werts digitaler Güter zeichnen sich insbesondere im Szenario der unternehmens- bzw. konzerninternen Aufteilung von Ge-

¹⁷⁷ Zur Diskussion um Tauschgeschäfte im USt-Recht, siehe auch: EuGH, Urt. v. 23. November 1988, *Naturally Yours Cosmetics Ltd/Commissioners of Customs and Excise*, Rs. C-230/87; EuGH, Urt. v. 2. Juni 1994, *Empire Stores Ltd/Commissioners of Customs and Excise*, Rs. C-33/93; EuGH, Urt. v. 3. Juli 1997, *Goldsmiths (Jewellers) Ltd/Commissioners of Customs and Excise*, Rs. C-330/95; EuGH, Urt. v. 26. September 2013, *Serebryannay vek EOOD/Direktor na Direksia 'Obzhalvane i upravlenie na izpalnenieto'*, Rs. C-283/12; EuGH, Urt. v. 19. Dezember 2012, *Direktor na Direksia 'Obzhalvane i upravlenie na izpalnenieto'/Orfey Bulgaria EOOD*, Rs. C-549/11; *Melan/Wecke*, DStR 2015, 2267; *Melan/Pfeiffer*, DStR 2017, 1072; *Pfeiffer*, *International VAT Monitor* 2016, 158; *Bal*, *Bulletin for International Taxation* 2018 [online veröffentlicht], Abschnitt 7; *Kollmann*, *Taxable Supplies and Their Consideration in European VAT – With Selected Examples of the Digital Economy*, IBFD Doctoral Series vol 46 (IBFD 2019), Abschnitt 5.3.2.2.; *Scheffler*, DStR 2018, 1783; *Grambeck*, DStR 2016, 2026; *Andersson*, *Bulletin for International Taxation* 2018, 684.

winnen ab: Dies kann einerseits der Fall sein, wenn Gewinne zwischen Stammhaus und Betriebsstätte (sofern vorhanden, s. o. Abschnitt 5.1.1, und zurechenbar) aufgeteilt werden müssen; oder andererseits, wenn digitale Güter innerhalb eines Konzerns zwischen Konzerngesellschaften transferiert werden. In letzterem Fall muss der Preis solcher Transaktionen gemäß Artikel 9 (1) des OECD MA auf Grundlage des Fremdvergleichsgrundsatzes ermittelt werden (s. u.).

Ist eine Betriebsstätte vorhanden, der die Gewinne aus dem Vertrieb digitaler Güter zugerechnet werden können, so wird die Betriebsstätte gemäß AOA¹⁷⁸ als „selbstständiges und eigenständiges Unternehmen“¹⁷⁹ angesehen. Für die Aufteilung der Gewinne zwischen Betriebsstätte und Stammhaus müssen die Gewinne der Betriebsstätte also gemäß Artikel 7 (2) des OECD MA so berechnet werden, als hätte die Betriebsstätte sie durch den Vertrieb digitaler Güter an Dritte erworben.

Ähnlich ist die Situation konzerninterner Transaktionen, die nach dem Fremdvergleichsgrundsatz¹⁸⁰ bepreist werden. Der Fremdvergleichsgrundsatz sieht vor, dass konzerninterne Transaktionen so bepreist werden, wie sie zwischen unabhängigen Dritten unter gleichen oder vergleichbaren Verhältnissen bepreist worden wären.¹⁸¹ Warum ist dies

178 „AOA“ steht für „Authorised OECD Approach“, der im Betriebsstättenbericht der OECD im Jahr 2008 erstmalig vorgestellt wurde. Für weitere Erläuterungen und die Entstehung des AOA, s. auch: Kraft, AStG § 1 Berichtigung von Einkünften, in: Kraft (Hrsg.), Außensteuergesetz, Beck 2019 (2. Aufl.), Rn. 590 ff.

179 Selbstständigkeitsfiktion der Betriebsstätte („Functionally Separate Entity Approach“ der OECD), s. Art. 7 (2) OECD MA und OECD, Betriebsstättenbericht 2010, Teil I, Tz. 50. S. auch: Kraft, AStG § 1 Berichtigung von Einkünften, in: Kraft (Hrsg.), Außensteuergesetz, Rn. 10 ff. zum Fremdvergleichsgrundsatz allgemein u. 650 zur Selbstständigkeitsfiktion der Betriebsstätte.

180 Engl.: „arm’s length principle“; s. auch Art. 9 (1) OECD MA: „Wenn a) ein Unternehmen eines Vertragsstaats unmittelbar oder mittelbar an der Geschäftsleitung, der Kontrolle oder dem Kapital eines Unternehmens des anderen Vertragsstaats beteiligt ist, oder b) dieselben Personen unmittelbar oder mittelbar an der Geschäftsleitung, der Kontrolle oder dem Kapital eines Unternehmens eines Vertragsstaats und eines Unternehmens des anderen Vertragsstaats beteiligt sind und in diesen Fällen die beiden Unternehmen in ihren kaufmännischen oder finanziellen Beziehungen an vereinbarte oder auferlegte Bedingungen gebunden sind, die von denen abweichen, die unabhängige Unternehmen miteinander vereinbaren würden, so dürfen die Gewinne, die eines der Unternehmen ohne diese Bedingungen erzielt hätte, wegen der Bedingungen aber nicht erzielt hat, den Gewinnen dieses Unternehmens zugerechnet und entsprechend besteuert werden“ (Unterstreichung hinzugefügt). Für weitere Erläuterungen, s.: Schwenke/Greil, Art. 9 MA Verbundene Unternehmen, in: Wassermeyer (Hrsg.), DBA, Beck 2019 (145. EL), Rn. 1 ff.

181 § 1 (1) AStG; Art. 9 (2) OECD MA; s. auch: Borstell, Kapitel C: Grundsätze, in: Vögele/Borstell/Engler (Hrsg.), Verrechnungspreise, Beck 2015 (4. Aufl.), Rn. 1 ff.

relevant? Würde man keine objektiven oder vergleichbaren Verrechnungspreise ermitteln, wären Tür und Tor zu willkürlichen Gewinnverschiebungen zwischen Konzerngesellschaften geöffnet.¹⁸² Somit könnten Konzerngewinne etwa in Niedrigsteuerländer verschoben werden. Deshalb ist das allgemeine Ziel, Steuerbemessungsgrundlagen, also Gewinne einzelner Gesellschaften, so zu ermitteln, dass sie realistisch sind und die Verrechnungspreisgestaltung nicht zur willkürlichen Gewinnverschiebung genutzt wird.¹⁸³

Zur Ermittlung des Preises, den ein unabhängiger Dritter in vergleichbaren Verhältnissen zahlen würde, gibt es verschiedene Methoden. Drei Standardmethoden versuchen einen vergleichbaren Preis zu ermitteln: die Preisvergleichsmethode,¹⁸⁴ die Wiederverkaufspreismethode¹⁸⁵ und die Kostenaufschlagsmethode.¹⁸⁶ Hilft eine dieser Methoden in einem bestimmten Sachverhalt nicht weiter, etwa weil es schlichtweg keine vergleichbaren Preise gibt, da es sich um ein Unikat handelt, so geht man zur Anwendung der Gewinnmethoden über (entweder Gewinnauf-

182 Man stelle sich etwa vor, dass eine Konzerngesellschaft Rechte an geistigem Eigentum hält, und einer Schwestergesellschaft die Nutzung dieser Rechte gestattet. Die Nutzung wird durch die Zahlung von Lizenzgebühren entlohnt. Ist die erste Gesellschaft in einem Niedrigsteuerland ansässig, so hat der Konzern ein gesteigertes Interesse, die Lizenzgebühren höchstmöglich zu veranschlagen, um so einen maximalen Konzerngewinn in das Niedrigsteuerland zu verschieben.

183 S. auch: *Borstell*, Kapitel C: Grundsätze, in: Vögele/Borstell/Engler (Hrsg.), Verrechnungspreise, Rn. 1.

184 „Comparable uncontrolled price method“. Vergleichsmaßstab ist der „zwischen unabhängigen Dritten vereinbarte Preis“. *Eigelshoven*, Artikel 9. Verbundene Unternehmen, in: Vogel/Lehner (Hrsg.), DBA, Rn. 72. *OECD*, OECD Transfer Pricing Guidelines for Multinational Enterprises and Tax Administrations 2017, verfügbar unter: https://read.oecd-ilibrary.org/taxation/oecd-transfer-pricing-guidelines-for-multinational-enterprises-and-tax-administrations-2017_tpg-2017-en#page104, Rn. 2.13 ff (im Folgenden: OECD Verrechnungspreisrichtlinien 2017).

185 „Resale price method“. Diese Methode wird i. d. R. angewendet, wenn die Lieferung zwischen verbundenen Unternehmen an ein fremdes, drittes Unternehmen weitergeleitet wird. Der Preis, den das dritte Unternehmen zahlt, dient als Grundlage zur Preisermittlung der Lieferung zwischen verbundenen Unternehmen. *Eigelshoven*, Artikel 9. Verbundene Unternehmen, in: Vogel/Lehner (Hrsg.), DBA, Rn. 74; OECD Verrechnungspreisrichtlinien 2017, Rn. 2.27 ff.

186 „Cost plus method“. Der Verrechnungspreis basiert auf den Kosten des Herstellers oder des Leistenden. *Eigelshoven*, Artikel 9. Verbundene Unternehmen, in: Vogel/Lehner (Hrsg.), DBA, Rn. 77 ff.; OECD Verrechnungspreisrichtlinien 2017, Rn. 2.45 ff.

teilungs¹⁸⁷ oder geschäftsfallbezogene Nettomargenmethode¹⁸⁸). Bei manchen digitalen Gütern, wie z. B. Musikdateien, ist es noch vorstellbar, einen Preisvergleich durchzuführen, da die gleichen Musikdateien von verschiedenen Anbietern vertrieben werden. Anders ist dies bspw. bei Algorithmen oder Rechten an geistigem Eigentum, die einen sehr unterschiedlichen Wert in den Händen verschiedener Besitzer*innen haben können, da diese sie unterschiedlich ausschöpfen können.¹⁸⁹ In solchen Fällen müssen die komplexeren Gewinnmethoden angewandt werden.¹⁹⁰

5.2.1.2 Daten

Ähnlich wie bei digitalen Gütern stellen sich auch Probleme in der Bepreisung von Daten. Der Verkauf, bzw. die Sammlung, Verarbeitung und Auswertung von Daten in einem bestimmten Land erfüllt zunächst mangels zwingender physischer Präsenz keinen Betriebsstättentatbestand. Falls diese Aktivitäten etwa durch ein Büro oder eine Zweigstelle in dem jeweiligen Land, in dem Nutzer*innen ansässig sind, deren Daten gesammelt werden, ausgeführt werden, so könnte eine Betriebsstätte bestehen. Wie auch bei digitalen Gütern stellt sich dann in einem nächsten Schritt das Problem der Gewinnaufteilung. Werden Daten an Dritte verkauft, so ist die Bepreisung noch relativ simpel, denn zumindest gibt es eine Bepreisung, und es werden Erträge verbucht. Werden Daten jedoch genutzt, wie z. B. indem sie ausgewertet und auf Grundlage dessen Werbeflächen angeboten werden, wird sich die Bepreisung an den Werbeerträgen orientieren; ist jedoch bereits weniger offensichtlich als beim einfachen Verkauf von Datensätzen.

187 „Profit split method“. Diese Methode wird insbesondere bei Transaktionen, deren Wertschöpfungsprozess wesentlich durch immaterielle Wirtschaftsgüter beeinflusst ist, angewandt. Der Gewinn oder Verlust wird auf Grundlage verschiedener Ansätze zwischen allen beteiligten Parteien aufgeteilt. *Eigelshoven*, Artikel 9. Verbundene Unternehmen, in: Vogel/Lehner (Hrsg.), DBA, Rn. 87 f.; OECD Verrechnungspreisrichtlinien 2017, Rn. 2.114 ff.

188 „Transactional net margin method“. Der Verrechnungspreis wird auf Grundlage eines Vergleichs von Nettorenditen aus ähnlichen Transaktionen zwischen zwei unverbundenen Unternehmen ermittelt. *Eigelshoven*, Artikel 9. Verbundene Unternehmen, in: Vogel/Lehner (Hrsg.), DBA, Rn. 81 a ff.; OECD Verrechnungspreisrichtlinien 2017, Rn. 2.64 ff.

189 Bspw. könnte ein unbekanntes soziales Netzwerk über dieselben Algorithmen wie Facebook verfügen und würde trotzdem nicht annähernd vergleichbare Umsätze erzielen, weil es ggf. noch nicht vergleichbar viele Nutzer hat.

190 Es kann durchaus kritisiert werden, dass insbesondere die beiden Gewinnmethoden in der Natur ihrer Anwendung recht wenig mit dem eigentlich zugrunde liegenden Fremdvergleich zu tun haben.

Bei konzerninternen Verkäufen von Datensätzen etwa ist die Vergleichbarkeit mit dritten, unabhängigen Unternehmen noch seltener gegeben als bei anderen digitalen Gütern, wie etwa Musiktitel, denen zumindest tw. ein objektiver, vergleichbarer Wert beigemessen werden kann. Reine Datensätze sind ein offensichtliches Beispiel dafür, wie unterschiedlich ein Wert in Abhängigkeit des Verfügungsberechtigten sein kann. Der Wert von Datensätzen bestimmt sich oftmals erst durch eine Möglichkeit, diese auszuwerten, etwa durch Algorithmen. Dementsprechend unwahrscheinlich ist eine Anwendung der drei Standardmethoden zur Ermittlung von Verrechnungspreisen.

5.2.1.3 Zwischenfazit

Die Werterfassung digitaler Güter und Daten ist teilweise schwierig, jedoch findet grundsätzlich eine Ertragsbesteuerung statt. Als problematisch erachten einige Staaten, dass sich die Aufteilung der Steuerbemessungsgrundlage mangels Erfüllung des Betriebsstättenatbestands in vielen Situationen verschiebt, und somit die Verteilung des Gesamtsteueraufkommens. Die ursprüngliche Verteilung des weltweiten Steueraufkommens zwischen Quellen- und Ansässigkeitsstaaten gerate somit aus der Waage. Da vermehrt Ansässigkeitsstaaten ihr Besteuerungsrecht unter Artikel 7 (1) des OECD MA (in seiner jetzigen Fassung) ausüben dürfen, ist die effektive Steuerlast von Unternehmen relativ frei „wählbar“, indem sie einen steuerlich vorteilhaften Ansässigkeitsstaat wählen. Das ist in den seltensten Fällen der Staat, in dem die digitalen Dienstleistungen, die Erträge erzielen, angeboten werden.

5.2.2 Umsatzsteuerliche Werterfassung

Die USt ist i. d. R. eine vergleichsweise anpassungsfähige Steuer für verschiedene Geschäftsmodelle, da sie schlichtweg gezahlte Entgelte besteuert. Fragen der Gewinnaufteilung, also der Aufteilung der Bemessungsgrundlage zwischen verschiedenen Staaten, stellen sich nicht.

5.2.2.1 Digitale Güter

In der USt stellen sich bei der Wertermittlung weniger Probleme dar, sofern es sich um entgeltliche Transaktionen handelt. Dies ist etwa bei vielen digitalen Gütern der Fall. Fragen und Schwierigkeiten existieren vor allem im praktischen Vollzug und bei Tauschgeschäften, wie sie z. B. im Online-Gaming durchgeführt werden.

Im Vollzug sind Bestimmungsländer gänzlich auf die Bereitwilligkeit der Unternehmen, ihre Steuern selbstständig zu erklären, angewiesen. Tun diese das nicht, sind die Staaten auf Kooperation der Ansässigkeitsländer dieser Unternehmen angewiesen, da die Möglichkeiten, extraterritorial zu vollstrecken, beschränkt sind. Der deutsche Gesetzgeber reagierte mit dem Gesetz zur Vermeidung von Umsatzsteuerausfällen beim Handel mit Waren im Internet vom 11. Dezember 2018¹⁹¹ bereits darauf, indem er die Betreiber*innen von elektronischen Marktplätzen einerseits dazu verpflichtet, bestimmte relevante Umsätze und Daten ihrer Nutzer*innen vorzuhalten,¹⁹² und andererseits für Umsatzsteuerausfälle der auf den Marktplätzen handelnden Unternehmen haftbar macht.¹⁹³

Überdies änderte die Europäische Union die MwStSystRL durch Richtlinie 2017/2455, die neue Bagatellgrenzen für bestimmte Dienstleistungen und Vorschriften zur Rechnungsstellung einführt; mit dem Ziel, die USt verstärkt an den elektronischen Handel anzupassen und den Vollzug zu verbessern.¹⁹⁴

Tauschgeschäfte sind insofern problematisch, als dass sie nicht besteuert werden, während entgeltliche Geschäfte besteuert werden; obwohl sie oftmals ersetzbar sind. Eine Steuerumgehung ist somit vergleichsweise einfach. Selbst wenn man alle Tauschgeschäfte besteuern würde, würde sich wieder die Frage der Auswertung, ähnlich wie im Ertragsteuerrecht, stellen.

191 BGBl. I 2018, S. 2338 ff. Vgl. dazu: BMF, Schreiben vom 14. 12. 2018 – III C 3 – S 7117-j/18/10002, abrufbar unter: https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Steuerarten/Umsatzsteuer/Umsatzsteuer-Anwendungserlass/2018-12-14-umsetzung-des-MwSt-Digitalpakets-zum-1-Januar-2019.html.

192 § 22f UStG.

193 § 25e i. V. m. § 3a (5) UStG. S. auch: *Schmittmann/Sinnig*, K&R 2019, 88 (94 f.); *Schmittmann/Sinnig*, K&R 2020, 111 (116).

194 S. auch: *Schmittmann/Sinnig*, K&R 2019, 88 (92).

5.2.2.2 Daten

Bei Daten verschärfen sich die im Abschnitt 5.2.2.1 angesprochenen Probleme, da eine Vielzahl digitaler Dienstleistungen im Tausch gegen Nutzer*innendaten, anstatt gegen Gebühr, angeboten werden (etwa soziale Netzwerke).

Um hier Gerechtigkeit zwischen verschiedenen Geschäftsmodellen (Mitgliedsbeitrag und dafür keine Werbeanzeigen im Vergleich zu keinem Mitgliedsbeitrag und dafür Werbeanzeigen) herzustellen, wäre es zwingend notwendig, Tauschgeschäfte zu besteuern. In der Literatur wird diskutiert, ob derartige Tauschgeschäfte der Umsatzsteuer unterliegen.¹⁹⁵ Derzeit werden Transaktionen, bei denen Nutzer*innen mit ihren Daten „zu zahlen“ scheinen, nicht besteuert.¹⁹⁶

Die Wertermittlung der Datennutzungsrechte scheint in der Praxis zumindest möglich zu sein: Einzelne Autor*innen berufen sich auf „regelrechte Preiskataloge für Nutzer*inneninformationen“, die öffentlich zugänglich seien.¹⁹⁷

5.2.2.3 Zwischenfazit

Das Hauptproblem der USt ist in der digitalisierten Wirtschaft der Vollzug. Der deutsche sowie der europäische Gesetzgeber nahmen sich dieser Probleme in der jüngeren Vergangenheit bereits an.

Eine finale Lösung zur Besteuerung von Tauschgeschäften, die ursprünglich vernachlässigbar schienen, heute jedoch zunehmend an Wichtigkeit gewinnen, ist noch nicht gefunden.¹⁹⁸ Eine Wertermittlung ist hier noch schwieriger als im Falle der Ertragsteuer, da der Wert aus Sicht des Leistungsempfängers, also des Nutzers, ermittelt werden müsste.

195 Bejahend: *Melan/Wecke*, DStR 2015, 2267 und 2811; *Pfeiffer*, International VAT Monitor 2016, 158; *Melan/Pfeiffer*, DStR 2017, 1072; ablehnend: *Grambeck*, DStR 2016, 2026; *Looks/Bergau*, MwStR 2016, 964.

196 *Grambeck*, DStR 2016, 2026; *Melan/Pfeiffer*, DStR 2017, 1072.

197 *Melan/Wecke*, DStR 2015, 2267 (2269). Fraglich ist natürlich, auf welcher Grundlage diese Werte geschätzt werden, insbesondere vor dem Hintergrund, dass die erwähnten Werte nicht bilanziell ermittelt werden.

198 *Grambeck*, DStR 2016, 2026 (2032); *Melan/Pfeiffer*, DStR 2017, 1072 (1077 f.).

5.3 Steuerbare Wertschöpfung durch Daten?!

Neben der Frage der Wertbestimmung digitaler Güter und Daten als solche beschäftigt die Steuerpolitik noch eine andere, globale Frage; nämlich die des adäquaten Ortes zur Besteuerung von Werten, die durch digitale Güter, aber insbesondere Daten, geschaffen werden.¹⁹⁹ Dogmatischer Kern der Diskussion ist die Annahme, dass digitale Güter in der Tat „anders“ als materielle Güter sind, und somit eine Anpassung des Steuersystems erfordern. Politisch handelt es sich um den Willen, Konzerne stärker zu besteuern.

Motiviert ist dieses Ziel durch mehrere Aspekte. Zum einen wird die Konzernbesteuerung durch den Wähler gerade im Rahmen rezenter Entwicklungen (z. B. Beihilfeermittlungen seitens der Europäischen Kommission zu bestimmten Steueroptimierungsmodellen²⁰⁰) und Enthüllungen (z. B. „Panama Papers“, „LuxLeaks“, „SwissLeaks“, etc.) kritisch hinterfragt. Solch kritische Hinterfragung fordert den um Wähler*innenstimmen bemühten Politiker zwangsläufig zum Handeln auf. Resultat ist eine anhängige Diskussion zur Neu- bzw. Umverteilung des Weltsteueraufkommens, was sich juristisch in Fragen zu Jurisdiktionsvorschriften niederschlägt. Zum anderen hat sich die wirtschaftliche Realität tatsächlich spürbar verändert: Während früher der Kunde eines Unternehmens „lediglich“ Empfänger von Gütern oder Dienstleistungen war, so ist er heute aktiver Bestandteil vieler Geschäftsmodelle und ihrer Wertschöpfungskette. Viele digitale Geschäftsmodelle würden ohne die aktive Partizipation des Kunden, der heute „Nutzer“ anstatt „Empfänger“ ist, schlichtweg nicht funktionieren. Dementsprechend rechtfertigen sich durchaus die Frage danach, ob es eine gewichtige Wertschöpfung durch

199 Die nachfolgende Darstellung der steuerpolitischen Debatte spiegelt den Stand Mitte 2019 wider. Für einen Überblick aller aktuellen Entwicklungen (Stand: September 2020), s. *Sinnig*, Update internationales und europäisches Steuerrecht, in: Taeger (Hrsg.), Den Wandel begleiten – IT-rechtliche Herausforderungen der Digitalisierung, 2020, 1055. S. demnächst auch: *Sinnig*, Internationales und Europäisches Steuerrecht, in: Taeger/Pohle/Kilian/Heussen (Hrsg.), Computerrechts-Handbuch – Informationstechnologie in der Rechts- und Wirtschaftspraxis, 34. Aufl. 2018, Erscheinung im Druck.

200 S. z. B.: Europäische Kommission, Entscheidung SA.38375 v. 9. Juni 2016 – Luxemburg/Fiat (Verfahren anhängig, Rs. T-755/15 u. T-759/15); Entscheidung SA.38373 v. 30. August 2016 – Irland/Apple (Verfahren anhängig, Rs. T-778/16, T-892/16 u. C-12/18, C-678/17); Entscheidung SA.38374 v. 21. Oktober 2015 – Niederlande/Starbucks (Verfahren anhängig, Rs. T-760/15, T-636/16 u. T-877/16).

ebensolche Nutzer gibt, die in der Ertragbesteuerung von Unternehmen widergespiegelt werden sollte.

Hauptforum dieser Diskussion ist auf internationaler Ebene das OECD „Base Erosion and Profit Shifting“ (BEPS) Projekt, das 2012 ins Leben gerufen wurde und in 15 Aktionspunkte aufgeteilt ist, die verschiedene Steuerplanungs- bzw. -optimierungspraktiken durch Änderungen der anwendbaren Vorschriften unterbinden sollen. Steuerrechtliche Herausforderungen der digitalisierten Wirtschaft werden im ersten Aktionspunkt²⁰¹ behandelt. Während einige der Aktionspunkte bereits zu Resultaten führten, die durch ein mehrseitiges Übereinkommen²⁰² das bestehende Regelwerk modifizieren, sind die (politischen und technischen) Verhandlungen zu Aktionspunkt 1 noch anhängig.

Grundlegend gibt es hierzu vor allem zwei Anmerkungen hervorzu-
bringen: Einerseits wird das Konzept der „Wertschöpfung“ im Rah-

201 OECD, Action 1: Tax Challenges Arising from Digitalisation, Informationen abrufbar unter: <https://www.oecd.org/tax/beps/beps-actions/action1/>. Im Rahmen dieses Aktionspunktes wurde 2015 ein erster Bericht und 2018 ein weiterer Zwischenbericht veröffentlicht. Im Jahr 2019 wurde eine „Policy Note“ veröffentlicht, zwei Öffentlichkeitsbeteiligungsverfahren geführt und ein Arbeitsprogramm vorgestellt. S. in der Reihenfolge: OECD, Addressing the Tax Challenges of the Digital Economy, Action 1 – 2015 Final Report, 5. Oktober 2015, abrufbar unter: https://read.oecd-ilibrary.org/taxation/addressing-the-tax-challenges-of-the-digital-economy-action-1-2015-final-report_9789264241046-en#page1; OECD, Tax Challenges Arising from Digitalisation – Interim Report 2018, 16. März 2018, abrufbar unter: https://read.oecd-ilibrary.org/taxation/tax-challenges-arising-from-digitalisation-interim-report_9789264293083-en#page1; OECD, Addressing the Tax Challenges of the Digitalisation of the Economy – Policy Note, 23. Januar 2019, abrufbar unter: <https://www.oecd.org/tax/beps/policy-note-beps-inclusive-framework-addressing-tax-challenges-digitalisation.pdf>; OECD, Public Consultation Document: Addressing the Tax Challenges of the Digitalisation of the Economy, 13. Februar 2019, abrufbar unter: <https://www.oecd.org/tax/beps/public-consultation-document-addressing-the-tax-challenges-of-the-digitalisation-of-the-economy.pdf>; OECD, Programme of Work, 29. Mai 2019; OECD, Public Consultation Document: Secretariat Proposal for a „Unified Approach“ under Pillar One – 9 October – 12 November 2019, 9. Oktober 2019, abrufbar unter: <https://www.oecd.org/tax/beps/public-consultation-document-secretariat-proposal-unified-approach-pillar-one.pdf>. Anfang 2020 wurde darüber hinaus ein „Statement“ veröffentlicht: OECD, Statement by the OECD/G20 Inclusive Framework on BEPS on the Two-Pillar Approach to Address the Tax Challenges Arising from the Digitalisation of the Economy, 31. Januar 2020, abrufbar unter <https://www.oecd.org/tax/beps/statement-by-the-oecd-g20-inclusive-framework-on-beps.htm>. Im Fortschrittsbericht der OECD von Mitte 2020 wird das Ziel, einen konkreten Lösungsvorschlag noch 2020 zu präsentieren, erneut bestätigt: OECD, OECD/G20 Inclusive Framework on BEPS – Progress report July 2019 – July 2020, 18. Juli 2020, S. 4.

202 OECD, Multilateral Convention to Implement Tax Treaty Related Measures to Prevent Base Erosion and Profit Shifting (MLI), Text des Übereinkommens und Erläuterungen abrufbar unter: <https://www.oecd.org/tax/treaties/multilateral-convention-to-implement-tax-treaty-related-measures-to-prevent-beps.htm>.

men dieser Gespräche kurz kritisch beleuchtet, und andererseits werden mögliche zukünftige steuerliche Anknüpfungspunkte zusammengefasst vorgetragen.

5.3.1 Digitale „Wertschöpfung“ im Ertragsteuerrecht

Das Prinzip der „Wertschöpfung“ (engl.: „value creation“) scheint in der Diskussion um die ertragsteuerrechtliche Behandlung digitaler Geschäftsmodelle fest verankert, obwohl es als grundlegendes Besteuerungsprinzip neu ist.²⁰³

„Wertschöpfung“ beschreibt, dass digitale Geschäftsmodelle laut der politischen Diskussion am Ort der Nutzer*innen einen wichtigen Faktor in der Produktions- bzw. Wertschöpfungskette verorten. Ort der Wertschöpfung sei dementsprechend der Aufenthaltsort der Nutzer*innen, wobei hier weniger auf seine Ansässigkeit, als auf seinen tatsächlichen Aufenthaltsort im Moment der Dienstleistungserbringung abgestellt wird.²⁰⁴ Wert für das digitalisierte Unternehmen schöpft der Nutzer durch Preisgabe seiner persönlichen Daten, seine Online Aktivität und sein Konsumverhalten, die von sozialen Netzwerken und Plattformen abgeschöpft und analysiert werden.

Kritisiert wird vor allem seitens vieler Staaten, dass an anderen als dem Ansässigkeitsort vieler Unternehmen „Werte geschöpft“ werden, die durch das „Betriebsstättenraster“ fallen und somit lediglich im Ansässigkeitsstaat des Unternehmens besteuert werden. Darüber hinaus wird in der Rechtslehre die Vagheit des Begriffs kritisiert,²⁰⁵ insbesondere weil

203 Hinterfragt wird vor allem, ob dieses Prinzip tatsächlich ein grundlegendes Prinzip der internationalen Steuerrechtsordnung ist, oder ob versucht wird, es als Rechtfertigung des politischen Vorstoßes einzuführen. So z. B.: *Olbert/Spengel*, World Tax Journal 2017, 3 (5, 12); *Schön*, Bulletin for International Taxation 2018, 278 (280); *Hey*, Bulletin for International Taxation 2018, 203 (203 ff.).

204 Dies zeigen diverse Vorschläge zu Digitalsteuern bzw. sog. „GAFA Steuern“, wie z. B. die französische „taxes sur les services numériques“ (s. insb. Art. 299 bis.-I.2° u. Art. 299 bis.-III. *Code général des impôts*) oder die europäische oder britische „digital services tax“ (HM Treasury, Budget 2018 – Digital Services Tax, abrufbar unter: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752172/DST_web.pdf; Art. 5 des RL-Entwurfs COM(2018) 148 v. 21. März 2018 zu einer europäischen Digitalsteuer).

205 S. *Hey*, Bulletin for International Taxation 2018, 203 (203); *Olbert/Spengel*, World Tax Journal 2017, 3 (16); *Schön*, Bulletin for International Taxation 2018, 278 (288).

es im Ertragsteuerrecht weniger um die Besteuerung der Schaffung eines (Mehr-)Werts, als vielmehr um die von Nettoerträgen geht.

5.3.2 OECD Public Consultation Document/Programme of Work 2019; Statement 2020: Vorschläge zu „nicht-physischen“ Steueranknüpfungspunkten

Während auf Ebene der EU zwei Lösungsvorschläge im März 2018 von der Europäischen Kommission hervorgebracht wurden,²⁰⁶ die im Rat jedoch nicht standhielten, nehmen die Diskussionen auf Ebene der OECD Form an. Die Vorgehensweise zur Besteuerung digitalisierter Unternehmen und ihrer „Wertschöpfung“ durch Nutzer*innendaten und -beteiligung wurde in zwei Säulen aufgeteilt: eine Anpassung der Steueranknüpfungspunkte und Gewinnverteilungsregeln (engl.: „revised nexus and profit attribution rules“) sowie eine Art Minimalbesteuerung, die sich aus zwei Maßnahmen zusammensetzt (engl.: „global anti-base erosion proposal“). Im nachfolgenden Abschnitt werden die neuen Steueranknüpfungspunkte der ersten Säule umrissen.

Inhaltlich soll jeder neue mögliche Anknüpfungspunkt auf anhaltenden lokalen Umsatz und andere Faktoren, die eine Verbindung zwischen dem im jeweiligen Staat erwirtschafteten Umsatz und der Geschäftsaktivität aufweist, die über den reinen Verkauf hinausgeht, abstellen. Solche Faktoren können entweder eine gewisse Anzahl von aktiven Nutzer*innen²⁰⁷ in dem jeweiligen Marktstaat, sog. „Marketing Intangibles“²⁰⁸ oder eine signifikante digitale oder wirtschaftliche Präsenz²⁰⁹ sein. Letzterer Vorschlag stellt auf eine Reihe von Merkmalen ab, wie z. B. die Bereit-

206 Europäische Kommission, Vorschlag für eine Richtlinie des Rates zur Festlegung von Vorschriften für die Unternehmensbesteuerung einer signifikanten digitalen Präsenz, 21. März 2018, COM(2018) 147; Europäische Kommission, Vorschlag für eine Richtlinie des Rates zum gemeinsamen System einer Digitalsteuer auf Erträge aus der Erbringung bestimmter digitaler Dienstleistungen, 21. März 2018, COM(2018) 148.

207 Sog. „user participation proposal“, s. OECD, Public Consultation Document, 2019, Rn. 17 ff.

208 Sog. „marketing intangibles proposal“. Als „marketing intangibles“ bezeichnet die OECD Marktdaten, aber auch die Wahrnehmung bzw. Reputation einer Marke in einem bestimmten Staat. OECD, Public Consultation Document, 2019, Rn. 29 ff.

209 Sog. „significant economic presence proposal“, das erst kurz vor Fertigstellung des Public Consultation Dokuments Einzug in ebendieses erhielt. OECD, Public Consultation Document, 2019, Rn. 50 ff.

stellung einer Webseite des Unternehmens in lokaler Sprache und Währung.²¹⁰

Zur Debatte steht 2019 noch die Implementierung dieser angepassten Regeln durch eine Ausweitung des Betriebsstättenkonzepts (Artikel 5 und 7 des OECD MA) oder durch eine gänzlich neue Vorschrift, die neben dem Betriebsstättenkonzept existieren soll.²¹¹

Im Jahr 2020 kristallisiert sich ein umfassender „Unified Approach“ heraus, der nicht nur digitalisierte, sondern auch andere Geschäftsmodelle betreffen sollte.²¹² Dies resultiert aus der Feststellung, dass das Problem digitalisierter Geschäftsmodelle, die keine physische Präsenz mehr in der Nähe ihrer Kund*innen benötigen, um ihre Dienstleistungen zu erbringen, durchaus auch auf andere kundenorientierte Geschäftsmodelle anwendbar ist.²¹³

Dieser neue steuerliche Anknüpfungspunkt umfasst demnach Unternehmen zweier Kategorien: automatisierte digitale Dienstleistungen und verbraucherorientierte („Consumer-Facing“) Unternehmen. Zur ersten Kategorie zählen unter anderem Online-Suchmaschinen, soziale Netzwerke, Online-Vermittlungsplattformen und -Marktplätze (hier auch B2B-Geschäfte), Streaming-Dienstleister, Cloud Computing Dienstleistungen und Online Werbedienstleistungen; also automatisierte digitale Dienstleistungen, die standardisiert einer großen Anzahl von Kund*innen und Nutzer*innen in verschiedenen Ländern angeboten werden.²¹⁴ Zur zweiten Kategorie zählen Unternehmen, die Güter und Dienstleistungen anbieten, die üblicherweise Endverbraucher*innen zu

210 Ebenda, Rn. 51.

211 OECD, Programme of Work, Rn. 40 und Box 2.1.

212 OECD, Statement by the OECD/G20 Inclusive Framework on BEPS on the Two-Pillar Approach to Address the Tax Challenges Arising from the Digitalisation of the Economy, 31. Januar 2020, Rn. 21–29.

213 OECD, Public Consultation Document 2, Rn. 22–23; OECD, Statement by the OECD/G20 Inclusive Framework on BEPS on the Two-Pillar Approach to Address the Tax Challenges Arising from the Digitalisation of the Economy, 31. Januar 2020, Rn. 18–20. Darüber hinaus ist eine Steuer, die spezifisch auf bestimmte Geschäftsmodelle abstellt, auch nicht besonders anpassungsfähig, was angesichts der rapiden Weiterentwicklung im digitalisierten Zeitalter zunehmend problematisch erscheint. Eine Abgrenzung betroffener digitalisierter Geschäftsmodelle und nicht betroffener Modelle erscheint schwierig. Fraglich ist, ob diese Abgrenzung im Falle der weitreichenderen Definition „kundenorientierter“ Geschäftsmodelle tatsächlich einfacher und erfolgreicher durchgeführt werden kann.

214 OECD, Statement by the OECD/G20 Inclusive Framework on BEPS on the Two-Pillar Approach to Address the Tax Challenges Arising from the Digitalisation of the Economy, 31. Januar 2020, Rn. 22: „These services will cover businesses that generate revenue from

persönlichen Nutzungszwecken verkauft werden, wie z.B. Kleidung, Kosmetik, Luxusgüter, Lebensmittel oder Kraftfahrzeuge.²¹⁵

5.4 Fazit und Ausblick

Abschließend ist jedenfalls festzuhalten, dass die Ausmaße der Debatte zu Beginn eindeutig verkannt wurden; jedoch mittlerweile erkannt und bearbeitet werden. Zur Frage dieses Beitrags, wie sich der Wert digitaler Güter und Daten im Steuerrecht abzeichnet, ist folgendes festzuhalten:

- Das Ertragsteuerrecht beruht zur Wertermittlung digitaler Güter und Daten in bestimmten, jedoch essentiellen, Situationen auf dem Fremdvergleichsgrundsatz, der bei unvergleichbaren Transaktionen an seine Grenzen stößt. Die Anwendung dieses Grundsatzes, sowohl im Rahmen der Gewinnaufteilung zwischen einzelnen Konzerngesellschaften, als auch zwischen Betriebsstätte und Stammhaus, fordert traditionelle Verrechnungspreismethoden heraus. Neue und einfache Lösungen zur Wertermittlung digitaler Güter und Daten sollten ausgearbeitet werden.
- „Wertschöpfung“ scheint grundlegend für die politische Findung einer neuen ertragsteuerlichen Nexusregel zu sein, auch wenn das Konzept juristisch nicht in der internationalen Steuerrechtsordnung verwurzelt ist. Der Anknüpfungspunkt im Produktionsstaat, den das Betriebsstättenkonzept umsetzt, scheint sich in Richtung des Marktstaats zu verschieben. Auf welche Art bestehende Vorschriften angepasst werden (sollten), um diese Verschiebung umzusetzen, steht noch offen.
- Umsatzsteuerrechtlich lassen sich Werte i. d. R. relativ einfach bestimmen, da das für eine Dienstleistung erbrachte Entgelt die steuerrechtliche Bemessungsgrundlage bildet. Problematisch ist bei elektronischen Dienstleistungen, bzw. dem Handel mit digitalen Gütern, oftmals der Vollzug. Der Gesetzgeber reagierte auf diese Problematik Ende 2018.

the provision of automated digital services that are provided on a standardised basis to a large population of customers or users across multiple jurisdictions“.

215 OECD, Statement by the OECD/G20 Inclusive Framework on BEPS on the Two-Pillar Approach to Address the Tax Challenges Arising from the Digitalisation of the Economy, 31. Januar 2020, Rn. 24–28.

- Die Bewertung von Tauschgeschäften in der Umsatzsteuer erfordert jedoch eine klare, dogmatische Lösung, um Ungleichbehandlung zwischen vergleichbaren Transaktionen zu vermeiden.

6 DER WERT DIGITALER GÜTER – ÖKONOMISCHE BETRACHTUNG

*Aline Blankertz*²¹⁶

*Dieser Beitrag gibt einen kurzen Überblick über den Wert von Daten aus zwei Perspektiven, der von Verbraucher*innen und der von Unternehmen. Nach einem kurzen Überblick über die ökonomischen Eigenschaften von Daten werden empirische Studien zur Verbraucher*innensicht auf den Wert von Daten – in Form von datengetriebenen Diensten und Datenschutz – beschrieben: Dass der Wert für Verbraucher*innen stark variiert, hängt einerseits vom Kontext der Daten und digitalen Dienste ab, andererseits aber auch von den unterschiedlichen (und unterschiedlich zuverlässigen) Methoden, über die der Wert erhoben und gemessen wird. Im Anschluss werden Werttreiber von Daten aus Unternehmensperspektive dargestellt: Die Langlebigkeit und der Zugang zu Daten in der Erhebung sind wesentliche Faktoren dafür, welche Wirkungen Daten auf den Wettbewerb haben und ob Datenmärkte entstehen können.*

6.1 Einleitung

Daten sind ein zunehmend wichtiger und wertvoller Teilbereich der Wirtschaft, dem man sich mit einer Vielzahl an Metaphern zu nähern versucht: Seien es Daten als Öl, das neue Geschäftsmodelle befeuert, Daten als Grundwasser, das von vielen Diensten zugleich genutzt werden kann, Daten als Währung, die Nutzer*innen mit Unternehmen im Austausch für Dienste geben, oder Daten als Schienen, die einen unersetzlichen Input für nachfolgende Wertschöpfungsstufen darstellen. Zugleich wird vielfach diskutiert, welche zusätzlichen Regeln Märkte möglicherweise brauchen, um datenbasierten Wettbewerb und Innovation sicherzustellen.

Für diese Diskussion ist es wichtig, den Wert von Daten und den auf ihnen basierenden Diensten angemessen zu erfassen. So kann die Debatte auf Evidenz basieren und berücksichtigen, welche Faktoren den Wert

²¹⁶ Mehr über die Autorin erfahren Sie im Autor*innenhinweis auf S. 107.

von Daten treiben, damit mögliche Eingriffe diesen Wert weitestgehend erhalten bzw. eine breitere Wertschöpfung ermöglichen.

6.2 Eigenschaften von Daten

Daten sind eine Form von digitalen Gütern und somit in vielerlei Hinsicht grundlegend anders als materielle Güter: Sie sind nicht physisch knapp, d.h. sie können ohne bzw. mit minimalen Kosten beliebig oft vervielfacht und nutzbar gemacht werden. Ökonom*innen nennen dies Nicht-Rivalität, die besagt, dass Daten mehrfach genutzt werden können, ohne dass sie abgenutzt oder aufgebraucht würden. Dies widerspricht den meisten o.g. Daten-Metaphern. In der praktischen Umsetzung werden Daten allerdings meist von einer datensammelnden Instanz, oft Unternehmen, erfasst und ihre Nutzung durch andere wird unterbunden. Dies verhindert, dass Daten ihr volles Potenzial entfalten, und motiviert Debatten über mögliche Markteingriffe, um breiteren Zugang zu Daten zu ermöglichen.

Das Sammeln von Daten erfolgt oftmals auf Märkten, die sich durch Mehrseitigkeit und starke Netzwerkeffekte auszeichnen. Dadurch finden für Daten üblicherweise keine Zahlungen statt, sondern das Sammeln von Daten wird durch Aktivitäten auf der anderen Marktseite subventioniert wie der Bereitstellung von beispielsweise sozialen Netzwerken oder Suchdiensten. Netzwerkeffekte bedeuten, dass mit Hilfe von Daten verbesserte Dienste es erleichtern können, noch mehr Daten zu sammeln. Damit einher gehen oft deutliche Skalenerträge: Die Fixkosten für den Aufbau einer Datensammlung sind hoch, da Dienste zur Datenerfassung und entsprechende Infrastruktur aufgebaut werden müssen. Die Kosten zusätzlicher Datenpunkte sind dafür meist sehr niedrig. Diese Faktoren können zu einer erheblichen Konzentration großer Datensets bei wenigen Unternehmen führen.

Eine besondere Untergruppe von Daten sind personenbezogene Daten. Diese zeichnen sich dadurch aus, dass sie zwar ebenfalls nicht physisch knapp sind, ihre Nutzung jedoch negative Externalitäten für die Person, auf die sie sich beziehen, verursachen kann. Diese können sich artikulieren in Form einer Verringerung der Privatsphäre, aber auch in Form ungewollter Personalisierung wie z. B. personalisierte höhere Preise oder

das Ausnutzen von persönlichen Entscheidungsschwächen. Im Rahmen der Datenschutzgrundverordnung haben Personen Einfluss darauf, welche Daten über sie genutzt werden dürfen, jedoch kann die Analyse von Daten aufgrund von Korrelation auch Aufschluss über Personen geben, die die Nutzung dieser Daten verhindern wollen.²¹⁷

6.3 Der Wert datenbasierter Dienste für Verbraucher*innen

Der Wert von Daten für Verbraucher*innen bemisst sich in erster Linie darüber, wozu die Daten genutzt werden bzw. auch, wozu sie nicht genutzt werden, insbesondere wenn sich die Nutzung negativ auswirken kann. Verbraucher*innen messen vielen datengetriebenen Diensten einen hohen Wert bei. Studien haben ermittelt, dass beispielsweise der Wert von Facebook für US-amerikanische Studierende in den Jahren 2018/2019 zwischen 42 und 160 USD pro Monat lag, siehe Tabelle 1.

Tabelle 1 Monatlicher Nutzen von Facebook pro Nutzer*in

Nutzen pro Monat (Median)	Land	Studie ²¹⁸
42 USD	USA	Brynjolfsson et al. 2018
97 USD	USA	Brynjolfsson et al. 2018 ¹
160 USD	USA	Corrigan et al. 2019 ²
100 USD	USA	Allcott et al. 2019

Anmerkungen: ¹ niedrigeres Durchschnittsalter der Stichprobe, ² extrapoliert von wöchentlichem Nutzen (Monat = 4 Wochen)

Diese Werte sind hoch, auch im Verhältnis zu den Werbeeinnahmen, die Facebook für 2018 mit durchschnittlich 6 USD pro Nutzer und Jahr angab (28 USD für Nutzer*innen in den USA und Kanada). Andere Dienste

217 Acemoglu, Makhdoumi, Malekian, Ozdaglar, “Too much data: prices and inefficiencies in data markets”, NBER Working Paper No. 26296, 2019.

218 Vollständige Referenzen: Corrigan, Alhabash, Rousu, Cash, 2018, How much is social media worth? Estimating the value of Facebook by paying users to stop using it, PloS one 13 (12):e0207101; Allcott, Braghieri, Eichmeyer, Gentzkow, 2019, The Welfare Effects of Social Media (No. w25514), National Bureau of Economic Research; Brynjolfsson, Collis, Diewert, Eggers, Fox, 2018, The Digital Economy, GDP and Consumer Welfare: Theory and Evidence; Brynjolfsson, Eggers, Gannamaneni, 2018, Measuring Welfare with Massive Online Choice Experiments: A Brief Introduction.

generieren ebenfalls einen erheblichen Wert für Verbraucher*innen, wie z. B. Google Maps (59 USD pro Nutzer*in und Monat) und Wikipedia (12,50 USD).²¹⁹ Allerdings können sich Nutzungsmuster und damit der Wert für Nutzer*innen schnell ändern, sodass nur begrenzt über die Zeit extrapoliert werden kann.

Verbraucher*innen messen auch der Nichtnutzung von Daten für bestimmte Zwecke, also dem Datenschutz, einen Wert bei. Beispielsweise haben verschiedene vom Datenschutz abgeleiteter Rechte einen Wert, der je nach Produkt variiert: Verbraucher*innen artikulieren eine deutlich positive Zahlungsbereitschaft dafür, dass Unternehmen bei einem Datenschutzverstoß hohe Strafen zahlen. Diese liegt zwischen 5 GBP für Daten über Stromverbrauch und 8 GBP für Krankenkassendaten.²²⁰ Für das Recht auf Portabilität liegt die Zahlungsbereitschaft nur bei Treuekarten über einem GBP. Verbraucher*innen artikulieren ebenfalls eine Bereitschaft, für mehr Privatsphäre in Apps zu zahlen: Die Unterbindung der Übermittlung des Standorts ist Verbraucher*innen etwa einen USD wert, ihrer Kontaktliste etwa 4 USD.²²¹ Allerdings ist fraglich, inwieweit diese Werte belastbar sind in Anbetracht der Tatsache, dass Verbraucher*innen selten tatsächlich für Apps zahlen.

6.3.1 Exkurs: Methoden zur Wertbestimmung aus Verbraucher*innensicht

Es ist eine Herausforderung für Ökonom*innen, den Wert von Daten für Verbraucher*innen zu bestimmen, denn die meisten Dienste werden zu einem Preis von Null angeboten. Es gibt einige Methoden, um sich dem Wert zu nähern. Grob zu unterscheiden ist zwischen Experimenten und Umfragen, wobei erstere prinzipiell belastbarer sind, da sie tatsächliches Verhalten testen. Letztere haben den Vorteil, dass sie schneller und einfacher durchzuführen sind.

Experimente zur Ermittlung des Werts digitaler Güter sind anspruchsvoll in der Durchführung und können erhebliche Kosten verursachen.

219 Brynjolfsson, Collis, Diewert, Eggers, Fox, 2018, The Digital Economy, GDP and Consumer Welfare: Theory and Evidence.

220 London Economics, 2017, The business benefits of improved trust via the GDPR.

221 Savage, Waldman, 2014, The Value of Online Privacy: Evidence from Smartphone Applications.

Beispielsweise können Verbraucher*innen ein Angebot erhalten, für die Zahlung eines Betrages einen Dienst für eine bestimmte Zeit nicht zu nutzen. Wenn sie das Angebot ablehnen, ist davon auszugehen, dass sie dem Dienst einen höheren Wert beimessen. Wenn sie es annehmen, liegt der Wert darunter – allerdings ist dann auch der angebotene Betrag an die Teilnehmenden zu zahlen. Eine Möglichkeit, die Kosten eines Experimentes zu senken, ist die Nutzung einer Lotterie, die erst nach der Durchführung ermittelt, welche Zahlungen tatsächlich durchgeführt werden. Die Überprüfung, ob die Absprache wie die Nichtnutzung eingehalten werden, macht das Ergebnis des Experiments ebenfalls zuverlässiger. Allerdings reagieren Teilnehmende auch darauf, dass sie wissen, dass bestimmte Aspekte ihres Verhaltens untersucht werden. Daher ist es besonders elegant, wenn die eigentliche Absicht des Experiments verborgen werden kann.²²²

Die Aussagekraft von Umfragen über den Wert von datengetriebenen Diensten variiert erheblich. Manche Umfragen erheben Aussagen zur Zahlungsbereitschaft für Dienste, indem sie fragen, welchen Betrag Teilnehmende für die Nutzung eines Dienstes für einen Zeitraum bereit sind zu zahlen. Dies ist problematisch, da ein Großteil der Dienste entgeltfrei verfügbar sind und dies Verbraucher*innen als „mentaler Anker“ dient. Alternativ können Umfragen die „Verlustbereitschaft“ testen, also in welcher Höhe Teilnehmende entschädigt werden wollten, um einen Dienst für einen Zeitraum nicht zu nutzen. Allerdings ist zu beachten, dass die Verlustbereitschaft üblicherweise knapp drei Mal höher ist als die Zahlungsbereitschaft,²²³ d.h. Menschen messen Dingen, die sie haben, einen systematisch höheren Wert zu als den, den sie bereit sind zu zahlen.

Um den Wert von Datenschutz zu bestimmen, ist er am besten als eine Produkteigenschaft zu verstehen. Den Wert solcher Eigenschaften lässt sich ebenfalls mit Experimenten, doch oft einfacher mit Umfragen ermitteln. In solchen Umfragen geben Teilnehmende an, welches von zwei bis drei Produkten sie vorziehen. Die Produkte werden durch verschiedene Eigenschaften charakterisiert, deren Ausprägungen variieren. Bei-

222 Siehe beispielsweise *Acquisti, John, Loewenstein*, 2013, What is privacy worth?, *Journal of Legal Studies*, 42:2, S. 249–74; hier findet das eigentliche Experiment im Rahmen der Entschädigung für die Teilnahme an einer Umfrage statt.

223 *Horowitz, McConnell*, 2002, A Review of WTA/WTP Studies, *Journal of Environmental Economics and Management* 44, S. 426–447.

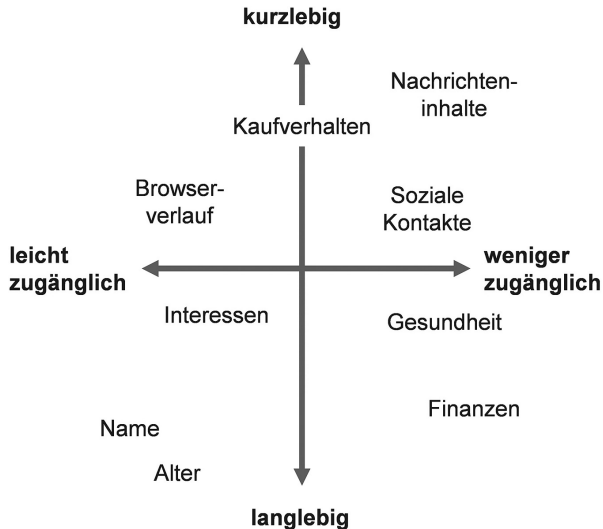
spielsweise können Teilnehmende auswählen zwischen verschiedenen Karten-Apps, die sich in Bezug auf ihren Preis, ihre Präzision und ihre Tracking-Optionen unterscheiden. Durch wiederholte Auswahl zwischen Produkten, die unterschiedliche Kombinationen aus Preis, Präzision und Tracking anbieten, kann auf die Zahlungsbereitschaft für weniger Tracking geschlossen werden.

Alle der o.g. Methoden zur Bestimmung des Werts von Daten für Verbraucher*innen haben bestimmte Schwachpunkte, sodass die Wahl der Methode in Abhängigkeit der konkreten Fragestellung erfolgen sollte. Es ist wichtig, die Ergebnisse im Zusammenhang mit der jeweiligen Methode zu interpretieren und beispielsweise Zahlungsbereitschaft und Verlustbereitschaft klar voneinander zu unterscheiden. Prinzipiell gilt, dass der Einsatz verschiedener Ansätze hilft, Ergebnisse zu validieren.

6.4 Der Wert von Daten für Unternehmen

Auch für Unternehmen gilt, dass der Wert von Daten nicht intrinsisch ist, sondern sich erst durch die Nutzungsmöglichkeiten ergibt. Dennoch gibt es Eigenschaften von Daten, die einen Einfluss darauf haben, wie wertvoll sie für das sammelnde Unternehmen sind. Ein wichtiger Aspekt ist die Replizierbarkeit von Daten: Leicht zu replizierende Daten sind tendenziell weniger wertvoll für das einzelne Unternehmen, da ihre Nutzung mit geringerer Wahrscheinlichkeit zu einem Wettbewerbsvorteil führt. Replizierbarkeit wiederum ist oft mit zwei anderen Faktoren verknüpft, nämlich der Langlebigkeit und die Zugänglichkeit, siehe Abbildung 1.

Abbildung 1 Eigenschaften ausgewählter persönlicher Datenpunkte



Quelle: Oxera (2018), „Consumer data in online markets“, Bericht für Which?

Langlebige Daten wie z. B. ein Geburtsdatum sind prinzipiell leichter replizierbar, da sie über einen längeren Zeitraum erhoben werden können. Gleiches gilt für einfacher zugängliche Daten wie z. B. Browserverläufe, die meist von mehreren Cookies parallel erfasst werden.

Einige Vorschläge zielen aktuell darauf ab, Datenzugang zu erzwingen, darunter der Entwurf zur 10. GWB-Novelle²²⁴ und der SPD-Vorstoß zu Daten für alle.²²⁵ Verpflichtender Zugang wirft allerdings viele Probleme in der Ausgestaltung auf, sodass freiwillige Lösungen oder eine Stärkung der Anreize vorzuziehen sind. Zugangspflichten sind am ehesten dann eine angemessene Lösung, wenn Anreize nicht ausreichen und die Daten hinreichend schlecht replizierbar sind (z. B. aufgrund von Kurzlebigkeit oder schlechter Zugänglichkeit).

²²⁴ Bundesministerium für Wirtschaft und Energie (2020), „Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer wettbewerbsrechtlicher Bestimmungen (GWB-Digitalisierungsgesetz)“.

²²⁵ SPD, Digitaler Fortschritt durch ein Daten-für-alle-Gesetz, Diskussionspapier der Parteivorsitzenden der Sozialdemokratischen Partei Deutschlands Andrea Nahles, abrufbar unter https://www.spd.de/fileadmin/Dokumente/Sonstiges/Daten_fuer_Alle.pdf.

Anreize für einen stärkeren Austausch von Daten und einer besseren Nutzung ihres Wertes lassen sich am besten in einem Marktkontext setzen: Unternehmen sind eher dann bereit, Daten zu teilen, wenn sie dafür eine entsprechende Gegenleistung erhalten. Dies kann am besten auf Datenmärkten geschehen, auf denen Transaktionen stattfinden, wenn der Wert der Daten für den Kaufenden über dem Wertverlust für den Teilenden liegt. Dieser Wertverlust kann sich daraus ergeben, dass das datenteilende Unternehmen nicht mehr allein über die Daten verfügt, sondern mit anderen Unternehmen – möglicherweise Wettbewerber*in oder Anbieter*in in vor- oder nachgelagerten Märkten – in der Datennutzung konkurriert. Allerdings kann dieser Wertverlust aufgrund der Nichtrivalität von Daten auch sehr niedrig sein. Datenmärkte befinden sich noch stark in der Entwicklung: Während Datenaustausch im Zusammenhang mit personalisierter Werbung bereits stark standardisiert und monetarisiert ist, lernen Unternehmen in vielen anderen Bereichen noch, wie hoch angemessene Preise sind und in welchem Format sie am besten geteilt werden. Beispiele sind die Mobilitätsbranche mit bspw. Caruso Dataplace, der IoT-Datenmarktplatz Streamr und Plattformen zum Austausch von Industriedaten wie International Data Spaces.

Wenn Daten nicht freiwillig geteilt werden, wird meist die Anwendung von Prinzipien der Lizenzierung standard-essentieller Patente gefordert: FRAND (fair, reasonable and non-discriminatory)-Lizenzen stellen sicher, dass Patententwickler*innen angemessen für ihre Innovation entschädigt werden. Denn wenn ein Patent in einen Standard aufgenommen wird, führt das zu einer breiten Nutzung des Patents, die einzelnen Patententwickler*innen viel Verhandlungsmacht geben. Durch FRAND verpflichten sich die Patentbesitzer*innen dazu, ihr Patent zu einer angemessenen Rate zu lizenzieren. FRAND-Prinzipien haben allerdings selbst im Patentbereich zu komplexen und langwierigen Rechtsstreitigkeiten geführt. Daher ist es fraglich, ob und wie diese Prinzipien auf Daten übertragen werden können. Im Datenkontext werden zwar (bisher) keine Standards geschaffen, doch die meisten Unternehmen halten zeitlich unlimitierte Quasi-Patente auf die von ihnen erhobenen Daten, sofern die Daten nicht repliziert werden. Um zu verhindern, dass eine Datenzugangspflicht Unternehmen davon abhält, Daten zu erheben, sollte die Preissetzung darauf abzielen, dass die Anreize zur Datenerhebung und zur innovativen Datennutzung bestehen bleiben.

6.4.1 Beispiel Online-Werbung

Ein Blick in verschiedene Branchen zeigt, wie Wert der Daten, Replizierbarkeit und Datenhandel zusammenhängen: In der Werbebranche gibt es mit Google und Facebook zwei große Marktteilnehmer, die die Wertschöpfungskette komplett abbilden. Gleichzeitig finden Datenerhebung und -handel unter Beteiligung einer Vielzahl weiterer Akteure statt, von den Werbenden, die eine Zielgruppe ansprechen wollen, über Plattformen, die im Namen der Werbenden in Echtzeit Gebote abgeben, zu Data-Brokern, die über verschiedene Quellen Datensätze anreichern und so versuchen, umfangreiche Profile über die Werbeadressat*innen zu erstellen. Während manche Nutzer*innen einen erheblichen Teil ihrer Zeit auf Facebook und Google verbringen, ist unklar, ob diese Plattformen bei den Daten eine ähnliche Vorrangstellung haben. Die Daten sind zumindest in gewissem Maße replizierbar, z. B. erstellen mehrere Marktteilnehmer*innen Interessenprofile (auch wenn diese auf unterschiedlichen Informationen basieren). Daten werden auch bereits gehandelt – dies stellt den wesentlichen Geschäftszweck der Datenbroker dar. Die Replizierbarkeit schränkt hierbei die Möglichkeit einzelner Unternehmen ein, Daten abzuschotten. Stattdessen haben mehrere Unternehmen prinzipiell die Möglichkeit, auf den Wert der Daten zuzugreifen. Somit ist davon auszugehen, dass eine Datenzugangspflicht unproduktiv wäre. Sie könnte sogar kontraproduktiv sein, wenn man berücksichtigt, dass die aktuell erhobenen Daten bereits häufig als problematisch gesehen werden, da sie Verbraucher*innenaktivitäten in einem fraglich großen Umfang erfassen.

6.4.2 Beispiel Automobil

Anders sieht es aus in der Automobilbranche. Dort sind die Daten über Fahrzeuge, einschließlich Fahrverhalten, Wartungsstand und Straßenverhältnisse, zunächst an das Auto selbst geknüpft und können nicht über andere Quellen mit vergleichbarem Aufwand erfasst werden. Gleichzeitig gibt es mehrere Marktteilnehmer*innen, die neben den Automobilherstellern selbst ein Interesse an der Nutzung der Daten haben, z. B. für neue Formate der Kfz-Versicherung, zur Unfallprävention oder Stadtplanung. In welchem Format welche Daten zugänglich gemacht werden, ist Gegenstand einer intensiven Diskussion zwischen Herstellern und ande-

ren Unternehmen. Die niedrige Replizierbarkeit der Daten, kombiniert mit den Bemühungen der Automobilhersteller, selbst datenbasierte Produkte zu entwickeln, führt bisher zu einem nur sehr moderaten Datenhandel. Daher scheinen hier eher Bedenken begründet, dass der Wert der Daten nicht vollständig gehoben wird, was wiederum für eine mögliche Datenzugangspflicht spricht.

6.5 Zusammenfassung

Der Wert von Daten variiert stark in Abhängigkeit davon, um welche Daten es geht und zu welchen Zwecken sie genutzt werden können. Es ist hilfreich, zwischen der Verbraucher*innen- und der Unternehmenssicht zu unterscheiden. Verbraucher*innen messen datengetriebenen Diensten oft einen sehr hohen Wert bei, der für manche Dienste im zweistelligen Bereich pro Monat liegt. Gleichzeitig schätzen Verbraucher*innen ihre aus dem Datenschutz abgeleiteten Rechte, z.B. wenn sie entscheiden können, bestimmte Daten nicht zu teilen. Auch wenn Verbraucher*innen nicht für Daten zahlen bzw. bezahlt werden, gibt es einige Methoden, diese Wertschätzung quantitativ näherungsweise zu bestimmen. Dabei ist es jedoch wichtig, Vor- und Nachteile verschiedener Ansätze abzuwägen und Ergebnisse richtig zu interpretieren.

Unternehmen befinden sich oft noch auf einer Lernkurve, um den Wert von Daten besser zu heben. Die Replizierbarkeit von Daten ist ein wichtiger Faktor dafür, in welchem Maße mehrere Unternehmen die Möglichkeit haben, Wert aus Daten zu schöpfen – und inwiefern regulatorische Eingriffe nötig sind. Prinzipiell ist marktbasierter Datenzugang einer Pflicht vorzuziehen, nicht zuletzt aufgrund der Schwierigkeiten einer angemessenen Entschädigung für erzwungene Datenteilung. Bisher stecken Datenmärkte noch in der Entwicklung, und es ist zu erwarten, dass mit liquideren Datenmärkten es einfacher wird, angemessene Preise zu setzen und teilbare Datenformate zu nutzen.

7 BLOCKCHAIN-BEWEIS

*Yvonne Schäfer*²²⁶

*Die Blockchain ist durch Kryptowährungen wie Bitcoin bekannt geworden. Es ist allerdings längst bekannt, dass die Blockchain nicht mehr nur für Kryptowährungen genutzt wird, sondern in den verschiedensten Branchen. Blockchain-Enthusiast*innen sind immer wieder auf der Suche nach sinnvollen Use Cases für die gehypte, neue Blockchain-Technologie. Einer der großen Vorteile der Blockchain ist, dass die Technologie als besonders sicher gilt.*

*Blockchain ist eine Technologie zur gesicherten Verarbeitung und Prüfung von Datentransaktionen auf Basis eines verteilten Peer-To-Peer-Netzwerks. Die Blockchain-Technologie nutzt kryptographische Verfahren, Konsensalgorithmen und rückwärtsverlinkte Blöcke, um Transaktionen praktisch unveränderbar zu machen.*²²⁷

Dieser Beitrag soll Impulse für den Einsatz der Blockchain-Technologie im Bereich des Gewerblichen Rechtsschutzes geben und aufzeigen, wie die Technologie als Beweismittel genutzt werden könnte.

7.1 Nachweis von Rechten

Da die Blockchain-Technologie durch die Kryptographie und die Unveränderbarkeit als besonders sicher und vertrauenswürdig gilt, könnte deren Einsatz sich zum Nachweis von Rechten etablieren.

7.1.1 Schutzrechte/Benutzungsnachweis

Gerade im Markenrecht sind Blockchain-Use-Cases denkbar. Bei Streitigkeiten um Marken muss häufig nachgewiesen werden, dass Marken ernsthaft benutzt werden. Die Anforderungen an den sog. Benutzungsnachweis

²²⁶ Mehr über die Autorin erfahren Sie im Autor*innenhinweis auf S. 110.

²²⁷ Bitkom, Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen Studienbericht 2019, S. 15, abrufbar unter: https://www.bitkom.org/sites/default/files/2019-06/190613_bitkom_studie_blockchain_2019_0.pdf.

nachweis sind in Deutschland in § 26 MarkenG geregelt. Als Benutzung gilt u. a. das Anbringen der Marke auf Waren (§ 26 Abs. 4 MarkenG) oder die Verwendung der Marken in Katalogen, in Presseberichten oder auf Rechnungen, wenn damit Produkte bezeichnet oder beschrieben werden. Solche Benutzungsnachweise sind meist aufwändig. Das gilt vor allem, wenn eine Marke für verschiedene Waren und Dienstleistungen Schutz genießt. In der Regel werden zahlreiche Dokumente vorgelegt, aus denen hervorgehen soll, wann, wo und wie die Marken ernsthaft genutzt wurden.

Um dies zu vereinfachen, wäre eine Datenbank auf Blockchain-Basis mit Angaben rund um eine Marke denkbar. Eine solche Datenbank könnte Angaben dazu enthalten, wann und in welchem Umfang die Marke angemeldet, registriert, lizenziert oder gewerblich verwendet wurde. Über Schnittstellen in den Handel oder durch Chips an den Markenprodukten könnte die Verwendung der Marke mit Zeitstempeln unmittelbar in die Datenbank gemeldet werden. Denkbar wären auch Schnittstellen zu den Markenregistern, um die dort hinterlegten Angaben zur Registrierung der Marken zu nutzen anstatt diese Angaben selbst in ein System einzupflegen.

In Amts- oder Gerichtsverfahren könnten durch eine solche Blockchain-Datenbank die Nutzungsnachweise ggfs. unkomplizierter geführt und Beweisprobleme vermieden werden. Würden auch die Markenämter ihre Markenregister auf Blockchain-Basis führen, könnte es vielleicht sogar einfacher werden, Markenämtern gegenüber darzulegen, dass und wie Marken in einem anderen (nationalen) Markenregister registriert sind.

Ein weiterer positiver Nebeneffekt einer solchen Marken-Datenbank auf Blockchain-Basis könnte sich bei der Übertragung von Markenportfolien zeigen. Durch die dezentrale Erfassung der Marken-Informationen könnten Übertragungen von Markenportfolien durch die sichere und vertrauenswürdige Technik unkomplizierter stattfinden. Due Diligences wären in diesem Zusammenhang weniger umfangreich oder teilweise sogar überflüssig.

7.1.2 Lizenzen/Urheberrechte

Die Nutzung der Blockchain-Technologie könnte auch beim Nachweis von Lizenzen und Urheberrechten hilfreich sein. Hier sind vor allem sog. Smart Contracts auf Blockchain-Basis interessant. Smart Contracts sind Computerprogramme auf Blockchain-Basis, in denen Vertragsbedingungen in Form von Wenn-Dann-Regelungen hinterlegt sind. Diese Vertragsbedingungen werden selbständig ausgeführt und überwacht.²²⁸ Solche Smart Contracts können den Schutz und die Durchsetzung von IP-Rechten automatisieren. Durch sie könnten Lizenzen vergeben werden. In dem Smart Contract würde dabei die Regel hinterlegt, dass ein Nutzungsrecht eingeräumt wird sobald die vereinbarte Zahlung geleistet wurde. Die Lizenz würde sodann in Echtzeit eingeräumt, nämlich sobald das Geld gezahlt wurde. Zwischenschritte, wie das Registrieren des Geldeingangs, würden entfallen. Im Bereich der Musikindustrie existieren bereits erste Plattformen auf Blockchain-Basis, die die Urheberrechte der Künstler*innen an den Titeln automatisch verwalten.²²⁹

Da Urheberrechte keine registrierten Schutzrechte sind, bietet sich eine Datenbank auf Blockchain-Basis ebenfalls an, um die Urheber- bzw. Nutzungsrechte nachzuweisen. In der Datenbank könnten die ersten Gedanken und Aktivitäten zu dem Werk registriert sein, das Urheberrechtsschutz genießt. Zeitstempel in der Datenbank könnten einen konkreten Nachweis bieten, wann das Urheberrecht entstanden ist.

7.2 Schutz von Geheimnissen

Die Blockchain-Technologie könnte auch dem Schutz von Geheimnissen dienen.

Bisher werden Vertraulichkeitsvereinbarungen geschlossen, mit denen sich Parteien gegenseitig zusagen, bestimmte Informationen geheim zu halten. Eine Geheimhaltungsvereinbarung, die vor Offenlegung der Geheimnisse geschlossen wird, zielt darauf ab, das Geheimnis noch nicht konkret in der Vereinbarung zu nennen. Geschützt sind Geheimnisse

²²⁸ Zur Funktionsweise siehe: <https://www.skwschwarz.de/aktuelles/artikel/artikel-detail/news/smart-contracts-intelligente-vertraege-der-zukunft/4/detail/News/>.

²²⁹ Siehe <https://peertracks.com/>.

aber auch nur so weit, wie das Geheimnis in der Vereinbarung beschrieben ist. Um das Geheimnis bestmöglich zu schützen, werden bei Verstoß gegen die Vereinbarungen meist Vertragsstrafen fällig.

Geschäftsgeheimnisse werden zwischenzeitlich durch das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) geschützt. Nach § 2 GeschGehG ist ein Geschäftsgeheimnis eine Information, die nicht allgemein bekannt oder ohne Weiteres zugänglich und daher von wirtschaftlichem Wert und Gegenstand von angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und bei der ein berechtigtes Interesse an der Geheimhaltung besteht. Bewertungsmaßstab für Geschäftsgeheimnisse ist daher der Wert des Geheimnisses, der Kreis der Mitwisser*innen und der Grund zur Weitergabe des Geheimnisses.

Nach § 16 GeschGehG kann das Gericht bei Geschäftsgeheimnisstreitsachen auf Antrag streitgegenständliche Informationen als geheimhaltungsbedürftig einstufen. Die Parteien, ihre Prozessvertreter*innen, Zeugen, Sachverständige, sonstige Vertreter*innen und alle sonstigen Personen, die an Geschäftsgeheimnisstreitsachen beteiligt sind oder die Zugang zu Dokumenten eines solchen Verfahrens haben, müssen als geheimhaltungsbedürftig eingestufte Informationen vertraulich behandeln und dürfen diese außerhalb eines gerichtlichen Verfahrens nicht nutzen oder offenlegen, es sei denn, dass sie von diesen außerhalb des Verfahrens Kenntnis erlangt haben.

Problematisch ist, dass das Geheimnis der Gegenseite gegenüber in allen Fällen der Zusammenarbeit offengelegt werden muss, um damit arbeiten zu können. Sofern vorher der Schutzbereich nicht weit genug abgesteckt ist, kann es zu Nachweisproblemen kommen, welche Informationen im Einzelfall der Geheimhaltung unterliegen. Vor allem im Hinblick auf § 16 GeschGehG scheint eine Mitteilung des Geschäftsgeheimnisses – im ungünstigsten Fall an einen Wettbewerber – besonders kritisch.

Für diese Problematik hat das Unternehmen Bernstein eine Blockchain-Lösung entwickelt. Bernstein ist eine Webanwendung, die es ermöglicht, gewerbliche Schutzrechte mit Hilfe der Blockchain zu verwalten und zu sichern. Bernstein-Zertifizierungen sollen die Existenz, Integrität und das Eigentum an hinterlegten Schutzrechten belegen.²³⁰ Das Wis-

230 <https://www.bernstein.io>, Stand 19.01.2020.

sen werde nicht an Dritte weitergegeben, auch nicht an Bernstein selbst, dank seiner sog. „Null-Wissen-Architektur“.²³¹

Durch die Bernstein-Webanwendung werden nach Angaben des Unternehmens digitale Aufzeichnungen von Innovations- und Entwicklungsprozessen mit der Bitcoin-Blockchain und den nationalen Zeitstempelbehörden (z. B. Bundesdruckerei) ermöglicht. Jedes digitale Asset könne bei Bernstein online registriert werden, um die Existenz, den Besitz und die Entwicklung im Laufe der Zeit in Echtzeit nachzuweisen. Die Daten würden dabei dank einer einzigartigen kryptographischen Schicht vollkommen privat bleiben.²³²

Diese Webanwendung könnte zum einen eine technisch wirksame Geheimhaltungsmaßnahme darstellen und zum anderen dazu dienen, dass Geheimnisse nicht mehr vorab konkret beschrieben werden müssen. Gleichwohl könnte der Nachweis von Geheimnissen gesichert sein, weil die relevanten Dokumente mit Zeitstempeln versehen und verschlüsselt auf der Blockchain-Datenbank abgelegt sind, die im Streitfall gesichtet werden können.

7.3 Akzeptanz von Blockchain-Beweisen vor Gericht

Bei all den vorgestellten Use-Case-Ideen stellt sich die Frage, ob Gerichte die Blockchain-Registrierungen als Beweismittel akzeptieren werden. Noch ist mangels tatsächlicher Anwendungsfälle in Deutschland unklar, ob die Blockchain-Technologie im Prozess vor deutschen Gerichten verwertet werden kann. In China sollen Beweismittel auf Blockchain-Basis bereits zugelassen sein.²³³

In Deutschland regelt die ZPO, welche Beweismittel zugelassen sind. Zugelassen sind im Rahmen des Strengbeweises die Beweismittel

- Augenschein (§§ 371 ff. ZPO),
- Zeuge (§§ 373 ff. ZPO),
- Sachverständiger (§§ 402 ff. ZPO),

231 <https://www.bernstein.io>, Stand 19.01.2020.

232 <https://www.bernstein.io>, Stand 19.01.2020.

233 <http://www.globaltimes.cn/content/1147520.shtml>; <https://www.btc-echo.de/china-will-geistiges-eigentum-per-blockchain-schuetzen/>, Stand: 19.01.2020.

- Urkunde (§§ 415 ff. ZPO),
- Parteivernehmung (§§ 445 ff. ZPO).

Zusätzlich gestattet § 294 ZPO auch die Versicherung an Eides Statt.²³⁴

Für einen Beweis auf Blockchain-Basis könnten sich die Beweismittel des Augenscheins oder der Urkunde anbieten. § 371 Abs. 1 S. 2 ZPO regelt, dass elektronische Dokumente dem Anscheinsbeweis unterliegen können, nicht dem Urkundsbeweis.²³⁵ Ist ein elektronisches Dokument Gegenstand des Beweises, wird der Beweis durch Vorlegung oder Übermittlung der Datei angetreten (§ 371 Abs. 1 S. 2 ZPO).

Der Blockchain-Beweis müsste als elektronisches Dokument bei Gericht vorgelegt werden, z. B. durch Vorlage des Datenträgers selbst oder einer Kopie der Datei. Nicht erforderlich ist, dass das Gericht selbst die Datei öffnen kann.²³⁶ Die Inaugenscheinnahme kann nach § 372 Abs. 1 ZPO auch durch einen Sachverständigen erfolgen.

Wenn die Nachweise, die mit der Blockchain-Technologie gespeichert wurden, dem Gericht vorgelegt werden und zumindest ein Sachverständiger diese auswerten kann, dann dürfte der Weg für Blockchain-Beweise offenstehen.

Wenn Rechte durch Signaturen nachgewiesen werden sollen, wie sie beispielsweise im Zusammenhang mit Rechteübertragungen auf einer Blockchain hinterlegt werden könnten, ist jedoch § 371a Abs. 1 ZPO zu beachten. § 371a Abs. 1 ZPO sieht vor, dass auf private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, die Vorschriften über die Beweiskraft privater Urkunden entsprechende Anwendung finden. § 371a Abs. 1 ZPO regelt weiter, dass der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich auf Grund der Prüfung der qualifizierten elektronischen Signatur nach Artikel 32 eIDAS-VO ergibt, nur durch Tatsachen erschüttert werden kann, die ernstliche Zweifel daran begründen, dass die Erklärung von der verantwortenden Person abgegeben worden ist. Die qualifizierte elektronische Signatur dient daher als geeignetes Beweismittel. Von der Regelung erfasst sind aber nur qualifizierte elektronische Signaturen, d. h. solche die von der eIDAS-VO erfasst werden.

²³⁴ *Prütting*, Münchener Kommentar zur ZPO, 5. Aufl. 2016, § 294, Rn. 14 ff. mwN.

²³⁵ *Zimmermann*, Münchener Kommentar zur ZPO, 5. Aufl. 2016, § 371, Rn. 8.

²³⁶ *Zimmermann*, Münchener Kommentar zur ZPO, 5. Aufl. 2016, § 371, Rn. 13.

Eine qualifizierte elektronische Signatur ist eine fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht (Art. 3 Nr. 12 eIDAS-VO).

Die eIDAS-VO dürfte auch den Weg dafür freimachen, dass Blockchain-Zeitstempel vor Gericht zukünftig als Beweis akzeptiert werden. Anforderungen an qualifizierte elektronische Zeitstempel ergeben sich aus Art. 42 eIDAS-VO. Art. 41 Abs. 1 eIDAS-VO regelt, dass einem elektronischen Zeitstempel die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden darf, weil er in elektronischer Form vorliegt oder nicht die Anforderungen an qualifizierte elektronische Zeitstempel erfüllt. Für qualifizierte elektronische Zeitstempel gilt nach Art. 41 Abs. 2 eIDAS-VO die Vermutung der Richtigkeit des Datums und der Zeit, die darin angegeben sind, sowie der Unversehrtheit der mit dem Datum und der Zeit verbundenen Daten.

Im Ergebnis sieht das deutsche Recht durchaus Möglichkeiten vor, Blockchain-Beweise zuzulassen.

Dieser Beitrag soll dazu anregen, die Blockchain-Technologie vor allem auch zum Schutz von gewerblichen Schutzrechten einzusetzen und entsprechende Use Cases umzusetzen und zu nutzen. Bisher fehlen praktische Anwendungsfälle vor Gericht, das Gesetz scheint jedoch ausreichende Möglichkeiten dafür zu bieten, dass Blockchain-Beweise anerkannt werden, wenn diese dem Gericht vorgelegt werden können.

8 ZUR NUTZUNG VON DASHCAMS UND BODYCAMS IM ÖFFENTLICHEN INTERESSE ZUR VERHINDERUNG VON STRAFTATEN UND ORDNUNGSWIDRIGKEITEN AUS SICHT DES RUSSISCHEN GESETZGEBERS

*Hermann Jakobi, LL. M.*²³⁷

Der Beitrag widmet sich dem praxisrelevanten Thema der Umsetzung der Sicherheitspolitik am Beispiel von Bodycams und Dashcams in der Tätigkeit der Polizei in Deutschland und Russland. Die technisch-organisatorischen Schwierigkeiten für die Polizei und für die betroffenen Privatpersonen werden beleuchtet. Abschließend werden Vorschläge für die Entwicklung der Persönlichkeitsrechte in der Praxis hinsichtlich der Anwendung der Dashcams und Bodycams im Rahmen der polizeilichen Aktivitäten entwickelt.

8.1 Einleitung

Wenn man Videos zu Dashcam-Aufnahmen bei YouTube sucht, sind viele Suchergebnisse aus Russland und der ehemaligen Sowjetrepublik zu finden. Dank der Digitalisierung und der relativ mangelhaften Rechtslage zu Dashcams, Bodycams und Drohnen, ist die Nutzung dieser Geräte in Russland stark vertreten. Die Kameras sind an jedem PKW leicht zu montieren und nehmen die gesamte Fahrt auf. Starnecker nennt diese Situation die kuriose Verbreitung der „Russenkameras“ im Internet.²³⁸ Dabei handelt es sich um Privataufnahmen. Es stellt sich jedoch die Frage, ob die Anwendung einer solchen Technik auch im öffentlichen Interesse steht.

Dementsprechend kann die Hauptthese des Aufsatzes wie folgt formuliert werden: Der russische Gesetzgeber ist weder am Rechtsschutz der Privatpersonen interessiert noch in der Lage, einen effektiven Schutz-

²³⁷ Mehr über den Autor erfahren Sie im Autor*innenhinweis auf S. 108.

²³⁸ Vgl. Starnecker, Videoüberwachung zur Risikoversorge, 2017, S. 23.

mechanismus für die Rechtmäßigkeit der polizeilichen Aktivitäten zu gewährleisten. Im Einzelnen geht es um die Begriffsbestimmung für das oben genannte öffentliche Interesse, sowie um die konkreten Probleme, die bei der rechtlichen Beurteilung der Videoüberwachung zu beleuchten sind. Besonders relevant ist auch etwa die Verwendung von Bodycams zum Zwecke der Eigensicherung von z. B. Polizeibeamt*innen.

Der Aufsatz konzentriert sich auf die Vorschriften des russischen Rechts und auf die Sicht des russischen Gesetzgebers, bzw. diverser russischer Rechtsprechung. Zudem werden einige aktuelle Beispiele der deutschen Rechtspraxis betrachtet. Dabei geht es um die Positionen zur informationellen Selbstbestimmung und dem Rechtsschutz einzelner Personen, die in der deutschen Rechtsliteratur stärker zu finden sind. Genauso gelten die Vorschläge als universell für alle beteiligten Parteien, unabhängig, ob eine Problemstellung aus Sicht des russischen oder des deutschen Gesetzgebers gelöst werden muss. Hauptsächlich werden die Body- und Dashcams im Rahmen des Aufsatzes betrachtet. Einige andere technischen Mittel, wie z. B. Drohnen werden nur teilweise oder beschränkt beleuchtet. Zu betonen ist auch, dass es nicht darum geht, die deutschen Rechtsvorschriften zur Videoüberwachung im öffentlichen Raum bloß ins russische Recht oder umgekehrt zu übernehmen. Sinn und Zweck dieses Aufsatzes ist, sich mit den „Stärken“ und „Schwächen“ der jeweiligen Rechtslage zu beschäftigen, um einen effektiven Schutzmechanismus zu schaffen. Dieser soll in möglichst vielen Aspekten betrachtet werden.

Der Aufsatz besteht aus zwei Teilen, einer kleinen „deutschen“ Übersicht zum Thema und aus einem größeren „russischen“ Teil. Eine Zusammenfassung schließt beide Teile ein. Im Rahmen des vorliegenden Aufsatzes werden die Quellen auf Deutsch und Russisch benutzt. Die Titel der Quellen auf Russisch sind zum besseren Verständnis in die deutsche Transliteration übersetzt. Russischen Vor- und Nachnamen sind mithilfe wissenschaftlicher Schreibweise ins Deutsche übersetzt.

8.2 Deutsche Rechtspraxis zur Verwendung von Body- und Dashcams

In diesem Zusammenhang wird sich im Rahmen dieses Teils mit dem deutschen Teil der Verwendung von Body- und Dashcams in der Rechtspraxis der deutschen Polizei beschäftigt.

Wie bereits erwähnt, ist die Verwendung technischer Mittel im Rahmen der Tätigkeit der Polizei und der Staatsbeamt*innen nicht verwunderlich. Heutzutage sind komplexe und fest installierten Systeme für die Videoüberwachung nicht mehr nötig. Ganz umgekehrt sind mobile Systeme, die leicht montiert werden können, viel praktischer für die Tätigkeit der Polizei.²³⁹ Die generelle Möglichkeit für die Verwendung mobiler Techniken statt- und neben installierten Systemen wurde z. B. vom bayerischen Gesetzgeber in der Bekanntmachung zum Polizeiaufgabengesetz (PAG) in der neuen Fassung vom Jahr 2018 bestätigt.²⁴⁰

Beispiele für diese mobilen Systeme sind stationäre Dashcams an Polizeifahrzeugen oder Bodycams, die Polizeibeamt*innen tragen können. Nun bleibt die Frage nach dem Begriff des öffentlichen Interesses bei der Videoüberwachung hinsichtlich Dashcams und Bodycams.²⁴¹ Aus der Auslegung der deutschen, bzw. europäischen rechtlichen Vorschriften zu Videoüberwachung ergibt sich keine Sonderregelung für diese Systeme im Vergleich zur stationären Technik. Für Lachenmann ergibt sich also öffentliches Interesse aus Art. 6 Abs. 1 Satz 1 lit. f DS-GVO und bedeutet mindestens die Notwendigkeit zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit, insb. in Bezug auf die Möglichkeit- und Erforderlichkeit verdächtige Personen zu verfolgen.²⁴² Aus der deutschen Rechtsliteratur ist der Sinn der Einführung von Videoüberwachung, einschl. Dashcams und Bodycams wie folgt zu formulieren — Privatpersonen können zur Verstärkung des Sicherheitsinteresses überwacht werden.²⁴³ Dieser Eingriff in die informationelle Selbstbestimmung durch

239 Über die Kosten für die Montage und Einführung, bzw. für die Schulung des Personals wird hier nicht diskutiert.

240 Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei (Polizeiaufgabengesetz – PAG) in der Fassung der Bekanntmachung vom 14. September 1990, das zuletzt durch § 1 des Gesetzes vom 18. Mai 2018 geändert worden ist: Bayerisches Gesetz- und Verordnungsblatt; S. 301.

241 Vgl. *Lachenmann*, Neue Anforderungen an die Videoüberwachung, ZD 2017, S. 407.

242 Vgl. *Lachenmann*, Neue Anforderungen an die Videoüberwachung, ZD 2017, S. 410.

243 Vgl. *Ziebarth*, Verbesserte Videoüberwachung?, ZD 2017, S. 467.

die Überwiegung des öffentlichen Interesses in der Staatssicherheit muss im Einzelfall geprüft werden, damit man davon ausgehen kann, dass der Schutzmechanismus vorliegt. Am Beispiel des PAG wäre diese Prüfung folgende: Abgesehen von der Kritik über das umstrittene Erfordernis einer drohenden Gefahr, darf die Polizei Privatpersonen sowohl zur Verhinderung von Ordnungswidrigkeiten (Straftaten) als auch zwecks der Eigenversicherung (z. B. zum Nachweis, dass die Polizeibeamt*innen nicht bestochen oder beleidigt werden etc.) mithilfe der Body- und Dashcams überwachen.²⁴⁴ Diese Nutzung darf nur dann zugelassen werden, wenn die Videoüberwachung geeignet, erforderlich und verhältnismäßig ist und nur unter der Berücksichtigung des Rechts auf informationelle Selbstbestimmung der betroffenen Bürger*innen durch Höhergewichtung des Sicherheitsinteresses möglich.²⁴⁵

Zusammenfassend kann man sagen, unter dem öffentlichen Interesse versteht man die Notwendigkeit, die Gesellschaft gegen Straftaten und Ordnungswidrigkeiten zu schützen, sowie die Eigenversicherung der Polizeibeamt*innen zu gewährleisten (Staatssicherheit). Das dreistufige Modell der Prüfung der Verwendung von Body- und Dashcams in der Rechtspraxis der Polizei ist im deutschen Recht als ein zentrales Element des Eingriffs in die informationelle Selbstbestimmung und Privatsphäre einzelner Privatpersonen zu verstehen.²⁴⁶

8.3 Russische Rechtspraxis zur Verwendung von Body- und Dashcams

Im Gegensatz zum deutschen Teil des Aufsatzes existiert keine ähnliche Diskussion – weder auf politischer Ebene noch in der Wissenschaft – in Russland. In diesem Zusammenhang stellt sich die Frage, ob der russische Gesetzgeber seine Rolle bei der Erfüllung des öffentlichen Interesses genauso versteht. Eine ganz klare Frage wäre, ob die in der deutschen Rechtsliteratur vertretenen Voraussetzungen bei der Prüfung des tatsächlichen Eingriffs in die informationelle Selbstbestimmung vorliegen (also Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit der

²⁴⁴ Vgl. *Leisner-Egensberger*, Polizeirecht im Umbruch: Die drohende Gefahr; DÖV 2018, S. 677.

²⁴⁵ Vgl. *Ziebarth*, Verbesserte Videoüberwachung?, ZD 2017, S. 468.

²⁴⁶ Vgl. *Brink, Wilhelm*, in: Wolff, Heinrich Amadeus/Brink, Stefan (Hg.): BeckOK Datenschutzrecht, 25. Ed., 01.08.2018, BDSG § 4 Rn. 3–6.

Nutzung von Body- und Dashcams). Im „Russland-Fall“ bezieht sich das öffentliche Interesse auf nichts anderes, als die permanente Möglichkeit der Aufzeichnung der beteiligten Parteien während des Dienstes, zur Beweiserleichterung bei Ordnungswidrigkeiten und Straftaten.²⁴⁷ Mit anderen Worten bedeutet das Folgendes: für den russischen Staat ist es nicht so wichtig, dass die Personen (und/oder ihre informationelle Selbstbestimmung), die eine Straftat oder eine Ordnungswidrigkeit begangen haben, 24/7 überwacht werden können. Auch die Privatsphäre der einzelnen Polizeibeamt*innen, die die Bodycams tragen, spielt keine Rolle. Vielmehr geht es darum, dass man dementsprechende „Datenpools“ für die Beweissicherung mithilfe Body- und Dashcams schaffen kann, um das Verfahren gegen eine Person schneller und „effizienter“ durchzuführen.²⁴⁸ Auch die Eigensicherung der Polizeibeamt*innen ist ein Teil dieses Beweisverfahrens. So könnte die Verstärkung des öffentlichen Sicherheitsinteresses bei der Eigensicherung ein „Mechanismus zur Abschreckung“ sein, um eventuell Korruption, Bestechung, Beleidigungen oder Anwendung von Gewalt von beiden Parteien (sowohl die Polizeibeamt*innen als auch Privatpersonen, die z. B. eine Ordnungswidrigkeit begangen haben) zu verhindern.²⁴⁹ Um den Schutz der informationellen Selbstbestimmung geht es in dem Diskurs des russischen öffentlichen Interesses fast nicht. Nicht verwunderlich ist, dass es kein Prüfungsmodell wie im deutschen Recht gibt. Stattdessen versucht der russische Gesetzgeber die technischen Standards zu entwickeln, um die Nutzung von Body- und Dashcams zumindest aus der technischen Seite zu begründen.

Dies kann aufgrund folgender Beispiele demonstriert werden.

247 Vgl. *Sevast'janov*, Über die Rechtspraxis der Verwendung von Dashcams bei der Polizei, Internetquelle, abrufbar unter: <http://dnevniknauki.ru/images/publications/2018/6/law/Sevastianov2.pdf> [Praktika primenenija kamer videonabljudenija dorožnoj obstanovki i sistem videonabljudenija patrol'nych avtomobilej] (zuletzt abgerufen am 15.07.2019).

248 Vgl. *Avrutin, Černikov, Bulavin*, Kommentar zum Gesetz „Über die Polizei“, 2017, S. 230 [Kommentarij k Federal'nomu zakonu „O policii“].

249 Videokameras gegen Korruption, Internetquelle, abrufbar unter: <https://25.xn--b1aew.xn--p1ai/news/item/12936103/> [Videokamery protiv korrupcii] (zuletzt abgerufen am 15.07.2019).

8.3.1 Obligatorische Nutzung der digitalen Technologien in der öffentlichen Verwaltung

Nach Art. 18 des Gesetzes „Über die Polizei“ darf die Polizei alle zur Verfügung stehenden technischen Geräte für die Audio- und Videoaufnahme im Rahmen der polizeilichen Aktivitäten verwenden, um dem öffentlichen Interesse an der Verhinderung von Straftaten und Ordnungswidrigkeiten gerecht zu werden. Einige Autor*innen in Russland betonen unter Hinweis auf Art. 11 Abs. 3 des Gesetzes „Über die Polizei“, die Nutzung von Body- und Dashcams sei keine freiwillige Aufgabe der Polizei, vielmehr geht es um ein Prinzip der obligatorischen Verwendung digitaler Technologien in der Rechtspraxis.²⁵⁰ In diesem Sinne lässt sich sagen, dass das öffentliche Interesse in Bezug auf die Nutzung von Body- und Dashcams nur einen speziellen Bereich bei der allgemeinen öffentlichen Verwaltung umfasst. Dieser Bereich richtet sich an die obligatorische Nutzung von Body- und Dashcams in der Rechtspraxis der Polizei, um die Beweisführung bei der Verhinderung der Straftaten und Ordnungswidrigkeiten, einschl. Verhalten der Polizeibeamt*innen selbst (Eigensicherung) zu erleichtern.²⁵¹

8.3.2 Ausführliche Beschreibung technischer Anforderungen

Wie bereits erwähnt, gibt es keine effektive Prüfung des Eingriffs in die informationelle Selbstbestimmung (Stichwort – dreistufiges Modell der Prüfung) im russischen Recht. Stattdessen versucht dieser Beitrag, die bereits vorhandenen Standards und Anforderungen weiterzuentwickeln. Ein Beispiel für diese Anforderung wäre die optimale Positionierung der Body- und Dashcams (am Fahrzeug), um bestmögliche Aufnahmen zu erhalten. Ob eine Kamera auch die Gesichter der Personen, die an der Tat nicht beteiligt sind, Landschaften, Privatgrundstücke, insb. Balkon oder Terrasse aufnehmen kann, wird seitens des russischen Gesetzgebers

250 Verordnung der Regierung der Russischen Föderation v. 01.11.2013 № 2036-r „Über die Entwicklungsstrategie im digitalen Bereich in der Russischen Föderation“; Das „Russische Amtsblatt“ v. 08.11.2013 [Rasporjaženije Pravitel'stva RF ot 01.01.2013 № 2036-r „Ob utverždenii Strategii razvitija otrasli informacionnyh technologij v Rossijskoj Federacii na 2014-2020 gody i na perspektivu do 2025 goda“].

251 Beschluss des Wirtschaftsgerichts v. 16.05.2016 Az.02AP-2711/2016 [Postanovlenie Vtorogo arbitražnogo apelljacionnogo suda ot 16.05.2016 № 02AP-2711/2016 po delu № A29-8660/2015].

nicht dezidiert geregelt. Vielmehr geht es um die Erfüllung der technischen Standards, dass die Videoüberwachung durchgeführt wird und die Ordnungswidrigkeiten verhindert werden, bzw. die Beweisführung im Rahmen eines Verfahrens erleichtert wird. Der informationelle Schutz von Privatpersonen wird folglich zu Gunsten eines funktionierenden Rechtsschutzes und der Aufrechterhaltung der öffentlichen Ordnung als nachrangig eingestuft.

Nicht zu vergessen ist, dass die Kameras eine stetig steigende Video- & Bildqualität aufweisen und ständig aufnehmen, sowie eine Gesichtserkennungsoption besitzen. Russische Politiker*innen und Polizeibeamt*innen fordern die Erweiterung der Anzahl der Videoaufnahmen und verwendeten Geräte. Ein Beispiel dafür ist die Initiative, Drohnen im Rahmen der Polizeiaktivitäten zu verwenden.²⁵² So vergisst man oft die Gefahr der massiven und unkontrollierten Videoaufnahmen, wie etwa eine pauschale Speicherung der Daten, die kaum begründet werden kann. Mit anderen Worten bedeutet das Folgendes: die Sicherheit und die gute Reputation der Polizei sind dem russischen Staat viel wichtiger, als die informationelle Selbstbestimmung und Privatsphäre der russischen Bevölkerung.²⁵³

8.4 Zusammenfassung und Fazit

Abschließend kann resümiert werden, dass weder die deutsche Rechtspraxis noch die russische Variante der Verwendung von Bodycams und Dashcams optimal sind. Das deutsche Vorgehen sieht aber eine starke Interessenabwägung zwischen der informationellen Selbstbestimmung auf der einen und den Bedürfnissen der deutschen Sicherheits- und Strafverfolgungsbehörden auf der anderen Seite vor. Das fehlt bei der Umsetzung der russischen Polizei- und Sicherheitspolitik. Nach der Interessenabwägung sind das Recht auf informationelle Selbstbestimmung

252 Russische Polizei wird Drohnen in der Praxis verwenden, Internetquelle, abrufbar unter: <https://russian.rt.com/article/144701> [SMI: Rossijskoj policii predložili ispolzovat' v rabote bespilotniki i natel'nye kamery] (zuletzt abgerufen am 15.07.2019).

253 Vgl. *Rudakov*, Über die einheitliche Anforderungen zu Body- und Dashcams in der Rechtspraxis der Polizei, *Vestnik ural'skogo juridičeskogo instituta MVD Rossii*, 2016, S. 43 [Formirovanie edinych techničeskich k portativnym videoregistratoram, ispol'zuemym sotrudnikami policii v pravoočranitel'noj dejatel'nosti].

und Schutz der Privatsphäre im russischen Recht nachrangig im Gegensatz zum öffentlichen Interesse an Sicherheit der ganzen Gesellschaft.

Unter dem öffentlichen Interesse versteht man fast das gleiche wie im deutschen Recht. Im Gegensatz zur deutschen Position zur Nutzung von Body- und Dashcams gibt es im russischen Recht kein Prüfungsmodell, nach dem man den Eingriff in die informationelle Selbstbestimmung „messen“ kann.

Um diesen starken Eingriff des russischen Staates in die informationelle Selbstbestimmung zu begrenzen, wäre es denkbar, die folgenden zwei wichtigen Punkte anzusprechen. Das gilt aber für den deutschen Gesetzgeber ebenso.

- Erstens ist eine Frist für die Speicherung der Daten festzulegen. Trotz der unterschiedlichen Rechtsvorschriften stellt sich die Frage, ob die Daten unverzüglich gelöscht werden können, wenn die Notwendigkeit für die Speicherung entfallen ist. In diesem Sinne lässt sich sagen, dass die Dauer an Einzelfall wissenschaftlich begründet werden muss.²⁵⁴
- Zweitens muss die verwendete Technik nur die Personen audiovisuell aufnehmen, welche im konkreten Fall Ordnungswidrigkeiten begehen; auf die Aufnahme von Personen, die an der Tat unbeteiligt sind, muss möglichst verzichtet werden. Als eine organisatorische Maßnahme kann man die in Deutschland vertretene Kennzeichen an der Uniform von Polizeibeamt*innen nennen, die darauf hinweisen, dass eine Videoüberwachung mithilfe der Bodycams durchgeführt wird. Nun bleibt die Frage, ob diese Kennzeichen groß bzw. aussagekräftig genug sein müssen, damit alle Privatpersonen verstehen können, dass sie potentiell betroffen werden. Auch wären die Kameras dergestalt denkbar, dass Privatpersonen sehen können, wer genau in diesem Moment gefilmt wird. Diese Kennzeichen an der Uniform von Polizeibeamt*innen und einige andere technische Maßnahmen, die in Deutschland gut funktionieren, sind in Russland nicht vorhanden. Nicht zuletzt sind die unabhängigen Aufsichtskommissionen von Expert*innen vonnöten, die die Tätigkeit der Polizei einer ständigen Rechtmäßigkeitskontrolle unterziehen können und den hinreichenden Schutz der Privatpersonen mit in ihre Bewertung einstellen.

²⁵⁴ Vgl. Rudakov, Borzenko, Probleme bei der Verwendung von Bodycams in der Rechtspraxis der Polizei, Konzept, 2017, S. 807 [Problemy primeneniya portativnykh videoregistratorov v dejatel'nosti učastkovogo upolnomochennogo policii].

Autor*innenhinweise

Dr. Anna K. Bernzen ist Rechtsreferendarin am Landgericht Frankfurt am Main. Zuvor hat sie an der Universität Osnabrück rechtsvergleichend zur Berichterstattung aus deutschen und englischen Gerichtssälen promoviert. Daneben war sie zuerst als juristische Mitarbeiterin bei White & Case LLP im Bereich „IT und Outsourcing“ tätig und anschließend als akademische Mitarbeiterin an den Universitäten Osnabrück und Mannheim im Recht des Geistigen Eigentums und im Staats- und Europarecht aktiv. Ihr Jurastudium mit dem Nebenfach Wirtschaftswissenschaften absolvierte sie an der Universität Mannheim und der University of Surrey in England. Studienbegleitend ließ sie sich in der Journalistischen Nachwuchsförderung, kurz JONA, der Konrad-Adenauer-Stiftung zur Journalistin ausbilden – eine Ausbildung mit Stationen z.B. beim Handelsblatt und in der ARD-Rechtsredaktion.

Aline Blankertz ist Projektleiterin für „Datenökonomie“ bei der Stiftung Neue Verantwortung und untersucht ökonomische, technische und gesellschaftliche Fragestellungen, um innovative datenpolitische Handlungsempfehlungen zu entwickeln. Davor leitete Aline Blankertz bei der wirtschaftswissenschaftlichen Beratung Oxera Analysen mit einem Fokus auf digitale Märkte und Wettbewerb und arbeitete zu verschiedenen Themen wie Plattformökonomie, Datenschutz, Algorithmen, Fairness in E-Commerce und Intermediärhaftung für u. a. Google, Skyscanner und die englische Verbraucherorganisation Which?. Außerdem gab sie Seminare für EU-Richter*innen zum Wettbewerb auf digitalen Märkten. Sie studierte an der Hochschule St. Gallen (Schweiz), Universidad Torcuato di Tella (Argentinien), University of Oxford (Großbritannien), WWU Münster und Chulalongkorn University (Thailand).

Dr. Klaus Friele hat ein Diplom in theoretischer Physik und einen Doktor in systematischer Musikwissenschaft von der Universität Hamburg. Sein Forschungsschwerpunkt sind Computer-gestützte Methoden in der Musikpsychologie. Nach Jahren als Softwareentwickler in der Industrie war er von 2008 bis 2012 Lehrkraft für systematische Musikwissenschaft der Universität Hamburg, worauf ein Forschungsaufenthalt am Centre for Digital Music an der Queen Mary University of London folgte. Von 2012 bis 2019 war er als wissenschaftlicher Mitarbeiter am Jazzomat Research Project und beim Dig-That-Lick Project an der Hochschule für Musik „Franz Liszt“ Weimar angestellt, wo er sich mit

digitaler Jazzforschung beschäftigte, und war zwischendurch für ein halbes Jahr als Post-Doc-Forscher am Max-Planck-Institut für empirische Ästhetik in Frankfurt/Main. Klaus Frieler ist seit über 10 Jahren als freiberuflicher Musikgutachter und wissenschaftlicher Berater tätig, u. a. für das LongGold-Projekt, einer Langzeitstudie zur musikalischen Entwicklung in der Adoleszenz.

Susan Gonscherowski ist Referentin für Grundsatzfragen der Digitalisierung und E-Government im Digitalisierungsministerium Schleswig-Holstein. Sie studierte Politikwissenschaft und öffentliches Recht an der Universität Kiel. 2016–2019 war sie als Wissenschaftliche Mitarbeiterin am Unabhängigen Landeszentrum für Datenschutz tätig und betreute hier unter anderem das EIDI-Projekt. Sie unterrichtet Student*innen an der Universität Kiel sowie der Fachhochschule für Verwaltung Altenholz und ist Co-Autorin verschiedener Fachbeiträge, u. a. zum Thema Datenschutzfolgenabschätzung.

Hans-Christian Gräfe ist Wissenschaftlicher Mitarbeiter am Weizenbaum-Institut für die vernetzte Gesellschaft und Lehrbeauftragter an der Technischen Universität Berlin. Sein Interesse liegt hauptsächlich im Medien- und Social Media-Recht, worin er forscht, lehrt und veröffentlicht. Daneben nimmt er am LL. M.-Programm im Immaterialgüter- und Medienrecht an der Humboldt-Universität Berlin teil. Das Referendariat hat Hans am Landgericht Münster absolviert. Stationen u. a. bei SKW Schwarz in Berlin – Team IT & Digital Business, der Deutschen Universität für Verwaltungswissenschaften Speyer – Seminar: Digitale Infrastrukturen, LEXEA Rechtsanwälten in Köln und dem Deutschen Generalkonsulat Barcelona. Studiert hat Hans in Marburg, Madrid und Münster. Am ITM in Münster erwarb er eine Zusatzqualifikation im Gewerblichen Rechtsschutz. Den Schwerpunkt legte er in Marburg auf das private Medienrecht.

Hermann Jakobi, LL. M. ist deutsch-russischer Jurist, M. A. in European Studies und DAAD-Stipendiat. Seine Forschungsinteressen umfassen das Polizei- und Sicherheitsrecht sowie das allgemeine Verwaltungsrecht. Im Rahmen seiner Tätigkeit als Kollegiat am DFG-Graduiertenkolleg 1681/2 »Privatheit und Digitalisierung« an der Universität Passau untersucht er die Verwendung von Dashcams bei der deutschen Polizei im öffentlichen Interesse in Bezug auf öffentliche Sicherheit und Ordnung. Dazu wird das russische Modell der Videoüberwachung des

Straßenverkehrs mithilfe von Dashcams analysiert, um das deutsche Polizeirecht aufgrund eines möglichen Rechtsexportes dementsprechend zu erneuern.

Jonas Kunze studiert Rechtswissenschaft an der Freien Universität Berlin. Seinen Schwerpunkt legte er auf das Immaterialgüterrecht, worin er bereits publiziert. Er unterstützt Telemedicus als Studentischer Mitarbeiter. Hier hilft er bei der Organisation der Sommerkonferenz sowie der Koordinierung des Blogs. Erste journalistische Erfahrungen konnte Jonas bei der Jugendpresse Deutschland e.V. sammeln. Als Beiratsmitglied betreut er dort die Rechtsberatung für Schülerzeitungen.

Fabian Rack kam bereits im Jurastudium über eigene Musikprojekte zum Urheberrecht. Er ist seit 2016 Rechtsanwalt und wissenschaftlicher Mitarbeiter bei FIZ Karlsruhe (Leibniz Institut für Informationsinfrastruktur) im Bereich Immaterialgüterrechte unter Leitung von Prof. Dr. Franziska Boehm. Seit März 2020 ist er assoziierter Partner bei iRights. Law in Berlin. Als Anwalt berät Fabian Rack u. a. Institutionen und Unternehmen zu Möglichkeiten der Digitalisierung, Beforschung und Zugänglichmachung von Material im Wissenschafts- und Kulturbereich. Er gibt Workshops und Seminare an Wissenschafts- und Kulturinstitutionen und in der juristischen Referendarausbildung in Baden-Württemberg. Seit seinem Studium wirkt er als Autor und Mitglied bei Telemedicus mit und hat von 2014 bis 2016 für Legal Tribune Online als Autor für die juristische Presseschau gearbeitet. In seiner Ausbildungszeit hat er bei verschiedenen NGOs Erfahrungen in den Bereichen Verbraucherschutz und digitale Bürgerrechte gesammelt.

Verena Reiter hat an der Goethe-Universität Frankfurt am Main im Fachbereich Amerikanistik promoviert. Im Rahmen ihres Dissertationsprojekts „Renegotiating American Nationalism: The Proxy War over Marriage Equality through the Lens of Un-Americanism“ untersuchte sie den Vorwurf des ‚un-Americanism‘ im innenpolitischen Diskurs der USA am Beispiel der Marriage Equality Debatte. Sie studierte Lehramt an der Universität Regensburg und legte dort 2015 ihr erstes Staatsexamen ab. Zudem forschte sie für ein Jahr als Visiting Scholar am Department of Political Science der University of California, Davis. Ihre Forschungsschwerpunkte liegen im Bereich der amerikanischen Politik- und Kulturwissenschaft. Sie interessiert sich insbesondere für Identitätspolitik, soziokulturellen Wandel, das US-Rechtssystem als auch für die

transatlantischen Beziehungen. Derzeit ist sie beruflich im Bereich der Studiengangsakkreditierung und der Qualitätssicherung von Studium und Lehre tätig.

Yvonne Schäfer ist Rechtsanwältin/Counsel bei SKW Schwarz in Frankfurt am Main. Sie ist Fachanwältin für gewerblichen Rechtsschutz und berät nationale und internationale Unternehmen in den Bereichen des IT- und IP-Rechts. Durch ihren Branchenfokus auf Digital Business berät Yvonne Schäfer ihre Mandanten in allen Rechtsfragen zu den Themen Know-How-Schutz, Big Data und FinTech. Sie unterstützt z. B. Online-Händler, Medienagenturen und Finanzdienstleister bei dem Entwurf von IT-Verträgen sowie im Bereich Social Media und in datenschutzrechtlichen Aspekten. Bei SKW Schwarz beschäftigt sich Yvonne Schäfer seit mehreren Jahren mit den Einsatzmöglichkeiten der Blockchain-Technologie, insbesondere für IP-Use Cases, u. a. in der kanzeleinternen Passion Group und bei Verbänden.

Julia Sinnig ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Europäisches und Internationales Steuerrecht der Universität Luxemburg. Im Rahmen ihrer Promotion beschäftigt sie sich mit dem Thema „Taxation, Data and Destination: An Analysis of the Compatibility of a (Digitalized) Destination-Based Corporate Tax and Destination-Based Cash-Flow Tax with International and EU Tax and Data Protection Law Frameworks“. Betreut wird das Dissertationsprojekt von Prof. Dr. Werner Haslechner, Generalanwältin (EuGH) Prof. DDr. Juliane Kokott und Prof. Dr. Mark D. Cole. Julia Sinnig studierte Rechtswissenschaften an der Universität Luxemburg und der Westfälischen Wilhelms-Universität Münster. Sie veröffentlicht und lehrt im Bereich des internationalen, europäischen und luxemburgischen Steuerrechts in deutscher, englischer und französischer Sprache.

Dr. Matthias Wübbeling hat an der TU Dortmund Informatik studiert. Nach seinem Diplom 2011 arbeitete er als Wissenschaftlicher Mitarbeiter an der Fakultät für Maschinenbau im Bereich der Elektromobilität. Anfang 2012 wechselte er in die Bundesstadt Bonn und arbeitet dort seitdem für das Fraunhofer FKIE und die Universität Bonn als Wissenschaftlicher Mitarbeiter. Als Sicherheitsexperte forscht er im Bereich Computer- und Netzwerksicherheit. Seine Promotion hat er 2019 zum Thema Prefix-Hijacking im Internetrouting abgeschlossen. Derzeit untersucht er unter anderem die Klassifikation von Internetrouting-Ano-

malien und den möglichen Umgang mit Identitätsdatenleaks und Folgen daraus. Darüber hinaus vermittelt er in der universitären Lehre Inhalte in den Bereichen hardwarenahe Programmierung, Microcontroller und angewandte IT-Sicherheit. Freiberuflich ist er Berater für IT-Sicherheit und Autor für Fachzeitschriften. Darüber hinaus engagiert er sich im Executive Committee des IEEE TCCC und in der Gesellschaft für Informatik. Er ist Mitglied des Speaker-Netzwerks blackstone432.de zum Thema Identitätsdiebstahl und Cyber Security.

„Über den Tellerrand“ – dieses Motto war Programm auf der Telemedicus Sommerkonferenz 2019. Mit interdisziplinären Beiträgen widmete sich die Konferenz der Komplexität der realen Welt im Digitalbereich. Dies spiegelt sich auch im Tagungsband wider. Fachübergreifend werden aktuelle Entwicklungen und Zukunftstrends betrachtet, zum Beispiel die Entwicklung der Pressefreiheit in den USA unter Trump, Music Data Mining oder der Wert digitaler Güter. Weiterhin durften wir auf der Soko19 mit unseren Speaker*innen und Teilnehmenden über Data Leaks, den Einsatz der Blockchain zu Beweis-zwecken sowie Dash- und Bodycams diskutieren. Die wesentlichen Themen der Konferenz dokumentieren wir in diesem Tagungsband.

Mit Beiträgen von:

Dr. Anna K. Bernzen, Aline Blankertz, Dr. Klaus Frieler, Susan Gonscherowski, Hans-Christian Gräfe, Hermann Jakobi, Jonas Kunze, Fabian Rack, Verena Reiter, Yvonne Schäfer, Julia Sinnig und Dr. Matthias Wübbeling.

