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

§ Telemedicus

Sommerkonferenz

Das Recht der Informationsgesellschaft

Tagungsband zur Konferenz

Tagungsband zur Sommerkonferenz 2022

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

Tagungsband zur Sommerkonferenz 2022

Telemedicus – Recht der Informationsgesellschaft

Telemedicus-Schriftenreihe

Band 6

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Vorschläge zur Zitierweise:

Autor:innen (2022). Titel. In Gräfe H.-C./Telemedicus (Hrsg.), Telemedicus – Recht der Informationsgesellschaft, Tagungsband zur Sommerkonferenz 2022 (S. xx–xx). Frankfurt a. M.: Deutscher Fachverlag.

Autor:innen, Titel, in Gräfe/Telemedicus: Tagungsband zur Sommerkonferenz 2022, S. xx–xx.

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.

ISBN 978-3-8005-1857-9

dfv Mediengruppe

Klimaneutral Druckprodukt ClimatePartner.com/10536-2202-1001

www.ruw.de

Druck: Druckerei Hachenburg – PMS GmbH, 57627 Hachenburg

Printed in Germany

Vorwort

Eine Sommerkonferenz 2022 in Präsenz – voller Ideen und Diskussionen, aber auch Updates und Austausch über die Rechtspraxis sowie nicht zuletzt Inspiration und Vernetzung. Dem eigenen Anspruch stellten sich die Telemedicus Redaktion und die Forschungsgruppe RIoT des Weizenbaum-Instituts. Schnell war uns dabei klar, dass wir einige Themen gesetzt sehen wollen. Viel davon findet sich in diesem Band wieder, wie die Beiträge zur Modernisierung des Zivilprozesses, zu NFTs sowie Juristischer Ausbildung und Legal Tech. Manche Themen hatten wir von vorneherein als interdisziplinäre Präsentationen vorgesehen, wie die Beiträge zu Predictive Analysis, Satelliten-Megakonstellationen und zum Metaverse.

Trotzdem wollten wir uns durch einen Call for Proposals spannenden Themenvorschlägen öffnen. Die Einladung ging insbesondere an Soko-Newcomer mit frischen Ideen – ganz gleich ob akademischer Nachwuchs oder (Nicht-)Jurist:innen aus der Praxis. Vom Widerhall waren wir begeistert und konnten viele der Vorschläge auf der Konferenz präsentieren. In diesem Band finden sich auch einige der Einreichungen wieder. So sei hingewiesen auf die Beiträge zu Public Value, zum Influencer Marketing, zu Technologie-Souveränität, zu Überindividuellen Problemen im Datenschutzrecht, zu Betroffenenrechten im eSport, zum Fediverse und zu Federated Learning.

Erstmalig auf der Soko22 hat es die Möglichkeit gegeben, Poster und Ideen in einem vertraulicheren Format vorzustellen. Auch auf diesen Aufruf hin durften wir ein paar sehr interessante Ansätze präsentieren. Das ursprünglich als Forschungsposter dargestellte Thema Projekt Synco (Cybersyn) liegt nun in diesem Band als Beitrag vor.

Uns bleibt, uns bei allen Autor:innen und dem Deutschen Fachverlag für die vertrauensvolle Zusammenarbeit zu bedanken. Ebenso danken wir allen unseren Sponsoren, die uns z. T. seit langen Jahren begleiten und z. T. gerade in diesem Jahr eine Präsenzkonferenz wieder ermöglichen wollten: den Rechtsanwaltskanzleien HÄRTING, Bird&Bird, SKW Schwarz, Osborne Clarke, DORNKAMP und Morrison Foerster sowie Microsoft, dem Game e. V. und dem iRights.Lab.

Schließlich geht ein großer Dank an das Weizenbaum-Institut als Mitveranstalter und Forschungsgruppen-PI Bettina Berendt sowie Forschungsgruppenleiter Stefan Ullrich! Ohne Eure Unterstützung hätte weder die Konferenz stattgefunden noch hätte vorliegender Tagungsband veröffentlicht werden können.

In der Publikation selbst wurde die ursprüngliche Vortragsreihenfolge beibehalten, um Vielfalt und Abwechslungsreichtum der Soko22 zu zeigen – eben das Recht der Informationsgesellschaft.

Hans-Christian Gräfe & Adrian Schneider
Berlin und Köln im November 2022

Inhaltsverzeichnis

1 Tagungsbericht

*Hans-Christian Gräfe, Karla Herb und Ertuğrul Can**

Das Recht der Informationsgesellschaft entwickelt sich rasant und ist aus der Nische in die breite Öffentlichkeit gerückt. Die Telemedicus Sommerkonferenz vereint dabei Rechtsexpert:innen aus der Praxis z. B. des IT-Rechts mit Jurist:innen aus der Forschung. Genauso wichtig wie der juristische Austausch ist die Einbettung der Rechtsfragen in einen gesellschaftlichen Zusammenhang und Interdisziplinarität. Das bedeutet vor allem eine technologische wie politische Einordnung anstehender und aktueller Herausforderungen.

Das Programm mischt daher Praxisbeiträge und rechtswissenschaftliche Forschungsthemen. Neue Regelungen wurden beleuchtet, wie das Digitale Vertragsrecht, der Digital Services Act, der Digital Markets Act oder der Chips Act. Weiterhin legen wir einen Fokus auf Phänomene aus dem Datenschutzrecht, rund um eSports und das Influencer Marketing. Wir diskutierten rechtliche und technische Neuheiten wie das Web 3.0, Legal Tech, Satelliten Mega-Konstellationen und die Modernisierung des Zivilprozesses. Schließlich widmeten wir uns der Verantwortung von Intermediären, dezentralen Kommunikationslösungen und der Rechtsdurchsetzung im digitalen Raum.

Der Tagungsbericht gibt das zweitägige Programm der Soko22 wieder. Wir konnten sehr abwechslungsreiche Themen zusammenstellen und bedanken uns bei allen Referierenden. Neben Vorträgen und viel Platz für Diskussionen gab es dieses Jahr erstmals einen kleinen Ausstellungsbereich.

1.1 Verbindung von Forschung, Praxis, Rechtsgebieten und Disziplinen

Die zweitägige Konferenz fand Anfang Juli in den Räumen von Microsoft in Berlin statt. Gemäß dem Weizenbaum-Motto, Forschungsinhalte in die Gesellschaft zu transferieren, unterstützten Kanzleien, Verbände und Think Tanks die Zusammenkunft finanziell und inhaltlich. Das Programm bestand so aus einer Mischung aus Praxisbeiträgen und rechtswissenschaftlichen Forschungsfragen vor allem aus dem IT- und Medienrecht. Ein *Call for Proposals* hatte einige hochkarätige Vorschläge ergeben – auch spannende Orchideenthemen haben eine Bühne für Austausch und Diskussion gefunden. Eine Besonderheit der Soko22 ist sicherlich, dass von Studierenden bis hin zu Professor:innen referieren, Rechtsanwält:innen neben

* Mehr über die Autor:innen erfahren Sie im Autor*innenhinweis auf S. 224 ff.

Wissenschaftler:innen auftreten und Themen interdisziplinär in Angriff genommen werden. Dies wiederum dem Weizenbaum-Spirit und einer vielfältigen Diskussion verpflichtet.

In der Keynote von *Benjamin Brake*, dem Abteilungsleiter für Digital- und Datenpolitik im Bundesministerium für Digitales und Verkehr, ging es direkt zur Sache. Deutschlands Datenstrategien sollen dafür sorgen, den Nachholbedarf bei vielen Themen der Digitalisierung zu beheben. Dazu gehört es u. a. den Ausbau digitaler Infrastrukturen voranzutreiben. Wichtig seien außerdem digitale Souveränität und die Frage, wie mit Desinformationen und Hassrede in sozialen Netzwerken umzugehen ist. Schließlich müssten die richtigen Rahmenbedingungen für einen selbstbestimmen und sicheren Umgang mit dem Netz geschaffen werden. Gerade im Hinblick auf anstehende Neuerungen einiger Regeln im Netzrecht entspann sich eine rege Diskussion mit dem Publikum.

1.2 Digitales Vertragsrecht

Das Recht der digitalen Produkte ist die größte Neuerung des Bürgerlichen Rechts seit 2002 und wurde im ersten Panel der Soko von gleich vier Referent:innen unter die Lupe genommen. *Dr. Anna Bernzen* befasste sich vor allem mit der Aktualisierungspflicht von digitalen Produkten, der Unternehmer:innen gegenüber Verbraucher:innen unterliegen. Wie lange diese Pflicht bestehe und was genau die Aktualisierungen beinhalten müssen, seien nur zwei der offenen Fragen, die die Gesetzgebung hinterlassen habe. Dr. *Zuha Ayar* warf einen Blick auf das Phänomen „Zahlen mit Daten" – wenn also Verbraucher:innen personenbezogene Daten als synallagmatische Gegenleistung bereitstellen. Dabei müsse der/die Unternehmer:in die Datenverarbeitung auch vor dem Hintergrund der DSGVO auf eine Rechtsgrundlage stützen. Regelmäßig erfolge dies über die Einwilligung. Diese sei nach dem Kopplungsverbot aber nicht „freiwillig" erteilt, wenn sie Bedingung für die Vertragserfüllung ist. Genau das wiederum sei jedoch die Krux des „Zahlens mit Daten". Auch hier bestehe also Klärungsbedürfnis. Mit einem Blick über den deutschen Tellerrand, hinterfragte *Prof. Dr. Martin Ebers*, inwieweit das europäische digitale Vertragsrecht neue Technologien ausreichend berücksichtigt. Abschließend stellte *Prof. Dr. Felix Buchmann* einige Fallbeispiele zur Diskussion, um mit den Konferenzteilnehmer:innen die neuen Regelungen auf den Prüfstand zu stellen.

1.3 Modernisierung des Zivilprozesses

Nicht weniger aktuell ging es mit dem zweiten Panel zur Modernisierung des Zivilprozesses weiter.[1] Einleitend schilderte *Dr. Cord Brügmann* die sich ändernden Rahmenbedingungen für den Zivilprozess und stellte Thesen für die anschließende Diskussion auf. *Dr. Simon Heetkamp* ging daran anknüpfend auf konkrete Innovationsvorschläge ein. Die KI „FRAUKE", die einen Fluggastrechtefall bearbeiten könne, die eAkte und der Einsatz der Videoverhandlung nach § 128a ZPO hätten öffentliche Aufmerksamkeit erfahren. Darüber hinaus stünden jedoch weitere Projekte wie der Einsatz von Chatbots für Rechtsantragsstellen, Spracherkennung für Protokollierungen und digitale Klagewege im Diskurs. Bei der Digitalisierung der Justiz sei vor allem entscheidend, dass die Richterschaft sie proaktiv vorantreibe. Nur so könne Deutschland eine Spitzenposition in Europa erreichen. Dass diese aktuell eher das Nachbarland Österreich einnehme, dafür plädierte *Dr. Ermano Geuer*. Er erläuterte, welche digitale Möglichkeiten den österreichischen Alltag von Justiz, Bürger:innen und Anwaltschaft schon lang erleichtern. So zum Beispiel die Ende der 1980er Jahre geschaffene digitale Mahnklage. Zudem könnten Bürger:innen gerichtliche Bekanntmachungen online einsehen und seit 2013 mittels Webanträgen umfassend am E-Government teilnehmen.

1.4 Verantwortung von Medienintermediären

Zur Verantwortung der Medienintermediäre stellte Weizenbaum-Direktor *Prof. Dr. Christoph Neuberger* zunächst ihren Einfluss auf die digitale Öffentlichkeit und damit die liberale Demokratie heraus. Entscheidend sei die Verwirklichung von Werten wie Informations- und Diskursqualität, Vielfalt und Verteilung von Meinungsmacht. Hierbei zeigten sich Defizite, die durch legislative Maßnahmen aufgefangen werden sollen. Mit dem nationalen Netzwerkdurchsetzungsgesetz und dem Medienstaatsvertrag seien die Betreiber digitaler Plattformen bereits stärker in die Pflicht genommen worden. Mit dem Digital Services Act habe die Europäische Union 2022 nachgezogen. Daran anschließend widmete sich *Mireille Thierfelder* genau der Frage, ob der Medienstaatsvertrag mit seinen Maßnahmen zur Vielfaltssicherung ausreiche.[2] Das Ergebnis fiel zwiespältig aus. Von einer Querdenker:innenprivilegierung könne zwar keine Rede sein, vollends überzeugen können die Regeln zu Transparenz und Auffindbarkeit jedoch nicht. Unter Einbindung der anwesenden Expert:innen im Publikum entspann sich

1 Vgl. den Beitrag von *Heetkamp/Geuer* auf S. 14–20.
2 Vgl. den Beitrag von *Thierfelder* auf S. 21–37.

die anschließende Diskussion um Lösungsansätze aus Wissenschaft und von den Medienintermediären selbst.

1.5 Satelliten-Megakonstellationen

Die Nutzung des Weltraums erlebt eine Blüte und ist nicht nur geopolitisch von großer Bedeutung. Den spannenden Technologie- und Rechtsfragen rund um *Satelliten Mega-Konstellationen* widmeten sich *Prof. Dr. Enrico Stoll* und *Prof. Dr. Marcus Schladebach*.[3] Die Vorträge drehten sich darum, ob das aus den 1960er Jahren stammende Weltraumrecht auf diese Möblierung des Weltraums wirksame Antworten zu geben wisse. Insbesondere ob die wirtschaftliche Nutzungsfreiheit des Weltraums bestimmten Grenzen unterliege, gerade weil nicht mehr nur Staaten als klassische Akteure im Weltraum handeln, sondern zunehmend Privatunternehmen. Grenzen könnten sich aus Kapazitätsbeschränkungen für das Platzieren von Satelliten ergeben. Denn die Nutzbarkeit der Erdumlaufbahnen durch alle Staaten wäre erheblich gefährdet, wenn sämtliche Satellitenpositionen durch wenige Staaten/Unternehmen bereits besetzt wären.

1.6 Datenschutzrecht, Rechtsdurchsetzung und neue Phänomene

Im Kontext von KI und Big Data ergeben sich neue Herausforderungen für den Datenschutz durch sogenannte prädiktive Analytik. Aus philosophischer und rechtswissenschaftlicher Perspektive widmeten sich *Prof. Dr. Rainer Mühlhoff* und *Prof. Dr. Hannah Ruschemeier* diesem Vermögen großer Plattformunternehmen, Informationen über nahezu beliebige Datensubjekte vorherzusagen.[4] Hierbei kann es sich um Informationen handeln, die das betroffene Subjekt nicht wissentlich von sich preisgegeben hat und nicht willentlich von sich preisgeben würde. Die für die Vorhersagemethoden verwendeten Modelle könnten aus anonym verarbeiteten Daten von Social-Media-Nutzer:innen trainiert werden.

Und auch die Beschäftigung mit Online-Sachverhalten kann nicht ohne Datenschutz- und Datenrecht geschehen: Ob die aktuelle Rechtslage angemessen auf überindividuelle Datenschutzprobleme reagiert, hat *Marvin Gülker* hinterfragt.[5] Solche treten bei zahlreichen Datenverarbeitungsvorgängen auf – von der Videoüberwachung bis zur künstlichen Intelligenz. Er kam zu

3 Vgl. den Beitrag von *Schladebach* auf S. 68–75.
4 Vgl. den Beitrag von *Mühlhoff/Ruschemeier* auf S. 38–67.
5 Vgl. den Beitrag von *Gülker* auf S. 76–100.

dem Ergebnis, dass der Gesetzgeber tätig werden müsse, um seine Schutzpflicht für das Recht auf informationelle Selbstbestimmung zu wahren. Ob Maßnahmen, wie die KI-Verordnung sie vorsehe, angemessene Lösungsansätze seien, müsse sich noch im rechtspolitischen Diskurs zeigen.

1.7 Abschottung des Internets: Regulierung und Rechtsdurchsetzung

Dem wohl Tagesaktuellsten widmeten sich *Prof. Dr. Christian-Henner Hentsch*, *Prof. Dr. Tobias Keber* und *Daniela Beaujean*. Sie diskutierten die geopolitischen Auswirkungen des Russisch-Ukrainischen Krieges auf das Internet und seine zunehmende Zersplitterung. Schon längere Zeit lasse sich eine Zersplitterung des Internets in unterschiedlich geregelte und regulierte Räume betrachten. Laut *Prof. Dr. Christian-Henner Hentsch* würden Regulierungsziele sich derzeit aber verschieben: Bislang habe die Internetregulierung zunächst die Ermöglichung im Blick gehabt (Providerprivileg in der eCommerce-RL), danach die Rechtsdurchsetzung (Enforcement-RL) und dann vor allem den Verbraucherschutz (NetzDG/DSA). Fraglich sei, ob künftig wohl auch ein weiteres Regulierungsziel „Demokratieschutz" hinzukäme. Jedenfalls würden neue legitime Regulierungszwecke auftauchen: Die Medienfreiheiten z. B. dürfen nur aufgrund von legitimen Zwecken eingeschränkt werden (Art. 10 EMRK). Das waren bislang vor allem die Rechte Dritter oder die öffentliche Sicherheit. Der Krieg mache jedoch deutlich, dass künftig wohl auch mehr die „territoriale Unversehrtheit" und „nationale Sicherheit" zu berücksichtigen sein könnte. Es lasse sich generell beobachten, dass die Aufsicht gestärkt werde: Internetregulierung hat bislang vor allem auf Pflichten und Haftung gesetzt und vielfach die Rechtsdurchsetzung „privatisiert". Das jüngste Beispiel hierfür sei die Clearingstelle Urheberrecht im Internet (CUII). Die Fälle RT DE und xHamster zeigten nun, dass die Regulierer aktiver werden – befördert durch die EU.

Prof. Dr. Tobias Keber betonte, dass der free flow of information kein absolutes Konzept sei. Das gelte für die nationale wie die internationale Ebene. Bei den Einschränkungen sei sorgsam zu differenzieren, ob individuelle Rechte (wie im Urheberrecht, z. B. bei der CUII), oder ein Staatsprinzip (wie die Demokratie) geschützt werden solle. Die Medien- und Kommunikationsfreiheiten dienen der Demokratie, schützen sie aber nur mittelbar. Ein auf dieser Grundlage begründetes Demokratiesicherungsrecht müsse prinzipienorientiert sein (Stichworte: Staatsferne und Pluralismus), aber außerhalb der Grenzen einer wehrhaften Demokratie (Art. 18 GG) nicht eingriffsorientiert. Informationsblockaden (auch wenn sie als Desinformationssperren gedacht seien) zum Schutz der Demokratie können nur ultima ratio sein und

bedürfen wirksamer verfahrensrechtlicher Garantien, was beispielsweise beim neuen Crisis Response Mechanism im Digital Services Act nicht der Fall sei.

Daniela Beaujean machte noch einmal deutlich, dass effektive Rechtsdurchsetzung im Internet trotzdem zur Aufrechterhaltung der Kreativ- und Medienwirtschaft erforderlich sei und zu Verwirklichung und Erhalt von Demokratien beitrage. Denn Informations-, Medien- und Meinungsfreiheit seien Kernbestandteil demokratischer Gesellschaften. Zur Sicherung kommunikativer Grundfreiheiten blieben aber Unabhängigkeit und Staatsferne essentiell, v. a. auch vor dem Hintergrund aktueller geopolitischer Fragen.

1.8 Influencer Marketing

Der BGH hat bereits fünfmal über Influencer-Marketing-Fälle entschieden.[6] Doch mit dem stetigen Auftauchen neuer Typen von Influencer:innen treten auch neue rechtliche Fragen auf. Passend dazu nahm *Marie Theres Neubauer* die Werbung sogenannter „Pharma-Influencer:innen" unter die Lupe.[7] Sie analysierte, inwieweit neben TMG, UWG und BGH-Urteilen das Heilmittelwerbegesetz hinreichende Kennzeichnungspflichten begründet. Solche seien vor allem bei verschreibungspflichtigen Medikamenten notwendig. Zwar fielen Influencer:innen wohl unter den Wortlaut des § 11 Abs. 1 S. 1 Nr. 2 HWG, der Werbung für OTC-Medikamente durch Prominente verbietet. Ob die Gesetzgebung dies künftig bestätige, sei aber aufgrund der wirtschaftlichen Bedeutung des Geschäftsmodells fraglich. Jedenfalls seien in Anbetracht der besonderen Schutzbedürftigkeit bereits erkrankter Verbraucher:innen bestehende Rechtsunsicherheiten zu beseitigen.

Den Bogen zurück zu allgemeinen Rechtspflichten im Influencer Marketing spannte *Prof. Dr. Marcus Schladebach* mit einem Interview mit *Dr. Martin Gerecke*. *Gerecke* sprach dabei insbesondere über sogenannte Corporate Influencer. Dabei sei zu unterscheiden zwischen angeleiteten, vertraglich umrissenen Influencer:innen der Unternehmen und Mitarbeiter:innen, die von sich aus Werbung für ihr Unternehmen machen, sogenannte organische Corporate Influencer. Gewisse Pflichten, wie z. B. Kennzeichnung von werbenden Beiträgen, herrschten für beide Arten. Auch seien Guidelines und verbindliche Absprachen für die Unternehmen sinnvoll. Schließlich müssten jeweils noch die technischen wie rechtlichen Besonderheiten der unterschiedlichen Kanäle beachtet werden.

6 Vgl. den Beitrag von *Lefeldt* auf S. 101–106.
7 Vgl. den Beitrag von *Neubauer* auf S. 107–114.

1.9 Ausstellungsbereich und Abendprogramm

Um Austausch und Inspiration zwischen Referent:innen und Besucher:innen noch mehr zu erhöhen, bot die Soko22 eine Ausstellungsfläche für Poster und Präsentationen.[8] Dort präsentierten Forscher:innen, Aktivist:innen und Start Ups mit engem Bezug zu IT, Jura und Medien ihre Projekte – u. a. zu KI, Avataren und Rechtsöffentlichkeit. Zum Ausklang des ersten Abend ließen die Teilnehmer:innen bei „Drinks and Games“ in den Räumen des Game Verbands gemeinsam die Eindrücke des ersten Tages Revue passieren und tauschten sich über Ideen und Projekte aus.

8 Vgl. den Beitrag von *Hünting* auf S. 216–223.

§ Telemedicus

Sommerkonferenz

Freitag, 8. Juli 2022

Uhrzeit	Lichthof	Meeting-Raum
9.00	**Begrüßung & Telemedicus Awards** *– Adrian Schneider & Dr. Guido Brinkel*	
9.30 – 10.00	**Keynote: Digital- und Datenpolitik** *– Benjamin Brake*	
10.00 - 11.30	**Digitales Vertragsrecht** *– Dr. Anna K. Bernzen, Dr. Zuhal Ayar, Prof. Dr. Martin Ebers & Prof. Dr. Felix Buchmann*	
11.30 - 12.30	**Modernisierung des Zivilprozesses** *– Prof. Dr. Giesela Rühl, Dr. Simon J. Heetkamp, Dr. Ermano Geuer & Dr. Cord Brügmann*	
12.30 - 13.15	*Mittagspause*	
13.15 - 14.15	**Verantwortung von Medienintermediären** *– Prof. Dr. Christoph Neuberger, Dr. Stephan Dreyer & Mireille Thierfelder*	**Prediktive Privatheit** *– Prof. Dr. Rainer Mülhoff & Prof. Dr. Hannah Ruschemeier*
14.15 - 15.15	**Satelliten-Megakonstellationen** *– Prof. Dr. Marcus Schladebach & Prof. Dr. Enrico Stoll*	**Überindividuelles Datenschutzrecht** *– Marvin Gülker*
15.15 - 15.45	*Kaffeepause*	
	... Fortsetzung nächste Seite ...	

Anmeldung & ausführliches Programm unter telemedicus.info/soko22

weizenbaum institut · HÄRTING · DORNKAMP · game · Medienpartner: Kommunikation & Recht · iRights.Lab · Osborne Clarke · Bird&Bird · SKW Schwarz · MORRISON FOERSTER

§ Telemedicus

Sommerkonferenz

Freitag, 8. Juli 2022

Uhrzeit	Lichthof	Meeting-Raum
	...	
15.15 - 15.45	*Kaffeepause*	
15.45 - 16.45	**Abschottung des Internets: Regulierung und Rechtsdurchsetzung** *– Prof. Dr. Christian-Henner Hentsch, Prof. Dr. Tobias Keber & Daniela Beaujean*	*Aufbau der Ausstellungsfläche*
16.45 - 17.45	**Influencer Marketing** *– Stefanie Lefeldt, Dr. Martin Gerecke & Marie-Theres Neubauer*	**Ausstellung: Poster, Stände & Technologie** *– s. Seite 4*
17.45 - 18.45	**Ausklang & Ausstellungspräsentation**	
	Ortswechsel	
Ab 19.00	**Drinks and Games** *– Game e.V.* *Friedrichstraße 165, 10117 Berlin*	

Anmeldung & ausführliches Programm unter telemedicus.info/soko22

weizenbaum institut · HÄRTING · DORNKAMP · game · Medienpartner: Kommunikation & Recht · iRights.Lab · Osborne Clarke · Bird&Bird · SKW Schwarz · MORRISON FOERSTER

1.10 Tag zwei: e-sportlicher Auftakt

Den Auftakt für den zweiten Konferenztag boten *Dr. Holger Jakob* und *Conrad S. Conrad* mit Beiträgen im Bereich eSports. *Conrad S. Conrad* befasste sich mit den Betroffenenrechten der DSGVO im eSport.[9] Dabei seien vor allem Auskunfts- und Löschansprüche sowie ein Recht auf Datenübertragbarkeit in einen neuen Account zu bedenken. Bislang habe das Thema in der Gaming-Szene keine große Aufmerksamkeit erfahren. In Anbetracht drohender Bußgeldsanktionen appellierte *Conrad* jedoch an die Akteur:innen, sich mit den Betroffenenrechten auseinanderzusetzen und Prozesse zum Umgang mit diesen zu entwickeln. Eine weitere spannende Frage stellt sich, wenn der Account eines/einer Spieler:in infolge eines Verstoßes (z. B. Cheating oder Hate Speech) gesperrt wird. Inwiefern Spieler:innen in einem solchen Fall Rechtsschutz genießen, hat *Dr. Holger Jakob* analysiert. Übertrage man die BGH-Rechtsprechung zu Facebook-Profilsperrungen, die Anforderungen an den Ablauf einer Sperrung stelle, müsse den Spieler:innen häufig ein Anspruch auf Freischaltung zustehen. Kartellrechtliche Schutzmöglichkeiten bestünden nur, wenn dem/der Game-Anbieter:in eine marktbeherrschende Stellung zukäme. Doch ob sich im eSport ein kartellrechtlich relevanter Markt abgrenzen ließe, sei nur eine von vielen noch offenen Fragen.

1.11 DSA und DMA

Nur wenige Tage vor der Soko22 verabschiedete das Europaparlament das Digitalpaket – bestehend u. a. aus dem Digital Services Act (DSA) und dem Digital Markets Act (DMA). Der DSA soll den Umgang mit illegalen Inhalten und Hatespeech auf digitalen Plattformen regeln und der DMA die Marktmacht von Internetriesen einhegen. *Dr. Christoph Krück* und *Johannes Schäufele* überprüften die Auswirkungen der neuen Gesetze auf Internetgiganten sowie mittlere und kleine Unternehmen. Ob sich DSA und DMA in ihrem Umfang und Detail positiv für alle Beteiligten auswirkt, sei noch nicht abzusehen. Ein Beitrag, der nicht passender und aktueller hätte sein können.

9 Vgl. den Beitrag von *Conrad* auf S. 115–128.

1.12 Hardwaresouveränität: Lieferkettenregulierung & Chips Act

Nach der anschließenden Kaffeepause ging es sodann weiter mit dem nächsten hochaktuellen EU-Rechtsakt. *Reinhold Beckmann* und *Prof. Dr. Dennis-Kenji Kipker* setzten sich in ihrem Vortrag mit dem im Februar 2022 durch die EU-Kommission vorgestellten *EU Chips Act* kritisch auseinander.[10] Der Rechtsakt adressiere ein Thema, dessen Problematik sich insbesondere in den letzten zwei Jahren offenbart habe. Denn spätestens mit Ausbruch der Corona-Pandemie wurde klar, dass globale Umbrüche erhebliche Folgen auf die Verfügbarkeit von vertrauenswürdiger Hardware haben können. Die sichtbarsten Folgen seien Lieferengpässe sowie eine schwindende Cybersecurity. Nach Vorstellung des neuen Regelungsinstrumentes gehe es insbesondere um die Frage, ob durch den Chips Act tatsächlich eine europäische Hardwaresouveränität erlangt werden kann, oder lediglich ein rechtlicher sowie wirtschaftlicher Mehraufwand für Unternehmen geschaffen wird.

1.13 IT-Security

Anschließend griff *Markus Drenger* das Thema IT-Security aus einer praxisnahen Perspektive auf. In seinem Vortrag ging er auf eine Situation ein, in welcher sich immer mehr Organisationen wiederfinden, nämlich Cyberattacken. Anhand des 1x1 der Cyber Incident Response präsentierte er, wie Ramsomware-Gruppierungen und -Angriffe funktionieren und welche Rolle das Darknet dabei spielt. Abschließend stellte er dar, was Betroffene im Falle eines Ramsomware-Angriffs stets tun bzw. unterlassen sollten.

1.14 NFT

Ein heiß diskutiertes Phänomen stellen sogenannte Non Fungible Tokens (NFT) dar.[11] *Patricia Ernst* und *Susan Bischoff* beantworteten die Fragen, ob es sich nur wieder um ein neues Buzzword oder eine echte Chance für den Kunst- und Filmmarkt handelt. Festzuhalten bliebe, dass es sich um einen wirtschaftlich bedeutsamen Faktor handelt. Ob es sich um valide Investitionsgüter handele, müsse der Markt noch zeigen. Auch rechtlich sei noch nicht durchentschieden, wie die nicht übertragbaren Wertmarken einzuschätzen seien. Feststehe nur, dass sie jedenfalls dem/der jeweiligen Urheber:in zustehen würden.

10 Vgl. den Beitrag von *Kipker* auf S. 129–137.
11 Vgl. den Beitrag von *Stützle/Ernst/Bischoff* auf S. 156–178.

1.15 Metaverse

Auch das Thema Web 3.0 bzw. Metaverse kann wohl nur interdisziplinär sinnvoll angegangen werden. Nachdem Weizenbaum-PI *Prof. Dr. Stefan Schmid* die technischen Grundlagen der Blockchain, Verschlüsselung und der Extended reality (XR) erläutert hatte, widmete sich *Prof. Dr. Boris Paal* den kartellrechtlichen Fragen.[12] Entscheidend sei der Umgang mit Daten und Künstlicher Intelligenz (KI), denn auch Cloud Computing müsse nicht unsicher sein. Kartellrechtlich relevant sei dann wiederum die Gewährleistung von fairem Marktzugang, insbes. für neue Akteur:innen. Dabei müsse sich auf technische Standards zur Interoperabilität verständigt werden. Hingewiesen sei insbesondere auf das Verbot wettbewerbsbeschränkender Vereinbarungen. Internes Wachstum sei allerdings nicht vom Kartellrecht erfasst.

1.16 Federated Learning & Federated Platforms

Ebenso interdisziplinär stellten *Leo Dessani* und *Maximilian Leicht* eine neue Chance für datenschutzfreundliche KI vor.[13] Das sogenannte Federated Learning biete eine Möglichkeit der dezentralen Datenverarbeitung im Machine Learning. Dadurch entfielen zwar nicht gänzlich datenschutzrechtliche Verpflichtungen, jedoch reduziere sich das Risiko für Betroffene durch die ausgelagerte Trainingsphase. Die beiden Referenten erläuterten die technischen Grundlagen und bewerteten diese im Hinblick auf ihre Chancen, Risiken und datenschutzrechtliche Folgen.

Bedeutend in puncto Dezentralisierung war auch der Beitrag von *Rebecca Sieber* zu Föderierten Plattformen.[14] Das sind soziale Netzwerke, die Nutzer:innen unabhängig von Unternehmen auf Open Source Software entwickeln, verbreiten und kontrollieren. Infolge offener Standards können Nutzer:innen netzwerkübergreifend im „Fediverse" miteinander kommunizieren. Rechte und Pflichten der Betreiber:innen einer Instanz bestimmen u. a. das Vertragsrecht, NetzDG und Datenschutzrecht. Da noch viel Rechtsunsicherheit herrsche, habe dies jedoch teils zu rigoroser Moderation geführt. Zu begrüßen sei allerdings die Selbstbestimmtheit von Internetdiskussion, die solche Plattformen vorantreiben.

12 Vgl. den Beitrag von *Pignolet/Schmid* auf S. 179–185 und den Beitrag von *Paal* auf S. 186–195.

13 Vgl. den Beitrag von *Leicht/Dessani* auf S. 196–210.

14 Vgl. den Beitrag von *Sieber* auf S. 138–155.

§ Telemedicus

Sommerkonferenz

Sonnabend, 9. Juli 2022

Uhrzeit	Lichthof	Meeting-Raum
10.00 - 10.45	**eSports: Accountsperren & DSGVO-Betroffenenrechte** *– Dr. Holger Jakob & Conrad S. Conrad*	**Ausstellung: Poster, Stände & Technologie** *– s. Seite 4*
10.45 - 11.30	**Digital Markets Act & Digital Services Act in der Praxis** *– Dr. Christoph Krück & Johannes Schäufele*	**Ausstellung: Poster, Stände & Technologie** *– s. Seite 4*
11.30 – 12.00	*Kaffeepause*	
12.00 – 12.45	**Hardwaresouveränität: Lieferkettenregulierung & Chips Act** *– Reinhold Beckmann & Prof. Dr. Dennis-Kenji Kipker*	**Föderierte Plattformen** *– Rebecca Sieber*
12.45 - 13.30	**Non Fungible Tokens** *– Christiane Stützle, Patricia Ernst & Susan Bischoff*	**IT-Security: Das 1x1 der Cyber Incident Response** *– Markus Drenger*
13.30 – 14.15	*Mittagssnack*	
	… Fortsetzung nächste Seite …	

Anmeldung & ausführliches Programm unter telemedicus.info/soko22

Medienpartner: Kommunikation & Recht

§ Telemedicus

Sommerkonferenz

Sonnabend, 9. Juli 2022

Uhrzeit	Lichthof	Meeting-Raum
	…	
13.30 – 14.15	*Mittagssnack*	
14.15 – 15.00	**Technik & Recht: Metaverse** *– Prof. Dr. Stefan Schmid & Prof. Dr. Boris Paal*	**Federated Learning als Chance für datenschutzfreundliche KI** *– Max Leicht & Leo Dessani*
15.00 - 15.45	**Ausbildung und Legal Tech** *– Dr. Christina-Maria Leeb, Dr. Christian Schlicht, Til Bußmann-Welsch & Jolanda Rose*	
15.45 - 16.00	*Abschied*	
	… Fortsetzung folgt?	

Ausstellung: Poster, Stände & Technologie		
Poster	**iur.crowd**	*Frederik Tholey & Til Bußmann-Welsch*
Poster	**Cybersyn**	*Sarah Hünting*
Poster	**Copresence Avatare**	*Radek Makowiak*
Stand	**ZVKI KI-osk**	
Stand	**Automatisierungs-Demystifizierungs-Diskurs-Maschine**	*Karla Herb & Ertugrul Can*
Poster	**…**	

Medienpartner: Kommunikation & Recht

1.17 Legal Tech und Ausbildung

Passend zum Abschluss warf die letzte Paneldiskussion einen Blick auf Realität und Zukunft für heranwachsende Jurist:innen.[15] *Dr. Christina Maria Leeb*, *Til Martin Bußmann-Welsch* und *Dr. Christian Schlicht* debattierten über „Erneuerungen der juristischen Ausbildung durch Legal Tech", moderiert von *Jolanda Rose*. Dabei untersuchten die Panelist:innen, die alle im Rahmen verschiedener Legal-Tech-Projekte aktiv sind, eine Fülle von Reformansätzen. Dass Legal-Tech-Veranstaltungen in die universitäre Ausbildung gehörten, darüber waren sich alle einig. Ob Studierende solche freiwillig oder im Rahmen des Pflichtfachkatalogs besuchen sollten, wurde kontrovers debattiert. Auch in puncto Staatsexamen bestünde Reformbedarf. Der Ablauf sei stärker an die Realität des juristischen Berufsalltags anzugleichen. Dazu wurden u. a. das „E-Examen" oder ein Zugriff auf juristische Datenbanken in den Prüfungen debattiert.

15 Vgl. den Beitrag von *Leeb/Bußmann-Welsch/Schlicht* auf S. 211–215.

2 Modernisierung des Zivilprozesses

*Simon Heetkamp & Ermano Geuer**

Die Modernisierung des Zivilprozesses ist derzeit in aller Munde. Das entsprechende Panel gab Raum für Impulsvorträge zum Status Quo der Digitalisierung der Justiz und zu den entsprechenden Modernisierungsbestrebungen in Deutschland und Österreich.

2.1 Modernisierungsbestrebungen im deutschen Zivilprozess

2.1.1 Status Quo

Häufig konnte man in den letzten Jahren den Eindruck gewinnen, es gäbe in der Justiz nur zwei Digitalisierungsthemen: die Einführung der eAkte & des elektronischen Rechtsverkehrs einerseits und die mündliche Verhandlung im Wege der Bild- und Tonübertragung, § 128a ZPO andererseits. Dass dies selbstverständlich nicht der Fall ist, belegt auch ein Blick in das Grundlagenpapier zur 74. Jahrestagung der Präsidentinnen und Präsidenten der Oberlandesgerichte, des Kammergerichts, des Bayerischen Obersten Landesgerichts und des BGH vom 23.–25.5.2022 mit dem Titel „Einsatz von KI und algorithmischen Systemen in der Justiz“.[1]

Das Grundlagenpapier listet u. a. auch die laufenden und geplanten Projekte in der deutschen Justiz zu KI und Algorithmen auf.[2] Zu diesen gehören:

- Automatisierte Anonymisierung von Gerichtsentscheidungen
- Semantische Metadatengewinnung und Textanalyse
- Tools zur verbesserten Aktendurchdringung (etwa automatische Erstellung eines Zeitstrahls; Textvergleich; Normverweisanalyse)
- Spracherkennung für Protokollierungen
- Chatbot für Rechtsantragsstelle

---

* Mehr über die Autor:innen erfahren Sie im Autor*innenhinweis auf S. 224 ff.

1 Online abrufbar unter: https://www.justiz.bayern.de/media/images/behoerden-und-gerichte/oberlandesgerichte/nuernberg/einsatz_von_ki_und_algorithmischen_systemen_in_der_justiz.pdf.

2 Siehe Anhang zum Grundlagenpapier. Für weitere Informationen zu KI-Anwendungen in der Justiz siehe auch: *Heetkamp/Schlicht*, Veranstaltungsbericht zum Symposium „Künstliche Intelligenz in der Justiz“, abrufbar unter: https://www.legal-tech.de/kuenstliche-intelligenz-in-der-justiz/.

- KI-Unterstützung für die Bearbeitung von Massenverfahren[3]

Viele weitere Digitalisierungs- und Modernisierungsvorschläge werden derzeit intensiv – und teils sehr kontrovers – diskutiert, u. a.:[4]

- Digitalisierung der Gerichtsöffentlichkeit
- Strukturierung des Parteivortrags im Basisdokument
- Digitale Klagewege
- Open Legal Data/Veröffentlichung von Gerichtsentscheidungen

Dabei ist festzustellen, dass KI schon in den Justizalltag dringt. So wurde in Presseberichten die neue Kollegin am AG Frankfurt a. M., FRAUKE, vorgestellt. FRAUKE steht dabei für „Frankfurter Urteils Konfigurator elektronisch" und ist eine KI, die die Richterinnen und Richter bei der Bearbeitung von Fluggastrechteklagen unterstützen soll.[5] Dabei wird der nun anstehende Praxistest zeigen, ob und wie gut die KI die Bearbeitung eines Falles leisten kann – etwa, wenn außergewöhnliche Fallkonstellationen vorliegen wie mehrfache Probleme bei der Flugabwicklung (Streik und Vogelschlag), sprachlich missverständliche Ausführungen (Anwalt, der mit Dragon diktiert, so dass statt „Vogelschlag" das Wort „Vorschlag" im Schriftsatz erscheint) oder widersprüchlicher Parteivortrag oder Anlagen, die nicht zum schriftsätzlichen Vortrag passen. Auch werden sich interessante Folgefragen stellen: Wie können/werden Legal Tech-Unternehmen auf die gerichtliche KI reagieren? Und: Wird – insbesondere bei regelmäßig überzeugenden Urteilsentwürfen der KI – die Gefahr entstehen, dass Richterinnen und Richter die Sachverhalte nicht mehr selbst ausreichend durchdringen?

2.1.2 Die „digitale richterschaft"

Anfang des Jahres 2022 haben *Dr. Simon J. Heetkamp* und *Dr. Christian Schlicht* (beide Richter am LG Köln) die „digitale richterschaft" gegründet.[6] Denn, während man im Bereich Legal Tech viele Veranstaltungen und Vereinigungen unter Federführung der Anwaltschaft und freien Wirtschaft

3 Siehe zu nicht technikbasierten Vorschlägen zum Umgang mit Massenverfahren die Initiativstellungnahme des Deutschen Richterbundes zur besseren Bewältigung von Massenverfahren in der Justiz, Mai 2022, online abrufbar unter: https://www.drb.de/fileadmin/DRB/pdf/Stellungnahmen/2022/DRB_220513_Stn_Nr_1_Massenverfahren.pdf.

4 Siehe zu weiteren Digitalisierungsthemen in der Justiz: *Schlicht/Heetkamp*, „Legal Tech in der Zivilgerichtsbarkeit – Chancen und Herausforderungen" – Ein Tagungsbericht, online abrufbar unter: https://www.legal-tech.de/legal-tech-in-der-zivilgerichtsbarkeit-tagungsbericht-teil-1/.

5 Siehe etwa: https://www.hessenschau.de/panorama/amtsgericht-frankfurt-kuenstliche-intelligenz-hilft-bei-massen-urteilen,amtsgericht-roboter-100.html.

6 Mehr Informationen unter: www.digitale-richterschaft.de.

findet, fehlte bisher ein Forum für Richterinnen und Richter zum Austausch über Digitalthemen und Innovationsprozesse in der Justiz. Die „digitale richterschaft“ möchte genau diese Plattform bieten, um einen (maßgeblich justizinternen) Austausch innerhalb des digitalaffinen Kolleg:innenkreises über die neuesten Technologieentwicklungen in der Justiz zu ermöglichen. Die Denkfabrik strebt eine bundesweite Vernetzung technikaffiner Richterinnen und Richter aller Gerichtsbarkeiten sowie von Staatsanwältinnen und Staatsanwälten an. Für die von der „digitalen richterschaft“ angebotene Mailingliste haben sich schon über 200 Personen angemeldet. Die Mailingliste gibt allen Beteiligten die Möglichkeit, auf (eigene) Veröffentlichungen, Veranstaltungen und Vorträge hinzuweisen, Fragen zu stellen, Themen für den künftigen Austausch vorzuschlagen und vieles mehr. Des Weiteren ist geplant, richterliche Digitalpaten für spezifische Digitalisierungsthemen zu benennen.

Die bisherigen Online-Vortragsveranstaltungen betrafen unter anderem folgende Themen:

- „Herausforderungen von Massenverfahren in der gerichtlichen Praxis“ (Richterin am AG Erding *Krzizok*) mit einem Fokus auf (digitale) Verbesserungsmöglichkeiten, um die gerichtliche Tätigkeit besser auf Massenverfahren vorzubereiten.
- „Einsatz von Virtual Reality-Technologie im Zivilverfahren“ (Richter am LG *Dr. Simon J. Heetkamp*)

Dass die einzelne Richterin bzw. der einzelne Richter für die Digitalisierung der Justiz von herausragender Bedeutung sein kann, zeigt auch ein Blick auf § 128a ZPO, der zwar seit gut 20 Jahren im Gesetz zu finden ist, aber vor der Corona-Pandemie kaum genutzt wurde. Eine Ausnahme ist eine Kollegin vom LG Hannover, *Gesine Irskens*, die schon seit 2017 die mündliche Verhandlung im Wege der Bild- und Tonübertragung in zahlreichen Verfahren anwandte,[7] so dass ihr Gericht durch die bestehenden Erfahrungen und die technische Ausstattung schneller auf die Corona-Pandemie durch vermehrte Videoverhandlungen reagieren konnte. Auch wenn es keine belastbaren, landes- oder bundesweiten Statistiken zum Einsatz von Videoverhandlungen gibt, so ist mit Blick auf die zugänglichen Zahlen davon auszugehen, dass in weniger als 20 % der Zivilverfahren eine Videoverhandlung stattfindet.[8]

---

7 Siehe auch *Irskens*, Betrifft: JUSTIZ 2020, 281.

8 Siehe etwa *Kaufmann*, lto.de vom 16.12.2020, „Gerichte wollen, Anwälte nicht – oder andersrum?“, online abrufbar unter: https://www.lto.de/recht/justiz/j/video-verhandlungen-128a-zpo-online-verfahren-gerichte-anwaelte-antrag-abgelehnt-ermessen-corona/, die für das LG Hannover eine Schätzung von 20 % angibt berichtet, dass am LG Dresden keine einzige Videoverhandlung durchgeführt wurde und das LG Bremen Videoverhandlungen nur in Einzelfällen einsetzt.

Dabei schätzen die Richterinnen und Richter selbst das Potenzial für Videoverhandlungen deutlich höher ein.[9]

2.1.3 Ausblick

Es kann mit einiger Sicherheit angenommen werden, dass der deutsche Zivilprozess in fünf bis zehn Jahren nicht mehr wiederzuerkennen ist. Für die Digitalisierung der Justiz wird auch entscheidend sein, dass sie von den Richterinnen und Richtern mitgetragen statt nur „ertragen" wird – das setzt voraus, dass die richterliche Arbeit durch die digitalen Tools objektiv und subjektiv besser wird.

Es ist zu hoffen, dass sich die Justiz an die Spitze der Digitalisierung stellt. Dazu gehört neben einer entsprechenden Haltung auch, dass Digitalthemen (wie etwa der Einsatz von Virtual-Reality-Technologie oder Augmented-Reality-Technologie) proaktiv vorangetrieben werden.

2.2 Der Blick nach Österreich

2.2.1 Einleitung

Österreich nimmt bei der Digitalisierung des Zivilprozesses eine gewisse Vorreiterrolle in Europa ein und begann bereits in den 1980ern damit, innovative Wege zu beschreiten. Nachfolgend sollen einige Meilensteine der Digitalisierung des Zivilprozesses aus österreichischer Sicht vorgestellt werden.

2.2.2 Einführung des elektronischen Rechtsverkehrs (sog. ADV-Mahnklage)

Erste Schritte zur Digitalisierung wurden bereits Ende der 1980er Jahre mit der Einführung der digitalen Mahnklage gesetzt.[10] Diesen gingen fast zehn Jahre Vorarbeiten voraus. Als technischer Partner wurde die Radio Austria AG (heute Teil der Telekom Austria) gewonnen und der Testbetrieb zum 1.1.1990 aufgenommen. Eine Triebfeder war die Einsparung von Portokosten.[11] Die Übermittlung fand über eine dafür entwickelte Software statt. Das österreichische Justizministerium bezeichnet die Einführung des elektroni-

9 Bei *Duhe/Weißenberger*, RDi 2022, 176, 178 schätzen Richterinnen und Richter 20–40 % der Verhandlungen als für Videoverhandlungen geeignet ein.

10 Verordnung des Bundesministers für Justiz vom 4.12.1989 über den elektronischen Rechtsverkehr (ERV), BGBl 1989/600.

11 ADV-Mahnklage: Wie funktioniert das? „Netzwerk Justiz": Elektronischer Rechtsver-

schen Rechtsverkehrs (ERV) zu diesem Zeitpunkt als weltführend.[12] Im Jahr 1999 kam der Rückverkehr durch Gerichte dazu, also die Möglichkeit, auch an Anwälte elektronisch zuzustellen.[13] Die Nutzung war freiwillig.

2.2.3 Einführung des Web-ERV

Während es gelungen war, das Mahnwesen weitgehend zu digitalisieren, lief die Übermittlung aller anderen Schriftsätze weiterhin postalisch. Der heutige ERV wurde unter dem Schlagwort „web-ERV" im Jahr 2007 begonnen. Dieser ermöglichte eine Einbringung sämtlicher Schriftsätze bei Gericht und einen entsprechenden Rückverkehr. Die Verordnung ERV 2006, welche mehrfach überarbeitet wurde, hat im Grunde immer noch Gültigkeit.[14] Anwält:innen und Notar:innen müssen den web-ERV benutzen, ebenso wie mittlerweile Banken und Versicherungen. Der web-ERV ist in gängige österreichische Anwaltssoftwares eingebaut, es gibt auch Anbieter:innen, die ein web-Interface für professionelle Nutzer:innen anbieten.

Der in den 2000er-Jahren vollzogene Schritt weg von Papier hin zur digitalen Einbringung von Schriftsätzen und zur digitalen Zustellung wurde auch zum Anlass genommen, das Grundbuch und das Firmenbuch (Handelsregister) vollständig zu digitalisieren.

Als weiterer Schritt wurde 2013 noch der sogenannte „ERV für alle" eingeführt.[15] Aufgrund der im Vergleich zu Deutschland wesentlich größeren Verbreitung digitaler Signaturen auf Mobilgeräten (sog Handysignatur), bestand für Bürger:innen damals bereits ein einfacher Weg zur Teilnahme am E-Government. Der ERV für alle wird als reines Uploadservice betrieben, also ohne Zustellmöglichkeit der Justiz an den Bürger:innen. Bürger:innen können über den ERV für alle einfache Anträge über Webformulare einbringen. Die Palette reicht von familienrechtlichen Anträgen (z. B. betreffend Adoptionen) über einfache Grundbuchsachen (z. B. Adresskorrekturen) bis hin zu Mahnklagen.

---

kehr im Justizbereich Verordnung des Bundesministers für Justiz vom 4.12.1989 über den elektronischen Rechtsverkehr (ERV), BGBl 1989/600, EDVuR 1989, 110.

12 https://www.justiz.gv.at/home/service/digitale-justiz/elektronischer-rechtsverkehr-(erv).967.de.html.

13 Die Teilnahme war damals freiwillig, es wurden aber bereits 40 % der Mahnklagen im Jahr 1998 auf diese Weise eingebracht; vgl. *Benn-Ibler*, AnwBl 1998, 597.

14 Verordnung der Bundesministerin für Justiz über den elektronischen Rechtsverkehr (ERV 2006), BGBl. II Nr. 481/2005.

15 Plattform abrufbar unter eingaben.justiz.gv.at.

2.2.4 Ediktsdatei

Als weiteres Positivbeispiel der Digitalisierung der Justiz in Österreich ist die Ediktsdatei zu nennen,[16] in der gerichtliche Bekanntmachungen online veröffentlicht werden. Auch hier begann die Veröffentlichung zunächst im Insolvenzbereich.

Mittlerweile umfasst die Ediktsdatei Bekanntmachungen aus dem familienrechtlichen und personenstandsrechtlichen Bereich, Bekanntmachungen der Grundbuchsgerichte, erbrechtliche Bekanntmachungen und Bekanntmachungen zur Kraftloserklärung von Urkunden. Auch Zustellungen werden über die Homepage bekannt gemacht. Ein Aushang bei Gericht ist nicht mehr erforderlich.

2.2.5 Einsatz von Videokonferenzen im Zivilprozess

Schließlich ist noch die technische Modernisierung der Justiz in Österreich hervorzuheben. Die verfahrensrechtlichen Voraussetzungen für Videovernehmungen bestehen seit 2005. Seit 2011 sind sämtliche Gerichte, Staatsanwaltschaften und Justizanstalten mit Videokonferenzanlagen ausgestattet. Im Jahr 2019 wurden bundesweit rund 4500 Videokonferenzen abgehalten, davon 11 % grenzüberschreitend.[17]

Während der Coronapandemie waren damit die technischen Voraussetzungen für Videoverhandlungen bereits von Anfang an gegeben. Die rechtlichen Voraussetzungen wurden im Covid19-Justizbegleitgesetz für die Dauer der Pandemie geschaffen.[18]

Die Regelung gilt zunächst befristet bis 31.12.2022, zurzeit sind Videokonferenzen nach § 277 öZPO nur vorgesehen als Hilfsmittel zur Beweisaufnahme. Es bestehen Überlegungen, Videoverhandlungen dauerhaft in die öZPO zu übernehmen. Ein Gesetzesentwurf in diese Richtung wurde aber vorerst noch zurückgezogen.

2.2.6 Fazit

Österreich hat sehr früh mit der Digitalisierung des Zivilprozesses begonnen. Die Erfolge sind beachtlich und bringen zahlreiche Erleichterungen für Justiz, Bürger:innen und Anwaltschaft. Es bleibt zu hoffen, dass auch beim Einsatz künstlicher Intelligenz und anderer moderner Technologien diese

16 https://edikte.justiz.gv.at/.

17 Vgl. hierzu die Broschüre „IT Anwendungen in der österreichischen Justiz“; abrufbar unter https://www.justiz.gv.at/home/service/digitale-justiz.955.de.html.

18 Vgl. *Schumacher*, Corona-Krise und das Zivilverfahren, AnwBl 2020/286.

Vorreiterrolle erhalten bleibt. Auch aus deutscher Sicht lohnt sich immer ein Blick nach Österreich, wenn das Thema Digitalisierung von Anwaltschaft und Justiz vorangetrieben werden soll.

3 Zwischen Public Value und Querdenker:innenprivilegierung – die Bedeutung des Medienstaatsvertrags für Medienintermediäre

*Mireille Thierfelder**

Mit Pandemiebeginn 2020 und dem Aufkommen von Querdenker:innen rückte ein lange stiefmütterlich behandeltes Problem in den Fokus der gesellschaftlichen Debatte: Der Umgang mit Fake News und Filterblasen in sozialen Netzwerken. Während viele Personen täglich den Podcast „Coronavirus-Update" des NDR mit *Prof. Dr. Drosten* und *Prof. Dr. Ciesek* verfolgten, um sich über den aktuellen Pandemieverlauf zu informieren, gelang es Menschen wie *Ken Jepsen* oder *Attila Hildmann* eine Gruppe um sich zu vereinigen, die nicht nur die Existenz des Virus leugnete, sondern auch die Grundtiefen der Demokratie zutiefst erschütterte. Eine Ära der alternativen Fakten entstand. Jedoch beließ diese Bewegung es nicht dabei, ihre Gesinnung bei Kundgebungen oder über die etablierten sozialen Netzwerke wie Facebook, Instagram oder Twitter kundzutun. Sie suchten sich neue Wege, wie Telegram oder ähnliches, um nun ausschließlich mit Gleichgesinnten zu kommunizieren. Das übliche Korrektiv des gesellschaftlichen Austauschs aufgrund anderer Meinungen blieb aus. Die gesellschaftliche Debatte verstummte. Stattdessen zogen sich diese Personen immer weiter von den „Schlafschafen" zurück und wurden immer resistenter – wenn nicht sogar vollständig immun – gegen wissenschaftliche Argumente. Doch wäre es fatal zu glauben, dass es sich bei diesem Strom lediglich um Personen handeln würde, die bewusst derartige Inhalte konsumieren und grundsätzlich eine interessante Auffassung zu dem Begriff Demokratie haben. Mit Hilfe des Internets wurde es diesen Menschen möglich, aus jeder Gesellschaftsschicht neue Mitglieder zu akquirieren und radikalisieren. Wie ein Lauffeuer verbreiteten sich die Inhalte derer, die offen den Staat und dessen Strukturen angriffen. Aber wie konnte das sein? Gab es keine Regularien, die die Querdenker:innen-Bewegung hätten verhindern können?

Der folgende Aufsatz befasst sich daher mit der Frage, inwiefern die momentanen Regulierungen des Medienstaatsvertrags (MStV) dazu geeignet sind, um eben diese Problematik zu lösen. Handelt es sich bei diesem Gesetz und den zugehörigen Landesmedienanstalten um Institutionen, die einen gesellschaftlichen Mehrwert (Public Value) bringen, oder wurde mit den Normen nicht vielmehr die bereits aufgeheizte Problematik der „Spaltung der Gesellschaft" noch mehr befeuert? Um diese Fragen zu beantworten, erfolgt

* Mehr über die Autorin erfahren Sie im Autor*innenhinweis auf S. 224 ff.

zunächst eine allgemeine Begriffsbestimmung von sowohl juristischen als auch nichtjuristischen Phänomenen, die in diesem Kontext von erheblicher Bedeutung sind (3.1). Darauffolgend sollen das Spannungsverhältnis zwischen den sozialen Medien und der Demokratie skizziert (3.2) und die Regelungsversuche des MStV (3.3) sowie in Kürze europarechtliche Aspekte (3.4) erläutert werden. Anschließend folgen weitere Vorschläge zur Lösung des gesellschaftlichen Problems (3.5), die zu einem abschließenden Fazit (3.6) führen.

3.1 Allgemeine Begriffsbestimmung

„Filterblasen", „Echo-Kammern", „Fake News" – es handelt sich hierbei um Begriffe, die in den alltäglichen gesellschaftlichen Diskurs Einzug gefunden haben. Sei es, dass ein amerikanischer Präsident eigenständig Desinformationen verbreitet oder ein vollumfänglicher Faktencheck bei seriösen Nachrichtensendungen aufgrund der Schnelllebigkeit der Nachrichten nicht vollumfänglich durchgeführt werden kann und so unrichtige Informationen verbreitet werden. Schnell werden derartige Fauxpas unter dem Begriff „Fake News" abgestempelt. Dabei ist vielen Verwender:innen dieses Begriffes nicht immer klar, was genau darunter zu verstehen ist. Häufig hat die Verwendung eine völlig konträre Bedeutung zu dem eigentlichen Inhalt der Aussage. Um in der komplexen Problematik des Aufsatzes keinerlei Verwirrungen zu erzeugen, werden nun einige Begriffe – sowohl juristischer als auch nicht-juristischer Natur – bestimmt.

3.1.1 Medienintermediäre

Medienintermediäre sind in § 2 Abs. 2 Nr. 16 MStV als „Telemed[ien], die auch journalistisch-redaktionelle Angebote Dritter aggregier[en], selektier[en] und allgemein zugänglich präsentier[en], ohne diese zu einem Gesamtangebot zusammenzufassen", legaldefiniert. Sie tragen mithin zumindest auch journalistisch-redaktionelle Angebote zusammen, wählen sie aus und zeigen sie den jeweiligen Nutzer:innen an, erstellen diese jedoch nicht selbstständig.[1] Das Filtern dieser Angebote erfolgt dabei über den Einsatz von Such- und Auswahlalgorithmen, sodass eine bestimmte Reihenfolge, in welcher die Inhalte gezeigt werden, entsteht.[2] Zudem folgen sie dem Grundsatz der „offenen Angebote" und stellen, im Gegensatz zu

1 *Martini*, BeckOK Informations- u. MedienR, § 2, Rn. 117; *Siara*, MMR 2020, 523 [523 f.].

2 *Gerecke/Stark*, GRUR 2021, 816 [819]; *Siara*, MMR 2020, 523 [523].

Medienplattformen, den Nutzer:innen kein Gesamtangebot zur Verfügung.[3] Allerdings kommt grundsätzlich jedermann die Möglichkeit zu, eigenständig Inhalte auf diesem Telemedium hochzuladen.[4] Die Norm ist als Auffangtatbestand konzipiert und soll unter anderem Suchmaschinen, Soziale Netzwerke und Blogging-Portale erfassen.[5] Besonders kennzeichnend für sie soll die besonders intensive Einwirkung auf die öffentliche Meinungsbildung sein, welche aus der Verbreitung eines spezifischen Inhalts resultiert.[6] Medienintermediäre fungieren als wesentlicher Informationsvermittler und -verbreiter im Internet und zudem als „Gatekeeper" für die individuelle und öffentliche Meinungsbildung.[7]

3.1.2 Journalistisch-redaktionelle Tätigkeit

Ein weiterer, in diesem Kontext immer wiederkehrender Ausdruck sind die journalistisch-redaktionellen Angebote, welche von den Medienintermediären zur Verfügung gestellt werden. Eine journalistisch-redaktionelle Tätigkeit ist jedenfalls immer dann anzunehmen, „wenn planvoll ein Angebot hergestellt wird, das sich nach der gesellschaftlichen Relevanz richtet"[8]. Ob eine solche Ausrichtung vorliegt, muss dabei an verschiedenen Kriterien gemessen werden, wobei besondere Bedeutung der Recherche, Gewichtung, Auswahl, Systematisierung, Strukturierung und Aufarbeitung der gesammelten Quellen zukommt.[9]

3.1.3 Filterblasen und Fake News

„Filterblase" und „Fake News" haben in den alltäglichen Sprachgebrauch Einzug gehalten. Doch wird häufig mit derartigen Begriffen sehr leichtfertig hantiert, ohne deren genaue Bedeutung zu kennen. Die „Filterblasen-Theorie" geht auf das Buch „The filter bubble: how the new personalized web is changing what we read and what we think" von *Eli Pariser* zurück und beschreibt dabei eine Art Echo-Kammer im Internet, welche lediglich ein bestimmtes Paradigma zulässt.[10] Diese verhindert jedoch die Konfrontation

3 *Martini*, BeckOK Informations- u. MedienR, § 2, Rn. 117.
4 *Hönig d'Orville*, ZUM 2019, 104 [106 f.]; *Martini*, BeckOK Informations- u. MedienR, § 2, Rn. 117a.
5 *Martini*, BeckOK Informations- u. MedienR, § 2 Rn. 18; *Paal/Heidtke*, ZUM 2020, 230 [233].
6 *Martini*, BeckOK Informations- u. MedienR, § 2, Rn. 120.
7 Begründung des Medienstaatsvertrags, 3; *Gerecke/Stark*, GRUR 2021, 816 [818].
8 *Schulz*, AfP 2017, 373 [374]; *Schneiders*, ZUM 2021, 480 [484].
9 *Martini*, BeckOK Informations- u. MedienR, § 2, Rn. 120.
10 *Holznagel*, MMR 2018, 18 [19].

mit widersprüchlichen Meinungen und sorgt dafür, dass ein konstruktiver Austausch nicht mehr stattfinden kann.[11]

„Fake News" – oder auch Desinformationen – hingegen sind die bewusste Verbreitung falscher Nachrichten.[12] Der Begriff umschreibt sowohl Phänomene wie Satire als auch Native Advertisement und Propaganda.[13] Meinungsäußerungen sind hingegen nicht von diesem Begriff erfasst.[14]

3.2 Medien und Demokratie im Spannungsverhältnis

Heutzutage nehmen Medienintermediäre im alltäglichen Leben eine besondere Bedeutung ein. Zunehmend viele Menschen – gerade die jüngeren Generationen – nutzen sie unter anderem, um sich über aktuelles Zeitgeschehen zu informieren.[15] Dies ist insoweit nicht verwunderlich, als dass etablierte seriöse Nachrichtensendungen wie die „tagesschau" der ARD oder „zdfheute" ebenfalls Kanäle auf diversen Medienintermediären betreiben. So kann man schnell, während man ohnehin Instagram verwendet, auch nebenbei die aktuellen Neuigkeiten nachschauen. Doch können beispielsweise bei der Nutzung von Sozialen Netzwerken als Hauptinformationsquelle auch eine Vielzahl von Situationen entstehen, welche das demokratische System gefährden. Gerade während der Corona-Pandemie wurde die immense Bedeutung von Medienintermediären nochmals deutlicher. So sahen sich auch die Sozialen Netzwerke gezwungen, Schritte gegen die Verbreitung wahrheitswidriger Inhalte vorzunehmen und die Sichtbarkeit von vertrauenswürdigen Informationen zu verstärken.[16]

Dass die Medien einen besonderen Stellenwert in der Gesellschaft einnehmen, ist wiederum kein Phänomen der Neuzeit. Bereits 1966 entschied das BVerfG in seinem Spiegel-Urteil, dass die Informierung der Bevölkerung eine wesentliche Grundlage politischer Willensbildung sei und die Presse diese gewährleisten müsse, um den öffentlichen Diskurs zu erhalten.[17] Den Journalist:innen wurde demnach die Aufgabe zuteil, als Gatekeeper für eine ausgewogene und vielfältige Wiedergabe der Meinungen zu sorgen.[18] Sie

11 *Holznagel*, a. a. O.
12 Wissenschaftlicher Dienst des Deutschen Bundestages, Fake News, Definition und Rechtslage, Az. WD 10 – 3000 – 003/17, S. 6; *Holznagel*, MMR 2018, 18 [18].
13 *Holznagel*, MMR 2018, 18 [18].
14 *Holznagel*, MMR 2018, 18 [19].
15 *Holznagel*, MMR 2018, 18 [19].
16 *Bayer/Holznagel/Korpisaari/Woods*, Perspective on Platform Regulation, S. 509 ff.; *Kalbhenn*, ZUM 2022, 266 [271].
17 *Flamme*, MMR 2021, 770 [770].
18 BVerfG Urteil v. 5.8.1966 – 1 BvR 586/62, 610/63, 512/64; *Flamme*, MMR 2021, 770 [770].

fungierten als gesellschaftliches Korrektiv und verhinderten eine Radikalisierung der unterschiedlichen Auffassungen. Dieses Korrektiv fehlt allerdings momentan im Internet noch. Es stellt eine erhebliche Herausforderung dar, für eine ausgewogene Auffindbarkeit von Inhalten zu sorgen. Denn wenn Informationen nicht gefunden werden können, können sie auch nicht als Grundlage der Meinungsbildung dienen.[19]

Häufig wird im Umgang mit Sozialen Netzwerken kritisiert, dass die von ihnen genutzten Algorithmen nicht auf die Wiedergabe eines pluralen Meinungsspektrums, sondern lediglich auf die Maximierung der Gewinne durch Werbeeinnahmen gerichtet sind.[20] So orientiert sich die algorithmische Informationsvermittlung vielmehr an spezifisch-individuellen Präferenzen als an journalistischen Sorgfaltspflichten.[21] Dabei kommt es regelmäßig dazu, dass sich nicht die qualitativ hochwertigsten, sondern vielmehr die emotionalsten Beiträge, die am meisten polarisieren, durchsetzen und somit weniger ausgewogene Informationen an die Öffentlichkeit gelangen.[22] Dies geht mit der Folge einer zunehmend polarisierten Gesellschaft einher.[23] Wut, Hass und Hetze sind dann Teil des alltäglichen Umgangs miteinander und treffen vermehrt Minderheiten, Politiker:innen und Wissenschaftler:innen.[24] In der Bekämpfung dieses Hasses und der Sicherung eines plattformübergreifenden rationalen Diskurses liegt somit eine sehr wichtige juristischen Aufgaben im Rahmen der Regulierung des Internets.[25]

Jedoch wäre es ebenfalls vermessen, Medienintermediäre – insbesondere die Sozialen Netzwerke – in Gänze zu verteufeln. Denn auf der anderen Seite handelt es sich bei Social Media um eine fundamentale und globale Kommunikationsstruktur.[26] Mit Hilfe dieser Strukturen war es Bewegungen wie „Fridays for Furure“ und „Black lives matter“ erst möglich, die ihnen zustehende Aufmerksamkeit zu erlangen und spürbare gesellschaftliche Veränderungen zu bewirken.

Leider bringt die Möglichkeit dieser intensiven Vernetzung untereinander nicht nur den positiven Effekt des globalen Austauschs mit sich. Denn gerade durch die Möglichkeit des „Teilens“ und der damit verbundenen raschen Verbreitung von Inhalten können gefährliche Schneeballeffekte, bzw. Viral-

19 *Flamme*, MMR 2021, 770 [770].
20 *Holznagel*, ZRP 2021, 229 [229].
21 *Stark/Magin*, Wandel der Öffentlichkeit u. Gesellschaft, S. 385; *Flamme*, MMR 2021, 770 [770].
22 *Schütz*, MMR 2020, 1 [1 f.]; *Flamme*, MMR 2021, 770 [770 f.].
23 *Flamme*, MMR 2021, 770 [771].
24 *Augsberg/Petras*, JuS 2022, 97 [98].
25 *Kalbhenn*, ZUM 2022, 266 [268].
26 *Jackob/Quiering/Maurer*, Traditionen u. Transformationen d. Öffentlichen, S. 91; *Schneiders*, ZUM 2021, 480 [481].

effekte, hervorgerufen werden.[27] Um diesen Effekten entgegenzuwirken ist es erforderlich, die Auffindbarkeit von Inhalten zu optimieren und so für ein plurales Meinungsspektrum zu sorgen.

In den letzten Entscheidungen zum Rundfunkbeitrag hat das BVerfG den öffentlich-rechtlichen Auftrag des Rundfunks konkretisiert und insbesondere seine gesamtgesellschaftliche Bedeutung herausgearbeitet.[28] Es liegt somit in der Aufgabe des Rundfunks, für ein plurales Meinungsbild zu sorgen. Diese Aufgabe muss er auch ins Internet übertragen. Jedoch muss bei dieser Umsetzung die Stärkung des Meinungspluralismus im Vordergrund stehen. Denn der Ausschluss von Nutzer:innen mit anderen Gesinnungen aus den Sozialen Medien muss hingegen mit der nötigen Restriktion behandelt und als letztmöglichstes Mittel betrachtet werden. Dieser Ausschluss kann derart weitreichende Folgen für die Grundrechte des Betroffenen, insbesondere für dessen Meinungsfreiheit aus Art. 5 Abs. 1 GG, haben, dass ein Ausschluss aus den Sozialen Netzwerken als schärfstes Schwert des Medienrechts verstanden werden muss.[29]

3.3 Regelungsversuche des Medienstaatsvertrags

Medien haben eine besonders wichtige Bedeutung in der Demokratie und stellen die „vierte Gewalt" im Staat dar. Es muss jedoch auch gewährleistet werden, dass die ihnen übertragene Macht nicht ausgenutzt und damit die Demokratie gefährdet wird. Rundfunk und Printmedien werden jedoch zunehmend von den „Neuen Medien" verdrängt. Und bei der Informationsvermittlung über Medienintermediäre ist die Gefahr des Machtmissbrauchs besonders hoch. Dies war auch dem Gesetzgeber bewusst und er versuchte mithilfe des Medienstaatsvertrags, diesen negativen Auswirkungen auf den Intermediären entgegenzuwirken. Dafür wurden im MStV Transparenz- (3.3.1) und Nichtdiskriminierungsgebote geschaffen (3.3.2) sowie die Pflicht zur Kennzeichnung von Social Bots (3.3.3) eigeführt.

3.3.1 Transparenzpflicht aus § 93 MStV

3.3.1.1 Regelungsinhalt und Telos der Norm

§ 93 MStV erlegt Medienintermediären einige Transparenzpflichten auf. Hierdurch soll eine Informationsasymmetrie abgeschwächt und den Nutzer:innen ein besseres Verständnis über die grundsätzliche Auswahl der

27 *Guggenberg*, ZRP 2017, 98 [98]; *Holznagel*, MMR 2018, 18 [19].
28 BVerfGE v. 18.7.2018; BVerfGE v. 5.8.2021; *Kalbhenn*, MMR 2022, 106 [106].
29 *Augsberg/Petras*, JuS 2022, 97 [97 f.].

Inhalte vermittelt werden.[30] Außerdem soll dem/der Anbieter:in journalistisch-redaktioneller Inhalte die Möglichkeit eingeräumt werden, sich auf die Funktionsweise von Intermediären einzustellen.[31] Die Aufgabe der Transparenzvorgaben ist es daher, den durchschnittlichen Nutzer:innen die wesentlichen Grundzüge der relevanten technischen Vorgänge zu erklären.[32] Dabei dürften für Suchmaschinen und Soziale Netzwerke unterschiedliche Informationen jeweils als relevant eingestuft werden.[33] Grundsätzlich müssen Medienintermediäre lediglich zentrale Kriterien transparent machen. Dabei handelt es sich um Kriterien, die aus Sicht der Nutzer:innen Einfluss auf die Wahrnehmbarkeit der Inhalte haben oder die grundsätzliche Funktionsweise bestimmen.[34] Dies umfasst unter anderem die Aggregation von Inhalten. Hierunter versteht man nach der Wirtschaftstheorie die Zusammenfassung mehrerer Einzelgrößen aufgrund eines gleichartigen Merkmals, um so Zusammenhänge zu verdeutlichen.[35] Im IT-Bereich bedeutet Aggregation die Verknüpfung und Verdichtung zu einheitlichen Kenngrößen und Parametern.[36] Selektion hingegen meint die Auswahl von Daten und deren Verknüpfungen.[37] Auch von Bedeutung ist außerdem die Präsentation, also die Art und Weise der Darstellung von Inhalten.[38] Besonders relevant ist dabei die Gewichtung der zentralen Kriterien zueinander.[39]

Zudem muss von den Intermediären offengelegt werden, ob die Aufnahme von Inhalten von einer Entgeltzahlung oder vergleichbaren geldwerten Leistungen abhängig gemacht wird und wie diese die Auffindbarkeit der Inhalte beeinflusst.[40] Auch sind Angaben zum Umgang mit personenbezogenen und sonstigen Daten zu machen sowie den Nutzer:innen die Möglichkeit

30 Amtliche Begründung zum Staatsvertrag zur Modernisierung der Medienordnung in Deutschland, S. 49 (https://www.rlp.de/fileadmin/rlp-stk/pdf-Dateien/Medienpolitik/Medienstaatsvertrag_Begru__ndung.pdf, zuletzt abgerufen: 28.8.2022; folgend als „Amtl. Begründung zum MStV" bezeichnet); *Zimmer/Liebermann*, Beck'sche Onlinekommentar Informations- und Medienrecht, 35. Auflage, München 2022, § 93 Rn. 1f (folgend als „BeckOK Informations- u. Medienrecht" bezeichnet); *Holznagel*, ZRP 2021, 229 [231 f.].

31 *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 93 Rn. 3.

32 Amtl. Begründung zum MStV, S. 49; *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 93 Rn. 14.

33 Zimmer/Liebermann, a. a. O.

34 *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 92 Rn. 19; Flamme, MMR 2021, 770 [772].

35 *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 93 Rn. 20.

36 *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 93 Rn. 20.

37 *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 93 Rn. 21.

38 *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 93 Rn. 22.

39 *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 93 Rn. 22.

40 *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 93 Rn. 24.

der Einflussnahme auf den Algorithmus aufzuzeigen.[41] Dies hat in einer verständlichen Sprache zu erfolgen Maßgeblich hierfür sind durchschnittliche Nutzer:innen, welche sich in einer typischen Benutzungssituation befinden.[42] Die Veröffentlichung von Betriebs- und Geschäftsgeheimnissen oder des Algorithmus selbst ist jedoch nicht erforderlich und auch nicht zielführend.[43] Medienintermediäre müssen außerdem Änderungen hinsichtlich der Kriterien oder der Funktionsweise des Algorithmus umgehend den Nutzer:innen wahrnehmbar machen.[44]

Anbieter:innen von Sozialen Netzwerken trifft zusätzlich die Pflicht, dass sie für die Kennzeichnung von Social Bots Sorge zu tragen haben. Geregelt ist dies in § 18 Abs. 3 MStV. Diese Transparenzverpflichtungen werden ex post kontrolliert und ein etwaiger Verstoß stellt eine Ordnungswidrigkeit gemäß § 115 Abs. 1 S. 2 Nr. 42–45, Abs. 2 MStV dar, welche mit einer Geldbuße bis zu 500.000Euro geahndet werden kann.[45]

3.3.1.2 Konkretisierung durch MI-Satzung

Um die Besonderheiten dieser Transparenzverpflichtung zu konkretisieren, wurde von den Landesmedienanstalten eine Satzung zur Regulierung von Medienintermediären (MI-Satzung) erlassen. Hier werden die Begriffe „leichte Wahrnehmbarkeit", „unmittelbar erreichbar" und „ständig verfügbar" in Form gegossen. Leicht wahrnehmbar ist gem. § 5 Abs. 2 S. 2 MI-Satzung eine Information dann, wenn sie sich von dem übrigen Inhalt abhebt. § 5 Abs. 3 S. 2 MI-Satzung gibt für die unmittelbare Erreichbarkeit vor, dass eine Information nicht mehr als zwei Links von der Ursprungsseite entfernt sein und nicht von einer vorherigen Registrierung oder einem Log-In abhängig gemacht werden darf. Außerdem müssen Nutzer:innen für die ständige Verfügbarkeit jederzeit auf die Information zugreifen können, vgl. § 5 Abs. 4 MI-Satzung.

3.3.1.3 Stellungnahme

Der Gesetzgeber hat mit dieser Regelung versucht, den Nutzer:innen die Möglichkeit zu geben, die Ergebnisse der journalistisch-redaktionellen Angebote der Medienintermediäre zu verstehen. Hierdurch könnten die

41 *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 93 Rn. 24 f.
42 Amtl. Begründung zum MStV, S. 49; *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 93 Rn. 28.
43 Amtl. Begründung zum MStV, S. 50; *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 93 Rn. 29 f.
44 Amtl. Begründung zum MStV, S. 50; *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 93 Rn. 34 f.
45 *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 93 Rn. 37.

Nutzer:innen zum Hinterfragen ihres eigenen Umgangs mit den Medienintermediären angeregt werden und gegebenenfalls eigenständig gegen den Algorithmus für eine plurale Meinungsvermittlung sorgen. So soll der Entstehung von Filterblasen und Echokammern entgegengewirkt werden. Dieser Gedanke ist aufgrund der Anknüpfung an die Mündigkeit der Bürger:innen sehr begrüßenswert. Es ist jedoch fraglich, ob dieses Vorgehen erfolgsversprechend ist. Es mag zwar sein, dass Nutzer:innen, die grundsätzlich an einer vielfältigen Informationsvermittlung interessiert sind, sich mit dem eigenen Algorithmus auseinandersetzen und diesen kritisch hinterfragen. Doch gerade im Spektrum der Querdenker:innen, die sich häufig der „alternativen Fakten" bedienen, qualitativ hochwertige Informationen leugnen und sowohl Meinungen als auch Tatsachenbehauptungen verbreiten, die teilweise strafrechtliche Relevanz haben, darf bezweifelt werden, dass sich diese kritisch mit dem Algorithmus auseinandersetzen. Vielmehr muss davon ausgegangen werden, dass von dieser Gruppierung ein einseitiger Algorithmus einen positiveren Anklang finden würde. Somit ist die Idee des § 93 MStV generell für die Demokratie wünschenswert. Der tatsächliche Erfolg der Norm muss jedoch bezweifelt werden.

3.3.2 Nichtdiskriminierungsverpflichtung aus § 94 MStV

3.3.2.1 Regelungsinhalt und Telos der Norm

Gemäß § 94 MStV ist es Medienintermediären nicht gestattet, journalistisch-redaktionelle Angebote zu diskriminieren. Sinn und Zweck der Norm ist es, eine strukturelle Gleichbehandlung von journalistisch-redaktionellen Angeboten zu gewährleisten und die verfassungsrechtliche Meinungsvielfalt zu schützen.[46] Dabei darf der Begriff der Diskriminierungsfreiheit nicht in einem kartellrechtlichen Kontext gesetzt, sondern muss medienrechtlich vor dem Hintergrund des Meinungspluralismus verstanden werden.[47] Es mag zwar teilweise zu Überschneidungen der beiden Bereiche kommen, doch darf die Vielfaltssicherung niemals unter wettbewerblichen Streitigkeiten leiden.[48] Von dem Nichtdiskriminierungsverbot des § 94 MStV sind insbesondere Medienintermediäre erfasst, die einen besonders hohen Einfluss auf die Wahrnehmbarkeit von journalistisch-redaktionell gestalteten Angeboten haben und damit als „Gatekeeper" fungieren.[49] Wann ein besonders hoher

46 Amtl. Begründung zum MStV, S. 51; LT NRW-Drs. 17/9052, 165; *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 94 Rn. 2; *Flamme*, MMR 2021, 770 [772].

47 Amtl. Begründung zum MStV, S. 51; *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 94 Rn. 2; *Flamme*, MMR 2021, 770 [772].

48 *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 94 Rn. 2.

49 Amtl. Begründung zum MStV, S. 51; *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 94 Rn. 3 f.

Einfluss des Medienintermediärs anzunehmen ist, ist jedoch im Normtext nicht genauer beschrieben. Dieser muss im Rahmen der Gesamtschau aller Umstände bestimmt werden.[50] Dabei können dann sowohl die kartellrechtlichen Maßstäbe als auch die medienkonzentrationsrechtlichen Schwellenwerte zu Hilfe genommen werden.[51] Ein wichtiges Indiz für einen hohen Einfluss kann daher laut den Landesmedienanstalten auch eine marktbeherrschende Stellung sein.[52] Jedoch muss sich immer auch vor Augen geführt werden, dass das Medienrecht ein eigenes Rechtsgebiet ist und kein Sonderkartellrecht darstellt.[53]

Relevant sind jedoch nur Angebote, die journalistisch-redaktionell gestaltet sind. Hierunter werden alle Angebote gefasst, welche ein gewisses Maß an Aktualität und Strukturierung aufweisen und deren Auswahl von einer gewissen gesellschaftlichen Relevanz gekennzeichnet ist.[54] Da durch die Diskriminierung das gesamte Angebot betroffen ist, reicht es aus, dass ein abgrenzbarer Teil oder Beitrag eines journalistisch-redaktionellen Angebots diskriminiert wird.[55]

Wichtig bei dieser Norm ist, dass die ungerechtfertigte Abweichung von den Vorgaben in § 93 Abs. 1 bis 3 MStV zu Lasten eines Angebots oder dessen unbillige Behinderung systematisch begangen werden muss. Denn eine unterschiedliche Behandlung von Angeboten ist regelmäßiger Bestandteil eines Medienintermediärs.[56] Eine Abweichung liegt vor, wenn in einer vergleichbaren Situation dasselbe Kriterium andersartig verwendet wird.[57] Ob diese jedoch sachlich gerechtfertigt ist, muss mittels einer Abwägung der widerstreitendenden Interessen der Beteiligten unter der Berücksichtigung der auf die Vielfaltssicherung gerichteten Zielsetzung, entschieden werden.[58] Als Ausprägung des Grundsatzes der kommunikativen Chancengleichheit soll so eine vergleichbare Ausgangslage für alle Anbieter:innen geschaffen werden.[59]

---

50 *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 94 Rn. 6.
51 Amtl. Begründung zum MStV, S. 51; *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 94 Rn. 6; *Flamme*, MMR 2021, 770 [772].
52 LT NRW-Drs. 17/9052, 165; *Zimmer/Lierbmann*, BeckOK Informations- u. Medienrecht, § 94 Rn. 6; *Flamme*, MMR 2021, 770 [772].
53 *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 94 Rn. 6.
54 *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 94 Rn. 7.
55 *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 94 Rn. 7.
56 Amtl. Begründung zum MStV, S. 51 f.; *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 94 Rn. 8; *Schneiders*, ZUM 2021, 480 [484 f.].
57 *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 94 Rn. 13; *Schneiders*, ZUM 2021, 480 [484 f.].
58 *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 94 Rn. 19.
59 *Zimmer/Liebermann*, BeckOK Informations- u. Medienrecht, § 94 Rn. 30.

3.3.2.2 Konkretisierung durch die MI-Satzung

Wie auch die Transparenzpflicht des § 93 MStV in der MI-Satzung konkretisiert wurde, so erfährt die Nichtdiskriminierungspflicht ebenfalls eine Konkretisierung in dieser Satzung. Für § 94 MstV sind insbesondere der § 8 MI-Satzung, welcher die systematische Abweichung genauer beleuchtet, sowie § 9 MI-Satzung, der die unbillige Behinderung erklärt, von zentraler Bedeutung. Gemäß § 8 Abs. 3 S. 1 MI-Satzung muss eine systematische Begehung mittels Gesamtschau positiv festgestellt werden. Indizien können hierbei Dauer, Regelmäßigkeit, Wiederholung oder Planmäßigkeit der Abweichung oder Behinderung sein, vgl. § 8 Abs. 3 S. 2 MStV. Zudem wird auf die Unbilligkeit der Behinderung konkreter eingegangen. Nach § 9 Abs. 4 MI-Satzung muss dies anhand einer Abwägung der widerstreitenden Interessen der Medienintermediäre, Inhalteanbieter:innen und Nutzer:innen beurteilt werden.

3.3.2.3 Stellungnahme

Die Regelung des § 94 MStV hat einen besonderen Wert für die Demokratie. Denn mit der grundsätzlichen Gleichbehandlung von journalistisch-redaktionellen Angeboten kann Machtmissbrauch eines Intermediärs entgegengewirkt werden. Zusätzlich ermöglicht die Norm auch, dass mittels einer sachlichen Rechtfertigung unterschiedliche Behandlung der Angebote weiterhin möglich ist und die Medienintermediäre nicht vor einer schlicht unlösbaren Aufgabe stehen. Es handelt sich bei § 94 MStV um eine der wichtigen Normen, wenn nicht sogar um die bislang wichtigste, im Kampf gegen Filterblasen und „Fake News“. Mit ihr können einseitige Algorithmen durchbrochen werden. Dies führt zur Stärkung der Meinungs- und Informationsvielfalt, der sich auch Querdenker:innen bei konsequenter Durchsetzung der Norm auf lange Sicht nicht verwehren können. Doch trotz ihrer besonderen Bedeutung handelt es sich vielmehr um ein stumpfes Schwert des Gesetzgebers. Denn zwar fordert die Norm die grundsätzliche Gleichbehandlung von journalistisch-redaktionellen Angeboten, bietet zugleich jedoch die Möglichkeit, diese unterschiedlich zu behandeln. Es besteht daher die Gefahr, dass Medienintermediäre diese Chance für sich nutzen und ausschließlich nach Gründen suchen, welche eine solche Ungleichbehandlung rechtfertigen könnte.

3.3.3 Kennzeichnungspflicht von Social Bots

Gemäß § 93 Abs. 4 MStV haben Medienintermediäre, die Soziale Netzwerke anbieten, die Pflicht, dort für die Kennzeichnung von Social Bots zu sorgen. § 18 Abs. 3 MStV regelt die Kennzeichnungspflichten von Social Bots. Es wird dabei von einem weiten Begriffsverständnis ausgegangen, welches un-

terschiedliche Nutzungssituationen von Social Bots erfassen soll.[60] Darunter sind grundsätzlich alle Softwareprogramme zu verstehen, welche menschliche Verhaltensweisen in Sozialen Netzwerken imitieren und dabei Beiträge automatisiert verfassen, kommentieren, liken oder teilen.[61] Eine Kennzeichnungspflicht besteht jedoch nur, wenn diese Nachahmung zu einer für die Kommunikation relevanten Identitätstäuschung führt.[62] Hierfür ist es erforderlich, dass eine menschliche anstatt einer künstlichen Identität vorgegeben wird.[63] Diese Identitätstäuschung muss dabei auf einem vollständig automatisierten Vorgang beruhen.[64] Ob eine solche Täuschung vorliegt, ist dabei je nach Kommunikationsgegenstand und Nutzungskontext unterschiedlich zu beurteilen.[65] Normzweck ist, die individuelle und öffentliche Meinungsbildung vor Desinformation zu schützen sowie die Integrität und Vertrauenswürdigkeit der zwischenmenschlichen Kommunikation zu stärken und das staatliche Interesse an einer funktionalen Kommunikationsordnung zu gewährleisten.[66] Von Bedeutung für diese Regelung sind Inhalte und Mitteilungen. Unter Inhalten versteht man dabei Tatsachenbehauptungen und Werturteile sowie gemischte Äußerungen jeglicher Art.[67] Diese müssen mittels eines automatisierten Computerprogramms erstellt werden, ohne dass dabei ein menschlicher Eingriff in den Erstellungsvorgang erfolgen darf.[68] Eine Art und Weise der Kennzeichnung ist dabei nicht vorgeschrieben.[69] Der kennzeichnende Hinweis muss lediglich dem Inhalt- oder der Mitteilung in gut lesbarer Form bei- oder vorangestellt werden.[70]

60 *Lent*, BeckOK Informations- u. Medienrecht, § 18 Rn. 13.
61 *Lent*, BeckOK Informations- u. Medienrecht, § 18 Rn. 13. *Löber/Roßnagel*, MMR 2019, 493 [494]; *Milker*, ZUM 2017, 216 [216 f.].
62 *Lent*, BeckOK Informations- u. Medienrecht, § 18 Rn. 13. *Milker*, ZUM 2017, 216 [219 f.].
63 *Lent*, a BeckOK Informations- u. Medienrecht, § 18 Rn. 13.
64 Lent, BeckOK Informations- u. Medienrecht, § 18 Rn. 13; *Milker*, ZUM 2017, 216 [217 f.].
65 Lent, BeckOK Informations- u. Medienrecht, § 18 Rn. 13.
66 LT-Drs. NRW 17/9052, 134; *Lent*, BeckOk Informations- u. Medienrecht, § 18 Rn. 14; *Löber/Roßnagel*, MMR 2019, 493 [496].
67 *Lent*, BeckOk Informations- u. Medienrecht, § 18 Rn. 18.
68 *Lent*, BeckOk Informations- u. Medienrecht, § 18 Rn. 19.
69 *Lent*, BeckOk Informations- u. Medienrecht, § 18 Rn. 21.
70 *Lent*, BeckOk Informations- u. Medienrecht, § 18 Rn. 22.

3.4 Europarechtliche Aspekte

Mit dem angekündigten Digital Services Act[71] wird ein neues medienrechtliches Zeitalter erwartet. Denn mit Hilfe dieser europarechtlichen Neuerung soll der Einfluss von Inhalteanbietern auf die öffentliche Meinungsbildung sowie deren Vielfalt besser reguliert werden.[72] Dabei folgt die Verordnung einem risikobasierten Ansatz, welcher bei steigender Nutzer:innenzahl eine stärkere Regulierung verlangt.[73] Trotz des „in der Tür Stehens" der europarechtlichen Verordnung kann davon ausgegangen werden, dass die nationalrechtlichen Normen weiterhin ihre Geltung behalten. Im Gegensatz zum MStV sollen hier jedoch nicht die Medienschaffenden im Mittelpunkt stehen.[74] Der Digital Service Act soll keine Regelungen, welche die medialen Inhalte betreffen, vorgeben.[75] Denn gerade im Bereich der Medienregulierung muss beachtet werden, dass aufgrund der unterschiedlichen bedeutenden nationalen Besonderheiten, eine europaweite Vollharmonisierung als nicht zielführend erachtet werden muss.[76]

3.5 Weitere Vorschläge zur Eindämmung des Problems

Wie sich bereits aufzeigen ließ, bieten die bisherigen Regelungsversuche keine wirkliche Lösung für ein immer präsenteres Problem: die Spaltung der Gesellschaft. Und gerade diese Spaltung wird insbesondere durch Soziale Netzwerke wie Facebook immer weiter vorangetrieben. Es ist wohl kaum von der Hand zu weisen, dass in den vergangenen Jahren das Internet immer wichtiger sowohl für die individuelle als auch öffentliche Meinungsbildung geworden ist. Immer mehr Nutzer:innen informieren sich über das Internet und nicht mehr über den klassischen Rundfunk.[77] Doch nicht alle. Es gibt auch weiterhin einen beständigen Teil, der sich vornehmlich über die klassischen Angebote informiert.[78] Um keine der beiden Gruppen zu benachteiligen, sollte daher ein noch pluraleres Meinungsbild sowohl im Rundfunk als auch auf Medienintermediären umgesetzt werden. Fraglich ist dann jedoch, wie eine solche Umsetzung im Konkreten aussehen müsste. Nachfolgend sollen zwei Ideen zur Bekämpfung von demokratiegefährdenden Phänome-

71 COM (2020) 825 final, 10.
72 COM (2020) 825 final, 35, Erwägungsgrund 56.
73 *Martini*, BeckOk Informations- u. Medienrecht, § 2 Rn. 127.
74 *Martini*, BeckOk Informations- u. Medienrecht, § 2 Rn. 127b.
75 COM (2020) 825 final, 10.
76 *Zimmer/Liebermann*, BeckOk Informations- u. Medienrecht, § 93 Rn. 41.
77 https://de.statista.com/statistik/daten/studie/170819/umfrage/informationsquelle-fuer-aktuelles-tagesgeschehen/ (zuletzt abgerufen am 30.8.2022).
78 https://de.statista.com/statistik/daten/studie/170819/umfrage/informationsquelle-fuer-aktuelles-tagesgeschehen/ (zuletzt abgerufen am 30.8.2022).

nen auf Medienintermediären besprochen sowie ein eigener Lösungsvorschlag vorgestellt werden.

3.5.1 Zwei-Säulen-Modell zur Sicherung der Meinungspluralität

3.5.1.1 Erklärung des Modells

Einen interessanten Ansatz hierzu stellt des Zwei-Säulen-Modell zur Regulierung von Medienintermediären dar.[79] Hierbei müsste jeder Medienintermediär ein Gesamtangebot erzeugen, welches sich aus zwei Algorithmen zusammensetzen würde. Dabei sollen die Angebote der ersten Säule immer noch aus den individuellen Inhalten bestehen, welche dem Algorithmus der Medienintermediäre selbst entspringen.[80] Zudem soll für diese Säule sowohl Transparenz als auch Missbrauchskontrolle inhaltlich als Vorgabe gelten.[81] Die zweite Säule hingegen soll, ungeachtet der persönlichen Präferenzen der Nutzer:innen, vielfältige Interessen wiedergeben.[82] Der Maßstab hierbei wäre lediglich die positive Ordnung für Medienintermediäre.[83] Die Kompetenz zu Regelung der Vielfaltssicherung würde bei den Ländern liegen.[84] Sowohl die erste als auch die zweite Säule müssten sich für die Generierung von Inhalten aus ein und demselben Datenpool bedienen.[85]

3.5.1.2 Stellungnahme

Die grundsätzliche Idee, das Konzept des dualistischen Rundfunks in das Internet zu übertragen, ist zunächst begrüßenswert. Jedoch muss diese Idee auch kritisch betrachtet werden. Eine Problematik besteht unter anderem darin, dass nicht wirklich ersichtlich ist, für welche Medienintermediäre die zweite Säule verpflichtend eingeführt werden müsse. Während diese Pflicht bei solchen mit einer enormen Relevanz für den individuellen und öffentlichen Meinungsbildungsprozess durchaus wünschenswert wäre, so könnte er für kleinere Medienintermediäre eine Vernichtung der Existenz herbeiführen. Es kann nicht davon ausgegangen werden, dass jede:r Anbieter:in eines Medienintermediärs in der Lage wäre, einen solchen zweiten Algorithmus in sein/ihr Angebot mit einzupflegen. Weiterhin problematisch scheint die Bereitstellung eines gemeinsamen Datenpools. Denn gerade eine der Be-

79 *Schwartmann/Hermann/Mühlenbeck*, MMR 2019, 498 [501 ff.].
80 *Schwartmann/Hermann/Mühlenbeck*, MMR 2019, 498 [501].
81 *Schwartmann/Hermann/Mühlenbeck*, MMR 2019, 498 [502].
82 *Schwartmann/Hermann/Mühlenbeck*, MMR 2019, 498 [501].
83 *Schwartmann/Hermann/Mühlenbeck*, MMR 2019, 498 [501].
84 *Schwartmann/Hermann/Mühlenbeck*, MMR 2019, 498 [502].
85 *Schwartmann/Hermann/Mühlenbeck*, MMR 2019, 498 [501].

sonderheiten im Internet ist, dass es die Möglichkeit gibt, sich aus verschiedenen noch so unbekannten Informationsquellen zu informieren. Mit der Vorgabe eines gemeinsamen Datenpools für den privaten sowie den allgemeinen Algorithmus würde jedoch diese Eigenart verloren gehen.

3.5.2 Neuer Medienstaatsvertrag

3.5.2.1 Darstellung der Neuerungen für Medienintermediäre für Vielfaltssicherung

Auch wenn der Medienstaatsvertrag erst 2020 seinen Vorgänger, den Rundfunkstaatsvertrag, ablöste, arbeiten die Länder bereits wieder an dessen Erneuerung.[86] In dieser soll sich erstmals ausdrücklich mit Empfehlungssystemen auseinandergesetzt werden, welche auf die Aggregation, Selektion und Vermittlung von Inhalten eingehen, vgl. § 30 Abs. 4 S. 2 MStV-E. Zudem soll mit Hilfe der §§ 26 Abs. 1 S. 10, 30 Abs. 4 S. 5 MStV-E das Angebot von öffentlich-rechtlichen Inhalten auf privaten Plattformen verstärkt werden, um so Nutzer:innenzahlen zu erhöhen.[87] Insgesamt sieht der Entwurf vor, Public-Value-zugehörige Angebote zu stärken.

3.5.2.2 Stellungnahme

Die momentane Rechtslage in Bezug auf Medienintermediäre zeigt, dass es dringend einer Verbesserung des noch sehr jungen Medienstaatsvertrags bedarf. Denn wie diese Arbeit gezeigt hat, sind die momentanen Regelungen nicht ausreichend, um einen vielfältigen Meinungsaustausch in der Demokratie zu gewährleisten. Begrüßenswert ist, dass der Wert öffentlich-rechtlicher Angebote gestärkt werden soll. Es stellt sich jedoch die Frage, inwiefern das Vorhaben von Erfolg gekennzeichnet sein wird. Gerade das Etablieren von Empfehlungssystemen könnte sich als stumpfes Schwert erweisen. Diese könnten von den Medienintermediären nämlich als bloße Empfehlungen wahrgenommen werden, ohne dass sie einen tatsächlichen Bedarf der Orientierung an ihnen empfinden. Somit würden sie ins Leere laufen. Vielversprechender erscheint hingegen zunächst das Vorhaben, das öffentlich-rechtliche Angebot zu verstärken. Bei genauerer Betrachtung der Normen stellt sich jedoch heraus, dass die Angebote nur dort gestärkt werden sollen, „wo die Nutzung üblicherweise besonders hoch ist“. Damit wird jedoch gerade genau das Ziel verfehlt, die Meinungs- und Informationsplu-

86 https://www.rlp.de/fileadmin/rlp-stk/pdf-Dateien/Medienpolitik/Synopse_MAEStV_Reform_OERR_Nov2021.pdf (Stand: 19.7.2022, 14:22).

87 *Rhein/Dreyer*, https://leibniz-hbi.de/de/blog/oeffentlich-rechtlicher-rundfunk-als-pionier (Stand: 19.7.2022, 15:30).

ralität dort zu etablieren, wo sie momentan fehlt, nämlich in den Filterblasen und Echokammern.

3.5.3 Eigener Lösungsansatz

Die vorhergenannten Lösungsansätze scheinen jedoch für die Praxis wenig Erfolg zu versprechen. Wie oben bereits ausführlich besprochen, übersehen beide Ansätze für die Demokratie wichtige Aspekte. Um solche fatalen Fehler jedoch gänzlich auszuschließen, müssen sie weitergedacht und kombiniert werden. Eine interessante Möglichkeit stellt sich durch die Kombination beider Vorhaben dar. Es sollte daher grundsätzlich über die Übertragung des dualistischen Rundfunksystems in einer auf das Internet angepassten Art und Weise nachgedacht werden. Selbstverständlich wird es nicht möglich sein, eine für sich stehende öffentlich-rechtlich Plattform zu schaffen. Das wäre auch nicht wünschenswert, da durch diese die Vorzüge des Internets unterlaufen würden. Um diese Vorteile zu wahren, dürfte nur ein gesamtgesellschaftlich-relevanter Algorithmus für meinungsbildungs-relevante Medienintermediäre eingeführt werden. Denn sobald ein Unternehmen die Möglichkeit innehat, in erheblicher und demokratiegefährdender Weise sowohl auf die öffentliche sowie individuelle Meinungsbildung einzuwirken, soll es auch alles Erforderliche dafür veranlassen, einen öffentlichen Diskurs sicherzustellen. Diese Verantwortung könnte sich aus Art. 5 GG herleiten lassen mit der Begründung, dass Medienintermediäre und insbesondere Soziale Netzwerke im Laufe der Zeit eine immer bedeutendere Rolle für die Meinungsäußerungsfreiheit eingenommen haben. So haben sie doch das Fernsehen als Informationsquelle in weiten Teilen verdrängt und den bekannten „Lagefeuereffekt“, welchen die Tagesnachrichten einst hatten, dem Erdboden gleich gemacht.

Jedoch muss auch dieser Vorschlag kritisch betrachtet werden. Denn Art. 5 Abs. 1 S. 1 GG gewährt neben der positiven Meinungsfreiheit auch die negative Informationsfreiheit, also das Recht, nicht mit jeder Information und Meinung eines anderen konfrontiert werden zu müssen.[88] Weiterhin ist die Einführung eines vorgeschriebenen Algorithmus ein nicht unerheblicher Eingriff in die Berufsfreiheit der meinungsbildungsrelevanten Unternehmen. Somit ist auch dieser Vorschlag nicht unkritisch zu betrachten. Nichtsdestotrotz leben wir in einer immer weiter auseinanderdriftenden Gesellschaft, in der es wenig Diskurs miteinander und wenig Verständnis für die Argumente der Gegenseite gibt. Ein solcher Diskurs und ein solches Verständnis sind jedoch lebensnotwendig für eine funktionierende Demokratie. Daher sollte man in Zeiten, in denen Wissenschaftler:innen angefeindet und

88 *Bethge*, Sachs Grundgesetz-Ko, Art. 5, Rn. 51 ff.; *Schulz*, Nomos Kommentar MedienR, 4. Auflage, Baden-Baden 2021, 1. Teil, 3.V., Rn. 29 ff.

Politiker:innen getötet werden, zumindest über diese Idee nachdenken, um neue Wege für das Miteinander im Internet zu denken.

3.6 Fazit

Gerade in Zeiten von Corona-Pandemie, Klimawandel und Krieg in der Ukraine wird deutlich, welchen erheblichen Einfluss Medienintermediäre auf unsere Demokratie haben. Auch Querdenker:innen-Bewegungen, gefolgt von Hass und Hetze, sind ein immer immenser werdendes Problem für unsere Gesellschaft. Unabhängig davon, dass Qualitätsjournalismus mehr gefördert sowie die Medienkompetenz der Bevölkerung deutlich gestärkt werden muss, zeigt der Aufsatz, dass die bisherigen Regelungen das gefährliche Heranrollen der Gesellschaftsspaltung momentan nicht bremsen können. Den bisherigen Nichtdiskriminierungs- und Transparenzverpflichtungen gelingt es nicht, ein plurales Meinungsbild auf Medienintermediären zu gewährleisten. Es mag mit Sicherheit nicht im Interesse des Gesetzgebers gelegen haben, dass der aktuelle Medienstaatsvertrag nicht wirksam das Aufkommen der Querdenker:innen-Bewegung verhindern konnte. Doch kann das kein Argument dafür sein, diesen Zustand einfach zu akzeptieren. Es ist nun die Zeit, den gesellschaftlichen Diskurs wieder zu stärken und das konstruktive Miteinander zu fördern. Daher ist die zügige Erneuerung der Regulierungen der Medienintermediäre unabdingbar, wenn im Zeitalter des Internets eine stabile Demokratie weiterhin gewährleistet werden soll.

4 Predictive Analytics und DSGVO: Ethische und rechtliche Implikationen

*Rainer Mühlhoff & Hannah Ruschemeier**

Der Beitrag untersucht die Herausforderungen prädiktiver Analytik aus ethischer und rechtlicher Sicht, insbesondere im Verhältnis zur Reichweite der DSGVO. Dabei werden zunächst die Grundlagen prädiktiver Analytik in Bezug auf Begriff, Technik und Verfahrensweise sowie anhand von Beispielen erläutert. Der ethische Schwerpunkt der Abhandlung analysiert Vorhersagemacht als Folge prädiktiver Analytik und greift als normativen Gegenbegriff das Konzept der prädiktiven Privatheit auf. In der Gestalt von Vorhersagemacht manifestiert sich eine aktuell virulente Spielart von Datenmacht bestimmter Akteure, die wiederum einen ethischen und gesellschaftlichen Bedarf nach der Formulierung eines neuen Schutzguts der prädiktiven Privatheit erzeugt. Ziel unserer theoretischen Konstruktion ist es, die kollektive Verursachungsstruktur prädiktiver Modelle abzubilden. Diese Erwägungen führen direkt zu den rechtlichen Implikationen: Das klassische Verständnis des Schutzguts der Privatheit ist zwar rechtlich umrissen – auch durch das Datenschutzrecht – aber nicht juristisch-normativ determiniert und dadurch entwicklungsoffen. Es wird gezeigt, dass die grundrechtsdogmatisch geprägte individualrechtliche Regelungskonzeption der DSGVO nicht in der Lage ist, die Auswirkungen prädiktiver Modelle adäquat zu erfassen. Dies bezieht sich sowohl auf den Anwendungsbereich im Allgemeinen als auch auf die Betroffenenrechte im Speziellen. Ansatzpunkte für eine Differenzierung zwischen Ausgangsdaten und abgeleiteten Daten finden sich allein in Art. 9 DSGVO; auf Big Data angewandt, lassen sich die Voraussetzungen der Norm nicht mehr begrenzen. Auch eine Anonymisierung von Daten kann die Erstellung prädiktiver Modelle nicht verhindern. Daran anschließend wird die Rechtsprechung des EuGH zu abgeleiteten Daten analysiert. Der Beitrag schließt mit einer Abgrenzung prädiktiver Privatheit zu verwandten Konzepten.

4.1 Auftakt

Big Data ist per Definition überindividuell, Grundrechtsschutz ist individuell. Prädiktive Analytik verarbeitet große Datenmengen einer Vielzahl von Personen. Die Funktionsweise prädiktiver Analytik entspricht damit nicht der dogmatischen Konzeption des Rechts auf informationelle Selbstbestim-

* Mehr über die Autor:innen erfahren Sie im Autor*innenhinweis auf S. 224 ff.

mung oder des Rechts auf Datenschutz der Europäischen Grundrechtecharta. Denn diese Grundrechte adressieren Informationssammlung und -verarbeitung in untrennbarer Verbindung mit dem Datenoutput, d. h., sie beruhen auf der Verbindung von Informationen mit individuellen Personen. Die DSGVO (und das nationale Datenschutzrecht) adressieren die Verarbeitung von Daten von Individuen ebenfalls nur in Bezug auf sie selbst. Somit führt der Komplex prädiktiver Analytik auch zu der Frage, wie der Umgang mit Informationen rechtlich ausgestaltet werden kann, für die es keine Freigabe von den betroffenen Personen gibt.[1]

4.2 Prädiktive Analytik: Grundlagen

4.2.1 Begriff und technische Verfahrensweise

Unter dem Begriff „prädiktive Analytik" fassen wir bestimmte Anwendungen von „Künstlicher Intelligenz-" (KI-), Datenanalyse- und computationale Statistikverfahren zusammen. Dabei ist eine funktionale Charakterisierung prädiktiver Analytik für die vorliegende Darstellung relevanter als eine Festlegung auf bestimmte Algorithmen, die den betreffenden Funktionen zugrunde liegen[2]: Unter prädiktiver Analytik verstehen wir die technologischen Verfahren zur Herstellung prädiktiver Modelle. Unter einem prädiktiven Modell verstehen wir eine algorithmische Routine, welche der Abschätzung unbekannter oder in der Zukunft liegender Informationen dient. Solche Prognosen können sich auf das Verhalten von Menschen beziehen, Ereignisse vorhersagen und Personen in Ähnlichkeitsgruppen einteilen. Ein prädiktives Modell erhält dabei typischerweise als Input die über ein zu beurteilendes Individuum oder einen Fall bekannten Informationen (im Folgenden „Hilfsdaten" genannt; z. B. Trackingdaten oder Social-Media-Nutzungsdaten über eine Nutzer:in) und gibt als Output eine Schätzung der modellierten Zielvariable zurück (z. B. sexuelle Identität des/der Nutzer:in).

Die entsprechenden prädiktiven Modelle werden typischerweise anhand großer Mengen von Trainingsdaten trainiert oder kalibriert. Das heißt, sie lernen auf der Grundlage einer großen empirischen Datenbasis ihre Vorhersagen zu stellen. Eine solche Datenbasis besteht aus Datenpaaren, in der über eine große Anzahl bekannter Fälle die Hilfsdaten (Input-Daten) und

1 Dabei kommt es nicht darauf an, ob Individuen im Internet bewusst Informationen über Dritte preisgeben, die prädiktive Datenanalyse ist darauf nicht angewiesen. *Eichenhofer*, e-Privacy, 2021, S. 152 geht aber wohl nur von einer Gefährdung der bewussten Informationspreisgabe über Dritte aus.

2 Vgl. *Mühlhoff*, Deutsche Zeitschrift für Philosophie, 68 (6): 867–90, 2020, doi: 10.1515/dzph-2020-0059.

die Zielinformationen zusammengefasst sind. Lernverfahren, welche ein Modell anhand von Trainingsdaten dieser Gestalt trainieren, bezeichnet man auch als „überwachte" (supervised) Lernverfahren, weil sie aus Beispielen lernen, für welche die zu modellierende Zielvariable bereits bekannt ist.

4.2.2 Anwendungsbeispiele

Generell ist prädiktive Analytik dann und dort interessant, wo anhand leicht verfügbarer Daten schwer zugängliche Informationen über beliebige Nutzer:innen abgeschätzt werden sollen.[3] Mediziner:innen von der University of Pennsylvania haben z. B. gezeigt, dass sich anhand von Nutzungsdaten von Social-Media-Plattformen vorhersagen lässt, ob ein:e Nutzer:in an Krankheiten wie Depression, Psychosen, Diabetes oder Bluthochdruck leidet.[4] Eine bekannte Studie von *Konsinski* et al. hat ermittelt, dass Facebook-Likes einer Facebook-Nutzer:in dazu verwendet werden können, „eine Reihe höchst sensibler persönlicher Attribute" über diese Nutzer:in vorherzusagen, „darunter sexuelle Orientierung, Ethnie, religiöse und politische Ansichten, Persönlichkeitseigenschaften, Intelligenz, Happiness, Suchtverhalten, Trennung der Eltern, Alter und Geschlecht".[5] Über diese für die meisten Nutzer:innen nicht erkennbare Verletzung ihrer informationellen Selbstbestimmung hinaus ist vor allem die *sekundäre* Verwendung solcher Prädiktionen relevant. Entsprechende prädiktive Analysen stoßen z. B. bei Versicherungskonzernen oder im Rahmen von Einstellungsverfahren auf großes Interesse, weil sie eine individuelle Risikobemessung erlauben. Dabei können Versicherungen ihre Kund:innen auch über Rabattierungsprogramme dazu „nudgen", durch Verwendung prädiktiver Modelle individuell etwas „zu sparen": Sogenannte „Pay-as-you-Drive"-Tarife von KFZ-Versicherungen z. B. verwenden Positions-Tracking und Beschleunigungssensoren in den Fahrzeugen, um mittels prädiktiver Analytik individuelle Versicherungsprämien in Abhängigkeit vom Fahrstil und Aufenthaltsort zu bestimmen.[6]

Eines der wichtigsten Anwendungsfelder prädiktiver Analytik ist die individualisierte Werbung (Targeted Advertising). Die Entscheidung, welche Werbung eines konkreten Internetnutzer:in beim Besuch einer Website oder

3 Vgl. *Mühlhoff*, in: Markschies/Hermann (Hrsg.) #VerantwortungKI – Künstliche Intelligenz und gesellschaftliche Folgen (Bd. 3), 2020.

4 Vgl. *Merchant/Asch/Crutschley/Ungar/Guntuku/Eichstedt/Hill/Padrez/Smith/Schwartz*, PLoS ONE, 14(6), 2019, doi: 10.1371/journal.pone.0215476.

5 Vgl. *Kosinski/Stillwell/Graepel*, Proceedings of the National Academy of Sciences, 110(15): 5802–5805, 2013, doi: 10.1073/pnas. 1218772110.

6 Vgl. *Roth/Aringer/Petersen/Nitschke*, in: Gritzalis/Weippl/Kotsis/Tjoa/Khalil (Eds), Trust, Privacy and Security in Digital Business, 2020.

bei der Benutzung einer Social-Media-Plattform in Echtzeit angezeigt wird, wird unter Einsatz prädiktiver Modelle getroffen. Dabei geht es darum, vorherzusagen, auf welche der im Katalog verfügbaren Werbeanzeigen eine konkrete (jedoch potenziell nicht identifizierte) Nutzer:in am wahrscheinlichsten klicken wird – für diese Vorhersagen werden prinzipiell alle über den/die Nutzer:in verfügbaren Daten verwendet (insbesondere Tracking-Daten, Daten über den Kontext des Werbe-Displays, wenn verfügbar auch Daten aus einem Nutzerprofil inklusive der aufgespeicherten historischen Daten des/der betreffenden Nutzer:in). Das „Engagement" des/der Nutzer:in mit einer Werbeanzeige wird dabei wiederum erfasst (z. B. Click-Tracking), sodass die tatsächliche Relevanz der Anzeige für den/die Nutzer:in mit der Vorhersage ständig abgeglichen werden kann. Die so gewonnenen Engagement-Daten können wiederum als Trainingsdaten in den Targeting-Algorithmus eingespeist werden, sodass das Targeting-Modell sich im laufenden Betrieb ständig selbst verbessert. Solche Verfahren können zu einem erheblichen Datenschutzrisiko werden, wenn der Gegenstand des Targetings z. B. Werbung für Medizinprodukte oder Medikamente ist, in welchem Fall das im Verfahren trainierte prädiktive Modell letztlich die Vorhersage von Krankheiten und somit sensiblen medizinischen Informationen für *beliebige* Plattformnutzer:innen ermöglicht.[7]

Das Credit Scoring ist eine weitere klassische Anwendungsdomäne prädiktiver Analytik. In der Literatur wird betont, dass durch den Einsatz von Big Data- und Machine-Learning-Verfahren ein wichtiger, aber oft übersehener qualitativer Unterschied zu den klassischen SchuFa und FICO-Scores entsteht. Beziehen die klassischen Scores sich für die individuelle Kreditwürdigkeitsbemessung nur auf die historischen Zahlungsdaten des betroffenen Individuums und leiten nach einem fest kodifizierten Prinzip aus dem vergangenen Verhalten eine Prognose über die zukünftige Zahlungsausfallwahrscheinlichkeit des Individuums ab, verwenden die neuen Modelle einen lateralen Abgleich mit vielen *anderen* Individuen[8]: Es sind schließlich die über *viele* Individuen gesammelten Finanzdaten, die zum Training prädiktiver Modelle zum Credit Scoring verwendet werden. Die resultierenden Beurteilungsmuster laufen daher leicht Gefahr, Menschen mit ähnlichen Inputdaten (die stark von ihrer sozio-ökonomischen Herkunft abhängen können) bei der Beurteilung in „Gruppenhaft" zu nehmen.[9] Die neuen Möglichkeiten prädiktiver Analytik anhand von Nutzungsdaten im Internet

7 So argumentieren *Mühlhoff & Willem*, Social Media Advertising for Clinical Studies: Ethical and Data Protection Implications of Online Targeting, 2022 (under review), preprint: https://rainermuehlhoff.de/media/publications/muehlhoff-willem-2022-SMACS-preprint.pdf.

8 Vgl. *O'Neil*, Weapons of Math Destruction, 2017, S. 143.

9 Vgl. *O'Neil* (Fn. 8) S. 145.

haben zusätzlich eine neue, alternative Industrie des Kreditrisikomanagements hervorgebracht. „All data is credit data" lautet der Leitspruch jener Sparte der Finanzindustrie, die mit alternativen Kreditrisikomodellen auch noch diejenigen mit Krediten versorgen möchte, die nach klassischen Beurteilungsmaßstäben nicht kreditwürdig sind: Sogenannte „payday lending"-Anbieter wie das vom Ex-Google-Mitarbeiter *Douglas Merrill* gegründete Fintec-Unternehmen *ZestFinance* oder die deutsche Firma *Kreditec* haben sich auf die Bereitstellung von Krediten und Finanzprodukten „[for] the world's unbanked" spezialisiert, um diese Kohorte mit Kurzkrediten zu versorgen, deren stets individuell berechneter Jahreszinssatz häufig im dreistelligen Bereich liegt.[10]

4.3 Vorhersagemacht als aktuelle Manifestation von Datenmacht

4.3.1.1 Zwei Verarbeitungsschritte: technische Implikationen

Für die ethische und rechtliche Problematisierung prädiktiver Analytik ist es hilfreich, sich zu vergegenwärtigen, dass es im Kontext der beschriebenen Verfahren *zwei* Schritte der Datenverarbeitung gibt, die auseinanderzuhalten sind.

Den ersten Schritt nennen wir das *Training eines prädiktiven Modells*. Hier werden geeignete Daten einer großen Zahl von Individuen, Nutzer:innen oder Vorfällen zusammengetragen, um unter Verwendung geeigneter (maschineller Lern-)Verfahren ein prädiktives Modell im Sinne von 4.2.1 zu trainieren. Bei den Trainingsdaten kann es sich auch um anonymisierte Daten handeln; entscheidend für das Verfahren ist lediglich, dass der Trainingsdatensatz aus Paarungen von „Hilfsdaten" und „Zielinformationen" für die einzelnen Individuen oder Vorfälle bestehen (z. B. Facebook-Likes einer Nutzer:in als Hilfsdaten, ihre explizite Angabe über ihre sexuelle Identität als Zielinformation; Angaben zur Identität der Nutzer:in können dabei gestrichen werden). Das in diesem Verarbeitungsschritt hergestellte prädiktive Modell ist grundsätzlich kein personenbezogenes Datum; es ist eine kalibrierte algorithmische Routine, um *zukünftig* über *beliebige* Indi-

10 Vgl. *O'Dwyer*, Are You Creditworthy? The Algorithm Will Decide, www.undark.org v. 5.7.2018, abrufbar unter https://undark.org/2018/05/07/algorithmic-credit-scoring-machine-learning/ (Stand: 21.9.2022); *Lippert*, ZestFinance issues small, high-rate loans, uses big data to weed out deadbeats, www.washingtonpost.com v. 11.10.2014, abrufbar unter https://www.washingtonpost.com/business/zestfinance-issues-small-high-rate-loans-uses-big-data-to-weed-out-deadbeats/2014/10/10/e34986b6-4d71-11e4-aa5e-7153e466a02d_story.html (Stand: 21.9.2022).

viduen oder Vorfälle eine Abschätzung der Zielvariable vornehmen zu können.

Den zweiten Schritt bezeichnen wir als *Inferenzschritt*. Dabei wird ein vorhandenes prädiktives Modell auf ein konkretes Individuum oder einen konkreten Sachverhalt angewandt, um die Zielinformationen über diesen konkreten Fall abzuschätzen. In der Regel ist dabei das Zielindividuum bekannt und identifizierbar (auch wenn es ggfs. als pseudonyme Nutzer:in einer Plattform in Erscheinung tritt). Verwendet werden für diesen Schritt die über das konkrete Bezugsindividuum gesammelten Hilfsdaten (z. B. Trackingdaten, Facebook-Likes); durch Anwendung des Vorhersagemodells auf diese Input-Daten entsteht eine Vorhersage der Zielinformationen über das Individuum. Im Allgemeinen werden in diesem Verarbeitungsschritt personenbezogene und mitunter auch sensible Informationen über ein identifizierbares Individuum gewonnen.

4.3.2 Vorhersagemacht

Es ist weitgehend unumstritten, dass der zweite Verarbeitungsschritt ethisch bedenklich ist, insofern durch Anwendung eines prädiktiven Modells potenziell ohne das Wissen und ohne die Zustimmung einer betroffenen Person personenbezogene und ggfs. sensible Informationen über sie gewonnen werden können.

Das Problem der Funktionsweise prädiktiver Analytik entsteht jedoch bereits im *ersten* und nicht erst im zweiten der oben skizzierten Verarbeitungsschritte: Hier manifestiert sich noch keine konkrete Privatsphärenverletzung eines konkreten Individuums, doch ein Akteur, der über ein prädiktives Modell verfügt, besitzt das *Vermögen*, über beliebige Individuen bestimmte Informationen anhand von Hilfsdaten abzuschätzen. Es handelt sich um einen Privatsphäreeingriff *in potentia* (dem Vermögen nach), der breite Schichten der Gesellschaft gleichermaßen und potenziell betrifft und „bedroht". Im ersten Verarbeitungsschritt entsteht deshalb das, was wir als *Vorhersagemacht* bezeichnen:[11] ein noch nicht aktualisiertes Vermögen, bestimmte ethisch und rechtlich relevante Handlungen auszuführen.

Wir argumentieren, dass die Instrumente der DSGVO nicht ausreichen, um den gesellschaftlichen und individuellen Risiken durch Vorhersagemacht, die sich meist bei privatwirtschaftlichen und gegebenenfalls auch bei öffentlichen datenverarbeitenden Organisationen akkumulieren, wirkungsvoll zu

11 Vgl. *Mühlhoff*, Predictive Privacy: Collective Data Protection in the Context of AI and Big Data, 2022 (under review), pre-print: https://rainermuehlhoff.de/media/publications/m%C3%BChlhoff_preprint-2022_predictive-privacy-and-collective-data-protection.pdf.

begegnen. Es ist daher ein neues Schutzkonzept notwendig, um das durch Datenakkumulation entstehende Vorhersagevermögen einzelner Akteure rechtlich zu kodifizieren und effektiv zu regulieren.

Diesem Vorhaben liegt eine Konzeption des Privatheits- und Datenschutzes zugrunde, die sich nicht auf den Schutz individueller Privatsphäre verengt, sondern dem Ausgleich informationeller Machtasymmetrien zwischen Gesellschaft und datenverarbeitenden Organisationen dient. Das Diktum *Wilhelm Steinmüllers*, „es geht [beim Datenschutz] nicht um Privatsphäre, sondern darum, eine Technologie sozial beherrschbar zu machen“[12], soll hiermit auf eine aktuelle und neue technologische Situation übertragen werden: die der Big Data- und KI-basierten prädiktiven Analytik, die erst seit den 2000er Jahren entstanden ist. Eine Orientierung des Datenschutzes auf den Ausgleich von Datenmacht wird seit langem debattiert und gelegentlich praktiziert;[13] der neue Beitrag unseres Ansatzes liegt in dem Hinweis, dass die spezifische Machtform der Vorhersagemacht die aktuellste Manifestation von Datenmacht ist.

4.4 Prädiktive Privatheit als ethisches Konzept

4.4.1 Definition

Um zunächst einen ethischen Wert zu konturieren, der durch die Technologien der prädiktiven Analytik potenziell verletzbar ist, greift der Artikel den Begriff der „prädiktiven Privatheit“ auf. Einer von uns hat unter diesem Titel ausgeführt, dass individuelle Privatsphäre auch auf dem Wege der Vorhersage oder Abschätzung von Informationen verletzbar ist, nicht nur durch Informationen, die über das betroffene Individuum explizit erfasst wurden.[14] So definiert *Mühlhoff* prädiktive Privatheit zunächst negativ:

Die prädiktive Privatheit einer Person oder Gruppe ist verletzt, wenn ohne ihr Wissen oder gegen ihren Willen durch den Abgleich mit den Daten vieler anderer Individuen persönliche Informationen über sie vorhergesagt werden.[15]

12 *Rost*, Interview mit Prof. Dr. Wilhelm Steinmüller, 2009, abrufbar unter https://www.maroki.de/pub/video/steinmueller/start_video_steinmueller.html (Stand: 21.9.2022); aktuell *Härting*, Interview mit Ari Ezra Waldmann, in: PinG 2022, 1–2.

13 Vgl. *von Lewinski*, Die Matrix des Datenschutzes, 2014, S. 56 ff.

14 Vgl. *Mühlhoff*, Ethics and Information Technology 23:675–690, 2021, doi: 10.1007/s10676-021-09606-x; *Mühlhoff*, 2020 (Fn. 3).

15 Vgl. *Mühlhoff*, 2021 (Fn. 14).

Dieser Begriff ist juristisch noch nicht direkt subsumtionsfähig, da er sich zunächst nur auf den zweiten der oben genannten Verarbeitungsschritte bezieht. Ethisch betrachtet birgt er jedoch bereits mehrere Herausforderungen:

Der Tatbestand einer Verletzung von Privatheit auf dem Wege der Vorhersage – insbesondere von Vorhersagen, die anhand von Massendaten vieler *anderer* Individuen erstellt wurden – findet bisher kaum gesellschaftliche Beachtung, ist für viele nicht Teil ihres moralischen Bewusstseins rund um Datenschutz und Privatsphäre im Internet, und ist auch akademisch kaum ethisch problematisiert worden.

Mühlhoff weist auf das besondere *Problem der „prediction gap"* hin, wenn algorithmische Prädiktionen in (automatisierte) Handlungsentscheidungen überführt werden[16]: Während die Ausgabe eines Vorhersagemodells im Allgemeinen ein mit individuellen Wahrscheinlichkeiten gewichteter Vektor *möglicher* Werte der Zielvariable ist (z. B. „80 % Übereinstimmung mit den heterosexuellen", „15 % Übereinstimmung mit den homosexuellen", „5 % Übereinstimmung mit den asexuellen", …), muss sich eine Handlungsroutine, die auf einer solchen Vorhersage aufbaut, für einen dieser möglichen Werte entscheiden (z. B. für den mit dem maximalen Wahrscheinlichkeitsgewicht) und wird sodann die Person so behandeln, *als ob* sie diese Eigenschaft besitzt. Im Hintergrund steht hier die Überführung einer statistischen Inferenz, die immer ein populationsbezogenes Wissen ist (Bezug auf die Grundgesamtheit, also alle Individuen), in eine Vorhersage über einen *Einzelfall* (Punkt-Prädiktion). Dieser Schritt ist von klassischer statistischer Argumentationsweise nicht gedeckt und entspricht dem Eingehen einer Wette über das Individuum (ebd.). Dieser Schritt bedeutet eine potenzielle Beschränkung der individuellen Autonomie, die ein ethisches Problem darstellt, das spezifisch für diese Art der Datenverarbeitung ist.

Ein weiteres Spezifikum des ethischen Problems prädiktiver Privatheit ist seine *kollektive Verursachungsstruktur*. Verletzungen prädiktiver Privatheit durch prädiktive Analytik sind nur dann und dort möglich, wo viele Individuen, die für die Herstellung der Modelle nötigen Daten über sich preisgeben und die datenverarbeitenden Organisationen nicht durch Regulierung an der Herstellung und/oder Verwendung solcher Modelle gehindert werden. Sofern der „Datenreichtum" von Plattformunternehmen also wesentliche Bedingung für die Möglichkeit prädiktiver Analytik ist, richten Daten, für deren Preisgabe sich die einzelne Nutzer:in frei entscheidet (z. B., weil sie denkt, „nichts zu verbergen zu haben" oder die Daten einzeln genommen nicht für besonders sensibel hält) potenziell Schaden *für andere* an – jedoch nur, wenn viele andere Einzelindividuen eine ähnliche Entscheidung in Bezug auf ihre Datenfreigebigkeit treffen.

16 *Mühlhoff*, 2021 (Fn. 14).

Dieses Problem der kollektiven Ermöglichung ist dem Problem der individuellen Treibhausgasemissionen im Kontext des Klimawandels ähnlich: Auch hier wirken die individuellen Emissionen als gesellschaftliche Externalitäten, sie gehen also mit Kosten einher, die alle treffen und in die individuelle Kosten-Nutzen-Abwägung des/der Nutzer:in nicht eingepreist sind.[17] Im Unterschied jedoch zur Frage, ob man beispielsweise ein emissionsstarkes oder emissionsarmes Verkehrsmittel benutzen sollte, ist die Entscheidung, ob man einen bestimmten datenbasierten Dienst nutzen sollte, im aktuellen gesellschaftlichen Diskurs ausschließlich als eine *individuelle* Entscheidung und Kosten-Nutzen-Abwägung geframet, das heißt, die potenziellen kollektiven Effekte in Bezug auf Datenschutzfolgen sind diskursiv weitestgehend ausgeblendet.

4.4.2 Prädiktive Privatheit als gesellschaftliches Schutzgut

Während die negative Definition prädiktiver Privatheit für die ethische Debatte (sowohl akademisch als auch gesellschaftlich) bereits Herausforderungen und Neuland bietet, ist diese Definition rechtlich noch schwierig händelbar, weil sie nicht ausreichend zu dem ersten der in 4.3.1 beschriebenen Verarbeitungsschritte vordringt. Für ein regulatorisches Projekt sollte – aus Gründen, die wir hier darstellen – ein Schutzkonzept entwickelt werden, das bereits im Schritt der Vorhersagemacht ansetzt und nicht erst dann greift, wenn sich eine individuelle Privatsphärenverletzung anhand von Prädiktionen manifestiert.

Zu diesem Zweck ist der negativen Definition prädiktiver Privatheit ein positives Verständnis prädiktiver Privatheit als gesellschaftliches Schutzgut beizustellen[18]: Prädiktive Privatheit als gesellschaftliches Schutzgut bezeichnet den Schutz des Gemeinwesens vor negativen Auswirkungen von Vorhersagemacht großer datenverarbeitender Organisationen. Prädiktive Privatheit formuliert somit den – zunächst ethisch begründeten – Anspruch, Individuen und die Gesellschaft im Ganzen gegen die unkontrollierte Akkumulation von Vorhersagemacht als Ausformung informationeller Machtasymmetrie zu schützen.[19]

17 Im Anschluss an diese Überlegungen wurde z. B. das Konzept „data pollution" vorgeschlagen, vgl. *Ben-Shakar*, Journal of Legal Analysis 11: 104–59, 2019, doi: 10.2139/ssrn.3191231.

18 So bereits argumentiert in *Mühlhoff*, 2022, (Fn. 11).

19 Vgl. *Mühlhoff*, 2022 (Fn. 11).

4.5 Das potenzielle rechtliche Schutzgut prädiktiver Privatheit

4.5.1 Offenheit des Schutzgutes Privatheit aus rechtlicher Sicht

Privatheit und Datenschutz sind nicht deckungsgleich,[20] das Gut der Privatheit wird aber durch das Datenschutzrecht ebenfalls geschützt. Während Privatheit als Wert verschiedenste Konnotationen haben kann, bezieht sich das Datenschutzrecht auf die Abwehr spezifischer Gefährdungslagen in der konkreten Situation der Verarbeitung personenbezogener Daten.[21] Vorstellungen von Privatheit sind hingegen nicht auf bestimmte Konzepte oder technische Vorgänge beschränkt. Deutlich wird dies auch durch eine Abstraktion beider Ansätze: Privatheit ist kein tatsächliches oder normativ-rechtlich vordefiniertes Schutzgut, welches typischerweise in einem bestimmten Rechtsbereich normativ eingekleidet wird. Im Gegensatz zu Institutsgarantien, wie dem Eigentum, oder tatsächlichen Vorprägungen, wie dem Schutz des menschlichen Lebens, ist Privatheit sozial konstruiert.[22] Die Bewertung, ob Privatheit als Wert schutzbedürftig ist, muss zwingend auf die Annahmen anderer Disziplinen zurückgreifen, da sie juristisch nicht beantwortet werden kann.[23] Deshalb sind rechtlich abgesicherte Formen des Schutzes von Privatheit besonders entwicklungsoffen gegenüber neuen und interdisziplinären Erkenntnissen, wie dem Konzept der prädiktiven Privatheit.

4.5.2 Individualrechtliche Regelungskonzeption der DSGVO und Grundrechtsdogmatik

Die Schwierigkeiten der DSGVO mit prädiktiven Modellen und abgeleiteten Daten liegen in ihrem Schutzzweck begründet. Datenschutz ist höchstpersönlicher Individualrechtsschutz. Es finden sich in der DSGVO deshalb konsequenterweise nur vereinzelte kollektive Elemente, wie z. B. in Art. 80 DSGVO auf der Ebene der Rechtsdurchsetzung. Die materiell-rechtliche Konstruktion des Datenschutzes beruht auf dem europäischen subjektiv-individuellen Grundrechtsverständnis.[24] Dass diese Ausrichtung zu Schutzlücken in der Praxis führt, ist unbestritten und zeigt sich am deutlichsten im Fall der Einwilligung als dem praktisch immer noch wichtigsten Erlaubnistatbestand für die Verarbeitung personenbezogener Daten.

---

20 Zur Abgrenzung: *Eichenhofer*, 2021 (Fn. 1), S. 51 ff.
21 *Eichenhofer*, 2021 (Fn. 1), S. 51.
22 *Gusy*, Jahrbuch des öffentlichen Rechts der Gegenwart. Neue Folge (JöR) 70, 2022, S. 415, 416.
23 *Gusy*, 2022 (Fn. 22), S. 415, 416.
24 Grundlegend: *Britz*, in: Hoffmann-Riem/Brandt (Hrsg.), Offene Rechtswissenschaft, 2010, S. 561 ff.

Der Aspekt, dass prädiktive Modelle nur durch die Verarbeitung einer Vielzahl von Daten verschiedener Personen erfolgen kann, ist rechtlich zurzeit nicht abgebildet. Dies setzt sich fort in der Beschränkung der DSGVO auf den Personenbezug. Abgeleitete Daten, auch aus anonymisierten Daten, lassen u. U. Schlüsse über höchstpersönliche Eigenschaften zu. Die Begrenzung der DSGVO auf den Prozess der personenbezogenen Datenverarbeitung berücksichtigt deshalb das kollektive Element der Modellierung nicht. Dem wird auch nicht dadurch abgeholfen, dass die Verwendung der Ergebnisse des Prädiktionsmodells, z. B. für Targeted Advertising, in den Anwendungsbereich der DSGVO fallen kann, wie Einzelbeispiele aus der Rechtsprechung zeigen (dazu 4.8).

Es ist ein Dilemma der europäischen Grundrechtskonstruktion[25], dass kollektive Rechtsgüter einem Vollzugs- und Durchsetzungsdefizit unterliegen, wie auch das Beispiel des Umweltrechts[26] ausdrücklich zeigt. Im Bereich des Datenschutzes sind die grundrechtstheoretischen Annahmen der Höchstpersönlichkeit der informationellen Selbstbestimmung durch die technischen Entwicklungen nicht mehr in der Praxis reflektiert. Dadurch stößt Datenschutzrecht zwingend an Grenzen. Eine Neukonzeption sollte den Blick für alternative theoretische Grundlagen weiten, anstatt die subjektiv-rechtliche Ausrichtung weiter überzustrapazieren. Dazu gehört auch, zu hinterfragen, ob die beschriebenen betroffenen kollektiven Rechtsgüter im Datenschutzrecht verankert werden sollten oder ob es Alternativen gibt. Die dogmatische Konstruktion des Rechts auf informationelle Selbstbestimmung als „akzessorisches Recht" steht diesen Überlegungen nicht entgegen, sondern öffnet die Tür zu kollektiven Elementen. Denn die Akzessorietät könnte sich auch auf neue, noch zu entwickelnde Rechtsgüter beziehen, wie die prädiktive Privatheit.

Der Schutz kollektiver Rechtsgüter ist der Rechtsordnung bekannt und wird z. B. im Strafrecht viel diskutiert.[27] Daraus folgt auch, dass nicht jeder Rechtsgüterschutz unmittelbar auf der Ebene der Grundrechte Niederschlag finden müsste. Die ausdrücklich normierte kollektive Dimension der Grundrechte ist zu Recht auf Art. 9 GG beschränkt.[28] Auch sonst steht das individuelle Grundrechtsverständnis einer Weiterentwicklung informationeller Selbstbestimmung in Richtung kollektiver Elemente nicht entgegen:

25 Umfassende Kritik der subjektiven Rechte bei *Menke*, Kritik der Rechte, 2018, S. 175 ff.
26 Zu kollektiven Rechten zum Erhalt der natürlichen Lebensgrundlagen: *Madjidian*, FoR 2011, S. 117 ff.
27 Statt vieler: *Aldoney Ramírez*, Der strafrechtliche Schutz von Geschäfts- und Betriebsgeheimnissen, 2009, S. 322 ff.
28 Zur Kehrseite der kollektiven Grundrechtseinwirkungen *Ruschemeier*, RW, 2020, S. 449 ff.

manche Freiheitsgewährleistungen, wie die Versammlungsfreiheit, sind nur kollektiv realisierbar.[29]

4.6 Anwendungsbereich der DSGVO: fehlende Erfassung prädiktiver Analytik

4.6.1 Einordnung in den Kontext von Angriffstypen im Datenschutz

Die rechtlichen Schutzlücken der DSGVO in Bezug auf prädiktive Modelle und ihre kollektive Verursachungsstruktur (siehe 4.4.1) zeigen sich besonders deutlich durch einen historischen Vergleich mit anderen wesentlichen Typen potenzieller Grundrechtsverletzungen durch Datenverarbeitung, die *de lege lata* in den Anwendungsbereich des Datenschutzrechts fallen.

Über die letzten 60 Jahre ist die Entwicklung des Datenschutzes stets mit wechselnden, gesellschaftlich und kulturell dominierenden Vorstellungen von möglichen Angriffsszenarien verknüpft gewesen. Insofern diese Angriffsszenarien mit jeweils aktuellen technologischen Entwicklungen und Neuerungen korrelieren, führt jede technologische Entwicklung potenziell auch zu neuen Anforderungen daran, was Datenschutz leisten soll. In einer groben Typologie ist es gewinnbringend, im Folgenden intrusive Privatheitsverletzungen von Re-Identifikationsangriffen, und diese wiederum von prädiktiven Privatheitsverletzungen zu unterscheiden.[30]

Das Angriffsszenario der *Intrusion* bezeichnet den klassischen unautorisierten Zugriff auf eine als vertraulich, abgeschirmt oder „privat" definierte Informationssphäre. Das kann z. B. durch unautorisierte Weitergabe anvertrauter Informationen, durch Einbrüche in Informationsverarbeitungssysteme von außen oder durch Ausnutzung von Schwachstellen solcher Systeme geschehen (Hacking, Spionage, Geheimdienstaktivitäten). Die wesentliche Struktur ist hier der gezielt beschaffte Zugriff auf Daten durch Unautorisierte, die eigentlich keinen Zugriff haben sollten (weil er durch Barrieren verhindert wird oder weil es, wie im Fall der Persönlichkeits- oder Intimsphären, moralisch nicht geboten ist). Nicht erst mit dem Aufkommen der elektronischen Datenverarbeitung wurde intrusiver Informationszugriff als Problem von Privatheit gefasst, siehe etwa das Aufkommen des modernen Rechts auf „Privacy" im amerikanischen Diskurs, veranlasst durch neue technische Möglichkeiten der

29 Zur kollektiven Dimension des Art. 19 Abs. 3 GG *Ingold*, Der Staat 53, 2014, S. 193 (196 ff.).

30 Vgl. *Mühlhoff*, Blätter für Deutsche und Internationale Politik 8: 13–16, 2020.

Fotografie.[31] Konzeptuell entscheidend ist, dass sich der Angriffstyp der Intrusion gezielt auf *bestimmte* Datensubjekte richtet und die gewaltsame Überschreitung einer technisch, moralisch oder rechtlich verbrieften Informationsbarriere beinhaltet, mit dem Ziel eigentlich unzugängliche Informationen zu beschaffen. Die Intrusion von Datenverarbeitungssystemen ist mangels Rechtsgrundlage und Betroffenheit personenbezogener Daten eine Verletzung von Art. 6 Abs. 1 DSGVO und damit unzweifelhaft rechtswidrig.

In den 1980er und 1990er Jahren wurde durch die steigende Verbreitung elektronischer Massendatenverarbeitung ein von der Intrusion qualitativ zu unterscheidender Angriffstyp als Problem des Datenschutzes virulent: die Gefahr der *Re-Identifikation* in statistischen Datensätzen. Z. B. durch die Digitalisierung des Gesundheitssystems trat die Situation auf, dass Einrichtungen wie Krankenhäuser oder Krankenversicherungen über digitale Patientendaten vieler tausend Patient:innen verfügten. Der nahezu flächendeckende Einsatz dieser Verfahren und die somit nahezu vollständige digitale Erfassung weiter Bevölkerungsteile hat sodann die Idee hervorgebracht, diesen „Datenreichtum" für statistische Zwecke auszunutzen, das heißt, z. B. aus den Daten vieler medizinischer Versorgungsvorgänge statistische Auswertungen über die medizinische Versorgung zu gewinnen. In diesem Kontext sind dann Anonymisierungsverfahren entstanden, die dem Zweck dienen sollten, zwar die einzelnen Individuen in den aggregierten Datensätzen zu schützen, zugleich aber den statistischen Wert der Datensätze zu erhalten.

In einem prominenten Fall wurden etwa im US-Bundesstaat Massachusetts in den 1990er Jahren die medizinischen Behandlungsdaten von rund 135000 staatlichen Bediensteten und ihren Familienangehörigen „anonymisiert" in einer Datenbank zu Forschungszwecken zusammengetragen. Es gelang jedoch der damaligen Informatikstudentin *Latanya Sweeney* durch das Kombinieren dieser Daten mit öffentlich zugänglichen Informationen aus dem Wähler:innen-Register von Massachusetts, die Krankenakte des damaligen Gouverneurs von Massachusetts, *William Weld*, zu rekonstruieren.[32] Der Vorfall sorgte für erhebliches Aufsehen und hat die Debatte um den Datenschutz in den Vereinigten Staaten stark geprägt. In der Informatik gilt *Sweeneys* Vorgehen als Musterbeispiel für einen Angriffstyp, der Informationen aus anderen zugänglichen Quellen heranzieht, um Personen in vermeintlich anonymisierten oder pseudonymisierten Datensätzen zu re-identifizieren. In der mathematischen Theorie der Datenbanksicherheit ist das

31 Vgl. *Warren/Brandeis*, in: Harvard Law Review 14(5):193–220, 1890; Tavani, Metaphilosophy 38(1): 1–22, 2007, doi: 10.1111/j.1467-9973.2006.00474.x.

32 Vgl. *Sweeney*, The Journal of Law, Medicine & Ethics, 25(2–3): 98–110, 1997, doi: 10.1111/j.1748-720x.1997.tb01885.x.

Prädikat „anonym“ heute daher nicht mehr gleichbedeutend mit „sicher“, sondern stellt ein stark vom Kontext abhängiges Kriterium dar.[33]

Sweeneys Projekt hatte starken regulatorischen Einfluss, denn es hat einen neuen Angriffsvektor auf Privatheit im Kontext elektronischer Massendatenverarbeitung zum Vorschein gebracht, der insbesondere im Kontext medizinischer Daten in der folgenden Zeit viel beachtet wurde (dies hat z. B. den US-amerikanischen *Health Insurance Portability and Accountability Act* (HIPAA) mit geprägt).[34] Konzeptuell ist der Angriffstyp der Re-Identifikation folgendermaßen zu charakterisieren: Es handelt sich wie bei der Intrusion um einen zielgerichteten Angriff auf einzelne Datensubjekte. Dabei werden jedoch keine technischen oder ethisch-moralischen Zugriffsbarrieren durchbrochen; Grundlage für den Angriff bilden vielmehr Daten, die gezielt, jedoch mit einem Anonymitätsversprechen veröffentlicht wurden. Einige Varianten von Re-Identifikationsangriffen nutzen dabei die Tatsache aus, dass in einem vermeintlich anonymisierten Datensatz die Informationen *vieler* Individuen enthalten sind – auch wenn die Attacke potenziell eine Einzelperson trifft, ist sie mitunter nur möglich, wenn der Datensatz auch die Daten vieler anderer enthält.[35] Zwar fällt die Verarbeitung anonymisierter Daten nicht in den Anwendungsbereich der DSGVO, in dem Moment, in dem Personen aber (re)-identifiziert werden, liegt eine erlaubnispflichtige Datenverarbeitung vor. Auch pseudonymisierte Daten weisen Personenbezug auf. Die konkreten rechtlichen Anforderungen an eine Anonymisierung von Daten sind umstritten (siehe 4.7).

Der Angriffsvektor *prädiktiver Privatheitsverletzung* stellt ein qualitativ von Intrusion und Re-Identifikation unterschiedenes Angriffsszenario dar (siehe Tabelle 1): Der markanteste und ethisch wie rechtlich folgenreichste Unterschied zur Re-Identifikation besteht darin, dass

1. prädiktive Angriffe potenziell Datensubjekte betreffen, die selbst nicht in den Trainingsdaten, die dem prädiktiven Modell zugrunde liegen, enthalten sind;
2. und darüber hinaus auch solche Informationen abzuschätzen erlauben, die das betroffene Datensubjekt selbst niemals preisgegeben hat (denn „sen-

33 Vgl. *Sweeney*, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5): 557–70, 2002, doi: 10.1142/S0218488502001648.

34 Vgl. *Ohm*, UCLA Law Review 57: 1701–1777, 2010.

35 Vgl. als weitere Beispiele für solche Attacken: *de Montjoye/Hidalgo/Verleysen/Blondel*, Scientific Reports 3(1), 2013, doi: 10.1038/srep01376; *Gymrek/McGuire/Golan/Halperin/Erlich*, Science 339(6117): 321–24, 2013, doi: 10.1126/science.1229566; *Narayanan/Shmatikov*, IEEE Symposium on Security and Privacy, 2008, doi: 10.1109/SP.2008.33; *Shokri/Stronati/Song/Shmatikov*, Proceedings of the IEEE Symposium on Security and Privacy, 2017, doi: 10.1109/SP.2017.41.

siblere“ Daten werden hier aus scheinbar weniger „sensiblen“ Daten abgeleitet).

Wir nennen dies die zweifache *Eskalationsstruktur* prädiktiver Angriffe. Im Vergleich dazu bringen Re-Identifikationsangriffe (1) nur Daten über Individuen hervor, die in dem anonymisiert veröffentlichten Datensatz enthalten sind und (2) nur Datenfelder, die über diese Individuen explizit erfasst wurden. Prädiktive Modelle dagegen können (1) auf beliebige dritte Individuen angewendet werden, sobald über sie Hilfsdaten (Input für das prädiktive Modell, z. B. Nutzungsdaten auf einer Social-Media-Plattform) bekannt sind, und (2) Informationen abschätzen, die die betroffenen Individuen gegenüber keiner dritten Partei jemals angegeben haben oder die sie vielleicht selbst nicht wissen (z. B. Krankheitsprognosen).[36] Ein weiteres Spezifikum prädiktiver Angriffe liegt darin, dass es sich dabei typischerweise um Streuangriffe handelt, die durch automatisierte Routinen auf viele Individuen (etwa: alle Nutzer:innen einer Social-Media-Plattform) potenziell und gleichzeitig angewendet werden; diese Methode beschränkt sich deshalb nicht auf gezielte Einzelangriffe auf bestimmte Datensubjekte. Z. B.: Sobald wenige, aber ausreichend viele Nutzer:innen einer großen Social-Media-Plattform in ihrem Profil explizit angegeben haben, dass sie rauchen, ist die Plattform in der Lage, ein prädiktives Modell zu trainieren, welches Nikotinkonsum anhand von Nutzungsdaten auf der Plattform abzuschätzen erlaubt. Dieses prädiktive Modell kann dann automatisiert auf *alle* Plattform-Nutzer:innen angewandt werden, sodass die Plattform in der Lage ist, diese Information, die die Mehrheit der Nutzer:innen eigentlich nicht angegeben hat, z. B. als mögliches Targeting-Kriterium für Werbekund:innen anzubieten.

Tabelle 1: Qualitativer Vergleich dominanter Angriffstypen

	Intrusion	Re-Identifikation	Prädiktion
Gewaltsamer Durchbruch von Zugriffsbarrieren?	JA	NEIN	NEIN
Zielsubjekt muss in den Daten sein?	JA	JA	NEIN
Bringt nur Informationen hervor, die über das Datensubjekt explizit erfasst wurden	JA	JA	NEIN
Beruht auf Massendaten	NEIN	JA	JA
Gezielter/individualisierter Angriff oder Streuangriff?	individualisiert	individualisiert	Streuangriff

36 Vgl. *Mühlhoff*, 2021 (Fn. 14).

4.6.2 Zwei Verarbeitungsschritte: rechtliche Implikation

Der Anwendungsbereich der DSGVO setzt die Verarbeitung personenbezogener Daten voraus. Daten, die statistischer Art oder aggregiert sind, weisen dann keinen Personenbezug auf, wenn sie sich auf eine Personengruppe beziehen.[37] Haben die Informationen, die im ersten Schritt bei der Erstellung prädiktiver Modelle genutzt werden, keinen Personenbezug, ist der Anwendungsbereich der DSGVO nicht eröffnet. Allerdings können die Korrelationen dazu führen, dass vermeintlich anonymisierte Daten doch wieder individuell zugeordnet werden können.[38] Wo die Grenze des Personenbezugs bei prädiktiven Modellen normativ liegt, ist unklar.[39] Geht man von einer niedrigen Schwelle aus, dürfte der größte Anteil prädiktiver Modelle unter die DSGVO fallen. Insbesondere, wenn man das überzeugende Drei-Elemente-Modell der Artikel-29-Datenschutzgruppe heranzieht.[40] Danach ist ein personenbezogenes Datum alternativ entweder bei einem Inhaltselement, Zweckelement oder Ergebniselement gegeben. Unabhängig von Zweck oder Ergebnis kann der Personenbezug damit auch bei Daten gegeben sein, die sich von Dritten ableiten, sich aber auf eine individualisierte Person beziehen.[41] Danach fallen die Ergebnisse (Inferenzen) prädiktiver Modelle in Form des zweiten Schritts der konkreten Prognose auch in den Anwendungsbereich der DSGVO. Das kollektive Element der Modellerstellung als Wechselwirkung ist hingegen nicht abgebildet. Denn die betroffene Person muss nicht selbst mit personenbezogenen Daten in der Modellerstellung auftauchen: Es ist ausreichend, dass Dritte ihre personenbezogenen Daten angeben. Betroffene im Sinne der DSGVO sind bei Modellerstellung (Training) und Anwendung (Inferenz) nicht deckungsgleich.

4.6.3 Verifizierbarkeit ist keine Voraussetzung des Personenbezugs

Die Verifizierbarkeit von Informationen hat keinen Einfluss darauf, ob sie als personenbezogene Daten zu qualifizieren sind. Ein Argument, dass nicht verifizierbare Informationen keine personenbezogenen Daten sein können, stützt sich darauf, dass das Betroffenenrecht des Art. 16 DSGVO (Recht auf Berichtigung) nicht anwendbar sei. Daraus folge, dass der gesamte Anwen-

37 *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), DS-GVO BDSG, 3. Aufl. 2020, Art. 4 Nr. 1 DSGVO, Rn. 15.
38 *Klar/Kühling* (Fn. 37), Art. 4 Nr. 1 DSGVO, Rn. 22.
39 Gegen den Personenbezug als rechtliches Kriterium: *Schmitz*, ZD 2018, S. 5 ff.
40 Artikel-29-Datenschutzgruppe, WP 136 – Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 20.6.2007, S. 11.
41 *Kühling*, DuD 45, 2021, S. 168 (169–171).

dungsbereich der DSGVO nicht eröffnet sei.[42] Darin liegt ein systematischer Fehlschluss: die Betroffenenrechte setzen voraus, dass der Anwendungsbereich der DSGVO eröffnet ist und nicht umgekehrt. Der Anwendungsbereich der DSGVO kann nicht von der Anwendbarkeit der Betroffenenrechte abhängen, da andernfalls alle weiteren Vorschriften obsolet wären. Bezüglich abgeleiteter Daten wird argumentiert, dass diese als Wahrscheinlichkeitsaussagen zu qualifizieren und damit nicht verifizierbar seien, ergo keine personenbezogenen Daten. Das trifft zu, wenn auf den Inhalt der Prognose abgestellt wird, z. B. dass Person A in der nächsten Zeit ein Haus kaufen oder straffällig wird. Der Zweck der Datenverarbeitung des prädiktiven Modells kann aber aufgrund der technischen Funktionsweise schon nicht die Richtigkeit der Aussage an sich, sondern die effiziente Prognoseerstellung sein. Legt man dies zugrunde, kann das Recht auf Berichtigung sich bei abgeleiteten Daten nicht auf das Prognoseergebnis, sondern allein auf die statistische Methodik beziehen. Hieran wird deutlich, dass eine Schutzlücke in Bezug auf die Ergebnisse prädiktiver Modelle besteht, die durch das von Wachter und Mittelstadt entwickelte *Right to Reasonable Inferences* geschlossen werden soll.[43]

Die spezifisch kollektiven Auswirkungen prädiktiver Modelle verdeutlichen hingegen den Unterschied zum *Right to Reasonable Inferences*[44], wo es darum geht, die Darstellung des Individuums durch abgeleitete Daten zu schützen (*Right on How to Be Seen*). Das kollektive Element der prädiktiven Datenanalyse wird durch neue individuell ausgerichtete Rechtspositionen wie ein *Right to Reasonable Inferences (RRI)* nicht erfasst; dieses kann sich allenfalls an die kollektive Datenauswertung anschließen. Die Ziele des RRI, einen Dialog mit den Betroffenen und der Gesellschaft darüber zu eröffnen, welche Verarbeitungspraktiken normativ akzeptabel sind,[45] verfolgen auch die Konzepte der prädiktiven Privatheit und kollektive Ansätze des Datenschutzes. Allerdings stoßen Individualrechte zwingend an ihre Grenzen, wenn es um überindividuelle Auswirkungen geht, hier ist eine grundlegend andere Ausrichtung erforderlich, auch um strukturelle Machtasymmetrien auszugleichen. Die Idee kollektiver Elemente des Datenschutzes kann sich mit dem RRI wechselseitig ergänzen.

Zudem können auch nicht verifizierbare Informationen Auswirkungen auf Betroffene haben, da diese nicht beeinflussen können, wie entsprechende Prognosen ausgelegt werden. Der EuGH wird dahingehend interpretiert,

42 *Malgieri*, PinG 2016, S. 133 (138) möchte für abgeleitete Daten nur „Verbraucherinnenrechte" und keine Betroffenenrechte einräumen; so auch die Argumentation der Beklagten in BVwG Österreich Teilanerkenntnis v. 26.11.2020 – W258 2217446-1/35E, BeckRS 2020, 51953 Rn. 61.

43 *Wachter/Mittelstadt*, Columbia Business Law Review 2019, S. 1.

44 *Wachter/Mittelstadt*, 2019 (Fn. 43).

45 *Wachter/Mittelstadt*, 2019 (Fn. 43) S. 1 (92).

dass er die Aufgabe des Datenschutzes nicht darin sieht, richtige Entscheidungen zu garantieren.[46] In Bezug auf Verwaltungsvorgänge im staatlichen Bereich ist dies überzeugend, denn dort existieren andere Mechanismen, welche die Richtigkeit der Entscheidung sichern (Rechtsschutz, Gesetzesbindung, rechtsstaatliche Verfahrensvorschriften). Die Argumentation des Schutzzwecks kann nur in die Richtung zielen, dass Datenschutzrecht bei abgeleiteten Daten dann nicht anwendbar ist, wenn es kontextbezogene andere Sicherheitsmechanismen hinsichtlich der Rechte der Betroffenen gibt. Daraus muss nicht zwingend im Umkehrschluss folgen, dass Datenschutz keine Handhabe gegen falsche Ableitungen bereitstellen kann, wenn anderweitige Sicherungsmechanismen ausscheiden und es allein um die Datenanalyse zum Zweck der Herstellung des prädiktiven Modells geht.

4.7 Anonymisierung und Betroffenenrechte

Daran schließt sich die Frage an, welche Betroffenenrechte bei prädiktiver Analytik *de lege lata* einschlägig sind und wie effektiv diese gegen kollektive und individuelle Beeinträchtigungen schützen.

Wie bereits erläutert, ist der erste Schritt der Erstellung des prädiktiven Modells (siehe 4.3.1) von der DSGVO nicht erfasst, wenn es sich nicht um personenbezogene Daten handelt, diese anonymisiert sind oder den Individuen nicht zugeordnet werden können, deren Informationen verarbeitet werden.[47] Auch gegenüber der Verwendung personenbezogener Daten, um Prognosen über *Dritte* zu erstellen, sieht die DSGVO keine Handhabung vor; das Verständnis der Betroffenenrechte ist stets auf die eigenen Daten begrenzt. Voraussetzung für die Betroffenenrechte sind das Vorliegen personenbezogener Daten, deren Zuordnung zu einer individuellen Person und die jeweiligen Tatbestandsvoraussetzungen des Rechts.

4.7.1 Anonymisierung als erlaubnispflichtige Datenverarbeitung und Regulierung prädiktiver Modelle?

An die Anonymisierung von Daten als potenziellen Verarbeitungsschritt bei der Erstellung eines prädiktiven Modells anzuknüpfen, löst die Problematik der Kollektivität nicht. Inwieweit absolute und relative Anonymisierungs-

46 *Wachter/Mittelstadt*, 2019 (Fn. 43) S. 1 (58).

47 Zur Unterscheidung von personenbezogenen und nicht-personenbezogenen Daten: *Finck/Pallas*, International Data Privacy Law, 10, 2020, doi: 10.1093/idpl/ipz026, S. 11. Die Löschpflicht der DSGVO sollte nicht durch Anonymisierung erfolgen können: *Roßnagel*, ZD, 2021, S. 188 (191 f.).

techniken überhaupt hinreichenden Schutz vor De-Identifikation bei Big Data Analysen gewähren können, ist zweifelhaft (siehe 4.6.1).[48]

Vielmehr ist die Frage der Sicherheit von Anonymisierung im Kontext prädiktiver Analytik für das Datenschutzrisiko prädiktiver Angriffe irrelevant, denn Prädiktion beruht nicht auf Re-Identifikation und kann sogar Individuen treffen, die gar nicht in dem zugrundeliegenden anonymisierten Datensatz enthalten sind. Mehr noch: In der Kommunikationsstrategie großer Plattformunternehmen werden Anonymisierungsversprechen als Mittel eingesetzt, Zustimmung für die Verarbeitung und Auswertung persönlicher Daten von Nutzer:innen „zu statistischen Zwecken" einzuholen, da sich die Nutzer:innen mit dem Schutz ihrer eigenen Anonymität in ihren Datenschutz- und Privatheitsbedürfnissen befriedet sehen. Im Kontext prädiktiver Privatheit ist diese Kommunikationsstrategie kontraproduktiv, denn das Training prädiktiver Modelle kann anhand von anonymisierten Daten erfolgen; eine Anonymisierung zu versprechen *ermöglicht* also diskursstrategisch die Herstellung prädiktiver Modelle.

Aus rechtlicher Perspektive definiert die DSGVO Anonymisierung selbst nicht, was zunächst nicht verwundert, da anonyme Daten *prima facie* gerade nicht in den Anwendungsbereich der Verordnung fallen. Ob die Anonymisierung von Daten eine rechtfertigungsbedürftige Datenverarbeitung ist und damit dem Erlaubnisvorbehalt des Art. 6 Abs. 1 DSGVO unterfällt, ist umstritten.[49] Das Recht auf Datenschutz soll durch Anonymisierung nicht berührt sein, liegt doch gerade kein personenbezogenes Datum mehr vor. Selbst wenn man davon ausgeht, dass eine Anonymisierung von Daten unter der DSGVO erlaubnispflichtig ist, zielen diese Argumente darauf, dass Personen ein Interesse daran haben, dass ihre personenbezogenen Daten erhalten bleiben.[50] Bezüglich prädiktiver Privatheit geht es aber um die Verhinderung der *sekundären* Datennutzung. Prädiktive Analysen zeigen gerade, dass es verschiedene Verwendungsmöglichkeiten anonymisierter Daten durch den Verarbeiter gibt. Problematisch dabei ist nicht der Vorgang des Anonymisierens, sondern die nachfolgende Verwendung der anonymen Daten zur Modellerstellung. Diese sekundäre Informationsverarbeitung ist in keinem Fall von der DSGVO erfasst.

48 Bereits: *Ohm*, UCLA Law Rev. 2009, S. 1701 ff.

49 Dafür: *Hornung/Wagner*, ZD 2020, S. 223; *Krebs/Hagenweiler*, Datenanonymisierung im Kontext von Künstlicher Intelligenz und Big Data, 2022, S. 126 ff.; *Kneuper*, Datenschutz für Softwareentwicklung und IT, 2021, S. 144; Positionspapier BfDI 29.6.2020, abrufbar unter: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/Positionen/Positionspapier-Anonymisierung-DSGVO-TKG.html (Stand: 21.9.2022); *Raji*, DuD 45 (2021), S. 303 (307); *Roßnagel*, 2021 (Fn. 47) S. 188 (189); a.A. mit beachtlichen Argumenten *Thüsing/Rombey*, ZD 2021, S. 548 f..

50 *Hornung/Wagner*, 2020 (Fn. 48) S. 223 (225) bejahen eine teleologische Reduktion, wenn keine grundrechtlich geschützten Interessen berührt sind.

Rein praktisch wird zudem eine Einwilligung seitens der Betroffenen wohl stets erteilt werden, gegen die Anonymisierung der eigenen Daten wird es wenige Einwände geben. Mangels Zweckbindung des prädiktiven Modells werden die kollektiven Dimensionen auch dann nicht offengelegt. Eine andere Problematik ist, inwieweit die Anonymisierung oder Löschung von bestimmten Daten zu anderen, ggf. unpräziseren Prädiktionen des Modells führen kann und ob betroffene Personen einen „Berichtigungsanspruch" haben.[51]

4.7.2 Betroffenenrechte

Auch die Betroffenenrechte der DSGVO führen angesichts des Risikos prädiktiver Analytik nicht weiter. Wenn das Auskunftsrecht des Art. 15 DSGVO einschlägig ist und im Anschluss die Löschung der eigenen Daten ermöglicht, stellt sich die Anschlussfrage, wie viele Datensubjekte die Löschungen ihrer Daten beanspruchen müssten, damit das prädiktive Modell nicht mehr funktioniert. Die individuelle Rechtsdurchsetzung gerät hier ebenso wie im Fall der Einwilligung an ihre Grenzen, da Auskunfts- und Löschungsrechte wiederum als höchstpersönliche Rechte der betroffenen Person zustehen. Selbiges gilt für die Transparenzpflichten der Art. 13 und 14 DSGVO; die Information, dass die eigenen Daten zu Prognosen über andere verwendet werden, ist nicht vom Schutzzweck der Norm umfasst, da dieser rein individuell verstanden wird.[52] Konsequenterweise bezieht sich der Berichtigungsanspruch damit nur auf die Methodik der Prognoseerstellung.

Im Kontext von „Künstlicher Intelligenz" und DSGVO wird oft darauf hingewiesen, dass das Recht auf Löschung, Art. 17 DSGVO, mit der Funktionsweise maschinell lernender Systeme in Konflikt gerät. Denn aus dem trainierten algorithmischen Modell können einzelne Datengrundlagen nicht singulär gelöscht werden, die Lösung dieses Problems ist offen.[53] In Bezug auf die kollektiven Auswirkungen prädiktiver Modelle müssten zudem erhebliche Datenmengen gelöscht werden, um das Vorhersagepotenzial des Modells überhaupt beeinflussen zu können, da Art. 17 DSGVO aber als Individualrecht ausgestaltet ist, dürften einzelne Löschung keine Auswirkungen haben.[54]

Art. 22 Abs. 1 DSGVO regelt nach überwiegender Auffassung ein Verbot vollautomatisierter Entscheidungen. Aufgrund des engen Verständnisses der

---

51 Zum Anspruch auf eine „Richtigkeit" der Ableitungen über individuelle Personen: *Wachter/Mittelstadt*, 2019 (Fn. 43) S. 1.

52 Statt aller: *Paal/Hennemann*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2021, Art. 13 DSGVO, Rn. 4.

53 Vgl. auch *Hornung*, in: Hoffmann-Riem (Hrsg.), Big Data – Regulative Herausforderungen, 2018, S. 81, 86.

54 *Hermstrüwer*, in: Hoffmann-Riem (Hrsg.), Big Data – Regulative Herausforderungen, 2018, S. 99, 106.

„ausschließlich auf einer vollautomatisierten Verarbeitung beruhenden Entscheidung", hat die ursprünglich als „KI-Vorschrift" gehandelte Norm sehr geringe praktische Relevanz. Denn durch einen *Human in the Loop*, der den *Output* eines Systems bestätigt, ist die Entscheidung nicht mehr vollautomatisiert, sondern das System fungiert entscheidungsunterstützend. Die von Art. 22 Abs. 3 DSGVO geforderten Maßnahmen beziehen sich als eine der wenigen Vorschriften auf das Ergebnis und nicht den Vorgang der Datenverarbeitung.[55] Als Verfahrensrechte von Betroffenen sind mindestens das Recht auf Erwirkung des Eingreifens einer Person, Darlegung des eigenen Standpunktes und Anfechtung der Entscheidung garantiert. Dies bezieht sich aber wiederum nur auf vollautomatisierte Entscheidungen bezüglich der jeweils betroffenen Person und nicht auf die vorgelagerte kollektive Datenauswertung zur Herstellung eines prädiktiven Modells. Auf dieser Ebene sind auch ähnliche Beeinträchtigungen i. S. d. Art. 22 Abs. 1 DSGVO schwer zu bestimmen; rechtliche Wirkung dürfte ihnen in den wenigsten Fällen zukommen.

4.7.3 Abgeleitete Daten als personenbezogene Daten: Beispiel Statistik

Nicht nur private Unternehmen nutzen prädiktive Analytik, auch staatliche Stellen greifen vermehrt auf solche Modelle zu. Neben den viel diskutierten Fällen des *Predictive Policings*, welches in Deutschland bisher nur in Bezug auf geografische und nicht-personenbezogene Vorhersagen zum Einsatz kommt, ist Imputation eine klassische Methode der amtlichen Statistik. Dabei werden fehlende Daten, z. B. aufgrund ausgefallener Antworten, durch verschiedene Methoden imputiert. Es wird eine Gruppe berechnet, deren Schätzwerte dem Wert im unvollständigen Datensatz am nächsten kommen und eine beliebige Person ausgewählt, deren Wert sodann im fehlenden Datensatz imputiert wird. Auch hier ist umstritten, ob es sich bei den imputierten Informationen um personenbezogene Daten handelt.

Ausgehend vom Auskunftsanspruch des Art. 15 Abs. 1 DSGVO lässt sich ein weites Verständnis des Begriffs der personenbezogenen Daten im Zusammenhang mit Art. 4 Nr. 1 DSGVO zugrunde legen, nachdem sich die Daten auf eine natürliche Person beziehen müssen. Dieses Kriterium erfüllen auch imputierte Daten. Andererseits ist der Auskunftsanspruch des Art. 15 Abs. 1 DSGVO an einen Aussagegehalt der Daten über die betreffende Person geknüpft. Imputierte Daten werden jedoch technisch generiert aus Daten Dritter und das lediglich für statistische Zwecke. Sie haben keinen Anspruch auf Richtigkeit oder einen Aussagegehalt in Bezug auf die Person. Wenn man nach Art. 15 Abs. 1 DSGVO für personenbezogene Daten, Art. 4 Nr. 1

55 *Wachter/Mittelstadt*, 2019 (Fn. 43) S. 1 (79).

DSGVO also einen inhaltlichen Bezug zur Person verlangt, fallen imputierte Daten nicht unter diesen Begriff.[56]

Dabei geht es nicht um den Inhalt, sondern um die Funktion. Diese kann man auf verschiedene Arten auslegen: erschöpft sich der Zweck der imputierten Daten in ihrer technischen Hilfsfunktion, bezieht sich die Vermutung der Richtigkeit nur auf die Person des ohnehin vollständigen Datensatzes. Versteht man den Zweck der Imputation darin, die Funktion der Information gerade auszublenden, da die imputierten Werte nicht anders als die erhobenen Werte behandelt werden, bezieht sie sich inhaltlich auf eine zumindest identifizierbare Person. Denn die Information leitet sich von B aus dem vollständigen Datensatz ab, bezieht sich aber auf A in der Gruppe des unvollständigen Datensatzes. Ob die statistische Annahme tatsächlich zutrifft, ist nicht entscheidend für die Qualifikation als personenbezogenes Datum. Denn der Zweck der Datenverarbeitung ist es, eine bestimmte Person zu beurteilen.

4.7.4 Differenzierung zwischen Ausgangsdaten und Ableitung, Art. 9 DSGVO als Vorbild?

Rechtsdogmatisch aufgeschlüsselt ist nicht primär die Begrenzung der DSGVO auf individuelle, personenbezogene Daten der blinde Fleck des Datenschutzes, sondern die Ignoranz gegenüber der Entstehungsweise dieser Daten, die bei prädiktiven Modellen sachlogisch nur durch die Interaktion und den Abgleich mit Daten anderer Personen erfolgen kann. Eine solche Differenzierung zwischen Informationsentstehung und -verarbeitung ist in der Systematik der DSGVO nur begrenzt angelegt. Allein Art. 9 DSGVO differenziert zwischen Quell- und Metadaten sowie dem Ergebnis der Datenverarbeitung und verfolgt damit einen risikobasierten Regulierungsansatz.[57]

Art. 9 Abs. 1 DSGVO unterscheidet zwei verschiedene Verbotstatbestände: Abs. 1, 1. Hs. verbietet die Verarbeitung personenbezogener Daten, aus denen bestimmte sensible Datenkategorien, wie z. B. die ethnische Herkunft hervorgehen. Damit betrifft das Verbot die Ausgangsdaten, die wiederum selbst nicht deckungsgleich mit den Daten des Verarbeitungsergebnisses sein müssen. Der Vorgang des *Hervorgehens* impliziert, dass die sensiblen Datenkategorien nicht bereits vorliegen müssen, sondern potenziell aus den Ausgangsdaten abgeleitet werden können. Dadurch soll dem Risiko, durch allgemeine Daten Rückschlüsse auf sensible Daten ziehen zu können, begegnet werden. Allgemeine Daten bergen die Gefahr, dass aus ihnen sensible Daten hervorgehen und gelten deswegen ebenfalls als sensitive Daten i. S. d. Art. 9 Abs. 1, 1. Hs. DSGVO. Die Differenzierung in Art. 9 Abs. 1 DSGVO

56 *Kühling*, 2021 (Fn. 41) S. 168 ff.
57 Dazu *Schneider*, ZD, 2017, S. 303 ff.

ist die einzige Referenz der DSGVO zu abgeleiteten Daten. Diese Unterscheidung zwischen Ausgangs- und abgeleiteten Daten ist aber im weiteren Schutzregime und insbesondere in den Betroffenenrechten nicht reflektiert.

Der 2. Hs. des Art. 9 Abs. 1 bezieht sich nicht darauf, welche Daten aus der Verarbeitung hervorgehen, sondern verbietet die Verarbeitung bestimmter Daten an sich, z. B. biometrischer Daten als Inhaltsdaten.

Bereits diese regelungstechnische Entscheidung ist umstritten; die Kritik richtet sich darauf, dass die in Art. 9 Abs. 1 DSGVO differenzierten Kategorien ein Diskriminierungsverbot umsetzen sollen, welches nicht vom Schutzzweck des Datenschutzrechts erfasst sei.[58] Dies überzeugt schon aufgrund des engen Zusammenhangs mit den Grundrechten, u. a. Art. 21 GRCh, nicht.[59] Ob die Zuordnung in Bezug auf die betroffene Person inhaltlich zutrifft, ist für den Schutzzweck schlicht nicht entscheidend.[60]

Zugleich offenbart die Regelungskonzeption des Art. 9 Abs. 1 DSGVO erhebliche Abgrenzungsschwierigkeiten und verdeutlicht, dass die DSGVO *de lege lata* nicht in der Lage ist, das Problem von Big Data zu erfassen. Denn potenziell kann inzwischen aus nahezu jeder Information Rückschluss auf sensible Daten gezogen werden, insbesondere wenn man die uferlose Kategorie der politischen Einstellung mit einbezieht. Auch muss die verantwortliche Stelle überhaupt in der Lage sein, zwischen gewöhnlichen oder sensiblen Daten zu differenzieren.[61] Die kategoriale Unterscheidung der DSGVO zwischen sensiblen und nicht-sensiblen Daten ist damit hinfällig, der besondere Schutz obsolet.

Als Abgrenzungskriterium zwischen sensiblen und nicht-sensiblen Daten wird die Intention der Datenverarbeitung diskutiert, bei den kontextbezogenen Informationen soll also eine Auswertungsabsicht bestehen, aus der wiederum sensible Daten hervorgehen können.[62] Geht die Absicht nicht aus den objektiven Umständen des Verarbeitungskontextes hervor, wird das subjektive Element jedoch praktisch nicht nachweisbar sein; auch normativ finden sich in Art. 9 Abs. 1 DSGVO für eine solche Auslegung keine Anhaltspunkte.[63]

---

58 *Schneider*, 2017 (Fn. 57) S. 303 (304).

59 *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2021, Art. 9, Rn. 1.

60 *Weichert*, in: Kühling/Buchner (Hrsg.), DS-GVO BDSG, 3. Aufl. 2020, Art. 9 DS-GVO, Rn. 24.

61 *Matejek/Mäusezahl*, ZD, 2019, S. 551 (552).

62 *Matejek/Mäusezahl*, 2019 (Fn. 61) S. 551 (553); *Schulz*, in: Gola/Eichler et al. (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 9 DS-GVO, Rn. 13; *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), DatenschutzR 2019, Art. 9 DSGVO, Rn. 11; *Wachter/Mittelstadt*, 2019 (Fn. 43) S. 1 (74); *Weichert*, DuD, 41, 2017, S. 538 (540 f.).

63 *Petri* (Fn. 62), Art. 9 DSGVO, Rn. 12.

Im Zweifel sei der Anwendungsbereich des Art. 9 DSGVO zu verneinen.[64] Dies kann nicht überzeugen, da es keine normativen Anhaltspunkte für eine grundsätzlich enge Auslegung gibt. Nach der inneren Systematik der Norm sprechen die weiten Ausnahmeregeln des Art. 9 Abs. 2 DSGVO eher für ein ebenfalls weites Verständnis des Anwendungsbereichs des Abs. 1.[65] Andere argumentieren mit einer vermeintlichen Perspektive, wonach eine signifikante Wahrscheinlichkeit bzw. Sicherheit vorliegen müsse, um aus den Ausgangsdaten sensible Daten ableiten zu können.[66] Nach einer weiteren Ansicht soll nur auf den konkreten Verarbeitungskontext und den Verarbeitungszweck abzustellen sein, mithin auf die konkret ausgeführte Verarbeitung.[67] Damit verschiebt sich der Anwendungsbereich des Art. 9 DSGVO allerdings zeitlich: wenn es darauf ankommt, dass Quelldaten für die Ableitung sensibler Daten tatsächlich genutzt werden, kann dies u. U. erst während des Verarbeitungsvorgangs selbst festgestellt werden. Auf das abstrakte Potenzial, dass aus den Quelldaten sensible Daten hervorgehen *können*, kommt es dann nicht mehr an. Ob dies im Hinblick auf prädiktive Modelle noch trägt, ist fraglich. Denn dort sind verschiedene Informationen miteinander vernetzt und die Mehrzahl der verarbeiteten personenbezogenen Daten kann theoretisch als Quelldaten für sensible Daten genutzt werden. Deshalb überzeugt es, zwar auf den konkreten Verarbeitungskontext abzustellen, die Geeignetheit und Wahrscheinlichkeit der Nutzung aber als ausreichend anzusehen.[68] Im Kontext der Verarbeitung von Big Data dürften diese Anforderungen schon aufgrund der den Verarbeitungskontext prägenden technischen Funktionsweise als stets erfüllt anzusehen sein.

Der Regelungsansatz des Art. 9 DSGVO, der zwischen Ausgangsdaten, also der Modellerstellung, und Ableitung differenziert, lässt sich von der Schutzrichtung her auf prädiktive Modelle übertragen: die Metadaten als Teil der kollektiven Datenauswertung bei Erstellung des prädiktiven Modells sind die Basis für individualbezogene Ableitungen. Die nicht-sensiblen Ausgangs- oder Proxy-Daten, aus denen die sensiblen Daten i. S. d. Art. 9 Abs. 1, 1. Hs. DSGVO hervorgehen können, entsprechen bei Übertragung auf prädiktive Modelle der kollektiven Datenanalyse. Aus beiden können aber entsprechende Ableitungen hervorgehen, die Individuen betreffen bzw. in die Kategorie sensibler Daten fallen.

---

64 *Schulz* (Fn. 62), Art. 9 DS-GVO, Rn. 13.

65 „weder enge noch weite Auslegung" *Weichert* (Fn. 60), Art. 9 DS-GVO, Rn. 22.

66 *Albers/Veit*, in: Brink/Wolff (Hrsg.), BeckOK Datenschutzrecht, 36. Ed. Stand: 1.5.2021, Art. 9 DS-GVO, Rn. 21 f.; *Petri* (Fn. 62), Art. 9 DSGVO, Rn. 12; *Schiff*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 9 DS-GVO, Rn. 13; *Bergauer*, in: Knyrim (Hrsg.), Datenschutz-Grundverordnung, 2016, S. 43 (60).

67 *Matejek/Mäusezahl*, 2019 (Fn. 61) S. 551 (553).

68 *Weichert* (Fn. 60), Art. 9 DS-GVO, Rn. 15.

Aufgrund dieser kollektiven Dimension kann eine Einwilligung nie tragfähige Grundlage entsprechender Prognoseentscheidungen sein, da die einzelne Person eben nur für sich und nicht für alle anderen Betroffenen einwilligen kann. Aus prädiktiven Modellen müsste dann ein Weiterverarbeitungsverbot für den Modelloutput der individuellen Daten gelten, auch wenn Betroffene in diese eingewilligt haben. Denn die Ergebnisse des Prädiktionsmodells können nur durch kollektive Datenanalyse entstehen: wie der Fall Facebook zeigt, durch Prognosen über Nutzer:innen, die ihrer Datenverarbeitung nicht explizit zugestimmt haben, oder sogar von Nichtnutzer:innen.[69] Dies verdeutlicht, dass die Kategorie der „Betroffenen" im Sinne des Datenschutzrechts weit über den in der DSGVO abgesteckten Rahmen hinausgehen.

Im Ergebnis entspricht diese Auslegung der Schutzrichtung des Art. 9 Abs. 1 DSGVO, der ausdrücklich anerkennt, dass die Persönlichkeitsrelevanz von Ausgangsdaten und Verarbeitungsergebnis nicht deckungsgleich sein muss, um ein Schutzbedürfnis zu begründen. Die Funktionsweise prädiktiver Analytik führt aber dazu, dass die Differenzierung zwischen Ausgangsdaten und potenziell besonders sensiblen Daten letztlich hinfällig ist, wenn aus großen Datensätzen prinzipiell alles abgeleitet werden kann.

4.8 Rechtsprechung zu abgeleiteten Daten

Der *Output* prädiktiver Modelle sind abgeleitete Daten, also Prognosen über die Betroffenen. Unabhängig davon, ob bereits die Erstellung dieser Modelle von der DSGVO erfasst ist, wird diskutiert, ob und inwieweit die Schutzwirkung für abgeleitete Daten überhaupt greift.[70] Dies setzt voraus, dass diese als personenbezogene Daten einzuordnen sind.

Die Rechtsprechung des EuGH ist zu den aufgeworfenen Fragen wenig ergiebig, auch wenn andernorts darauf hingewiesen wird, dass sich der Gerichtshof zur Qualifikation von abgeleiteten Daten geäußert habe.[71] Es war im Rahmen eines Vorabentscheidungsverfahrens streitig, ob die i. V. m. einer Person getätigten abstrakten rechtlichen Bewertungen, also die „Schlussfolgerungen" der Datenverarbeitung selbst, als personenbezogene Daten zu qualifizieren waren.[72] Der EuGH entschied, dass die rechtliche Analyse als Prozess zu quali-

69 *Horvát/Horvát* et al., PloS one, 7, 2012, e34740; was auch im eklatanten Widerspruch zum Grundsatz der Vertraulichkeit und Transparenz steht, Art. 5 Abs. 1 a), f) DSGVO.

70 *Wachter/Mittelstadt*, 2019 (Fn. 43) S. 1 (47) gehen von einem eingeschränkten Schutz für abgeleitete Daten aus.

71 *Wachter/Mittelstadt*, 2019 (Fn. 43) S. 1 (29 ff.).

72 EuGH Urt. v. 17.7.2014 – C-141/12 und C-372/12, ECLI:EU:C:2014:2081 –YS u. a. – ZD 2014, 515. Im Anschluss: AG München, Teilurteil vom 4.9.2019 – 155 C 1510/18, ZD 2019, 569.

fizieren und nicht selbst ein personenbezogenes Datum sei. Die der Entscheidung zugrundeliegenden Tatsachen hingegen sind personenbezogene Daten, da sie individuell auf die Person bezogen seien. Es leuchtet ein, zwischen dem Prozess der Rechtsanalyse und den zugrundeliegenden persönlichen Informationen zu differenzieren. Dennoch lassen sich aus dieser Entscheidung keine Rückschlüsse ziehen, ob der EuGH abgeleitete Daten als personenbezogen qualifiziert. Denn die Argumentation des Gerichts bezog sich nicht auf die strukturelle Eigenschaft abgeleiteter Daten, sondern ist rein kontextbezogen: Die in Rede stehende „rechtliche Analyse" war im konkreten Fall Teil des Verwaltungsverfahrens zur Erteilung einer Aufenthaltserlaubnis. Diese rechtliche Analyse ist die Sachverhaltsaufbereitung und rechtliche Beurteilung der zuständigen Behörde zur Vorbereitung einer abschließenden Entscheidung, konkret eingekleidet in die prozessuale Situation des Auskunftsanspruchs nach Art. 15 DSGVO.[73] Der EuGH argumentiert nachvollziehbar mit dem Schutzzweck der DSGVO in der speziellen Situation des Verwaltungsverfahrens: das Auskunftsrecht soll den Betroffenen ermöglichen, die Berichtigung, Löschung oder Sperrung der Daten zu verlangen. Diese Folgen können sich aber nicht auf die rechtliche Analyse der Behörde beziehen,[74] denn diese richtet sich nach der Gesetzesbindung der Verwaltung im Bereich der Rechtsanwendung und nicht nach dem Schutz der persönlichen Daten. Mittelbar ist dies auch eine Frage der Gewaltenteilung; die Überprüfung der Rechtsauffassung der Behörde kann im Rahmen eines Rechtsbehelfsverfahrens und nicht im Wege des individuellen Auskunftsanspruchs erfolgen. Aus dieser Konstellation lassen sich daher keine verallgemeinerungsfähigen Aussagen über die Qualifikation abgeleiteter Daten herleiten.

Dies gilt auch für den in diesem Zusammenhang zitierten Fall *Nowak*[75]. Dort ging es um den Auskunftsanspruch eines Prüflings bezüglich einer endgültig nicht bestandenen Zulassungsprüfung. Der EuGH hat die Anmerkungen des Prüfers als personenbezogene Daten eingeordnet, da diese Informationen über den Prüfling selbst darstellen; dazu gehören auch Stellungnahmen und Beurteilungen.[76] Zwar hat das Gericht die Anwendung des Rechts auf Berichtigung[77] abgelehnt, daraus lässt sich aber keine geringere Schutzwirkung für abgeleitete Daten ablesen. Denn die Argumentation war wiederum nicht systematisch, sondern teleologisch-kontextbezogen. Bei Prüfungsleistungen

73 Anstoß des Verfahrens war die Änderung der Verwaltungspraxis, den Betroffenen die rechtliche Analyse nicht mehr auf einfachen Antrag zu übermitteln, sondern stattdessen eine Zusammenfassung der enthaltenden und verarbeiteten personenbezogenen Daten und Stellen die damit befasst waren, EuGH Urt. v. 17.7.2014 – C-141/12 und C-372/12, ZD 2014, 515.

74 EuGH (Fn. 73), Rn. 45.

75 EuGH (2. Kammer), Urteil vom 20.12.2017 – C-434/16 – NJW 2018, 767.

76 EuGH (Fn. 75), Rn. 34.

77 Damals noch Art. 12b RL 95/46 vor Inkrafttreten der DSGVO, EuGH a. a. O., Rn. 52.

widerstrebt es denklogisch dem Zweck der Datenverarbeitung – respektive der Prüfung selbst – wenn die Antworten später korrigiert werden können. Deshalb lässt sich auch aus dieser Entscheidung keine geringere Schutzwirkung der DSGVO für abgeleitete Daten ablesen, die als personenbezogene Daten zu qualifizieren sind. Dies gilt allerdings nur für die individuelle Komponente identifizierbarer Betroffener.

Auf dieser Wertungslinie liegen auch die Urteile des österreichischen BVerwG und des Oberen Gerichtshofs, die entschieden haben, dass Angaben zu Wahrscheinlichkeitsaussagen über bestimmte Affinitäten einer Person personenbezogene Daten im Sinne der DSGVO sind.[78] Prozessualer Hintergrund dieser Entscheidungen ist auch, dass vor Inkrafttreten der DSGVO in Österreich der Auskunftsanspruch nach § 32 DSG 2000 nur von der Datenschutzbehörde und nicht von den Betroffenen geltend gemacht werden konnte, diese ausschließliche Zuständigkeit aber vor dem Hintergrund des Art. 15 DSGVO nicht mehr gelten kann.

Das BVwG entschied klar, dass die Verarbeitung personenbezogener Daten, aus denen Parteiaffinitäten abgeleitet werden, auch als Wahrscheinlichkeitswerte Personenbezug aufweisen.[79] Dies überzeugt vom Ergebnis und methodisch, da das Gericht sich auf die kohärent entwickelten Merkmale der Artikel-29-Datenschutzgruppe zur Definition personenbezogener Daten, Inhalt – Zweck – Auswirkung stützt.[80] Interessant an der Entscheidung ist auch der Vergleich zur amtlichen Statistik, die nach Auffassung des Gerichts nicht personenbezogene Zusammenhänge zwischen soziodemografischen Daten und dem Interesse an bestimmten Parteien herstellt; die in Rede stehende Parteiaffinität des Verfahrens bezog sich aber darauf, Streuverluste in der Werbung zu vermeiden, setzte also zur Zweckerreichung die Verknüpfung mit Individuen voraus.[81] Vor allem schließt das BVwG nicht von der Unanwendbarkeit des Art. 16 DSGVO darauf, dass Wahrscheinlichkeitsaussagen dem gesamten Anwendungsbereich der DSGVO entzogen seien. Systematisch ist letzteres schon nicht überzeugend und zudem auch faktisch unzutreffend: Zweck der Datenverarbeitung ist nicht die Richtigkeit der Zuordnung, sondern allein ihre methodisch fundierte Einschätzung.[82]

Wahrscheinlichkeitsaussagen als abgeleitete Daten prädiktiver Modelle fallen damit in den Anwendungsbereich der DSGVO. Damit ist aber der kollektiven Dimension der Modellerstellung nicht hinreichend Rechnung getragen,

78 BVwG Österreich Teilanerkenntnis v. 26.11.2020 – W258 2217446-1/35E, BeckRS 2020, 51953; OGH Wien, Urteil vom 18.2.2021 – 6 Ob 127/20z (OLG Linz), BeckRS 2021, 20609.
79 BVwGÖ (Fn. 78), Rn. 55 ff.
80 BVwGÖ (Fn. 78), Rn. 60 ff.
81 BVwGÖ (Fn. 78), Rn. 65.
82 BVwGÖ (Fn. 78), Rn. 71.

weil sich die Betroffenenrechte und die DSGVO insgesamt nur auf die Daten der einzelnen Person beziehen und nicht auf ihre Auswirkungen auf Dritte.

4.9 Group Privacy vs. Individual Privacy vs. Collective Privacy?

Um das Schutzgut der prädiktiven Privatheit rechtlich zu flankieren, ist eine Einordnung in das vorherrschende Verständnis von individuell-subjektiven, kollektiven und „Gruppen"-Rechten hilfreich. Die Anerkennung von Privatheit als gesellschaftlichen Wert ist zunächst unerlässlich, um daraus weitere Rechte abzuleiten. Ohne Privatheit gibt es keine demokratischen Gesellschaften und keine Rechtsstaatlichkeit, die humanzentrierten Rechtsgüterschutz gewährleistet.[83] Individualrechtlich gibt es aber kein Grundrecht auf eine demokratische Gesellschaft, diese setzt sich zusammen aus der Summe der Einzelrechte des Individuums, die im Wechselspiel mit anderen subjektiven und objektiven Rechten die verfassungsrechtlichen Prinzipien in die Rechtsrealität transformieren.

4.9.1 Verwandte Konzepte in der philosophischen Debatte

In der philosophischen Debatte gibt es verschiedene Begriffsvorschläge, um das ethische Problem vorhergesagter Informationen zu konzeptualisieren. Wir verwenden in Abgrenzung dazu den Begriff der prädiktiven Privatheit.[84] *Loi* und *Christen* haben den Begriff der „inferential privacy" verwendet, um mögliche Privatheitsverletzungen durch Vorhersagen zu problematisieren.[85] Im Unterschied zu prädiktiver Privatheit erkennen *Loi* und *Christen* jedoch das ethische Problem der „prediction gap" nicht richtig an (siehe 4.4.1) und erfassen mit ihrem Begriff nur dann eine Privatheitsverletzung, wenn die vorhergesagte Information auf logisch gültigen Schlussfolgerungen beruht. Derselbe Einwand trifft *Mittelstadts* und *Wachters* Konzept eines *Right to Reasonable Inferences*[86] (dazu bereits oben 4.6.2): Prädiktive Privatheit zielt darauf ab, auch die Verwendung von „reasonably inferred" Informationen als ethisch und rechtlich bedenklich einzustufen und präsentiert damit eine *stärkere* Forderung als das Recht auf nachvollziehbare Schlussfolgerungen.[87] In ähnlicher

83 *Hildebrandt*, Theoretical Inquiries in Law, 20(1):83–121, 2019, S. 83, 84, doi: 10.1515/til-2019-0004.
84 *Mühlhoff*, 2021 (Fn. 14); *Mühlhoff*, 2020 (Fn. 3).
85 Vgl. *Loi/Christen*, Philosophy & Technology, 33:207–224, 2020, doi: 10.1007/s13347-019-00351-0.
86 Vgl. Wachter/Mittelstadt (Fn. 43).
87 *Mühlhoff*, 2021 (Fn. 14).

Weise unterscheidet sich prädiktive Privatheit von *Hildebrandts* Plädoyer für einen „paradigm shift from data to knowledge protection" angesichts von Verletzungen der Privatsphäre durch Profiling.[88] In der Philosophie wird Wissen als wahre und gerechtfertigte Meinung verstanden. Die Verletzung der prädiktiven Privatsphäre setzt jedoch nicht voraus, dass eine Vorhersage wirklich gültig und somit als Wissen zu qualifizieren ist. Daher geht die Paradigmenbeschreibung eines „Wissensschutzes" am hier vorliegenden Problem vorbei.[89] Schließlich unterscheidet sich prädiktive Privatheit auch von dem viel diskutierten Konzept der „Group Privacy".[90] Denn das Konzept der prädiktive Privatheit knüpft die ethischen und rechtlichen Bedenken nicht an die Voraussetzung, dass die Verletzung von Privatsphäre durch Vorhersagen auf Gruppenebene erfolgen muss, also eine bestimmte Kohorte von Individuen identisch und synchron betreffen muss. Die prädiktive Modellierung stellt eine neue Bedrohung für die Privatsphäre dar, weil sie einen neuen Bereich von Informationen verfügbar macht – Informationen, die nie aufgezeichnet wurden, sondern nur über die betroffenen Personen im Sinne einer Wette auf das wahrscheinlichste Ergebnis vorhergesagt werden. Die Gefahr des Missbrauchs dieser Art von Informationen ist unabhängig davon, ob die Algorithmen durch virtuelle Gruppierung von Personen vorgehen oder in anderer Weise verfahren.

4.9.2 Rechtsfolgen von Group Privacy

Am Fall des Konzepts der Group Privacy wird deutlich, dass die kollektive Dimension des Datenschutzes mehrere Ebenen umfasst: materiell-rechtlich und prozessual, als Gruppenrecht, als Recht, nicht Teil einer Gruppe zu sein, als Recht der individuellen Mitglieder der Gruppe; Rechte aufgrund der Gruppenzugehörigkeit – innerhalb und außerhalb der Gruppe. Es gibt bisher keinen kohärenten oder stabilen Rahmen für Group Privacy, was auch an fehlenden philosophischen Rechtfertigungen liegt, die zu einer Schwächung von Grund- und Menschenrechten führt.[91]

Die Abgrenzung zwischen individuellen Rechten und kollektiven Rechten oder Gruppenrechten ist im Hinblick auf Privatheitsschutz besonders erschwert,

88 Vgl. *Hildebrandt*, Who Is Profiling Who? Invisible Visibility, In: Gutwirth/Poullet/De Hert/de Terwange/Nouwt (Eds.) Reinventing Data Protection?, 2009.

89 So argumentiert *Mühlhoff*, 2022, under review (Fn. 11).

90 Vgl. *Floridi*, Philosophy & Technology 27(1): 1–3, 2014, doi: 10.1007/s13347-014-0157-8; *Mittelstadt*, Philosophy & Technology, 30(4): 475–94, 2017, doi: 10.1007/s13347-017-0253-7; *Taylor/Floridi/van der Sloot*, Group Privacy: New Challenges of Data Technologies, 2016; *Helm*, Digital Culture & Society, 2(2): 137–52, 2016, https://doi.org/10.14361/dcs-2016-0209.

91 *Morsink*, HUM 15 (1993), S. 357, 397 ("It seems, therefore, that the war, which prompted the writing of a Declaration with a set of universal and absolute values, did not provide a philosophy with which to defend that set.").

wenn man diesen als gesellschaftlichen und sozialen Wert ansieht. Nach dem Ansatz der Group Privacy stellt prädiktive Analytik Prognosen über Individuen aufgrund ihrer Gruppenzugehörigkeit und umgekehrt: Annahmen über die Gruppe speisen sich aus den zugehörigen Individuen.[92] Group Privacy kann sich somit als Individualrecht darstellen, welches einzelne Personen aufgrund ihrer Gruppenzugehörigkeit ableiten oder als Recht der Gruppe an sich.

Die Gefahren prädiktiver Analytik werden durch Konzepte zur Group Privacy deshalb nur partiell adressiert, da es weniger um Rechte aufgrund einer Gruppenzugehörigkeit geht oder um Gruppenrechte, sondern um das Recht, gerade nicht Teil einer Gruppe zu sein.

4.10 Conclusio

Kollektive Elemente von Privatheit und Datenschutz können und sollen bereits aus gewichtigen Gründen des auch im Zeitalter allgegenwärtiger Datenanalyse wichtigen Individualrechtsschutz diesen nicht ersetzen, sondern allenfalls ergänzen. Das begründete Bedürfnis eines Schutzguts der prädiktiven Privatheit verdeutlicht, dass die DSGVO nicht auf den Schutz vor Big-Data-Analysen und prädiktiven Modelle ausgerichtet ist, da es hierbei um ein Schutzbedürfnis geht, welches bereits auf der Ebene der Vorhersagemacht und nicht erst im Einzelfall manifester Ausübung dieser Macht einsetzt. Die Grenzen der individualrechtlichen Schutzkonzeption des Datenschutzrechts zeigen sich also darin, dass individuelle Datenfreigabeentscheidungen und Betroffenenrechte nicht mehr in der Lage sind, die beschriebenen Risiken prädiktiver Analytik-Technologie einzuhegen. Vorhersagemacht als die spezifische Form von Datenmacht im Kontext prädiktiver Analytik führt schließlich auch insofern zu neuen regelungstechnischen Fragen, als entsprechende privatheitsgefährdende Modelle faktisch nur von einer begrenzten Zahl durchaus identifizierbarer Institutionen, insbesondere privater Unternehmen und z. T. Staaten[93] eingesetzt werden (können). Die auf dieser Beobachtung aufbauende Kritik an der horizontalen Regelungskonzeption der DSGVO ist nicht neu. Es widerstrebt schlicht dem Gerechtigkeitsempfinden, dass Facebook, Google, Apple oder Amazon denselben Pflichten unterliegen sollen, wie der lokale Kindergarten. Aus rechtsstaatlichen Gesichtspunkten stellt sich daher die Frage nach der konstruktiven Entwicklung des Datenschutzes als eines Rechtsgebiets, welches zunehmend nicht mehr in der Lage ist, auf aktuelle tatsächliche Herausforderungen zu reagieren.

---

92 *Puri*, Cornell Journal of Law and Public Policy 2020, S. 477 (483).

93 *Maamar*, CR 2018, S. 820 ff. zum Social Scoring in China. Zur Fluggastdatenanalyse nach der PNR-Richtlinie: *Ruschemeier*, Predictive Policing, in: Ebers (Hrsg.) Legal Tech, i. E. Jüngst aber: EuGH C-817/19, ECLI:EU:C:2022:491.

5 Satelliten-Megakonstellationen im Weltraumrecht

*Marcus Schladebach**

Die Digitalisierung des Weltraums hat längst begonnen: Wurden in den vergangenen Jahrzehnten einzelne Kommunikationssatelliten in erdnahe Umlaufbahnen (Low Earth Orbit) verbracht, baut das US-Unternehmen „Space X" derzeit eine riesige Satelliten-Megakonstellation mit dem Namen „Starlink". Durch tausende miteinander verbundene Satelliten soll ein hochleistungsfähiges Internetangebot für die gesamte Welt ermöglicht werden. Dies lässt sich einerseits als technische Meisterleistung feiern, andererseits aber auch als kapazitive und optische Überlastung des internationalen Gemeinschaftsraums „Weltraum" verurteilen. Gelegentlich ist sogar von einem „Kulturimperialismus" die Rede. Zudem lässt das Projekt die Entstehung weiteren Weltraumschrotts befürchten. Weitere Unternehmen wie „Oneweb" wollen folgen.

Ob das aus den 1960er Jahren stammende Weltraumrecht auf diese „Möblierung des Weltraums" wirksame Antworten zu geben weiß, wird folgend untersucht. Dabei wird man vor allem fragen müssen, ob die wirtschaftliche Nutzungsfreiheit des Weltraums (Art. I WRV) bestimmten Grenzen unterliegt, gerade weil es sich nicht mehr nur um Staaten als klassische Akteure im Weltraum, sondern um Privatunternehmen handelt. Grenzen könnten sich aus Kapazitätsbeschränkungen für das Platzieren von Satelliten ergeben. Denn die Nutzbarkeit der Erdumlaufbahnen durch alle Staaten wäre erheblich gefährdet, wenn sämtliche Satellitenpositionen durch wenige Staaten/Unternehmen bereits besetzt wären. Es stellt sich daher auch ein Verteilungsproblem, für das in den 1970er Jahren interessante Kriterien zwischen Industrienationen und Entwicklungsländern vereinbart wurden.

5.1 Problemstellung

Satelliten-Megakonstellationen sind Verbundsysteme aus einer Vielzahl von Satelliten, die in der unteren Erdumlaufbahn hauptsächlich dazu platziert werden, um verbesserte Internetdienstleistungen anzubieten. Optisch erscheinen sie als Perlen- bzw. Lichterkette, die gelegentlich von der Erde aus mit bloßem Auge zu erkennen ist. Wichtigste Akteure sind private Raumfahrtunternehmen wie Space X von *Elon Musk* mit seinem Projekt

* Mehr über den Autor erfahren Sie im Autor:innenhinweis auf S. 224 ff.

„Starlink“,[1] das von Amazon verfolgte „Kuiper Project“ sowie das 2012 gegründete Unternehmen „OneWeb“, das im März 2020 zwar Insolvenz anmeldete, jedoch seit Dezember 2020 wieder Satelliten im erdnahen Orbit platziert. Am weitesten fortgeschritten ist der Aufbau von Starlink, für das bereits ca. 2400 Satelliten in den Weltraum befördert wurden und das insgesamt ca. 12000 Satelliten umfassen soll. Auch die EU hat die Potenziale solcher Megakonstellationen erkannt und plant den Aufbau eines Satellitennetzes.[2] Der nachfolgende Beitrag will – soweit ersichtlich erstmals – der Frage nachgehen, ob eine derart umfangreiche Platzierung von Satelliten wie die Megakonstellation „Starlink“ mit dem Weltraumrecht vereinbar ist.

5.2 Weltraumrechtlicher Rahmen

5.2.1 Der Weltraumvertrag als Rechtsgrundlage

Rechtsgrundlage für die Beurteilung ist der UN-Weltraumvertrag von 1967. Sein Zustandekommen war eine Konsequenz der technologischen Entwicklungen in den späten 1950er Jahren.[3] Nach den erfolgreichen Starts des sowjetischen Satelliten „Sputnik 1“ am 4.10.1957 und des US-amerikanischen Satelliten „Explorer 1“ am 31.1.1958 begann der neu gegründete UN-Weltraumausschuss ab 1959 über die Notwendigkeit geeigneter rechtlicher Regelungen zu beraten. Mit den ersten bemannten Weltraumflügen von *Juri Gagarin* (12.4.1961) und *Alan Shepard* (5.5.1961) gewann die Frage nach der zulässigen Nutzung des Weltraums weitere Dringlichkeit. Eine vom UN-Weltraumausschuss vorbereitete UN-Resolution über Rechtsgrundsätze staatlicher Aktivitäten im Weltraum wurde von der UN-Generalversammlung am 13.12.1963 angenommen[4] und mündete sodann in den Weltraumvertrag (WRV) vom 27.1.1967,[5] der bislang von 109 Staaten ratifiziert worden ist. Hierin bestätigte sich erneut die Erkenntnis, dass neue technische Erfindungen zu neuem Recht führen.[6] Wie für die Befahrung der Meere mit dem Seerecht und für die Nutzbarkeit des Luftraums mit dem Luftrecht, führte die technische Erschließung des Weltraums durch den Menschen zur Schaffung des Weltraumrechts. Dieses Teilgebiet des besonderen Völkerrechts ist daher keine oft behauptete Kuriosität, sondern eine zwingend zu erwartende Konsequenz.

---

1 www.starlink.com; *Scheuer*, Handelsblatt v. 26.8.2022.
2 EU-Kommission, Union Connectivity Programm, COM (2022) 57 final (15.2.2022).
3 *Schladebach*, Weltraumrecht, 2020, § 1 Rn. 1; ders., APuZ 69 (2019), B 29–30, S. 26.
4 UNGA, Res. 1962 (XVIII).
5 BGBl. 1969 II S. 1967; 610 UNTS 205.
6 *Schladebach*, Weltraumrecht, 2020, § 1 Rn. 2.

5.2.2 Private Raumfahrtunternehmen als Adressaten

In Art. I WRV wird die Erforschung und Nutzung des Weltraums und aller Himmelskörper zur Sache der gesamten Menschheit erklärt. Mit Blick auf das hier verortete „Common Heritage/Concern of Mankind"-Prinzip ist zu betonen, dass mit „Nutzung" in erster Linie eine wirtschaftliche Nutzung gemeint ist[7] und sich Raumfahrtakteure nicht lediglich auf Forschungsaktivitäten beschränken müssen. Trotz dieses Bekenntnisses erscheint fraglich, ob neben Staaten als damals wie heute maßgebliche Hauptakteure auch private Raumfahrtunternehmen in die weltraumvertraglichen Pflichten eingebunden sind. Denn Raumfahrt war lange Zeit eine staatliche Angelegenheit, weil nur staatliche Agenturen über ausreichend personelle und finanzielle Kapazitäten verfügten, um die äußerst kostenintensiven Missionen erfolgreich durchzuführen. In jüngerer Zeit nehmen aber Weltraumaktivitäten privater Raumfahrtunternehmen kontinuierlich zu, was die Frage nach deren rechtlicher Verortung im WRV aufwirft.

Vor dem Hintergrund der beschriebenen staatlichen Dominanz in der Raumfahrt der 1960er Jahre muss es als geradezu visionär angesehen werden, dass Art. VI WRV bereits private Raumfahrtunternehmen in die Weltraumrechtsordnung einbezog. Nach Art. VI S. 1 WRV sind die Vertragsstaaten völkerrechtlich verantwortlich für nationale Tätigkeiten im Weltraum (…), gleichviel ob staatliche Stellen oder nichtstaatliche Rechtsträger dort tätig werden, und sorgen dafür, dass nationale Tätigkeiten nach Maßgabe dieses Vertrags durchgeführt werden. Art. VI S. 2 WRV legt fest, dass Tätigkeiten nichtstaatlicher Rechtsträger im Weltraum (..) der Genehmigung und ständigen Aufsicht durch den zuständigen Vertragsstaat bedürfen. Der Weltraumvertrag formuliert damit zwei zentrale Bedingungen für private Raumfahrtunternehmen:

(1) Da Tätigkeiten „nichtstaatlicher Rechtsträger" auch als „nationale Tätigkeiten im Weltraum" gelten (Art. VI S. 1 WRV), sind diese „nach Maßgabe dieses Vertrags" durchzuführen. Private Raumfahrtunternehmen unterliegen daher dem WRV.

(2) Zudem bedarf es der Genehmigung und ständigen Aufsicht über die Unternehmen. Die Genehmigung durch den Staat muss hinsichtlich des Tatbestands und der Rechtsfolge in einem nationalen Gesetz geregelt werden. Die ständige Aufsicht verlangt eine permanente Navigationskontrolle über den privaten Weltraumgegenstand und effektive Möglichkeiten des Staates, um steuernd in die private Mission eingreifen zu können. Die Schaffung nationalen Rechts, in dem die Genehmigung und die ständige Aufsicht normiert

7 *Hobe*, Die rechtlichen Rahmenbedingungen der wirtschaftlichen Nutzung des Weltraums, 1992, S. 64 ff.; ders., Space Law, 2019, S. 143 ff.; *Schladebach*, DVBl. 2022, 753 (755).

sind, ist keine bloße Empfehlung oder eine sinnvolle Obliegenheit des Staates, mit der er sich als völkerrechtlich verantwortlicher Akteur vor unzuverlässigen privaten Unternehmen schützen kann. Vielmehr handelt es sich um eine durch Art. VI WRV statuierte völkerrechtliche Pflicht.[8] Deshalb können private Unternehmen erst dann rechtmäßig im Weltraum operieren, wenn sie zuvor die Genehmigung nach nationalem Recht erhalten haben.

5.3 Positionierung von Satelliten

5.3.1 Interessenlage

Das gegenwärtig größte ökonomische Interesse privater Raumfahrtunternehmen besteht darin, Kommunikationssatelliten im erdnahen Orbit zu positionieren und zu nutzen. Diese Vorhaben sind – wie bereits erwähnt – von Art. I WRV gedeckt, der die Freiheit der Nutzung des Weltraums normiert. „Nutzung" meint dabei in erster Linie eine wirtschaftliche Nutzung. Satelliten lassen sich zu zivilen und militärischen Zwecken nutzen. So können sie für die Kommunikation/Rundfunk, Telekommunikation, Internet, Wetterbeobachtung, Naturkatastrophenvorhersage, Navigation im Luftverkehr, Schiffsverkehr, Straßenverkehr sowie für Erdbeobachtung und Vermessung eingesetzt werden. Darüber hinaus dienen sie militärischen Zwecken. Weite Teile der heutigen digitalen Kommunikation beruhen auf Satellitentechnik, was der Gesellschaft erst dann eindrücklich bewusstwerden wird, wenn es zu Ausfällen oder zumindest Einschränkungen des Datenverkehrs kommt.

Jedes Privatunternehmen, das einen Satelliten im Weltraum platzieren will, muss über seinen Heimatstaat die Zuteilung einer Sendefrequenz und einer damit verbundenen konkreten Orbitposition bei der International Telecommunication Union (ITU) in Genf beantragen. Die ITU, deren völkerrechtlicher Status als Internationale Organisation nicht unumstritten ist,[9] agiert auf der Grundlage der ITU Constitution und der ITU Convention und prüft die Anträge auf Frequenzzuweisung nach Maßgabe zweier Prinzipien: Zum einen wird ausschließlich technisch geprüft, ob die beantragte Frequenz/Orbitposition auf der entsprechenden Umlaufbahn noch vorhanden ist und ob diese so weiten Abstand von den existierenden Positionen hält, dass keine Interferenzen auftreten. Soweit es keine technischen Einwände gibt, werden dem Staat und sodann dem Unternehmen Frequenz und Orbitposition zugeteilt. Ist diese Position jedoch von zwei oder mehreren Staaten beantragt worden, so gilt das zweite wesentliche Zuteilungsprinzip: First come, first

8 *von Kries/Schmidt-Tedd/Schrogl*, Grundzüge des Raumfahrtrechts, 2002, S. 48 ff.; *Schladebach*, ZRP 2011, 173 ff.; ders., DRiZ 2019, 392 (393); ders., DVBl. 2022, 753 (754).

9 *von Kries/Schmidt-Tedd/Schrogl*, Grundzüge des Raumfahrtrechts, 2002, S. 62–64.

served.[10] In Deutschland ist das Bundesministerium für Wirtschaft und Klimaschutz zuständig, für das die Bundesnetzagentur (BNetzA) handelt.

5.3.2 Verteilungskonflikte

Die Zuteilung von Satellitenpositionen nach „first come, first served" hat schon seit langem zu Verteilungskonflikten zwischen den aktiv Raumfahrt treibenden Industrienationen und den noch zurückhaltenden Entwicklungsländern geführt. Letztere fühlten sich unter Hinweis auf ihre noch gering entwickelten Raumfahrtkapazitäten von der Weltraumnutzung ausgeschlossen und kritisierten ein neues „Race to Space". Verwiesen wurde insbesondere darauf, dass Art. I WRV die Nutzung des Weltraums „im Interesse aller Länder ohne Ansehen ihres wirtschaftlichen und wissenschaftlichen Entwicklungsstandes" garantiert. Hinsichtlich der Zunahme westlicher Rundfunksatelliten in den 1970er Jahren wurde zudem ein „Kulturimperialismus" moniert. Die Entwicklungsländer konnten im Zuge der Neuen Weltwirtschaftsordnung indes durchsetzen[11], dass im ITU-Recht die Erdumlaufbahnen zu „begrenzten natürlichen Ressourcen" erklärt wurden,[12] was jedem ITU-Vertragsstaat zumindest eine Orbitposition auf jeder Erdumlaufbahn – unabhängig vom wirtschaftlichen Status und der tatsächlichen Nutzbarkeit – sicherte. Das erscheint nicht viel, entspricht aber der Forderung des Weltraumvertrags, dass der Weltraum als hoheitsfreier Gemeinschaftsraum keinem Staat allein, sondern allen Staaten gemeinsam gehört.

5.4 Elon Musk's Starlink im Weltraumrecht

5.4.1 Ausgangslage

Das in diesem Kontext gegenwärtig bedeutendste Projekt ist die Satelliten-Megakonstellation „Starlink" des Raumfahrtunternehmens Space X von *Elon Musk*. Tausende miteinander verbundene Kommunikationssatelliten sollen ein neuartiges Internetangebot für die ganze Welt ermöglichen, so dass man mit einem Smartphone jeden Ort auf der Welt erreichen kann.[13] Dies ist keine Ankündigung geblieben, sondern kontinuierlich transportieren Falcon-9-Raketen Satelliten in die untere Erdumlaufbahn und vergrößern die Netzstrukturen im Weltraum. Es muss in Ermangelung von Belegen unterstellt werden, dass Space X nach den US-internen Regelungen bei der US

10 *von Kries/Schmidt-Tedd/Schrogl*, Grundzüge des Raumfahrtrechts, 2002, S. 157; *Catalano Sgrosso*, International Space Law, 2011, S. 430; *Hobe*, Space Law, 2019, S. 146.
11 *Ipsen/Hobe*, Völkerrecht, 7. Aufl. 2018, § 47 Rn. 31.
12 *Catalano Sgrosso*, International Space Law, 2011, S. 430.
13 So die Ankündigung Elon Musks Ende August 2022, *Scheuer*, Handelsblatt v. 26.8.2022.

Federal Communications Commission (FCC) zahlreiche Anträge auf Zuweisung von Frequenzen gestellt hat. Es muss weiterhin unterstellt werden, dass die FCC sodann bei der ITU diese Zuteilung beantragt hat. Die riesige Zahl an in den unteren Erdorbit verbrachte Satelliten zeigt darüber hinaus an, dass die Zuteilung von der ITU an die FCC und sodann an Space X erfolgt sein muss.

Völkerrechtlich könnte in Frage gestellt werden, ob die USA überhaupt an dieses internationale Zuweisungsverfahren der ITU gebunden ist. Denn bekanntlich zeichnen sich die USA nicht dadurch aus, ihre Handlungsbefugnisse durch den Beitritt zu internationalen Abkommen gern begrenzen zu wollen. Das UN-Seerechtsübereinkommen und das Statut über den Internationalen Strafgerichtshof sind Beispiele dieser bedauerlichen Haltung. Jedoch sind die USA seit 1908 Mitglied der ITU und haben 1997 die aktuell geltende ITU-Convention ratifiziert. Somit gilt das ITU-Verfahren auch für die USA und insbesondere für das Projekt „Starlink".

5.4.2 Zulässigkeit

Bei der Bewertung der Zulässigkeit von Starlink ist zunächst zu betonen, dass sich Starlink als privatwirtschaftliche Initiative auf die wirtschaftliche Nutzungsfreiheit des Art. I WRV berufen kann. Gleichwohl wird eine solche Nutzung nicht unbeschränkt gewährt, sondern muss die durch den WRV gezogenen Grenzen beachten. Solche Grenzen könnten sich aus dem Aneignungsverbot des Art. II WRV, der Pflicht zur Berücksichtigung von Drittstaateninteressen nach Art. IX S. 1 WRV und aus den Erfordernissen des Umweltschutzes gem. Art. IX S. 2 WRV ergeben.

5.4.2.1 Aneignungsverbot

So könnte in der Vereinnahmung der Erdumlaufbahnen eine verbotene nationale Aneignung von Teilen des Weltraums nach Art. II WRV zu sehen sein. Die Vorschrift verbietet über ihren Wortlaut „national" hinaus jedwede Aneignung: Da sich Privatunternehmen nach Art. VI S. 1 WRV ebenfalls an das Weltraumrecht zu halten haben, muss auch eine Aneignung durch Private dem Aneignungsverbot des Art. II WRV unterfallen. Wird nunmehr eine Umlaufbahn so stark in Anspruch genommen, dass andere Interessenten von einer Nutzung absehen, so könnte darin eine verbotene Aneignung liegen. Insofern ist von einer Verdrängungs- oder Übernutzung zu sprechen. Ohne Zweifel ist die Zahl der in den Weltraum zu verbringenden Starlink-Satelliten sehr hoch, was bei anderen Staaten durchaus Demotivationseffekte auslösen könnte. Die ihnen – hier von Art. I WRV – zugestandenen eigenen Rechte würden sie dann nicht mehr wahrnehmen wollen, was zu problema-

tischen *chilling effects* führt. Jedoch dürfte die Grenze zu einer Übernutzung noch nicht überschritten sein. Insbesondere werden von Space X nur die rechtlichen Möglichkeiten genutzt, die das internationale Recht in Form der ITU-Convention enthält. Die Wahrnehmung völkerrechtlich eingeräumter Möglichkeiten impliziert die Vermutung rechtskonformen Verhaltens. Eine verbotene Aneignung ist darin nicht zu erkennen.

5.4.2.2 Interessen von Drittstaaten

Eine weitere eventuell kollidierende Rechtsposition könnte aus Art. IX S. 1 WRV folgen, wonach bei der Weltraumtätigkeit auf Interessen anderer Vertragsstaaten Rücksicht zu nehmen ist. Auch diese Pflicht könnte gefährdet sein, wenn praktisch unbegrenzt Satelliten in die besonders attraktiven unteren Erdumlaufbahnen verbracht werden. Allerdings wird man hier zu berücksichtigen haben, dass die Interessen von Drittstaaten nicht klar bestimmt werden können. Vor allem wird man ihnen nicht unterstellen können, dass sie generell gegen dieses Satellitennetzwerk sind, von dem der eine oder andere Staat womöglich auch profitiert. Daher können aus Art. IX S. 1 WRV keine hier einschlägigen Grenzen abgeleitet werden.

5.4.2.3 Umweltschutz

Der dritte weltraumrechtliche Einwand ist der Umweltschutz und graduell viel erheblicher. Nach Art. IX S. 2 WRV sind Kontaminationen und sonstige Veränderungen der kosmischen Umwelt zu unterlassen. Diese vielfach unterschätzte Vorschrift kann in ihrer allgemeinen Bedeutung für das internationale Umweltrecht nicht hoch genug gewürdigt werden. Während vielfach der Beginn internationalen Umweltrechts auf die Stockholm-Konferenz der UN im Juni 1972 und die dort verabschiedete Stockholm Declaration datiert wird, übersieht die Fachöffentlichkeit, dass mit Art. IX S. 2 WRV bereits viel früher eine multilateral angelegte Umweltschutznorm bestand. Überdies ist diese Norm im Völkervertragsrecht niedergelegt, nicht lediglich im Range unverbindlicher UN-Deklarationen.

Verlieren nun die vielen tausenden Starlink-Satelliten nach wenigen Jahren ihre Funktionsfähigkeit und veralten sie technisch, entstehen Unmengen von Weltraumschrott, für deren verantwortungsvolle Beseitigung es noch keine effektiven Konzepte gibt. Obwohl schon seit vielen Jahren auf die Gefahren durch Weltraumschrott, gerade auch für die aktive Raumfahrt, hingewiesen und eine neue Regelung im Rahmen des WRV vorgeschlagen worden ist,[14] verharren viele Staaten in einer Abwehrhaltung: Die Rückho-

14 *Schladebach*, Max Planck Yearbook of UN Law 17 (2013), 61 ff.; s. auch *Hobe/Mey*, ZLW 2009, 388 ff.; *Mey*, ZLW 2012, 251 ff.

lung von Weltraumschrott sei zu kostenintensiv und außerdem habe es noch keine nennenswerten Schäden gegeben.[15] Dass diese Haltung hochproblematisch ist, bedarf keiner weiteren Begründung. Auch die rechtlich unverbindlichen „Space Debris Mitigation Guidelines" der technischen Unterabteilung des UN-Weltraumausschusses von 2007[16] tragen zur Problemlösung kaum bei; sie setzen auf den Einsatz umweltschonender Materialien beim Bau von Weltraumgegenständen, sehen aber keine Rückholverpflichtung des Startstaats vor. Das Starlink-Projekt sorgt für die massive Zunahme von Weltraumschrott in einigen Jahren, was weder durch ein erkennbares Rückholkonzept abgefedert wird, noch mit den sonstigen umweltschonenden Ambitionen des Unternehmers *Elon Musk* korrespondiert. Da somit eine erhebliche Verschmutzung der Weltraumumwelt zu gewärtigen ist, dürfte Starlink nicht mit Art. IX S. 2 WRV vereinbar sein.

Ein weiterer kritischer Umweltaspekt besteht in der Gefahr durch Lichtverschmutzung.[17] Diese neuartige Erscheinungsform der Weltraumverschmutzung ist zunächst durch Planetarien thematisiert worden, hat aber darüber hinaus auch Auswirkungen auf Erdbeobachtungssysteme, die aus dem Weltall in Richtung Erde agieren. Insoweit könnte die Einführung einer Umweltverträglichkeitsprüfung (UVP) für vergleichbare Weltraumnutzungen erwogen werden. Eine UVP ist für Großvorhaben mittlerweile völkergewohnheitsrechtlich gefordert, wie sich aus der IGH-Entscheidung „Pulp Mills" (2010) und dem ISGH-Gutachten „Nauru" (2011) ergibt.[18] In der Konsequenz könnte das bedeuten, dass Raumfahrtmissionen unter den Vorbehalt einer positiven UVP gestellt werden. Gegenwärtig sind die Erkenntnisse zu einer Beeinträchtigung der Weltraumumwelt durch Lichtverschmutzung aber noch zu diffus, als dass daraus ein weiterer durchgreifender umweltrechtlicher Einwand gegen die Zulässigkeit von Starlink abgeleitet werden kann.

5.5 Fazit

Im Ergebnis kann ein Verstoß von Starlink gegen das Aneignungsverbot des Art. II WRV zwar nicht angenommen werden. Es sprechen jedoch gewichtige Gründe dafür, dass dieses Projekt wegen der Gefahr einer exponentiellen Zunahme von Weltraumschrott mit den umweltrechtlichen Wertungen des Weltraumrechts nicht vereinbar und daher insgesamt unzulässig sein dürfte.

---

15 Dazu schon *Schladebach*, JuS 2008, 217 (220).
16 Dazu *Benkö/Schrogl*, ZLW 2008, 335 ff.
17 *Jakhu/Pelton/Mishra*, in: Benkö/Schrogl, Outer Space. Future for Humankind, 2021, S. 267 ff.
18 *Epiney*, in: Proelß, Internationales Umweltrecht, 2017, § 4 Rn. 19 ff.

6 Überindividuelle Probleme im Datenschutzrecht

*Marvin Gülker**

Seit Jahren beklagt die Post-Privacy-Bewegung die Unfähigkeit des Rechts, die Regulierung des Internets und der Überwachung in den Griff zu bekommen. Staat und Private verarbeiten heute Daten in nie gekanntem Ausmaß. Dies stellt das Recht vor gesamtgesellschaftliche Herausforderungen, die die Frage nach sich ziehen, ob das Datenschutzrecht hierauf noch angemessen reagiert. Sporadische Ansätze wie ein „Right to Explanation" sollen die ad hoc vorgefundenen Lücken füllen, doch das eigentliche Problem ist ein tieferes und strukturelleres, das die Axt an die Wurzel des Datenschutzrechts, das Recht auf informationelle Selbstbestimmung, legt. Der Beitrag sucht hierfür Lösungen innerhalb und außerhalb des Datenschutzrechts, die zwar die Grenzen des geltenden Datenschutzrechts aufzeigen, aber keineswegs in einer Kapitulation des Rechts münden.

6.1 Einleitung

Seit jeher fürchten Datenschützer:innen die Entstehung des allwissenden Überwachungsstaates, den uns *Orwells* dystopischer Roman „1984" anschaulich vor Augen führt. Im Volkszählungsurteil von 1983 hat das BVerfG diese Befürchtungen rezipiert und hat zur Verteidigung aus Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG das Recht auf informationelle Selbstbestimmung abgeleitet.[1] Dieses bildete den Ausgangspunkt für die weitere Entwicklung des Datenschutzrechts. Als Grundrecht ist es jedoch ein subjektives Recht, und diese Subjektivität stößt in der fortschreitenden Digitalisierung mehr und mehr auf gesamtgesellschaftliche Fragen. Es ist an der Zeit, diese als übergreifende Problematik anzuerkennen (6.2). Nachdem der Spartenbezug bisheriger Lösungsansätze aufgezeigt wurde (6.3), wird die große Lösung versucht (6.4).

6.2 Das Phänomen, oder: wo das Datenschutzrecht versagt

Bevor um die Lösungen eines Problems gerungen werden kann, ist es notwendig, sich über Inhalt und Ausmaß des Problems klarzuwerden. Wie sich zeigen wird, gibt es zwischen verschiedenen scheinbar disparaten Vorgän-

* Mehr über die Autor:innen erfahren Sie im Autor:innenhinweis auf S. 224 ff.

1 BVerfGE 65, 1 (41 ff.) – Volkszählung.

gen eine Verbindungslinie, die das zentrale Datenschutzproblem im digitalen Zeitalter kennzeichnet. Zu deren Aufdeckung ist es zunächst notwendig, anhand einiger Beispiele die Defizite des Datenschutzrechts aufzuarbeiten.

6.2.1 Beispiele

6.2.1.1 Videoüberwachung

Fall 1: A ist ein Gegner der Videoüberwachung. Beim Einkaufen muss er feststellen, dass sämtliche Supermärkte seiner Stadt offen Videokameras einsetzen, um Diebe sowohl abzuschrecken als auch effektiv verfolgen zu können. Er pickt sich Supermarktbetreiberin *S* heraus und verlangt die Einstellung der Videoüberwachung.

Der Fall illustriert, wie der Fokus des Datenschutzrechts auf den Einzelnen versagt, wenn sich viele oder sogar alle Verantwortlichen in einem bestimmten Lebensbereich ähnlich verhalten. Die Installation von Videoüberwachung in Supermärkten zwecks Schutz vor Ladendiebstahl ist derart alltäglich, dass sie nur selten Gegenstand der Rechtsprechung wird. In Strafverfahren werden derartige Aufnahmen bedenkenlos verwendet[2] und die ältere Literatur und Rechtsprechung sah hier von vornherein kein Problem.[3] § 4 Abs. 1 S. 2 Nr. 1 BDSG ordnet die Videoüberwachung von „Einkaufszentren“ ausdrücklich „als ein besonders wichtiges Interesse“ ein. Der Norm bzw. ihrem Vorläufer in § 6b BDSG-alt ist zwar attestiert worden, dass sie nichts legalisiere, was zum Zeitpunkt des Inkrafttretens nicht schon legal gewesen sei,[4] jedoch macht sie exemplarisch deutlich, in welche Richtung das Pendel der Interessenabwägung ausschlägt.

§ 4 BDSG ist nach h. M. europarechtswidrig, soweit er die Videoüberwachung durch Private regelt.[5] Rechtsgrundlage der Videoüberwachung ist in diesen Fällen allein Art. 6 Abs. 1 lit. f DSGVO, d. h. die allgemeine Interessenabwägung, für die die Erwägungsgründe 47 und 49 der DSGVO zumindest nahelegen, dass die Abwendung von Straftaten gegen eigene Rechte und Rechtsgüter zugunsten der Zulässigkeit zu berücksichtigen ist.[6] Die Polizeiliche Kriminalstatistik weist für 2019 insgesamt 303552

2 Aus jüngerer Zeit LG Paderborn, Urt. v. 14.10.2019 – 03 Ns 109/19, Rn. 35 – juris.
3 BayObLG, NJW 2002, 2893 (2893); AG Berlin-Mitte, NJW-RR 2004, 531 (533); *Huff*, JuS 2005, 896 (898).
4 *Ziebarth*, ZD 2017, 467 (468 f.).
5 BVerwG, NJW 2019, 2556, Rn. 47; *Starnecker*, in: Gola/Heckmann (Hrsg.), BDSG, Kommentar, 3. Aufl. 2019, BDSG § 4 Rn. 11; *Buchner*, in: Kühling/Buchner (Hrsg.), DSGVO/BDSG, Kommentar, 3. Aufl. 2020, BDSG § 4 Rn. 3.
6 *Schulz*, in: Gola (Hrsg.), Datenschutz-Grundverordnung, Kommentar, 2. Aufl. 2018, DSGVO Art. 6 Rn. 152.

erfasste Fälle einfachen Ladendiebstahls aus,[7] die Schäden gehen in die Milliarden.[8] Man wird bei einem derartigen Alltagsphänomen annehmen dürfen, dass beim Betrieb von Supermärkten tendenziell von einer Gefahr von Ladendiebstählen auszugehen ist, die jedenfalls die offene Videoüberwachung rechtfertigen dürfte.[9] Den berechtigten Interessen des/der Marktbetreiber:in und der Kund:innen steht ein nur geringer Eingriff in das Persönlichkeitsrecht gegenüber,[10] da die Kund:innen bloß in ihrer Sozialsphäre betroffen sind.[11] Auch die Branchenüblichkeit der Videoüberwachung[12] in Supermärkten dürfte vor diesem Hintergrund anerkannt sein. Aus dem Urteil des OLG Stuttgart zur Videoüberwachung im Supermarkt lässt sich nichts Gegenteiliges folgern, da der Verantwortliche in diesem Fall lediglich an Beweislastregelungen gescheitert ist[13] – ein Praxishinweis darauf, dass man gut daran tut, die Dokumentationspflichten aus Art. 5 Abs. 2 DSGVO einzuhalten. Nicht angängig dürfte es dagegen sein, die Interessenabwägung allzu pauschal vorzunehmen und mit der Vorinstanz offene und verdeckte Videoüberwachung undifferenziert gleichermaßen mit dem Diebstahlsschutz zu rechtfertigen.[14] Ohne die Details hier weiter ausbreiten zu müssen, wird doch zumindest eines deutlich: Videoüberwachung im Supermarkt ist im Grundsatz zulässig. Das bestätigt sich in der alltäglichen, auch von A im Beispielsfall gemachten Erfahrung, dass Supermärkte gänzlich ohne Videoüberwachung praktisch nicht mehr vorkommen.

Auf diese Weise ergibt sich in deutschen Supermärkten eine flächendeckende Überwachungslandschaft. Das kann dem einzelnen Supermarktbetreiber kaum zum Vorwurf gemacht werden, denn er hat dabei nur die eigenen Interessen in Form des Schutzes vor Ladendiebstahl im Blick.[15] Das Datenschutzrecht hat dem wenig entgegenzusetzen. Art. 6 Abs. 1 UAbs. 1 lit. f

7 Bundeskriminalamt, Polizeiliche Kriminalstatistik, Version 2.0, 67. Ausgabe, Band 4, S. 40.

8 *Ashelm*, https://www.faz.net/-16880023 (zuletzt aufgerufen am 1.6.2022).

9 *Lang*, Private Videoüberwachung im öffentlichen Raum, 2008, 289; vgl. in diesem Sinne auch VG Ansbach, Urt. v. 23.2.2022 – AN 14 K 20.00083, Rn. 45 – juris.

10 VG Ansbach, Urt. v. 23.2.2022 – AN 14 K 20.00083, Rn. 45 – juris; *Lachenmann*, in: Taeger (Hrsg.), Big Data & Co – Neue Herausforderungen für das Informationsrecht, 2014, 391 (402).

11 OVG Saarlouis, ZD 2018, 134, Rn. 40. Deshalb ist das Beispiel bei Europäischer Datenschutzausschuss, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Version 2.0, S. 11 zu pauschal.

12 Zu diesem Kriterium BVerwG, NJW 2019, 2556, Rn. 47.

13 OLG Stuttgart, ZD 2022, 105, Rn. 22 ff.

14 LG Stuttgart, Urt. v. 22.7.2020 – 21 O 82/19, Rn. 30 – juris; kritisch dazu mit Recht *Weichert*, DuD 2021, 61 (62); früher schon *Lang* (Fn. 9), 304.

15 Der besondere Bereich der Mitarbeiterüberwachung bleibt vorliegend ausgeklammert. Vgl. dazu *Venetis/Oberwetter*, NJW 2016, 1051 (1051 ff.); *Maschmann*, in: Kühling/Buchner (Fn. 5), BDSG § 26 Rn. 45 ff.

DSGVO bestimmt ausdrücklich, dass gegeneinander abzuwägen sind die „berechtigten Interessen des Verantwortlichen oder eines Dritten" mit den „Interessen oder Grundrechte[n] und Grundfreiheiten der betroffenen Person", wobei der „Dritte" nicht die gesamte Öffentlichkeit ist, wie aus Art. 4 Nr. 10 DSGVO folgt. Es handelt sich also um eine bloß bipolare Abwägung. Die gesamtgesellschaftliche Problematik bleibt außen vor, abgewogen werden miteinander jeweils subjektiv-öffentliche Rechte. Der Individualfokus des Datenschutzrechts[16] wird offenbar.

Die hier behandelte Fallgruppe macht den Individualfokus auch an anderer Stelle deutlich. In den Fällen, in denen Einzelpersonen gegen private Videoüberwachung vorgingen, waren sie stets selbst zumindest gelegentlich Gegenstand der Aufnahmen.[17] Das ist nach der Konzeption des Datenschutzrechts auch zwingend notwendig. Wenn A im Fall 1 den Supermarkt der *S* nämlich nie frequentiert hat und das auch nicht vorhat, dann liegt weder datenschutzrechtlich eine Erhebung seiner personenbezogenen Daten vor noch ist er aus Verfassungsperspektive in seinem Recht auf informationelle Selbstbestimmung betroffen. Gleichwohl ändert sein Fernbleiben nichts an der gestellten Diagnose, dass eine flächendeckende Überwachungslandschaft vorliegt. Spätestens hier zeigt sich deutlich die Grenze des Datenschutzrechts.

6.2.1.2 Bargeld

Es ist hier nicht der Ort, um über das rechtspolitische Für und Wider des Bargelds zu debattieren. Es genügt, darauf zu verweisen, dass Befürworter:innen der Beibehaltung von Barzahlungsmöglichkeiten genügend Energie aufwenden, um entsprechende Fälle bis vor den EuGH zu tragen,[18] sodass man zumindest die Relevanz der Debatte anerkennen muss. Staatliches Einschreiten gegen die Zahlung mit Bargeld steht freilich kaum zu befürchten. Aus der hier untersuchten Perspektive viel interessanter ist die durch die Corona-Pandemie in greifbare Nähe gerückte Abkehr einer Mehrheit privater Unternehmen vom Bargeld als Zahlungsmittel. So man der Zahlung in bar Persönlichkeitsschutzfunktion zubilligt,[19] entsteht dieselbe Situation wie bei der Videoüberwachung in Supermärkten: Gezwungen dazu ist niemand, aber wenn der bereitwillige Barzahler keinen Vertragspartner mehr findet, der Bargeld annimmt, ist die Situation für ihn dieselbe, als wenn er zur unbaren Zahlung gezwungen wäre.

16 *Bull*, DÖV 2022, 261 (271).
17 Vgl. die Sachverhalte bei AG Berlin-Mitte, NJW-RR 2004, 531 und LG Stuttgart, Urt. v. 22.7.2020 – 21 O 82/19.
18 Vgl. EuGH, NJW 2021, 1081 – Barzahlung des Rundfunkbeitrags.
19 Vgl. *Eibl*, Privatheit durch Bargeld?, 2020, 307 ff.

6.2.1.3 Künstliche Intelligenz

Eine scheinbar ganz andere Problematik stellt sich im Bereich der sogenannten „Künstlichen Intelligenz“ (KI). Bekanntlich ist die Definition dieses Begriffs schwierig.[20] Hier soll der Fokus auf solchen Systemen liegen, die die berüchtigte „Blackbox“-Problematik aufweisen:[21] Wie genau ein auf „Deep Learning“ basierendes System zu seiner Entscheidung gelangt, ist nach dem derzeitigen Stand der Technik nicht nachvollziehbar. Oftmals ist die Ausgabe derartiger Systeme aber so nah am Gewollten, dass sich die Erwartungen geradezu ins Unermessliche steigern. KI ist aber nicht magisch, sondern eine Technik, die erforschbaren Naturgesetzen folgt – wer das verkennt, der verunmöglicht eine sachliche Diskussion.[22] Auch die Jurisprudenz ist vor derartigen Annahmen, die KI Rechtssubjektivität zuschreiben wollen, scheinbar nicht gefeit.[23] Nach dieser notwendigen Klarstellung lässt sich folgender Fall diskutieren.

Fall 2:[24] B will einen Mobilfunkvertrag auf der Webseite der *M GmbH* abschließen, weil das der günstigste, wenngleich nicht einzige Anbieter solcher Dienste ist. Im Bestellprozess erteilt sie ihre Einwilligung dazu, dass zu Zwecken der Ermittlung der Zahlungsausfallwahrscheinlichkeit ihr öffentliches Facebook-Profil vollautomatisiert analyisiert werden darf. Sodann wird ihr der Vertragsschluss vollautomatisiert mit der Begründung verweigert, das selbstlernende System der *M* habe eine hohe Zahlungsausfallwahrscheinlichkeit ermittelt. *B*, die ihre dunkle Hautfarbe auf Facebook in ihrem Profilbild stolz und absichtlich öffentlich zur Schau stellt, hat einen Verdacht, weshalb ihr trotz tadelloser Bonität bei allen großen deutschen Auskunfteien der Vertragsschluss verweigert wird. B verlangt von *M* Schmerzensgeld. *M* gibt zutreffend an, dass die Trainingsphase des Systems abgeschlossen war, bevor B überhaupt ihr Facebook-Konto eröffnet hatte, und lehnt die Zahlung schon allein deshalb ab.

Derartige Probleme „intelligenter“ Systeme sind lange bekannt.[25] Man spricht vom „machine bias“.[26] Nun handelt es sich bei der ethnischen Herkunft nicht nur überhaupt um ein personenbezogenes Datum (Art. 4 Nr. 1

20 *Herberger*, NJW 2018, 2825 (2825 ff.).
21 Näher *Martini*, Blackbox Algorithmus, 2019, 41 ff.
22 *Herrmann*, FIfF-Kommunikation 4/2020, 12 (14 f.).
23 Vgl. *Kunesch*, JB ÖffR 2021, 305 (313 ff.); nachdrücklich gegen solche Bestrebungen *Bull*, Der Staat 58 (2019), 57 (65 f.).
24 Der Fall wurde gegenüber der im Vortrag vorgestellten Fassung leicht abgewandelt, um die Problematik besser herauszustellen.
25 Vgl. *Thoneick*, DIE ZEIT v. 30.7.2020, 29; *Kolleck/Orwat*, Mögliche Diskriminierung durch algorithmische Entscheidungssysteme und maschinelles Lernen – ein Überblick, 2020, 32 ff.
26 *Martini*, (Fn. 21), 47 ff.

DSGVO), sondern sogar um besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO. Was hat das Datenschutzrecht also zu dem Problem zu sagen?

Ein Anspruch auf Schmerzensgeld ließe sich im Datenschutzrecht nur auf Art. 82 Abs. 1 DSGVO gründen. Hier sind dabei zunächst zwei Dinge auseinanderzuhalten: die Trainingsphase des selbstlernenden Systems und seine Anwendung. In beiden Fällen werden personenbezogene Daten verarbeitet, sodass der Anwendungsbereich der DSGVO nach Art. 2 DSGVO sicher eröffnet ist, allerdings handelt es sich wegen der zeitlichen Abfolge – B hat ihr Facebook-Konto später eröffnet – in der Trainingsphase nicht um personenbezogene Daten gerade der *B*. Bereits das hindert nach einer (allerdings bestrittenen) Auffassung ihre Aktivlegitimation im Rahmen des Art. 82 Abs. 1 DSGVO.[27] Auch, wenn man dem nicht folgt, lässt sich in der Trainingsphase der nach Art. 82 Abs. 1 DSGVO erforderliche Verstoß gegen die DSGVO regelmäßig nicht feststellen, da die Korrelationsbildung nicht von der DSGVO geregelt wird.[28] Was die Erhebung der zur Korrelationsbildung verwendeten personenbezogenen Daten angeht, darf man saubere Arbeit der *M* unterstellen und von einer Rechtmäßigkeit ausgehen.

In der zweiten Phase liegen zweifellos personenbezogene Daten der B vor, sodass sich die Streitfrage nach der Aktivlegitimation bei Art. 82 Abs. 1 DSGVO nicht mehr stellt. Ein Verstoß gegen die DSGVO liegt möglicherweise überraschend allerdings nicht in einer Verletzung des Art. 9 DSGVO, denn unabhängig von der Frage, ob die *M* überhaupt die Hautfarbe der B verarbeitet hat, hat die B ihr Profilbild selbst öffentlich gemacht. Das führt nach Art. 9 Abs. 2 lit. e DSGVO zur Unanwendbarkeit des Verbots in Art. 9 Abs. 1 DSGVO. Die Beurteilung der Rechtmäßigkeit der Datenverarbeitung richtet sich damit nur nach dem allgemeineren Art. 6 Abs. 1 DSGVO.[29] Die Verarbeitung des Profilbilds beruht nun auf einer Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO. Deren Wirksamkeit steht das relative Kopplungsverbot aus Art. 7 Abs. 4 DSGVO nicht entgegen, denn es gibt andere alternative Anbieter und die günstigen Preise bei *M* beruhen wohl gerade auf der innovativen Datenverarbeitungstechnik zur Minimierung von Zahlungsausfallrisiken.[30] Die im Rahmen von Art. 7 Abs. 4 DSGVO besonders neuralgische Übermittlung von Daten an Dritte findet im vorliegenden Fall gerade nicht statt. Dem weiteren Einwand, in der Verarbeitung aber gerade der Hautfarbe

27 *Gola/Piltz*, in: Gola (Fn. 6), DSGVO Art. 82 Rn. 10; *Kreße*, in: Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Handkommentar, 2. Aufl. 2018, DSGVO Art. 82 Rn. 11; a. A. *Bergt*, in: Kühling/Buchner (Fn. 5), DSGVO Art. 82 Rn. 14 f.

28 *von Lewinski*, Die Matrix des Datenschutzes, 2014, 56.

29 *Schulz*, in: Gola (Fn. 6), DSGVO Art. 9 Rn. 25.

30 Vgl. zu diesen Kriterien *Buchner/Kühling*, in: Kühling/Buchner (Fn. 5), DSGVO Art. 7 Rn. 47 und 52 f.

aus dem Profilbild habe die B nicht eingewilligt, steht die Ungewissheit von deren Verarbeitung entgegen – B ist für diese Behauptung nach den allgemeinen zivilprozessualen Regeln beweisbelastet. *M* wird eine Verarbeitung der Hautfarbe nicht nur niemals zugeben, wegen der „Blackbox"-Problematik kann sie sie auch gar nicht kennen.[31] Deshalb wird der B auch der datenschutzrechtliche Auskunftsanspruch aus Art. 15 Abs. 1 DSGVO nicht helfen – eine solche Auskunft ist unmöglich (§ 275 Abs. 1 BGB, oder, falls man dessen Anwendung im europarechtlichen Kontext scheut, nach dem allgemeinen Rechtsgrundsatz „impossibilium nulla est obligatio"). Ist also die Verarbeitung des Profilbilds nach Art. 6 DSGVO rechtmäßig, bleibt als letzte Hürde noch Art. 22 DSGVO zu betrachten. Die Norm regelt nicht das Profiling, sondern stellt nur die darauf basierende Entscheidung unter besonderen Rechtfertigungsvorbehalt.[32] Zwar dürfte tatsächlich ein Fall des Art. 22 Abs. 1 DSGVO vorliegen, aber die Einwilligung der B führt über Art. 22 Abs. 2 lit. c DSGVO auch hier zur Rechtmäßigkeit, jedenfalls dann, wenn man unterstellt, dass die flankierenden Schutzmaßnahmen nach Art. 22 Abs. 3 DSGVO von *M* eingehalten worden sind, also insbesondere eine Gegendarstellungsmöglichkeit eingeräumt wurde. Art. 22 Abs. 4 DSGVO verbietet zwar unter gewissen Umständen ausschließlich automatisierte Entscheidungen auf Basis besonderer Arten personenbezogener Daten wie etwa der Hautfarbe, aber abgesehen von der Frage, ob die Norm eigentlich nur auf Art. 9 Abs. 1 DSGVO oder auch auf Art. 9 Abs. 2 DSGVO verweist – in letzterem Falle wäre sie hier gar nicht einschlägig – ist die B für diese Verarbeitung wieder beweisbelastet. Es lässt sich also auch in der zweiten Phase kein DSGVO-Verstoß feststellen. An der Beweislastproblematik würde schließlich auch ein denkbarer Anspruch aus § 21 Abs. 2 AGG scheitern.[33] B wird kein Schmerzensgeld bekommen.

Prozessual ist die Angelegenheit damit geklärt. Nimmt man an, dass das selbstlernende Webseitensystem tatsächlich die Hautfarbe mit einer höheren Zahlungsausfallwahrscheinlichkeit korreliert hat, bleibt aber ein ausgesprochen fader Beigeschmack. Er findet seine Berechtigung darin, dass der „machine bias" oft auf unausgewogene Trainingsdaten zurückführbar[34] und deshalb vermutlich[35] auch korrigierbar ist. Diese bestehen aus einer großen Menge personenbezogener Daten einer Vielzahl von Personen – nicht um-

31 Vgl. *von Lewinski/de Barros Fritz*, NZA 2018, 620 (622).

32 *von Lewinski*, in: BeckOK DatenSR, 40. Ed. 1.5.2022, DSGVO Art. 22 Rn. 5 ff.

33 Vgl. zu Ansprüchen aus dem AGG *von Lewinski/de Barros Fritz*, NZA 2018, 620 (622).

34 *Kolleck/Orwat* (Fn. 25), 32; *Martini* (Fn. 21), 50 f.

35 Dass der „machine bias" technisch vermeidbar ist, soll hier unterstellt werden, ist aber keineswegs gewiss. Selbstlernende Systeme sind prädestiniert dafür, statt ausdrücklich verbotener Merkmale (z. B. Geschlecht) Stellvertretermerkmale wie die besuchte (Mädchen-)Schule heranzuziehen, wie insbesondere Amazon erfahren musste, *Dastin*, https://www.reuters.com/article/-idUSKCN1MK08G (zuletzt aufgerufen am 15.6.2022).

sonst ist die Rede von „Big Data“. Das Datenschutzrecht bietet aber keine Handhabe, die Trainingsdaten zu regulieren, schon gar nicht für die betroffene Person einer Verarbeitung auf Grundlage dieser Trainingsdaten. Es zeigt sich wieder die Grenze der Individualität des Datenschutzrechts. Das deckt sich mit den Ausführungen der EU-Kommission im Weißbuch zu KI, die die Risiken von KI vornehmlich in gesamtgesellschaftlichen Problematiken erblicken.[36] *Mühlhoff* hat für dieses Problem jüngst den Begriff „prädikative Privatheit“ vorgeschlagen: es werden Aussagen über eine Person aus den statistisch aggregierten Daten anderer Personen abgeleitet.[37] Freilich hat *Heller* denselben Befund bereits vor über zehn Jahren festgestellt.[38] Bemerkenswert ist allerdings, wie *Heller* und *Mühlhoff* auf der Grundlage derselben empirischen Ausgangslage zu diametral unterschiedlichen Schlussfolgerungen gelangen: während ersterer die „Post-Privacy“ einläutet und Privatheit für tot erklärt, führt letzterer ein neues ethisches Konzept zum Schutz von Privatheit ein. Im Datenschutzrecht findet bislang allerdings weder der eine noch der andere Ansatz Resonanz.

6.2.1.4 Die Identifikationsnummer nach dem RegMoG

Das Registermodernisierungsgesetz (RegMoG)[39] hat durch die Einführung von § 1 IDNrG die steuerliche Identifikationsnummer nach § 139b AO zu einem Kennzeichen von allgemeiner Bedeutung im Sinne des Art. 87 DSGVO aufgewertet.[40] Das geschah vornehmlich, um die Digitalisierung von Verwaltungsdienstleistungen zu fördern, da Uneindeutigkeiten bei der Personenidentifikation eine manuelle Intervention von Sachbearbeiter:innen der Verwaltung notwendig machen und zum Abbruch eigentlich automatisierbarer Prozesse führen.[41] Auch wenn man über „Digitalisierung als Politikziel“ trefflich streiten kann,[42] handelt es sich um eine zu respektierende Entscheidung des demokratisch legitimierten Gesetzgebers. Diffuse Ängste vor einer Rückkehr des Nationalsozialismus[43] vermögen daran nichts zu ändern, denn Diktaturen erheben die zur Gängelung ihrer Bevölkerung noch

36 Vgl. COM(2020) 65 final, 12 ff. Vgl. zu den wenigen (vorliegend nicht einschlägigen) datenschutzrechtlichen Regelungen mit gesamtgesellschaftlicher Perspektive auch *von Lewinski* (Fn. 28), 55 ff.

37 *Mühlhoff*, Ethics Inf. Technol. 23 (2021), 675 (679); dazu auch in diesem Tagungsband der Beitrag von *Mühlhoff/Ruschemeier*, S. 38ff.

38 *Heller*, Post-Privacy, 2011, 12.

39 Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze, BGBl. I 2021, 591.

40 *von Lewinski/Gülker*, DVBl. 2021, 633 (633).

41 BT-Drs. 19/24226, 36; a. A. *Bull*, DÖV 2022, 261 (266), der als Hauptziel des Gesetzes Kostenersparnis ausmacht.

42 Dazu *Bull*, CR 2019, 478 (478 ff.).

43 Vgl. *padeluun*, FIfF-Kommunikation 4/2020, 59 (60).

fehlenden Daten ohnehin rasch.[44] Verschiedene Stimmen in der Literatur haben dem RegMoG daher auch seine Verfassungsmäßigkeit bescheinigt.[45]

Dennoch gehört auch die Registermodernisierung in den Reigen der hier zu behandelnden problematischen Themen. In der Zuweisung und Nutzung der Identifikationsnummer liegt ein rechtfertigungsbedürftiger Eingriff in das Grundrecht auf informationelle Selbstbestimmung, dessen Intensität allerdings von der Ausgestaltung der Steuer-Identifikationsnummer im Detail abhängt.[46] Ausschlaggebend sind hier Verknüpfungsmöglichkeiten. Diese wurden durch das RegMoG aber nicht verändert, sondern bestehende rechtliche Zusammenführungsverbote gelten fort. Es kommt lediglich zu einer faktischen Vereinfachung von Datenzusammenführung durch Beseitigung von Uneindeutigkeiten. Den damit verbundenen gestiegenen Missbrauchsmöglichkeiten begegnet das RegMoG durch verschiedene technische und organisatorische Maßnahmen einschließlich eines „Datenschutzcockpits" (§ 10 OZG).[47] Unter dem Strich bleibt damit ein für den Einzelnen eher leichter Grundrechtseingriff übrig. Dennoch darf man in der Fokussierung auf das Grundrecht des Einzelnen die Dimension des RegMoG nicht unterschätzen: ausnahmslos jeder (steuerpflichtige) Bürger erhält eine eindeutige Personenkennziffer, gegen deren Zuteilung er sich nicht (erfolgreich) zur Wehr setzen kann. Es handelt sich bei der Registermodernisierung also um eine Maßnahme, der man mit den Worten des BVerfG eine „große Streubreite"[48] attestieren kann, die hinsichtlich der Anzahl betroffener Personen diejenige der Vorratsdatenspeicherung noch übertreffen dürfte. Stellt man entsprechend der individuellen Abwehrfunktion der Grundrechte nur auf den Einzelnen ab, wird das Problem nicht in seiner vollen Dimension erfasst.

6.2.1.5 Vorratsdatenspeicherung

Mit der Vorratsdatenspeicherung nun ist *das* Thema überindividueller Betroffenheit schlechthin angesprochen. Die Vorratsdatenspeicherung lebt davon, dass gerade die Daten möglichst vieler Personen erfasst werden, um diese dann ungestört auswerten zu können. Im Vergleich zur Registermodernisierung hat die Vorratsdatenspeicherung schon gegenüber dem Einzel-

44 Am Beispiel ausgerechnet der Nationalsozialisten *Heller* (Fn. 38), 158 ff.; ebenso *Bull*, https://verfassungsblog.de/die-numerierung-der-buerger-effizienzdenken-versus-ueberwachungsangst/ (zuletzt aufgerufen am 28.5.2021).

45 *von Lewinski/Gülker*, DVBl. 2021, 633 (634 ff.); *Peuker*, NVwZ 2021, 1167 (1169 ff.).

46 *Martini/Wagner/Wenzel*, Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, 2017, S. 21.

47 Näher *von Lewinski/Gülker*, DVBl. 2021, 633 (640 f.).

48 BVerfGE 113, 348 (383) – Vorbeugende Telekommunikationsüberwachung; BVerfGE 125, 260 (318) – Vorratsdatenspeicherung; BVerfGE 150, 244, Rn. 98 – Kfz-Kennzeichenkontrollen II.

nen ein erhebliches Gewicht, da seine gesamte persönliche Telekommunikation aufgezeichnet wird, woraus sich „tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten […] gewinnen [und] bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen [lassen].“[49] Von daher können Vorratsdatenspeicherung und Registermodernisierung verfassungsrechtlich nicht über einen Kamm geschoren werden. Gleichwohl bestehen strukturelle Ähnlichkeiten, die die Behandlung unter dem gemeinsamen Oberbegriff des überindividuellen Datenschutzproblems gerechtfertigt erscheinen lassen. Hier wie dort kann man sich der staatlichen Erfassung nicht entziehen, weil die Staatsmaßnahme gegen den größten Teil der Bevölkerung gerichtet ist.

6.2.1.6 Soziale Medien einschließlich Sofortnachrichtendienste

Zum Abschluss der Fallbetrachtung sollen noch die sogenannten sozialen Medien auf überindividuelle Problematiken untersucht werden. Die verschiedenen Plattformen des Meta-Konzerns (ehemals Facebook) sind ein Massenphänomen. Die klassische „Facebook“-Plattform hatte 2019 in Deutschland etwa 32 Millionen monatliche Nutzer:innen,[50] d. h. bei ca. 83,2 Millionen Bundesbürger:innen 2019[51] fast die Hälfte der Bevölkerung. Der 25. ARD/ZDF-Onlinestudie zufolge nutzten 2021 73 % der 14- bis 29-Jährigen in Deutschland das ebenfalls zu Meta gehörende „Instagram“ mindestens wöchentlich,[52] der auch zu Meta gehörende Sofortnachrichtendienst „WhatsApp“ wird sogar von 70 % aller Deutschen täglich genutzt.[53] Damit gewinnt Meta einen signifikanten Einfluss auf die Bewegungsmöglichkeiten der Deutschen im Bereich der sozialen Medien. Das allein macht die Meta-Plattformen aber noch nicht zu einem Untersuchungsgegenstand für diesen Beitrag, denn marktbeherrschende Unternehmen gibt es bekanntlich in vielen Bereichen. Interesse wecken sie erst durch den Netzwerkeffekt. Dabei handelt es sich um das Phänomen, dass bei bestimmten Gütern der Nutzen dieser Güter mit steigender Nutzer:innenzahl zunimmt, was insbesondere bei Internetplattformen wegen deren Kontaktmöglichkeiten der Fall ist.[54] Nach dem Motto: wer hat, dem wird gegeben, entfaltet sich ein faktischer Zwang gegenüber denjenigen, die noch nicht Mitglied

49 BVerfGE 125, 260 (319) – Vorratsdatenspeicherung.
50 *Roth*, https://allfacebook.de/zahlen_fakten/offiziell-facebook-nutzerzahlen-deutschland (zuletzt aufgerufen am 4.6.2022).
51 Statistisches Bundesamt/Wissenschaftszentrum Berlin für Sozialforschung/Bundesinstitut für Bevölkerungsforschung, Datenreport 2021, S. 11.
52 *Beisch/Koch*, Media Perspektiven 10/2021, 486 (500).
53 *Beisch/Koch*, Media Perspektiven 10/2021, 486 (496).
54 *Simon/Clausen/Tacke*, https://wirtschaftslexikon.gabler.de/definition/netzwerkeffekte-51385/version-274556 (zuletzt aufgerufen am 15.6.2022).

der meistgenutzten Plattform sind. Wer „WhatsApp“ nicht nutzt, der wird schnell zum Ausgeschlossenen. Darin liegt kein unüberwindlicher Zwang, doch erfordert, wie der *Verf.* aus eigener Erfahrung zu berichten weiß, schon die Nichtnutzung von „WhatsApp“ neben einer gewissen Widerstandsfähigkeit einige Überredungskünste zugunsten anderer Sofortnachrichtendienste. Wer sich Sofortnachrichtendiensten insgesamt verweigert, gilt als Sonderling.

Ganz ähnlich wie in den früheren Gruppen wird in diesen Fällen dem Einzelnen die Hoheit über seine Lebensgestaltung ein Stück weit aus der Hand genommen. Will er nicht ausgeschlossen werden, muss der Einzelne sich auf die große Plattform einlassen und einen Vertrag mit einer der Meta-Töchter abschließen. Damit ist er gedrängt bis gezwungen, Metas Vertragsbedingungen und Datenverarbeitungspraxis zu akzeptieren. Da Meta bekanntlich aus den personenbezogenen Daten seiner Nutzer:innen Gewinn zieht, lastet auf dem Einzelnen die Entscheidung zwischen totaler digitaler Abschottung und freizügiger Datenpreisgabe, tertium non datur. Ein Dilemma, das sich als Ergebnis eines überindividuellen Problems darstellt. Wenn überhaupt, dann prüft nicht er, sondern prüfen Dritte wie Verbraucherschutzorganisationen[55] oder Datenschutzaufsichtsbehörden[56] die Praktiken der sozialen Medien. Bestenfalls bringt der Einzelne die Energie auf, *nach Vertragsschluss* gegen unliebsame Vertragsklauseln zu klagen.[57] Informationelle Selbstbestimmung wird zur Illusion.

6.2.2 Systematisierung

Die verschiedenen betrachteten Fälle lassen sich systematisieren (6.2.2.1) und zu einer Problemdefinition zusammenziehen (6.2.2.2).

6.2.2.1 Gruppenbildung

Gemeinsam ist zunächst allen betrachteten Fallgruppen, dass der Einzelne in der Ausübung seiner informationellen Selbstbestimmung gehemmt wird, obwohl ihm diese Freiheit vordergründig zugestanden wird. Die Gründe dafür unterscheiden sich allerdings:

- Bei der Videoüberwachung und einer möglichen schleichenden Bedeutungslosigkeit des Bargelds führt das gleichartige Verhalten einer Vielzahl für sich genommen eher unbedeutender Privater zu einer faktischen Schmälerung der Wahlfreiheit. Wer willens ist, weiter mit Bargeld zu be-

55 So im Fall EuGH, WRP 2022, 684 – Meta/vzbv.

56 So im Fall OVG Hamburg, ZD 2018, 230 – Datenzusammenführung Facebook/Whats App.

57 So im Fall BGH, NJW 2022, 1314 – Klarnamenpflicht bei Facebook.

zahlen oder unwillens, sich im Supermarkt auf Video bannen zu lassen, findet keine Vertragspartner mehr.

- In den sozialen Medien führt der Netzwerkeffekt zu einer Sogwirkung zugunsten einiger weniger, anders als bei der Videoüberwachung dadurch großer und bedeutsamer Privater. Das erzeugt letztlich nicht anders als im Falle der Videoüberwachung einen faktischen Zwang, die Datenverarbeitung über sich ergehen zu lassen.
- Bei der künstlichen Intelligenz kommt es durch ungünstige Relationen in den Trainingsdaten zu Diskriminierungen. Es steht dem Einzelnen aber nicht zu Gebote, die Trainingsdaten zu beeinflussen. Diese werden aus dem immensen Datenfundus des Internet („Big Data“) aus dem Verhalten der Mehrheit der Gesellschaft entnommen, welches Computer in unnachgiebiger mathematischer Präzision als diskriminierend festhalten und über die neuen automatisierten Entscheidungsprozesse fortschreiben. Wer einer automatisierten Einzelfallentscheidung nach Art. 22 DSGVO unterworfen wird, ist gezwungen, die damit einhergehende Diskriminierung zu ertragen.
- Flächendeckenden Staatsmaßnahmen mit „großer Streubreite“ wie Vorratsdatenspeicherung und Registermodernisierung kann man schon von Rechts wegen nicht entkommen und muss sie ertragen.

Damit zeigen sich zwei Hauptgruppen. Überindividuelle Datenschutzprobleme können entweder von Privaten (die ersten drei Fälle) oder vom Staat ausgehen (letzter Fall). Während es bei der Staatsmacht nur um das Problem der „großen Streubreite“ geht, ist das Bild bei den Privaten bunter. Einerseits kann eine Vielzahl von kleinen Privaten einen Mehrheitsstandard setzen, dem der Einzelne sich nur schwer entziehen kann. Damit dies auch einer kleinen Anzahl großer Privater gelingt, bedarf es demgegenüber eines zusätzlichen Faktors in Form des Netzwerkeffekts, dann aber unterscheidet sich die Wirkung auf den Einzelnen in ihrem faktischen Zwang nicht mehr von derjenigen, die eine Vielzahl kleiner Privater auslöst. Bei KI handelt es sich zum gegenwärtigen Zeitpunkt angesichts der geringen Verbreitung noch um ein Sonderproblem, das seine Einordnung in die Fragen überindividuellen Datenschutzes der Kuratierung der Trainingsdaten verdankt. Mit zunehmender Verbreitung von KI aber kann sich dieses Sonderproblem zur oben genannten ersten Gruppe hinzugesellen. Setzt erst einmal eine Vielzahl kleiner Privater KI ein – etwa, wenn sämtliche Versicherungsunternehmen dies zur Prämienbemessung tun –, dann kann man sich dem nicht mehr entziehen und wird zusätzlich noch Opfer der Diskriminierungsproblematik.

6.2.2.2 Definition des Problems

Die so gewonnenen Erkenntnisse erlauben es, den Schluss einer gemeinsamen verbindenden Problematik zu ziehen, die hier als überindividuelles Datenschutzproblem bezeichnet werden soll. Dieses wird auf Grundlage der obigen Fallgruppenbildung nunmehr definiert wie folgt:

Ein überindividuelles Datenschutzproblem liegt vor, wenn der Einzelne sich der Verarbeitung seiner personenbezogenen Daten nicht mehr entziehen kann, weil dies entweder de jure untersagt ist – Fall der staatlichen Datenverarbeitung mit großer Streubreite – oder weil dies de facto ohne Inkaufnahme erheblicher sozialer Nachteile unmöglich ist – Fall der Datenverarbeitung durch qualifizierte Private. Private sind qualifiziert, wenn entweder eine flächendeckende gleichgerichtete Datenverarbeitung einer Vielzahl voneinander unabhängiger „kleiner" Privater oder wenn eine Datenverarbeitung von vom Netzwerkeffekt profitierender „großer" Privater gegeben ist.

6.2.3 Zwischenergebnis: Individualfokus als Schwäche

Mit dieser Definition wird die Schwäche des Datenschutzrechts grell sichtbar. Denn seine Antwort auf die vermeintlichen Probleme des digitalen Zeitalters liegt in der Ermächtigung des Individuums zu einer selbstbestimmten Entscheidung. Dabei verkennt es im Bereich der privaten Datenverarbeitung, dass der Mensch kein solitäres Wesen ist, sondern in und von der Gemeinschaft mit anderen Menschen lebt. Entscheidungen über die Verarbeitung personenbezogener Daten sind wegen sozialen Drucks, der keineswegs durch den/die Anbieter:in der Datenverarbeitung, sondern von Kolleg:innen, Freund:innen und Familienmitgliedern ausgeübt wird, oft in Wahrheit fremdbestimmt. Indem das Datenschutzrecht informationelle Selbstbestimmung aber nur gegenüber dem Verantwortlichen sichert, blendet es die soziale Wirklichkeit aus. Gegenüber staatlicher überindividueller Datenverarbeitung liegt die größte Errungenschaft des Datenschutzrechts in seitenlangen Katalogen zur Regelung von Datenübermittlungsbefugnissen (vgl. exemplarisch §§ 22–24 TTDSG), ohne dass der/die Einzelne wirklich darüber bestimmen dürfte, was mit seinen/ihren personenbezogenen Daten geschieht.

Die Definition erlaubt aber auch, die bisher in verschiedenen Teilbereichen vorgeschlagenen Lösungen zu evaluieren. Gibt es einen Weg, das geltende Recht so auszulegen, dass das so definierte überindividuelle Datenschutzproblem beseitigt wird?

6.3 Lösungsansätze

6.3.1 Weite Auslegung des Datenschutzrechts

Die EU-Kommission hat der DSGVO unter Verweis auf eine internationale Vorbildwirkung eine globale Vorreiterrolle attestiert.[58] Es liegt daher nahe, die Lösung überindividueller Datenschutzprobleme auch im Datenschutzrecht als dem Rechtsgebiet des digitalen Zeitalters zu suchen. Wie oben aber bereits angedeutet wurde, gestaltet sich das schwierig. Schon das Volkszählungsurteil stellte mit dem Recht auf informationelle Selbstbestimmung die Handlungsmöglichkeiten und die Entscheidungsfreiheit des Einzelnen in den Mittelpunkt.[59] Das setzt sich im Datenschutzrecht fort. Indem etwa umfassende Transparenz angeordnet wird (Artt. 13–15 DSGVO), soll der Einzelne zu einer informierten, eben selbstbestimmten Entscheidung ermächtigt werden. Das ist aber nutzlos, wenn man auf die Datenverarbeitung trotzdem keinen Einfluss hat – man irrt in einem „Spiegelkabinett" herum, indem man alles sieht und doch nicht herauskommt.[60] Selbst dabei versagt aber das Datenschutzrecht noch, da sich ein „Right to Explanation" bezüglich automatisierter Entscheidungsfindung nicht aus der DSGVO ableiten lässt.[61] Selbst wenn das anders wäre,[62] führte eine erhöhte Transparenz nicht dazu, dass man auf den automatisierten Datenverarbeitungsvorgang Einfluss nehmen könnte. Zugespitzt formuliert liegt die Lösung des Datenschutzrechts für das Problem ausufernder Videoüberwachung also darin, Warntafeln mit Kamerasymbolen zu fordern. Dadurch wird nicht eine Kamera weniger errichtet. In den Worten der Post-Privacy-Bewegung: „Hilfe, das Internet ist überall"!.[63]

Führt Transparenz nicht weiter, müssen andere Mittel herhalten. Schon 2004 hat das AG Berlin-Mitte zur Videoüberwachung eines privaten, aber öffentlich zugänglichen Arkadengangs neben einem großen Berliner Kaufhaus dem vorgebrachten Argument, der Kläger könne doch die Straßenseite wechseln, die „immer stärker zunehmende Überwachungsdichte in Berlin" entgegengehalten, die für den Kläger „zu einem Zickzacklauf führen würde".[64] Dieselbe Argumentation findet sich nun viele Jahre später unter dem Schlagwort „Überwachungsdruck" im Dashcam-Urteil des BGH.[65] In beiden Fällen wird die Interessenabwägung nach dem heutigen Art. 6 Abs. 1

58 COM(2020) 264 final, 3.
59 Vgl. BVerfGE 65, 1 (42 f.) – Volkszählung.
60 So das plastische Beispiel bei *Hoepman*, in: Bayamlioğlu u. a. (Hrsg.), Being Profiled: Cogitas Ergo Sum, 2018, 46 (47).
61 *Wachter/Mittelstadt/Floridi*, IDPL 7 (2017), 76 (79 ff.).
62 So *Hoffmann/Kevekordes*, DuD 2021, 609 (610).
63 *Heller,* (Fn. 38), 17.
64 AG Berlin-Mitte, NJW-RR 2004, 531 (533).
65 BGH, NJW 2018, 2883, Rn. 26 – Dashcams.

lit. f DSGVO mit einem objektiven Kriterium aufgeladen. Damit strukturell verwandt ist die wiederkehrende, bereits erwähnte Argumentation des BVerfG zur erhöhten Eingriffsintensität kraft „großer Streubreite“[66] oder kraft Ausrichtung von Maßnahmen „auf eine unbestimmte Vielzahl von Personen […], die von vornherein hierzu keinerlei Anlass gegeben haben“[67]. Diese Herangehensweise ist gut gemeint, wirkt aber unbeholfen. An ihr ist mit Recht kritisiert worden, dass sie das tradierte System subjektiv-öffentlichen Rechtsschutzes sprengt, da Ausgangspunkt und Schutzobjekt im Datenschutzrecht wie auch im Grundrechtsschutz stets der Einzelne ist.[68] Dem Datenschutzrecht eine ganz objektive Dimension beilegen zu wollen, indem man eine „‚systemic‘ and ‚process-based‘ perspective that takes into account the whole socio-technical process of [automated decision making]“[69] einnimmt, geht daher an Inhalt und Intention der DSGVO vorbei. Art. 5 Abs. 2 DSGVO, den diese Argumentation zum Ausgangspunkt nimmt,[70] löst sich nur scheinbar von der individuellen Perspektive. Richtig ist, dass Art. 5 DSGVO einzelfallübergreifende Prinzipien enthält.[71] Daher muss auch nicht jeder einzelne Datenverarbeitungsvorgang protokolliert werden.[72] Die Grundsätze aus Art. 5 Abs. 1 DSGVO haben zwar durchaus auch insoweit eine objektive Dimension, als dass sie den Verantwortlichen auch dann verpflichten, wenn die betroffene Person ihre Betroffenenrechte nicht geltend macht.[73] Die Anknüpfung an die betroffene Person ist aber schon deshalb nicht entbehrlich, weil alle Prinzipien in Art. 5 Abs. 1 DSGVO nach dessen Eingangsformulierung das Vorliegen „[p]ersonenbezogene[r] Daten“ voraussetzen, die gem Art. 4 Nr. 1 DSGVO nun einmal Individualbezug haben. Für dieses Verständnis spricht ferner die Bußgeldbewehrung durch Art. 83 Abs. 5 lit. a DSGVO, denn die Gestaltung der Gesellschaft als Ganzes liegt außerhalb der Handlungsmöglichkeiten des einzelnen Verantwortlichen. Gegen einen bestimmten Verantwortlichen etwa für flächendeckende Videoüberwachungslandschaften in Supermärkten auch durch andere Verantwortliche ein Bußgeld verhängen zu wollen, grenzte an Beliebigkeit. Die Grundsätze dienen damit nur dazu, eine rechtswidrige Datenverarbeitung im Einzelfall zu unterbinden, nicht aber dazu, Vorstellungen über die Organisation der Gesellschaft vermittelst des Datenschutzrechts zu Wirksamkeit

66 BVerfGE 113, 348 (383) – Vorbeugende Telekommunikationsüberwachung; BVerfGE 125, 260 (318) – Vorratsdatenspeicherung.
67 BVerfGE 150, 244, Rn. 98 – Kfz-Kennzeichenkontrollen II.
68 *Bull*, DÖV 2022, 261 (271).
69 *de Hert/Lazcoz*, EDPL 2021, 31 (36).
70 *de Hert/Lazcoz*, EDPL 2021, 31 (35).
71 *Breyer*, DuD 2018, 311 (315).
72 *Herbst*, in: Kühling/Buchner (Fn. 5), DSGVO Art. 5 Rn. 80; *Breyer*, DuD 2018, 311 (315 f.).
73 *Herbst*, in: Kühling/Buchner (Fn. 5), DSGVO Art. 5 Rn. 1.

zu verhelfen. Ähnliches gilt für die ebenfalls angeführten[74] Art. 32 und 35 DSGVO, auch i. V. m. Art. 22 DSGVO. Alle diese Normen stellen stets den Einzelnen und seine personenbezogenen Daten in den Vordergrund.

6.3.2 Neue Einzelrechtsakte

Die Kommission scheint einer weiten Auslegung des Datenschutzrechts ebenfalls eher ablehnend gegenüber zu stehen. Anders lässt sich die Vielzahl von Gesetzesvorhaben, die sich in näherer Zukunft zahlreichen spezifischen Problemen der Digitalisierung annehmen sollen, jedenfalls nicht recht erklären. So soll ein Digital Markets Act den Netzwerkeffekt bändigen[75] und eine KI-Verordnung das Problem mit den Trainingsdaten angehen.[76] Insgesamt plant die EU-Kommission 52 Gesetzesvorhaben im Digitalbereich.[77] Alle diese Vorschläge lösen das ihnen gestellte Problem in mehr oder minder tauglicher Weise. Von der hier gewählten Perspektive muss man ihnen allerdings den Vorwurf machen, dass sie nur *das ihnen gestellte Problem* lösen. Es handelt sich um eine Vielzahl von Einzelrechtsakten, denen ein übergreifender Zugriff auf die gemeinsame Problematik der Überindividualität fehlt. Der Gesetzgeber reagiert statt zu agieren; ein Problem tut sich auf und das Gesetz regelt das Problem erst ex post. Puristen, darunter Anhänger der Post-Privacy-Bewegung, müssen darin die Wirkungslosigkeit des Rechts erkennen.[78] In sich schlüssig ist diese Position nicht. Denn wo das Recht nicht regulierend eingreift, gilt die allgemeine Handlungsfreiheit (Art. 2 Abs. 1 GG), die man bei der Post-Privacy-Bewegung gerade für durch den Datenschutz gefährdet hält. Tatsächlich handelt es sich nur um ein ganz normales Prozedere. Im Namen der Freiheit wartet das Recht ab, bevor es regulierend oder gar verbietend eingreift, worin man keine Kapitulation des Rechts vor der Technik erblicken kann.[79] Dennoch ist als Zwischenergebnis zu diesem Punkt festzuhalten, dass man ein übergreifendes Problem nicht mit einer Vielzahl unabgestimmter Einzelgesetze zu Unterproblemen in den Griff bekommen kann.

74 *de Hert/Lazcoz*, EDPL 2021, 31 (35 f.).
75 COM(2020) 842 final, 1.
76 COM(2021) 206 final, 34.
77 *Schmitz*, ZD 2022, 189 (189).
78 *Heller,* (Fn. 38), 20 ff.
79 *Bull*, Der Staat 58 (2019), 57 (59 ff.).

6.3.3 Verfassungsrechtliche Lösung

Wenn die Lösung nicht auf einfachrechtlicher Ebene auffindbar ist, dann vielleicht auf Ebene der Verfassung. Wie sich aber zeigen wird, sind alle drei diesbezüglich vertretenen Ansätze zu verwerfen.

6.3.3.1 Additiver Grundrechtseingriff

Klar hat speziell bezogen auf umfassende Visualisierungen des öffentlichen Raums insbesondere durch Googles „Street View" vorgeschlagen, das Institut des additiven Grundrechtseingriffs fruchtbar zu machen.[80] Eine Vielzahl von Akteuren nehme Maßnahmen von für sich genommen nur geringer Grundrechtsrelevanz vor, die erst in der in der Summe von größerer Bedeutung seien.[81] Das BVerfG hat in zwei Entscheidungen das Konzept des additiven Grundrechtseingriffs anerkannt.[82]

Dennoch liegt in diesem Ansatz eine Verkennung der Funktionsweise des additiven Grundrechtseingriffs.[83] Trotz Divergenzen zu seiner Funktionsweise im Detail[84] besteht weitgehend Einigkeit darin, dass sich die Einzelmaßnahmen *gegen dieselbe Person* richten müssen.[85] Diese Bedingung ist bei keinem der oben unter 6.2.2.1 betrachteten Bereiche erfüllt. Entsprechend der unter 6.2.2.2 gegebenen Problemdefinition geht es um Fälle, in denen eine Vielzahl von Personen betroffen ist. Lediglich *Kloepfer* hat zwischen einer vertikalen und einer horizontalen Eingriffsaddition unterscheiden wollen, wobei die vertikale Eingriffsaddition die Summierung von Eingriffen gegenüber einzelnen Personen und die horizontale Eingriffsaddition die Betroffenheit breiter Bevölkerungsteile erfasse.[86] Seine vertikale Eingriffsaddition ist identisch mit dem Verständnis des additiven Grundrechtseingriffs der h. M., und er selbst sieht dort auch „das schwerer wiegende Problem"[87]. Für die von ihm so bezeichnete horizontale Eingriffsaddition schlägt er beiläufig und ohne weitere Ausführungen die Anwendung der ob-

80 *Klar*, MMR 2012, 788 (790) ähnl. ohne Begr. *Geminn*, in: Schröder (Hrsg.), Bayerisches Datenschutzgesetz, 2021, BayDSG Art. 24 Rn. 76.
81 *Klar*, MMR 2012, 788 (790).
82 Vgl. BVerfGE 112, 304 (319 f.) – Global Positioning System; BVerfGE 114, 196 (247) – Beitragssatzsicherungsgesetz.
83 *Starnecker*, Videoüberwachung zur Risikovorsorge, 2017, 366.
84 So fordert *Lücke*, DVBl. 2001, 1469 (1470) eine Zweckgleichheit der einzelnen Grundrechtseingriffe, die *Kirchhof*, NJW 2006, 732 (734) ausdrücklich ablehnt.
85 *Lücke*, DVBl. 2001, 1469 (1470); *Voßkuhle/Kaiser*, JuS 2009, 313 (314); *Kirchhof*, NJW 2006, 732 (734); *Starnecker* (Fn. 83), 366; *Ruschemeier*, Der additive Grundrechtseingriff, 2019, 140 f.
86 *Kloepfer*, VerwArch 74 (1983), 201 (214).
87 *Kloepfer*, VerwArch 74 (1983), 201 (214).

jektiven Grundrechtsfunktionen vor.[88] Damit nimmt er die Diskussion um die Überwachungsgesamtrechnung vorweg, von der im nächsten Abschnitt die Rede sein soll.

Schließlich wurden unter dem Begriff des additiven Grundrechtseingriffs bisher nur Staatsmaßnahmen diskutiert. Wie die Fallbetrachtung unter 6.2.2.1 ergeben hat, sind aber heute Private ein maßgeblicher Faktor in der Entstehung von Überwachungslandschaften. Zu deren Erfassung müsste die Dogmatik des additiven Grundrechtseingriffs noch um die Kombination mit anderen Instituten wie etwa der mittelbaren Drittwirkung erweitert werden. Bis dahin ist der additive Grundrechtseingriff kein brauchbares Institut zur Lösung überindividueller Datenschutzprobleme.

6.3.3.2 Überwachungsgesamtrechnung und Freiheitsbestandsanalyse

Der Begriff „Überwachungsgesamtrechnung" wurde von *Roßnagel* im Anschluss an die Entscheidung des BVerfG zur Vorratsdatenspeicherung geprägt.[89] Er sieht in der Passage, in der das BVerfG den Gesetzgeber „in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung"[90] anhält, den Ausgangspunkt für eine doppelte Verhältnismäßigkeitsprüfung, die einmal individuell und einmal gesamtgesellschaftlich anhand aller bestehenden Überwachungsmaßnahmen in Gesamtschau ausgeführt werden müsse.[91] Eine solche doppelte Verhältnismäßigkeitsprüfung hat das BVerfG aber weder in dieser noch in einer anderen Entscheidung durchgeführt. Anderes folgt auch nicht aus dem gelegentlichen Rekurs des Gerichts auf eine „große Streubreite". Soweit das BVerfG hierauf zurückgreift, wird der Begriff ausschließlich zur Begründung einer hohen Eingriffsintensität genutzt,[92] d. h. die „große Streubreite" erhöht die Anforderungen an die später zu prüfende Angemessenheit. Eine doppelte Verhältnismäßigkeitsprüfung ist damit nicht verbunden.

Sieht man also genauer hin, kommen Zweifel an der These auf, das Urteil zur Vorratsdatenspeicherung enthalte eine Anwendung der objektiven Dimension der Grundrechte im Sinne *Kloepfers*.[93] Weder dieses Urteil noch die Entscheidungen zur „großen Streubreite" stellen eine Verbindung zur in

88 *Kloepfer*, VerwArch 74 (1983), 201 (214).
89 *Roßnagel*, NJW 2010, 1238 (1242).
90 BVerfGE 125, 260 (324) – Vorratsdatenspeicherung.
91 *Roßnagel*, NJW 2010, 1238 (1240); dem folgend *Braun/Albrecht*, VR 2017, 151 (152); kritisch dazu *Hornung/Schnabel*, DVBl. 2010, 824 (827).
92 Vgl. BVerfGE 113, 348 (383) – Vorbeugende Telekommunikationsüberwachung; BVerfGE 125, 260 (318) – Vorratsdatenspeicherung; BVerfGE 150, 244, Rn. 98 – Kfz-Kennzeichenkontrollen II.
93 Vgl. *Kloepfer*, VerwArch 74 (1983), 201 (214).

der *Lüth*-Entscheidung begründeten objektiven Grundrechtsdimension[94] her. Die maßgebliche Passage des Urteils liest sich angesichts der Wortwahl („Gesetzgebung […], die auf eine möglichst flächendeckende vorsorgliche Speicherung […] zielte", „im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger,", „Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf")[95] weniger wie Überlegungen zur objektiven Grundrechtsdimension, als vielmehr wie eine Paraphrase entsprechender Ausführungen des Mikrozensus-Beschlusses, in dem davon die Rede war, dass es mit „der Menschenwürde […] nicht zu vereinbaren [sei], wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren"[96]. Hier steht aber der Einzelne im Mittelpunkt. Die Wortwahl „solche Gesetzgebung wäre […] von vornherein mit der Verfassung unvereinbar"[97] deckt den eigentlichen dogmatischen Anknüpfungspunkt auf: es geht nicht um die objektive Grundrechtsdimension, sondern um den legitimen Zweck als erste Stufe der Verhältnismäßigkeitsprüfung. Das BVerfG wiederholt hier also unter Rückgriff auf Gedankengut des Mikrozensus-Beschlusses die zutreffende Erkenntnis, dass die Errichtung eines totalen Überwachungsstaats kein legitimer Zweck ist, weil ein solcher Zweck mit der Menschenwürde unvereinbar ist. Dieses Verbot, und nicht die Durchführung der Überwachungsgesamtrechnung, wird in den Rang der Verfassungsidentität[98] gehoben.[99] Die absichtliche Errichtung eines totalen Überwachungsstaats war aber nie das Ziel einer Bundesregierung, sondern „nur" die Erhöhung der Sicherheit oder doch zumindest des subjektiven Sicherheitsgefühls. Ob freilich letzteres ein legitimes Ziel ist, steht allerdings auf einem anderen Blatt und kann hier nicht vertieft werden.

Hinzu gesellen sich weitere Probleme. Die schwierige Operationalisierung der Überwachungsgesamtrechnung ist mehrfach kritisiert worden.[100] Ein sinnvoller, objektiver Bewertungsmaßstab lässt sich nicht finden.[101] Daran ändert auch das jüngst vorgestellte „Überwachungsbarometer für Deutschland" nichts. Dessen Autoren räumen selbst ein, dass sich eine absolute numerische Grenze für verfassungsrechtlich noch zulässigen Überwachungs-

94 BVerfGE 7, 198 (205) – Lüth.
95 Alle Zitate aus BVerfGE 125, 260 (324) – Vorratsdatenspeicherung.
96 BVerfGE 27, 1 (6) – Mikrozensus.
97 BVerfGE 125, 260 (324) – Vorratsdatenspeicherung.
98 Vgl. BVerfGE 125, 260 (324) – Vorratsdatenspeicherung.
99 A.A. *Roßnagel*, NJW 2010, 1238 (1242).
100 *Bieker/Bremert/Hagendorff*, in: Roßnagel/Friedewald/Hansen (Hrsg.), Die Fortentwicklung des Datenschutzes, 2018, 139 (144 ff.); *Hornung/Schnabel*, DVBl. 2010, 824 (827).
101 *Pohle*, FIfF-Kommunikation 4/2019, 37 (39).

druck nicht ziehen lässt.[102] Die Überwachungsgesamtrechnung bleibt immer eine wertungsabhängige Frage,[103] ist also inhärent subjektiv. Außerdem ist eine gewisse Fixierung auf staatliche Überwachung festzustellen,[104] die die oben erwähnten privaten Fallgestaltungen auslässt. Dem von *Pohle* selbst vorgestellten Gegenkonzept der Freiheitsbestandsanalyse[105] ist allerdings derselbe Vorwurf zu machen, zudem fordert er mit der verpflichtenden Beibringung empirischer Nachweise im Rahmen von Geeignetheit und Erforderlichkeit nichts weniger als eine Abkehr von der Einschätzungsprärogative des Gesetzgebers. Hierfür ist vor dem Hintergrund der Gewaltenteilung kein Raum. Sowohl die Freiheitsbestandsanalyse als auch die Überwachungsgesamtrechnung schließlich sind speziell auf Überwachungsfragen zugeschnittene Konzepte. Beide verfehlen den hier thematisierten Anspruch, eine generelle Lösung für überindividuelle Datenschutzprobleme zu liefern.

Mit alledem soll der Vorratsdatenspeicherung aber nicht per se Verfassungsmäßigkeit zugesprochen werden. Sie ist auch ohne die Einbeziehung objektiver Grundrechtsdimensionen ein erheblicher Grundrechtseingriff, von dem manche annehmen, das BVerfG habe ihn nur zur Vermeidung eines Konflikts mit dem EuGH gebilligt.[106] Immerhin wird praktisch das gesamte Online-Verhalten eines Betroffenen monatelang ex post nachvollziehbar. Auch das genügt für ein grundrechtswidriges „diffus bedrohliches Gefühl des Beobachtetseins“[107]. Auch die Geeignetheit der Vorratsdatenspeicherung darf man in Frage stellen.[108] Damit steht gegenüber staatlicher Massenüberwachung – also solcher de jure – ein effektives verfassungsrechtliches Abwehrmittel bereit.

6.3.3.3 Mittelbare Drittwirkung und staatsgleiche Grundrechtsbindung

Je nach Fallgestaltung können aber auch Private hinreichend qualifiziert sein, um dem Einzelnen de facto seine informationelle Selbstbestimmung abzuschneiden. Da liegt es nahe, diese Privaten unmittelbar an die Grundrechte zu binden und damit in der Prüfung der Grundrechte als Abwehrrechte eine generalisierbare Lösung für überindividuelle Datenschutzprobleme zu erblicken. Und tatsächlich hat das BVerfG bereits mehrfach davon gesprochen, dass „die mittelbare Grundrechtsbindung Privater einer Grund-

102 *Poscher/Kilchling/Landerer*, Überwachungsbarometer für Deutschland, 2022, 7.
103 *Moser-Knierim*, Vorratsdatenspeicherung, 2014, 237; *Pohle*, FIfF-Kommunikation 4/2019, 37 (39).
104 *Pohle*, FIfF-Kommunikation 4/2019, 37 (38).
105 *Pohle*, FIfF-Kommunikation 4/2019, 37 (40 f.).
106 Etwa *Hornung/Schnabel*, DVBl. 2010, 824 (828).
107 BVerfGE 125, 260 (320) – Vorratsdatenspeicherung.
108 Vgl. *Albrecht u. a.*, Schutzlücken durch Wegfall der Vorratsdatenspeicherung?, 2011.

rechtsbindung des Staates […] nahe oder auch gleich kommen“[109] könne. Speziell zur Facebook-Betreiberin Meta blieb es bislang allerdings bei Andeutungen.[110] Das BVerfG versucht zwar, diese neue, strengere Handhabung Privater unter Rückgriff auf die anerkannte Rechtsfigur der mittelbaren Drittwirkung zu kaschieren.[111] Tatsächlich leitet es aber unmittelbar aus der Verfassung Pflichten für Private ab.[112] Man kann für das so feststehende Ergebnis dann noch versuchen, eine Privatrechtsnorm zu finden, in der sich die so vorgefundene verfassungsrechtliche Wertung gewissermaßen ins einfache Recht hinein „entlädt“. Je nach Konstellation – man denke an die Videoüberwachung oder künstliche Intelligenz – steht eine solche Norm aber nicht zur Verfügung. Es liegt in der Konsequenz dieser Denkweise, dass dann notfalls ein extensiv verstandener § 242 BGB herhalten muss, um die verfassungsrechtlich vorgeschriebene Wertung irgendwie ins Privatrecht zu übertragen.[113] An diesem Punkt sollte man dann aber ehrlicherweise ganz auf die zivilrechtliche Einkleidung verzichten und offen von einer unmittelbaren Grundrechtsbindung Privater sprechen.

Die staatsgleiche Grundrechtsbindung ist kein Fall der mittelbaren Drittwirkung mehr, sondern kehrt sie um, da der Einfluss der Grundrechte nicht mehr legislativ mediatisiert werden muss.[114] Es werden nicht mehr auslegungsbedürftige Privatrechtsnormen mit der Ausstrahlungswirkung der objektiven Werteordnung der Grundrechte gefüllt, sondern Privatrechtsnormen für vorgegebene verfassungsrechtliche Wertungen gesucht (und gefunden).[115] Darin liegt ein Übergriff in die Sphäre des Gesetzgebers, der dazu aufgerufen ist, die widerstreitenden Grundrechte Privater miteinander in Ausgleich zu bringen. Folgen alle Antworten auf die maßgeblichen Fragen des Freiheitsausgleichs unter Privaten bereits aus der Verfassung, verengt sich der Spielraum des Gesetzgebers.[116] Konsequent zu Ende gedacht, wird er in dieser Argumentation überflüssig. Das aber ist mit der Staatsstruktur des Grundgesetzes nicht in Einklang zu bringen. Der faktische Befund,

109 BVerfGE 128, 226 (249) – Fraport; BVerfG, NJW 2015, 2485, Rn. 6 – Bierdosen-Flashmob; BVerfGE 148, 267, Rn. 33 – Stadionverbot; BVerfGE 152, 152, Rn. 88 – Recht auf Vergessen I.

110 Vgl. BVerfG, NJW 2019, 1935, Rn. 15 u. 18 ff. – Der III. Weg.

111 BVerfGE 148, 267, Rn. 32 – Stadionverbot.

112 *Michl*, JZ 2018, 910 (912); *Smets*, NVwZ 2019, 34 (35).

113 Irritierenderweise hat das BVerfG sich an anderer Stelle genau gegen eine solche Umfunktionierung von § 242 BGB ausgesprochen, *Hellgardt*, JZ 2018, 901 (902) unter Verweis auf BVerfGE 138, 377 (395 f.) – Mutmaßlicher Vater.

114 *Michl*, JZ 2018, 910 (917).

115 Exemplarisch *Raue*, JZ 2018, 961 (969 f.), der erst die mittelbare Drittwirkung diagnostiziert und dann Privatrechtsnormen zur Verwirklichung sucht.

116 *Michl*, JZ 2018, 910 (917).

dass der Gesetzgeber sich vor dieser Aufgabe drückt,[117] rechtfertigt keine staatsgleiche Grundrechtsbindung Privater. Statt den „Jurisdiktionsstaat“[118] herbeizuführen, sollte das BVerfG besser den Gesetzgeber zu mehr Tätigkeit anhalten.[119]

Der staatsgleichen Grundrechtsbindung Privater fehlt eine tragfähige Rechtfertigung.[120] Unter Privaten – gerade auch gegenüber „mächtigen“ Privaten – ist die Funktion der Grundrechte eine grundlegend andere. Sie kann deshalb nicht als Baustein für ein übergreifendes Werkzeug gegen überindividuelle Datenschutzprobleme herangezogen werden.

6.4 Eigene Überlegung

6.4.1 Keine übergreifende Lösung für Staat und Private

Die Betrachtung der bisher vorgebrachten Lösungsansätze zeigt zweierlei. Zum einen sind sie oft – wie namentlich die Überwachungsgesamtrechnung und das „Right to Explanation“ – zu spartenspezifisch, um für alle Formen überindividueller Datenschutzprobleme generalisiert zu werden. Zum anderen leiden die generalisierbaren Lösungen, etwa der horizontale additive Grundrechtseingriff und die staatsgleiche Grundrechtsbindung, unter dogmatischen Mängeln. Die vielversprechendste Lösung, nämlich alle überindividuellen Probleme entweder direkt oder im Wege einer staatsgleichen Grundrechtsbindung Privater an der Abwehrfunktion der Grundrechte zu messen, scheitert an der Unübertragbarkeit dieser Funktion auf privatrechtliche Verhältnisse. Das lässt in der Summe nur einen Schluss zu: eine ganzheitliche Lösung gibt es nicht.

Gibt man sich mit der tradierten Trennung von Staat und Privaten zufrieden, lassen sich aber in diesen Bereichen umfassende Lösungen finden. Überindividuelle Datenschutzprobleme, die de jure ausgelöst werden, sind auf den Staat zurückführbar und man kann ihnen deshalb ganz klassisch beikommen, indem sie an den Grundrechten, insbesondere dem Recht auf informationelle Selbstbestimmung, gemessen werden. Ob diese über ihre Individualschutzfunktion hinaus um eine Überwachungsgesamtrechnung erweitert werden müssen, kann für die Zwecke dieser Abhandlung offen bleiben; auf die zweifelhafte Grundlage und Notwendigkeit dieser These wurde oben unter 6.3.3.2 bereits hingewiesen. Werden überindividuelle Datenschutzprobleme dagegen de facto ausgelöst, weil Private handeln, sind andere Maßstäbe

117 *Smets*, NVwZ 2019, 34 (37).
118 Vgl. *Voßkuhle*, JuS 2019, 417 (418).
119 *Hellgardt*, JZ 2018, 901 (902).
120 So schon BVerfGE 128, 226 (275) – Fraport (Sondervotum *Schluckebier*).

anzulegen. Werden Private „mächtig“, liegt dahinter nichts anderes als ein gestörter Wettbewerb unter Privaten, den zu entstören Staatsaufgabe ist.[121] Nachfolgend soll deshalb der Fokus darauf liegen, auf dieser Basis eine für überindividuelle de-facto-Probleme generalisierbare Lösung zu finden.

6.4.2 Lösung überindividueller Datenschutzprobleme unter Privaten

Das BVerfG unterliegt in der Fraport- und Stadionverbot-Rechtsprechung erkennbar dem Irrtum, dass die mittelbare Drittwirkung der einzige Weg sei, auf dem die Grundrechte auf das Privatrecht einwirken. Dem ist aber nicht so. *Canaris* hat herausgearbeitet, dass nicht weniger als drei Arten der Einwirkung auf das Privatrecht zu unterscheiden sind:[122]

1. Bezüglich der privatrechtlichen Gesetzesnormen liegt eine unmittelbare Geltung gegenüber dem Gesetzgeber vor (Abwehrfunktion).
2. Bezüglich der Handelns Privater liegt eine mittelbare Drittwirkung vor, die in die Auslegung von Generalklauseln einstrahlt (objektive Werteordnung).
3. Soweit Generalklauseln nicht einschlägig sind, ist das private Handeln nicht selbst Gegenstand der Grundrechte, sondern nur des einfachen Rechts. In diesen Fällen wirken die Grundrechte aber als Schutzpflichten gegenüber Gesetzgeber und Gerichten (Schutzpflichtwirkung).

Das BVerfG vermischt in der genannten Rechtsprechungslinie die zweite und die dritte Gruppe. Dem ist, wie oben unter 6.3.3.3 gezeigt wurde, wegen Untergrabung des Gewaltenteilungsgrundsatzes nicht zu folgen. Stattdessen soll hier im Anschluss an *Canaris* die überindividuelle Problematik im Datenschutzrecht bei Privaten über die zweite und dritte Gruppe aufgelöst werden, da die erste mangels vorhandener Normen zu überindividuellen Datenschutzproblemen nicht einschlägig ist.

Soweit zunächst die zweite Gruppe einschlägig ist, ergeben sich keine nennenswerten Probleme. Wie der BGH im Verfahren zu Facebooks AGB-Klauseln zu Hassrede korrekt ausgeführt hat, unterliegt Meta keiner staatsgleichen Grundrechtsbindung, sondern lediglich § 307 Abs. 1 S. 1 BGB, dessen Generalklausel „Treu und Glauben“ nach der Maßgabe der *Lüth*-Entscheidung über die objektive Werteordnung der Grundrechte[123] in praktischer Konkordanz auszufüllen ist.[124] Ob man den dann gefundenen, aus

121 *Canaris*, AcP 184 (1984), 201 (207).
122 *Canaris*, AcP 184 (1984), 201 (224 ff.).
123 BVerfGE 7, 198 (205) – Lüth.
124 BGH, NJW 2021, 3179, Rn. 59 – Hassrede bei Facebook.

einer mittelbaren Drittwirkung von Art. 5 Abs. 1 S. 1 GG und Art. 3 Abs. 1 GG (!) hergeleiteten, doch sehr spezifischen und an die Stadionverbot-Entscheidung des BVerfG erinnernden Verfahrenserfordernissen zur Löschung von Hassrede in Form von Aufklärungs-, Begründungs- und Anhörungspflichten[125] zustimmt oder nicht, spielt dann keine Rolle mehr. Maßgeblich ist nur der dogmatische Ausgangspunkt im Privat- statt im Verfassungsrecht. Es stimmt zwar, dass wegen Fehlens einer spezifischen gesetzlichen Regelung das praktische Ergebnis sich *derzeit* nicht vom Ansatz des BVerfG unterscheidet. Es divergiert aber, sobald der Gesetzgeber tätig wird. Denn im Verständnis des BVerfG folgen die genannten Verfahrenspflichten direkt aus dem Grundgesetz, sind also dem einfachen Gesetzgeber von vornherein entzogen. Im hier vertretenen Verständnis kann er aber eine abweichende Regelung treffen, die den Zugriff auf die mittelbare Drittwirkung versperrt, soweit nicht ausdrücklich eine Generalklausel vorgesehen wird. Freilich gelten für solche Regelungen dann wiederum die Anforderungen der ersten Gruppe, sie sind also keineswegs beliebig formulierbar. Konkret bedeutet das, dass der Gesetzgeber also ein anderes Verfahren vorschreiben könnte, als der BGH es in seinem Urteil vorgesehen hat, ohne dass dies verfassungsrechtlich zu beanstanden wäre. Das BVerfG müsste ein solches Gesetz für verfassungswidrig erachten.

Ist weder die erste noch die zweite Gruppe einschlägig, fehlen Regelungen des privaten Verhaltens. Bedeutung hat das derzeit für die oben geschilderten Fälle der Videoüberwachung, der Bargeldakzeptanz und der künstlichen Intelligenz. Den Gesetzgeber treffen in diesem Falle Schutzpflichten;[126] die Schutzpflichtendimension des Rechts auf informationelle Selbstbestimmung und des Fernmeldegeheimnisses hat das BVerfG auch mehrfach angesprochen.[127] Allerdings steht dem Gesetzgeber in der Schutzpflichtendogmatik „ein sehr weiter Gestaltungs- und Konkretisierungsspielraum“[128] zu. Wegen der grundsätzlichen Unbestimmtheit von Schutzpflichten sind diese nur dann verletzt, „wenn Schutzvorkehrungen entweder überhaupt nicht getroffen sind, wenn die getroffenen Regelungen und Maßnahmen offensichtlich ungeeignet oder völlig unzulänglich sind, das gebotene Schutzziel zu erreichen, oder wenn sie erheblich hinter dem Schutzziel zurückbleiben“[129]. Mit dieser Formulierung lässt sich die gegenwärtige Lage in den genannten Gebieten gut umschreiben. Die Regelungen im Bereich der privaten Video-

125 BGH, NJW 2021, 3179, Rn. 83 ff. – Hassrede bei Facebook.

126 *Canaris*, AcP 184 (1984), 201 (225 ff.).

127 BVerfGE 158, 170, Rn. 32 – IT-Sicherheitslücken; BVerfG, NJW 2013, 3086, Rn. 20.

128 *Canaris*, AcP 184 (1984), 201 (226); vgl. auch BVerfGE 157, 30, Rn. 152 – Klimaschutz; BVerfGE 158, 170, Rn. 49 – IT-Sicherheitslücken; BVerfG, NJW 2013, 3086, Rn. 21.

129 BVerfGE 157, 30, Rn. 152 – Klimaschutz; BVerfGE 158, 170, Rn. 50 – IT-Sicherheitslücken; BVerfGE 142, 313, Rn. 70 – Zwangsbehandlung.

überwachung (§ 4 BDSG) und der Bargeldannahmepflicht (§ 14 Abs. 1 S. 2 BBankG) sind wegen Europarechtswidrigkeit[130] völlig unzulänglich. Im Bereich der künstlichen Intelligenz sind nach richtiger Lesart (oben 6.3.1) überhaupt keine Schutzmaßnahmen getroffen worden. In allen diesen Fällen verletzt der Gesetzgeber seine Schutzpflichten und wäre durch das BVerfG zum Handeln anzuhalten. Wegen Art. 1 Abs. 3 GG ist aber auch die fachgerichtliche Rechtsprechung angehalten, bei derartigen (Aus-)Fällen unter Ausnutzung der Rechtsfortbildungsmöglichkeiten dieser Schutzpflicht nachzukommen.[131] Wie schon bei der zweiten Gruppe erhebt das aber nicht diese Rechtsfortbildungsmaßnahmen in einen Verfassungsrang. Wird der Gesetzgeber doch noch tätig, kann er von ihnen abweichen. Die Fachgerichte sind von der Erfüllung der Schutzpflicht dann „erlöst".

6.5 Fazit und Ausblick

Überindividuelle Probleme im Datenschutzrecht sind de facto durch Private oder de jure durch den Staat induziert. Eine übergreifende, einheitliche Lösungsmöglichkeit dafür gibt es nicht, insbesondere liegt sie nicht in der Ausweitung der grundrechtlichen Abwehrfunktion auch auf Private. Stattdessen ist für den Staatsbereich auf herkömmliche Prüfungsmethoden zurückzugreifen, wohingegen im privaten Bereich allein und entgegen dem BVerfG eine Schutzpflichtenlösung zulässig ist, da andere Ansätze die Gewaltenteilung auflösen. Diese Schutzpflichten sind dort, wo überindividuelle Datenschutzprobleme – von der Videoüberwachung bis zur künstlichen Intelligenz – auftreten, gegenwärtig allerdings verletzt und zwingen Legislative wie Judikative zum Handeln. Soweit letztere handelt, haben ihre Rechtsfortbildungen allerdings nicht Verfassungsrang und können vom Gesetzgeber geändert werden.

Den richtigen Weg zeigt die EU-Kommission auf. Vorschläge wie die geplanten Verordnungen zu KI und digitalen Märkten gehen das gestörte Wettbewerbsverhältnis an und stellen das Gleichgewicht unter den Privaten wieder her. Ob die gewählten Maßnahmen die richtigen sind, muss sich im rechtspolitischen Diskurs erweisen, nicht in der Herleitung verfassungsrechtlich vermeintlich zwingender Vorgaben.

130 Zu § 4 BDSG BVerwG, NJW 2019, 2556, Rn. 47; zu § 14 BBankG EuGH, NJW 2021, 1081, Rn. 56 ff. – Barzahlung des Rundfunkbeitrags.

131 *Canaris*, AcP 184 (1984), 201 (227).

7 Influencer Marketing – was jetzt noch?

*Stefanie Lefeldt**

„Werbung wegen Abmahnung", „Werbung, selbstgekauft" oder „Anzeige wegen Markensichtbarkeit" müssen wir dank dem BGH auf Instagram nicht mehr lesen. Aber: war's das jetzt? Ist im Influencer Marketing jetzt alles klar und geregelt? Wird es keine Abmahnungen und Gerichtsverfahren mehr geben? Spoiler: Nein. Das Feld des Influencer Marketing bietet zahlreiche weitere ungeklärte Punkte. Weiterhin kommen in rasanter Geschwindigkeit neue Werbeformen hinzu, die neu bewertet und eingeordnet werden müssen. Dieser Beitrag versucht einen Überblick über die noch offenen Punkte und künftige Problemfelder zu geben.

7.1 Was ist passiert?

Nachdem in den vergangenen Jahren zahlreiche Land- und Oberlandesgerichte sehr unterschiedlich zum Thema Influencer Marketing entschieden hatten,[1] herrschte noch größere Verwirrung hinsichtlich der Frage nach der Kennzeichnungspflicht bei sog. Tap Tags auf Instagram. Dabei ging es vorrangig um solche Beiträge, für die keine Gegenleistung durch die vertaggten Firmen erbracht wurde. Influencer:innen konnten teilweise sogar nachweisen, die Produkte selbst gekauft zu haben.[2] Influencer:innen sahen keine Notwendigkeit für eine Werbekennzeichnung und auch die Landesmedienanstalten hatten diese für derartige Beiträge nie gefordert. Die verschiedenen Gerichtsentscheidungen gingen aber meist zu Lasten der Influencer:innen aus, sodass sowohl diese, als auch Verbände, Vereine und Landesmedienanstalten mit Spannung auf die ersten Entscheidungen des BGH zu dem Thema gewartet haben. Im Herbst 2021 war es dann so weit: die Verfahren der Influencerinnen *Luisa Maxime Huss*, *Cathy Hummels* und *Leonie Hanne* wurden vom BGH entschieden.[3] Der BGH sah für die Kennzeichnung selbst erworbener Produkte keine Kennzeichnungspflicht und räumte den medienrechtlichen Normen als bereichsspezifischen Spezialvorschriften Vorrang gegenüber den UWG-Normen ein.[4]

---

* Mehr über die Autorin erfahren Sie im Autor:innenhinweis auf S. 224 ff.

1 OLG Celle (13 U 53/16), LG Itzehoe (3 O 151/18), KG Berlin (5 U 83/18), OLG Braunschweig (2 U 78/19), OLG München (29 U 2333/19), OLG Karlsruhe (6 U 38/19), OLG Koblenz (9 U 595/20), OLG Köln (6 U 103/20).

2 Z. B. Verfahren „Vreni Frost" KG Berlin (5 U 83/18).

3 BGH I ZR 90/20, I ZR 126/20, I ZR 125/20.

4 Detailliert zu den Entscheidungen: Konsequenzen der BGH-Trias zum Influencer-Mar-

Es folgten die Entscheidungen zu *Diana zur Löwen* und *Vanessa Lock* im Januar 2022.[5] Bereits kurze Zeit später wurden die vom BGH aufgestellten Grundsätze vom OLG Frankfurt a. M. umgesetzt[6]: hier ging es um Beiträge über kostenlos zur Verfügung gestellte E-Books, die nicht werblich gekennzeichnet waren. Das OLG nahm hier eine Kennzeichnungspflicht an.

Hatten die ersten drei Entscheidungen des BGH keine Auswirkungen auf die Aufsichtspraxis der Landesmedienanstalten, so passten sie die Kennzeichnungsmatrix nach den neusten beiden BGH-Entscheidungen im Mai 2022 an.[7] Kostenlos zur Verfügung gestellte Produkte sind nun auch nach Auffassung der Landesmedienanstalten kennzeichnungspflichtig. Der Fall *Vanessa Lock* ist mittlerweile am Bundeverfassungsgericht anhängig, nachdem der BGH eine Anhörungsrüge gegen das Urteil vom 13.1.2022 zurückgewiesen hatte.[8]

7.2 Was hat der BGH noch nicht entschieden?

Der BGH hat sich an einigen Stellen so ausgedrückt, dass zumindest bei der Autorin noch ein paar Fragezeichen vorhanden sind.

Das betrifft zunächst die Aussage, dass es bei einem Tap Tag ohne Gegenleistung darauf ankäme, ob der Beitrag nach seinem Gesamteindruck übertrieben werblich sei. Dies sei eine Einzelfallentscheidung. Nun haben auch die Landesmedienanstalten in der Vergangenheit die Auffassung vertreten, dass z. B. Werbesprache oder starke Lobpreisungen ein Indiz für eine Kennzeichnungspflicht sein könnten. Insgesamt stellt sich aber folgende Frage: soll man Influencer:innen an dieser Stelle raten, eine negative Sache über das Produkt zu sagen, damit der Beitrag nicht zu werblich ist? Hier bleibt eine gewisse Unsicherheit, was der BGH als übertrieben werblich ansieht, sodass es in der Zukunft sicherlich weitere Gerichtsentscheidungen zu dem Thema geben wird.

Der BGH führt weiter aus, dass dann aber bei der Verlinkung auf eine Internetseite des Herstellers des abgebildeten Produkts regelmäßig ein werblicher Überschuss vorliege. Dies ist insofern etwa verwunderlich, als dass die meisten Tap Tags ja auf Internetseiten (nämlich Instagram Pages von Marken, diese sind ebenso „Internetseiten", nämlich Telemedien) führen und auf

keting: Verträge, Medienrecht und Überkennzeichnung, *Lefeldt/Heins/Laoutoumai*, CR 2022, 100.

5 BGH I ZR 35/21, I ZR 9/21.

6 OLG Frankfurt 6 U 56/21.

7 https://www.die-medienanstalten.de/fileadmin/user_upload/Rechtsgrundlagen/Richtlinien/ua_Leitfaden_Medienanstalten_Werbekennzeichnung_Online-Medien.pdf.

8 BGH I ZR 9/21, Beschluss vom 21. April 2022; BVerfG – 1 BvR 1223/22 (anhängig).

vielen dieser Instagram Accounts direkt Shops eingebunden sind. Beispiel: Vertaggt ein:e Influencer:in den Adidas-Instagram-Account, dann können Nutzer:innen auf diesem Account direkt auf „Shop ansehen“ klicken und werden dann über einzelne Produkte direkt auf die Website von Adidas weitergeleitet. Der Unterschied des Tap Tags zur Verlinkung auf die Website erschließt sich daher nicht wirklich. Verbraucher:innen werden bei beiden Varianten mit dem Shop des Anbieters konfrontiert. Nur am Rande sei gesagt, dass eine derartige Konfrontation durchschnittlichen Internetnutzer:innen aber auch zugemutet werden kann. So sagt auch der BGH: „[…] da gemäß § 3 Abs. 4 S. 1 UWG auf die Sicht des durchschnittlich informierten, situationsadäquat aufmerksamen und verständigen Verbrauchers abzustellen ist, der zu den angesprochenen Verkehrskreisen gehört. Dieser ist kein Neuling.“[9]

Offen ist auch, was der BGH genau unter einer deutlichen Kennzeichnung versteht. Er hat jedenfalls eine Werbekennzeichnung im Fließtext des Instagram-Beitrags, die „weder in Farbe noch Schriftbild hervorgehoben erfolgte“ nicht ausreichen lassen.[10] Dabei wäre zumindest der Autorin neu, dass der Text in Captions von Instagram-Beiträgen farblich anders gestaltet werden kann. Auch eine Art Hervorhebung, z. B. in Form einer Art Textmarkierung scheint es zumindest derzeit bei Instagram nicht zu geben. Letztlich bleibt daher auch hier die Empfehlung, die Werbekennzeichnung, wie auch von den Landesmedienanstalten empfohlen, an den Beginn des Beitrags zu setzen.

7.3 Was könnte noch relevant werden?

7.3.1 UWG-Novelle

Fraglich ist, ob die am 28.5.2022 in Kraft getretene UWG-Novelle im Punkt Influencer Marketing Auswirkungen auf die Kennzeichnungspraxis haben wird. Nachdem der BGH nun grundsätzlich geklärt hat, dass selbsterworbene Produkte bei einem Tap Tag nicht werblich gekennzeichnet werden müssen, erscheint die Novellierung des UWG an diesem Punkt für viele überflüssig. Die Novellierung sieht vor, dass eine Pflicht zur Werbekennzeichnung nur besteht, wenn Influencer:innen eine Gegenleistung erhalten. Der Erhalt oder das Versprechen einer Gegenleistung wird zunächst gesetzlich vermutet – diese Vermutung können Influencer:innen aber widerlegen, z. B. durch Vorlage einer Quittung.[11] Es bleibt abzuwarten, ob diese Neue-

9 BGH I ZR 125/20, Rn. 45.
10 BGH I ZR 9/21, Rn. 42.
11 Siehe Gesetzesbegründung unter https://dserver.bundestag.de/btd/19/278/1927873.pdf.

rung auch zu weiteren Abmahnungen führt. Sie wird von einigen Stimmen als Schlechterstellung für Inluencer:innen bewertet.[12]

7.3.2 Network Marketing

Die Corona-Pandemie hat das Themenfeld Network Marketing in den sozialen Medien befeuert. Diese neue Art der Tupperparties finden jetzt online statt. Es werden Kosmetika, exogene Ketone und Küchengeräte angeboten, sowie andere Provisionsgeschäfte abgewickelt und dies meist ohne werbliche Kennzeichnung. Nach Auffassung der Landesmedienanstalten müssen diese Beiträge werblich gekennzeichnet sein. Abmahnungen aus diesem Bereich sind der Autorin (bislang noch) nicht bekannt.

7.3.3 Neue Affiliate-Werbeformen

In den letzten Jahren tauchten immer wieder neue Affiliate-Werbeformen, wie z. B. LTK (früher LIKEtoKNOW.it) auf. Affiliate Links sind werblich zu kennzeichnen, dies muss aber oft bei jedem neuen Affiliate Tool von vorne erklärt werden. Hier sind zahlreiche neue Formen, Varianten und auch plattformeigene Tools denkbar, die zu Abmahnungen oder Verfahren führen könnten, sofern Influencer:innen derartige Links nicht kennzeichnen.

7.3.4 Gewinnspiele

Bei Gewinnspielen auf Social Media herrscht oft Unsicherheit – welche Vorgaben kommen von den Plattformen, wer ist hier eigentlich zuständige Behörde für Aufsichtsverfahren, wenn Gewinne nicht ausgeschüttet werden usw. Es gibt bislang wenig (bekannte) Abmahnungen aus dem Bereich, auch hier sollte aber weiterhin Vorsicht geboten sein. Teilnahmebedingungen sollten klar vermitteln, wie und bis wann man teilnimmt, was der Gewinn ist und Influencer:innen sollten die Gewinnerauswahl dokumentieren. „Seid besonders aktiv in den Kommies“ könnte z. B. als Teilnahmebedingung zu unklar sein.

7.3.5 Corporate, Health und Pharma Influencer:innen

Einige Firmen setzen mittlerweile auf eigene Mitarbeiter:innen als sog. Corporate Influencer:innen. Darunter versteht man meist Mitarbeiter:innen, die vertraglich festgelegt und angeleitet Social Media Inhalte für ihren Ar-

12 https://www.laoutoumai.de/rechtsgebiete/influencer-und-recht/82-neue-regeln-zur-werbekennzeichnung-von-influencer-beitraegen.

beitgeber erstellen und diesen damit bewerben. Im Unterschied dazu könnte man „organische Corporate Influencer“ verstehen, die bereits von sich aus und ohne Auftrag des Arbeitgebers online „Werbung“ machen. Ob Beiträge von Corporate-Influencer:innen gekennzeichnet werden müssen, ist bislang nicht entschieden, scheint aber wahrscheinlich, sofern tatsächlich eine vertragliche Vereinbarung und Vergütung vorliegt.[13]

Viele Baustellen entstehen derzeit im Bereich der Bewerbung von Medikamenten und Lebensmitteln. Bei Lebensmitteln ist bei der Bewerbung innerhalb der EU die sog. Health-Claims-Verordnung zu beachten. Hier scheinen sich momentan insbesondere die Abmahnungen und Verfahren zu gesundheitsbezogenen Angaben zu häufen. Hier führen derzeit insbesondere die Verbraucherzentralen Verfahren, in denen es oft um Nahrungsergänzungsmittel geht.[14]

Auch der Bereich der Pharma Influencer:innen ist auf dem Vormarsch und bietet zahlreiche Stolpersteine.[15] Das Heilmittelwerbegesetz (HWG) stellt Vorgaben dafür auf, dass Werbung für Heilmittel z. B. nicht irreführend sein darf. Werbung mit Bildern ist grundsätzlich nur unter bestimmten Voraussetzungen zulässig. Bei Schönheitsoperationen dürfen keine Vorher-Nachher-Darstellungen gezeigt werden (§ 11 Abs. 1 S. 3 HWG).

Ein Bereich, der hier im Rahmen der Corona-Pandemie relevant wurde: Die Bewerbung von Medizinprodukten wie Nasenspray oder Kaugummi als Mittel gegen Corona. Auch hier führen die Verbraucherzentralen derzeit zahlreiche Verfahren.[16] Derartige Verfahren können auch Influencer:innen und ihre Werbeversprechen betreffen.[17]

7.3.6 Podcasts

Der Bereich Podcasts ist bislang offenbar ausschließlich von den Landesmedienanstalten aufgegriffen worden, die nach der Novelle des Rundfunkstaatsvertrags Podcasts in ihre Kennzeichnungsmatrix aufgenommen hatten. Hintergrund ist, dass der Medienstaatsvertrag mit rundfunkähnlichen Telemedien nun auch die hörfunkähnlichen Telemedien und damit eben auch in

13 Detailliert zu dem Thema: OMR Education mit Dr. Martin Gerecke https://askomr.podigee.io/206-werbekennzeichnung-durch-corporate-influencer-mit-dr-martin-gerecke.

14 https://www.verbraucherzentrale.nrw/pressemeldungen/presse-nrw/vorgehen-gegen-unzulaessige-werbung-fuer-nahrungsergaenzungsmittel-70606.

15 Mehr zum Thema Pharma Influencer in diesem Tagungsband: Marie-Theres Neubauer, Pharma Influencer – Zu Risiken und Nebenwirkungen klick’ auf den Link in der Bio!, S. 107 ff.

16 https://www.verbraucherzentrale.nrw/pressemeldungen/presse-nrw/verbraucherzentrale-nrw-geht-gegen-angebliche-anticoronamittel-vor-72175.

17 Beispiel: https://www.instagram.com/p/CeSutTNq_a1/.

aller Regel Podcasts erfasst. Die Werbekennzeichnung in Podcasts erfolgte öfter noch durch falsche Begriffe (Werbeblöcke werden als Sponsorings bezeichnet oder Rabattcodes werden gar nicht werblich gekennzeichnet). Zuletzt zeichnete sich im Podcast-Bereich aber auch die Erstellung eigener Werbetrenner vermehrt ab.[18] Von Abmahnungen scheint der Bereich bislang weitgehend verschont geblieben.

7.4 Fazit

Das Influencer Marketing wird Gerichte, Verbände und Landesmedienanstalten auch die nächsten Jahre noch beschäftigen. Auf Grund der Schnelllebigkeit dieser Branche, bei der Gesetze und Gerichte nicht mithalten können, wird es immer wieder neue Phänomene geben, die nicht so ganz unter bisherige Normen passen. Die Länge der Gerichtsverfahren führt dazu, dass Influencer:innen in derartigen Fällen lange keine Sicherheiten haben.

18 Mehr zum Thema Werbung in Podcasts: https://mabb.de/uber-die-mabb/aktuelles/neuigkeiten-details/werbung-in-podcasts.html.

8 Pharma Influencer – Zu Risiken und Nebenwirkungen klick' auf den Link in der Bio!

*Marie-Theres Neubauer**

Werbende Influencer:innen sind Teil einer etablierten, auf manchen Märkten bereits vorherrschenden Marketingstrategie. Die vermeintliche Authentizität der Werbenden und das daraus resultierende große Vertrauen ihrer Followerschaft in die Empfehlungen bewirkt, dass auch Arzneimittelhersteller vermehrt auf solche „Pharma Influencer"[1] als Werbepartner:innen setzen. Durch die Normierungen des TMGs, des UWGs und BGH-Richter:innenspruch sind inzwischen rechtliche Rahmenbedingungen, insbesondere für die Art und Weise der Kennzeichnung der Werbung, gesetzt. Handelt es sich bei einem angepriesenen Produkt jedoch um eines, das „Risiken und Nebenwirkungen" birgt, greifen die Regelungen des Heilmittelwerbegesetzes. § 11 Abs. 1 S. 1 Nr. 2 HWG verbietet „Prominentenwerbung" auch für nicht rezeptpflichtige OTC-Arzneimittel. Ungewiss ist bislang, ob dieser besondere Status für Personen, „die auf Grund ihrer Bekanntheit zum Arzneimittelverbrauch anregen können", genauso auf Influencer:innen anwendbar ist.

8.1 Pharma Influencer

8.1.1 Influencer

„Wer heute verkaufen will, setzt auf Influencer Marketing".[2] Das gilt inzwischen überall, auch für die medizinische Versorgung. Aus diesem Grund treten immer mehr Unternehmen aus dem Pharma-Bereich an Influencer:innen heran. Im Rahmen dieser Kooperationen werben solche Pharma Influencer dann innerhalb ihrer persönlichen Social-Media-Auftritte für konkrete Heilmittel von Pharmazie-Unternehmen. Oft handelt es sich bei den Werbenden selbst um von einer Krankheit Betroffene, die das entsprechende Heilmittel vorstellen. Solche Influencer:innen werden auch Pinfluencer[3] genannt.

---

* Mehr über die Autorin erfahren Sie im Autor:innenhinweis auf S. 224 ff.

1 www.audimedes.com, https://www.audimedes.com/de/expertenblog/drei-dinge-die-sie-unbedingt-bei-der-kooperation-mit-patienten-influencern-beachten-sollten/, Stand: 4.8.2022.

2 www.medwatch.de, https://medwatch.de/2022/04/13/influencer-arzneimittel-werbung/, Stand: 12.8.2022.

3 www.healthrelations.de, https://www.healthrelations.de/pinfluencer-patienten-influencer/, 9.4.2021, Stand: 12.8.2022.

8.1.2 Das Marketing

Ein zu bewerbendes Produkt wird sodann häufig im Rahmen einer „Disease-Awareness"-Kampagne positioniert. Dabei soll grundsätzlich Aufmerksamkeit für konkrete Krankheitsbilder geschaffen und im Zuge dessen, mögliche – insbesondere hauseigene – Therapien vorgestellt werden.[4]

Daneben kommt es aber ebenso vor, dass ein Arzneimittel, wie es für Influencer Marketing üblich ist, eher beiläufig im Rahmen der täglichen Inhalte in einem Online-Beitrag (insbes. in „Stories") gezeigt, dessen Name und Inhaltsstoffe genannt, ein Erfahrungsbericht geteilt und das Produkt als „Must-Have" für eine Linderung bzw. gegen eine Krankheit angepriesen wird.[5]

Meist wird zusätzlich auf die entsprechende Social-Media-Präsenz entweder des Produktes oder der Marke oder des gesamten Unternehmens hingewiesen und/oder das konkrete Produkt mittels „Tap Tag" mit nur einem Klick beziehbar unverzüglich „zur Verfügung gestellt".[6]

Der Natur von Influencer:innen entspricht es, wie ein guter Freund aufzutreten. Ihre nahezu ununterbrochene, alltägliche Präsenz bewirkt, dass die Followerschaft ihre:n Influencer:in manchmal häufiger sieht als die eigenen tatsächlichen Freund:innen. Die Followerschaft kann oftmals jede Lebensphase nahezu live begleiten. Diese vermeintliche Nähe erzeugt großes Vertrauen, Verbindlichkeit und das Gefühl, man kenne die Person auf dem Bildschirm persönlich und gut. Dadurch erhalten die Meinungsmacher:innen einen erheblichen Glaubwürdigkeitsvorteil. Bewerben sie ein Produkt, hat es oft den Anschein, als teilten sie lediglich einen Erfahrungsbericht.

8.2 Arzneimittelwerbung

8.2.1 Zulässige Werbung

Publikumswerbung ist, anders als Werbung vor einem Fachpublikum, für verschreibungspflichtige Medikamente generell verboten. Eine situationsbedingte Ausnahme stellt sich dar, wenn Aufklärungsbedarf für die Allgemeinheit besteht und die „konkrete Gestaltung der Werbung keine Gefahr des Fehlgebrauchs eines Medikaments erwarten lässt".[7]

---

4 *Tillmanns*, PharmR 2021, 247, 248.

5 S. bspw., https://www.instagram.com/p/Ce59WVwLTC3/; https://www.instagram.com/s/aGlnaGxpZ2h0OjE3OTUwMDE3OTY3Mjg4MDI1?story_media_id=2071283917702132985&igshid=YmMyMTA2M2Y=, Stand: 12.8.2022.

6 Ebd.

7 *Streinz/Klaus,* in: Dauses/Ludwigs, C. V. Rn. 136; BGH Urt. v. 26.3.2009 – ZR 213/06 Rn. 22.

Grundsätzlich geworben werden darf vor einem Laienpublikum hingegen für nicht verschreibungspflichtige „Over-the-Counter"-Medikamente (OTC-Medikamente), sofern die konkrete Werbung bestimmte Bedingungen erfüllt.[8]

8.2.2 Kennzeichnungspflichten

Die Kennzeichnungspflichten für Influencer-Werbung sind durch drei parallele BGH-Urteile und die Neuregelung in § 5a Abs. 4 UWG in ihrem Grundsatz nunmehr deutlich: Hat ein Influencer für einen werbenden Post eine Gegenleistung erhalten und/oder gilt die Werbung als übertrieben,[9] muss innerhalb des Posts schriftlich und gut erkennbar „Werbung" oder „Anzeige" angegeben werden.[10] Im Falle eines Videos ist es nicht ausreichend, einmalig zu Beginn auf den Werbecharakter des Inhalts hinzuweisen. Es muss ein „unmissverständlicher, auf den ersten Blick erkennbarer solcher Hinweis erfolgen".[11] Das gilt nicht, wenn sich aus den Umständen für den vom BGH als maßgeblichen Rezipienten festgelegten „durchschnittlich informierten, situationsadäquat aufmerksamen und verständigen Verbraucher"[12] ergibt, dass es sich um eine geschäftliche Handlung, also Werbung handelt.[13] Bezieht sich diese Werbung jedoch auf ein Produkt, das Risiken und Nebenwirkungen birgt, greifen die Regelungen des § 4 HWG, das die Kennzeichnung der Produktbewerbung von Arzneimitteln reguliert.[14]

Neben dem durch § 4 Abs. 3 HWG bestimmten Text „Zu Risiken und Nebenwirkungen lesen Sie die Packungsbeilage/das Etikett und fragen Sie Ihren Arzt oder Apotheker" muss eine Werbung, die in § 4 Abs. 1 HWG genannten verpflichtenden Mindestangaben enthalten.[15]

8.2.3 Schleichwerbung im Sinne des § 11 Abs. 1 S. 1 Nr. 9 HWG

Die Art und Weise der Werbung, Produktanpreisung eher beiläufig in die täglichen dargestellten Inhalte mit einzubeziehen, birgt die Gefahr, Schleich-

8 *Streinz/Klaus,* in: Dauses/Ludwigs, C. V. Rn. 143.
9 *Peifer*, GRUR 2021, 1453, 1459.
10 BGH Urt. v. 9.9.2021 – I ZR 90/20 Influencer I, NJW 2021, 3450 Rn. 52, 60, 110 ; I ZR 125/20 Influencer II, GRUR 2021, 1414 Rn. 55, 67 f., 34; I ZR 126/20 Influencer III, MMR 2021, 892 Rn. 38–40, 43.
11 *Janning/Mäder/Hebbinghaus*, PharmR 2021, 49, 53.
12 BGH Urt. v. 9.9.2021 – I ZR 126/20 Influencer III, MMR 2021, 892 Rn. 55 m. w. N.
13 *Peifer*, GRUR 2021, 1453 (1459).
14 *Streinz/Klaus,* in: Dauses/Ludwigs, C. V. Rn. 129.
15 *Streinz/Klaus,* in: Dauses/Ludwigs, C. V. Rn. 144.

werbung im Sinne des § 11 Abs. 1 S. 1 Nr. 9 HWG zu sein. Unzulässig sind „Veröffentlichungen, deren Werbezweck missverständlich oder nicht deutlich erkennbar ist". „Veröffentlichungen" meint grundsätzlich Print-Publikationen.[16] Nach hiesiger Ansicht zutreffend wird jedoch auch vertreten, dass Online-Werbungen von solchen Veröffentlichungen umfasst sind.[17] Nicht nur die konkrete, meist sehr junge Zielgruppe des Influencer Marketings informiert sich überwiegend im Internet und über soziale Medien. Auch sonst googelt nahezu jede Person zunächst, entgegen allgemein bekanntem ärztlichen Rat, mögliche Ursachen bei aufkommenden Krankheitssymptomen. Es ist also nur konsequent, Veröffentlichungen im Internet im Sinne des Schutzzwecks der Norm mit einzubeziehen. Denn vor allem Internetbeiträge haben – oftmals den Anschein erweckend, es handle sich um reine Erfahrungsberichte – den Glaubwürdigkeitsvorsprung,[18] den der § 11 Abs. 1 S. 1 Nr. 9 verhindern möchte.

8.2.4 Anwendbarkeit der §§ 5a IV UWG, 4 HWG

Wie zu Beginn ausgeführt, sind die elementaren Kennzeichnungspflichten für Influencer Marketing festgesetzt.[19] Insoweit sind für eine Beurteilung der werbenden Pharma Influencer zunächst ebendiese Regulierungen maßgebend.

Für Werbung, die sich auf konkrete Heilmittelprodukte bezieht, sind hingegen die Regulierungen des Heilmittelwerbegesetzes, zu Kennzeichnungspflichten insbesondere der § 4 HWG, einschlägig.[20]

Die Vorschriften des UWG und des HWG sind kongruent.[21] In Fällen, in denen beide Normen einschlägig sind, sind UWG und HWG nebeneinander anwendbar.

Tatsächlich müsste der/die Influencer:in in Fällen, in denen er/sie ein Pharmazie-Produkt bewirbt, also die spezielle Normierung von Influencer-Werbung des § 5a Abs. 4 UWG und daneben die Bestimmungen aus § 4 HWG beachten.

16 *Köber,* in: MüKoUWG II. E. VII. Rn. 79.
17 *Janning/Mäder/Hebbinghaus*, PharmR 2021, 49, 51 m. w. N.
18 Ebd.
19 Vgl. Fn. 10 und insbes. § 5a IV UWG.
20 *Streinz/Klaus,* in: Dauses/Ludwigs, C. V. Rn. 129.
21 OLG Stuttgart Urt. v. 19.11.2009 – 2 U 40/09, BeckRS 2010, 12627, B. I. 4. B. cc.

8.2.5 Empfehlende Prominentenwerbung

Unzulässig nach § 11 Abs. 1 S. 1 Nr. 2 HWG ist Werbung für OTC-Arzneimittel von „Personen, die aufgrund ihrer Bekanntheit zum Arzneimittelverbrauch anregen können". (Laien-)Verbraucher:innen sollen vor Werbeaussagen geschützt werden, von denen mangels sachlicher Information die Gefahr einer Beeinflussung oder Irreführung ausgeht.[22] Eine Anpreisung handelt sich immer dann um solch sogenannte empfehlende Prominentenwerbung, wenn der Prominente nicht als reines Werbegesicht auftritt, sondern als „individuelle Gewährsperson" für ein bestimmtes Arzneimittelprodukt. Unterschieden wird somit zwischen unzulässigen Werbungen, die den Anschein erwecken, ein Prominenter stünde höchstpersönlich „hinter" einem Produkt und „schwöre darauf" und solch zulässiger Werbung, in der eine bekannte Persönlichkeit nur den „Werbekopf" hinhält.[23]

Die Unterscheidung im praktischen Einzelfall ist mitunter schwierig. Selbstredend werden die Testimonials als Werbestrategie eingesetzt, um den Verbraucher zu animieren, seinem großen Vorbild nachzueifern und das gezeigte Produkt zu kaufen.

Fraglich ist die Zuordnung von Influencer:innen zu Prominenten. Ausgangslage ist wieder die Werbebotschaft von einem bekannten Vorbild, jedoch eines, das der Verbraucher tagtäglich in sozialen Netzwerken verfolgt. Die vermeintliche Authentizität der Werbenden suggeriert dem Verbraucher ein nahes, vertrauensbasiertes, gar freundschaftliches Verhältnis zwischen Influencer:in und Follower:in. Der bereits hervorgerufene starke Wunsch, das gezeigte Produkt zu erwerben, wird nunmehr bei dem Follower um ein Vielfaches maximiert, da die Empfehlungswirkung in den Vordergrund rückt und der/die Follower:in denkt, „sein:e"/"ihr:e" Influencer:in empfehle ihm persönlich etwas, das ihm helfe.

Das Heilmittelwerbegesetz enthält keine Regelungen zur speziellen Werbestrategie des Influencer Marketings. Gleichermaßen verhält es sich mit der Rechtsprechung, die sich mit einer Klärung der Fragen, ob und gegebenenfalls wann Influencer:innen als Prominente im Sinne des § 11 Abs. 1 S. 1 Nr. 2 HWG gelten, bislang nicht befasst.

Ausschlaggebend für die Zuordnung eines Influencers ist wohl seine Reichweite. Influencer:innen werden anhand Ihrer Follower:innenanzahl von den Wirtschaftswissenschaften in Nano-, Micro-, Macro-, Mega- und Giga-Influencer:innen,[24] hier nun abstrahiert in Micro- und Macro-Influencer:innen, unterteilt.

---

22 *Streinz/Klaus,* in: Dauses/Ludwigs, C. V. Rn. 146.

23 OLG Karlsruhe Urt. v. 8.4.2015 – 6 U 66/13, NJW-RR 2016, 111, 112 Rn. 21.

24 *Kilian,* in: Theobald/Gaiser, Brand Evolution, S. 468.

8.2.5.1 Macro-Influencer:innen

Macro-Influencer:innen generieren hunderttausende bis mehrere Millionen Follower in sozialen Netzwerken.[25] Die erhebliche Anzahl an täglichen Zusehenden begründet zunächst die Zuordnung als Prominente im Sinne des § 11 Abs. 1 S. 1 Nr. 2 HWG.[26] Zudem entspricht eine solche Einordnung dem Sinn und Zweck des § 11 Abs. 2 S. 1 Nr. 2 HWG, der Werbeaussagen Dritter vorbeugen will, die gegenüber ihren Rezipienten durch eine Art Vertrauensvorteil den Anschein von Objektivität und Neutralität erwecken können.[27] Tatsächlich können Influencer:innen im Übrigen oftmals wesentlich mehr Follower vorweisen als klassische Prominente, die in sozialen Netzwerken schlicht weniger aktiv sind.

8.2.5.2 Micro-Influencer:innen

Micro-Influencer:innen haben mit einer Follower:innen-Anzahl von 1000 bis 100000[28] hingegen eine geringere Reichweite und positionieren ihre Inhalte vorzugsweise in Nischenbereichen. Es wird daher teils angenommen, dass hier nicht § 11 Abs. 1 S. 1 Nr. 2 HWG einschlägig ist. Anwendbar soll jedoch § 11 Abs. 1 S. 1 Nr. 11 HWG sein, der „Äußerungen von Dritten, die in missbräuchlicher, abstoßender oder irreführender Weise erfolgen", verbietet.[29]

Nach hiesiger Ansicht erhält folgender Beurteilungsansatz insoweit nicht ausreichend Beachtung:

Micro-Influencer:innen sind trotz ihrer „geringen" Reichweite in diesem Sinne ganz „normale" Influencer:innen. Ihr Wesen und ihre Aufgabe ist es, Waren oder Dienstleistungen von Unternehmen zu empfehlen. Die Gefahr der Beeinflussung, die den Schutzzweck des § 11 Abs. 1 S. 1 Nr. 2 HWG begründet, steckt bereits im Namen des/der Botschafter:in: Influencer (= „Beeinflusser").[30] Aufgrund der Bindung, die viele Follower:innen zu „ihren" Influencer:innen aufbauen, ist eine Beeinflussung durch Influencer:innen generell bedeutend wahrscheinlicher als die Beeinflussung durch einen meist distanzierteren klassischen Prominenten. Micro-Influencer:innen sind obendrein in ihrem Tun meist engagierter. Sie streben regelmäßig eifriger an, eine höhere Reichweite zu generieren und legen zu diesem Zweck einen größeren Fokus auf einen stetigen persönlichen Aus-

25 www.de.statistics.de, https://de.statista.com/statistik/daten/studie/1247300/umfrage/influencer-nach-anzahl-der-instagram-follower-weltweit/, Stand: 19.8.2022.
26 *Janning/Mäder/Hebbinghaus*, PharmaR 2021, 49, 50.
27 OLG Nürnberg, Urt. v. 10.9.2013 – 3 U 1071/13 m. w. N.
28 Siehe Fn. 25.
29 *Janning/Mäder/Hebbinghaus*, PharmaR 2021, 49, 51.
30 *Fritzsche,* in: Spickhoff, HWG, § 11 Rn. 9.

tausch mit ihrer Follower:innenschaft. Dadurch werden sie noch nahbarer. Micro-Influencer:innen können also, obwohl sie weniger Leute erreichen und weniger „bekannt" sind, diese „wenigen" Leute im Sinne des § 11 Abs. 1 S. 1 Nr. 2 HWG eher zum Arzneimittelverbrauch anregen.[31] Dadurch wird angenommen werden dürfen, dass Micro-Influencer:innen von ihren Follower:innen das größtmögliche Vertrauen einer noch immer fremden Person entgegengebracht wird und sie dem Stellenwert eines/einer guten Freund:in im Digitalisierungszeitalter sehr nah kommen.

8.2.5.3 Der Rezipient

Influencer:innen erreichen überwiegend meist junge, „[für Werbung] längst verloren geglaubte […] Jugendliche oder Menschen, die kein Fernsehen mehr schauen"[32] und an „Stories" als Dauerwerbesendungen gewöhnt sind. Die Angabe am Seitenrand des Bildschirms, dass gerade zum Darstellungszeitpunkt eine Kooperation mit einem Unternehmen stattfindet oder sogar der klare Hinweis „Werbung", bewirken überwiegend nicht, dass das Vertrauen, welches eine Followerschaft in „ihren" Influencer hat, gemindert wird. Die vermeintliche Authentizität provoziert vielmehr weiterhin, dass jede Influencer:innen-Werbung als Empfehlung eines/einer guten Freund:in interpretiert wird, der/die dem Rezipienten „nur Gutes" wolle. Rezipienten vergessen oder registrieren schlichtweg nicht, dass der/die Influencer:in eigene wirtschaftliche Interessen zum Zeitpunkt des Postens verfolgt.[33]

Aber gerade bei einer so intendierten Medikamentenwerbung ist maßgebend, den tatsächlichen Rezipientenkreis neu zu bewerten. Arzneimittelwerbung richtet sich vorwiegend an Verbraucher:innen, die höchstwahrscheinlich erkrankt sind. Sie sind daher anfälliger für hoffnungsweckende Werbebotschaften und mithin schutzbedürftiger. Ein Kaufwunsch, der durch die Botschaft, dass beispielsweise ein neues Wundermittel gegen die Hautkrankheit Akne gefunden wurde, hervorgerufen werden kann, wird durch das große Vorbild als Botschafter:in erheblich verstärkt. Grund dafür ist die Art und Weise, Produktanpreisung im privaten Alltag zu inszenieren. Fälle, in denen ein:e Influencer:in über die Social-Media-Auftritte des Unternehmens oder des konkreten Produkts wirbt, sollten u. U. anders zu beurteilen

31 *Kieu*, T.A. (2022). Consumer Engagement in Online Product Reviews: A Win-Win for Firms and Micro-Influencers: An Abstract. In: Allen, J., Jochims, B., Wu, S. (eds) Celebrating the Past and Future of Marketing and Discovery with Social Impact. AMSAC-WC 2021. Developments in Marketing Science: Proceedings of the Academy of Marketing Science. Springer, Cham. https://doi.org/10.1007/978-3-030-95346-1_115.

32 *Kost/Seeger*, Influencer Marketing, S. 13 m. w. N. („Wenzel 2017").

33 www.omsels.info OKUWG, HWG Nr. 11, 3., https://www.omsels.info/die-verbote-oder-was-darf-ich-nicht/2-heilmittelwerbegesetz/11-hwg-werbung-ausserhalb-der-fachkreise/nr-11-aeusserungen-dritter, Stand: 15.8.2022.

sein. Denn für die Beurteilung, ob Influencer:innen als Prominente im Sinne des § 11 Abs. 1 S. 1 Nr. 2 HWG anzuerkennen sind, darf nicht verkannt werden, dass das Influencer Marketing wirtschaftlich und gesellschaftlich einen erheblichen Stellenwert hat.

8.3 Fazit

Das vergleichsweise neue Werbephänomen zeigt ziemlich deutlich, dass die Rechtsordnung regelmäßig eine gewisse Zeitspanne vergehen lässt, bevor sie dort auf gesellschaftliche Entwicklungen reagiert, wo sie Regelungsbedürfnisse sieht.[34] Konkrete Regelungen für Influencer Marketing im Heilmittelwerbegesetz sind jedoch allemal überfällig, denn die allgemeinen Kennzeichnungspflichten sind schlicht unzureichend, wenn Heilmittel beworben werden. Dass ein:e Influencer:in trotz Vorliegen aller Tatbestandsmerkmale des § 11 Abs. 1 S. 1 Nr. 2 HWG zukünftig lediglich als Prominente:r in diesem Sinne eingestuft und mithin Influencer Marketing für OTC-Medikamente gänzlich unzulässig wird, ist aufgrund des Stellenwertes des Geschäftsmodells nur schwer vorstellbar.

In Hinblick auf influencer:innen-spezifische Regelungen sollte an den Regulierenden appelliert werden, tatsächlich realistisch beide Betroffenen zu berücksichtigen. Besondere Beachtung sollten die vermutlich erkrankten Rezipienten einerseits und die durch Rechtsunsicherheit eingeschränkten Kooperationspartner:innen andererseits erhalten. Gerade weil sich in den letzten Jahren gezeigt hat, dass Influencer Marketing nunmehr als beliebtes Werbeformat etabliert ist und ebendies nach den „Influencer I-III"-Urteilen des BGH gleichermaßen von der Justiz zur Kenntnis genommen wurde, ist es höchste Zeit in Sachen Rechtssicherheit zu kooperieren.

34 *Schladebach*, ZdiW 2022, 168, 172 VII.

9 Umsetzung der Betroffenenrechte der DSGVO im eSports

*Conrad S. Conrad**

Mit den sog. Betroffenenrechten aus dem europäischen Datenschutzrecht (Kapitel III der DSGVO) haben sich hierzulande nicht nur die „datenhungrigen" Unternehmen, sondern auch zunehmend die Gerichte zu befassen. Diese Situation resultiert unter anderem aus den Auskunfts- und Löschbegehren von betroffenen Personen, die in vielfältigen Konstellationen auftreten und dem Verantwortlichen in der Praxis wegen einiger Unklarheiten und angesichts komplexer Vorgänge – insbesondere im digitalen Bereich – große Schwierigkeiten bereiten können.

In der Gaming-Szene (allen voran dem eSports), die seit jeher von umfangreichen Verarbeitungsprozessen von personenbezogenen Daten der Spieler:innen geprägt ist, scheint dieses Thema (noch) nicht präsent zu sein. Dabei stellen sich gerade hier sehr spannende Fragen: Welche personenbezogenen Daten wären von einem Anspruch auf Auskunft und/oder Kopie nach Art. 15 Abs. 1, Abs. 3 DSGVO erfasst? Lassen sich Erfolge aus einem Account nach dem Recht auf Datenübertragbarkeit gem. Art. 20 DSGVO in einen neuen Account übermitteln? Und können Spieler:innen mithilfe eines Löschersuchens nach Art. 17 Abs. 1 DSGVO einzelne Ergebnisse/Turniere beeinflussen, indem sie einzelne Partien oder Datenverarbeitungvorgänge löschen (lassen)?

9.1 Anwendungsbereich der DSGVO

Eine Verarbeitung personenbezogener Daten im Sinne von Art. 4 Nr. 2 DSGVO dürfte im eSports immer dann anzunehmen sein, wenn Spieler:innen einen Gaming Account bzw. ein Profil mit zahlreichen Angaben zur eigenen Person und/oder des gespielten Charakters eigenständig einrichten und mit einem Endgerät die entsprechende Software (das Game) benutzen, darüber auf externen Servern diverse Interaktionen ausführen und ggfs. mit anderen Spieler:innen über diese Anwendung kommunizieren. Auch können diese Profile mit weiteren Plattformen oder Drittdiensten verknüpft werden. Eine entsprechende Verarbeitung personenbezogener Daten durch die Serverbetreiber, den Publisher/Spieleanbieter und auch sonstigen zugehörigen Webseiten bzw. Portalen (Communitys, Ligen o. ä.) im Internet liegt daher unbestritten vor.

---

* Mehr über den Autor erfahren Sie im Autor*innenhinweis auf S. 224 ff.

Spannender ist die Frage, welche Information hierbei als personenbezogenes Datum im Sinne von Art. 4 Nr. 1 DSGVO gilt. Denn neben dem Vor- und Nachnamen, einer E-Mail-Adresse bzw. den typischen Accountdaten, der (persönlichen) IP-Adresse beim Abruf von Webseiten und Servern im Internet oder Zahlungsdaten bei In-App- bzw. In-Game-Käufen könnte diskutiert werden, ob auch spielbezogene Statistiken (Frags, Siege, Erfolge, Level uvm.) oder gar die eigenen Spielzüge, z. B. auf einer Map, als ein personenbezogenes Datum gelten. Letzteres wären individuelle, einzigartige Bewegungen und Handlungen von Spielcharakteren auf einem virtuellen Spielfeld, die bei diversen Spielen aus der eSports-Szene aufgezeichnet werden können (sog. Demos oder Replays) und sogar die Taktik im Spiel erkennen lassen. Diese Fragestellung wäre insbesondere für das Recht auf Kopie nach Art. 15 Abs. 3 DSGVO von enormer Relevanz, müssten all diese Daten dann ggfs. als solche an die betroffene Person herausgegeben werden.

Des Weiteren wären die jeweiligen Akteure im Gaming-Bereich, z. B. die Publisher, Hersteller, Ligabetreiber, Serverbetreiber und weitere technische Dienstleister (z. B. twitch) nach Maßgabe der Rollen der DSGVO voneinander datenschutzrechtlich abzugrenzen.[1] Daher wäre zu prüfen, welches Unternehmen bzw. welcher Akteur als datenschutzrechtlich Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO gilt, d. h. *„allein oder gemeinsam über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.* Hingegen können zahlreiche involvierte Dienstleister als Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO in Betracht kommen, wenn sie personenbezogene Daten im Auftrag des Verantwortlichen weisungsgebunden verarbeiten. Daraus ergibt sich für die jeweiligen Stellen das Erfordernis, entsprechende datenschutzrechtliche Vereinbarungen zu schließen. Allen voran wäre bei ausschließlich weisungsgebundener Tätigkeit ein Vertrag über die Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO zu schließen oder – wenn mehrere Stellen über Verarbeitungszwecke und -mittel entscheiden, eine Vereinbarung über die gemeinsame Verantwortlichkeit nach Art. 26 Abs. 1 DSGVO mit der Regelung der einzelnen Pflichten und Aufgaben. Bei Dienstleistern außerhalb der EU bzw. des EWR müssten ggfs. zusätzliche Vereinbarungen (die aktuell geltenden Standarddatenschutzklauseln der EU-Kommission vom 4.6.2021[2]) vereinbart werden.

1 Mehr hierzu: EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.0, 7. Juli 2021; https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_de.pdf.

2 https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=de.

9.2 Die Betroffenenrechte

Die Rechte der von Datenverarbeitungen betroffenen Personen sind im dritten Kapitel der DSGVO in den Art. 12 ff. DSGVO geregelt und nehmen eine wichtige Funktion im europäischen Datenschutzrecht ein, geben sie doch der betroffenen Person ein eigenes Steuerungsinstrument. Diese kann unter anderem vom Verantwortlichen Auskunft über die sie betreffende Datenverarbeitung, eine Kopie der verarbeiteten Daten (Art. 15 Abs. 1, Abs. 3 DSGVO) oder die Löschung personenbezogener Daten verlangen (Art. 17 Abs. 1 DSGVO), aber auch Widerspruch gegen die Datenverarbeitung einlegen (Art. 21 DSGVO).

Die Betroffenenrechte sind grundsätzlich binnen eines Monats von der Stelle, die für die Datenverarbeitung gem. Art. 4 Nr. 7 DSGVO verantwortlich ist, zu prüfen und ggfs. dann je nach Situation auch umzusetzen. Bei komplexen oder einer hohen Anzahl an Anfragen wäre eine Verlängerung der Frist um zwei weitere Monate gem. Art. 12 Abs. 3 S. 2 DSGVO möglich; allerdings trifft den Verantwortlichen für die Begründung dieser Ausnahmesituation die Beweislast sowie die Mitteilungspflicht (Art. 5 Abs. 2, Art. 12 Abs. 3 S. 3 DSGVO). Im Übrigen müssen auch die weiteren Anforderungen und Ausnahmen bei der Bearbeitung geltend gemachter Betroffenenrechte nach Art. 12 DSGVO durch den Verantwortlichen beachtet werden (z. B. die Unentgeltlichkeit der Erfüllung nach Art. 12 Abs. 5 S. 1 DSGVO).

9.3 Besonderheiten im Gaming (eSports)

Bei der Prüfung und Umsetzung der Betroffenenrechte bestehen diverse Besonderheiten im Einzelfall, auf die Unternehmen vorbereitet sein sollten.

9.3.1 Praktische Schwierigkeiten im Allgemeinen

Denn bereits allgemein können die Erkennung eines geltend gemachten Anspruchs und folglich die interne Prüfung (Koordination) der Anfrage einem Verantwortlichen erhebliche Schwierigkeiten bereiten, z. B. aufgrund fehlender Sensibilisierung bzw. Awareness bei den Beschäftigten sowie fehlender internen Bearbeitungs- und Dokumentationsprozesse. Je nach Geschäftsmodell sollten grundsätzlich alle Beschäftigten mit etwaigem Kundenkontakt und an zentralen Stellen datenschutzrechtlich geschult worden sein, damit Ansprüche aus den Betroffenenrechten als solche identifiziert und an die interne Koordination oder eine andere Stelle unverzüglich weitergeleitet werden.

Auch die Reihenfolge der Bearbeitung von Betroffenenanfragen gilt es zu beachten, sodass bei der parallelen Geltendmachung mehrerer, sich teils

überschneidender Ansprüche (z. B. die gleichzeitige Geltendmachung von Auskunft nach Art. 15 Abs. 1 DSGVO und Löschung nach Art. 17 Abs. 1 DSGVO) das Anliegen zufriedenstellend und datenschutzkonform umgesetzt wird. Im konkreten Fall wäre regelmäßig zunächst die Auskunft nach Art. 15 Abs. 1 DSGVO zu erteilen und anschließend die etwaige Löschung gem. Art. 17 Abs. 1 DSGVO vorzubereiten bzw. umzusetzen. Bei der Abwicklung in umgekehrter Reihenfolge würde der Anspruch auf Auskunft schlussendlich ins Leere laufen, wenn kurz zuvor sämtliche personenbezogene Daten zur Person gelöscht worden sind.

Doch auch die Reichweite der Auskunft nach Art. 15 DSGVO löst für datenschutzrechtlich Verantwortliche nach wie vor und trotz der bestehenden BGH-Rechtsprechung,[3] in der ein weiter Anwendungsbereich bestätigt wurde, in der Umsetzung Probleme aus. Oftmals ist unklar, welche Daten konkret von dem Regelungsgehalt in Art. 15 Abs. 1 und Abs. 3 DSGVO erfasst sind[4] und inwiefern der Anspruch auf eine (erste) unentgeltliche Kopie beschränkt werden kann.[5] Fraglich ist deshalb, ob im Wege einer abgestuften Beauskunftung zunächst nur die Information über Kategorien der personenbezogenen Daten oder lediglich Stammdaten mitgeteilt werden können – oder aber ob sämtliche Daten erfasst werden müssen, die zu/über die betroffene Person verarbeitet werden.[6]

Zuletzt wird oftmals vergessen, dass eine Betroffenenanfrage und die damit einhergehende Prüfung bzw. Beantwortung eine eigenständige Verarbeitung personenbezogener Daten nach Art. 4 Nr. 2 DSGVO darstellt und somit (neue) Informationspflichten aus Art. 13 DSGVO begründet, die sodann bei der Datenverarbeitung der anfragenden Person mitzuteilen sind. Dies könnte durch die Übersendung der Datenschutzhinweise bei einer Eingangsbestätigung des Anspruchs oder spätestens bei Mitteilung der Antwort an die betroffene Person erfolgen. Sodann gelten diesbezüglich die allgemeinen Anforderungen aus Art. 12 ff. DSGVO; weswegen diese Datenschutzhinweise in verständlicher Sprache ergehen sowie umfassend und korrekt sein müssen. Diese wären im Zweifel an die Sprache und das Verständnis der betroffenen Person anzupassen, insbesondere bei minderjährigen Personen.[7]

Abschließend ist angesichts der Nachweispflicht des Verantwortlichen (im Sinne der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO) die Dokumentati-

3 BGH, Urt. v. 15.6.2021 – Az.: VI ZR 576/19.

4 Vgl. EDSA Guidelines 01/2022 vom 18. Januar 2022, https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf.

5 Vgl. hierzu auch den Vorlagebeschluss des BGH, Beschl. vom 29.3.2022 – Az.: IV ZR 1352/20.

6 Zu den Grenzen des Auskunftsanspruchs vgl. BGH, Urt. v. 15.6.2021 – Az.: VI ZR 576/19; einschränkend FG München, Urt. v. 5.5.2022 – Az.: 15 K 193/20.

7 Vgl. ErwG. 60 S. 2.

on des gesamten Vorgangs zu gewährleisten und selbige an einem gesicherten Ort für drei Jahre vorzuhalten – und anschließend zu löschen.

9.3.2 Praktische Schwierigkeiten aus der speziellen Situation im eSports

Im eSports ergeben sich weitere Schwierigkeiten: Im ersten Schritt stellt sich die bereits oben aufgeworfene Frage zu der datenschutzrechtlichen Verantwortlichkeit im Sinne von Art. 4 Nr. 7 DSGVO für die stattfindenden Datenverarbeitungen. Die Problematik tritt zutage, wenn der Anspruch aus den Betroffenenrechten z. B. an einen Auftragsverarbeiter nach Art. 28 DSGVO oder gemeinsamen Verantwortlichen nach Art. 26 DSGVO gerichtet wird. Es wäre daher vorab zu bestimmen, welche datenschutzrechtliche Rolle z. B. ein Ligabetreiber, der Serverhoster, ein Publisher oder ein Clan im Hinblick auf die Datenverarbeitung der Spieler:innen einnimmt. Sodann wären entsprechende Verträge (z. B. nach Art. 28 DSGVO) abzuschließen, in denen der Umgang mit derartigen Anfragen für jeden Beteiligten geregelt wird.

Bislang ungeklärt und daher der Einzelfallentscheidung des zuständigen Verantwortlichen überlassen ist die Situation der Wahrnehmung der Betroffenenrechte durch Eltern bei Kindern. Die Eltern-Kind-Konstellation dürfte bei bestimmten Games nicht ganz unwahrscheinlich sein, da viele Spiele vor allem bei Kindern und Jugendlichen beliebt sind. Hier wäre es durchaus denkbar, dass die Eltern im Rahmen des Auskunfts- und Kopieanspruchs nach Art. 15 Abs. 1 und Abs. 3 DSGVO in Erfahrung bringen wollen, welche personenbezogene Daten der Publisher bzw. der Betreiber über das eigene Kind[8] verarbeitet, z. B. auch um die Spielzeiten auszuwerten und ggfs. sogar Ansprüche gegenüber den Betreiber zu prüfen. Letzteres könnte ggfs. sogar als rechtsmissbräuchlich erachtet werden, wenn andere Ziele (der Eltern) verfolgt werden.

Ferner könnte ein Szenario dahingehend bestehen, dass die Prüfung der Identität der betroffenen Person (um eine Auskunft an die falsche Person zu vermeiden) die Übersendung einer Ausweiskopie erfordert, wenn nur Accountdaten bekannt sind (bei mehreren Spieler:innen) oder die Identität nicht auf andere Wege bestätigt werden könnte. Jedoch sollte hiervon nur in Ausnahmefällen Gebrauch gemacht werden (vgl. Art. 12 Abs. 1 S. 1 DSGVO). Zudem sind dann die personenbezogenen Daten, die nicht für die Prüfung der Identifikation der Person erforderlich sind, nach dem Grundsatz der Datenminierung aus Art. 5 Abs. 1 lit. c DSGVO unkenntlich zu machen und nach Feststellung der Person wieder zu löschen.

8 Vgl. hierzu BGH Urt. v. 28.1.2015 – Az.: XII ZR 201/13.

Für viel Diskussion sorgt die Prüfung der etwaigen Annahme des unverhältnismäßigen Aufwands bei der Umsetzung des Betroffenenrechts, allen voran bei der Beauskunftung nach Art. 15 Abs. 1 oder Abs. 3 DSGVO.[9] Hier könnten Sever-Logfiles oder Spielzüge einen immensen Umfang an Daten einnehmen und unter Umständen einen unverhältnismäßigen Aufwand seitens des Verantwortlichen nahelegen. Auch Mehrfach- bzw. exzessive Anfragen wären im Hinblick auf den sich daraus ergebenen Aufwand zu bewerten und könnten sogar Verweigerungsgründe im Hinblick auf die Bearbeitung des Anspruchs hervorrufen (vgl. Art. 12 Abs. 5 DSGVO).

Zuletzt stellt sich die Frage, wie eine angemessene Sicherheit für die personenbezogenen Daten bei der Übermittlung der Antwort, beispielsweise bei der Kopie nach Art. 15 Abs. 3 DSGVO zu gewährleisten ist. Diesbezüglich könnte die Übermittlung der Daten per E-Mail-Versand vorgenommen oder der Download der Daten aus einem Account bereitgestellt werden. Die Zusendung per Briefpost dürfte hingegen meistens ausscheiden, da zum einen die Adressdaten unbekannt sind und zum anderen der Verantwortliche ggfs. im Ausland sitzt. Zudem ist anzunehmen, dass viele Betroffene den Antrag elektronisch geltend machen. In diesem Fall ist der Verantwortliche i. d. R. dazu aufgefordert, auch elektronisch zu antworten (Art. 12 Abs. 3 S. 4 DSGVO). Einen zwingenden Verweis auf die Übermittlung der Daten via Briefpost an die Wohnadresse sieht die DSGVO vor dem Hintergrund der Regelung in Art. 12 Abs. 3 S. 4 DSGVO auch gar nicht vor.

9.4 Fallbeispiele

Anhand einiger ausgewählter Fallbeispiele soll im Folgenden die Geltendmachung einiger der datenschutzrechtlichen Betroffenenrechte im eSports besprochen werden.

9.4.1 Auskunft und Kopie nach Art. 15 Abs. 1 und 3 DSGVO

Vermutlich der naheliegendste Fall aus den Betroffenenrechten wäre der Anspruch auf Auskunft, respektive auf Erhalt einer Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind (Art. 15 Abs. 1 bzw. 3

9 Der Wortlaut von Art. 15 DSGVO sieht eine „Verhältnismäßigkeitsprüfung" nicht vor (anders als in Art. 14 Abs. 5 lit. b) DSGVO oder § 34 Abs. 1 BDSG), aber die Rechtsprechung geht hierauf teilweise ein, Vgl. AG Pankow, Urt. v. 28.3.2022 – Az.: 4 C 199/21; vgl. auch nach altem Recht: LG Heidelberg, Urt. v. 6.2.2020 – Az.: 4 O 6/19; a. A. OLG Stuttgart, Urt. v. 17.6.2021 – Az.: 7 U 325/20; Vgl. auch *König*, CR 2019, 295, 300; *Dix*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO, 1. Auflage 2019, Art. 15 Rn. 36.

DSGVO).[10] So könnten sich beispielsweise die Spieler:innen hiermit gegen den Publisher richten.

Im ersten Schritt sollte klar ersichtlich sein, wer überhaupt Verantwortlicher für die Datenverarbeitung ist, d. h. auf welchen Prozess sich der Antrag bezieht, denn bekanntlich sind die Betroffenenrechte nur von der für die Datenverarbeitung verantwortlichen Stelle umzusetzen. Dementsprechend gilt es für die unterschiedlichen Unternehmen und Akteure, sich ihrer jeweiligen datenschutzrechtlichen Rolle bewusst zu sein, die betroffene Person bereits bei Datenerhebung über die verantwortliche Stelle zu informieren und demnach entweder die Anfrage an den Verantwortlichen (im Falle einer Auftragsverarbeitung mit selbigen nach Art. 28 DSGVO) weiterzuleiten, oder ggfs. selbst zu beantworten, sofern eine eigene oder eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO besteht. Diese Einschätzung erfordert sowohl das Verständnis der Vertragslage als auch die Kenntnis der tatsächlichen Datenflüsse bzw. Datenverarbeitungsvorgänge.

Große Anstrengungen dürften bei der Bestimmung des Umfangs bzw. des Inhalts einer angeforderten „Kopie" zu unternehmen sein. Welche personenbezogenen Daten wären von diesem Anspruch umfasst? Diese Problematik gilt insbesondere bei Logfiles, Hintergrunddaten oder auch spielbezogenen Daten (Spielzügen?), die an verschiedenen Stellen in umfangreichen Maße verarbeitet werden und ggfs. gar nicht herauszufiltern sind.[11]

Sodann wären auch die etwaigen „Verweigerungsgründe" zu prüfen. Denn besteht die Unmöglichkeit der Umsetzung mangels Identifizierbarkeit der Person (vgl. Art. 12 Abs. 2 S. 2 DSGVO) oder ein unverhältnismäßiger Aufwand, könnte sich der Verantwortliche unter Umständen im Rahmen einer eigenen Risikoeinschätzung auf diese Ausnahme berufen und von einer Beantwortung absehen. Die Unverhältnismäßigkeit könnte sich ggfs. aus immensen Datenmengen (bei jahrelanger Spielzeit) und komplexen Datenbanken ergeben.[12] Die Verweigerung wäre auch bei offenkundig unbegründeten oder exzessiven Anträgen zu überlegen (Art. 12 Abs. 5 S. 2 lit. b DSGVO), was diskutiert werden könnte bei Anfragen durch die Eltern/den Clan oder einer Häufung des gleichgelagerten Anskunftsverlangen (z. B. wenn die Spieler:innen mehrmals während eines Wettbewerbs diesen Anspruch geltend machen).

Zudem darf gem. Art. 15 Abs. 4 DSGVO das *„Recht auf Erhalt einer Kopie [..] die Rechte und Freiheiten anderer Personen nicht beeinträchtigen"*.

---

10 Siehe hierzu, *Engeler/Quiel*, NJW 2019, 2201, 2201ff; *Lembke/Fischels*, NZA 2022, 513, 513ff; *Brink/Joos*, ZD 2019, 483, 483 ff.

11 Vgl. BGH, Urt. v. 15.6.2021 – Az.: VI ZR 576/19.

12 Vgl. *Frank*, in: Gola, DSGVO, 2. Auflage 2018, Art. 15 Rn. 38ff; Siehe hierzu auch Fußnote 9.

Im Rahmen einer dann vorzunehmenden Interessenabwägung[13] wären die Rechte und Freiheiten anderer Personen, z. B. anderer (Mit-)Spieler:innen zu berücksichtigen, die bei den Matches bzw. auf dem Server ebenfalls anwesend waren und an verschiedenen Stellen von der Datenverarbeitung betroffen sind. So könnten diese z. B. im In Game Chat/Voice Chat in Erscheinung getreten sein und bei der Herausgabe der Kopie derart umfassend in ihren Rechten berührt werden, sodass die sie betreffenden Daten möglicherweise zu entfernen oder unkenntlich zu machen wären, was eine aufwendige Filterung und Bearbeitung der Daten erfordern kann. Und bei einer Übertragung von einem Turnier per Live-Stream oder per Twitch[14] könnten sogar Zuschauer:innen oder Moderator:innen gefimt worden sein.

Sofern sich die betroffene Person – und sei es aus anderen Gründen – zum Zeitpunkt des Antrags in einem Gerichtsverfahren mit dem Verantwortlichen befindet, sollte die Rechtsmissbräuchlichkeit des Anspruchs geprüft werden, z. B. wenn der betroffenen Person die Daten bereits bekannt sind oder selbige aus sonstigen Gründen kein schutzwürdiges Interesse vortragen kann, beispielsweise wenn der Anspruch das eigentliche Ziel verfolgt, Informationen über die Gegner:innen herauszufinden oder die eigene Vergütung zu verbessern.[15]

Im Falle der Umsetzung des Anspruchs auf Kopie nach Art. 15 Abs. 3 DSGVO hat der Verantwortliche (wie bei allen anderen Betroffenenrechten auch) weitere Anforderungen zu erfüllen, die von einer fristgerechten Antwort (ggfs. nach Verlängerung der Frist um zwei weitere Monate bei komplexen Anfragen) bis hin zur Information über die Datenverarbeitung nach Art. 13 DSGVO in der korrekten Sprache reichen – all jenes setzt die direkte Kommunikation mit der betroffenen Person voraus. Auch die geeignete Übermittlung der Antwort, z. B. als Download im Account oder aber per E-Mail oder Briefpost spielt eine Rolle wie auch deren Lesbarkeit. Die entsprechende Dokumentation der gesamten Korrespondenz für drei Jahre (Art. 5 Abs. 2 DSGVO) schließt diesen Vorgang ab.

9.4.2 Löschung aller Daten nach Art. 17 Abs. 1 DSGVO

Das Recht auf Löschung nach Art. 17 Abs. 1 DSGVO stellt Unternehmen ohnehin vor große Schwierigkeiten, dürfte aber im Bereich des Gamings

13 Vgl. BGH, Urt. v. 22.2.2022 – Az.: VI ZR 14/21.

14 Ein bekanntes Live-Streaming Portal mit Chat-Funktionen für Zuschauer:innen und Profilen.

15 Vgl. LG Kassel, Urt. v. 5.7.22 – Az.: 5 O 1954/21; LG Frankenthal, Urt. v. 12.1.2021 – Az.: 1 HK O 4/19; LG Krefeld, Urt. v. 6.10.2021 – Az.: 2 O 448/20; OLG Hamm, Beschl. v. 15.11.2021 – Az.: 20 U 269/21; LG Wuppertal, Urt. v. 29.7.2021 – Az.: 4 O 409/20.

noch zusätzlich für Brisanz sorgen. Dies lässt sich mit dem Szenario veranschaulichen, dass Spieler:innen von bestimmten Akteuren des eSports die Löschung bestimmter oder gar sämtlicher personenbezogener Daten gem. Art. 17 Abs. 1 DSGVO verlangt.[16]

Sofern sich der Anspruch an den für die Datenverarbeitung Verantwortlichen gem. Art. 4 Nr. 7 DSGVO richtet, müsste dieser die Voraussetzungen aus Art. 17 Abs. 1 DSGVO prüfen und ggfs. dem Löschgesuch nachkommen.

So wäre zu prüfen, ob die betroffene Person überhaupt einen Anspruch auf Löschung gem. Art. 17 Abs. 1 DSGVO hat. Dieser könnte sich ergeben, sofern die personenbezogenen Daten für die Zweck, für die sie erhoben oder auf sonstiger Weise verarbeitet wurden, nicht mehr notwendig sind (Art. 17 Abs. 1 lit. a DSGVO). Liegt hier jedoch gerade mit der Datenverarbeitung, beispielsweise im Rahmen einer Liga oder eines Wettbewerbs der Zweck in der auf Dauer angelegten Verarbeitung und beweissicheren Dokumentation der Ergebnisse, wäre der Zweck offenkundig nicht entfallen. Insbesondere bei Turnieren mit hohen Preisgeldern oder weltweiten Rankings, aus denen sich lizenzierte Meisterschaften oder Titel ergeben, dürfte die Datenverarbeitung zur Erfassung der Ergebnisse weiterhin notwendig sein und auf eine dauerhafte Darstellung/Nutzung während der fortlaufenden Existenz dieses Wettbewerbs abzielen – oder aber ein neuer Zweck (nach Zweckänderung) wie z. B. die Archivierung der Datenverarbeitung bestehen.[17] Aber auch der Widerruf der Einwilligung gem. Art. 17 Abs. 1 lit. b DSGVO dürfte nicht in Betracht kommen, wenn die Datenverarbeitung aus Gründen der Rechssicherheit auf Basis eines geschlossenen Vertrags (z. B. Teilnahmevertrag/Teilnahmebedingungen, Spieler:innenvertrag oder Lizenzvertrag) eines Veranstalters erfolgt und nicht auf die Einwilligung gestützt wird.[18] Daneben wäre eine Löschung nach Widerspruch im Sinne von Art. 21 Abs. 1 DSGVO denkbar, sofern die Datenverarbeitung nicht auf einen Vertrag, sondern auf das berechtigte Interesse nach Art. 6 Abs. 1 S. 1 lit. f DSGVO gestützt wurde,[19] wie es vielleicht bei Fotoaufnahmen auf Events oder bestimmten Auswertungen der Spiele/Ergebnisse der Fall sein mag. Eine unrechtmäßige Datenverarbeitung als Löschgrund (Art. 17 Abs. 1 lit. d DSGVO) dürfte hingegen nicht vorliegen, sofern der Veranstalter oder der Publisher/Hersteller des Spiels die Rechtmäßigkeit der Datenverarbeitung auf Basis eines Vertrages oder den Nutzungsbedingungen beweisen kann. Im Ergebnis dürfte

16 Vgl. hierzu grundsätzlich: BGH, Urt. v. 3.5.2022 – Az.: VI ZR 832/20.

17 Vgl. *Herbst*, in: Kühling/Buchner, DS-GVO, Art. 17 Rn. 21 ff.; *Kamann/Braun*, in: Ehmann/Selmayr, DS-GVO, Art. 17 Rn. 22.

18 Vgl. hierzu: https://e-sportrecht.de/kinder-und-jugendliche-im-e-sport/.

19 Vgl. Zum Anspruch auf Löschung gegenüber der SCHUFA und deren berechtigtes Interesse: OLG Köln, Urt. v. 27.1.2022 – Az.: 15 U 153/21.

in den meisten Fällen deshalb wohl – zumindest während der aktiven Teilnahme/Nutzung des Games durch die Spieler:innen – kein Anspruch auf Löschung nach Art. 17 Abs. 1 DSGVO gegeben sein.

Sofern die Anspruchsvoraussetzungen zunächst doch erfüllt sein sollten, wäre zu prüfen, auf welche personenbezogenen Daten (und ggfs. welchen Zeitraum) sich das Löschgesuch der Spieler:innen konkret bezieht. Maßgeblich sollte daher bei komplexen Vorgängen die Präzisierung des Anliegens durch die betroffene Person sein. Auf dieser Ebene kann es einen Unterschied ausmachen, ob nur die Löschung einer bestimmten Datenverarbeitung, also beispielsweise nur einer bestimmte Partie oder Bericherstattung über ein Event angestrebt wird oder die Löschung sämtlicher Daten der betroffenen Person erfolgen soll. Im Hinblick auf Turnierspiele und Wettbewerbe dürfte jedoch bereits die Löschung einer Partie zu einer folgenreichen Beeinflussung des Ausgangs eines Wettbewerbs führen, weswegen die Auswirkung der Löschung eines Spieles vergleichbar wäre mit der Löschung aller Daten.

Nichtdestotrotz kann der Verantwortliche unter Umständen auch „Versagungsgründe" nach Art. 17 Abs. 3 DSGVO vortragen. Denn der Anspruch auf Löschung gem. Art. 17 Abs. 1 DSGVO (wie im Übrigen auch nach Abs. 2) gilt nicht, sofern die gegenständliche Datenverarbeitung beispielsweise zur Ausübung der Meinungsfreiheit und Informationsfreiheit[20] (Art. 17 Abs. 3 lit. a DSGVO) oder zur Erfüllung einer rechtlichen Verpflichtung (Art. 17 Abs. 3 lit. b DSGVO) erforderlich ist. Denkbar wäre es, dass sich der Verantwortliche – wenn es bspw. um die Berichterstattung zu offiziellen Begegnungen geht – als Teil der Presse oder einem vergleichbaren weltweiten Medium („Community") betrachtet und die Datenverarbeitung, also z. B. die Berichterstattung über ein Event oder Verwendung von Spieldaten für ein Turnier auf diese Ausnahme stützt und bei bedeutenden Wettkämpfen diese Daten als primäre Informationsquelle der Welt zur Verfügung stellt.[21] Und auch eine rechtliche Verpflichtung zur einzelnen Datenverarbeitungen könnte sich bei Preisgeldern und Turnieren ergeben, wenn diese Daten aus zivil- und steuerrechtlichen Gründen aufzubewahren sind,[22] z. B. als Nachweis der Spielberechtigung bzw. der Teilnahme an dem Turnier unter Einhaltung der geltenden Regeln, woraus sich die Vergütung der Spieler:innen, etwaige Nebenkostenabrechnungen (Reisekosten) und auch die Auszahlung von Preisgeldern/Gewinnen ergeben – aber auch Ansprüche von Sponsoren/Li-

20 Vgl. BGH, Urt. v. 3.5.2022 – Az.: VI ZR 832/20.

21 Zu den Voraussetzungen eines Anspruchs auf Löschung im Hinblick auf das Medienprivileg vgl. auch BGH, Urt. v. 15.2.2022 – Az.: VI ZR 692/20 (Arztsuche- und Bewertungsportal); vgl. auch *Schaub*, GRUR 2022, 465, 466 ff.

22 Vgl. *Weichert*, DuD 2021, 755, 757.

zenzgebern.[23] Zudem könnte die Datenverarbeitung im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke („Ewige-Tabelle“) betreffen (Art. 17 Abs. 3 lit. d DSGVO) und wäre daher von der Löschung ausgenommen, was allerdings nur bei herausragenden Meisterschaften („olympische Spiele“) anzunehmen sein dürfte. Zuletzt wäre zu prüfen, ob die Datenverarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist, wenn konkrete Anzeichen bestehen, dass eine Manipultation und rechtliche Auseinandersetzungen der Ergebnisse in Wettbewerben vorliegen und daher ein Rechtstreit droht (Art. 17 Abs. 3 lit. e DSGVO), so dass diese Daten dann auch von dem Löschgesuch ausgenommen wären. Es wäre freilich ein paradoxes Bild, wenn allein die Löschung von bestimmten Daten aus einem Spiel oder einem Turnier zur Beeinflussung der Ergebnisse führen, damit per se (neue) Ansprüche auf Schadensersatz oder Rückforderung von ausgezahlten Leistungen/Preisgeldern begründen und deshalb diese Ausnahmevorschrift greifen würde.

Ferner können auch im Hinblick auf den Löschanspruch aus Art. 17 Abs. 1 und Abs. 2 DSGVO die allgemeinen Verweigerungsgründe aufseiten des Verantwortlichen diskutiert werden, wie beispielsweise die Unmöglichkeit der Umsetzung mangels Identifizierbarkeit der Person oder die Annahme eines offenkundig unbegründeten oder exzessiven Antrags (Art. 12 Abs. 5, Art. 11 Abs. 2 S. 2 DSGVO).

Falls der Anspruch auf Löschung nach Art. 17 Abs. 1 DSGVO grundsätzlich begründet wäre und dem keine Verweigerungsgründe entgegenstünden, muss sich der Verantwortliche bei der Umsetzung des Ersuchens mit weiteren Anforderungen auseinandersetzen. Dies beginnt mit der Wahrung der Frist bzw. der i. d. R. „unverzüglichen“ Umsetzung des Löschgesuchs bis hin zur etwaigen Reichweite des Anspruchs. Schließlich lässt sich diskutieren, ob die betroffenen Daten auch aus Backups und Archiven zu entfernen wären.[24] Zuletzt ist weiterhin unklar, ob und inwiefern die vollzogene Löschung zu beweisen ist, z. B. durch die Erstellung eines Löschprotokolls oder der Existenz eines Löschkonzepts.

Im Übrigen würde auch eine Anonymiserung[25] der Datenverarbeitung keinen Sinn ergeben, wenn aus oben genannten Gründen gerade die Darstellung der Ergebnisse bzw. des Ausgangs von Turnieren, deren Berichterstattung und bisweilen auch die Aufbewahrungspflichten bestehen.

---

23 Einschränkend: Gesetzliche Aufbewahrungspflichten stellen keine Rechtfertigung dar, um nicht rechtmäßig erhobene Daten dauerhaft speichern zu dürfen, so das OLG Dresden, Urt. v. 14.12.2021 – Az.: 4 U 1278/21.

24 Vgl. hierzu die Wertung von § 34 Abs. 1 Nr. 2 lit. b) BDSG bzw. § 35 Abs. 1 BDSG.

25 Vgl. *Roßnagel*, ZD 2021, 188, 191 ff.

9.4.3 Recht auf Datenübertragbarkeit nach Art. 20 DSGVO

Ein kaum bedachtes Szenario ist der Fall, dass Spieler:innen die Übertragung ihrer Daten (in einen neuen Account) wünschen.[26] So wäre im Rahmen des sog. Rechts auf Datenübertragbarkeit aus Art. 20 Abs. 1 DSGVO[27] zu prüfen, welche personenbezogene Daten hiervon überhaupt erfasst wären; denn der Anwendungsbereich umfasst nur solche Daten, die die betroffene Personen „einem Verantwortlichen bereitgestellt hat". Zudem besteht der Anspruch nur sofern die *„Verarbeitung auf einer Einwilligung gemäß Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a oder auf einem Vertrag gemäß Art. 6 Abs. 1 lit. b beruht"* und *„die Verarbeitung mithilfe automatisierter Verfahren erfolgt"*. Diese Voraussetzungen könnten bei einer Datenverarbeitung durch einen Ligabetreiber bzw. bei Wettbewerben erfüllt sein, sofern die Spieler:innen einen Vertrag mit dem Verantwortlichen geschlossen haben und die Datenverarbeitung durch die Teilnahme an diesem Wettbewerb auf Basis eines Vertrags gem. Art 6 Abs. 1 S. 1 lit. b DSGVO beruht (Teilnahmevertrag, Lizenzvertrag u. ä.). Werden personenbezogene Daten der Person nicht auf Basis einer Einwilligung oder eines Vertrags erhoben und automatisiert verarbeitet, können sie nicht Gegenstand des Anspruchs aus Art. 20 Abs. 1 DSGVO sein.

Als eine weitere Hürde dürfte sich die Umsetzung herausstellen: Die betroffene Person soll diese Daten in einem strukturierten, gängigen und maschinenlesbaren Format erhalten, respektive sind die Daten an einen anderen Verantwortlichen zu übermitteln. Schließlich wirft diese Norm auch Fragen nach einer Datenkompatibilität auf, denn nur vergleichbare Systeme bzw. Datenbanken dürften überhaupt die hiermit gewünschte Datenübertragbarkeit erlauben.[28] Sodann wären technische Funktionen (Export/Import) zu fordern, um dem Anspruch aus Art. 20 Abs. 1 DSGVO gerecht zu werden. Dahingehend könnten sich die angesprochenen Verantwortlichen damit verteidigen, dass eine solche Systemkompatibilität derzeit nicht vorläge oder diese Funktionen nicht bestünden. Bei selbstentwickelten Plattformen spricht viel für dieses Argument, auch wenn mittlerweile derartige Funktionen aus dem Grundsatz von privacy by design (Art. 25 Abs. 1 DSGVO) mittelbar zu fordern sein dürften.

Zuletzt wären auch bei dem Anspruch auf Datenübertragbarkeit die Versagungs- und allgemeinen Verweigerungsgründe (vgl. Art. 12 Abs. 5 DSGVO) zu erwähnen, die ggfs. der Umsetzung entgegenstehen. So darf das Recht

26 Siehe *Westphal/Wichtermann*, ZD 2019, 191, 191 ff.

27 Vgl. hierzu eine Studie der Stiftung Datenschutz, https://stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/Datenportabilitaet/stiftungdatenschutz_abschlussbericht_Hyperlinks_20180124_01_web.pdf.

28 Hierzu wird grundsätzlich aufgefordert, so ErwG. 68 S. 2.

auf Datenübertragbarkeit gem. Art. 20 Abs. 4 DSGVO *„die Rechte und Freiheiten anderer Personen nicht beeinträchtigen."* – doch diese Situation wäre im Rahmen der Interessenabwägung anzunehmen, wenn bei der Übertragung der Daten in einen neuen Account oder auf eine neue Plattform auch personenbezogene Daten anderer Personen, z. B. Mitspieler:innen berührt wären und folglich deren Daten sodann ohne Wissen und Zustimmung ebenfalls auf einem neuen Account oder auf einem neuen Portal veröffentlicht werden und unter Umständen sogar dann neue Verpflichtungen für diese begründen würden. Diesbezüglich besteht auch die Informationspflicht nach Art. 13 und 14 DSGVO des Verantwortlichen.

9.5 Drohende Folgen

Die drohenden Folgen etwaiger Verstöße gegen die Vorgaben aus der DSGVO bei der Bearbeitung von Betroffenenanfragen lassen sich nicht von der Hand weisen.

Die fehlerhafte Umsetzung der Betroffenenrechte kann zu Sanktionen der Aufsichtsbehörden, z. B. einem Bußgeld gegenüber dem Verantwortlichen, führen.[29] Denkbar wäre darüber hinaus auch der Schadensersatzanspruch der betroffenen Person – nach Art. 82 DSGVO bzw. § 823 BGB.[30] Letzteres beschäftigt derzeit die Gerichte hierzulande und birgt mangels höchstrichterlicher Entscheidung in der Frage eines etwaigen Schwellenwertes zur Annahme eines Schadens im Sinne von Art. 82 DSGVO erhebliche Rechtsunsicherheit.[31]

Ferner könnte sich die betroffene Person bei unzureichender Umsetzung des jeweiligen Anspruchs aus den Betroffenenrechten bei einer Aufsichtsbehörde im Datenschutzrecht beschweren, die daraufhin in der Regel den Vorfall prüfen und ggfs. Maßnahmen (wie die oben genannten Geldbußen) einleitet wird. Derartige Beschwerden sind oftmals das Einfallstor für weitere Kontrollen durch die Aufsichtsbehörden.

---

29 Vgl. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20190919-PM-Bussgelder.pdf (Pressemitteilung LfD Berlin, 19.9.2019); Siehe auch hierzu das Bußgeld in Höhe von 525.000 Euro gegen ein Medienunternehmen aus den Niederlanden wegen fehlerhaften Umgang mit Betroffenenanfragen, https://www.datenschutz-notizen.de/aufsichtsbehoerde-verhaengt-bussgeld-in-hoehe-von-525-000-euro-gegen-medienunternehmen-0234081.

30 Siehe hierzu u. a.: Schadensersatz wegen verspäteter und unvollständiger Auskunft: LAG Hamm, Urt. v. 11.5.2021 – Az.: 6 Sa 1260/20; Schadensersatz wegen unvollständiger Auskunft: LAG Niedersachsen, Urt. v. 22.10.2021 – Az.: 16 Sa 761/20; Mehr hierzu *Wybitul/Leibold*, ZD 2022, 207 ff.

31 Vgl. LG Leipzig, Urt. v. 23.12.2021 – Az.: 03 O 1268/21; LAG Hamm, Urt. v. 11.5.2021 – Az.: 6 Sa 1260/20.

Soweit lässt sich konstatieren: Ein mangelhafter interner Umgang mit Anfragen und Ansprüchen aus den Betroffenenrechten deckt ein fehlerhaftes Datenschutzmanagement auf, d. h. es können weitere Pflichtverletzungen aus der DSGVO unter Umständen sichtbar werden.

9.6 Fazit

Es dürfte deutlich geworden sein, welche (datenschutz-)rechtliche Risiken drohen und warum sich alle Akteure im eSports mit den Betroffenenrechten aus der DSGVO auseinandersetzen sollten.

Aus den genannten Gründen lassen sich folgende Empfehlungen aussprechen:

- Zunächst sollten alle Akteure im eSports ihre jeweilige datenschutzrechtliche Rolle prüfen und ein entsprechendes Datenschutzmanagement etablieren. Es sind daher auch entsprechende datenschutzrechtliche Vereinbarungen, beispielsweise Verträge über die Auftragsverarbeitung gem. Art. 28 Abs. 3 DSGVO oder die gemeinsame Verantwortlichkeit nach Art. 26 Abs. 2 DSGVO zu schließen. Gleiches gilt entsprechend für einen Datentransfer außerhalb der EU bzw. des EWR.
- Die Verantwortlichen haben die Informationspflichten aus Art. 13 und 14 DSGVO umzusetzen und transparent an geeigneter Stelle über die Datenverarbeitung sowie die weiteren Akteure und deren Rollen zu informieren.
- Es sollten insbesondere auch Prozesse zum Umgang mit Betroffenenrechten festgelegt – und auch sichergestellt werden! Dieses umfasst auch das Nachkommen der Informationspflichten aus Art. 12 ff. DSGVO im Rahmen der Anfragen sowie die interne Dokumentation der entsprechenden Vorgänge an einem hierfür vorgegebenen Ort für drei Jahre.
- Somit bietet es sich an, konkrete technische Lösungen und/oder vertragliche Regelungen zu treffen bzw. umzusetzen, um Risiken des fehlerhaften Umgangs mit den Betroffenenrechten zu minimieren.

10 Technologie-Souveränität durch europäische Gesetzgebung? – Der Entwurf des neuen EU Chips Act und sein regulatorisches und politisches Framework

*Dennis-Kenji Kipker**

Halbleiter sind das Rückgrat der Digitalwirtschaft – zu diesem Ergebnis ist auch die EU gelangt. Das Thema digitale Souveränität wird mit Sicherheit eine der Schlüsselfragen der 2020er-Jahre, ist jedoch mehr und mehr vom Funktionieren weltweiter Lieferketten abhängig – und in einer Zeit wachsender politischer Spannungen und Unsicherheiten mit erheblichen Herausforderungen verbunden. 22 europäische Mitgliedstaaten haben daher bereits im Dezember 2020 eine gemeinsame Erklärung unterzeichnet, in der sie ihren Wunsch nach Zusammenarbeit in der europäischen Technologieentwicklung bekräftigt haben.

Wie stark heutige Fertigungs- und Lieferprozesse auf weltweite Stabilität angewiesen sind, hat unlängst die Corona-Pandemie gezeigt – Unfälle auf wichtigen Handelsrouten, politische Konflikte und Kriege sorgten und sorgen ebenfalls für Probleme. Als Beispiel hat etwa die EU-Kommission die in einigen Mitgliedstaaten erheblichen Produktionskürzungen in der Automobilindustrie im vergangenen Jahr angeführt, die vor allem auf den Mangel von Halbleitern aus Fernost zurückzuführen waren. Dies belegt eindrücklich, wie die Wettbewerbsfähigkeit, Resilienz und weitere Digitalisierung des europäischen Binnenmarktes in erheblicher Weise von der Halbleiterentwicklung abhängig sind.

10.1 Mehr als ein Gesetz

Mit dem EU Chips Act wird in Zukunft anvisiert, die Ziele der europäischen digitalpolitischen Strategie umzusetzen. Das bedeutet unter anderem, dass die EU bis zum Jahr 2030 über einen globalen Marktanteil von 20 % in der Halbleiterfertigung verfügen will. Dieses Ziel lässt sich nicht durch eine einzelne rechtliche Regulierung erzielen, sondern erfordert umfassende Investitionen, neue Regularien sowie erhebliche Umstrukturierungspläne für die europäische Digitalwirtschaft, weshalb der EU Chips Act nur einen – wohl

---

* Mehr über den Autor erfahren Sie im Autor:innenhinweis auf S. 224 ff. Anm. d. Hrsg.: Der Beitrag wurde zuerst in der kes Ausgabe 2/2022 veröffentlicht. Die Zweitveröffentlichung hier erfolgt mit freundlicher Zustimmung der DATAKONTEXT GmbH.

aber den Hauptbestandteil – eines umfassenderen Rahmenwerks bilden wird,[1] das sich aus den folgenden Komponenten zusammensetzt:

- a Chips Act for Europe[2]
- a Regulation establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act) including Annex I: Actions – Technical description of the Initiative: scope of actions, Annex II: Measurable Indicators to Monitor the Implementation and to Report on the Progress of the Initiative Towards the Achievement of its Objectives, and Annex III: Synergies with Union Programmes[3]
- a Council Regulation amending Regulation (EU) 2021/2085 establishing the Joint Undertakings under Horizon Europe, as regards the Chips Joint Undertaking[4]
- Commission Recommendation on a common Union toolbox to address semiconductor shortages and an EU mechanism for monitoring the semiconductor ecosystem.[5]

10.2 Sofortmaßnahmen

Die „Common Union Toolbox" liefert dabei erste operative Maßnahmen schon vor Inkrafttreten des Chips Act. Sie verfolgt das Ziel, eine rasche, wirksame und koordinierte Reaktion der EU auf die derzeitigen Lieferengpässe bei Halbleitern und auf künftige ähnliche Fälle zu ermöglichen, indem

1 European Commission, European Chips Act: Communication, Regulation, Joint Undertaking and Recommendation, Überblicksbeitrag, Februar 2022, https://digital-strategy.ec.europa.eu/en/library/european-chips-act-communication-regulation-joint-undertaking-and- recommendation.

2 Europäische Kommission, Ein Chip-Gesetz für Europa, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Februar 2022, https://ec.europa.eu/newsroom/dae/redirection/document/83088.

3 European Commission, Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act), Februar 2022, https://ec.europa.eu/newsroom/dae/redirection/document/83090 – nebst Anhängen https://ec.europa.eu/ newsroom/dae/redirection/document/83084.

4 Europäische Kommission, Vorschlag für eine Verordnung des Rates zur Änderung der Verordnung (EU) 2021/2085 zur Gründung der Gemeinsamen Unternehmen im Rahmen von „Horizont Europa" hinsichtlich des Gemeinsamen Unternehmens für Chips, Februar 2022, https://ec.europa.eu/newsroom/dae/redirection/document/83089.

5 Europäische Kommission, Empfehlung der Kommission (…) über ein gemeinsames Instrumentarium der Union zur Behebung von Lieferengpässen bei Halbleitern und einen EU-Mechanismus zur Überwachung des Halbleiter-Ökosystems, Februar 2022, https://ec.europa.eu/newsroom/dae/redirection/document/83093.

ein Überwachungsmechanismus durch eine europäische Expert:innengruppe für Halbleiter aktiviert wird.

Dazu gehört allem voran eine aktive Zusammenarbeit der Mitgliedstaaten, um Informationen über den aktuellen Stand der Halbleiterkrise auf den jeweiligen nationalen Märkten auszutauschen – entsprechend sind von Unternehmensverbänden beziehungsweise von einzelnen Halbleiter- oder Geräteherstellern Informationen über deren Liefervermögen einzuholen. Überdies umfasst die Risikobewertung die Erfassung geeigneter Frühwarnindikatoren mit Blick auf Störungen der Halbleiter-Lieferkette.

Ähnlich wie schon in den vergangenen Jahren für die kritischen Infrastrukturen wird den Mitgliedstaaten vorgeschlagen, die wichtigsten Kategorien von Halbleiteranwendern zu ermitteln – besonders auch solche aus kritischen Sektoren. Dazu werden einschlägige Interessenverbände, einschließlich Branchen- und Industrieverbände, und Vertreter der wichtigsten Anwenderkategorien dazu aufgefordert, Informationen zu folgenden Punkten zu übermitteln, welche die Mitgliedstaaten für eine Meldung an die EU-Kommission nutzen können:

- ungewöhnliche Nachfragesteigerungen
- bekannte Störungen der Lieferketten
- Nichtverfügbarkeit wichtiger Halbleiter oder Rohstoffe
- überdurchschnittlich lange Vorlaufzeiten
- Lieferverzögerungen
- außergewöhnliche Preissteigerungen.

Entsprechende kurzfristige Krisenreaktionsmaßnahmen mit Blick auf die strategische Halbleiterversorgung in der EU können gemäß der Kommissionsempfehlung Folgendes umfassen:

- Dialog mit Herstellern: Vorrang für krisenrelevante Produkte, um die Betriebskontinuität von kritischen Sektoren zu gewährleisten
- Erteilung eines Mandats an die EU-Kommission, damit diese als *zentrale Beschaffungsstelle* im Namen von zwei oder mehr Mitgliedstaaten bei der Vergabe öffentlicher Aufträge für krisenrelevante Produkte für bestimmte kritische Sektoren tätig wird
- *Ausfuhrkontrolle* von krisenrelevanten Produkten
- Aufnahme von *koordinierten Konsultationen oder Zusammenarbeit mit Drittländern,* um kooperative Lösungen zur Bewältigung von Unterbrechungen der Lieferkette zu finden.

Der vorläufige Charakter dieser Empfehlung der EU-Kommission wird durch die entsprechende Bestimmung im Dokument deutlich, dass die Emp-

fehlung nach Inkrafttreten des EU Chips Act aufgehoben werden kann – gleichzeitig verdeutlicht dies aber auch die schon gegenwärtige Relevanz des Themas, indem die EU-Kommission von einer fortdauernden „Halbleiterkrise" spricht. Deshalb bilden die zuvor in der „Toolbox" beschriebenen Maßnahmen einen Weg, um bereits jetzt kurzfristig zu reagieren, ohne den weiteren zeitlichen Verlauf des Gesetzgebungsverfahrens des EU Chips Act abwarten zu müssen.

Mittelfristig verfolgt die europäische Strategie den Ansatz, die Fertigungs- und Entwicklungskapazitäten innerhalb der EU zu stärken, um durch verbesserte Technologie-Souveränität ein höheres Maß an Resilienz zu gewährleisten. Das langfristige politische Ziel der EU-Kommission liegt in der Übernahme der technologischen Führungsrolle im Halbleitersegment und der damit verbundenen wirtschaftlichen Souveränität im globalen Rahmen. Diese Entwicklung wird durch eine umfassende finanzielle Förderung der EU zur Halbleiterentwicklung im Rahmen der sogenannten „Chips for Europe"-Initiative (s. u.) und des „EU Chips Fund" unterstützt und adressiert vor allem die Bereiche High Performance Computing, künstliche Intelligenz und Cybersecurity.

10.3 Zentrale Definitionen

Der inklusive der Begründung und haushaltsrechtlicher Rahmenbedingungen insgesamt 101 Seiten lange Entwurf des EU Chips Act lässt sich mit seinen Vorgaben in diese europäische Gesamtstrategie einordnen und gibt so gesehen vertiefend und strategisch langfristig die Vorgaben der aktuell geltenden europäischen Toolbox zur Überwachung des Halbleiter-Ökosystems wieder. Daher finden sich hier an verschiedenen Stellen teils auch inhaltliche Überschneidungen.

Zu Beginn des Gesetzes werden in Kap. 1, Art. 2 zentrale und teils weit gefasste Begriffsdefinitionen aufgeführt, von denen an dieser Stelle einige aufgeführt werden sollen:

- *Halbleiter*: Material, entweder elementar, wie Silizium, oder eine Verbindung wie Siliziumkarbid, dessen elektrische Leitfähigkeit verändert werden kann – oder ein Bauteil, das aus einer Reihe von Schichten aus halbleitenden, isolierenden und leitenden Materialen besteht, die nach einem vorgegebenen Muster angeordnet sind, und das dazu bestimmt ist, genau definierte elektronische oder photonische Funktionen oder beides zu erfüllen
- *Chip:* elektronisches Bauelement, das verschiedene Funktionselemente auf einem einzigen Stück Halbleitermaterial umfasst – typischerweise in

Form von Speicher-, Logik-, Prozessor- und Analoggeräten –, auch als „integrierte Schaltung“ bezeichnet

- *Halbleiter-Lieferkette:* System von Tätigkeiten, Organisationen, Akteuren, Technologie, Informationen, Ressourcen und Dienstleistungen, die an der Produktion von Halbleitern beteiligt sind, einschließlich Rohstoffen, Fertigungsanlagen, Entwurf, Herstellung, Montage, Prüfung und Verpackung
- *Halbleiter-Wertschöpfungskette:* Gesamtheit der Tätigkeiten im Zusammenhang mit einem Halbleiterprodukt von seiner Konzeption bis zu seiner Endanwendung, einschließlich Rohstoffen, Fertigungsanlagen, Forschung, Entwurf, Herstellung, Prüfung, Montage und Verpackung bis zur Einbettung und Validierung in Endprodukten
- *Krisenrelevante Produkte:* Halbleiter, Zwischenprodukte und Rohstoffe, die zur Herstellung von Halbleitern oder Zwischenprodukten benötigt werden, die von der Halbleiterkrise betroffen oder von strategischer Bedeutung für die Behebung der Halbleiterkrise oder ihrer wirtschaftlichen Auswirkungen sind.

10.4 Chips for Europe

Das zweite Kapitel des Gesetzentwurfs definiert die Grundsätze der „Chips for Europe“-Initiative. Hierzu gehören neben dem zeitlichen Rahmen auch die Anknüpfung an die Förderprogramme „Horizon Europe“ und „Digital Europe“. Art. 4 legt mit den Zielen fest, dass Technologie zu entwickeln ist, die weit über den aktuellen Stand der Technik hinausgeht. Dazu werden fünf Zielsetzungen operationialisiert:

- der Aufbau fortgeschrittener, in der Breite angelegter Entwurfskapazitäten für integrierte Halbleitertechnologie,
- die Verbesserung bestehender und Entwicklung neuer fortschrittlicher Pilotlinien,
- der Aufbau neuer Entwicklungskapazitäten für Quanten-Chips,
- der Aufbau eines Netzwerks von Kompetenzzentren für Halbleiter in der EU und
- die Einrichtung des „EU Chips Fund“, um besonders Start Ups, Scale Ups und KMUs einen erleichterten Zugang zu Finanzierungsmöglichkeiten zu gewähren.

Ein „European Chips Infrastructure Consortium“ (ECIC) begleitet dabei die Durchführung förderfähiger Maßnahmen und erstellt einen jährlichen Tätigkeitsbericht (Art. 7). Die Einrichtung und die Aufgaben des

europäischen Netzwerks von Kompetenzzentren für Halbleiter werden in Art. 8 beschrieben – das umfasst unter anderem die Beschleunigung von Entwicklungsprozessen, den Kompetenzaufbau, die Erleichterung des Wissenstransfers sowie die Entwicklung von Ausbildungskapazitäten und eines europäischen Talentpools zur Begegnung des Fachkräftemangels.

10.5 Schutz der Lieferkette

Kapitel 3 hat den Schutz der Halbleiter-Lieferkette zum Gegenstand und regelt mit Art. 10 die Förderung von sogenannten „integrierten Produktionsanlagen“ (Integrated Production Facilities) als „First-of-a-kind Facilities“. Darunter zu verstehen sind Industrieanlagen zur Halbleiterherstellung für die gesamte Verarbeitung eines Halbleiterwafers sowie Zusammenbau und Prüfung jeder einzelnen integrierten Schaltung, die in der EU im Wesentlichen noch nicht vorhanden ist oder zu deren Bau man sich verpflichtet hat und die unter anderem bessere Leistung, Prozessinnovation oder Energie- und Umweltleistung ermöglichen. Auf diese Weise sollen die integrierten Produktionsanlagen einen Beitrag zur Versorgungssicherheit des europäischen Binnenmarktes leisten.

Das Gesetz nennt einen Kriterienkatalog, welche Anforderungen eine integrierte Produktionsanlage erfüllen sollte. Hervorzuheben ist in diesem Zusammenhang, dass eine integrierte Produktionsanlage garantiert, nicht der extraterritorialen Anwendung von Gemeinwohlverpflichtungen von Drittländern in einer Weise unterworfen zu sein, welche die Versorgungssicherheit kritischer Sektoren in der EU beeinträchtigt.

Art. 11 betrifft sogenannte „Open EU Foundries“: Diese sind ebenfalls „First-of-a-kind Facilities“ in der EU, die Produktionskapazitäten für unabhängige Unternehmen bereitstellen und damit zur Versorgungssicherheit im Binnenmarkt beitragen. Auch hier werden verschiedene, von diesen Unternehmen zu erfüllende Anforderungen benannt – unter anderem positive Auswirkungen auf die EU-Halbleiter-Wertschöpfungskette oder die Investition in Chips der nächsten Generation.

Ein detailliertes Bewerbungs- und Anerkennungsverfahren mit Entscheidungshoheit der EU-Kommission für „Integrated Production Facilities“ und „Open EU Foundries“ regelt Art. 12: Soweit Chip-Produktionsanlagen als eine dieser Facilities anerkannt sind, dienen sie dem öffentlichen Interesse und genießen daher priorisierte Behandlung in den Mitgliedstaaten – beispielsweise bei der Erteilung von Genehmigungen und zur Vereinfachung sowie Beschleunigung von Administrativprozessen (Art. 14).

10.6 Marktmonitoring und Krisenmanagement

Das vierte Kapitel der Entwurfsfassung des EU Chips Act trägt den Titel „Überwachung und Krisenreaktion". Neben der Förderung und Entwicklung eigener Produktionskapazitäten im Halbleitersektor geht es hier vorrangig darum, Versorgungsengpässe zeitnah festzustellen und darauf schnell, angemessen und politisch sowie behördlich koordiniert mitgliedstaatenübergreifend zu reagieren.

Hierzu wird in Art. 15 die regelmäßige Überwachung der Halbleiter-Lieferkette vorgeschrieben. Diese Überwachung umfasst die Einbeziehung von Frühwarnindikatoren („Union Risk Assessment", Art. 16) sowie Nachfrageschwankungen und Unterbrechungen der Lieferkette. Bei eingetretener Gefahrenlage sieht das Gesetz die Einberufung des „European Semiconductor Boards" („Establishment and Tasks" gem. Art. 23) vor, um über die koordinierte Beschaffung von Halbleiterprodukten zu entscheiden und Lösungen zur Unterbrechung der Lieferkette zu ermitteln. Zur mitgliedstaatlichen Überwachungsaufgabe gehört gemäß Art. 17 ebenso, die wichtigsten Marktteilnehmer entlang der Halbleiter-Lieferkette in ihrem Hoheitsgebiet zu ermitteln.

Art. 18 beschreibt die Aktivierung des „Krisenstadiums" durch die EU-Kommission bei Vorliegen einer „Halbleiterkrise" – also den Fall, dass schwerwiegende Störungen in der Versorgung mit Halbleitern auftreten, die zu erheblichen Engpässen führen und hierdurch kritische Sektoren und die Wirtschaft erheblich negativ beeinträchtigen. Mit der Aktivierung des Krisenstadiums gehen verschiedene weitere Maßnahmen einher, die gem. Art. 19 Bestandteil der „Emergency Toolbox" sind:

- Einholung von Informationen unter anderem über Produktionskapazitäten von Unternehmen (Art. 20, bußgeldbewehrt),
- die Priorisierung von Aufträgen im Hinblick auf krisenrelevante Produkte (Art. 21 und damit einhergehend grundsätzlich die Verpflichtung der Unternehmen, Aufträge mit Prioritätseinstufung anzunehmen) sowie
- die mitgliedstaatlich-gemeinsame und durch die EU-Kommission koordinierte Beschaffung von Halbleiterprodukten (Art. 22).

10.7 Gremien

Governance-Strukturen und Bußgelder werden in den Kapiteln 5 und 6 bestimmt. Die Einrichtung und die Aufgaben des „European Semiconductor Boards" mit seiner Hauptberatungsaufgabe gegenüber der EU-Kommission richten sich nach den Art. 23, 24 und 25. Das Board setzt sich aus

Vertreter:innen der Mitgliedstaaten zusammen – den Vorsitz führt ein EU-Kommissionsvertreter und es hält mindestens einmal jährlich eine ordentliche Sitzung ab. Als Beobachter können beispielsweise Organisationen eingeladen werden, die Interessen der Halbleiterindustrie vertreten, sowie Forschungs- und Technologieorganisationen.

Gemäß Art. 26 benennt jeder Mitgliedstaat mindestens eine für die Umsetzung der Vorgaben aus dem EU Chips Act zuständige Behörde. Mit Blick auf die Sanktionen und Bußgelder unterscheidet Art. 28 zwischen einem zahlenmäßig festgesetzten Bußgeld bis maximal 300000 € und einem maximalen prozentualen Bußgeld von 1,5 % des durchschnittlichen Tagesumsatzes des vorangegangenen Geschäftsjahres eines Unternehmens. Gemäß Art. 33 wird die Arbeit der EU-Kommission von einem Halbleiterausschuss („Semiconductor Committee“) unterstützt.

10.8 Fazit und Ausblick

Auf den ersten Blick scheint der EU mit dem Chips-Act und seinem flankierenden Rahmenwerk ein sinnvoller Vorstoß geglückt zu sein, um die technologische Souveränität im Halbleitersegment auf globalen Märkten wiederherzustellen.

Kommission und europäischer Gesetzgeber legen einen abgestimmten Katalog vor, der sich aus kurzfristigen Sofortmaßnahmen, mittelfristigen Monitoring-Komponenten inklusive einer Risikoanalyse und einer langfristigen und strategischen (finanziellen) Chip-Förderung zusammensetzt. Auf diese Weise werden wirtschaftliche Unterstützung, Informationsaustausch, Regulierung und Überwachung sowie mitgliedstaatliche und globale Kooperation in einer zentralen Frage der 2020er-Jahre zusammengeführt. Dies zeigt ebenso, dass der Entwurf des EU Chips Act nicht bei der Halbleiterentwicklung und -fertigung endet, sondern in den ganzheitlichen europäischen Rahmen zur strategischen Entwicklung digitaler Souveränität einzuordnen ist – ein Thema, das zurzeit an vielen Fronten angegangen wird.

Nichtsdestotrotz wird sich in der Praxis erst noch zeigen müssen, wie effektiv das neue Regelungskonzept in seiner Gesamtheit tatsächlich ist – erste Hinweise liefert hier sicherlich die „Common Union Toolbox“, die einige Maßnahmen des EU Chips Act vorwegnimmt.

In jedem Fall stellt aber allein die Notwendigkeit für die neue europäische Gesetzgebung zur Technologie-Souveränität das Ergebnis eines bereits seit Jahrzehnten währenden Technologieausverkaufs dar, der nun innerhalb weniger Jahre rückgängig gemacht werden soll, nachdem die wirtschaftlichen und politischen Folgen vor allem in den letzten zwei Jahren mehr als deut-

lich geworden sind. Ob dies tatsächlich vornehmlich durch Gesetze, politische Strategien und Fördermittel möglich ist, wird sich zeigen. GAIA-X kann in diesem Zusammenhang durchaus als ein europäisches Projekt zitiert werden, dessen angekündigte Erfolge mit Blick auf die Erlangung von Technologie-Souveränität bislang weitgehend ausgeblieben sind.

Umso befremdlicher wirkt es, wenn die europäischen Dokumente zum Chips Act von „globalen Führungsrollen“ und „Quantenchips“ sprechen, wo doch zuvorderst und kurzfristig nur die Versorgungssicherheit mit Halbleiterbauteilen gewährleistet werden soll. Längerfristig steht an dieser Stelle die generelle Frage im Raum, inwieweit man technische Innovationen politisch triggern kann.

Noch ist das Gesetzgebungsverfahren zum EU Chips Act zwar nicht abgeschlossen, aber der vorliegende Entwurf und sein Rahmenwerk geben schon jetzt einen deutlichen Ausblick auf die Zukunft dieses Rechtsakts, der nach seinem Inkrafttreten unmittelbar in allen europäischen Mitgliedstaaten gelten wird.

11 Zwischen Katzen-GIFs, politischem Diskurs und gelebter Utopie – Rechtliche Fragen rund ums Fediverse

*Rebecca Sieber**

Dieser Beitrag beschreibt das sogenannte Fediverse als föderierte soziale Netzwerke, deren einzelne Instanzen dezentral mit freier Open Source Software betrieben werden. Mittels offener Protokolle können die verschiedenen Plattformen miteinander kommunizieren. Ziel dieses Beitrags ist es, einen Überblick über rechtliche und philosophische Fragen zum Fediverse zu geben. Der Fokus liegt dabei auf vertragsrechtlichen, deliktsrechtlichen und datenschutzrechtlichen Fragen aus Sicht von Betreiber:innen in Deutschland. Abschließend wird die interdisziplinäre Kritik am Fediverse diskutiert.

11.1 Einleitung

Im April kündigte der Milliardär Elon Musk, an, Twitter kaufen zu wollen.[1] Dadurch wurde vielen progressiven Nutzer:innen ein Kernproblem proprietärer und zentralisierter Online-Plattformen bewusst: Diese Plattformen können jederzeit die Besitzer:innen wechseln und ohne Mitsprache ihrer Nutzer:innen umgestaltet werden.[2] Auf der Suche nach Alternativen stießen diese Twitter-Nutzer:innen vor allem auf „Mastodon".[3] Mastodon[4] ist eine Fediverse-Software von vielen, hat bisher allerdings die meiste Aufmerksamkeit erhalten.[5]

---

* Mehr über die Autorin erfahren Sie im Autor:innenhinweis auf S. 224 ff.

1 *Turner/Adler*, „Elon Musk Makes $43 Billion Unsolicited Bid to Take Twitter Private", Bloomberg News v. 14.4.2022, https://www.bloomberg.com/news/articles/2022-04-14/elon-musk-launches-43-billion-hostile-takeover-of-twitter.

2 *Beckedahl*, „Die Machtkonzentration ist gefährlich", netzpolitik.org v. 14.4.2022, https://netzpolitik.org/2022/elon-musk-will-twitter-kaufen-die-machtkonzentration-ist-gefaehrlich/.

3 *Hauck*, „Das kann die Twitter-Alternative Mastodon", SZ.de v. 28.4.2022, https://www.sueddeutsche.de/wirtschaft/mastodon-twitter-netzwerk-dezentral-1.5574623.

4 https://joinmastodon.org/.

5 Der bisher einzige juristische Beitrag über das Fediverse ist ein Podcast über Mastodon von *Marcus Richter* und *Thomas Schwenke* mit *Malte Engeler*, „Mastodon und Haftung für dezentrale Netzwerke", Rechtsbelehrung Folge 60 (Jura-Podcast) v. 31.10.2018, https://rechtsbelehrung.com/mastodon-und-haftung-fuer-dezentrale-netzwerke-rechtsbelehrung-folge-60-jura-podcast/.

11.2 Der Begriff des Fediverse

11.2.1 Föderierung (Dezentralisierung)

Entscheidend für das Fediverse ist das Konzept der Föderation, eine Form der Dezentralisierung.[6] Das Fediverse ist ein soziales Netzwerk, das nicht von einem einzigen Unternehmen betrieben wird. Es ist vielmehr über viele „Instanzen" verteilt, die jeweils auf einem oder mehreren Servern betrieben werden. Diese Instanzen bestehen unabhängig voneinander und können jeweils eigene Nutzungsregeln festlegen.

11.2.2 Offene Kommunikationsprotokolle

Mittels offener Protokolle oder Standards können die einzelnen Instanzen miteinander kommunizieren – ähnlich wie bei der E-Mail.[7] Zum Teil werden nur solche Plattformen zum Fediverse gezählt, die den offenen Standard ActivityPub[8] nutzen.[9] Es gibt jedoch eine Vielzahl von Software im Fediverse, die zum Teil auch andere Protokolle verwenden.[10]

11.2.3 Free/libre/Open Source Software (FLOSS)

Ein Großteil der Fediverse-Software ist unter der GNU Affero General Public License (AGPL)[11] lizenziert.[12] Die AGPL erlaubt es allen Menschen oder Organisationen, eine Fediverse-Instanz auf eigenen Servern zu betreiben oder die Software zu verändern, solange der Quellcode unter der gleichen Lizenz veröffentlicht wird.[13] Es handelt sich also um eine freie

6 *Zulli et al*., Rethinking the "social" in "social media": Insights into topology, abstraction, and scale on the Mastodon social network, New media & society, 2020, Vol. 22 (7), 1188 (1192).

7 *La Cava et al*., Understanding the growth of the Fediverse through the lens of Mastodon, Appl Netw Sci (2021) 6:64, S. 2.

8 W3C Recommendation v. 23.1.2018, https://www.w3.org/TR/activitypub/.

9 *Shaw*, Decentralized Social Networks: Pros and Cons of the Mastodon Platform, UMM CSci Senior Seminar Conference, November 2020, https://umm-csci.github.io/senior-seminar/seminars/spring2020/shaw.pdf.

10 Siehe das Schaubild von *Imke Senst* und *Mike Kuketz*: https://www.kuketz-blog.de/das-fediverse-unendliche-weiten-als-schaubild-diagramm/. Zu erwähnen sind auch ältere Protokolle wie diaspora oder OStatus.

11 Siehe den Lizenztext unter https://www.gnu.org/licenses/agpl-3.0.html.

12 *La Cava et al.,* Understanding the growth of the Fediverse through the lens of Mastodon, Appl Netw Sci (2021) 6:64, S. 2; *Zulli et al.,* Rethinking the "social" in "social media": Insights into topology, abstraction, and scale on the Mastodon social network, New media & society, 2020, Vol. 22 (7), 1188 [Zulli et al.] (1193).

13 Free Software Foundation, „Why the Affero AGPL", https://www.gnu.org/licenses/why-affero-gpl.html.

Copyleft-Lizenz, die die sogenannten „vier Software-Freiheiten“ gewährleistet.[14] Dadurch kann nicht nur der zugrundeliegende Code untersucht, sondern auch von Nutzer:innen selbst weiterentwickelt werden.[15]

11.2.4 Soziale Netzwerke

Einem weiten Verständnis nach umfasst das Fediverse auch Messenger, die auf Protokollen wie XMPP oder Matrix basieren. Für diese ergeben sich technische und rechtliche Besonderheiten.[16] Bisher sind diese jedoch nur mit Bridges mit sozialen Netzwerken im engeren Sinne kompatibel. Im Netzwerkdurchsetzungsgesetz (NetzDG) werden soziale Netzwerke als Plattformen definiert, die dazu bestimmt sind, dass Nutzer:innen beliebige Inhalte mit anderen Nutzer:innen teilen oder der Öffentlichkeit zugänglich machen.[17] Plattformen zur Individualkommunikation werden hingegen nicht erfasst.[18] Die Abgrenzung zu Messengern mit Gruppenchat-Funktion bleibt aber auch mit dieser Definition schwierig.[19] Im allgemeinen Sprachgebrauch zeichnen sich soziale Netzwerke durch eine oder mehrere „Timelines“ oder „Feeds“ aus, in denen die geteilten Beiträge der vernetzten Nutzer:innen aggregiert oder zusammengestellt werden.

11.2.5 Föderation als sozialer Vorgang

Das Fediverse wird aufgrund seiner Struktur auch als „sozialeres“ Netzwerk bezeichnet.[20] Zudem werden die Inhalte nur aufgrund der Interaktionen zwischen Nutzer:innen über Instanzen hinweg ausgetauscht.[21] Insofern ist die Föderation nicht nur ein technischer, sondern auch ein sozialer Vorgang, der gewisse gemeinsame „Werte“ oder „Commitments“ voraussetzt.[22] Außerdem besteht die Möglichkeit der „Deföderation“ mittels Blockieren oder Stummschalten. Wie die Föderation ist auch die Deföderation ein sozialer

14 Free Software Foundation, „What is Free Software“?, https://www.gnu.org/philosophy/free-sw.html.
15 *Zulli et al.,* S. 1193 f.
16 Siehe zu den datenschutzrechtlichen Problemen von Matrix: *Franz*, Ein Fehler in der Matrix, CR-online.de, 2.6.2022, https://www.cr-online.de/blog/2022/06/02/ein-fehler-in-der-matrix/.
17 § 1 Abs. 1 S. 1 NetzDG.
18 § 1 Abs. 1 S. 2 NetzDG.
19 *Liesching*, in: Spindler/Schmitz (Hrsg.) Telemediengesetz, 2. Aufl. 2018, Rn. 54, 60.
20 Vgl. *Zulli et al*., S. 1194.
21 Vgl. *Shaw*, S. 1 f.
22 *Boyle/Gehl/Zulli/Yang/Brown*, The Promises, Problems and Possibilites for Alt-Networks, AoIR Selected Papers of Internet Research, 2021. https://doi.org/10.5210/spir.v2021i0.12090, S. 7.

Vorgang, der informell über „FediBlock“-Listen und sogenannte Hashtags koordiniert wird.[23] Insofern handelt es sich beim Fediverse eigentlich um viele mehrere Netzwerke, die nur teilweise oder auch gar nicht miteinander verbunden sein können.

11.3 Fediverse-spezifische Rechtsfragen

11.3.1 Rechtliche Beziehungen im Fediverse

11.3.1.1 Betreiber:innen einer Instanz

Die Instanzen werden unter anderem von Privatpersonen und Vereinen, aber auch von Unternehmen betrieben.[24] Im Verhältnis zwischen mehreren Betreiber:innen, Administator:innen und Moderator:innen einer Instanz können sich, je nach Rechtsform, unterschiedliche Rechtsfragen stellen. Besonderheiten gelten auch, wenn eine Instanz von einem Application Service Provider gehostet und gewartet wird.

11.3.1.2 Betreiber:innen – Entwickler:innen

Im Allgemeinen bereitet es Instanzbetreiber:innen wenig Schwierigkeiten, die Lizenzbedingungen der AGPL einzuhalten. Als Gegenbeispiel dient die von Donald Trump angekündigte Plattform „Truth Social“. Schon vor dem offiziellen Start in den USA stellte sich heraus, dass die Trump Media & Technology Group (TMTG) sich großzügig am Programmcode von Mastodon bedient und diesen als „eigenen“ ausgegeben hatte.[25] Auch die Alt-Right-Instanz Gab ist in der Vergangenheit durch Urheberrechtsverletzungen aufgefallen.[26] Es mag als Kehrseite der Software-Freiheiten erscheinen, dass die Nutzung durch Alt-Right-Netzwerke nicht verboten werden kann. Durch die Lizenzbedingungen kann aber immerhin eine gewisse Transparenz dieser Plattformen hergestellt werden.[27]

---

23 Siehe z. B. https://joinfediverse.wiki/index.php?title=FediBlock.

24 *Raman et al.*, Challenges in the Decentralised Web: The Mastodon Case, IMC ’19: Proceedings of the Internet Measurement Conference, New York 2019, https://doi.org/10.1145/3355369.3355572 [Raman et. al], S. 224.

25 *Rochko*, „Trump’s new social media platform found using Mastodon code“, Stellungnahme v. 29.10.2021, https://blog.joinmastodon.org/2021/10/trumps-new-social-media-platform-found-using-mastodon-code/.

26 *Rochko*, „Gab switches to Mastodon’s code“, Update v. 1.3.2021, https://blog.joinmastodon.org/2019/07/statement-on-gabs-fork-of-mastodon/.

27 Inzwischen haben sowohl die TMTG als auch Gab auf anwaltliche Schreiben der Entwickler:innen reagiert und den Code, wenn auch auf zweifelhafte Weise, veröffentlicht.

11.3.1.3 Betreiber:innen – Betreiber:innen

Wenn Betreiber:innen verschiedener Instanzen das gleiche Kommunikationsprotokoll nutzen, ist dies zunächst kein rechtsgeschäftlicher, sondern ein faktischer Vorgang. Die Betreiber:innen können zwar, je nach Software, beeinflussen, mit welchen Instanzen sie Nutzer:inneninhalte austauschen. Damit bestehen aber grundsätzlich keine Unterschiede zur E-Mail, bei der sich Anbieter:innen und Nutzer:innen ebenfalls gegenseitig blockieren können.

11.3.1.4 Betreiber:innen – Nutzer:innen der eigenen Instanz

Den rechtlichen Beziehungen zwischen Betreiber:innen und Nutzer:innen kann sich grob anhand folgender Kategorien angenähert werden:

11.3.1.4.1 Einzelnutzer:innen-Instanz

Sofern der/die Betreiber:in alleinige:r Nutzer:in der Instanz ist, besteht kein rechtliches Verhältnis.

11.3.1.4.2 Persönliche oder familiäre Instanz

Oft werden Instanzen nur für Freunde und Familie zur Verfügung gestellt. Ähnlich familiär sind solche Instanzen, bei denen eine Registrierung nur auf Einladung hin möglich ist. In diesen Fällen ist fraglich, ob ein Vertrag besteht.[28]

11.3.1.4.3 Freizeitlich oder ehrenamtlich betriebene Instanz

Ein Großteil der Fediverse-Instanzen ist offen für Registrierungen und wird unentgeltlich in der Freizeit, im Rahmen eines Ehrenamts oder „beruflich nebenher“ von einzelnen oder mehreren Personen betrieben. Die Instanzen werden in der Regel auch nicht über Werbung oder Datenverkauf finanziert. Teilweise wird zu Spenden aufgerufen oder ein Nutzungsbeitrag erhoben.

11.3.1.4.4 Geschäftliche Instanz

In seltenen Fällen werden Instanzen entgeltlich im Rahmen einer beruflichen oder gewerblichen Tätigkeit betrieben.[29] Diese Betreiber:innen können Unternehmer:innen und auch Kaufleute im handelsrechtlichen Sinne sein – unabhängig von einer Gewinnerzielungsabsicht.[30] Dies trifft beispielsweise

28 *Schäfer*, in: MüKo BGB, 8. Aufl. 2020, § 662 Rn. 27.
29 Ein Beispiel ist die Instanz Gab, die wesentliche Funktionen hinter einer Paywall verbirgt.
30 *Micklitz*, in: MüKo BGB, 9. Aufl. 2021, § 14 Rn. 23 ff.

auch auf gemeinnützige Vereine zu.[31] Teilweise wird auch eine Tätigkeit am Markt mit anderen Wettbewerber:innen vorausgesetzt.[32] Der Charakter des Fediverse ist allerdings grundsätzlich nicht kompetitiv, sondern kooperativ.

11.3.1.5 Betreiber:innen – Nutzer:innen anderer Instanzen

Zwischen Betreiber:innen und Nutzer:innen anderer Instanzen besteht kein vertragliches Verhältnis. Sobald sich Nutzer:innen folgen, werden die Inhalte der anderen Instanz auf der eigenen repliziert. Insofern kommt auch in diesem Verhältnis Datenschutzrecht zur Anwendung. Nutzer:innen können also beispielsweise Auskunfts- und Löschansprüche geltend machen.

11.3.2 Grundrechte

11.3.2.1 Unmittelbare Grundrechtsbindung staatlicher Betreiber:innen

Es gibt Instanzen, die von Behörden betrieben werden.[33] Bürger:innen können sich dort nicht registrieren, sondern jeweils nur Bundesbehörden oder Institutionen der EU. Staatliche Betreiber:innen sind unmittelbar an Grundrechte gebunden.[34] Daher ist etwa das Blockieren anderer Nutzer:innen oder Instanzen ein Eingriff in die Meinungs- und Informationsfreiheit, der zu rechtfertigen ist. Solche Fälle sind im Fediverse bisher nicht bekannt, aber ähnlich zu beurteilen wie das Blockieren durch staatliche Accounts in anderen sozialen Netzwerken.[35]

11.3.2.2 Mittelbare Drittwirkung der Grundrechte

Im Verhältnis zwischen Privatpersonen wirken sich Grundrechte nur mittelbar aus.[36] Die Grundrechte der Beteiligten sind etwa zu beachten, wenn ein Gericht die Nutzungsregeln einer Instanz interpretiert.[37] Eine faktische Grundrechtsbindung der Betreiber:innen, wie sie für große soziale Medi-

31 *Schäuble*, in: Hausmann/Odersky (Hrsg.), Internationales Privatrecht in der Notar- und Gestaltungspraxis, 4. Aufl. 2021, § 16 Schuldvertragsrecht Rn. 98.
32 *Faber*, ZEuP 1998, 854 (869 f., 876 ff.).
33 Dazu zählt die Instanz „social.bund.de“, die vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit betrieben wird, ebenso wie „EU Voice“, betrieben vom Europäischen Datenschutzbeauftragten.
34 Art. 1 Abs. 3 GG.
35 *Neumann*, „Grundrechte im digitalen Raum: Darf die Regierung ihre Kritiker auf Facebook und Twitter blockieren?“, vorgänge Nr. 228, 91–98.
36 BVerfG, Beschl. v. 11.4.2018 – 1 BvR 3080/09, NJW 2018, 1667 (1668).
37 Vgl. BGH, Urt. v. 29.7.2021 – III ZR 192/20, CR 2022, 179 (184).

en kontrovers diskutiert wird,[38] besteht im Fediverse (erst recht) nicht. Die Nutzer:innen im Fediverse sind zu einem viel geringeren Grade von einer bestimmten Instanz abhängig.[39] Trotz technischer Hürden und Unausgereiftheiten, steht es Nutzer:innen frei, die Instanz zu wechseln und sogar Inhalte und Follower:innen zu importieren. Der Code ist öffentlich zugänglich und kann grundsätzlich auch verändert werden.

11.3.3 Vertrags- und Verbraucherrecht

11.3.3.1 Vertragstyp

Im Fediverse können die Nutzungsverträge ganz unterschiedlich ausgestaltet sein. Im Allgemeinen werden Social-Media-Nutzungsverträge als gemischte Verträge angesehen, die Elemente von Miete, Dienstleistung und Werkvertrag enthalten.[40] Andere gehen von einem Vertragstyp „eigener Art" aus.[41] Bei Fediverse-Instanzen, die unentgeltlich betrieben werden, kommt vor allem ein Auftrag in Betracht.[42] Ein kleiner Nutzungsbetrag steht dem nicht unbedingt entgegen. Schließlich kann im Rahmen des unentgeltlichen Auftrags auch eine Aufwandsentschädigung als Vorschuss geltend gemacht werden.[43] Fraglich ist auch, ob größere Spenden den Auftrag nachträglich in einen entgeltlichen Vertrag „umwandeln" können.[44]

11.3.3.2 Rechtsbindungswille

Ob überhaupt ein Vertrag besteht, hängt vom Einzelfall ab und davon, ob beide Beteiligten ein erkennbares Interesse an rechtlich verbindlichen Regeln haben.[45] Für ein bloßes Gefälligkeitsverhältnis sprechen mögliche Haftungsrisiken, die den Betreiber:innen nicht zumutbar wären, oder eine mangelnde rechtliche und wirtschaftliche Bedeutung des Nutzungsverhält-

38 Dagegen BGH, Urt. v. 29.7.2021 – III ZR 192/20, CR 2022, 179 (185); Siehe zur faktischen Macht von Online-Plattformen: *Przemysław*, „Terms of Service are not Contracts – Beyond Contract Law in the Regulation of Online Platforms", in: Grundmann (Hrsg.), European Contract Law in the Digital Age, 2018, S. 154 ff.

39 Vgl. BVerfG, Beschl. v. 22.5.2019 – 1 BvQ 42/19, NJW 2019, 1935 (1936); BGH, Urt. v. 29.7.2021 – III ZR 192/20, CR 2022, 179 (186).

40 Siehe *Spindler*, CR 2019, 238 (239); *Wurmnest*, in: MüKo BGB, 9. Aufl. 2022, § 307 Rn. 144.

41 OLG München v. 24.8.2018 – 18 W 1294/18, AfP 2019, 57; zitiert nach *Spindler*, CR 2019, 238 (239) m. w. N.

42 Vgl. *Beurskens*, NJW 2018, 3418 (3419); *Bräutigam/Richter*, in: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, S. 91 f.

43 §§ 669, 670 BGB.

44 So *Wiese*, in: Schulze (Hrsg.), BGB. Kommentar, 11. Aufl. 2021, § 662 Rn. 8.

45 *Bachmann*, in: MüKo BGB, 9. Aufl. 2022, § 241 Rn. 235 ff.; *Friehe*, NJW 2020, 1697 (1697).

nisses.[46] Die kostenlose Nutzungsmöglichkeit spricht nicht zwangsläufig gegen einen Vertrag.[47] Umgekehrt ist aber das Bestehen einer Gegenleistung ein starkes Indiz für einen Rechtsbindungswillen.[48] Weitere Indizien sind das Vorhandensein von Nutzungsregeln und AGB sowie die Registrierung mit einer E-Mail-Adresse.[49] Für proprietäre und zentralisierte Social-Media-Plattformen ist anerkannt, dass es sich um einen Vertrag handelt.[50] Zu Recht wird aber auch kritisiert, dass deren AGB eher der Ausübung eines Eigentumsrechts ähneln. da sie lediglich einseitig Pflichten der Nutzer:innen regeln und im Gegenzug keinerlei Rechte gewähren.[51] Im Fediverse besteht zwar die Besonderheit, dass Nutzer:innen in viel geringerem Maße auf Instanzbetreiber:innen angewiesen sind, da sie die Instanz jederzeit wechseln können. Jedoch können beispielsweise alte Beiträge noch nicht importiert werden.[52] Insofern haben Nutzer:innen ein erkennbares Interesse daran, dass eine Instanz nicht völlig ohne Vorwarnung abgeschaltet wird. Umgekehrt haben auch Betreiber:innen ein Interesse an einer hohen Aktivität auf ihrer Instanz.[53]

11.3.3.3 Rechtsfolgen

Welche Ansprüche sich aus dem Vertrag ergeben, hängt stark von den jeweiligen AGB ab.[54] Betreiber:innen könnten etwa eine Aufwandsentschädigung oder die Einhaltung von bestimmten Nutzungsregeln verlangen. Die Nutzer:innen haben aus dem Auftrag einen Anspruch auf Zugang, wenn sie zum Beispiel unrechtmäßig gesperrt wurden.[55] Möglich wäre auch ein Anspruch auf Schadensersatz in Form der Wiederherstellung eines unrechtmäßig gelöschten Beitrags.[56] Die Betreiber:innen dürfen – jedenfalls die eigenen – Nutzer:innen und deren Beiträge nicht willkürlich sperren und

46 Siehe nur BGH, Urt. v. 16.5.1974 – II ZR 12/73, NJW 1974, 1705 (1706 f.); zitiert nach *Mansel*, in: Jauernig (Hrsg.), BGB Kommentar, 18. Aufl. 2021, § 241 Rn. 24 m. w. N.

47 BGH, Urt. v. 22.6.1956 – I ZR 198/54, NJW 1956, 1313 (1313), zitiert nach *Bachmann*, in: MüKo BGB, 9. Aufl. 2022, § 241 Rn. 241 m. w. N.

48 *Bachmann*, in: MüKo BGB, 9. Aufl. 2022, § 241 Rn. 242; Kreutz, ZUM 2018, 162 (167).

49 Vgl. *Kreutz*, ZUM 2018, 162 (166 f.).

50 Siehe nur BGH, Urt. v. 29.7.2021 – III ZR 179/20, CR 2022, 179 (181); *Friehe*, NJW 2020, 1697 (1697).

51 *Przemysław*, „Terms of Service are not Contracts – Beyond Contract Law in the Regulation of Online Platforms", in: Grundmann (Hrsg.), European Contract Law in the Digital Age, 2018, S. 143 ff.

52 https://github.com/mastodon/mastodon/issues/5774.

53 Vgl. *Zulli et al.*, S. 1196.

54 *Boosfeld*, GPR 2022, 70 (71).

55 Vgl. BVerfG, Beschl. v. 22.5.2019 – 1 BvQ 42/19, NJW 2019, 1935 (1936).

56 BGH, Urt. v. 29.7.2021 – III ZR 192/20, CR 2022, 179 (191).

haben sich bei der Moderation an ihre eigenen Instanzregeln zu halten.[57] Je nach Sachverhalt sollten auch im Fediverse Nutzer:innen vor einer Sperrung möglichst angehört werden.[58] Schwieriger zu beurteilen ist, ob Nutzer:innen Schadensersatzansprüche geltend machen können, wenn eine Instanz ausfällt oder unangekündigt abgeschaltet wird. Anders als bei anderen Gefälligkeitsverträgen gibt es beim Auftrag kein Haftungsprivileg.[59] Auch ein stillschweigender Haftungsausschluss kann nicht unbedingt angenommen werden.[60] Betreiber:innen können sich aber grundsätzlich in AGB entsprechend absichern.

11.3.3.4 Verbraucherrecht

Seit Anfang 2022 enthält das BGB neue Vorschriften über digitale Produkte. Diese gelten unabhängig vom Vertragstyp,[61] sodass auch das Bereitstellen einer Fediverse-Instanz als digitale „Dienstleistung" in Betracht kommt. Allerdings gelten diese Regelungen nur für Unternehmer-Verbraucher-Verhältnisse, bei denen Nutzer:innen mit Geld oder Daten „bezahlen".[62] Das ist im Fediverse aber regelmäßig nicht der Fall.[63] Ob eine Aufwandsentschädigung in Form eines Nutzungsbeitrags oder gar eine Spende als Gegenleistung gelten kann, ist zweifelhaft.[64] Die praktische Bedeutung der Gewährleistungsansprüche dürfte im Fediverse auch eher gering sein.

Die Nutzungsbedingungen dürfen außerdem keine unfairen Klauseln enthalten.[65] Handelt es sich bei den Nutzer:innen um Verbraucher:innen, kann beispielsweise die Haftung für vorsätzliches und grob fahrlässiges Verhalten nicht ausgeschlossen werden.[66] Dies setzt im Einzelfall voraus, dass der:die jeweilige Nutzer:in eine „natürliche" Person oder Mensch ist und das Fediverse-Profil nicht überwiegend zu beruflichen oder gewerblichen Tätigkeiten nutzt.[67]

---

57 Vgl. BGH, Urt. v. 29.7.2021 – III ZR 192/20, CR 2022, 179 (188).
58 BGH, Urt. v. 29.7.2021 – III ZR 192/20, CR 2022, 179 (188 f.).
59 *Schäfer*, in: MüKo BGB, 8. Aufl. 2020, § 662 Rn. 2, 73.
60 *Westphalen*, in: Westphalen/Thüsing (Hrsg.), Vertragsrecht und AGB-Klauselwerke, Freizeichnungs- und Haftungsbegrenzungen, 48. EL 2022, Rn. 14.
61 Begr. RegE, BT-Drs. 19/27653, S. 38.
62 § 327 Abs. 1, 3 BGB; Begr. RegE, BT-Drs. 19/27653, S. 38.
63 Die Daten werden vielmehr gemäß der Ausnahme in § 327 Abs. 2 i. V. m. § 312 Abs. 1a S. 2 BGB von Instanzbetreiber:innen nur verarbeitet, um die Leistungspflichten und an sie gestellte rechtliche Anforderungen zu erfüllen.
64 Dies hängt wohl auch davon ab, ob ein Auftrag als gegenseitiger Vertrag angesehen wird, vgl. *Schäfer*, in: MüKo BGB, 8. Aufl. 2020, § 662 Rn. 17.
65 §§ 305 ff. BGB.
66 § 309 Nr. 7 lit. b BGB.
67 Siehe *Micklitz*, in: MüKo BGB, 9. Aufl. 2021, § 13 Rn. 52 ff.

11.3.4 Haftung für rechtswidrige Inhalte

11.3.4.1 Ist eine Fediverse-Instanz ein „Dienst“?

Für besonders viel Unsicherheit sorgen Schadensersatz- und Unterlassungsansprüche aufgrund von Urheberrechts- und Persönlichkeitsrechtsverletzungen. Die Haftungsprivilegien des Telemediengesetzes (TMG) scheinen dem Wortlaut nach nicht so recht auf unentgeltliche Fediverse-Instanzen zu passen. Der Begriff des „Diensteanbieters“ setzt die die Richtlinie über den elektronischen „Geschäftsverkehr“[68] um.[69] Dort werden „Dienste der Informationsgesellschaft“ definiert als „jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung.“[70] Fediverse-Instanzen sind in der Regel zwar unentgeltlich, bilden damit aber im Vergleich zu anderen sozialen Medien eine Ausnahme. Zudem ist der Begriff des Diensteanbieters weit zu verstehen und erfasst auch nichtgewerbliche Angebote.[71] Es kommt vor allem nicht darauf an, dass die Dienstleistung von dem bezahlt wird, dem sie zugutekommt, sodass auch spendenfinanzierte Instanzen darunter fallen können.[72] Sofern die Instanzen auf eine gewisse Dauer angelegt sind oder nicht ausschließlich persönlichen Zwecken dienen, unterliegen sie auch den Impressumspflichten[73] – wie auch die Accountinhaber:innen.[74] Vom Urheberrechts-Diensteanbieter-Gesetz (UrhDaG) sind hingegen nur Betreiber:innen mit Gewinnerzielungsabsicht erfasst.[75]

11.3.4.2 Haftungsprivileg nach dem TMG

Fediverse-Instanzen sind als soziale Netzwerke weder journalistisch-redaktionell gestaltete Inhalte[76] noch „reine“ Telekommunikations-

68 RL 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt.

69 Begr. RegE, BT-Drs. 16/3078, S. 1, 11.

70 Art. 1 Nr. 1 lit. b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9.9.2015 über ein informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. EU Nr. L 241 vom 17.9.2015, S. 1).

71 *Ricke*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, § 2 Rn. 1.

72 EuGH, Urt. v. 26.4.1988 – C-352/85.

73 § 5 TMG.

74 *Ricke*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, § 2 Rn. 2.

75 § 2 Abs. 1 UrhDaG setzt einen Dienst der Informationsgesellschaft voraus, der das Bereitstellen von urheberrechtlichen Inhalten als Hauptzweck verfolgt und diese Inhalte mit Gewinnerzielungsabsicht bewirbt.

76 *Spindler*, in: Spindler/Schmitz, TMG, 2. Aufl. 2018, § 1 Rn. 78.

dienste[77], sondern Telemedien, auf die das TMG Anwendung findet.[78] Betreiber:innen haften als Host-Provider erst nach Kenntnisnahme für rechtswidrige Inhalte, müssen dann jedoch „unverzüglich" tätig werden.[79] Die geforderte Reaktionszeit kann je nach Schwere der Rechtsverletzung und erforderlicher Prüfungs- und Überlegungszeit variieren.[80] Im Fediverse könnten Betreiber:innen grundsätzlich nicht nur für die Inhalte ihrer eigenen Nutzer:innen, sondern auch für die von anderen Instanzen haften.

Auch die sogenannte Störerhaftung setzt voraus, dass Verhaltenspflichten verletzt werden.[81] Neben Prüf- und Überwachungspflichten hinsichtlich der Nutzer:inneninhalte kommen im Fediverse auch Sorgfaltspflichten zum Blockieren bestimmter Instanzen in Betracht. Die Verletzung einer Verhaltenspflicht setzt aber stets Kenntnis von der jeweiligen Rechtsverletzung voraus[82]. Insofern kommt eine Haftung beispielsweise in Betracht, wenn Löschanfragen von anderen Instanzen hinsichtlich illegaler Inhalte absichtlich unterbunden werden.[83] Grundsätzliche Änderungen werden sich auch nicht aus dem vom Europäischen Parlament verabschiedeten Gesetz für digitale Dienste (DSA) ergeben.[84] Allerdings wird es der DSA erfordern, die Oberfläche für das Melden von Inhalten anzupassen.[85]

11.3.4.3 NetzDG

Die Pflichten des NetzDG zum Umgang mit Nutzerbeschwerden gelten nur für Betreiber:innen von sozialen Netzwerken mit Gewinnerzielungsabsicht.[86] Zudem gilt für soziale Netzwerke mit weniger als zwei Millionen Nutzer:innen im Inland ein eingeschränktes Pflichtenprogramm.[87] Insge-

77 *Ricke*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, § 1 Rn. 6 ff.
78 *Ricke*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, § 1 Rn. 12.
79 § 10 TMG. In Hinblick auf das Usenet betrachtet *Spindler* die spiegelnden Usenet-Server aufgrund der Speicherzeitbegrenzung als Cache-Provider im Sinne des § 9 TMG, in: Spindler/Schmitz, TMG, 2. Aufl. 2018, § 9 Rn. 10. Das Fediverse und das Usenet sind aufgrund ihrer unterschiedlichen Struktur jedoch nur bedingt vergleichbar. Regelmäßig gelöscht werden im Fediverse meist nur Medienanhänge wie Bilddateien.
80 *Paal/Hennemann*, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 36. Edition, § 10 Rn. 46; *Spindler*, in: Spindler/Schmitz, TMG, 2. Aufl. 2018, § 10 Rn. 54.
81 BGH, Beschl. v. 13.9.2018 – I ZR 140/15, BGH GRUR 2018, 1132 (1137).
82 BGH, Beschl. v. 20.9.2018 – I ZR 53/17, BGH GRUR 2018, 1239 (1244), Rn. 43.
83 Dies entspricht auch dem Rechtsgedanken von § 9 S. 1 Nr. 5 TMG.
84 Artt. 5, 6 DSA.
85 Art. 14 Abs. 2 DSA.
86 § 1 Abs. 1 S. 2 NetzDG.
87 § 1 Abs. 2 NetzDG.

samt hat das Fediverse zwar mindestens über fünf Millionen Nutzer:innen.[88] Das NetzDG gilt jedoch nur für soziale Netzwerke, die eine Registrierung und Zustimmung zu bestimmten Nutzungsregeln voraussetzen.[89] Es kann insofern nur auf die Nutzer:innenzahlen einer einzelnen Instanz ankommen. Nach derzeitigem Stand gibt es keine Fediverse-Instanz, die mehr als zwei Millionen registrierte Nutzer:innen zählt.[90] Eine Ausnahme von dieser Ausnahme gilt für Videosharing-Plattformdienste wie PeerTube. Diese müssen mit Nutzer:innen wirksam vereinbaren, dass gewisse strafbare Inhalte verboten sind.[91]

11.3.5 Datenschutzrecht

11.3.5.1 Datenschutz-Grundverordnung (DSGVO)

11.3.5.1.1 Verantwortliche

Im Fediverse stellt sich die Frage, wer überhaupt Adressat:in der Pflichten aus der DSGVO ist. Verantwortlich ist die natürliche oder juristische Person, Behörde oder andere Stelle, die über die Zwecke und Mittel der Datenverarbeitung entscheidet.[92] Zweifellos ist der:die Betreiber:in einer Instanz für die Datenverarbeitung auf ihrem eigenen Server verantwortlich. Es könnten aber auch mehrere Personen gemeinsam verantwortlich sein.[93] Die gemeinsam Verantwortlichen sind dazu verpflichtet, in transparenter Form festzulegen, wer von ihnen welche datenschutzrechtlichen Pflichten übernimmt.[94]

In Betracht kommt einerseits eine Mitverantwortlichkeit der Nutzer:innen. Nach dem EuGH ist die datenschutzrechtliche Verantwortlichkeit grundsätzlich weit auszulegen.[95] Die bloße Nutzung eines sozialen Netzwerks allein begründet jedoch noch keine Mitverantwortlichkeit.[96] Auf den Fediverse-Plattformen stehen jedenfalls keine mit „Facebook Insights“ vergleichbare Funktionen zur Erstellung von Statistiken mittels Cookies bereit, um die Seite auf ein bestimmtes Zielpublikum auszurichten.[97] Je nach Soft-

88 Davon sind etwa zwei bis drei Millionen aktive Nutzer:innen, siehe https://the-federation.info/; *Zulli et al.,* S. 1190.
89 BT-Drs. 18/13013, S. 19; *Liesching*, Netzwerkdurchsetzungsgesetz. 1. Online-Auflage 2018, § 1 Rn. 10.
90 Vgl. zu Mastodon: https://instances.social.
91 Dazu zählt etwa die öffentliche Aufforderung zu Straftaten gem. § 111 StGB oder die Volksverhetzung, § 130 StGB, § 3e Abs. 2, 4 NetzDG.
92 Art. 4 lit. 7 DSGVO.
93 Art. 26 Abs. 1 S. 1 DSGVO.
94 Art. 26 Abs. 1 S. 2 DSGVO.
95 EuGH, Urt. v. 5.6.2018 – C-210/16, EuZW 2018, 534 (536), Rn. 26 ff.
96 EuGH, Urt. v. 5.6.2018 – C-210/16, EuZW 2018, 534 (536), Rn. 35.
97 Aus dem gleichen Grund kommt auch eine Auftragsdatenverarbeitung nicht in Betracht.

ware der Instanz können die Nutzer:innen selbst einstellen, ob die Liste ihrer Follower:innen offengelegt wird. Durch ihre Interaktion mit anderen Nutzer:innen können sie zudem mitbeeinflussen, an welche anderen Instanzen Daten weitergegeben werden. Die Datenverarbeitungsvorgänge und Standardeinstellungen hängen aber maßgeblich davon ab, welche Software die Betreiber:innen ausgewählt haben und auf ihren Servern betreiben. Meines Erachtens ist eine gemeinsame Verantwortlichkeit lediglich denkbar, wenn Nutzer:innen personenbezogene Daten von Dritten teilen.

Zweifelhaft ist auch, ob Betreiber:innen verschiedener, föderierender Instanzen gemeinsam verantwortlich sein können. Auch hier kann eine Parallele zu E-Mail-Providern gezogen werden, die E-Mails jeweils auf dem eigenen Server speichern. In beiden Fällen handelt es sich allerdings um unterschiedliche Datenverarbeitungsvorgänge, die jeweils in der Sphäre desjenigen Providers liegen, der die Daten speichert. Betreiber:innen sind insofern nur für die Daten verantwortlich, die auf den eigenen Servern gespeichert sind – nicht jedoch für die Kopien, die auf anderen Instanzen gespeichert sind.

11.3.5.1.2 Rechtsgrundlagen der Datenverarbeitung

Die Datenschutzerklärungen im Fediverse schweigen häufig zu den Rechtsgrundlagen der Datenverarbeitungen.[98] Hierbei ist zwischen den personenbezogenen Daten von eigenen Nutzer:innen und von Nutzer:innen anderer Instanzen zu differenzieren. Es können grundsätzlich auch mehrere Rechtsgrundlagen gleichzeitig einschlägig sein.[99] Insbesondere Accountdaten wie die E-Mail-Adresse sind für Betreiber:innen notwendig, um den Nutzungsvertrag zu erfüllen. Diese Datenverarbeitungen sind damit von Art. 6 Abs. 1 lit. b DSGVO gedeckt. Gleiches gilt für die geteilten Beiträge und Profilinformationen.[100] Diese Inhalte werden zudem freiwillig, im Rahmen einer eindeutig bestätigenden Handlung geteilt, womit auch eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO gegeben ist. Die Nutzer:innen können schließlich selbst durch technische Voreinstellungen und die Verwaltung ihrer Kontakte festlegen, gegenüber wem sie ihre Inhalte teilen. Für Nutzer:innen im Fediverse ist es vorhersehbar, dass ihre geteilten Inhalte auch an andere Instanzen weitergegeben werden. Die Funktionsweise des Fediverse besteht gerade darin, dass Inhalte auch dezentral von anderen Instanzen abgerufen werden können. Insofern entspricht die Föderation der Instanzen auch dem berechtigten Interesse der Betreiber:innen nach Art. 6

98 Siehe entsprechende Anforderung in Art. 13 Abs. 1 lit. c DSGVO.
99 Art. 6 DSGVO fordert, dass „mindestens eine“ der Rechtsgrundlagen erfüllt ist.
100 Vgl. die Datenschutzerklärung auf https://legal.social/terms.

Abs. 1 lit. f DSGVO.[101] Gleiches gilt für die Speicherung von IP-Adressen, die technischen und organisatorischen Maßnahmen dient.

11.3.5.1.3 „Recht auf Vergessenwerden"

Nutzer:innen können eigene Beiträge auf ihrer Instanz selbst löschen. Wird ein Beitrag gelöscht, wird diese Information zunächst automatisch an alle Instanzen weitergegeben, mit denen die Instanz föderiert. Im Idealfall werden mit der Löschung also auch alle Kopien auf anderen Servern gelöscht. Dies kann jedoch eine Weile dauern und theoretisch auch von Instanzbetreiber:innen unterbunden werden. Gerade bei der Föderation zwischen Plattformen, die unterschiedliche Software verwenden, kann es hier zu Problemen kommen.[102] Eine Pflicht zur Weiterleitung von Löschanfragen besteht nur für solche personenbezogene Daten, die der Verantwortliche selbst „öffentlich gemacht" hat.[103] Die Nutzer:innen können also von den Betreiber:innen lediglich Auskunft darüber verlangen, mit welchen Instanzen föderiert wird,[104] und diese gegebenenfalls einzeln zur Löschung auffordern. In Hinblick auf ein „Recht auf Vergessenwerden" ist die Funktionsweise des Fediverse also, wie auch des Internets allgemein, durchaus problematisch.

11.3.5.2 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)

Das Verhältnis zwischen Telemediendatenschutz und DSGVO ist kompliziert. Eigentlich hat die DSGVO als unmittelbar geltendes EU-Recht Anwendungsvorrang. Die speziellen Vorschriften des TTDSG können aber die DSGVO verdrängen, wenn sie die E-Privacy-Richtlinie umsetzen und dasselbe Ziel wie die DSGVO verfolgen, das heißt den Schutz personenbezogener Daten.[105] Zu beachten ist auch, dass die Nutzer:innen ebenfalls Adressaten des TTDSG sein können.

11.3.5.2.1 Fernmeldegeheimnis

Fraglich ist, ob für Instanzbetreiber:innen auch das Fernmeldegeheimnis gilt. Direktnachrichten über Mikro-Blogging-Dienste wie Mastodon sind nicht

101 Vgl. die Datenschutzerklärung auf https://freiburg.social/terms (Stand September 2020).
102 Siehe zum Beispiel https://github.com/pfefferle/wordpress-activitypub/issues/16.
103 Art. 17 Abs. 2 DSGVO.
104 Art. 15 Abs. 1 lit. c DSGVO.
105 Art. 95 DSGVO.

Ende-zu-Ende-verschlüsselt.[106] Betreiber:innen haben also Zugriff auf diese Inhalte. Das Fernmeldegeheimnis nach TTDSG gilt nur für Anbieter:innen von Telekommunikationsdiensten. Eine Fediverse-Instanz käme als interpersoneller Kommunikationsdienst in Betracht. Soziale Netzwerke und Blogs sollen aber gerade nicht davon erfasst sein.[107] In diesen Fällen ist die interpersonale Kommunikation, die gegenüber einem durch den Sender begrenzten Personenkreis erfolgt, lediglich eine Nebenfunktion von geringer Bedeutung für den Dienst insgesamt. Direktnachrichten sind auch nicht auf allen Fediverse-Plattformen vorgesehen. Dennoch sind Betreiber:innen im Rahmen der DSGVO und ihrer vertraglichen Schutzpflichten zur Wahrung der Vertraulichkeit verpflichtet.

11.3.5.2.2 Technische und organisatorische Vorkehrungen

Die Regelungen zu technischen und organisatorischen Vorkehrungen für Telemedien beruhen eigentlich nicht auf der E-Privacy-Richtlinie. Ihr Verhältnis zur DSGVO ist daher unklar.[108] Bedeutung erlangen diese Vorschriften jedenfalls wohl über den Anwendungsbereich der DSGVO hinaus, das heißt etwa im Bereich des Haushaltsprivileg oder sofern keine personenbezogenen Daten verarbeitet werden.[109] Aus der DSGVO und dem TTDSG ergibt sich beispielsweise eine Pflicht zur Transportverschlüsselung, welche bei den gängigen Fediverse-Plattformen auch umgesetzt ist. Zudem sind Instanzbetreiber:innen dazu verpflichtet, den Server mittels Sicherheits-Updates aktuell zu halten.

11.3.5.2.3 „Cookie-Banner-Pflicht“

Für Unsicherheit sorgt auch, ob Instanzbetreiber:innen verpflichtet sind, eine Einwilligung in das Setzen von „Cookies“ einzuholen. Die verschiedenen Fediverse-Plattformen sehen schließlich keine „Cookie-Banner“ vor. Regelmäßig werden jedoch nur Session-IDs im lokalen Speicher der Nutzer:innen abgelegt, um deren Login beizubehalten. Diese können von den Nutzer:innen durch Schließen des Browser-Fensters gelöscht werden. Insofern handelt es sich wohl um technisch notwendige Cookies, die ohne Einwilligung gesetzt werden können.[110]

---

106 Vgl. https://github.com/mastodon/mastodon/pull/13820.
107 Erwägungsgrund 17 des Europäischen Kodex für Kommunikation.
108 *Moos*, in: Taeger/Gabel, (Hrsg.) DSGVO – BDSG – TTDSG, 4. Aufl. 2022, § 19 TTDSG Rn. 3.
109 *Eckhardt/Lepperhoff*, in: Schwartmann/Jaspers/Eckhardt (Hrsg.), TTDSG, 1. Aufl. 2022, § 19 Rn. 11 f.
110 *Sesing*, MMR 2021, 544 (545).

11.4 Kritik am Fediverse

11.4.1 „Digitaler Feudalismus“

Trotz des allgemeinen Enthusiasmus über das Fediverse werden nach wie vor bestehende Hierarchien zwischen Betreiber:innen und Nutzer:innen kritisiert.[111] Die Betreiber:innen werden mit „Herren“ aus der Feudalzeit verglichen, welche einen Dienst für ihre „Sklaven“ bereitstellen.[112] Schließlich sei ein Instanzwechsel nicht unbedingt einfach.[113] Es wird dennoch anerkannt, dass Moderator:innen im Fediverse wesentlich mehr Mühe und Arbeit haben als Feudalherren.[114] Da es sich um selbstregulierendes und emergentes System handelt, realisiere sich zwangsläufig das sogenannte Zipfsche Gesetz, nach dem wenige Server viele Nutzer:innen unterhalten.[115] Es lässt sich auch eine Konzentration auf wenige Hosting-Provider beobachten.[116] Dadurch ist die „digitale Autonomie“ im Fediverse gewissen Grenzen ausgesetzt.[117] Hoheit über die eigenen Daten kann schließlich nur durch den Betrieb einer eigenen Instanz erlangt werden. Dies setzt jedoch technische Fähigkeiten sowie finanzielle Mittel voraus, die in der Gesellschaft ungleich verteilt sind.[118] Die dezentrale Struktur hat allerdings den Vorteil, dass Data Mining wesentlich erschwert ist.[119]

11.4.2 Filterblasen und Echokammern

Es ist anerkannt, dass Online-Plattformen wie Facebook oder Twitter „Hate Speech“ und „Fake News“ befördern. Die Frage ist, ob das Fediverse strukturell bessere Bedingungen für Internetdiskussionen bietet. Dies liegt jedenfalls nahe, da die Anzeige der Inhalte nicht durch Empfehlungsalgorithmen manipuliert wird,[120] welche vor allem solche Beiträge bevorzugen, die besonders viel Reaktion in Form von Empörung provozieren. Gelegentlich wird die Kritik geäußert, dass die teilweise rigorosen Moderationspraktiken

111 *Lulamoon/Patton*, Software and Anarchy, Draft of April 17, 2021, https://applied-langua.ge/software-and-anarchy.pdf [Lulamoon/Patton], S. 36 ff.
112 *Lulamoon/Patton*, S. 37.
113 *Lulamoon/Patton*, S. 37.
114 *Lulamoon/Patton*, S. 38; *Zulli et al*., Rethinking the “social” in “social media”: Insights into topology, abstraction, and scale on the Mastodon social network, New media & society, 2020, Vol. 22 (7), 1188 (1200).
115 *Lulamoon/Patton*, S. 27 Fn. 6; Das „Zipfsche Gesetz“ spiegelt sich auch zu einem gewissen Grad in den Zahlen auf bspw. https://instances.social wieder.
116 *Raman et al*., S. 221 ff.; *Shaw*, S. 4.
117 *Lulamoon/Patton*, S. 37.
118 *Zulli et al.*, S. 1199 f.
119 *Raman et al*., S. 217; *Zulli et al*., S. 1197.
120 *Zulli et al.*, S. 1194.

im Fediverse „Filterblasen“ oder „Echokammern“ befördern, in denen nur noch mit Gleichgesinnten diskutiert wird.[121] Die Befürchtung, dass dadurch „Parallelnetzwerke“ entstehen, ist nicht unberechtigt. Es ist noch nicht hinreichend untersucht, ob eine Radikalisierung bestimmter Gruppen durch diese Struktur reduziert oder gefördert wird.[122] Andererseits kann das Fediverse eine ganz neue Perspektive auf diese Problematik eröffnen. Zum einen kann eine starke Moderation bestimmten marginalisierten Gruppen eine Teilhabe an sozialen Netzwerken überhaupt erst ermöglichen.[123] Zum anderen beruht die Föderation gerade auf den freiwilligen und selbstbestimmten Entscheidungen der Mitglieder.[124] Fediverse-Gemeinschaften können als „rekursive Öffentlichkeiten“ begriffen werden, in denen sowohl technische als auch soziale Diskursbedingungen ständig gemeinsam ausgehandelt werden.[125] Dadurch kann eine sehr viel größere Diversität erreicht werden als in den proprietären, zentralisierten sozialen Netzwerken.[126]

11.4.3 Dezentralisierung und Demokratisierung als Lösungsansätze

Ein Lösungsansatz für die angesprochenen Probleme besteht in einer noch dezentraleren Struktur. Es wäre wünschenswert, dass der Betrieb einer eigenen Fediverse-Instanz noch einfacher wird. Auch „Managed Hosting“-Angebote könnten ausgebaut werden. Interessant werden könnten auch Peer-to-Peer-Netzwerke wie das Projekt ScuttleButt.[127] Ein weiterer Vorschlag besteht darin, die Filterfunktionen der Nutzer:innen auszubauen, hin zu einer verteilten Moderation.[128] Bestehende soziale Probleme können jedoch durch Technik allein nicht gelöst werden.

Ein anderer Lösungsansatz liegt in der Demokratisierung oder Vergesellschaftung großer Instanzen. Vor allem hinsichtlich der Moderation wäre mehr Transparenz und Mitbestimmung durch die Nutzer:innen zu begrüßen.

---

121 *Zulli et al*., S. 1200; *Shaw*, S. 3.
122 *Zulli et al*., S. 1200 f.
123 Vgl. *Lulamoon/Patton*, S. 38.
124 *Boyle/Gehl/Zulli/Yang/Brow*n, The Promises, Problems and Possibilites for Alt-Networks, AoIR Selected Papers of Internet Research, 2021. https://doi.org/10.5210/spir.v2021i0.12090, S. 7 f.
125 *Kelty*, Two Bits, Durham/London 2008, S. 3, 7, 28 ff.; *Zulli et al*., S. 1194 f., 1198.
126 *Shaw*, S. 3.
127 https://scuttlebutt.nz/.
128 Es wird der Vorschlag des „collaborative filtering“ genannt, welches bisher vor im Target Advertising eingesetzt wird, *Dlorah*, A Parastatal problem, 2020, https://applied-langua.ge/posts/parastatal-problem.html.

Diese könnten demokratischer organisiert werden, indem sie von Vereinen oder Genossenschaften betrieben werden.[129]

11.5 Fazit: Lehren aus dem Fediverse

Die aufgeworfenen Rechtsfragen führen bei vielen Betreiber:innen von Fediverse-Instanzen zu Unsicherheit. Die Folgen sind teilweise gravierend: So hatte eine Betreiberin eine andere Instanz aufgrund ihrer Nutzungsregeln blockiert, die besagen: „don't do anything illegal, unless it's the moral thing to do." Es wäre wünschenswert, dass die juristische Diskussion zum Fediverse an Fahrt aufnimmt und Klarheit für Betreiber:innen schafft. Das Fediverse läuft teilweise „unter dem Radar" des Rechts. Aufgrund der dezentralen Struktur bestehen viele Probleme der „Walled Gardens" nicht.[130] Insbesondere verhindert die Interoperabilität zwischen Plattformen Lock-in-Effekte. Andererseits erfüllen große, beliebte Instanzen im Fediverse durchaus eine gewisse „Gatekeeper"-Funktion. Es ist daher auch nicht völlig unproblematisch, wenn Nutzer:innen völlig willkürlich gesperrt oder ganze Instanzen geblockt werden. Das Fediverse ist jedoch eindeutig ein Schritt hin zu mehr digitaler Autonomie. Der kooperative Charakter fordert viele Grundannahmen der Digitalwirtschaft heraus.[131] Darin zeigt sich die transformative Kraft des Fediverse, das durchaus als eine Art utopisches Experimentierfeld betrachtet werden kann.

129 Der Betrieb durch Städte, Gemeinden oder bestehende Organisationen würde auch eine nachhaltigere Finanzierung des Fediverse ermöglichen, siehe *Hasecke*, Fediverse und Selbstorganisation, Free and Open Source Software Conference (FrOSCon) 2022, https://media.ccc.de/v/froscon2022-2763-fediverse_und_selbstorganisation.

130 Vgl. *La Cava/Greco/Tagarelli*, Understanding the growth of the Fediverse through the lens of Mastodon, Appl Netw Sci (2021) 6:64, 20, 31.

131 Zum Beispiel wird auch die Bedeutung von Nutzer:innenzahlen für den Erfolg eines sozialen Netzwerks hinterfragt: *Zulli et al.,* S. 1195.

12 NFT – Just another Buzzword oder neue Chancen für den Kunst- und Filmmarkt?

*Christiane Stützle, Patricia Ernst & Susan Bischoff**

NFT – Ist das Kunst oder kann das weg? Non-fungible Token sind seit dem vergangenen Jahr in aller Munde. Doch im gleißenden Licht ihres popkulturellen Erfolges wird nur selten erkennbar, welche Verwertungs- und Nutzungsmöglichkeiten sich tatsächlich hinter diesem Blockchain-Gut verbergen. Dieser Beitrag untersucht die aus den technischen Grundlagen von NFTs folgenden, neuen Möglichkeiten für die Kreativbranche mit einem Fokus auf urheberrechtliche Fragestellungen. Dabei werden auch erste Rechtsstreitigkeiten vorgestellt, die hervorheben, wie viele rechtliche Unklarheiten im Themenkomplex „NFT" gegenwärtig noch bestehen.

12.1 Einleitung

Metaverse, Krypto, New Digital Economy, DAO, Blockchain – die vermeintlich bevorstehende Verlagerung des Lebensmittelpunkts in das Web 3.0 wird von einer Reihe vielversprechender Buzzwords begleitet. Zu diesen gehört auch das Akronym NFT, das sich mittlerweile größerer Bekanntheit erfreut.

NFT steht für Non-fungible Token, also für eine nicht austauschbare Wertmarke. Die Wertmarke, der Token, repräsentiert einen Vermögenswert, typischerweise einen digitalen oder digitalisierten Inhalt wie eine Grafik oder ein Video, aber auch physische Güter wie eine Skulptur oder eine Immobilie. Diese Repräsentation eines Vermögenswertes erfolgt durch einen Datensatz auf einer Blockchain, der den Inhaber der dort hinterlegten Krypto-Wallet als den Inhaber des NFT – nicht aber des tokenisierten Vermögenswertes – ausweist. Non-fungible, also nicht austauschbar, sind diese Token deshalb, weil sie nicht teilbar und zugleich einmalig sind, denn sie existieren in ihrer konkreten Form stets nur einmal auf der Blockchain.[1] NFTs sind daher einzigartig, sie erhalten und steigern ihren Wert allein durch Handel.[2] Anders verhält es sich bei Fungible Token, etwa bei Kryptowährungen. Ein

* Mehr über die Autorinnen erfahren Sie im Autor:innenhinweis auf S. 224 ff.

1 Der Einzigartigkeit eines jeden NFT steht nicht entgegen, dass ein NFT in einer gewissen Auflage verwertet werden kann. Handelt es sich bei dem NFT nicht um ein Unikat, dann wird von dem tokenisierten Vermögenswert eine der gewählten Auflage entsprechende Stückzahl von NFTs generiert, wobei jedes für sich durch die auf der Blockchain hinterlegten Informationen (zu diesen unter 12.3.3) einzigartig ist.

2 *Hoeren/Prinz*, CR 2021, 565 (566).

Bitcoin ist beliebig durch einen anderen Bitcoin austauschbar, denn beiden wird derselbe Wert zugeordnet. Diese Differenzierung existiert indes auch in der analogen Welt. Während Geldscheine des gleichen Wertes oder Goldbarren gleichen Gewichts beliebig austauschbar sind, sind es Immobilien oder Kunstwerke nicht.

12.2 Der Aufstieg – und Fall? – von NFTs

NFTs sind längst im Mainstream angekommen. Um ein Nischenthema für besonders Technik- und Digitalaffine handelt es sich schon länger nicht mehr. Dies zeigt nicht zuletzt der NFT-Handel in traditionellen Auktionshäusern wie *Sotheby's* oder *Christie's*,[3] das Endorsement durch Prominente und Kollaborationen globaler Marken[4] sowie die Kür als „Wort des Jahres 2021" durch das *Collins Dictionary*[5].

Die wirtschaftlichen Zahlen sind auch durchaus beeindruckend. Mit Beginn des Jahres 2021 nahm der NFT-Handel deutlich an Volumen zu. Der breiteren Öffentlichkeit dürfte das Thema spätestens im März des vergangenen Jahres durch die Versteigerung eines NFT an der Digitalgrafik „Everydays: The First 5000 Days" von Mike Winkelmann (Künstlername *Beeple*) über *Christie's* für gut 69 Millionen USD bekannt geworden sein.[6] Das tokeni-

3 Christie's verzeichnete im Jahr 2021 NFT-Verkäufe über insgesamt 150 Millionen USD, wovon die Hälfte auf eine einzige Versteigerung entfiel (von „Everydays", dazu sogleich): Artnet News, Boosted by Private Sales and NFTs, Christie's Brought in a Total of $7.1 Billion in 2021 – Its Best Results in Five Years (20.12.2021), verfügbar unter: https://news.artnet.com/market/christies-reports-2021-results-best-five-years-2052122 (alle Links sind zuletzt am 23.8.2022 abgerufen worden). NFT-Versteigerungen über Sotheby's generierten 2021 insgesamt 100 Millionen USD, außerdem erreichte das Auktionshaus auch dank seiner separaten Plattform „Sotheby's Metaverse" (https://metaverse.sothebys.com) eine Vielzahl neuer, junger Kunden: Bloomberg, Sotheby's Makes $100 Million in NFT Sales With Younger Audience (15.12.2021), verfügbar unter: https://www.bloomberg.com/news/articles/2021-12-15/sotheby-s-makes-100-million-in-nft-sales-with-younger-audience.

4 So haben beispielsweise Justin Bieber, Madonna, Snoop Dogg, Eminem, Jimmy Fallon, Serena Williams und Shaquille O'Neal verlautbaren lassen, Inhaber von Bored Apes-NFTs zu sein, vgl. Klage von Yuga Labs, Inc. gegen Ryder Ripps u. a. vom 24.6.2022 vor dem U. S. District Court Central District of California, Case-No. 2:22-cv-04355 (zu diesem Verfahren unter 12.3.3.2.4), S. 7, verfügbar unter: https://tmsnrt.rs/3Nk3d9b (über Reuters, https://www.reuters.com/legal/transactional/bored-ape-nft-maker-yuga-labs-sues-artist-claiming-he-copied-tokens-2022-06-27/). Mit eben diesen Bored Apes haben bekannte Marken und Unternehmen wie Adidas und Universal Music Group zusammengearbeitet, vgl. Yuga Labs Klage, a. a. O., S. 8.

5 https://www.collinsdictionary.com/de/woty.

6 Eine Abbildung sowie Informationen über das Kunstwerk und den Künstler finden sich auf https://onlineonly.christies.com/s/beeple-first-5000-days/beeple-b-1981-1/112924.

sierte Werk besteht aus 5000 Einzelbildern, die der Künstler, der vor dieser Rekordversteigerung nie eine Einzelausstellung gehabt hatte, seit 2007 täglich auf seinem *Instagram*-Account veröffentlichte. Bei dem Käufer des NFT handelt es sich um einen Investmentfonds namens „Metapurse", der sich für seine NFT-Schätze sogleich von einem auf digitale Räume spezialisierten Designer ein virtuelles Museum hatte bauen lassen.[7] Einen weiteren Rekord stellte der Verkauf von knapp 313000 einzelnen NFTs an der Digitalkreation „Merge" von *Pak* im Dezember 2021 über die NFT-Plattform *Nifty Gateway* auf.[8] Mit dem Gesamterlös von 91,8 Millionen USD überholt „Merge" den bislang höchsten Verkaufserlös für ein Kunstwerk eines lebenden Künstlers, „Rabbit" von *Jeff Koons* (91 Millionen USD).[9]

Im Nachgang der ersten spektakulären Verkäufe digitaler Künstler:innen begannen auch Museen, NFTs an ihren physischen Bestandswerken zu verkaufen. So hat beispielsweise das *British Museum* unlängst NFTs an 20 Gemälden von *William Turner* versteigert.[10] Dies war sowohl für das Museum, als auch für Sammler:innen deshalb besonders interessant, weil diese Gemälde ausweislich der Nachlassbedingungen jeweils nur für wenige Wochen gezeigt und niemals verliehen werden dürfen.[11] Viele Museen dürften die neuartigen Verwertungsmöglichkeiten an Werken von Meistern wie *Monet*, *van Gogh* oder *Klimt* genutzt haben, um pandemiebedingte Einnahmeverluste zu kompensieren.[12]

---

7 The Art Newspaper, Virtual museum to be built to house Beeple's record-breaking digital work (13.3.2021), verfügbar unter: https://www.theartnewspaper.com/2021/03/13/virtual-museum-to-be-built-to-house-beeples-record-breaking-digital-work.

8 Informationen zum Kunstwerk und Verkauf finden sich auf https://www.niftygateway.com/collections/pakmerge.

9 Mit Blick auf die Generierung des Verkaufspreises durch hunderttausende Einzeltransaktionen lässt sich allerdings darüber streiten, ob „Merge" dieses Ranking tatsächlich verdient.

10 Informationen zum Verkauf finden sich auf https://www.lacollection.io/nft-marketplace.

11 Tatler, The British Museum to auction NFTs of famed works by JMW Turner (21.1.2022), verfügbar unter: https://www.tatler.com/article/british-museum-turner-nfts-auction-lacollection.

12 Vgl. etwa Verkauf von NFTs an Werken u. a. von da Vinci, van Gogh, Kandinsky und Monet durch das Hermitage Museum (Saint Petersburg): https://www.binance.com/en/nft/events/winterpalace; an Klimt's „Der Kuss" durch das Belvedere (Potsdam): https://thekiss.art/s/about.html. Kürzlich sind die Museen in Italien vom zuständigen Minister allerdings angewiesen worden, vorübergehend keine NFT-Aktionen unter Zusammenarbeit mit Drittanbietern durchzuführen: Artnet News, Italy Instructs Museums to Halt Contracts With NFT Companies, Citing 'Unregulated' Terms That Could Affect the Country's Cultural Heritage (11.7.2022), verfügbar unter: https://news.artnet.com/market/cinello-nft-michaelangelo-2145003.

Das Gesamtvolumen des NFT-Handels wird für das Jahr 2021, je nach den zu Grunde gelegten Daten, auf bis zu 25 Milliarden USD beziffert.[13] Sowohl in der traditionellen Presse, als auch in den sozialen Medien wurde dennoch zuletzt bereits der Abgesang auf NFTs eingeläutet.[14] Dies steht nicht zuletzt im Zusammenhang mit dem allgemeinen Crash von Kryptowährungen im Frühjahr 2022, der den Wert von mit Kryptowährungen gehandelten und somit höchst volatilen NFTs regelrecht pulverisierte.[15] Auch unabhängig hiervon scheint die Nachfrage an NFTs abzunehmen: Das Verkaufsvolumen ist seit Anfang des Jahres um 75 Prozent zurückgegangen.[16] Ein NFT an dem ersten Tweet von Twitter-Gründer *Jack Dorsey* etwa wurde im März 2021 für 2,9 Millionen USD verkauft, gegenwärtig liegt das Höchstgebot bei gerade einmal 422 USD.[17] Der Floor-Preis der beliebten NFT-Kollektion „Bored Apes Yacht Club", also der Preis für das günstigste NFT aus der Sammlung, rutschte von über 420000 USD im Mai 2022 auf unter 90000 USD im Juni und bewegt sich gegenwärtig bei etwa 108000 USD.[18]

In diese angespannte Stimmungslage hinein spielen auch die vermehrten Meldungen von NFT-"Hacks", zu denen beeindruckend hohe Verlustsummen vermeldet werden.[19] Das ist bemerkenswert, da NFTs von dem Ver-

13 Reuters, NFT sales hit $25 billion in 2021, but growth shows signs of slowing (11.1.2022), verfügbar unter: https://www.reuters.com/markets/europe/nft-sales-hit-25-billion-2021-growth-shows-signs-slowing-2022-01-10/.

14 Vgl. nur beispielhaft Deutschlandfunk Kultur, Das Problem mit dem Hype (2.4.2022), verfügbar unter: https://www.deutschlandfunkkultur.de/debatte-um-zukunft-von-kryptotechnologie-100.html; Handelszeitung, Warum der NFT-Markt zusammenbrechen wird (28.1.2022), verfügbar unter: https://www.handelszeitung.ch/geld/warum-der-nft-markt-zusammenbrechen-wird; grundsätzlich kritisch Süddeutsche Zeitung, NFTs – die große Kapitalismus-Parodie (10.2.2022), verfügbar unter: https://www.sueddeutsche.de/wirtschaft/digitale-wertgegenstaende-nfts-die-grosse-kapitalismus-parodie-1.5526123; grundsätzlich kritisch ob des „Web 3.0"-Versprechens The New York Times, What Is Happening to the People Falling for Crypto and NFTs (5.5.2022), verfügbar unter: https://www.nytimes.com/2022/05/05/opinion/crypto-nfts-web3.html.

15 Ein Ether (die Cryptowährungseinheit auf der Ethereum-Blockchain) erreichte im November 2021 einen Wert von über 4.000 Euro, entsprach im Juni 2022 aber nur noch 950 Euro.

16 TechCrunch, The NFT slump is real (8.6.2022), verfügbar unter: https://tcrn.ch/3H3AqnO.

17 Initialer Verkauf einsehbar unter https://v.cent.co/tweet/20; aktuelle Gebote für das NFT unter https://opensea.io/assets/matic/0x28009881f0ffe85c90725b8b02be55773647c64a/20.

18 Stand 22.8.2022, für historische und aktuelle Floor-Preise vgl. https://nftpricefloor.com/bored-ape-yacht-club. Zu den Bored Apes unter 12.3.3.2.4 und 12.4.2.3.

19 Vgl. nur t3n, Discord-Hacker klauten NFT-Projekten allein im Mai 22 Millionen Dollar (1.8.2022), verfügbar unter: https://t3n.de/news/discord-hacker-klauen-bored-apes-nft-1489029/; Vice, Hacker Steals $1.4 Million in NFTs From Collector In One Sweep (25.5.2022), verfügbar unter: https://www.vice.com/en/article/pkp7pm/hacker-

sprechen leben, dass ihre zu Grunde liegende Technologie unkorrumpierbar sei. Tatsächlich nutzten die bisherigen Hacks durch Social Engineering und Phishing-Attacken auch stets die Schwachstelle Mensch aus.[20]

Trotz dieser negativen Schlagzeilen setzt sich die Technologie sukzessive aufgrund ihrer neuartigen Nutzungs- und Vertriebsform am Markt durch. Eine Großzahl relevanter Unternehmen aus der Kreativindustrie beschäftigt sich gegenwärtig auf die eine oder andere Weise mit dem Thema und lotet Einsatzmöglichkeiten aus. Diese hängen maßgeblich von der rechtlichen Einordnung des Phänomens NFT und den Chancen dieser neuen Technologie ab.

12.3 Die Chancen stecken im Detail: Technische Grundlagen und Funktionsweisen von NFTs

Die digitalen Eigenarten und technischen Ausgestaltungen von NFTs und ihrem Handel erlauben Kreativen neue Formen der finanziellen Verwertung ihres Schaffens und mitunter auch ansprechendere Nutzungsmöglichkeiten für Erwerber:innen. Eine Erörterung der technischen Grundlagen ist daher unabdingbar.

12.3.1 Vorbereitung zur Herstellung eines NFT

Einleitend ist festzuhalten, dass NFTs ebenso wie Kryptowährungen auf der Blockchain-Technologie, also dezentralisierten Datenbankensystemen, basieren. NFTs finden beinahe ausnahmslos auf der Ethereum-Blockchain statt, was insbesondere in ihrer Smart-Contract-Kompatibilität begründet liegt, hierzu sogleich. Dieser Beitrag wird am Beispiel einer fiktiven Künstlerin die NFT-Funktionsweise beim Verkauf eines Kunstwerks erläutern. Bei dem Kunstwerk kann es sich etwa um ein ursprünglich physisches Gemälde oder auch um einen originär digitalen Inhalt wie eine Grafik handeln. Die

steals-dollar14-million-in-nfts-from-collector-in-one-sweep; The Verge, $1.7 million in NFTs stolen in apparent phishing attack on OpenSea users (20.2.2022), verfügbar unter: https://www.theverge.com/2022/2/20/22943228/opensea-phishing-hack-smart-contract-bug-stolen-nft.

20 Eine mögliche, soweit ersichtlich einzige, Ausnahme hiervon könnte die sog. „Sleepminting"-Attacke auf Beeple's „Everydays"-NFT im April 2021 gewesen sein. Dabei soll für das „Unterjubeln" des NFT-Klons in die Wallet des vermeintlichen Erstellers Beeple eine Schwachstelle des Smart Contract-Standards ERC721 ausgenutzt worden sein, allerdings ist unklar, ob dies wirklich möglich ist, vgl. Artnet News, The Gray Market: How a Brazen Hack of That $69 Million Beeple Revealed the True Vulnerability of the NFT Market (and Other Insights) (21.4.2021), verfügbar unter: https://news.artnet.com/opinion/sleepminting-nftheft-monsieur-personne-1960744.

Künstlerin kann, das entsprechende technische Knowhow vorausgesetzt, das NFT nun selbst erstellen oder hierfür auf eine der mittlerweile zahlreichen Plattformen zurückgreifen, die häufig zugleich auch als NFT-Handelsplätze fungieren.[21] Der „Herstellungsprozess" des NFT auf der Blockchain ist aber in jedem Fall derselbe.[22]

Bei Verwendung einer Plattform, welche eine NFT-Erstellung in wenigen Schritten ermöglicht, verknüpft die Künstlerin zunächst ihre Krypto-Wallet mit dieser Website. Dabei handelt es sich, wie der Begriff bereits verrät, gewissermaßen um ein Äquivalent der analogen Geldbörse für Kryptowerte wie Kryptowährungen oder NFT. Allerdings enthält die Krypto-Wallet den Kryptowert selbst nicht, sondern lediglich die Schlüssel (Keys), also den Code für den Zugriff auf diese Werte. Während ein solcher Speicherort grundsätzlich auch körperlicher Natur, etwa in Form eines USB-Stick-ähnlichen Ledger oder schlicht ein Stück Papier, sein kann, setzt die Nutzung von NFT-Handelsplattformen die Verknüpfung mit einer von spezifischen Anbietern bereitgestellten, browser- oder App-basierten Crypto-Wallet voraus. Über eine solche entrichtet die Künstlerin sodann die für die Einrichtung ihres Profils und für die folgenden Transaktionen anfallenden Gebühren (sog. „gas fees") in der jeweiligen Kryptowährung der verwendeten Blockchain. Für die ganz überwiegend auf der Ethereum-Blockchain gehandelten NFTs sind diese Gebühren in der Kryptowährung Ether zu entrichten. Dann lädt die Künstlerin ihr digitales „Asset", das durch das NFT tokenisiert werden soll, also etwa eine .JPEG, .GIF oder .MP4-Datei, auf die Plattform hoch und gibt gegebenenfalls noch einen Link an, über welchen Kaufinteressenten Informationen über das verknüpfte Werk und die Künstlerin erhalten können. Ferner kann die Künstlerin festlegen, in welcher Auflage (Scarcety) das NFT verfügbar sein soll.

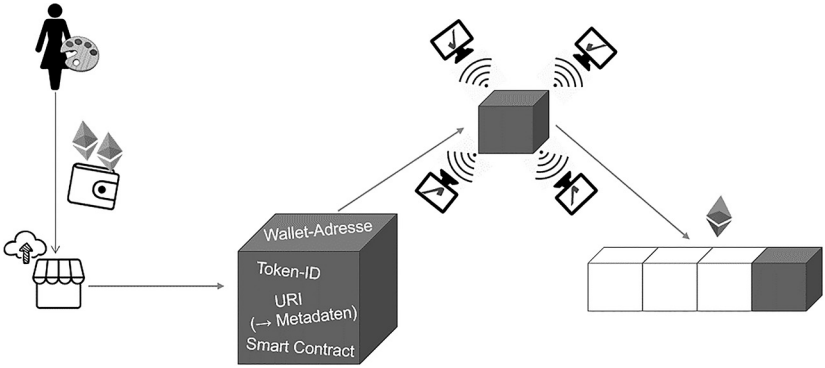
12.3.2 Der Herstellungsprozess: Minten eines NFT

Nun kann der NFT-Herstellungsprozess beginnen. Dieser wird, wie die „Schaffung" von Kryptowährungseinheiten, in Anlehnung an das Prägen von Münzen als „Minten" bezeichnet. Hierfür wird ein Datensatz, ein Block, erstellt, der die betreffenden Transaktionsdaten enthält. Dieser Block wird sodann wie bei einer jeden Transaktion auf einer Blockchain dezentral durch eine Vielzahl von Rechnern, den „Nodes", kollektiv verifiziert. Die an der Lösung des algorithmischen Rätsels erfolgreich beteiligten „Miner" erhalten eine Belohnung, die aus den gezahlten „gas fees" bereitgestellt wird.

---

21 Zu den einzelnen Unterkategorien solcher Plattformen (offene Marktplätze; kollektionsbasierte Marktplätze; kuratierte Marktplätze) *Bodó u.* a., E. I.P. R. 2022, 267 (270 f.).

22 Zu diesem Prozess umfassend *Guadamuz*, JIPLP 2021, 1 (2 ff.).



Dieses „Proof of Work"-Verfahren und die dezentrale Speicherung der gesamten Blockchain auf allen Nodes gewährleisten die Manipulationssicherheit der Blockchain-Technologie. Böswillige Interventionen sind technisch denkbar, werden mit zunehmendem Umfang einer Blockchain aber unattraktiver.[23] Der kollektiv verifizierte Datensatz wird mit der bestehenden Blockchain verknüpft, mithin unveränderlich auf ihr festgeschrieben, und die derart ergänzte Blockchain auf allen Nodes gespeichert. Dieses Verfahren, also die Festschreibung der Transaktionsinformationen in einem Block, seine dezentrale Verifikation und Verkettung mit der Blockchain, findet schließlich auch bei jeder folgenden NFT-Transaktion, mithin bei jedem Verkauf des NFT statt. Die Transaktionsdaten, d. h. wer (respektive welches Pseudonym) wem wann für wie viele Ether welches NFT übertragen hat, sind stets und von jedermann einsehbar. Von vielen wird dies als großer Vorteil im Sinne der Transparenz, Nachvollziehbarkeit und damit Schaffung einer digitalen Provenienz, bspw. für Kunstwerke, eingeordnet.[24]

Anzumerken ist, dass das „Proof of Work"-Verfahren durch die benötigten Rechnerkapazitäten einen sehr hohen Energiebedarf erfordert. Dieser Energiebedarf steigt stetig weiter, da die Blockchain durch weitere Transaktionen immer umfangreicher wird. Zum Vergleich: allein das Minten auf der

23 Das „Proof of Work"-Verfahren erlaubt eine gewisse Manipulation durch eine Gruppe von Minern, die mehr als 50 Prozent der Gesamtrechenleistung des Netzwerks kontrolliert (sog. „51 % attack"), wovon auch schon mehrere Blockchains betroffen waren, vgl. MIT Digital Currency Initiative, https://dci.mit.edu/51-attacks. Gegenwärtig würde es Angreifern etwa 950.000 USD pro Stunde kosten, um genügend Rechenleistung (Hashing Power) für eine solche Attacke auf die Ethereum-Blockchain bereitzustellen. Zum technisch bislang uneindeutigen Sleepminting vgl. Fn. 20.

24 Vgl. *Hoeren/Prinz*, CR 2021, 565 (566, 567). Dazu auch unter 12.4.2.4.

Ethereum-Blockchain benötigt im Jahr mehr Energie als ganz Irland,[25] der CO_2-Abdruck dieser Blockchain entspricht in etwa dem von Norwegen.[26] Zwar ist dieser Verbrauch nicht allein NFTs zuzuschreiben, da auch die Kryptowährung Ether auf dieser Blockchain existiert und transferiert wird. Neuste Untersuchungen geben allerdings an, dass allein das Minten eines NFT im Schnitt etwa 83 Kilogramm CO_2 verbraucht, wobei jedes Gebot, jeder Verkauf, jede Transaktion erneut Emissionen generiert.[27] Die Transaktion eines frisch geminteten, an das erste Gebot verkauften NFT verursacht damit deutlich mehr CO_2 als eine Flugreise von München nach Berlin.[28] Bemühungen um umweltschonendere Alternativen sind daher in jedem Fall dringend erforderlich, soll der NFT-Handel eine Zukunft haben.[29]

12.3.3 Der Inhalt eines NFT-Datensatzes auf der Blockchain

Ein NFT ist daher lediglich eine einzigartige digitale Wertmarke für einen Vermögenswert (Asset), die auf der Blockchain hinterlegt ist. Insbesondere ist das NFT kein urheberrechtliches Werk im Sinne des § 2 Abs. 2 UrhG. Es entsteht vielmehr eine Art verbrieftes digitales „Original" des mit dem NFT verknüpften Inhalts. Einen solchen Exklusivitäts- und Originalitätsstempel kennt der digitale Raum sonst nicht. Die Besonderheiten der rechtlichen Bewertung von NFTs und die Chancen aus dem NFT-Handel folgen indes aus den im generierten Blockchain-Datensatz enthaltenen Informationen.

---

25 *Truby u. a.*, Blockchain, climate damage, and death: Policy interventions to reduce the carbon emissions, mortality, and net-zero implications of non-fungible tokens and Bitcoin, Energy Research & Social Science 2022, S. 4, verfügbar unter: https://doi.org/10.1016/j.erss.2022.102499; TIME, Digital NFT Art Is Booming—But at What Cost? (18.3.2021), verfügbar unter: https://time.com/5947911/nft-environmental-toll/.

26 Digiconomist, Ethereum Energy Consumption Index, verfügbar unter: https://digiconomist.net/ethereum-energy-consumption.

27 Monopol Magazin, Mit Feuer gegen Feuer (1.6.2022), verfügbar unter: https://www.monopol-magazin.de/mit-feuer-gegen-feuer-kuenstler-kyle-mcdonald-will-nft-emissionen-mit-nfts-kompensieren, unter Bezugnahme auf eine Studie des Branchendienstes NFT Club (https://nftclub.com/eco-impact-of-nfts/).

28 Unter Zugrundelegung der in den Quellen von Fn. 27 angegebenen Verbrauchsdaten aus 83 kg CO2 für das Minten, 23 kg CO2 für das Gebot, 51 kg CO2 für den Verkauf und 30 kg CO2 für den Transfer ergibt sich ein CO2-Ausstoß von 187 kg, dem Emissionen von etwa 154 kg CO2 pro Person für einen Flug zwischen München und Berlin (zu berechnen etwa über https://www.atmosfair.de/de/kompensieren/flug/) entgegenstehen.

29 Als nächster Schritt ist dabei die Umstellung vom „Proof-of-Work"- auf das „Proof-of-Stake"-Verfahren zu erwarten, der für die Ethereum-Blockchain noch in diesem Jahr realisiert werden soll, vgl. hierzu und zur dadurch veränderten Funktionsweise TIME, Proof of Work vs. Proof of Stake: Ethereum's Recent Price Surge Shows Why the Difference Matters (29.7.2022), verfügbar unter: https://time.com/nextadvisor/investing/cryptocurrency/proof-of-work-vs-proof-of-stake/.

12.3.3.1 Token-ID, Krypto-Wallet

Der Datensatz enthält zum einen die „Token ID", die das NFT unmissverständlich und einzigartig ausweist, sowie eine Verknüpfung mit der Krypto-Wallet-Adresse des NFT-Erstellers beziehungsweise später des letzten Erwerbers. Allein die Person, die faktischen Zugang zu dieser Wallet hat, kann daher auf das NFT zugreifen und es weiterübertragen.

12.3.3.2 Verweis auf Metadaten: Urheberrechtliche Implikationen & erste Rechtsverfahren

Im Blockchain-Datensatz eines NFT findet sich ferner ein Verweis auf Metadaten zur genauen Definition des tokenisierten Inhalts in Form eines URI (Universal Resource Identifier). Dieser URI besteht entweder aus einem Verweis auf eine klassische URL, also einem Link auf eine Website, auf welcher sich die Darstellung des tokenisierten Inhalts, etwa einer Grafik, findet. Üblicher ist es jedoch aus Gründen der Speicherungssicherheit, einen URI-Verweis auf einen IPFS (Interplanetary File System) Hash zu verwenden. Dabei handelt es sich um eine Art digitalen Fingerabdruck für dezentral gespeicherte Inhalte.[30] Über den URI-Verweis wird das NFT mit dem repräsentierten, tokenisierten Inhalt verknüpft. Der NFT-Datensatz auf der Blockchain enthält daher in aller Regel – mit der prominenten Ausnahme von *Pak*'s „Merge"[31]– den tokenisierten Inhalt selbst nicht, dieser wird vielmehr außerhalb der Blockchain (off-chain) gespeichert. Eine Speicherung im Blockchain-Datensatz wäre zwar möglich, entsprechende Bild-, Ton- oder Videodateien sind aber zu groß, als dass ihre Speicherung in der Blockchain wirtschaftlich effizient wäre. Denn die für eine Tokenisierung eines Kinofilms mit Speicherung der gesamten Filmdatei im Datensatz benötigten „gas fees" würden die Produktionskosten des Films bei weitem übersteigen.

An dieser Stelle sind zwei Aspekte hervorzuheben.

Zum einen zeigt sich, dass das NFT in seiner technischen „Existenz" als Datensatz auf der Blockchain unabhängig von dem durch die Wertmarke repräsentierten Vermögenswert ist. Dieser wird lediglich extern verlinkt und nicht selbst abgebildet. Folge ist, dass das NFT als Wertmarke funktions- und denkbar wertlos wird, wenn der verknüpfte Inhalt an der in der Blockchain gespeicherten Fundstelle nicht mehr aufrufbar ist.

---

30 *Hoeren/Prinz*, CR 2021, 565 (566).

31 Bei „Merge" wird das Kunstwerk – oder genauer: werden die einzelnen Teile der Gesamtgrafik – dynamisch (d. h., die Visualisierung wird mit Erwerb weiterer NFTs schrittweise „größer") durch den Smart Contract (zu diesem sogleich unter 12.3.3.3), also on-chain, erzeugt, vgl. https://www.niftygateway.com/collections/pakmerge.

Zum anderen wirkt sich diese Referenzlösung auch auf die urheberrechtliche Bewertung aus. Selbst wenn das NFT ein urheberrechtliches Werk, wie eine Skulptur, ein Buch oder eine Digitalgrafik tokenisiert, sind das Minten eines NFT und seine „Übertragung" urheberrechtlich nicht relevant, denn das Werk bzw. seine Vervielfältigung wird im Blockchain-Datensatz nicht wiedergegeben. In anderen Worten: Mintet eine Person ein NFT an einem urheberrechtlich geschützten Werk, ohne Urheber oder abgeleiteter Rechteinhaber an diesem zu sein, so kann der Urheber hiergegen in der Regel nicht aus dem Urheberrecht vorgehen. Denn aufgrund der Off-chain-Speicherung des Werks beziehungsweise seiner Vervielfältigung kommt eine Urheberrechtsverletzung nur unter dem Gesichtspunkt der Linkhaftung in Betracht, die vor dem Hintergrund der ausdifferenzierten EuGH-Kasuistik nur in wenigen Sachverhaltskonstellationen vorliegen wird.[32] Das wäre insbesondere dann der Fall, wenn die Abbildung zuvor nicht oder etwa nur hinter einer Paywall verfügbar war, aber nun durch die NFT-Verlinkung allgemein öffentlich verfügbar gemacht würde.

Urhebern und urheberrechtlichen Rechteinhabern erscheint das Minten und Veräußern von NFTs an ihren Werken durch Dritte dennoch als unbefugtes Verwerten und Monetarisieren ihres Schaffens. In der Praxis wird solchen Sachverhalten auf unterschiedlichen Wegen begegnet.

12.3.3.2.1 Öffentliche Distanzierung: Fall Picasso-Erben

Die erste Möglichkeit kommt ohne eine Inanspruchnahme konkreter Rechtspositionen aus und besteht in einer öffentlichen Distanzierung von dem NFT. Hierdurch wird, ist der Urheber öffentlich bekannt, dem NFT das Originalitätsversprechen und damit seine Sammlerrelevanz faktisch entzogen. Diesen Weg beschritt die Nachlassgemeinschaft von *Pablo Picasso*, als im Januar dieses Jahres zwei der Erben die weltweit ersten *Picasso*-NFTs ankündigten.[33] Die Nachlassgemeinschaft, welche alle Rechte an *Picasso*'s

32 Hierzu insbesondere EuGH, Urt. v. 13.2.2014 – C-466/12 – Svensson, GRUR 2014, 360; Beschl. v. 21.10.2014 – C-348/13 – BestWater, GRUR 2014, 1196; Urt. v. 8.9.2016 – C-160/15 – GS Media, GRUR 2016, 1152; Urt. v. 7.8.2018 – C-161/17 – Cordoba, GRUR 2018, 911; Urt. v. 9.3.2021 – C-392/19 – VG Bild-Kunst, GRUR 2021, 706; *Dreier*, in: Dreier/Schulze, Urheberrechtsgesetz 7. Auflage 2022, UrhG § 19a Rn. 6b. Mit Blick auf NFTs *Guadamuz*, JIPLP 2021, 1 (14 ff.) zum EU- und UK-Recht; *Bodó u. a.*, E. I.P. R. 2022, 267 (277 f.). Zur Einordnung in das U. S.-amerikanisches Urheberrecht, dort eine Urheberrechtsverletzung durch bloße Verlinkung ablehnend *Behzadi*, The Fiction of NFTs and Copyright Infringement (2022), S. 4 f., verfügbar unter: https://ssrn.com/abstract=4025604.

33 Artnet News, Picasso's Granddaughter and Her DJ Son Want to Mint 1,010 NFTs Based on the Artist's Work. The Rest of the Family Is Not Having It (27.1.2022), verfügbar unter: https://news.artnet.com/market/picasso-nft-2064495; After Pushback From the Picasso Estate, the Artist's Great-Grandson's NFT Sale Is…a Bit of a Flop (7.2.2022),

Werken verwaltet, distanzierte sich öffentlichkeitswirksam von dem Projekt und bezeichnete vorsorglich alle NFTs als „Fälschungen". Die NFTs wurden ab Februar 2022 zum Kauf angeboten, die beteiligte NFT-Handelsplattform versah die Auktionen allerdings von sich aus mit dem Hinweis, dass die NFTs „*not related to Pablo Picasso, his name, and his work*" seien.[34] Nichtsdestotrotz fanden die NFTs ihre Käufer, Sondereditionen wechselten für bis zu 41000 USD den Inhaber. Freilich ist kaum abzuschätzen, welchen Verkaufspreis die NFTs ohne eine derartige ausdrückliche Distanzierung durch die *Picasso*-Marke erzielt hätten.

12.3.3.2.2 Einschreiten der NFT-Plattformen: Fall Stormtrooper Helme

Eine außerrechtliche Lösung steht auch im Mittelpunkt des Verkaufs von NFTs eines Londoner Kurators an *Stormtrooper* Helmen, die Jahre zuvor in dem von ihm organisierten Projekt „Art Wars" von bekannten Künstlern wie *Damien Hirst* und *David Bailey* künstlerisch gestaltet worden waren.[35] Angeboten wurden gut 1100 NFTs, von denen etwa 100 auf Fotografien der betreffenden Helme verlinkten. Die Künstler waren vorab lediglich über einen Newsletter über das NFT-Projekt informiert worden. *Damien Hirst* intervenierte bereits vor Beginn der NFT-Auktion, sodass die seinen Helm betreffenden NFTs nicht zum Verkauf gelangten.[36] In Folge der Beschwerden der übrigen Künstler sperrte die Plattform *OpenSea* schließlich alle übrigen NFTs. Da diese aber teilweise bereits verkauft worden waren, blieben den neuen Inhabern, so ein enttäuschter Käufer, „*NFTs with no value and no future perspective*".[37] Nicht öffentlich bekannt wurde, ob sich die Künstler auf der Grundlage einer konkreten Rechtsposition gegen diesen NFT-Verkauf wandten. Von *Hirst*'s Rechtsvertretung war lediglich zu vernehmen, dass der NFT-Ersteller nicht Rechteinhaber der Helmwerke sei und auch keine „Lizenz" zur Herstellung der NFTs habe.[38] Wie soeben erörtert,

---

verfügbar unter: https://news.artnet.com/market/florian-picasso-sells-nfts-with-accompanying-single-john-legend-nas-2069352.

34 https://www.niftygateway.com/collections/picasso.

35 https://artwars.net/.

36 The Art Newspaper, 'May the image rights be with you': Artists claim Art Wars sold NFTs linked to their designs for Stormtrooper helmets without their permission (23.11.2021), verfügbar unter: https://www.theartnewspaper.com/2021/11/23/artists-claim-art-wars-sold-nfts-linked-to-their-art-for-millions-allegedly-without-their-permission.

37 The Art Newspaper, 'We hold NFTs with no value and no future perspective': aggrieved Art Wars NFT investors speak out over dispute (17.2.2022), verfügbar unter: https://www.theartnewspaper.com/2022/02/17/aggrieved-art-wars-nft-investors-speak-out-over-dispute.

38 S. Fn. 36.

scheidet eine Urheberrechtsverletzung und damit auch jede Frage nach einer Nutzungslizenz des NFT-Erstellers aber aus, sofern sich die Abbildungen der Helme nur als urheberrechtlich irrelevante Linkreferenzen in den NFT-Datensätzen finden. Zu denken wäre daher eher an marken- und wettbewerbsrechtliche Ansprüche, da die NFTs unter ausdrücklicher Verwendung von und in Bezugnahme auf die Namen der Künstler der physischen Helmwerke vermarktet wurden. Soweit ersichtlich, wird es aber auch in diesem Fall keine gerichtliche Klärung geben, denn der Kurator hatte sich frühzeitig einsichtig und reuevoll gezeigt.[39]

12.3.3.2.3 Urheberrechtsklage: Fall Miramax vs. Tarantino

Eine gerichtliche Auseinandersetzung mit dem NFT-Angebot eines an dem verknüpften Werk urheberrechtlich (vermeintlich) Unberechtigten ist dagegen im Fall *Miramax vs. Tarantino* zu erwarten.[40] Die im November 2021 von dem Filmstudio *Miramax* beim *Court for the Central District of California* eingereichte Klage richtet sich gegen den namhaften Regisseur *Quentin Tarantino*, der eine NFT-Kollektion an dem von ihm handschriftlich verfassten Original-Drehbuch des Films *Pulp Fiction* (1994) angekündigt hatte. Jedes NFT erfasst den entsprechenden Drehbuchteil einer von sieben Filmszenen in Form von Scans der betreffenden Drehbuchseiten nebst einem persönlichen Audiokommentar von *Tarantino*. 1993 hatte *Tarantino*, Drehbuchautor und Regisseur von *Pulp Fiction*, *Miramax* an dem Filmwerk „*all rights (including all copyrights and trademarks) in and to the Film (and all elements thereof in all stages of development and production) now or hereafter known*“ eingeräumt.[41] Von dieser Rechteeinräumung waren indes einige konkrete Nutzungsrechte ausgenommen worden, insbesondere hatte sich *Tarantino* das Recht für „*print publication (including without limitation screenplay publication, ‘making of’ books, comic books and novelization, in audio and electronic formats as well, as applicable), interactive media*“ vorbehalten.[42] Auf dieser Grundlage erkennt *Miramax* in dem NFT-Projekt Verletzungen vertraglicher Pflichten und ihrer Urheberrechte, sowie ein wegen der Eignung zur Irreführung des angesprochenen Verkehrs ob der Her-

39 Vgl. Financial Times, Stormtrooper ‘Art Wars’ sparks legal action (25.11.2021), verfügbar unter: https://www.ft.com/content/ce92dbd0-1e16-49a2-b506-29dc66b7a131.

40 Klage von Miramax, LLC gegen Quentin Tarantino vom 16.11.2021 vor dem U.S. District Court Central District of California, Case-No. 2:21-cv-08979, verfügbar unter: https://tmsnrt.rs/3FoffuE (über Reuters, https://www.reuters.com/legal/transactional/miramax-sues-quentin-tarantino-over-pulp-fiction-nfts-2021-11-16/).

41 Miramax Klage (Fn. 40), S. 4 Nr. 20. Genauer war diese Vereinbarung zwischen Tarantino und Lawrence Bender, Produzent von Pulp Fiction, einerseits und Miramax’ Vorgängerunternehmen andererseits geschlossen worden.

42 Miramax Klage (Fn. 40), S. 5.

kunft der NFTs markenrechts- und wettbewerbswidriges Verhalten durch *Tarantino*.[43] Insbesondere handele es sich bei der NFT-Verwertung nicht um eine „print"-Veröffentlichung des Drehbuchs im Sinne des vertraglichen Rechtevorbehalts, ferner sei der NFT-Verkauf ohnehin eine einmalige Transaktion und keine derartige „Veröffentlichung".[44] Abzuwarten bleibt, welche konkreten Handlungen *Tarantino*'s das Gericht bei der urheberrechtlichen Bewertung des Falls zu Grunde legen wird. Die Klageschrift wird diesbezüglich wenig konkret.[45] Interessant dürfte diesbezüglich neben der Datensatzreferenz auf off-chain gespeicherte Drehbuchscans insbesondere sein, dass dem NFT-Erwerber ausweislich des *NFT Purchase and License Agreement* ein einfaches, nicht-übertragbares, auf die Zeit der NFT-Inhaberschaft begrenztes Recht zur nicht-kommerziellen Nutzung an dem tokenisierten Werk, mithin an dem betreffenden „*segment of the original Quentin Tarantino's handwritten ‚Pulp Fiction' screenplay*" eingeräumt wird.[46]

12.3.3.2.4 Marken- und Wettbewerbsklage: Fall Yuga Labs vs. Ryder Ripps

Auf eine gerichtliche Entscheidung, wiederum durch den *Court for the Central District of California*, ist auch in der Streitigkeit *Yuga Labs vs. Ryder Ripps* zu hoffen. *Yuga Labs, Inc.*, das Unternehmen hinter der wohl bekanntesten und zeitweise wertvollsten NFT-Kollektion *Bored Ape Yacht Club* (BAYC), hat im Juni 2022 Klage gegen den Konzeptkünstler *Ryder Ripps* eingereicht.[47] Die BAYC-Kollektion besteht aus 10000 NFTs an jeweils einzigartigen Profilbildern von Cartoon-Affen. Die unterschiedlich ausgestalteten Merkmale („Traits") der Affen wie Hintergrund, Ohrringe, Augen, Fell oder Hut, welche jeweils von unterschiedlicher Rarität sind (so haben beispielsweise 13 Prozent aller Apes einen orangefarbenen Hintergrund, aber nur 0,46 Prozent ein goldenes Fell), wurden von einem Algorithmus zu

43 Miramax Klage (Fn. 40): Breach of Contract, S. 15 f.; Copyright Infringement, S. 16 f.; Trademark Infringement, S. 18; Unfair Competition, S. 18 f.

44 Miramax Klage (Fn. 40), S. 13. Abzuwarten bleibt insbesondere, ob das Gericht diesbezüglich der Argumentation des Beklagten folgen wird, dass Miramax nie urheberrechtliche Nutzungsrechte an dem Drehbuch als solchem, sondern lediglich zur Nutzung des Drehbuchs für die Herstellung des Films als ein von diesem abgeleiteten Werk eingeräumt worden waren.

45 Der „Copyright Infringement" Passus der Klageschrift (Fn. 40, S. 16 f.) spricht etwa vom „sale of rights relating to Pulp Fiction" durch Tarantino (Rz. 56, vgl. auch Rz. 35–42), was mit Blick auf den bereits erörterten Inhalt eines NFT-Geschäfts durchaus unbestimmt ist.

46 Vgl. Ziff. 5 i. V. m. Ziff. 1 Secret NFT Purchase and License Agreement, verfügbar unter: https://tarantinonfts.com/terms.

47 S. Fn. 4.

10000 Affenbildern zusammengesetzt.[48] Mit Beginn des Jahres 2022 überstieg das Handelsvolumen der BAYC-NFTs die 1 Milliarde USD Schwelle.[49] *Ripps* hatte die gesamte BAYC-Kollektion nachgebaut und im Mai 2022 unter dem Namen „RR/BAYC" 10000 NFTs mit Verlinkungen auf die originalen *Yuga Labs Bored Apes* angeboten, womit er 1,8 Millionen USD Gewinn gemacht haben soll.[50] Der Künstler versteht seine NFTs, denen er die Beschreibung „*you can't copy an NFT*" zugewiesen hat, als aufklärerisches, satirisches Projekt im Geiste der Appropriation Art.[51] Bemerkenswert, wenngleich mit Blick auf die urheberrechtlichen Implikationen eines NFT-Datensatzes auf der Blockchain nicht überraschend, ist, dass sich die Klage von *Yuga Labs* gegen *Ribbs* nicht auf urheberrechtliche Ansprüche stützt. Vielmehr wird der Beklagte aus Wettbewerbs- und Markenrecht in Anspruch genommen.[52]

12.3.3.3 Smart Contracts

Einige Blockchains unterstützen zudem sog. Smart Contracts. Die größte und etablierteste dieser kompatiblen Blockchains ist die Ethereum-Blockchain, auf welcher, wie bereits erwähnt, der Großteil aller NFTs gemintet und gehandelt wird.[53] Grund dafür ist, dass Smart Contracts für NFTs besonders interessant sind.

Bei Smart Contracts handelt es sich um eine im Blockchain-Datensatz unveränderlich hinterlegte Code-Sequenz, mithin um ein Computerprotokoll

48 Hier ergibt sich eine Schnittstelle mit der Frage der urheberrechtlichen Schutzfähigkeit von durch Künstlicher Intelligenz oder anderweitig automatisiert „erschaffener" Inhalte, zu dieser Frage *Olbrich u. a.*, GRUR 2022, 870; *Hugenholtz/Quintais*, IIC 2021, 1193; *Ory/Sorge*, NJW 2019, 710; *Stützle/Ernst*, Transparenz ist das Schlüsselwort (5.2.2019), verfügbar unter: https://www.medienpolitik.net/2019/02/transparenz-ist-das-schluesselwort/.

49 Vgl. https://markets.businessinsider.com/news/currencies/bored-ape-yacht-club-nft-sales-1-billion-opensea-bayc-2022-1. Im Rahmen einer Christie's Auktion wurden beispielsweise 101 Bored Apes NFTs für 24,4 Millionen USD weiterverkauft, vgl. Yuga Labs Klage (Fn. 4), S. 7. Zum Fall des Floor-Preises in der ersten Jahreshälfte vgl. oben unter 12.2, Fn. 18.

50 Artnet News, Artist Ryder Ripps Called the Bored Ape Yacht Club NFTs Racist. Now, Yuga Labs Is Suing Him for Trademark Infringement and Harassment (29.6.2022), verfügbar unter: https://news.artnet.com/art-world/yuga-labs-v-ryder-ripps-bayc-2137737.

51 https://rrbayc.com/.

52 Yuga Labs Klage (Fn. 4): False Designation of Origin, S. 28 f.; False Advertising, S. 29 f., 36 f.; Cybersquatting, S. 30 ff.; Trademark Infringement, S. 32 f.; Unfair Competition, S. 34 ff.; Unjust Enrichment, S. 37 f.; Conversion, S. 38 f.; Interference with Prospective Economic Advantage, S. 39 ff.

53 Tarantino plant dagegen, seine NFTs auf der ebenfalls Smart-Contract-fähigen Secret Network-Blockchain zu minten, andere relevante NFT-Blockchains sind insbesondere Solana, Flow, EOS, Tezos und Tron.

und damit um ein Computerprogramm.[54] Der Smart Contract führt automatisiert eine bestimmte Folge aus, sobald die festgelegten Voraussetzungen erfüllt sind („*if this, then that*"). Der Fantasie für die Verwendung von Smart Contracts sind kaum Grenzen gesetzt, ihr Einsatz reicht heute schon von Autoleasing-Verträgen bis zur automatisierten Auszahlung von Crowdfunding, sobald die Kampagne den anvisierten Spendenbetrag erreicht hat. Diese „Code is law"-Wirkung[55]von Smart Contracts ermöglicht es NFT-Erstellern, sich eine automatisiert ausgeführte Beteiligung an allen künftigen Transaktionen des NFT, mithin bei jeglichen Weiterverkäufen, zu sichern.[56] Wie hoch diese NFT-Royalties sind, also welcher Prozentbetrag vom Verkaufspreis von Seiten des Verkäufers an den NFT-Ersteller abzuführen ist, legt der Ersteller beim Minten des NFT fest. So ermöglicht es die größte NFT-Handelsplattform *OpenSea* NFT-Erstellern beim Minten, Royalties zwischen 0 und 10 Prozent festzulegen.[57] Dies wird zusammen mit der Adresse der entsprechenden Krypto-Wallet in den Smart Contract implementiert, mit diesem unveränderlich auf der Blockchain gespeichert und jede Folgetransaktion, also die Verknüpfung der Krypto-Wallet des NFT-Erwerbers im Blockchain-Datensatz, nur mit Beteiligungszahlung an den NFT-Ersteller ausgeführt.

12.4 Analoger Kunsthandel vs. NFT-Erwerb: Ein Vergleich der Rechtspositionen

Welche Vorteile und Verwertungsmöglichkeiten bieten NFTs aufgrund dieser technischen Besonderheiten nun also im Vergleich mit dem analogen Handel?

12.4.1 Der Kunsthandel in der analogen Welt

Bei der Verwertung eines analogen, physischen Kunstwerks besteht die Transaktion zwischen Künstlerin und Erwerber aus einem Austausch der physischen Werkverkörperung mit einem Gegenwert, üblicherweise Geld. Offenkundig verlässt dadurch das Kunstwerk selbst die Sphäre und damit die Verfügungsgewalt der Künstlerin. Da allerdings streng zwischen dem

54 Ausführlich zu Smart Contracts *De Filippi u. a.*, Internet Policy Review 2021, verfügbar unter: https://policyreview.info/glossary/smart-contracts.

55 Das vielbesprochene „Code is law"-Konzept geht zurück auf *Lawrence Lessig* in Havard Magazine, Code is law – On Libery in Cyberspace (1.1.2000), verfügbar unter: https://www.harvardmagazine.com/2000/01/code-is-law-html.

56 *Guadamuz*, JIPLP 2021, 1 (10 f.).

57 Vgl. https://support.opensea.io/hc/en-us/articles/1500009575482-How-do-creator-earnings-work-on-OpenSea-.

gegenständlichen Kunstwerk einerseits und den Rechten an dem durch dieses verkörperten urheberrechtlichen „Werkes“ zu trennen ist, werden dem Erwerber durch diese Transaktion nicht zugleich auch urheberrechtliche Nutzungsrechte eingeräumt. Das bedeutet: Auch weiterhin dürfen allein die Künstlerin sowie die von ihr hierzu ermächtigten Personen Abbildungen des Werkes online stellen oder zu kommerziellen Zwecken vervielfältigen. Dieses Auseinanderfallen von Eigentums- und Urheberrechten zeigt sich beispielsweise, wenn Filmaufnahmen im Haus des Erwerbers stattfinden. Als verfügungsberechtigter Hauseigentümer kann er diese Aufnahmen und ihre Verwertung zwar grundsätzlich gestatten, nicht aber mit Blick auf das in seinem Wohnzimmer hängende Gemälde, das er von der Künstlerin erworben hat. Selbstverständlich können sich Künstlerin und Erwerber neben der Eigentumsübertragung auch auf die Einräumung von urheberrechtlichen Nutzungsrechten einigen, das ist indes nicht üblich.

Das Urheberrecht steht daher einer kommerziellen Nutzung des Kunstwerks durch den Erwerber weitestgehend entgegen. In der Regel wird dem Erwerber jedenfalls das Ausstellen des Kunstwerks erlaubt sein, denn die negatorische Wirkung des dem Urheber zugewiesenen Ausstellungsrechts des § 18 UrhG beschränkt sich auf das Original und Vervielfältigungsstücke eines bislang *unveröffentlichten* Werkes. Hat die Künstlerin ihr Werk bereits veröffentlicht, so ist ihr Ausstellungsrecht verbraucht.[58] Indem sich auch das Verbreitungsrecht der Künstlerin aus § 17 Abs. 1 UrhG spätestens durch die Eigentumsübertragung an den Erwerber gemäß § 17 Abs. 2 UrhG erschöpft hat, vermag der Erwerber das Werkstück auch weiterzuveräußern.[59]

Die Künstlerin wird an solchen Folgeverkäufen grundsätzlich nicht beteiligt. In Betracht kommt allenfalls das gesetzliche, verwertungsgesellschaftspflichtige Folgerecht aus § 26 UrhG, welches allerdings nur für Transaktionen an Werken der bildenden Künste oder Lichtbildwerke unter einer Beteiligung von Kunsthändler:innen oder Versteigerern sowie oberhalb einer Mindestverkaufsschwelle von 400 Euro eingreift und dann nur zwischen 0,25 und 4 Prozent des Veräußerungserlöses, in jedem Fall nicht mehr als 12500 Euro, beträgt. Betraf das Rechtsgeschäft zwischen Künstlerin und Erwerber kein physisches Kunstwerk, sondern ein unkörperliches Werk wie etwa eine Digitalgrafik oder ein Video und stellt sich die Verwertung daher nicht als Verkauf, sondern als Einräumung von Nutzungsrechten dar, dann käme allenfalls die sog. „Bestseller-Vergütung“ aus § 32a UrhG in Betracht. Dieser gesetzliche Anspruch auf Nachvergütung setzt indes voraus, dass der

58 Vgl. Amtliche Begründung UrhG v. 23.3.1962, BT-Drs. IV/270, 48; BGH, Urt. v. 23.2.1995 – I ZR 68/93 – Mauer-Bilder, GRUR 1995, 673 (674). Anders als die Erschöpfung des Verbreitungsrechts, § 17 Abs. 2 UrhG, belegt der Rechteverbrauch nicht ein konkretes Werkexemplar, sondern die Schöpfung als solche.

59 Das Recht zur Vermietung erschöpft sich dagegen nicht, vgl. § 17 Abs. 2 UrhG aE.

Lizenznehmer aus der Werknutzung Erträge und Vorteile generiert, zu denen sich die ursprüngliche Vergütung der Künstlerin als unverhältnismäßig niedrig erweist.[60]

12.4.2 Der Handel mit NFTs

Von dieser analogen Ausgangslage sind bei der Verwertung von NFTs Unterschiede auszumachen, die sowohl neue Verwertungsmöglichkeiten begründen, als auch ein zusätzliches Instrument zur Dokumentation der Rechteinhaberschaft bieten.

12.4.2.1 Fortlaufende Vergütung der NFT-Erstellerin

Bei der Verwertung eines NFT erhält die Künstlerin für die Transaktion wie in der analogen Welt eine Vergütung, in aller Regel gezahlt in Form der Kryptowährung der genutzten Blockchain, üblicherweise also in Ether. Bei der Weiterverwertung eines NFT ergibt sich für die Künstlerin der bereits besprochene, aus der „Code is law"-Natur der Smart Contracts folgende Vorteil einer automatisierten Folgevergütung.[61]

12.4.2.2 NFT-Erwerber erlangt keine Rechtsposition am NFT oder am tokenisierten Werk

Der Erwerber des NFT wird durch die Verknüpfung seiner Krypto-Wallet in dem Blockchain-Datensatz gewissermaßen als „Owner", also „Inhaber" des NFT hinterlegt und kann sodann über dieses verfügen. Mangels Sacheigenschaft nach § 90 BGB kann an einem NFT kein Eigentum im Sinne des § 903 BGB bestehen,[62] was in anderen Rechtsordnungen zukünftig aber durchaus anders zu bewerten sein kann.[63] Im Gegensatz zum analogen Kunsthandel

60 Dieser Anspruch, mit Art. 20 Richtlinie (EU) 2019/790 nun unionsweit vorgesehen, wird gerichtlich selten, dann aber überwiegend im Bereich der Filmwerke, der von hohen Vorabinvestitionen geprägt ist und in welchem wirtschaftliche Erfolge schwer abzuschätzen sind, geltend gemacht, vgl. hierzu ausführlich *Stützle*, in: Raue/Hegemann, Münchener Anwaltshandbuch Urheber- und Markenrecht 3. Auflage 2022 (erscheint bald), § 11 Rn. 128 ff.

61 Hierzu oben unter 12.3.3.3.

62 So auch *Hoeren/Prinz*, CR 2021, 565 (567) mit ausführlicher Darstellung der Argumente für und gegen eine analoge Anwendung der sachenrechtlichen Vorschriften sowie ihrer Folgen; *Rauer/Bibi*, ZUM 2022, 20 (24); *Tobler*, DSRITB 2021, 251 (256).

63 So machte der England and Wales High Court erst kürzlich die folgende Überlegung zur Grundlage für eine einstweilige Verfügung gegen die NFT-Handelsplattform OpenSea: „There is clearly going to be an issue at some stage as to whether non-fungible tokens constitute property for the purposes of the law of England and Wales, but I am satisfied on the basis of the submissions made on behalf of the claimant that there is at

wird der NFT-Erwerber auch nicht Eigentümer oder sonstiger Rechteinhaber an dem verknüpften Kunstwerk, denn das NFT und eine Inhaberschaft an diesem sind auch diesbezüglich kein tauglicher Bezugspunkt für Eigentum oder Besitz.[64] Selbstverständlich können die Parteien eine solche Eigentumsübertragung an dem tokenisierten Werk oder Vermögenswert aber separat neben dem NFT-Geschäft herbeiführen.

Dass der NFT-Erwerber an dem tokenisierten Werkexemplar selbst keine Rechtsstellung erlangt, bringt für die Künstlerin den reziproken Vorteil, dass dieses und die alleinige Verfügungsbefugnis hierüber bei ihr verbleiben. Für einige Werke ermöglicht dieser Umstand überhaupt erst eine lukrative Verwertung. So können etwa Kostüme oder Set-Gegenstände von Filmen und Serien monetarisiert werden, ohne dass diese aus dem Fundus herausgegeben werden müssen. Noch deutlicher zeigt sich dieser Vorteil bei präservierungsbedürftigen Werken, deren Erhaltung die Museen und Kunstsammlungen neben einer NFT-Verwertung weiterhin sicherstellen können. Gegen diesen Vorteil einer NFT-Verwertung könnte indes eingewandt werden, dass auch von physischen Gemälden oder Digitalgrafiken analoge wie digitale Kopien verwertet werden können, ohne dass das entsprechende Original die Herrschaftssphäre des Urhebers verlassen muss. Allerdings stellt sich das NFT gerade als eine Art handelbares digitales „Original" dar, für welches eine künstliche Exklusivität geschaffen wird. In der analogen Welt wäre dies allenfalls mit stark limitierten Kunstdrucken vergleichbar.

12.4.2.3 Urheberrechtliche Nutzungsrechte am tokenisierten Werk müssen separat eingeräumt werden

Aus der NFT-Transaktion als solcher folgen zudem keine urheberrechtlichen Nutzungsrechte des Erwerbers an dem tokenisierten Werk oder an der in dem Blockchain-Datensatz verlinkten Darstellung. Nicht zuletzt mit Blick auf die urheberrechtliche Zweckübertragungslehre ist auch eine konkludente Übertragung von Nutzungsrechten durch Erstellung und Veräußerung eines NFT abzulehnen.[65] Der NFT-Owner kann niemanden davon abhalten, im Internet frei verfügbare Abbildungen des Werks abzuspeichern. Dieses „right click and save"-Argument wird häufig gegen die Sinn- und Werthaltigkeit von NFTs angeführt.[66]

---

least a realistically arguable case that such tokens are to be treated as property as a matter of English law.", Urt. v. 10.3.2022, Case-No. CL-2022-00010 Osbourne v Persons Unknown & Anor [2022] EWHC 1021 (Comm), unter Rn. 8.

64 Vgl. auch *Bodó u. a.*, E.I.P.R. 2022, 267 (275 f.).

65 Im Ergebnis so auch *Hoeren/Prinz*, CR 2021, 565 (570).

66 Hierzu Vice, What the Hell Is 'Right-Clicker Mentality'? (3.11.2021), verfügbar unter: https://www.vice.com/en/article/5dgzed/what-the-hell-is-right-clicker-mentality.

Selbstverständlich steht es den Parteien aber frei, eine Einräumung von Nutzungsrechten im Sinne des § 31 UrhG zu vereinbaren. Denkbar ist, eine solche Lizenzvereinbarung in dem Smart Contract auf der Blockchain zu implementieren. Anders als bei der automatisierten Folgevergütung würde eine solche lizenzvertragliche Hinterlegung indes nicht von der „Code is law"-Wirkung des Smart Contract profitieren, da urheberrechtlich relevante Nutzungen des tokenisierten Werkes anders als NFT-Übertragungen offchain stattfinden und somit einer automatisierten Überwachung durch den Smart Contract entzogen sind.[67] Profitieren würde eine Implementierung des Lizenzvertrags in der Blockchain allerdings von der Unveränderlichkeit und öffentlichen Einsehbarkeit.

Bislang üblicher sind entsprechende Klauseln in den AGB der jeweiligen NFT-Sammlungen. So räumt die älteste aller NFT-Kollektionen, „CryptoKitties", dem Erwerber eines NFT „*a worldwide, non-exclusive, non-transferable, royalty-free license to use, copy, and display the Art [any art, design, and drawings that may be associated with a CryptoKitty]*" sowohl für „*personal, non-commercial use*" als auch „*for the purpose of commercializing your own merchandising that includes, contains, or consists of the Art for your Purchased Kitty*" ein, jedoch wird eine solche kommerzielle Nutzung auf einen jährlichen Bruttoerlös von 100000 USD beschränkt.[68] Allerdings bedarf es stets eines genauen Blicks auf die Nutzungsbedingungen des konkreten NFT-Anbieters, auch in der jeweils aktuellen Form. Die Terms and Conditions der NFT-Kollektion „CryptoPunks" weisen den NFT-Erwerber:innen bspw. keinerlei Nutzungsrechte an den verknüpften Avatar-Bildern zu, was sich ausweislich einer Ankündigung im Zuge einer Akquisition der Kollektion durch das Bored-Ape-Unternehmen *Yuga Labs* nun ändern soll.[69] So wird es dem Inhaber eines CryptoPunks-NFT erst künftig erlaubt sein, den tokenisierten Avatar seines NFT als Hexagon-Profilbild auf *Twitter* einzustellen.[70] Dem Erwerber eines Bored-Ape-NFT wird dagegen

67 Daher werden Lizenzen kaum im Blockchain-Datensatz implementiert, vgl. *Bodó u. a.*, E.I.P.R. 2022, 267 (272).

68 CryptoKitties Terms of Use (Stand 15.11.2018), Ziff. 3. A., C. i., ii., verfügbar unter: https://www.cryptokitties.co/terms-of-use.

69 CryptoPunks Terms and Conditions (Stand 11.3.2022), verfügbar unter: https://cryptopunks.app/cryptopunks/terms; Yuga Labs Mitteilung vom 11.3.2022, verfügbar unter: https://mirror.xyz/0xEc9f53fA69682833FBd760C104B5D61aE29221E0/Km81y6Mc3O5LzS0wnrghVIV0HnZgLOd4wsnfcGw3_2I; hierzu umfassend auch *Lee*, The Cryptic Case of the CryptoPunks Licenses: The Mystery Over the Licenses for CryptoPunks NFTs (2022), verfügbar unter: https://ssrn.com/abstract=3978963.

70 Seit Januar 2022 ermöglicht Twitter Nutzern seiner gebührenpflichtigen „Twitter Blue"-Option in einigen Ländern, sich über eine Verknüpfung ihrer Crypto-Wallet als Inhaber eines NFT auszuweisen und dieses in besonderer, sechseckiger Form als Profilbild einzustellen.

seit jeher eine „*worldwide, royalty-free license to use, copy, and display the purchased Art*“, sowohl für den „*own personal, non-commercial use*“, als auch „*for the purpose of creating derivative works („commercial use“)*“, z. B. für Merchandising eingeräumt.[71]

Eine wirksame Einräumung von Nutzungsrechten an einem tokenisierten Werk setzt voraus, dass der NFT-Ersteller tatsächlich (alleinbefugter) Urheber oder entsprechend befugter, derivativer Rechteinhaber an dem in Bezug genommenen Werk ist, was – zumindest außerhalb etablierter NFT-Kollektionen – für den Erwerber nicht ohne Weiteres nachvollziehbar ist. Ein gutgläubiger Erwerb von urheberrechtlichen Nutzungsrechten scheidet aus, dem NFT-Erwerber trifft außerdem das Risiko einer Darlegungs- und Beweislast für den lückenlosen Rechteerwerb.[72]

Die Frage urheberrechtlicher Nutzungsbefugnisse des NFT-Erwerbers an dem tokenisierten Werk dürfte jedenfalls künftig zu einigen Rechtsstreitigkeiten führen. Dabei wird es im Wesentlichen auf eine Auslegung der jeweils geltenden Terms and Conditions der betreffenden NFTs ankommen. Der insoweit äußerst interessante Fall des dem Schauspieler *Seth Green* durch eine Phishing-Attacke abhandengekommenen Bored Ape #8398, der Hauptprotagonist einer von *Green* entwickelten TV-Serie werden sollte, wirft ein Licht auf auslegungsbedürftige Punkte. Hierzu gehört die möglicherweise unauflöslich mit dem tokenisierten Affen-Avatar verbundenen Nutzungslizenz. Die BAYC Terms and Conditions sprechen zunächst von „*When you purchase an NFT, you own the underlying Bored Ape, the Art, completely*.“ und knüpfen für die eingeräumten Nutzungsrechte sodann uneindeutig an eine „*continued compliance with these Terms*“ an.[73] Es ist beinahe zu bedauern, dass dieser Fall keine gerichtliche Erörterung erfahren wird, da *Green*

71 Bored Ape Yacht Club Terms and Conditions, verfügbar unter: https://boredapeyachtclub.com/#/terms.

72 Zum Ausschluss eines gutgläubigen Erwerbs urheberrechtlicher Befugnisse bereits BGH, Urt. v. 21.11.1958 – I ZR 98/57 – Der Heiligenhof, GRUR 1959, 200 (203); vgl. auch *Schulze*, in: Dreier/Schulze, Urheberrechtsgesetz 7. Auflage 2022, UrhG § 31 Rn. 24; *Wandtke*, in: Wandtke/Bullinger, Urheberrecht 6. Auflage 2022, UrhG vor § 31 Rn. 45 f.

73 Zu diesem Fall etwa Forbes, How Scammers Stole Seth Green's Bored Ape Yacht Club NFT And Converted It To Cash (11.7.2022), verfügbar unter: https://www.forbes.com/sites/ericmack/2022/07/11/how-scammers-stole-seth-greens-bored-ape-yacht-club-nft-and-converted-it-to-cash/?sh=247136871f85; ARTnews, Comedian Seth Green Loses Bored Ape NFTs in Hack: “Well frens it happened to me.” (18.5.2022), verfügbar unter: https://www.artnews.com/art-news/news/seth-green-nfts-hack-bored-ape-1234629220/.

den Bored Ape von dem neuen Inhaber, der sich unter U. S.-amerikanischen Recht auf einen gutgläubigen Erwerb des NFT beruft, zurückerworben hat.[74]

12.4.2.4 Nachweis der Rechtekette

Schließlich können NFTs und ihre unveränderliche, öffentliche einsehbare Hinterlegung auf der Blockchain auch im Kunstbereich eine grundbuchartige Rechtssicherheit schaffen. Diese Möglichkeit einer digitalen Provenienz beschränkt sich nicht auf den reinen NFT-Handel. Vielmehr kann auch der Handel physischer Kunstwerke von einer derartigen Erfassung auf der Blockchain, praktisch umgesetzt durch die „Übertragung" eines entsprechenden NFT, begleitet werden. Ein solches, physische wie digitale Kunst erfassendes, Kunstregister von *Artory* mit Sitz in New York wird bereits von renommierten Auktionshäusern wie *Christie's* und *Sotheby's*, aber auch von der größten NFT-Handelsplattform *OpenSea* verwendet.[75]

12.5 Zusammenfassung und Fazit

Aus dem NFT-Handel ergeben sich bereits heute mannigfaltige neue Verwertungsmöglichkeiten für die Kreativbranche. Das Versprechen einer digitalen Exklusivität und Originalität schafft eine für den digitalen Raum einzigartige Nachfrage von Sammler:innen wie auch Spekulant:innen, welche Künstler:innen für sich monetarisieren können, ohne das Werk aus ihrer Zugriffssphäre herausgeben zu müssen. Dabei profitieren sie von der Möglichkeit automatisiert abgeführter Folgevergütungen, die sich aus den technischen Eigenarten von NFTs ergibt. Soweit gewünscht, etwa zum Zwecke einer lebhaften und sichtbaren Fankultur, können Künstler:innen den NFT-Erwerber:innen auch urheberrechtliche Nutzungsrechte an den tokenisierten Werken einräumen. Solche Nutzungsmöglichkeiten können passgenau die Bedürfnisse abdecken, die aus dem Wunsch der Partizipation am digitalen Leben entstehen – von digitalen Sammelkarten bis hin zur Nachbildung exklusiver, künstlich verknappter „Güter" in der digitalen Welt. Letztere kann besondere Relevanz in der Zusammenschau mit der Entwicklung des Metaversums entwickeln. Für den Erwerber kann sich in diesen Fällen ein NFT-Erwerb, insbesondere unter flankierender Einräumung von Nutzungsrechten, tatsächlich als ein „Mehr" gegenüber dem Kunsthandel der analogen Welt darstellen.

---

74 Vgl. Artnet News, 'Scooby-Doo' Star Seth Green Just Bought Back His Stolen Bored Ape NFT for $100,000 More Than He Originally Paid for It (10.6.2022), verfügbar unter: https://news.artnet.com/market/seth-green-bored-ape-returned-2128272.

75 Vgl. www.artory.com.

Festzustellen ist indes auch, dass der NFT-Erwerber *per se* keinerlei Rechtsstellung, insbesondere kein Eigentum oder Nutzungsrechte an dem Off-Blockchain-Werk erlangt, sondern allein „Zugriff" auf das on-chain NFT. Ob der Erwerber daher tatsächlich urheberrechtliche Nutzungsbefugnisse erlangt und den durch sein NFT tokenisierten CryptoPunk als Profilbild nutzen oder die tokenisierte Adidas-Jacke mit seinem Avatar durch das Metaversum tragen darf, bedarf stets einer genauen Prüfung der entsprechenden Nutzungsbedingungen. Mit Spannung zu erwarten sind überdies die (gerichtlichen) Entwicklungen mit Blick auf das Minten und Verwerten von NFTs an urheberrechtlichen Werken durch andere Personen als die urheberrechtlich Berechtigten.

Abschließend bleibt festzuhalten, dass der NFT-Handel auch heute schon eine derart transparente Ausgestaltung erlaubt, dass sich alle Transaktionsbeteiligten über die Nutzungsmöglichkeiten und ihre rechtlichen Grenzen bewusst sein können. Unter dieser Prämisse ist der NFT-Handel durchaus als zukunftstaugliches Verwertungs- und Vermarktungsfeld für die Kreativbranche zu bewerten, sei es als digitale Wertmarke für Fan-Gimmicks[76] oder für eine Berechtigung zum Werkgenuss,[77] als digitale Ergänzung von Sammlungen an Film-Memorabilien wie *Tarantino*'s Drehbuchentwurf, als Übertragung der Fankultur eines Films in das Metaversum[78]oder schlichtweg als Instrument der Vorabfinanzierung für Filmproduktionen[79] bis hin zur Verflechtung einer NFT-Fankultur mit integralen Bestandteilen einer Serien-Storyline.[80] Diese Beispiele zeigen deutlich: NFTs bieten eine wirt-

76 So hat etwa die Band Kings of Leon im vergangenen Jahr NFTs an ihrem neuen Album verkauft, durch welche die Erwerber – je nach NFT-Kategorie – etwa einen Download des Albums, bestimmte VIP-Rechte für die Tour oder zusätzliche Medien wie ein sich bewegendes Album-Cover erhalten, https://opensea.io/collection/kings-of-leon-yellowheart.

77 Die Band Muse wird ihr neues Album als limitierte NFT-Version mit einer automatisierten Folgevergütung in Höhe von 15 Prozent herausbringen, Erwerber erhalten mit dem NFT einen „digital signierten" Download des Albums: The Guardian, Sales from the crypto: Muse NFT album to become first new chart-eligible format in seven years (1.8.2022), verfügbar unter: https://www.theguardian.com/music/2022/aug/01/muse-release-nft-edition-album-will-of-the-people-charts.

78 So beispielsweise durch den Verkauf von 100.000 einzigartigen Matrix-Avataren durch Warner Bros. (https://niftys.com/thematrix), die für jeweils 50 USD sofort ausverkauft waren.

79 Vgl. Süddeutsche Zeitung, NFTs in Hollywood – Geld aus dem Nichts (13.12.2021), verfügbar unter: https://www.sueddeutsche.de/kultur/nft-martin-scorsese-filmproduktion-niels-juul-hollywood-1.5486913.

80 So hat Fox Entertainment für das kommende Jahr eine Animationsserie „curated entirely on the blockchain" angekündigt, die von einer gesonderten NFT-Plattform begleitet werden wird und NFT-Erwerbern Stimmrechte über Show-Details zuweist, vgl. https://www.krapopolis.com/.

schaftlich und marketingbezogen hochinteressante Möglichkeit, neue Verwertungskanäle für Kreativinhalte aufzubauen.

13 Die technologischen Ansätze und Herausforderungen des Web3 und Metaverse

*Yvonne-Anne Pignolet & Stefan Schmid**

Dieser Artikel gibt eine Übersicht über die technologischen Ansätze und Herausforderungen des Web3 und des Metaverse. Das Web3 ist eine dezentralere und partizipativere Form des heutigen World Wide Webs, in dem digitale Güter „tokenisiert" werden können und die Benutzer die Kontrolle und Rechte über ihre Daten behalten: Sowohl Besitztum („Ownership") als auch die Verwaltung und Steuerung („Governance") sind verteilt. Das Web3 kann durch Blockchain-Technologien realisiert werden, auf dem dann Anwendungen wie ein Metaverse, eine von Computern erzeugte virtuelle Welt, mit Hilfe von Smart Contracts implementiert werden. Wir diskutieren Sicherheits- und Effizienzaspekte dieser Technologien, sowie spezifische Herausforderungen der Governance, Ownership und Tokenisierung.

13.1 Einführung

Web3 und Metaverse sind zurzeit in aller Munde. Die beiden Schlagworte werden manchmal sogar als Synonyme benutzt, unterscheiden sich aber. Vereinfacht gesagt versteht man unter Web3 eine „dezentralere" und „partizipativere" Form des WWW. Während die Benutzer:innen im Web1 vor allem Inhalte „lesen" können, können sie im Web2 auch Inhalte „posten", zum Beispiel auf sozialen Netzwerken wie Facebook. Bei Web2 werden diese Inhalte durch große Firmen verarbeitet und verbreitet. Mit Web3 wird das Teilen von Inhalten (inklusive Rechten oder Programmcode) dezentral: die Benutzer:innen behalten die Kontrolle über die Daten selbst. Digitale Güter können „tokenisiert", das heißt in kleine Teile („Tokens") segmentiert werden, die jeweils einen anderen Besitzer haben können.

Im Web3 werden somit sowohl Besitztum („Ownership") als auch die Verwaltung und Steuerung („Governance") verteilt, und Besitzer:innen der Tokens entscheiden zusammen, mit digitalen Abstimmungen, wie sich zum Beispiel eine Anwendung weiterentwickeln soll. Die entsprechenden Programme und Protokolle werden als „Smart Contracts" bezeichnet, da sie Vorgänge automatisch ausführen und dokumentieren, wenn die nötigen Bedingungen erfüllt sind, und somit traditionelle Verträge ersetzen können. Web3 kann durch dezentrale Blockchain-Technologien realisiert werden, wie es zum Beispiel beim Internet Computer, Algorand oder Avalanche der

* Mehr über die Autor:innen erfahren Sie im Autor*innenhinweis auf S. 224 ff.

Fall ist. Der Handel mit Kryptowährungen kann als Teilbereich von Web3 angesehen werden. Weitere Anwendungen des Web3, welche schon heute Milliarden umsetzen, sind beispielsweise non-fungible tokens (NFTs, unteilbare und eindeutige Repräsentation von digitalen oder physikalischen Gegenständen), Marktplätze und Anwendungen basierend auf Daten die vom Benutzer selber kontrolliert werden (zum Beispiel von einer Autoblackbox), Stable Coins mit automatischen Preisbildungsmechanismen und weltweitem, schnellen und günstigen Zahlungsverkehr, und viele mehr.

Metaverse, also eine von Computern erzeugte virtuelle 3D Welt, in welcher sich die Benutzer:innen bewegen und interagieren, kann als Anwendung auf Web3 umgesetzt werden. Zugang zum Metaverse erfolgt zum Beispiel via Headset oder auch immer mehr über haptische („fühlbare“) Technologien.

Die technologischen Herausforderungen von Web3 und Metaverse sind vielfältig und betreffen verschiedene Aspekte. In diesem Artikel werden einige wichtige Herausforderungen und Lösungsansätze genauer beleuchtet. Das Ziel des Artikels ist es, eine Einführung zu geben, und nicht eine umfassende oder wissenschaftliche Abhandlung zu sein. Er enthält deshalb auch keine wissenschaftlichen Literaturhinweise.

13.2 Sicherheit und Privatsphäre

Web3- und Metaverse-Anwendungen müssen sehr hohen Sicherheitsanforderungen genügen. Im Web3 betreffen diese Anforderungen beispielsweise die teuren digitalen Güter und Portfolios von Kryptowährungen, die dort verwaltet werden und eine sichere und korrekte Governance kritisch machen. Das Metaverse wiederum muss beispielsweise die Privatsphäre der Benutzer:innen schützen und, wo nötig, Anonymität bieten.

Einige Herausforderungen in diesem Bereich sind nicht neu, aber immer noch sehr aktuell, beispielsweise bezüglich der Verwendung von Passwörtern: Passwörter sind in der Praxis oft problematisch und während sich Technologien immer mehr in Richtung passwortfreier Identitäten hin entwickeln, oft mit Hardware-basierten Lösungen für Gesichtserkennung, Irisscan oder Fingerabdrücken, haben letztere Ansätze eigene Nachteile und sind unflexibel, was deren Einsatz im Alltag zum Teil schwierig macht.

Web3 und Metaverse werfen auch wichtige grundsätzliche Fragen auf, zum Beispiel wieviel und welche Informationen andere Benutzer:innen über meine Aktionen haben dürfen und welche die Plattformbetreiber. Kryptowährungen wie Bitcoin bieten eine sogenannte Pseudo-Anonymität: Benutzer:innen dürfen so viele Pseudonyme erstellen wie sie möchten, die Transaktionen zwischen den Pseudonymen sind dann aber öffentlich. Für

gewisse Anwendungen kann aber eine volle Anonymität wünschenswert sein, zum Beispiel dass weder die Benutzer:innen noch die Plattformbetreiber wissen, wie groß eine Transaktion war oder sogar ob sie überhaupt stattgefunden hat. Eine volle Anonymität birgt allerdings auch Gefahren und kann missbraucht werden (z. B. für Geldwäsche). Welche Art von Anonymität angeboten werden soll und wie sie umgesetzt wird, muss also von Fall zu Fall bestimmt werden.

Wichtige Sicherheitsfragen stellen sich auch bezüglich Cloud Computing: viele Web3- und Metaverse-Anwendungen werden in Rechenzentren laufen – aus Ressourcen- und Effizienzgründen. Die moderne Kryptographie bietet einige interessante Ansätze, Cloud Ressourcen sicher zu nutzen. Beispielsweise können mittels sogenannter homomorpher Verschlüsselung und sicherer Multiparty Computation, Berechnungen in der Cloud stattfinden, ohne dass ein Cloud Provider die Daten, auf denen er rechnet, einsehen kann.

Auch Hardware-basierte Trusted Execution Environments sind eine wichtige Technologie, um Interaktionen vor Plattformbetreibern geheim zu halten. Mit der sogenannten „Attestation"-Technik kann verifiziert werden, dass diese vom Plattformbetreiber auch tatsächlich benutzt werden. Allerdings lässt sich ein Restrisiko nicht vermeiden: Side-Channel-Attacken (zum Beispiel mit Spannungsmessungen durch den Plattform Betreiber) können nicht ausgeschlossen werden. Außerdem müssen die Benutzer:innen auch dem Hardware-Hersteller vertrauen.

Spezielle Technologien werden auch für die besonderen Sicherheitsanforderungen von Smart Contracts benötigt. So kann es in gewissen Anwendungen wünschenswert sein, den Source Code von Smart Contracts geheim zu halten. Technologien wie Garbled Circuits oder Oblivious RAM unterstützen solche Anwendungen, sind aber immer noch Gegenstand aktiver Forschung. Eine grundsätzliche Frage ist, ob Smart Contracts veränderbar oder unveränderbar sein sollen: ein unveränderbarer Smart Contract ist einfacher zu verifizieren, ein veränderbarer flexibler in der Anwendung.

13.3 Effizienz und Skalierbarkeit

Viele Blockchain-basierte Technologien haben den Ruf, langsam und ineffizient zu sein. Grundsätzlich gilt: Um Dezentralität mit minimalem Vertrauen zu erreichen, muss Fehlertoleranz gewährleistet sein. Das erfordert Redundanz: Daten müssen verteilt gespeichert und berechnet und transportiert werden, was Overheads mit sich bringt. In Web2-Umgebungen liegt der Fokus der Fehlertoleranz auf technischen Ausfällen von Maschinen, welche aber grundsätzlich alle die Protokolle gemäß Spezifikation ausführen. Im

Gegensatz dazu erfordert Web3 eine Fehlertoleranz gegen böswilliges Verhalten: eine kleine Anzahl von böswilligen Akteuren darf keine negativen Auswirkungen auf die Sicherheit und Erreichbarkeit haben. Dazu müssen stärkere Fehlermodelle beim Design und der Analyse der Protokolle und Softwareentwicklung berücksichtigt werden.

Ein besonderes Augenmerk fällt auf die sogenannten Consensus Protokolle, welche es ermöglichen, dass alle beteiligten Maschinen sich einigen, welche Operationen in welcher Reihenfolge als nächstes ausgeführt werden. Je nach Protokoll kann dieser Prozess riesige Energiemengen verschlingen und zum Flaschenhals werden.

Allerdings haben die neuen Generationen von Protokollen hier viele Fortschritte gemacht und erlauben es, tausende Operationen gleichzeitig in wenigen Sekunden unumkehrbar abzuwickeln, und dies ohne energie-aufwändige Verfahren wie zum Beispiel bei Bitcoin. Diese Protokolle noch effizienter zu machen, ist Gegenstand aktueller Forschung.

Es gibt jedoch auch fundamentale Grenzen. Ein globaler Konsensus braucht mehrere sogenannte Round-Trip-Times (RTTs), welche selbst bei Lichtgeschwindigkeit in der Größenordnung von ca. 100 Millisekunden liegen. Außerdem steigt die minimale Anzahl ausgetauschter Nachrichten für deterministische Entscheidungen quadratisch mit der Anzahl beteiligter Maschinen. Deshalb ist ein wichtiger Ansatz für eine höhere Geschwindigkeit Sharding: Wenn sich eine Teilmenge der involvierten Rechner untereinander einigen kann, kann sich die Laufzeit signifikant verbessern, vor allem auch, wenn sie sich geografisch in der Nähe befinden. Das steht allerdings im Konflikt zur Dezentralisierung. Wichtig ist es auch, zwischen Schreib- und Leseoperationen zu unterscheiden: Leseoperationen sind oft wesentlich schneller, da sie keinen Consensus benötigen; das Überprüfen der Authentizität und Integrität der gelesenen Daten erfordert jedoch kryptographische Protokolle, sowohl bei Schreibe- und Lese-Operationen.

Effizienz- und Skalierbarkeits-Fragen betreffen auch den Speicher: Alle Transaktionen für immer global zu speichern und zu verwalten kann teuer sein. Eine wichtige Frage ist, ob und wie eine „Auditability" auf effizientere Art sichergestellt werden kann: Wie können also Transaktionen später verifiziert werden, ohne dass alle Daten gespeichert werden? Oft sind hierzu spezifische Lösungen nötig, zugeschnitten auf den Use Case.

Sogenannte „2nd Layer Solutions", wie Payment Channel Networks und Rollups, sind wichtige Technologien, um Blockchain-Technologien effizienter zu machen. Das Ziel dieser Technologien ist es, die Anzahl nötiger Consensus Operationen zu reduzieren und Transaktionen „lokal beweisbar" zu machen, mittels dezentraler „Peer-to-Peer-Technologien".

Hohe Performanz-Anforderungen können auch beim Zugang zum Metaverse entstehen: Virtual- und Augmented-Reality-Technologien, 360-Grad-Kameras oder 3D holographische Displays, können Bandbreiten in der Größenordnung von mehreren Terabit pro Sekunde erfordern – mehr als heutige 5G Netzwerke bieten. Aktuell wird sehr aktiv an 6G Kommunikationstechnologien geforscht, insbesondere auch in Deutschland.

13.4 Governance

Während im Web2 die Benutzer:innen noch abhängig von der Governance großer Firmen waren, sollen die Benutzer:innen des Web3 direkt involviert werden können. Welche Form diese Beteiligung haben wird, hängt von der Plattform ab und ist Gegenstand aktueller Debatten. Eine zu fein-granulare Beteiligung der Benutzer:innen, zum Beispiel zu technischen Detailfragen, kann diese überfordern und zu geringer Stimmbeteiligung führen.

Ein interessantes Konzept bietet dazu die „flüssige Demokratie“, welche es erlaubt, die eigene Stimme entweder persönlich abzugeben, oder an eine andere Entität zu delegieren. Anders als bei einer traditionellen indirekten Demokratie, bei der Repräsentanten für alle Themen und für eine mehrjährige Periode gewählt werden, erlaubt eine flüssige Demokratie den Beteiligten die Stimmübertragung jederzeit zu widerrufen und auf bestimmte Themenfelder oder sogar individuelle Abstimmungen und Wahlen zu beschränken. Dies soll in einem evolutionären Prozess die Stimmen bei kompetenten Entscheidungsträger:innen anhäufen. Aktuell wird auch untersucht, mit welchen Anreizsystemen Benutzer:innen zum Abstimmen motiviert werden können.

Eine verwandte Frage ist, wieviel Stimmrecht ein Benutzer haben soll. Ein Ansatz könnte sein, die Stimme des Benutzers proportional zu seiner Anzahl Tokens zu zählen. Allerdings sind Tokens oft sehr ungleichmäßig über Benutzer:innen verteilt, was zu „rich getting richer“-Phänomenen führen kann. Ein alternativer, „Per-Person-Ansatz“ kann technisch schwierig umzusetzen sein und bedarf eines „Proof of Personhood“: Es muss möglich sein, sogenannte Sybil-Attacken zu verhindern, wo sich ein Benutzer als mehrere Personen ausgeben kann. Diese Anforderung kann auch in Konflikt stehen mit der Anforderung von Anonymität von Benutzer:innen. Existierende Technologien wie Computational Puzzles sind in der Praxis aber oft teuer und unpraktisch.

13.5 Tokenization und Ownership

Im Web3 können Benutzer:innen selber bestimmen respektive mitbestimmen, wie ihre Daten genutzt werden, und von deren Monetarisierung profitieren. Eine wichtige technologische Herausforderung hier betrifft die Verwaltung der Ownership: Während heute zum Beispiel Grundbucheinträge oft föderal organisiert sind (z. B. pro Gemeinde oder Land), sollen im Web3 Ownerships global und redundant gespeichert werden, selbst für kleine Tokens und potenziell für sehr lange Zeit. Dies führt nicht nur zu großen Datenmengen und somit Herausforderungen für die Skalierbarkeit wie oben diskutiert, sondern bringt auch Anforderungen an die Langlebigkeit von Speichermedien und die Verfügbarkeit von Geräten zu deren Verarbeitung. Wie eine sehr langfristige und „dichte" Speicherung von Information erfolgen kann, ist eine aktuelle Forschungsfrage.

Das Speichern von Keys ist besonders interessant: Aufgrund der dezentralen Natur des Web3 haben Benutzer:innen plötzlich eine große Eigenverantwortung, die Sicherheit ihrer Daten sicherzustellen – dies ist eine der Hauptherausforderungen dieser neuen Technologie. Einerseits müssen Schlüssel sicher gespeichert werden und sollten zum Beispiel nicht übers Internet gestohlen werden können. Andererseits soll es aber auch möglich sein, Schlüssel weiterzugeben, zum Beispiel soll es möglich sein, Tokens an Nachkommen zu vererben. Wichtige Technologien hier basieren auf Key Sharing und Threshold-Kryptographie, welche es erlauben, Schlüssel auch redundant und somit fehlertolerant zu verwalten. Viele neuartige Dienste, wie Custody Solutions, bieten Lösungen zur Schlüsselverwaltung, allerdings zum Preis einer neuen Abhängigkeit von den Dienstanbietern, welche wiederum gegen die Idee des Web3 sprechen kann.

Die Regulierung solcher neuartiger Systeme erfordert ebenfalls neue Technologien. Insbesondere erfordert eine automatisierte Regulierung klare formale Definitionen, die sich auf Smart Contracts abbilden lassen. Außerdem muss es möglich sein, steuerbare und rechtlich relevante Ereignisse automatisiert feststellen zu können.

Je nach Gebiet kann Web3 in Zukunft auch die Durchsetzung von Rechten unterstützen. Zum Beispiel wird erforscht, wie benutzerspezifische digitale Wasserzeichen erstellt und verwendet werden können, um Urheberrechtsverletzungen mit Authentizitäts- und Integritätsgarantien von Blockchain-Plattformen zu verfolgen.

Je dezentraler ein System jedoch ist, desto mehr wird es sich mit Herausforderungen mit Akteuren in unterschiedlichen Rechtsprechungen auseinandersetzen müssen. Es stellt sich zum Beispiel die Frage, wie der Zugang zu Material, welches in bestimmten Ländern verboten ist, eingeschränkt werden kann, wenn die Betreiber der Maschinen wegen der oben beschriebenen

Verschlüsselungs- und Berechnungs-Technologien gar keine Kenntnis vom Inhalt haben.

13.6 Diskussion

Die meisten diskutierten Technologien haben das Ziel, die vom Web3 angestrebte Dezentralität zu erreichen. Es gibt allerdings viele praktische Aspekte, die in der Realität zu einer Zentralisierung führen können und dadurch beispielsweise eine Zensur ermöglichen. Wenn Infrastruktur nur auf einer kleinen Anzahl Betreiber läuft (z. B. nur auf einer Handvoll Cloud Providern) oder nur durch eine kleine Anzahl Internet Service Provider verbunden ist, wenn die Maschinen nur in wenigen Staaten betrieben werden oder an Abstimmungen nur „Power-User“ teilnehmen oder die größten Token Holders überproportional viel Gewicht erreichen, kann das in der Praxis den Zielen des Web3 widersprechen.

Zusammenfassend haben Web3 und Metaverse das Potenzial, unsere Gesellschaft nachhaltig zu verändern. In vielen Bereichen sind die wissenschaftlichen Grundlagen für diese Veränderung bereits vorhanden, zum Beispiel dank moderner Kryptographie. Wichtige Fragen sind aber aktuell noch nicht zufriedenstellend beantwortet, insbesondere zu den „menschlichen Faktoren“. Parallel zu den rechtlichen Grundlagen müssen effiziente Technologien entwickelt werden, die es den Benutzer:innen einfach machen, sich intuitiv und sicher in den neuen digitalen Welten zu bewegen. Eine weitere spannende Frage betrifft, inwiefern verschiedene Metaverses und Blockchains zusammenarbeiten werden und sich ergänzen können – und gleichzeitig ihre Unabhängigkeit bewahren.

14 Metaversum und Recht

*Boris Paal**

Das Phänomen Metaversum erfährt aus guten Gründen zunehmende Aufmerksamkeit. Dies hat sich zuletzt auch im Oktober 2021 in der Umbenennung von Facebook in Meta manifestiert, wobei Facebook/Meta hiermit vor allem auch seine Ausrichtung auf den neuen Megatrend „Metaversum" zum Ausdruck bringen will.[1] Während die einen im Metaversum vor allem eine Weiterentwicklung (nur) des Gamings sehen, erwarten andere eine tiefgreifende Veränderung der gesamten Arbeits- und Lebenswelt. Der vorliegende Beitrag wird sich (ausschließlich) auf die rechtlichen Implikationen des Metaversums fokussieren.

14.1 Einführung

Der Begriff „Metaversum" geht zurück auf den Science-Fiction-Roman *Snow Crash* des Autors *Neal Stephenson* aus dem Jahr 1992, in welchem die Akteure aus einer dystopischen Welt der Zukunft immer wieder in das Metaversum fliehen. Verstehen lässt sich das Metaversum als ein weiterer Entwicklungsschritt des Internets: Vergleichbar mit dem Übergang vom Web 1.0 zum Web 2.0, bei welchem Nutzerinteraktionen hinzugetreten sind, sollen nun mit dem Aufbruch in das Metaversum zusätzliche Elemente der physischen in der virtuellen Welt abgebildet werden.[2]

Zentrales Merkmal des Metaversums ist die durch die virtuelle Ausgestaltung geschaffene Möglichkeit, über sämtliche Distanzen hinweg mit einer nahezu beliebig großen Zahl von Nutzer:innen komfortabel und authentisch – vor allem durch Avatare – zu interagieren. Die Nutzung des Metaversums soll auf diese Weise die Erlebnismöglichkeiten der bisher grund-

---

* Mehr über den Autor erfahren Sie im Autor:innenhinweis auf S. 224 ff. Eine frühere Befassung des Autors mit Rechtsfragen des Metaversums ist bereits im Mai 2022 in der LRZ veröffentlicht worden: https://lrz.legal/de/lrz/kartell-recht-und-das-metaversum, zuletzt aufgerufen am 13.7.2022. Der vorliegende Beitrag setzt auf diesen Überlegungen auf und aktualisiert die dortigen Ausführungen. Der Vortragsstil wurde im Wesentlich beibehalten.

1 Meta, 28.10.2021, https://about.fb.com/news/2021/10/facebook-company-is-now-meta/, zuletzt aufgerufen am 13.7.2022.

2 Der Begriff Web 3.0 wird tendenziell eher für das dezentralisierte Internet verwendet; zum Verhältnis der Begrifflichkeiten Web 3.0 und Metaverse eingehend *Marr, Bernard*, Forbes, 22.2.2022, https://www.forbes.com/sites/bernardmarr/2022/02/22/the-important-difference-between-web3-and-the-metaverse/?sh=6b0128345af3, zuletzt aufgerufen am 13.7.2022.

sätzlich getrennten physischen und virtuellen Welt kombinieren sowie durch diese Verknüpfungen vollkommen neuartige Erlebnisse und Erfahrungen ermöglichen.

Der Erfolg des Metaversums steht und fällt mit der Verfügbarkeit sowie dem Einsatz von Technologien, so vor allem *Virtual Reality* (VR), *Augmented Reality* (AR) und *Mixed Reality*.[3] Für die Ermöglichung und Nutzung dieser Technologien ist eine entsprechend attraktiv und komfortabel einsetzbare Hardware erforderlich, konkret Brillen, Headsets oder ähnliche Geräte. Weiterhin wird den Fragen von Interoperabilität und Standardsetzung eine hervorgehobene Bedeutung zukommen.

Am deutlichsten sichtbar werden die Perspektiven des Metaversums im Gaming-Bereich: Bereits im Jahr 2003 konnten Gamer in dem Online-Spiel *Second Life* in Gestalt eines Avatars ein virtuelles „Leben" führen. Das beliebte Online-Battle-Royale-Spiel *Fortnite* und die Onlinespielplattform *Roblox* lassen sich ebenfalls als Erscheinungsformen des Metaversums verstehen. Einen anderen Ansatz der virtuellen Abbildung der physischen Welt verfolgt die auf der Ethereum-Blockchain-Protokolls basierende 3D-Plattform *Decentraland*. In dieser virtuellen Sphäre können Nutzer:innen „Grundstücke" kaufen. Solche „Grundstücke" sind, umgerechnet aus *Mana*, der virtuellen Währung des Spiels, bereits für sechs- oder sogar auch siebenstellige Dollar-Beträge verkauft worden.[4] Über den Gaming-Bereich hinaus finden sich weitere Ausformungen des Metaversums beispielsweise in virtuellen Meetings im Bildungs- und Lehrbereich oder in virtuellen (Live-)Auftritten im Kultursektor. Allerdings existiert bislang (noch) keine einheitliche Darstellung oder Definition des Metaversums. Perspektivisch denkbar ist sowohl eine vollständig interoperable Infrastruktur als auch eine Vielzahl von Plattformen mit Gatekeeper-Status – worauf noch einzugehen sein wird.[5]

14.2 Rechtsfragen im Metaversum

Das Metaversum, welches sich als rechtliche Querschnittsmaterie darstellt, wirft zahlreiche neuartige Rechtsfragen auf. Beispielhaft benannt werden können hier Fragen des Immaterialgüterrechts (etwa Marken- oder Urheberrecht), die sich aus der zunehmenden Präsenz von (grenzüberschreitend agierenden) Unternehmen im Metaversum ergeben. Aufgrund der sozialen

3 Einen Überblick über die technologischen Grundlagen des Metaverse bieten *Wang et al*., A Survey on Metaverse: Fundamentals, Security, and Privacy, 5.3.2022, https://arxiv.org/abs/2203.02662, S. 1 f., 5 f., zuletzt aufgerufen am 13.7.2022.

4 *Omelchenko/Buckler*, beincrypto, 7.1.2022, https://beincrypto.com/the-cost-of-virtual-land-in-decentraland-just-blew-past-3-5-million/, zuletzt aufgerufen am 13.7.2022.

5 Hierzu nachfolgend 14.4.

Interaktion im Metaversum können zudem auch verhaltensbezogene Rechtsnormen, so etwa Tatbestände im Zusammenhang mit der persönlichen Ehre oder der sexuellen Selbstbestimmung, relevant werden. Insbesondere der Einsatz der Blockchain-Technologie im Kontext von sog. *Smart Contracts* und Zahlungen mittels Kryptowährungen weisen zudem komplexe vertragsrechtliche Herausforderungen auf. Mit der Verwendung der Blockchain-Technologie als dinglicher Übertragungsmechanismus im Kontext des Metaversums sind überdies sachenrechtliche Fragestellungen eröffnet.

Insgesamt dürfte die durch das Metaversum angestoßene Verlagerung von Interaktionen und Transaktionen in virtuelle Sphären einen (weiteren) Schritt weg von körperlichem Eigentum hin zu einer stärkeren Bedeutung von geistigem Eigentum und entsprechenden Lizenzen mit sich bringen. Zudem werden IT-Sicherheitsthemen und damit im Zusammenhang stehende Rechtsfragen im Hinblick auf die durch das Metaversum hervorgerufene Simulation einer realen und sozialen Umgebung in eine neue Dimension gehoben.[6]

14.3 Kartellrecht und Datenschutzrecht

Im Ausgangspunkt sind vornehmlich zwei Rechtsgebiete zentral für die rechtliche Rahmung und somit auch für die weitere Entwicklung des Metaversums: Das Datenschutzrecht und das Kartellrecht. Die zunehmende Verflechtung dieser Rechtsgebiete wurde zuletzt vor allem durch das Verfahren des *Bundeskartellamts* gegen *Facebook* aufgrund des Vorwurfs missbräuchlicher Datenschutzpraktiken deutlich. Das *Bundeskartellamt* stützte sich in seiner Verfügung gegen *Facebook*[7] angesichts der Begründung des kartellrechtlich untersagten Missbrauchs einer marktbeherrschenden Stellung auf das Vorliegen eines Verstoßes der verwendeten Datenschutzbestimmungen (und deren praktischer Handhabung) gegen die Vorgaben des Datenschutzrechts. *Facebook* hatte zunächst bei dem *OLG Düsseldorf* erfolgreich die aufschiebende Wirkung hinsichtlich der vom *Bundeskartellamt* erlassenen Verfügung erwirkt.[8] Diese Entscheidung hat der *BGH* im Juni 2020 sodann aufgehoben, woraufhin *Facebook* mit einem erneuten Eilantrag auf Anordnung der aufschiebenden Wirkung vor dem *OLG Düsseldorf* abermals

6 *Bell*, 28.3.2022, Official Microsoft Blog, https://blogs.microsoft.com/blog/2022/03/28/the-metaverse-is-coming-here-are-the-cornerstones-for-securing-it/, zuletzt aufgerufen am 13.7.2022.; eingehend zu verschiedenen Sicherheitsproblemen *Wang et al*., A Survey on Metaverse: Fundamentals, Security, and Privacy, 5.3.2022, https://arxiv.org/abs/2203.02662, S. 7 ff., zuletzt aufgerufen am 13.7.2022.

7 BKartA, Beschluss vom 6.2.2019, B6-22/16, BeckRS 2019, 48995.

8 OLG Düsseldorf, Beschluss vom 26.8.2019, VI-Kart 1/19 (V), BeckRS 2019, 18837.

erfolgreich war.[9] Die Nichtzulassungsbeschwerde des *Bundeskartellamts* vor dem *BGH* sowie die Vorlage (Art. 267 AEUV) des *OLG Düsseldorf* an den *EuGH* im Hauptverfahren stehen noch zur Entscheidung an.[10] Das Urteil des *EuGH* im Hinblick auf die vorgelegten Fragen wird (aller Voraussicht nach) hierbei auch und gerade für die weitere Entwicklung des Metaversums bedeutsame Problemfelder im Zusammenhang mit der Zulässigkeit der Verarbeitung von Nutzer:innendaten für kommerzielle Zwecke sowie des Verhältnisses von Datenschutz- und Kartellrecht klären.

14.4 Kartellrechtlicher Zugriff

Das Metaversum lässt die Herausbildung einer Vielzahl an neuen Märkten mit großer Veränderungsdynamik erwarten, womit auch und gerade besondere Anforderungen an die Handhabung der Kontrollinstrumente und Regulierungsmechanismen des Kartellrechts einhergehen. Den Kartellrechtsbehörden wird die ebenso voraussetzungsreiche wie herausfordernde Aufgabe zukommen, bei der Anwendung des Kartellrechts das Spannungsfeld der Gewährleistung von Rechtssicherheit, Entwicklungsoffenheit und Verbraucherschutz im Metaversum angemessen aufzulösen. Hervorgehobene Bedeutung hat hierbei die Gewährleistung eines fairen Marktzugangs, auch und gerade für den Markteintritt neuer Akteure und Wettbewerber.

14.4.1 Wettbewerbsbeschränkende Vereinbarungen

Die sowohl für Akzeptanz als auch Aktivität des Metaversums notwendige globale Abdeckung, Erstreckung sowie Reichweite dürfte eine Verständigung auf technische Standards im Sinne einer Interoperabilität verschiedener relevanter Plattformen und Welten erforderlich machen, um eine attraktive Nutzung des Metaversums zu ermöglichen, ohne auf tatsächliche und technische Barrieren zu stoßen. Bei der hierzu erforderlichen Verständigung auf einheitliche Standards muss das kartellrechtliche Verbot einer wettbewerbsbeschränkenden Vereinbarung berücksichtigt werden (vgl. Art. 101 AEUV; § 1 GWB).

14.4.2 Missbrauch einer marktbeherrschenden Stellung

Entscheidende Bedeutung für die kartellrechtliche (unionale und nationale) Beurteilung des Metaversums kommt den Konstellationen eines (mög-

9 OLG Düsseldorf, Beschluss vom 30.11.2020, B6-22/16, BeckRS 2020, 33848.

10 OLG Düsseldorf, Vorlagebeschluss vom 24.3.2021 – Kart 2/19 (V), EuZW 2021, 680, EuGH, ECLI:DE:OLGD:2021:0324.KART2.19V.00.

lichen) Missbrauchs einer marktbeherrschenden Stellung nach Art. 102 AEUV bzw. § 19 ff. GWB zu. Die in diesem Zusammenhang zentrale (Vor-) Frage der Marktabgrenzung stellt sich im Metaversum als besonders komplex dar: Zum einen hat das Metaversum bereits im Ausgangspunkt einen grenzüberschreitenden Charakter. Zum anderen sind innerhalb des Metaversums vielfältige, neuartige Geschäftsmodelle zu erwarten. Überdies ist im Metaversum mit dem Auftreten von für die Marktkonzentration digitaler Plattformen (mit-)entscheidenden Lock-In- und Netzwerkeffekten sowie von Zentralisierungsentwicklungen zu rechnen.

Das Metaversum dürfte in noch stärkerem Maße als bisherige Entwicklungsstufen des Internets von wesentlichen Infrastrukturen, Schnittstellen und Standards (*Essential Facilities*) abhängen. Interessenkonflikte können insoweit vor allem auch entstehen zwischen Unternehmen, die durch die Kontrolle von wesentlichen Einrichtungen den Zugang zum Metaversum vermitteln, Anbietern innerhalb der Wertschöpfungskette des Metaversums, die auf diesen Zugang angewiesen sind, und verschiedenen gemeinwohlrelevanten Zielsetzungen. Vor diesem Hintergrund wird Unternehmen, die über zentrale Schalt- und Schnittstellen gebieten, eine mit besonderen Pflichten einhergehende Intermediärs- und Gatekeeperrolle zukommen. Zu diesen besonderen Pflichten dürfte vor allem auch die Gewährung eines fairen Zugangs zu angemessenen Konditionen gehören. Denn es wird im Metaversum nicht zuletzt auch darauf ankommen, eine unangemessene Benachteiligung der Angebote von Fremdanbietern über die von dominanten Anbietern kontrollierten Zugänge zu verhindern.

14.4.3 Fusionskontrolle

In Ansehung der ausgeprägten rechtlichen und tatsächlichen Komplexität von Missbrauchsverfahren wird in den das Metaversum betreffenden Sachverhaltskonstellationen zudem die Vorabkontrolle von Unternehmenszusammenschlüssen nach der Fusionskontrollverordnung (EU-Ebene) bzw. den §§ 35 ff. GWB (nationale Ebene) eine hervorgehobene Bedeutung zukommen. Dabei ist die kartellrechtliche Vorabkontrolle durch Zusammenschlussverfahren regelmäßig weniger eingriffsintensiv als eine nachlaufende Missbrauchskontrolle. In diesem Zusammenhang wurde *Meta* jüngst vorgeworfen, im AR/VR-Sektor die bereits im Rahmen des Erwerbs von *Instagram* und *WhatsApp* verfolgte Strategie sog. „Killer-Akquisitionen" fortzusetzen.[11] Insgesamt wird der komplexen Frage der Marktabgrenzung eine besondere Aufmerksamkeit zukommen müssen.

11 *McLaughlin*, 3.12.2020, https://www.bloomberg.com/news/articles/2020-12-03/facebook-accused-of-squeezing-rival-startups-in-virtual-reality, zuletzt aufgerufen am 13.7.2022.

14.5 Datenschutzrechtlicher Zugriff

Im Metaversum wird angesichts des Einsatzes von AR-/VR-Technologien eine Vielzahl an sensiblen personenbezogenen Daten gesammelt (werden), so dass die für das Internet bestehenden datenschutzrechtlichen Bedenken potenziert zu werden drohen.[12] Der Verarbeitung unterfallen werden im Zusammenhang mit der angestrebten Verschmelzung von digitaler und physischer Welt insbesondere personenbezogene Daten über Bewegungen, Verhalten, psychische und physische Reaktionen sowie visuelle Daten. Aus einer Gesamtschau dieser Datenkategorien ergibt sich ein erhebliches Potenzial für weitere technische Innovation und wirtschaftliche Verwertung.

Hierbei könnte personalisierte Werbung (*Targeted Advitising*) im Metaversum in eine neue Dimension vorstoßen, wenn und soweit entsprechende Werbeanzeigen etwa direkt in die virtuelle Umgebung eingebettet und für die Personalisierung eine Vielzahl weiterer Datenpunkte verwendet werden. Aus Nutzer:innensicht vielversprechend dürfte nicht zuletzt die Entwicklung neuer Produkte auf Grundlage der im Metaversum gewonnen Daten sein. Mit der digitalen Erfassung und Abbildung von Menschen in einer 3D-Umgebung kann im Metaversum zugleich aber auch eine deutlich umfassendere Profilbildung und Überwachung stattfinden als noch im bisherigen Web 2.0. Der dynamisch anwachsende Bestand an marktrelevanten Daten ist aus wettbewerbsrechtlicher Sicht vor allem für die Frage nach der Marktbeherrschung gemäß § 18 Abs. 3 Nr. 3, Abs. 3a Nr. 4 GWB zu berücksichtigen.

14.5.1 Datenschutzgrundverordnung (DSGVO)

Das Datenschutzrecht zielt auch und gerade auf einen Schutz der informationellen Selbstbestimmung ab. Als umfassendes unionsweites Regelungswerk mit Ausstrahlungswirkung auch über Europa hinaus (sog. *Brussels Effect*) ist hier vor allem die DSGVO relevant, die die Verarbeitung personenbezogener Daten im Ausgangspunkt mit einem präventiven Verbot mit Erlaubnisvorbehalt belegt. Die Erlaubnistatbestände der DSGVO sind in Art. 6 enumerativ aufgezählt. Im Kontext des Metaversums werden insbesondere die Erlaubnistatbestände der lit. a (Einwilligung), lit. b (Vertrag) und lit. f (Interessenabwägung) relevant sein.

An Komplexität gewinnen dürfte im Metaversum mit seinen entgrenzten physisch/virtuellen Welten zudem die Frage nach der räumlichen Anwendbarkeit der jeweiligen Datenschutzrechtsnorm. Entscheidend für die sachliche Anwendbarkeit der DSGVO ist der Personenbezug der in Rede stehenden Daten (vgl. die Legaldefinition in Art. 2 Abs. 1 DSGVO). Maßgebliches

12 Siehe *Eglistone/Carter*, Critical questions for Facebook's virtual reality: data, power and the metaverse, Internet Policy Review, Volume 10, Issue 4, S. 8.

Kriterium für die Frage nach dem Vorliegen eines Personenbezuges ist nach Art. 4 Nr. 1 DSGVO die direkte oder indirekte Identifizierbarkeit der jeweiligen Person.

In einer Studie aus dem Jahr 2020 konnten etwa 95 % der Testpersonen anhand einer fünfminütigen Aufzeichnung ihrer Körperbewegungen in einer VR/AR-Umgebung eindeutig identifiziert werden.[13] Aus der Aufzeichnung entsprechender physischer Muster dürften zudem auch Rückschlüsse auf besonders sensible Informationen gezogen und so etwa biometrische Daten nach Art. 4 Nr. 14 DSGVO[14] oder Gesundheitsdaten nach Art. 4 Nr. 15 DSGVO mit den besonderen, erhöhten Rechtmäßigkeitsanforderungen an die Verarbeitung nach Art. 9 DSGVO gewonnen werden (können).

Die im Sinne der Transparenz der Datenverarbeitung nach den Art. 12 ff. DSGVO erforderlichen Informationen werden im Zuge der Entwicklung hin zu einem ubiquitären Metaversum an Komplexität deutlich zunehmen und vor allem das Modell der auf umfassender Information beruhenden Einwilligung (zusätzlich) an seine Grenzen bringen. Besondere Schwierigkeiten wird im Kontext des Metaversums überdies die Frage nach der Zurechnung von Verantwortlichkeit für die Datenverarbeitungen aufwerfen (vgl. Art. 4 Nr. 7 DSGVO). Die Komplexität dieser Fragen leitet sich nicht zuletzt auch aus der Vielzahl an im Metaversum handelnden Akteuren und deren mannigfaltigen sowie multipolaren Interaktionen ab, wodurch mit Blick auf die Zusammenarbeit und die wechselseitigen Beiträge bei der Datenverarbeitung auch und gerade die Frage nach einer gemeinsamen Verantwortlichkeit auf der Grundlage und am Maßstab von Art. 4 Nr. 7 i. V. m. Art. 26 Abs. 1 S. 1 DSGVO aufgeworfen ist.

14.5.2 Gemeinsame Verantwortlichkeit

Eine gemeinsame Verantwortlichkeit liegt nach Art. 26 Abs. 1 S. 1 DSGVO vor, sofern zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung festlegen. Im Hinblick auf die insoweit bestehenden Anforderungen kann auf den Kriterienkatalog zurückgegriffen werden, den der *EuGH* – unter Zugrundelegung eines weiten Verständnisses – in drei noch zur Vorgängervorschrift (Art. 2 lit. a DS-RL) ergangenen Urteilen formuliert hat.[15] Nach dieser Judikatur setzt eine gemeinsame Verantwort-

13 *Miller et al*., Personal identifiability of user tracking data during observation of 360-degree VR video, Nature, 15.10.2020, https://www.nature.com/articles/s41598-020-74486-y, zuletzt aufgerufen am 13.7.2022.

14 *Eglistone/Carter*, Critical questions for Facebook's virtual reality: data, power, and the metaverse, Internet Policy Review, Volume 10, Issue 4, S. 16.

15 EuGH, Urt. v. 5.6.2018 – C-210/16, NJW 2018, 2537 – Wirtschaftsakademie Schleswig-Holstein; EuGH, Urt. v. 10.7.2018 – C-25/17, NJW 2019, 285 – Zeugen Jeho-

lichkeit keine gleichwertigen Verantwortungsbeiträge im Hinblick auf die Verarbeitung voraus; die beteiligten Akteure sollen vielmehr „in verschiedenen Phasen und in unterschiedlichem Ausmaß in der Weise einbezogen sein [können], dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist".[16] Zudem müsse auch nicht jeder Akteur Zugang zu den betreffenden personenbezogenen Daten haben.[17] Folgt man dieser Lesart, so kann zur Begründung einer gemeinsamen Verantwortlichkeit bereits eine untergeordnete bzw. auf verschiedene Phasen der Verarbeitung beschränkte Beeinflussung der Zwecke und Mittel der Verarbeitung genügen. Vor diesem Hintergrund sind (auch) im Metaversum herausfordernde Abgrenzungsfragen aufgeworfen, da mit einer datenschutzrechtlichen Verantwortlichkeit zahlreiche Pflichten (so bspw. für technisch-organisatorische Maßnahmen, Auskunfts- und Informationspflichten) und Risiken (bspw. betreffend Sanktionen und Schadensersatz) einhergehen.

14.5.3 Recht auf Vergessenwerden, Datenportabilität und Personalisierung

Herausgehobene Bedeutung dürfte im Metaversum dem Recht auf Vergessenwerden gemäß Art. 17 DSGVO zukommen. Schließlich soll das Metaversum ein Raum für umfassende soziale Interaktion sein und wird als solcher ein Bedürfnis hervorrufen, etwa Informationen über sensible (private) Verhaltensweisen der dauerhaften Aufzeichnung zu entziehen. Als Regelung mit wettbewerblichem Charakter wird ferner das in Art. 20 DSGVO niedergelegte Recht auf Datenportabilität relevant sein. Schließlich könnten auch die generell im Zusammenhang mit der Personalisierung von Online-Angeboten diskutierten Bedrohungen (wie etwa eine Verhaltensmanipulation) durch das tiefe Eindringen des Metaversums in die physische Welt potenziert sowie durch die große Menge an sensiblen personenbezogenen Daten vertieft werden. Aus diesen Entwicklungstendenzen erwachsen gewaltige Herausforderungen auch und gerade für das Datenschutzrecht.

---

vas; EuGH, Urt. v. 29.7.2019 – C-40/17, NJW 2019, 2755 – Fashion ID. Vgl. insoweit auch das weitgehend ähnliche Verständnis der Artikel-29-Datenschutzgruppe (WP 169, S. 23 ff.) sowie nunmehr auch EDPB, Guidelines 07/2020, Version 2.0 vom 7.7.2021, S. 19 ff.

16 EuGH, Urt. v. 5.6.2018 – C-210/16, NJW 2018, 2537 Rn. 43 – Wirtschaftsakademie Schleswig-Holstein; EuGH, Urt. v. 10.7.2018 – C-25/17, NJW 2019, 285 Rn. 66 – Zeugen Jehovas; EuGH, Urt. v. 29.7.2019 – C-40/17, NJW 2019, 2755 Rn. 70 – Fashion ID.

17 EuGH, Urt. v. 5.6.2018 – C-210/16, NJW 2018, 2537 Rn. 43 – Wirtschaftsakademie Schleswig-Holstein; EuGH, Urt. v. 10.7.2018 – C-25/17, NJW 2019, 285 Rn. 69 – Zeugen Jehovas; EuGH, Urt. v. 29.7.2019 – C-40/17, NJW 2019, 2755 Rn. 69 – Fashion ID.

14.5.4 Perspektiven und Handlungsbedarfe

Nach alledem dürfte das Datenschutzrecht (mit-)entscheidend dafür sein, in welche Richtung sich die Datenökonomie unter den Bedingungen des Metaversums entwickelt. Die bestehenden datenschutzrechtlichen Regelungen sind hierbei im Ausgangspunkt durchaus geeignet, mit den Herausforderungen durch das Metaversum umzugehen. Klarheit über den Bedarf zur Nachjustierung des Regelungsregimes wird sich erst im Laufe der weiteren Entwicklung des Metaversums ergeben. In Abhängigkeit von der Entwicklung des Metaversums mag der bestehende *one-size-fits-all*-Ansatz der DSGVO hierbei durch spezifischere Regelungen zu ergänzen oder zu modifizieren sein. In diesem Zusammenhang wird es insbesondere auch auf die Auslegung und Anwendung der bestehenden Vorschriften durch Aufsichtsbehörden und Gerichte ankommen. Es empfiehlt sich überdies, auch und gerade auf die Entwicklung einheitlicher internationaler Standards hinzuwirken.

14.6 Plattformregulierung

Weiterhin ist der Blick zu richten auf die Plattformregulierung mit ihren konkreten Ausprägungen in der 10. GWB-Novelle (GWB-Digitalisierungsgesetz), im Digital Services Act und im Digital Markets Act. Während mit dem GWB-Digitalisierungsgesetz und dem Digital Markets Acts auf ökonomische Besonderheiten von digitalen Plattformen, wie etwa Netzwerk- und Lock-In-Effekte, reagiert werden soll, verfolgt der Digital Services Act primär außerökonomische Zielsetzungen, so vor allem auch den Schutz vor illegalen Inhalten oder die Erhöhung der Transparenz digitaler Plattformen. Das Metaversum könnte insoweit einen neuen Anwendungsbereich der Plattformregulierung darstellen.

14.7 KI-Regulierung

Technologien der Künstlichen Intelligenz wird auch und gerade im Metaversum eine gestiegene Bedeutung zukommen. Hier ergeben sich im Zusammenhang mit dem Training der Algorithmen komplexe Fragen des Datenschutzrechts und des geistigen Eigentums. Bei dem Einsatz von Systemen der Künstlichen Intelligenz werden die Aspekte von Diskriminierung und Zurechnung von Verantwortlichkeiten eine zentrale Rolle spielen. Vor diesem Hintergrund sowie zur Unterbindung einer (ggf. auch subliminalen) Verhaltensbeeinflussung durch entsprechende Systeme wird es vor allem auch auf eine vorausschauende rechtliche Einhegung ankommen. Im Bereich der Künstlichen Intelligenz finden sich auf Unionsebene insoweit be-

reits bedeutsame Regulierungsinitiativen. Zu nennen ist hier insbesondere der Entwurf der *EU-Kommission* für eine Verordnung zur Regulierung von KI-Systemen vom April 2021.[18] Dieser Entwurf gibt das Ziel einer Förderung von KI-Technologien in Europa und deren Nutzung im Interesse der Menschheit vor. Zu diesem Zweck werden KI-Systeme klassifiziert in unzulässige Systeme, solche mit hohem Risiko, solche mit begrenztem Risiko und schließlich Systeme ohne bzw. mit lediglich einem geringen Risiko. Im Januar 2022 wurden auf Unionsebene zudem Konsultationen zur Regelung der zivilrechtlichen Haftung im Zusammenhang mit Systemen Künstlicher Intelligenz gestartet.

14.8 Zusammenfassung und Ausblick

In welchem Ausmaß und in welche Richtung sich das Metaversum entwickeln wird und wer die maßgeblichen Akteure sein werden, bleibt mit Spannung abzuwarten. Ob sich die Erwartungen einer grundlegenden Revolution des Geschäfts-, Privat- und Arbeitslebens realisieren werden, ist noch ungewiss. Festzuhalten ist jedenfalls schon zu diesem Zeitpunkt, dass das Metaversum gravierende technische und soziale Neuerungen mit sich bringen wird, auf die auch und gerade das Recht angemessene Antworten finden muss.

Die mit dieser Entwicklung im Zusammenhang stehenden Rechtsfragen sollten bereits frühzeitig auf breiter Basis diskutiert werden, damit das Recht eine gestaltende und ordnende Rolle einnehmen kann. Im Zuge der weiteren Entwicklung des Metaversums sollte der maßgebliche Rechtsrahmen in diesem Sinne fortlaufend überprüft und den Entwicklungen angepasst werden. Die Komplexität der zu erwartenden Entwicklungen verlangt nach einer regulatorischen Einbeziehung von Erkenntnissen insbesondere aus den Bereichen Recht, Ethik, Soziologie, Ökonomie und Technik. Zudem sind wegen der grenzüberschreitenden Natur des Metaversums vor allem auch länder- und rechtsordnungsübergreifenden Ansätze vorzugswürdig. Besondere Aufmerksamkeit verdienen Fragen zur Ausgestaltung und Gewährleistung des Zugangs zum Metaversum sowie betreffend die Zuordnung von Verantwortlichkeit. Hier wird es darauf ankommen, zur Setzung von Wettbewerbs- und Innovationsanreizen eine geeignete Balance zwischen regulatorischem Over-Enforcement und einem Laissez-faire-Ansatz zu finden.

18 EU-Kommission, 21.4.2021, Vorschlag für eine Europäische Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM(2021) 206 final.

15 Federated Learning als Chance für datenschutzfreundliche KI?

*Maximilian Leicht & Leo Dessani**

Federated Learning ist ein vielversprechender Ansatz, um den Einsatz von Machine-Learning-Systemen datenschutzfreundlich(er) zu gestalten. Dieser Beitrag erläutert die technischen Grundlagen sowie mögliche Risiken durch Angriffe auf Federated-Learning-Anwendungen. Darauf aufbauend werden jeweilige datenschutzrechtliche Implikationen skizziert. Diese stehen im Kontrast zu den ebenso relevanten Regelungen in § 25 TTDSG bzw. Art. 5 Abs. 3 E-Privacy-RL.

15.1 Bedarf für Federated Learning

Das zentrale Trainieren[1] von Machine-Learning-Modellen (ML-Modellen)[2] stellt Verantwortliche vor große Herausforderungen, da oftmals personenbezogene Daten als Trainingsdaten verwendet werden. Für die Verarbeitung dieser Daten ist das Datenschutzrecht anwendbar. Insbesondere müssen Verantwortliche für die dem Training zugrundeliegende Datenverarbeitung eine geeignete Rechtsgrundlage nachweisen können sowie bei der Verarbeitung von Bestandsdaten die Anforderungen an die häufig vorliegende Zweckänderung i. S. d. Art. 6 Abs. 4 DSGVO beachten.[3] Liegen besondere Kategorien personenbezogener Daten vor, ist zudem der im

* Mehr über die Autoren erfahren Sie im Autor:innenhinweis auf S. 224 ff. Die Autoren danken den Teilnehmenden an der Sommerkonferenz für wertvolle Anregungen, die diesen Beitrag bereichert haben. Dieser Beitrag entstand im Rahmen des Projektes „PAIRS“ (www.pairs-projekt.de, Förderkennzeichen: 01MK21008H), welches durch das Bundesministerium für Wirtschaft und Klimaschutz finanziert wird.

1 Im Folgenden wird synonym zum Begriff des Trainings der Begriff „Optimierung“ verwendet.

2 Für eine Erläuterung zu Begriff und Funktionsweise vgl. etwa *Huth*, in: Kaulartz/Braegelmann, Rechtshandbuch Artificial Intelligence and Machine Learning (1. Auflage 2020), Kapitel 2.3, Rn. 25 ff.; Bundesamt für Sicherheit in der Informationstechnik (BSI), Sicherer, robuster und nachvollziehbarer Einsatz von KI, v. 9.2.2021, S. 4, abrufbar: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Herausforderungen_und_Massnahmen_KI.pdf (zuletzt abgerufen am 31.8.2022); oder *Leicht/Sorge*, Einsatz von KI-Systemen im Unternehmen, in: Roth/Corsten, Handbuch Digitalisierung, S. 1281 (1287).

3 Die datenschutzrechtlichen Anforderungen für das Training und den Einsatz von ML-Modellen werden in der Literatur ausführlich behandelt; für eine Übersicht vgl. nur: *Niemann/Kevekordes*, CR 2020, 17–25; *Niemann/Kevekordes*, CR 2020, 179–184; *Kaulartz/Huth*, DSB 2019, 276 (276 ff.).

Vergleich zu Art. 6 Abs. 1 DSGVO enger gefasste Art. 9 DSGVO einschlägig, dessen Anwendungsbereich der EuGH kürzlich weit auslegte.[4] Auch Betroffenenrechte wie Informationspflichten (Art. 13, 14 DSGVO) und das Recht auf Löschung (Art. 17 DSGVO) sind relevant.[5]

Neben rechtlichen Verpflichtungen ergeben sich durch die zentrale Speicherung personenbezogener Daten[6] sowie durch deren zentrale (Weiter-)Verarbeitung auch technische Risiken. Zum einen kann eine Übertragung der Trainingsdaten an die zentrale Stelle[7] erforderlich sein – sofern diese noch nicht über die Daten verfügt oder sie selbst erhebt. Die Übertragung kann Risiken für die Vertraulichkeit und die Integrität der Daten bergen, etwa wenn Daten während des Transports verändert werden oder Dritte Kenntnis vom Inhalt der Übertragung nehmen können. Dieses Risiko kann jedoch durch die Verwendung von sicher konfigurierter TLS-Verschlüsselung (z. B. HTTPS) auf ein Minimum reduziert werden.[8]

Unabhängig von dem Risiko während des Transports verbleibt zudem die Problematik, dass die zentrale Stelle über alle personenbezogenen Trainingsdaten verfügt und zumindest theoretisch in der Lage ist, sie auszuwerten und ggf. Rückschlüsse auf einzelne Personen und deren Verhalten zu ziehen. Auch ein Datenabfluss der dort gespeicherten Daten infolge eines Angriffs auf den zentralen Server könnte dazu führen, dass personenbezogene Daten zumindest einzelner Nutzer:innen offengelegt werden.

Das zentrale Training von ML-Modellen hat daher sowohl technische Risiken als auch – diese Risiken adressierend – datenschutzrechtliche Verpflichtungen des Verantwortlichen zur Folge. Im Folgenden wird deshalb skizziert, ob der Einsatz von Federated Learning eine Minimierung dieser Risiken und Pflichten erreichen kann. Hierzu wird zunächst die Funktionsweise von Federated Learning erläutert.

---

4 EuGH v. 1.8.2022, Rs. C-184/20, Rn. 119 ff.

5 Vgl. *Niemann/Kevekordes*, CR 2020, 179 (182 f.).

6 Die Daten können beispielsweise in einem Storage-Cluster mit RAID-Funktionalität in einem Rechenzentrum gespeichert werden, um den Ausfall mehrerer Festplatten oder eines einzelnen Servers kompensieren zu können.

7 Je nach Implementierung verwendet die zentrale Stelle ein Setup aus mehreren Servern, zur Vereinfachung wird im Folgenden von einem einzelnen Server ausgegangen und der Begriff als Synonym für die eingesetzte technische Infrastruktur der zentralen Stelle für Federated-Learning-Anwendungen verwendet.

8 Es gilt dabei zu beachten, dass nur die TLS-Versionen 1.2 oder 1.3 zum Einsatz kommen, die aktuell dem Stand der Technik entsprechen. TLS 1.0 und 1.1 wurden mit dem RFC 8996 abgekündigt. Zu beachten ist zudem die Richtlinie TR-02102-2 des BSI, insbesondere die dort enthaltenen Empfehlungen zu Cipher-Suiten.

15.2 Funktionsweise von Federated Learning

Federated Learning[9] – ein Teilbereich des Machine Learning – stellt einen Ansatz dar, um verteilt gespeicherte (personenbezogene) Daten für das Training eines ML-Modells zu verwenden. Insbesondere hebt dieser Abschnitt das sog. Model-Centric, Cross-Device Federated Learning hervor. Dabei handelt es sich um einen weitverbreiteten Ansatz, bei dem sich die Trainingsdaten auf Endgeräten von Nutzer:innen befinden und der beispielsweise von Google zur Optimierung der Wortvorschläge für die Android-Tastatur *Gboard* genutzt wird.

Im Folgenden wird zunächst erläutert, welche Arten von Federated Learning in der technischen Literatur unterschieden werden (Abschnitt 15.2.1). Darauf aufbauend wird die Funktionsweise von Model-Centric, Cross-Device Federated Learning genauer erläutert (Abschnitt 15.2.2).

15.2.1 Arten von Federated Learning

Der Begriff Federated Learning kann im Detail weiter unterteilt werden nach der Art der Datenbereitstellung, der Art der verwendeten Datensätze und der Aufteilung der Daten.

Die Datenbereitstellung lässt sich unterteilen in Model-Centric Federated Learning und Data-Centric Federated Learning.[10] Bei Model-Centric Federated Learning ist die Optimierung des zentral verwalteten Modells mit *verteilten Daten* das primäre Ziel. Bei Data-Centric Federated Learning werden dagegen Daten auf einem zentralen Server bereitgestellt, die für das Training von mehreren Modellen verwendet werden können. Entwickler:innen schicken ihr jeweiliges Modell an den zentralen Server und lassen es mit den dort gespeicherten Daten trainieren, ohne die Daten aber selbst zu erhalten – es handelt sich sozusagen um voneinander unabhängige „*verteilte Modelle*“. Streng genommen umfasst obige Federated-Learning-Definition Data-Centric Federated Learning nicht; da dies aber aktuell kaum verbreitet ist, wird im Folgenden nur Model-Centric Federated Learning behandelt.

Die Art der Datenbereitstellung lässt sich bei Model-Centric Federated Learning unterteilen in Cross-Device und Cross-Silo Federated Learning:

9 *McMahan, B., Moore, E., Ramage, D., Hampson, S. & y Arcas, B.A.* (2017). Communication-efficient learning of deep networks from decentralized data. In: *Artificial intelligence and statistics*, PMLR, S. 1273–1282.

10 *Śmietanka, M., Pithadia, H. & Treleaven, P.* (2020). Federated Learning for Privacy-Preserving Data Access. Available at SSRN 3696609.

Cross-Device Federated Learning beschreibt das Training auf (vielen) verschiedenen Endgeräten.[11] Dabei speichern die Endgeräte das vom zentralen Server verteilte Modell, optimieren es mit den lokal gespeicherten (personenbezogenen) Daten und senden es anschließend zurück an den zentralen Server.[12] Dies geschieht in der Regel über einen längeren Zeitraum (z. B. mehrere Wochen oder Monate).

Cross-Silo Federated Learning beschreibt das Training mit Datensätzen verschiedener Partner („Datensilos"), wobei deren Anzahl meist gering ist.[13] In Betracht kommen beispielsweise Gesundheitsdaten mehrerer Krankenhäuser oder Finanzdaten verschiedener Kreditinstitute. Auch bei dieser Art wird das zu optimierende, vom Server verteilte Modell gespeichert, lokal trainiert und anschließend wieder zurück an den Server übertragen.

Schließlich lässt sich die Aufteilung der Daten in Horizontal und Vertical Federated Learning[14] unterteilen:

Beim Horizontal Federated Learning (auch Sample-based Federated Learning[15]) werden Datensätze mit denselben Merkmalen verwendet, um gemeinsam ein Modell zu trainieren. Der Begriff *Merkmal* (engl. *Feature*) beschreibt die Eigenschaften, die zur Charakterisierung der Daten verwendet werden. Beispielsweise können zwei Automobilhersteller, deren Kund:innengruppen nur eine kleine Schnittmenge haben (kaum gleiche Kund:innen), für ein ML-Modell zur Fahrsicherheit jeweils die gleiche Art von Sensordaten aus ihren vernetzten Fahrzeugen nutzen.

Beim Vertical Federated Learning (auch Feature-based Federated Learning[16]) werden verschiedene Datensätze mit unterschiedlichen Merkmalen verwendet, um gemeinsam ein Modell zu trainieren. Beispielsweise können zwei regional ansässige Unternehmen, ein Supermarkt und eine Bank, aufgrund ihrer geografischen Nähe gleiche Kund:innengruppen haben, deren Schnittmenge groß ist (viele gleiche Kund:innen). Da der Supermarkt das Kaufver-

---

11 *Karimireddy, S. P., Jaggi, M., Kale, S., Mohri, M., Reddi, S., Stich, S. U. & Suresh, A. T.* (2021). Breaking the centralized barrier for cross-device federated learning. Advances in Neural Information Processing Systems, 34, S. 28663–28676.

12 Je nach Implementierung kann die Vorgehensweise im Detail abweichen, etwa kann eine Implementierung gewählt werden, bei welcher die Endgeräte das Modell vom Server laden.

13 *Zhang, C., Li, S., Xia, J., Wang, W., Yan, F. & Liu, Y.* (2020). BatchCrypt: Efficient homomorphic encryption for Cross-Silo federated learning. In: 2020 USENIX annual technical conference (USENIX ATC 20), S. 493–506.

14 *Yang, Q., Liu, Y., Chen, T. & Tong, Y.* (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2), S. 1–19.

15 Ebd.

16 Ebd.

halten und die Bank das Einnahme- und Ausgabeverhalten ihrer jeweiligen Kund:innen speichern, sind die Merkmale der Datensätze unterschiedlich.

Der Vollständigkeit halber ist darüber hinaus noch Federated Transfer Learning[17] zu erwähnen, was jedoch für diesen Beitrag keine Relevanz hat.

Abschließend ist wichtig zu betonen, dass sich Federated Learning grundlegend von Distributed Machine Learning unterscheidet: Bei Distributed Machine Learning findet das Rechnen in einem Server-Verbund, auch Cluster genannt, statt. Intention ist hierbei die Aufteilung von Rechenleistung auf verschiedene physische Serversysteme, nicht die dezentrale Speicherung von Trainingsdaten.

15.2.2 Model-Centric, Cross-Device Federated Learning

Besonders interessant ist eine nähere Betrachtung der technischen Funktionsweise von Model-Centric, Cross-Device Federated Learning, da dabei eine Vielzahl von Endgeräten beteiligt ist, auf denen personenbezogene Daten gespeichert werden. Nach der Speicherung des zu trainierenden Modells von dem zentralen Server auf dem Endgerät erfolgt das Training lokal mithilfe von Machine-Learning-Frameworks wie *TensorFlow*[18] oder *PyTorch*[19]. Dabei werden die Eigenschaften des zu trainierenden Modells – die sog. Modellparameter – optimiert. Für das Erreichen eines signifikanten Trainingseffekts ist es erforderlich, dass für die jeweilige Federated-Learning-Anwendung stets ausreichend Endgeräte verfügbar sind. Daten, die nicht für das Training bestimmt sind (z. B. Passwörter bei der Eingabe in dafür vorgesehene Felder) sollten vom Training ausgenommen werden. Nach dem Training wird nur das optimierte Modell bzw. die Modellparameter (i. d. R. transportverschlüsselt[20]) zurück an den zentralen Server übertragen, nicht aber die personenbezogenen Daten. Auf dem zentralen Server werden dann die optimierten Modelle aller Endgeräte zusammengeführt; so ergibt sich ein neues, gesamt-optimiertes Modell.

---

17 Vgl. *Liu, Y., Kang, Y., Xing, C., Chen, T. & Yang, Q.* (2020). A secure federated transfer learning framework. IEEE Intelligent Systems, 35(4), S. 70–82.

18 Vgl. https://www.tensorflow.org/ (zuletzt abgerufen am 30.8.2022).

19 Vgl. https://pytorch.org/ (zuletzt abgerufen am 30.8.2022).

20 Auch eine (zusätzliche) Ende-zu-Ende-Verschlüsselung der Daten ist je nach Implementierung denkbar, falls beispielsweise das erforderliche Vertrauen in den Rechenzentrumsbetreiber, an dessen Servern die aktualisierten Modellparameter gesendet werden, nicht gegeben ist. Im Normalfall besteht jedoch keine Notwendigkeit, da an der Übertragung ohnehin nur das Endgerät und der zentrale Server beteiligt sind und die aktualisierten Modellparameter zur Zusammenführung zu einem gesamt-optimierten Modell nicht verschlüsselt vorliegen dürfen.

Der Vorteil dieses dezentralen Ansatzes liegt auf der Hand: Lokales Training ermöglicht grundsätzlich, alle vorhandenen Nutzerdaten im Klartext verwenden zu können. Damit besteht das Potential, Modelle ohne die Notwendigkeit von Aggregierungen oder Pseudonymisierungen datenschutzfreundlich zu trainieren. Daher stellt Federated Learning eine vielversprechende Anwendung im Bereich des sog. Privacy-Preserving Machine Learning dar.[21]

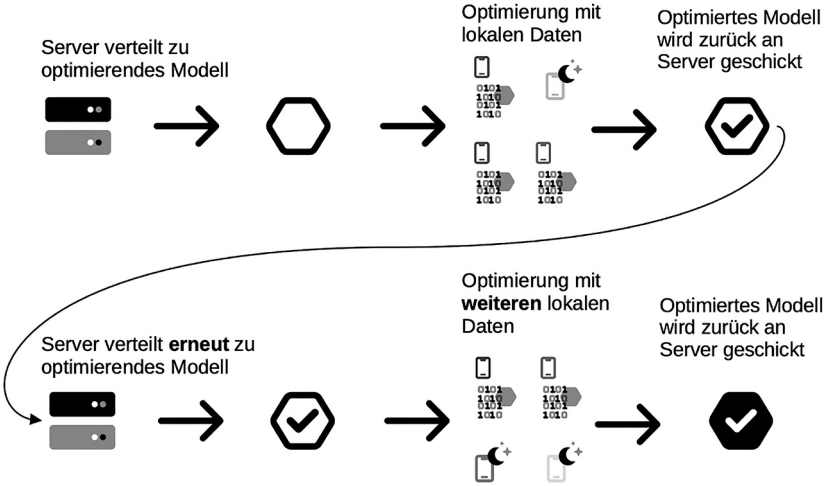


Abbildung 1: Model-Centric, Cross-Device Federated Learning: In einem ersten Schritt speichern die verfügbaren Endgeräte das vom zentralen Server verteilte, zu optimierende Modell. Anschließend erfolgt die Optimierung des Modells lokal auf den Endgeräten mit nur dort gespeicherten Daten. Möglicherweise sind einige Endgeräte zum Zeitpunkt der Optimierung nicht verfügbar (kein ausreichender Akkustand, Flugmodus, etc.); die Optimierung kann daher auch mit einer Teilmenge aller möglichen Endgeräte erfolgen. Danach schicken die Endgeräte die optimierten Modellparameter zurück an den zentralen Server. Im zweiten Schritt beginnt der Ablauf von vorne. Die verfügbaren Endgeräte speichern das (nun optimierte) vom Server verschickte Modell, diesmal werden für die weitere Optimierung jedoch andere Endgeräte verwendet. Die jeweiligen neuen Modellparameter werden an den zentralen Server geschickt und fließen wieder in die Optimierung des Gesamtmodells ein. Dieser Zyklus kann beliebig oft über einen längeren Zeitraum hinweg wiederholt werden.

21 Für mögliche Anwendungsbereiche vgl. nur: *Alam, T. & Gupta, R.* (2022). Federated Learning and Its Role in the Privacy Preservation of IoT Devices. Future Internet, 14(9), S. 246; *Dayan, I. et al.* (2021). Federated learning for predicting clinical outcomes in patients with COVID-19. *Nature medicine*, *27*(10), S. 1735–1743; *Yang, Q., Liu, Y., Chen, T. & Tong, Y.* (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2), S. 1–19.

15.3 Datenschutzrechtliche Folgen und Einordnung

Durch den Einsatz von Federated Learning können somit sowohl das Risiko bei der Übertragung an die zentrale Stelle als auch Risiken aus der zentralen Speicherung von Daten minimiert werden. Von den Endgeräten an den Server werden lediglich Modellparameter übertragen – nicht die Trainingsdaten selbst. In der Folge existiert auch keine zentrale Stelle, welche über alle Trainingsdaten verfügt (bzw., im Falle des zentralen Trainings, verfügen muss). Zwar kann für die zentrale Stelle auch die Übermittlung der Modellparameter durch das einzelne Endgerät noch personenbezogen sein;[22] allerdings ist damit bereits ein deutlich verringertes Risiko für Betroffene verbunden.[23] Gleichzeitig ist ein Training auf realen personenbezogenen Trainingsdaten als Klardaten möglich – ohne, dass der Verantwortliche auf die Anonymisierung von Trainingsdaten oder auf synthetische Trainingsdaten zurückgreifen müsste. Aktuelle Arbeiten in der technischen Datenschutzforschung deuten darauf hin, dass gerade die Verwendung von synthetischen Trainingsdaten mit Blick auf den Zielkonflikt *privacy-gain vs. utility* entgegen der damit verbundenen Hoffnungen nur selten bessere Ergebnisse erzielt als klassische Anonymisierungsverfahren.[24] Dieser Zielkonflikt ist allerdings allgegenwärtig bei der Verwendung von sog. Privacy Preserving Technologies[25] und wird auch im Kontext von Federated Learning thematisiert.[26]

Trotzdem ist der Einsatz von Federated Learning auch aus datenschutzrechtlicher Sicht für Verantwortliche vorteilhaft und grundsätzlich empfehlenswert. Die resultierende Risikominimierung kann etwa im Rahmen einer Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO berücksichtigt werden.[27] Daneben ist Federated Learning richtig implementiert als geeignete technische Maßnahme i. S. d. Art. 25 Abs. 1, Art. 32 Abs. 1 DSGVO einzuordnen und kann auch im Rahmen einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO als risikoreduzierende Maßnahme relevant werden.

---

22 *Kaulartz*, in: Kaulartz/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, Kapitel 8.9, Rn. 27.

23 Dennoch sind Angriffe auf die Modelle denkbar, welche Risiken für Betroffene zur Folge haben können; siehe dazu im folgenden Abschnitt.

24 *Stadler, T., Oprisanu, B. & Troncoso, C.* (2022). Synthetic data–anonymisation groundhog day. In: 31st USENIX Security Symposium (USENIX Security 22), S. 1451–1468.

25 Vgl. etwa für eine Thematisierung des Zielkonflikts hinsichtlich des Anonymisierungsverfahrens Differential Privacy: *Bagdasaryan, E., Poursaeed, O. & Shmatikov, V.* (2019). Differential privacy has disparate impact on model accuracy in: Advances in Neural Information Processing Systems 32: Annual Conference on Neural Information Processing Systems 2019, NeurIPS 2019, S. 15453–15462.

26 *Yin, X., Zhu, Y. & Hu, J.* (2021). A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions. In: ACM Computing Surveys (CSUR), 54(6), Article no. 131, S. 26.

27 *Kaulartz/Huth*, DSB 2019, 276 (278).

Trotz der grundsätzlich datenschutzfreundlichen Konzeption sind technische Angriffe auf bereits trainierte Federated-Learning-Modelle möglich; diese werden im Folgenden erläutert und eingeordnet.

15.4 Angriffe auf Federated-Learning-Modelle

Auf ML-Modelle sind im Allgemeinen mehrere technische Angriffe denkbar; auch Federated-Learning-Anwendungen sind daher nicht vor Angriffen gefeit.[28] Im Folgenden werden Membership-Inference- und Model-Inversion-Angriffe beschrieben[29], die besonders relevant sind,[30] da Federated Learning gerade mögliche Rückschlüsse auf einzelne Personen erschweren soll.

Membership-Inference-Angriffe[31] zielen darauf ab herauszufinden, ob ein bestimmter Datensatz zum Trainieren eines ML-Modells verwendet wurde. Dabei ist potentiell die Herstellung eines Personenbezugs möglich, wenn der Angriff glückt. Der Angriff kann auf zwei Arten durchgeführt werden: Bei der aktiven Angriffsvariante wird das Trainingsverfahren manipuliert. Bei dem Angreifer kann es sich beispielsweise um einen Nutzer der Federated-Learning-Anwendung handeln, der seine aktualisierten Modellparameter nachteilig verändert, oder um die zentrale Stelle, die die erhaltenen aktualisierten Modellparameter manipuliert, bevor sie erneut an die Nutzer:innen ausgespielt werden.[32] Bei der passiven Angriffsvariante werden – entweder durch die zentrale Stelle oder durch einen Angreifer mit entsprechendem Zugang – Rückschlüsse aus der Beobachtung der aktualisierten Modellparameter gezogen.[33] Dabei ist es ausschlaggebend, welche konkreten Informationen über eine Person bekannt werden. Für ein besseres Verständnis lohnt sich die Betrachtung eines Beispiels: Die Information, dass eine konkrete Person mit ihren Daten am Training teilgenommen hat, kann je nach Anwendung weniger sensibel sein als medizinische Diagnosen, die die Person

28 *Liu, P., Xu, X. & Wang, W.* (2022). Threats, attacks and defenses to federated learning: issues, taxonomy and perspectives. *Cybersecurity*, *5*(1), S. 1–19.

29 Ebd.

30 Vgl. auch BSI, Sicherer, robuster und nachvollziehbarer Einsatz von KI, v. 9.2.2021, S. 5, abrufbar: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Herausforderungen_und_Massnahmen_KI.pdf (zuletzt abgerufen am 31.8.2022).

31 *Shokri, R., Stronati, M., Song, C. & Shmatikov, V.* (2017). Membership inference attacks against machine learning models. In *2017 IEEE symposium on security and privacy (SP)*, S. 3–18.

32 *Nasr, M., Shokri, R. & Houmansadr, A.* (2019). Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning. In *2019 IEEE symposium on security and privacy (SP)*, S. 739–753.

33 Ebd.

über die Tastatur eingegeben und beispielsweise an ihren Hausarzt übermittelt hat. Zugleich sind jedoch auch Anwendungen denkbar, bei denen lediglich die Tatsache, dass Daten einer Person Teil der Trainingsdaten sind, ein besonders sensibles Datum darstellen kann – etwa bei auf bestimmte Zielgruppen zugeschnittene Dating-Apps.[34]

Model-Inversion-Angriffe[35] zielen darauf ab, Trainingsdaten aus einem trainierten Modell zu extrahieren. Auch hier ist potentiell die Herstellung eines Personenbezugs zu einer konkreten Person möglich, wenn der Angriffe glückt. Ein gutes Beispiel für einen solchen Angriff liefern *Fredrikson et al.*:[36] Ein Angreifer kann ein erkennbares Bild einer Person erstellen, wenn er lediglich Zugriff auf die Schnittstelle (API) eines Gesichtserkennungssystems und den Namen der Person hat, deren Gesicht von dem Gesichtserkennungssystem erkannt wird.

Die durch diese Angriffe entstehende Möglichkeit eines Personenbezugs muss auch aus rechtlicher Sicht von Verantwortlichen berücksichtigt werden. Entscheidender Anknüpfungspunkt ist die Identifizierbarkeit i. S. d. Art. 4 Nr. 1 DSGVO. Konkretisiert wird dies durch ErwG 26 S. 3, 4 DSGVO: Ist es nach allgemeinem Ermessen wahrscheinlich, dass die Angriffe als Mittel (ggf. in Kombination mit weiteren Mitteln[37]) zur Identifizierung einer natürlichen Person genutzt werden, so ist die Identifizierbarkeit zu bejahen. Hinsichtlich der Frage, ob dies wahrscheinlich ist, „sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden" (ErwG 26 S. 4); zu berücksichtigen ist auch „die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen" (ErwG 26 S. 4).

Die Einordnung dieser technischen Angriffe wurde in der rechtswissenschaftlichen Literatur bereits aufgegriffen;[38] eine trennscharfe und zugleich verallgemeinerbare Abgrenzung, wann das Risiko eines Angriffs so hoch ist,

---

34 So bejahte die norwegische Datenschutzaufsichtsbehörde, dass bereits die Information, dass eine betroffene Person Nutzer:in der App „Grindr" ist, ein Datum i. S. d. Art. 9 DSGVO darstellt, vgl. Datatilsynet, Administrative fine – Grindr LLC, 13.12.2021, abrufbar: https://www.datatilsynet.no/contentassets/8ad827efefcb489ab1c7ba129609edb5/administrative-fine---grindr-llc.pdf; S. 40.

35 *Fredrikson, M., Jha, S. & Ristenpart, T.* (2015, October). Model inversion attacks that exploit confidence information and basic countermeasures. In: *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*, S. 1322–1333.

36 Ebd.

37 Denkbar ist etwa die kombinierte Nutzung von gezielten Recherchen in sozialen Netzwerken oder einer umgekehrten Bildersuche und einem Model-Inversion-Angriff.

38 Früh bereits: *Veale M, Binns R, Edwards L.* 2018 Algorithms that remember: model inversion attacks and data protection law. Phil. Trans. R. Soc. A 376, 20180083; vgl. daneben: *Kaulartz*, in: Kaulartz/Braegelmann, Rechtshandbuch Artificial Intelligence and Machine Learning, Kapitel 8.9, Rn. 2, 9 ff.; *Puschky*, ZD-Aktuell 2022, 00019;

dass ein ML-Modell bereits aufgrund der Existenz der Angriffsmöglichkeit als personenbezogenes Datum eingeordnet werden muss, hat sich jedoch bisher – soweit erkennbar – nicht herausgebildet. Aufgrund der Vielfältigkeit möglicher Datenverarbeitungen und der Natur des Begriffs des Personenbezugs nach Art. 4 Nr. 1 DSGVO dürften auch zukünftig lediglich Annäherungen zu erwarten sein.

An dieser Stelle wichtig ist jedenfalls, dass diese Angriffe – wie bereits oben erwähnt – auch auf Federated-Learning-Anwendungen möglich sind. Da Verantwortliche bei der Verwendung von Federated Learning – grundsätzlich zu Recht – davon ausgehen, besonders datenschutzfreundlich zu agieren, ist das Risiko der Herstellung eines Personenbezugs hier besonders relevant. Zugleich kann sich der datenschutzfreundliche Ansatz auch positiv auswirken: So ist es etwa für Model-Inversion-Angriffe erforderlich, zumindest bestimmte Daten einer Person zu kennen – welche auch aus öffentlich zugänglichen Quellen wie Social-Media-Profilen stammen können, um dadurch weitere, beim Training des Modells verwendete personenbezogene Daten aus dem Modell zu rekonstruieren.[39] Durch die Verteilung der Trainingsdaten auf zahlreiche Endgeräte kann diese Kenntnis erschwert werden, was grundsätzlich eine zusätzliche Hürde für potentielle Angreifer darstellt.

Im Ergebnis sollten Verantwortliche die durch die dargestellten Angriffe entstehenden Risiken frühzeitig berücksichtigen und diese durch geeignete technische und organisatorische Maßnahmen adressieren.[40] Die Angriffe stellen jedoch keinen Grund dar, grundsätzlich auf Federated-Learning-Anwendungen zu verzichten – deren Durchführung ist nicht trivial, das Risiko kann bei Federated-Learning-Modellen im Gegensatz zu „klassischen" ML-Modellen bereits etwas verringert sein und ist insbesondere einzelfallabhängig von den verwendeten Trainingsdaten, dem potentiellen Zugriff auf Modell und Trainingsdaten sowie daraus ableitbaren Aussagen.

Leicht/Sorge, Einsatz von KI-Systemen im Unternehmen, in: Roth/Corsten, Handbuch Digitalisierung, S. 1281 (1296 ff.).

39 In Bezug auf zentral trainierte ML-Modelle: *Kaulartz*, in: Kaulartz/Braegelmann, Rechtshandbuch Artificial Intelligence and Machine Learning, Kapitel 8.9 Rn. 13.

40 Für einen Überblick, welche Maßnahmen in der technischen Datenschutzforschung hierfür diskutiert werden, vgl. *Yin, X., Zhu, Y. & Hu, J.* (2021). A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions. In: ACM Computing Surveys (CSUR), 54(6), Article no. 131, S. 22 ff.

15.5 Art. 5 Abs. 3 E-Privacy-RL als Showstopper?

Unabhängig von originär datenschutzrechtlichen Fragestellungen ist im Rahmen des Trainings und des Einsatzes von Federated-Learning-Anwendungen auch Art. 5 Abs. 3 E-Privacy-RL relevant.[41] Die Norm ist inzwischen in § 25 TTDSG unionsrechtskonform im nationalen Recht umgesetzt.[42] Sie schützt die informationelle Integrität von Endgeräten.[43] Gegenstand der Regelung ist, dass die Speicherung von Informationen in dem Endgerät eines Endnutzers sowie der Zugriff auf bereits dort gespeicherte Informationen einer Einwilligung bedarf (§ 25 Abs. 1 TTDSG). Ob die Informationen einen Personenbezug aufweisen, ist nicht relevant.[44] Für die Anforderungen an diese Einwilligung verweist die Norm auf die DSGVO. Als Ausnahme von Abs. 1 und damit als gesetzliche Rechtfertigung eines Zugriffs bzw. einer Speicherung sind in § 25 Abs. 2 Nr. 1, 2 TTDSG nur zwei relativ eng begrenzte Erlaubnistatbestände vorgesehen. Relevant ist hier v. a. § 25 Abs. 2 Nr. 2 TTDSG, wonach dann keine Einwilligung erforderlich ist, wenn die Speicherung von bzw. der Zugriff auf Informationen „unbedingt erforderlich ist, damit der Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann".

Der Begriff des Endgeräts i. S. d. Art. 5 Abs. 3 E-Privacy-RL ist dabei weit auszulegen; das TTDSG verwendet den synonym zu verstehenden Begriff der „Endeinrichtung" und definiert diese in § 2 Abs. 2 Nr. 6 TTDSG als „jede direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtung zum Aussenden, Verarbeiten oder Empfangen von Nachrichten; sowohl bei direkten als auch bei indirekten Anschlüssen kann die Verbindung über Draht, optische Faser oder elektromagnetisch hergestellt werden; bei einem indirekten Anschluss ist zwischen der Endeinrichtung und der Schnittstelle des öffentlichen Netzes ein Gerät geschaltet."

---

41 Hinsichtlich des Streitstandes zum Verhältnis zwischen Art. 5 Abs. 3 ePrivacy-RL und der DSGVO sei an dieser Stelle lediglich verwiesen auf: *Hanloser*, ZD 2021, 399 (399 f.); *Grages*, CR 2021, 834 (836 f.); *Schwartmann/Reif/Burkhardt*, in: Schwartmann/Jaspers/Eckhardt TTDSG, § 25 Rn. 11 f.; *Ettig*, in: Taeger/Gabel TTDSG (4. Auflage 2022), § 25 Rn. 16, 18; *Schneider*, in: Assion TTDSG, § 25 Rn. 13 mit Verweis auf EDSA, Stellungnahme 5/2019, Rn. 40.

42 *Schneider*, in: Assion TTDSG, § 25 Rn. 13.

43 *Assion*, NJW-Aktuell 43/2019; *Heun/Assion*, in: Auernhammer DSGVO (7. Auflage 2020), Art. 95 Rn. 4; *Herrmann*, in: Assion TTDSG, § 1 Rn. 22; *Golland*, NJW 2021, 2238 (2239); auf das Adjektiv „informationelle" wird in der Literatur tlw. verzichtet, ohne dass damit eine unterschiedliche Bedeutung verbunden sein dürfte, vgl. etwa: *Hanloser*, ZD 2021, 399 (399); *Schneider*, in: Assion TTDSG, § 25 Rn. 23.

44 EuGH v. 1.10.2019 – Rs. C-673/17 (Planet49), Rn. 69; *Grages*, CR 2021, 834 (835).

Die Gesetzesbegründung des TTDSG nennt beispielhaft Küchengeräte, Heizkörperthermostate und Alarmsysteme als mögliche Endeinrichtungen.[45]

Folglich werden zahlreiche Endgeräte des Internet of Things unter diese Regelung fallen.[46] Die langjährige Bezeichnung „Cookie-Richtlinie" ist daher nur in Bezug auf einen Teil der unter Art. 5 Abs. 3 E-Privacy-RL fallenden Sachverhalte korrekt.[47] Umfasst sind neben der Speicherung und dem Zugriff auf Cookies im Webbrowser gerade auch zahlreiche andere Sachverhalte, in denen Informationen in einem Endgerät gespeichert oder auf dort gespeicherte Informationen zugegriffen werden soll.[48]

Relevant ist hinsichtlich des Trainings und Einsatzes von Federated-Learning-Anwendungen also, ob durch die Übermittlung des zu trainierenden Modells vom Server an die Endgeräte bzw. durch die Übermittlung der Modellparameter ein Zugriff bzw. eine Speicherung von Informationen i. S. d. § 25 Abs. 1 TTDSG vorliegt. Im Folgenden wird dabei zwischen dem Training einerseits und dem produktiven Einsatz andererseits unterschieden.

Hinsichtlich letzterem werden typischerweise durch die Ausführung der Anwendung durch den Nutzer Daten auf dem Endgerät gespeichert bzw. anderweitig verarbeitet. Hierfür kann etwa ein aktualisiertes Modell von dem zentralen Server übermittelt und auf dem Endgerät gespeichert werden. Insoweit handelt es sich aber um einen kaum von der Funktionalität der Anwendung zu trennenden Vorgang, sodass dies die Voraussetzung „unbedingt erforderlich" regelmäßig erfüllen dürfte. Fraglich ist dagegen, ob der Nutzer auch ausdrücklich einen föderierten Dienst gewünscht haben muss. Hier sollte die juristische Analyse jedoch eng am technischen Sachverhalt erfolgen. Mit Blick auf den Wortlaut der Norm ist lediglich der Vorgang der Speicherung bzw. des Zugriffs relevant. Wird eine Federated-Learning-Anwendung ausgeführt, so ist zwar denkbar, dass vor der lokalen Verarbeitung ein aktualisiertes Modell übermittelt und auf dem Endgerät gespeichert wird. Andere Speicherungen oder Zugriffe dürften jedoch typischerweise nicht vorliegen, sodass die Tatsache, dass das Training des Dienstes föderal erfolgte und weitere Endgeräte an der Entstehung des übermittelten Modells beteiligt waren, für die Beurteilung von § 25 Abs. 2 Nr. 2 TTDSG in der Regel nicht erheblich ist. Es ist daher nicht erforderlich, dass der Wunsch des Nutzers ausdrücklich die Nutzung einer föderierten Anwendung umfasst. Diese Ansicht zugrunde gelegt, lässt sich ein Einsatz von Federated-Learning-Anwendungen und damit verbundene Speicherungen von aktualisier-

45 BT-Drs. 19/27441, S. 38.
46 Vgl. BT-Drs. 19/27441, S. 38.
47 *Schneider*, in: Assion TTDSG, § 25 Rn. 2.
48 *Schneider*, in: Assion TTDSG, § 25 Rn. 2.

ten Modellen auf Endgeräten von Nutzern über § 25 Abs. 2 Nr. 2 TTDSG ohne das Erfordernis einer Einwilligung rechtfertigen.

Anders kann dies bei der Beurteilung der Trainingsphase gesehen werden. Dabei wird nicht nur ein aktualisiertes Modell auf dem Endgerät gespeichert, vielmehr werden nach erfolgtem lokalen Training optimierte Modellparameter an die zentrale Stelle übermittelt. Wird in letzterem ein Zugriff i. S. d. § 25 Abs. 1 TTDSG gesehen, so dürfte eine Rechtfertigung über § 25 Abs. 2 Nr. 2 TTDSG schwerer fallen, als dies beim produktiven Einsatz der Federated-Learning-Anwendung der Fall ist. Nutzer:innen werden regelmäßig nicht ausdrücklich ein Training des Modells wünschen, sondern sind lediglich an dem Einsatz des bereits optimierten Modells interessiert. Hierfür ist jedoch die Durchführung des Trainings auf dem einzelnen betrachteten Endgerät sowie der Zugriff auf optimierte Parameter nicht unbedingt erforderlich. In diesen Fällen könnte also eine Einwilligung erforderlich sein. Dies würde jedoch erfordern, dass auch eine Aussendung dieser Modellparameter einen Zugriff i. S. d. § 25 Abs. 1 TTDSG darstellt – was nach dem Wortlaut der Norm zumindest nicht explizit umfasst ist.

Im Ergebnis kommt es darauf jedoch nur an, wenn nicht bereits die Speicherung des aktualisierten Modells auf dem Endgerät zu Trainingszwecken einer Einwilligung bedarf. Anders als beim produktiven Einsatz einer Federated-Learning-Anwendung erfolgt die Speicherung des Modells nicht aufgrund des ausdrücklichen Wunsches des Nutzers. Es stellt daher einen entscheidenden Unterschied dar, ob der Nutzer einen Telemediendienst nutzen möchte, zu dessen Erbringung eine lokale Datenverarbeitung (hier in Form der Speicherung eines aktualisierten Modells) erforderlich ist – oder ob ein aktualisiertes Modell in Endgeräten gespeichert werden soll, damit diese das Modell mit den lokal verfügbaren Daten trainieren. Letzteres würde erfordern, dass der Nutzer genau einen solchen Telemediendienst, welcher das Training zum Gegenstand hat, wünscht. Davon dürfte häufig nicht auszugehen sein, sodass das Training von Federated-Learning-Anwendungen bereits aufgrund der Speicherung des zu trainierenden Modells im Endgerät einer Einwilligung bedarf.

Dieses Ergebnis steht im Kontrast zu der Erleichterung für Verantwortliche, welche beim Einsatz von datenschutzfreundlichen Technologien – aufgrund der damit verbundenen Risikoreduzierung für Betroffene auch zurecht – hinsichtlich der DSGVO entsteht, etwa bezüglich der Rechtsgrundlage der Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO.

Federated-Learning-Anwendungen sind dabei nur ein Beispiel für die zugrunde liegenden abweichenden Wertungen des Art. 5 Abs. 3 E-Privacy-RL im Vergleich zu jenen des Art. 6 Abs. 1 DSGVO. Während Verantwortliche für eine Datenverarbeitung nach Art. 6 Abs. 1 DSGVO auf einen weiteren

Katalog an möglichen Rechtfertigungsgründen zurückgreifen können, ist Art. 5 Abs. 3 E-Privacy-RL deutlich restriktiver formuliert. Ein Gleichlauf ist aufgrund der unterschiedlichen Schutzrichtungen[49] auch keinesfalls zwingend.

Denkbar ist dennoch, dass Art. 5 Abs. 3 E-Privacy-RL in Fällen wie dem vorliegenden als „Showstopper" fungiert. Dies hat zwar keine zwingenden rechtlichen Gründe – die Einholung einer Einwilligung ist ja stets möglich. Jedoch könnte das Erfordernis einer Einwilligung seitens der Verantwortlichen den Anreiz verringern, diese datenschutzfreundliche Technologie einzusetzen. Wenn ohnehin eine Einwilligung nach Art. 5 Abs. 3 E-Privacy-RL für das Training erforderlich ist, so erhöht dies ggf. den Anreiz, (dann ebenso einwilligungsbasiert) zentral trainierte ML-Systeme einzusetzen. Eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO könnte sodann im selben, aufgrund der E-Privacy-RL ohnehin erforderlichen Prozess eingeholt werden.

Auch für Betroffene kann es missverständlich erscheinen, wenn sie (auch) beim Einsatz von besonders datenschutzfreundlichen Technologien mit Einwilligungen konfrontiert werden. Zurecht wird die Allgegenwärtigkeit der Einwilligung und ein ggf. damit verbundener Verlust einer Warnfunktion für Betroffene u. a. unter dem Stichwort „Cookie-Fatigue" kritisch diskutiert.

Zugleich ist die informationelle Integrität von Endgeräten ein besonders wichtiges und schützenswertes Gut. Diese Ausführungen sollen daher keineswegs ein Plädoyer zur weitgehenden Aufweichung dieses Schutzes darstellen. Vielmehr soll damit beispielhaft verdeutlicht werden, wie die bisher ausgebliebene Abstimmung von Art. 5 Abs. 3 E-Privacy-RL und der DSGVO – auch und gerade beim Einsatz von datenschutzfreundlichen Technologien – einen bemerkenswerten Kontrast der rechtlichen Rahmenbedingungen verursachen kann. Zudem verbleiben trotz dieses Kontrasts Vorteile für Verantwortliche, die auf Federated Learning als datenschutzfreundliche Technologie setzen: Auch wenn eine Einwilligung erforderlich ist, verbleibt die Verringerung des Risikos für Betroffene, welche sich verschiedentlich positiv auswirkt und etwa im Rahmen von Art. 32 Abs. 1 oder Art. 35 DSGVO sowie ggf. bei Datenpannen i. S. d. Art. 33, 34 DSGVO nutzbar gemacht werden kann. Unabhängig von einer perspektivisch möglichen Änderung der Rechtslage lohnt es sich deshalb, Einsatzmöglichkeiten für Federated-Learning-Anwendungen zu prüfen.

49 Vgl. *Grages*, CR 2021, 834 (835 f.); *Heun/Assion*, in: Auernhammer DSGVO, Art. 95 Rn. 4.

15.6 Fazit und Ergebnis

Klassische ML-Anwendungen verarbeiten personenbezogene Daten zentral und halten die Trainingsdaten in einem zentralen Datenspeicher vor. Federated Learning ermöglicht dagegen das Auslagern des Trainings auf Endgeräte. (Personenbezogene) Trainingsdaten bleiben so auf den Endgeräten und müssen nicht an den zentralen Server übermittelt werden. Dennoch sind auf Federated-Learning-Anwendungen – wie bei allen ML-Anwendungen – Angriffe möglich. Besonders relevant in Bezug auf eine mögliche Herstellung eines Personenbezugs sind Membership-Inference- und Model-Inversion-Angriffe. Verantwortliche sollten insoweit eine Einzelfallprüfung vornehmen; entscheidend ist dabei u. a., von welchen Kenntnissen über die Trainingsdaten und die Modelle bei potentiellen Angreifer:innen auszugehen ist. Unter Hinzuziehung von geeigneten technischen und organisatorischen Maßnahmen können diese Risiken jedoch angemessen adressiert werden; zugleich ergeben sich zukünftig durch Federated Learning zahlreiche neue, datenschutzfreundlichere oder durch den Einsatz erst datenschutzkonforme Anwendungsbereiche.

Eine bisher ungelöste Herausforderung besteht im Umgang mit § 25 TTDSG. Zumindest hinsichtlich der Trainingsphase von Federated-Learning-Anwendungen dürfte nach hier vertretener Auffassung eine Einwilligung nach § 25 Abs. 1 TTDSG erforderlich sein. Dies verdeutlicht exemplarisch und besonders bemerkenswert – gerade, weil hier eine grundsätzlich datenschutzfreundliche(re) Technologie eingesetzt werden soll – den Kontrast von Art. 5 Abs. 3 E-Privacy-RL zur DSGVO. Abzuwarten bleibt, inwieweit dieser Kontrast im Falle einer ggf. zukünftig geltenden E-Privacy-VO bestehen bleibt.

16 Erneuerung der Ausbildung durch Legal Tech

*Christina-Maria Leeb, Til Bußmann-Welsch & Christian Schlicht**

Im Rahmen der diesjährigen Telemedicus Sommerkonferenz wurde kontrovers über „Legal Tech" in der juristischen Ausbildung und im Referendariat diskutiert. Die Schwerpunkte der Diskussion und unsere Standpunkte sollen zusätzliche Impulse für die weitere Reform geben.

16.1 Legal Tech als fester Bestandteil der juristischen Ausbildung

Die Verfasser:innen verstehen den Begriff „Legal Tech" im Zusammenhang mit der juristischen Ausbildung speziell für die Zwecke dieses Beitrags weit.[1] Gemeint sind jedwede Aspekte der Digitalisierung der juristischen Arbeit. In allen juristischen Berufsfeldern ist die Digitalisierung präsent. Eine sinnvolle Vorbereitung sowohl auf die klassischen juristischen Berufsbilder als auch auf alle angrenzenden und fachfremden Berufe, in denen Jurist:innen arbeiten, ist ohne Digitalisierungskenntnisse schon heute nicht mehr zeitgemäß. Die Verfasserin und die Verfasser sind sich einig, dass „Legal Tech" ein fester Bestandteil der juristischen Ausbildung sein muss.

Zu begrüßen sind daher Initiativen und Gesetzesänderungen, die auf eine weitere Einbindung von „Legal Tech" in das Jurastudium abzielen. Etwa das neue Juristenausbildungsgesetz Nordrhein-Westfalen (JAG NRW), das am 17.2.2022 in Kraft trat, sieht hierzu eine Freisemesterregelung vor (§ 25 Abs. 2 Nr. 4 JAG NRW n. F.[2]).[3] Dieser Weg berücksichtigt, dass Jurastudent:innen regelmäßig „examensfixiert" und „klausurtaktisch" lernen

---

* Mehr über die Autor:innen erfahren Sie im Autor:innenhinweis auf S. 224 ff.

1 Zum unterschiedlichen Begriffsverständnis etwa *Leeb,* Digitalisierung, Legal Technology und Innovation, 2019, S. 50 ff.

2 „Bei der Berechnung der Semesterzahl nach Absatz 1 Satz 1 bleiben unberücksichtigt und gelten nicht als Unterbrechung: ein Semester für eine an einer inländischen Hochschule nachweislich erfolgreich abgeschlossene fremdsprachige rechtswissenschaftliche Ausbildung oder eine Ausbildung im Bereich Digitalisierung und Recht, die sich über mindestens sechzehn Semesterwochenstunden erstreckt hat." (Unterstreichung nur hier).

3 Eine anschauliche Zusammenfassung der Neuregelungen findet sich unter https://landesfachschaft.de/2021/12/neues-jag-tritt-im-februar-2022-in-kraft-neuregelungen-im-ueberblick/.

und ihre Lehrveranstaltungen auswählen.[4] Alternativ zu einem Freisemester wäre die Aufnahme in den Pflichtfachkatalog erwägenswert. Uneinigkeit herrschte auf dem Panel bei der Frage, ob es sinnvoll sei, bloß freiwillige Veranstaltungen zu (juristischen) Technologiethemen anzubieten. Dafür wurde insbesondere angeführt, dass niederschwellige Angebote auch bei denen Interesse wecken könnten, die bisher mit dem Themenbereich „Legal Tech" noch nicht in Berührung gekommen waren. Dagegen wurde angeführt, dass solche Veranstaltungen neben dem Pflichtfachkatalog nur wenig Resonanz erfahren könnten, weil die Student:innen sich auf examensrelevante Bereiche fokussierten. Wer sich gleichwohl für Digitalthemen interessiere, müsse zwangsläufig überobligatorisch viele Veranstaltungen besuchen.

Dass Legal-Tech-Veranstaltungen auf große Resonanz stoßen, zeigt beispielhaft die Initiative Bayerns, wo im Rahmen des Referendariats nach einer Auftaktveranstaltung in Gestalt des „Innovationstages Legal Tech" am 16.2.2022 mehrere vertiefende Zusatzveranstaltungen stattfinden werden.[5] Darüber hinaus wird demnächst ein neues Berufsfeld zu dieser Thematik angeboten. Das Berufsfeld bildet im bayerischen Referendariat einen gewichtigen Teil der mündlichen Prüfung in der ZJS und bestimmt die Wahlstation.

Neben speziellen „Legal Tech"-Angeboten sollten im Rahmen der gesamten juristischen Ausbildung technische Sachverhalte in allen Rechtsgebieten den Stellenwert erhalten, den sie in der realen Welt inzwischen einnehmen.[6] Beispielhaft betrifft dies Verkäufe über Internetplattformen, bargeldlosen Zahlungsverkehr, den Handel mit Bitcoins, die elektronische Kommunikation mit Gerichten, Behörden und Privatpersonen oder die öffentlich-rechtliche Genehmigung neuer Technologien.[7] Auch hier ist aber wichtig, zunächst das juristische und methodische „Rüstzeug" zu vermitteln, um dieses angemessen auf technische, komplexe Sachverhalte anwenden zu können.

---

4 Eine hiervon losgelöste Frage ist selbstverständlich, inwieweit diese Motivationslage sinnvoll ist und welche weiteren Schritte ergriffen werden könnten, um sich hiervon zu lösen.

5 Vgl. hierzu *Leeb,* Innovationstag Legal Tech für Rechtsreferendarinnen und Rechtsreferendare, abrufbar unter https://legal-tech-verzeichnis.de/legal-tech-ausbildung-karriere-magazin-1-22/#legal-tech-ausbildung-karriere-magazin-01-2022/1/.

6 Nach Aussage eines Referenten des bayrischen Justizministeriums im Gespräch mit Bußmann-Welsch äußerte dieser beispielsweise bereits, dass Examensklausuren mit kaufrechtlichem Einschlag aufgrund der Änderungen durch die Richtlinie über digitale Inhalte wohl kaum noch im klassischen Sinne „analog" ausgestaltet werden könnten.

7 Exemplarisch für eine gelungene Verflechtung etwa die Anfängerklausur – Zivilrecht: BGB AT – Elektroauto gegen Bitcoins? von *Herberger*, JuS 2022, 326 ff.

16.2 Methodische, didaktische und digitale Fähigkeiten statt Stofffülle

Der Pflichtfachstoff in den juristischen Examina sollte weiter reduziert werden. Nur so besteht überhaupt die Chance, dass Jurastudent:innen sich mit neuen Aspekten der Digitalisierung auseinandersetzen. Umstritten war hingegen die Frage, ob und inwieweit Jurastudent:innen besondere digitale Fähigkeiten vermittelt werden sollten. Auf dem Panel bestand Einigkeit, den Fokus auf (digitale) Recherchekompetenzen zu legen. Die heutige universitäre Examensvorbereitung und die Staatsexamensklausuren beruhen noch überwiegend auf dem Gedanken, dass Wissen nicht allgemein verfügbar ist und (auswendig) gelernt werden muss (Wissen statt Können). Tatsächlich ist Wissen aufgrund moderner Technologie aber auf Geräte ausgelagert und kann im Berufsalltag jederzeit abgerufen werden. Diesen Aspekt – nicht aber das Grundverständnis und die Fähigkeit, das passende Wissen „aufzuspüren" – gilt es in der Ausbildung und im Examen stärker zu berücksichtigen (Können statt Wissen).

Dies könnte einerseits dadurch geschehen, dass weniger Wissen abgeprüft wird, andererseits durch die Möglichkeit, (auch im ersten Examen) Kommentare sowie – das wäre neu – juristische Datenbanken oder allgemein zugängliche Quellen nutzen zu können. Letzteres würde den Alltag bei Gericht, in Kanzleien und Unternehmen abbilden und auf die Tätigkeit als Jurist:in noch besser vorbereiten. Soweit Universitäten kostenlose Seminare zur juristischen Recherche anbieten, ist dies überaus erfreulich und an alle Student:innen kann nur appelliert werden, diese zu besuchen. Sofern es noch Universitäten gibt, die solche Angebote nicht haben, müssen diese dringend geschaffen und im Übrigen erweitert werden.

Sollten allen Jurastudent:innen überdies auch der Umgang mit spezieller Software oder gar Programmierkenntnisse vermittelt werden? Diese Überlegungen stießen in der Diskussion eher auf Ablehnung. Allen Interessierten sei es unbenommen, sich neben dem Jurastudium in diesem Bereich fortzubilden. Das Jurastudium solle nicht „halbe Jurist:innen und halbe Informatiker:innen" ausbilden. Schließlich werden sich perspektivisch weitere Fragen stellen, wie mit nicht-linearen Arbeitsprodukten umzugehen sein wird. Dies schließt jedoch nicht aus, dass dem jeweiligen Geiste der Zeit entsprechende Softwarelösungen auch in den studentischen Alltag Einzug halten.[8] Heute wird an den Universitäten noch ganz überwiegend mit starren Sachverhalten, Aktenstücken und Aufsätzen gearbeitet. Auch dies entspricht nicht mehr allerorts der komplexen und kollaborativen Arbeitsweise an dy-

8 Begrüßenswert sind etwa Veranstaltungen wie die von *Anton Sefkow* an der Universität Hamburg, vgl. https://legal-tech-verzeichnis.de/fachartikel/studienseminar-mit-legal-tech-recht-gestalten-mltrg/.

namischen und hybriden Dokumenten und Medien, etwa in geteilten Datenräumen.

16.3 E-Examen & weitere Reformdiskussionen, insbesondere zum Bachelor

Sehr zu begrüßen ist die Möglichkeit, Examensklausuren elektronisch anfertigen zu können. Dies ist bereits heute in Sachsen und Sachsen-Anhalt der Fall.[9] Ab dem 1.1.2024 sind etwa auch die Justizprüfungsämter in Nordrhein-Westfalen verpflichtet, den Examenskandidat:innen eine elektronische Anfertigung der Klausuren zu ermöglichen (§ 10 Abs. 1 S. 3 JAG NRW n. F.).[10] Dass Prüflinge sich dann entscheiden können, ob sie die Arbeiten wie gehabt per Hand oder aber am Computer anfertigen wollen, ist zumindest für eine Übergangszeit sinnvoll.

Abseits der Fragestellungen zu „Legal Tech" war die generelle Reformierung des Jurastudiums (und Referendariats) Thema der Paneldiskussion. Die Einführung des Bachelor ist ausdrücklich zu begrüßen.[11] Es nimmt Jurastudent:innen die Angst, ohne erfolgreich abgeschlossenes Examen mit „leeren Händen da zu stehen". Zugleich bietet der Bachelor denjenigen, die sich während des Studiums zu einer anderen (Querschnitts-)Thematik hin orientieren möchten, die nötige Durchlässigkeit. Allerdings sollte die Möglichkeit, vor Gerichten mit Anwaltszwang auftreten zu dürfen, nach der Mehrheit der Diskutant:innen, weiterhin auf diejenigen Personen beschränkt bleiben, die beide juristische Staatsexamina erfolgreich abgeschlossen haben.

9 https://www.lto.de/karriere/jura-referendariat/stories/detail/welche-bundeslaender-fuehren-e-examen-ein-jura-referendariat-studium-digitalisierung.

10 Berlin und Brandenburg planen den Einstieg nach Aussage des Kammergerichtes und des Gemeinsamen Juristischen Prüfungsamtes der Länder Berlin und Brandenburg Ende des Jahres 2023.

11 Anders etwa *Chiusi*, https://www.faz.net/aktuell/politik/staat-und-recht/sinnhaftigkeit-des-bachelors-fuer-jurastudenten-18138005.html; dagegen etwa *Ogorek*, https://www.faz.net/aktuell/politik/staat-und-recht/kritik-am-bachelor-im-jurastudium-offenbart-reformunwillen-18170307.html; *Heymann*/*Luft*/*Reith*, https://www.faz.net/aktuell/politik/staat-und-recht/sollte-ein-jura-bachelor-eingefuehrt-werden-18193063.html. Vgl. hierzu auch die Folge 217 des FAZ Einspruch-Podcast, abrufbar unter https://www.faz.net/podcasts/f-a-z-einspruch-podcast/jura-bachelor-statt-staatsexamen-debatte-zwischen-professorinnen-18169957.html.

16.4 Zusammenfassung und Ausblick

Die kurze Podiumsdiskussion bot nur die Gelegenheit, die vorstehenden Themen ausschnittweise anzureißen. Erfreulich ist, dass bereits einzelne Reformvorschläge umgesetzt wurden oder sich einzelne Bundesländer Reformdiskussionen öffnen.[12] Es bleibt zu hoffen, dass die Auswertung der professionsübergreifenden Abstimmung der Initiative *iur.reform* Politik, Wissenschaft und Praxis neue Einblicke liefert und hieraus konkrete Verbesserungen erwachsen.[13]

12 Vgl. insoweit den Entwurf eines Gesetzes zur Änderung des Niedersächsischen Gesetzes zur Ausbildung der Juristinnen und Juristen der Fraktionen von SPD und CDU sowie dem Antrag „Juristenausbildung zukunftsfest aufstellen" der FDP-Fraktion des Landes Niedersachsen.

13 Zu den Reformoptionen: https://iurreform.de/reformoptionen/. An der Abstimmung haben sich rund 12.000 Jurist:innen aus dem gesamten Bundesgebiet und über alle Professionen hinweg beteiligt.

17 Das Projekt Synco (Cybersyn) – Verdatung und Globalsteuerung in Chile Anfang der 1970er Jahre

*Sarah Hünting**

Während sich die Bundesregierung in Deutschland mittels des Stabilitätsgesetzes (Gesetz zur Förderung der Stabilität und des Wachstums der Wirtschaft 1967) an einer rechtlichen Grundlage für das Konzept der Globalsteuerung versuchte, entwarf *Stafford Beer* 1970 im Auftrag des chilenischen Präsidenten *Salvador Allende* das Projekt Cybersyn. Dieses sollte zur Echtzeit-Regulierung der Sozialwirtschaft in Chile beitragen. Der erste weltweite Versuch einer datengestützten wirtschaftlichen Globalsteuerung. Beide Ideen werden in diesem Beitrag genauer dargestellt und mögliche Bezüge zum Sozialkreditsystem in China dargestellt.

17.1 Eine datengesteuerte Regulierung

Big Data[1] soll neue Möglichkeiten bieten. Gleichzeitig wächst die Kritik an der Datenspeicherung wegen des mangelnden Schutzes der Privatsphäre und der Zentralisierung der Daten. Rufe nach einer datengesteuerten dynamischen Regulierung gab es bereits in der Vergangenheit.

In Chile führte diese Idee unter Mitwirkung des Konzeptes der „Globalsteuerung" der Wirtschaft[2] zur Schaffung von Cybersyn (Cybernetic Synergy), einem Computersystem, das zur Verwaltung der sozialistischen Wirtschaft geschaffen wurde. Im gleichen Zeitrahmen beschäftigte sich auch die deutsche Politik mit dem Konzept der Globalsteuerung. Im Jahr 1967 verabschiedete der Deutsche Bundestag das „Gesetz zur Förderung der Stabilität

---

* Mehr über die Autorin erfahren Sie im Autor:innenhinweis auf S. 224 ff.

1 Eine große Datenmenge, häufig auch definiert durch die vier Merkmale, Volumen (extreme Datenmengen), Varietät (verschiedene Datenformate), Velozität (schnelle Veränderung von Daten) und Value (Mehrwert, der sich durch Daten generieren lässt), mehr dazu siehe *Zeisel*, Big Data und Data Science in der strategischen Beschaffung, 2020, S. 3.

2 „Globalsteuerung" ist der dauerhafte Prozess staatlicher Einwirkung auf den Verlauf der wirtschaftlichen Entwicklung, genauer „die staatliche Beeinflussung der Makrorelationen über eine entsprechende Haushalts-, Kredit- und Steuerpolitik bei gleichzeitiger Selbstregulierung des Mikrobereiches", *Frotscher/Kramer*, Wirtschaftsverfassungs- und Wirtschaftsverwaltungsrecht, JuS Schriftenreihe 7. Auflage, S. 13.

und des Wachstums der Wirtschaft“ (StabG).[3] Ziel der damaligen wie auch der heutigen Bundesregierung ist die Vollbeschäftigung, Preisstabilität, außenwirtschaftliches Gleichgewicht und ein angemessenes Wirtschaftswachstum, auch als „magisches Viereck“ bekannt.[4]

Grundlage des staatlichen Handelns sind dabei ebenfalls Daten – in diesem Fall anhand des jährlich von der Bundesregierung vorzulegenden Wirtschaftsberichts. Erfolge zeigten sich unter anderem in der niedrigen Arbeitslosigkeit (0,9 Prozent) zum Ende der Legislaturperiode (1969).[5] Ihren niedrigsten Wert erreichte diese 1970 mit 0,7 Prozent.[6] Allerding deuteten sich die Grenzen der Globalsteuerung schon 1973 im Rahmen der Ölkrise an und die deutsche Politik entfernte sich von der Idee einer einheitlichen Steuerung in den 90er Jahren. Heute gewinnt das Konzept und die aufgeworfenen Fragen im Rahmen der Wirtschaftspolitik wieder mehr Aufmerksamkeit. Das Stabilitätsgesetz gilt nach wie vor.[7]

Neben der Globalsteuerung steckt hinter dem Projekt Cybersyn der Versuch die Wirtschaft im Land mittels Daten zu erfassen und zu repräsentieren. Eine solche Sammlung von Daten kann man ebenfalls im Rahmen der Registermodernisierung[8] in Deutschland beobachten, wobei neben dem steuerlichen Unternehmenskennzeichen auch eine Personenkennziffer[9] zur Datenerhebung konzipiert wurde. Folglich werden sowohl juristische als auch natürliche Personen erfasst.[10] Ähnliches zeigt die Anwendung des Statistikregistergesetzes,[11] wobei dieses auch als deutsches Pendant zu Cybersyn betrachtet werden kann. Mittels des Gesetzes wurde zuletzt 2019 die EU-Rahmenverordnung[12] in nationales Recht umgesetzt. Ziel ist eine EU-weite Harmonisierung der Unternehmensstatistik und eine breitere Einbeziehung wirtschaftlicher Aktivitäten. Die EU verspricht sich hieraus

3 Gesetz zur Förderung der Stabilität und des Wachstums der Wirtschaft vom 8.6.1967, BGBl. I, 582; zuletzt geändert durch VO vom 31.8.201, BGBl. I, 1474.
4 § 1 S. 2 StabG; *v. Arnim*, Volkswirtschaftspolitik, 6. Aufl. 1998, S. 144 f.
5 Statistisches Bundesamt, Registrierte Arbeitslose, Arbeitslosenquote nach Gebietsstand, Stand 1.7.2022 (https://www.destatis.de/DE/Themen/Wirtschaft/Konjunkturindikatoren/Lange-Reihen/Arbeitsmarkt/lrarb003ga.html 29.7.2022).
6 Statistisches Bundesamt, Registrierte Arbeitslose, Arbeitslosenquote nach Gebietsstand, Stand 1.7.2022 (https://www.destatis.de/DE/Themen/Wirtschaft/Konjunkturindikatoren/Lange-Reihen/Arbeitsmarkt/lrarb003ga.html 29.7.2022).
7 *Frotscher/Kramer*, Wirtschaftsverfassungs- und Wirtschaftsverwaltungsrecht, JuS Schriftenreihe 7. Auflage, S. 116.
8 Registermodernisierungsgesetz vom 28.3.2021, zuletzt geändert durch Gesetz vom 9.7.2021, BGBl. I S. 2467.
9 § 139b AO.
10 § 139a AO.
11 Statistikregistergesetz vom 16.6.1998, zuletzt geändert durch Gesetz vom 10.8.2021, BGBl. I S. 3436.
12 Regulation on European Business Statistics Nr. 2019/2152.

eine verbesserte qualitative Abbildung der europäischen Unternehmenslandschaft und eine bessere intraeuropäische Vergleichbarkeit der statistischen Daten.

Zurück zu den Ursprüngen, wo Cybersyn als Vorreiter dieser Konzepte dazu beitragen sollte, eine Echtzeit-Kontrolle der Wirtschaft zu ermöglichen.[13]

17.1.1 Historischer Abriss

Chile 1970, *Salvador Allende* gewann die Wahlen mit einer knappen Mehrheit, musste jedoch vom Kongress bestätigt werden, da er nicht über die absolute Mehrheit verfügte.[14] Die Bemühungen des rechten Flügels konzentrierten sich darauf, diese Ratifizierung zu verhindern und schufen ein Klima der Angst, wirtschaftlichen Unsicherheit und Gewalt. Am 24.10.1970 ratifizierte der Kongress *Allende* als ersten demokratisch gewählten sozialistischen Präsidenten von Chile. Seinen endgültigen Sieg errang er dank der Intervention der Christdemokraten, die die Mehrheit im Parlament stellten.[15]

Der „chilenische Weg zum Sozialismus“[16] brachte tiefgreifende demokratische und soziale Reformen und Veränderungen in der wirtschaftlichen, politischen und sozialen Struktur mit sich: Die Verstaatlichung des Kupfers, die Vertiefung der Agrarreform, die Ausweitung der Rechte im Gesundheits- und Bildungswesen, die Kontrolle der Produktpreise und die Verstaatlichung von Unternehmen, die von der Regierung als strategisch angesehen wurden.[17]

Die politische Kampagne des Terrors und der Konfrontation, welche bereits bei den Wahlen herrschte, wurde auch während der Regierung *Allendes* fortgesetzt: Sie richtete sich gegen die von der Regierung im Parlament vorgestellten Projekte, organisierte die Verknappung von Grunderzeugnissen, internationale Boykotte und Streiks der Unternehmer:innen. Am

13 *Medina*, Designing Freedom, Regulating a Nation: Socialist Cybernetics in Allende’s Chile, Journal of Latin American Studies Vol. 38, No. 3, Aug. 2006, S. 572.

14 *Puelma*, Chile 1970–1973, Die Zerschlagung einer Demokratie, Allendes chilenischer Weg zum sozialistischen Volksstaat, S. 9.

15 *Puelma*, Chile 1970–1973, Die Zerschlagung einer Demokratie, Allendes chilenischer Weg zum sozialistischen Volksstaat, S. 11 f.

16 Der Weg zum Sozialismus sollte unter Wahrung demokratischer Strukturen erfolgen. *Medina*, Designing Freedom, Regulating a Nation: Socialist Cybernetics in Allende’s Chile, Journal of Latin American Studies Vol. 38, No. 3, Aug. 2006, S. 595; *Puelma*, Chile 1970–1973, Die Zerschlagung einer Demokratie, Allendes chilenischer Weg zum sozialistischen Volksstaat, S. 16 f.

17 *Puelma*, Chile 1970–1973, Die Zerschlagung einer Demokratie, Allendes chilenischer Weg zum sozialistischen Volksstaat, S. 18 f.

11.9.1973 wurde die Regierung durch einen von der Opposition angeführten Militärputsch gestürzt.[18]

17.1.2 Die Idee

Nach der Verstaatlichung und Eingliederung verschiedener volkseigener Betriebe in den Staat sah sich das Wirtschaftssystem der Regierung *Allendes* mit der Notwendigkeit konfrontiert, alle Informationen aus staatlichen und neu verstaatlichten Unternehmen zu koordinieren. Um dies zu erreichen, musste ein dynamisches und flexibles Informationsübertragungssystem geschaffen werden.

1970 wurde *Fernando Flores* zum technischen Generaldirektor der CORFO (Corporación para el Fomento de la Producción de Chile)[19] ernannt. Er war für die Verwaltung und Koordinierung zwischen den verstaatlichten Unternehmen und dem Staat zuständig. Zusammen mit *Raúl Espejo*,[20] der ebenfalls bei CORFO arbeitete, schrieb er einen Brief an *Stafford Beer*,[21] um ihn einzuladen, das Viable System Model (VSM)[22] in Chile einzuführen, ein Modell, das in seinem Buch „The Brain of The Firm"[23] beschrieben wurde.[24] Beer akzeptierte und das Projekt begann 1971 mit seiner Entwicklung. Nach einer mehrmonatigen Entwicklungszeit wurde das kybernetische Regierungsprojekt vom Präsidenten *Salvador Allende* zur Umsetzung genehmigt. Das Projekt Cybersyn sollte eine Echtzeit Steuerung der Wirtschaft ermöglichen. Dabei sollten sowohl die Produktions- als auch die Nachfra-

18 *Puelma*, Chile 1970–1973, Die Zerschlagung einer Demokratie, Allendes chilenischer Weg zum sozialistischen Volksstaat, S. 91.

19 Gesellschaft für die Förderung der Produktion in Chile.

20 *Medina*, Designing Freedom, Regulating a Nation: Socialist Cybernetics in Allende's Chile, Journal of Latin American Studies Vol. 38, No. 3, Aug. 2006, S. 577–578.

21 Mehr zu Stafford Beer siehe *Medina*, Designing Freedom, Regulating a Nation: Socialist Cybernetics in Allende's Chile, Journal of Latin American Studies Vol. 38, No. 3, Aug. 2006, S. 576–577.

22 Das VSM stellt eine Struktur von teilautonomen Systemen dar, die sich an Umwelten anpassen sollen. Es kann in Form von zwei Varianten eingesetzt werden, einerseits zur Diagnose von Problemen in der bestehenden Organisation, andererseits zur Entwicklung neuer und effizienter Strukturen. Mehr dazu *Rezaee, Z., Azar, A., Erz, A. M.B. et al.* Application of Viable System Model in Diagnosis of Organizational Structure. Syst Pract Action Res 32, 273–295 (2019).

23 *Beer*, Brain of the Firm, 1972.

24 *Medina*, Designing Freedom, Regulating a Nation: Socialist Cybernetics in Allende's Chile, Journal of Latin American Studies Vol. 38, No. 3, Aug. 2006, S. 571.

gestrukturen identifiziert und zu einem Abgleich gebracht werden und mit einer zentralen Steuerung der Produktion verbunden werden.[25]

17.1.3 Cybersyn

Beer und das chilenische Team entwarfen die Komponenten des Cybersyn-Projekts, analog des Viable System Models (VSM). Das VSM stellt eine Struktur von teilautonomen Systemen dar, die sich an Umwelten anpassen sollen. Nach Beers Vorstellung kann jede Organisation mittels des VSMs abgebildet werden. Das VSM kann auf zwei Arten eingesetzt werden: zur Diagnose von Problemen in der bestehenden Organisation oder zur Entwicklung neuer und effizienterer Strukturen. Gemäß Beer benötigt ein System für seine Lebensfähigkeit fünf Systeme oder strukturelle Komponenten, die im VSM eingeführt wurden.

Diese fünf Systeme[26] teilten sich bei Cybersyn wie folgt auf:

1) Industrie Chiles;
2) Cybernet, ein Kommunikations- und Koordinationsnetzwerk für den Datenaustausch in Echtzeit, welches via 500 Telefax-Maschinen hergestellt wurde und so eine Vielzahl der verstaatlichten Produktionsstätten im Land verlinkte;
3) Cyberstride, ein integriertes Software- und Hardwaresystem, das die Daten des Systems verarbeiten sollte, Gefahrenpotenziale erkennen und ihre Komplexität reduzieren;
4) CHECO (CHilean ECOnomy), ein dynamisches Modell für die Erstellung aktueller 10-Jahres-Simulationen, auf der Grundlage der eingespeisten Daten. Die von Cyberstride verarbeiteten Output-Daten der Systeme 1 bis 3 sollten für ein tägliches Update von Checo verwendet werden;
5) Operations Room, ein Betriebsraum, der als Gesprächsraum für politische Entscheidungen konzipiert war; hier sollten auf der Basis der in den Systemen 3 und 4 gesammelten und aufbereiteten Real-Time- und Simulations-Informationen grundsätzliche Entscheidungslinien festgelegt werden.

---

25 *Medina*, Designing Freedom, Regulating a Nation: Socialist Cybernetics in Allende's Chile, Journal of Latin American Studies Vol. 38, No. 3, Aug. 2006, S. 599.

26 *Arnold* in Geitz/Vater/Zimmer-Merkle, Black Boxes – Versiegelungskontexte und Öffnungsversuche, S. 29; *Medina*, Designing Freedom, Regulating a Nation: Socialist Cybernetics in Allende's Chile, Journal of Latin American Studies Vol. 38, No. 3, Aug. 2006, S. 585, 587–590.

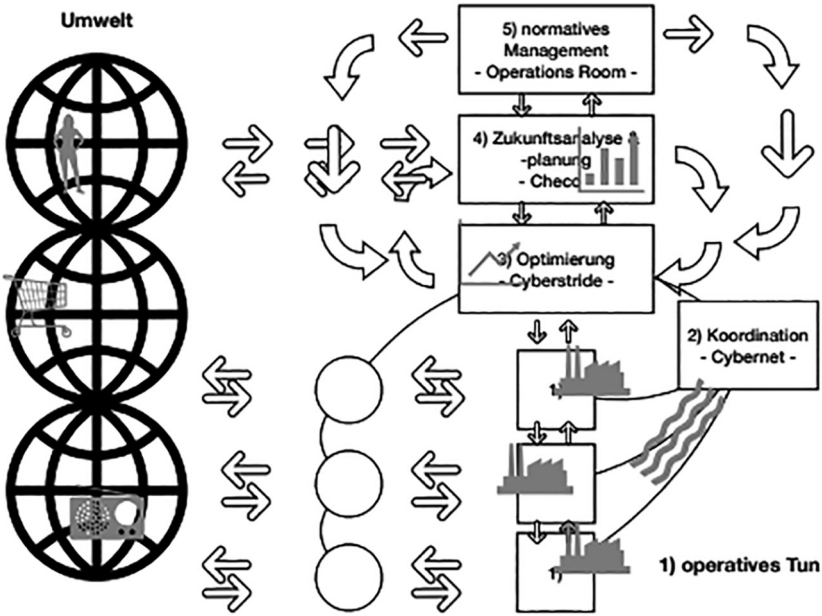


Abbildung 1: Die Systeme des VSM auf Cybersyn angewandt

17.1.4 „Paro de Octubre“

Im November 1971 wurde das Netz in ganz Chile in verschiedenen Fabriken, die bereits über Fernschreiber verfügten, eingeführt.[27] Ende 1972 wurde das Cybersyn-Projekt auf die Probe gestellt: Im September 1972 wurde ein Transportstreik angekündigt, der am 8.10. beginnen sollte, um den Vorschlag der Regierung abzulehnen, eine staatliche Transportgesellschaft zu gründen, die als Bedrohung des Privateigentums angesehen wurde. Der Transportstreik begann in den frühen Morgenstunden des Montags, 9.10.1972, in mehreren Provinzen und breitete sich landesweit aus. Die Arbeitsniederlegung unterbrach die Versorgungswege, den Transport von Rohstoffen und Produkten und behinderte auch den Weg der Menschen zu ihren Arbeitsplätzen, da auch die Personenbeförderungsunternehmen in den Städten betroffen waren. Der rechte Flügel mobilisierte, kämpfte auf der Straße und polarisierte die Situation, was sich auf die Wirtschaft auswirkte und die politische Krise verschärfte.

27 *Medina*, Diseñar la libertad, regular una nación. El socialism cibernético en el Chile de Salvador Allende, Redes, Vol. 20, No. 38, Bernal, Juni 2014, S. 147.

In jenen Tagen bildete sich der „Movimiento Patriótico de Recuperación Gremial“ (MOPARE),[28] in dem LKW-Besitzer:innen oder Fahrer:innen organisiert waren, die der Regierung *Allende* treu ergeben waren, um die Versorgung und Anbindung des Landes zu gewährleisten.[29] Die Regierung nutzte das sich gerade im Aufbau befindliche Computersystem, um die Verteilung der knappen Güter mittels dieser treuen Fahrer:innen zu koordinieren. Im Palacio de la Moneda – der „Opsroom“ war noch nicht fertiggestellt – wurde eine zentrale Einsatzzentrale eingerichtet und an das Telex-Netz angeschlossen, das ursprünglich für das Cybersyn-Projekt eingerichtet worden war. Tag und Nacht kamen in der eingerichteten Zentrale Faxe an, um die Ressourcen dorthin zu lenken, wo sie am dringendsten gebraucht wurden.[30] Obwohl der Streik nicht nur das Land schwächte, sondern auch einige für die Regierung verhängnisvolle politische Veränderungen mit sich brachte, wurde Präsident *Allende* im Oktober nicht gestürzt. Aufgrund der auf diese Weise garantierten schnellen Reaktionszeiten auf sich verändernde Sachlagen konnte der Schaden für die Wirtschaft und die Regierung minimiert werden.[31]

17.2 Der heutige Nachfolger: Das Social Credit System

Im Mai 2018 erläuterte ein chinesischer Rechtswissenschaftler,[32] dass Künstliche Intelligenz in der sozialistischen Marktwirtschaft Chinas durch die Analyse großer Datenmengen und robuste Rückkopplungsschleifen eine rationale Ressourcenzuweisung vornehmen könnte[33] – was praktisch dem kybernetischen Modell einer sozialistischen Wirtschaft entspricht, das in Cybersyn vorgestellt wurde. Für die Umsetzung dieser Idee bedarf es des ungehinderten Zugangs zu Daten für die chinesische Regierung. Das chinesische Sozialkreditsystem (SCS)[34] könnte als Teil dieser Vision gesehen werden.

---

28 Patriotische Bewegung für den Wiederaufbau der Gewerkschaften.

29 *Medina*, Designing Freedom, Regulating a Nation: Socialist Cybernetics in Allende’s Chile, Journal of Latin American Studies Vol. 38, No. 3, Aug. 2006, S. 593.

30 *Medina*, Diseñar la libertad, regular una nación. El socialism cibernético en el Chile de Salvador Allende, Redes, Vol. 20, No. 38, Bernal, Juni 2014, S. 147–148.

31 *Medina*, Diseñar la libertad, regular una nación. El socialism cibernético en el Chile de Salvador Allende, Redes, Vol. 20, No. 38, Bernal, Juni 2014, S. 148.

32 *Prof. Dr. Feng Xiang*, Professor der Rechtswissenschaften an der Tsinghua University.

33 *Feng Xiang*, AI will spell the end of capitalism, The Washington post, May 2018 (https://www.washingtonpost.com/news/theworldpost/wp/2018/05/03/end-of-capitalism/ 29.7.2022).

34 Social Credit System, rechtliche Grundlagen sind u. a. State Council of the People’s Republic of China: Planning Outline for the Construction of a Social Credit System (2014–2020).

Aktuelle Ansätze in China zielen darauf ab, nicht nur die Unternehmen, sondern ebenso die Gesellschaft selbst zu „steuern". In der Volksrepublik China soll dies mittels des SCS, das seit dem Jahr 2003 entwickelt wird,[35] umgesetzt werden. Derzeit wird das SCS in Bezug auf die Bevölkerung bereits in mehreren Städten in China lokal umgesetzt.[36] Grundlage der Steuerung sind umfangreiche Datenbestände und die Vornahme von Bewertungen, ebenso werden Verhaltenspräferenzen und das persönliche Netzwerk, in denen sich die Individuen bewegen, miterfasst und zusammengeführt.[37] Seit 2019 ist das SCS für Unternehmen größtenteils umgesetzt worden und fußt auf ca. 350 nationalen und ca. 1000 lokalen Regelungen.[38] Auch das Verhalten von Unternehmen wird im Zuge des SCS verdatet. Dies erfolgt anhand von Parametern wie Steuern, Zöllen, Umweltschutz und Produktqualität sowie einer parallelen Reihe von Aufzeichnungen über die Einhaltung von Vorschriften (z. B. in Bezug auf Antimonopolfälle, Datentransfer, Preisgestaltung und Lizenzen).[39]

35 Report at the 16th National Congress of the Chinese Communist Party, Database of Past CCP National Congresses, 8 November 2002.

36 Vgl. Measures to Implement the Construction of the Social Credit System in Sichuan Province, promulgated by the Sichuan Provincial People's Gov't, effective Aug. 25, 2016.

37 *Chen/Lin/Liu*, The Power and Perils of China's Social Credit Megaproject, Columbia Journal of Asian Law, Vol. 32(1), 2018, S. 10–13.

38 Siehe auch *Fongern/Wang/Yu* in *Everling*, Social Credit Rating, Das chinesische Sozialkreditsystem für Unternehmen – Hintergünde und praktische Hinweise, 2020, S. 571–582.

39 Chinas Social Credit-System für Unternehmen, Oktober 2019, Rödl & Partner, https://www.roedl.de/themen/china-social-credit-unternehmen (30.7.2022).

Autor:innenhinweise

Susan Bischoff, LL. M. (Glasgow) ist Volljuristin, promoviert zu urheberrechtlichen Fragestellungen in der digitalen Welt an der Universität Freiburg und ist als wissenschaftliche Mitarbeiterin bei Morrison & Foerster tätig. Der Schwerpunkt ihrer Tätigkeit liegt im nationalen und internationalen gewerblichen Rechtsschutz in den Bereichen Film, Kunst, Medien und Entertainment, sowie der Plattformenregulierung.

Dipl. Jur. Til Martin Bußmann-Welsch hat im Jahr 2019 die erste juristische Staatsprüfung absolviert und ist gegenwärtig Referendar am Kammergericht Berlin. In den vergangenen zweieinhalb Jahren hat er an seiner Promotion im Bereich der statistischen Auswertung richterlichen Verhaltens gearbeitet, deren Finalisierung kurz vor dem Abschluss steht. Er ist zudem Mitgründer eines Start-Ups zur Datenanalyse im Recht (iur.crowd) und Ko-Initiator der bundesweiten Kampagne zur Reform der juristischen Ausbildung in Deutschland „iur.reform".

Ertuğrul Can ist Studierender an der Universität Potsdam. Dort hat er den universitären Schwerpunktbereich Medien- und Wirtschaftsrecht absolviert. Gleichzeitig ist er studentischer Mitarbeiter in der Forschungsgruppe „Verantwortung und das Internet der Dinge" am Weizenbaum-Institut, wo er Forschungsbeiträge zu medienrechtlichen Themen leistet. Sein Forschungsinteresse liegt insbesondere im Social-Media-Recht.

Conrad S. Conrad ist Volljurist, geprüfter Datenschutzbeauftragter und arbeitet derzeit als Senior Berater Datenschutz bei der datenschutz nord GmbH am Hamburger Standort. Er ist seit mehreren Jahren in der Beratung im Datenschutzrecht tätig und kann diverse Veröffentlichungen zum Datenschutzrecht in den Fachmedien vorweisen. Das Studium der Rechtswissenschaft konnte er mit erfolgreichem Abschluss des Ersten Staatsexamen an der Universität Hamburg mit dem Wahlschwerpunktbereich „Information und Kommunikation" abschließen. Während des Studiums konnte er schon bei einigen Kanzleien und Projekten erste Praxiserfahrung sammeln. Anschließend folgte der erfolgreiche Abschluss des Referendariats in Schleswig-Holstein am LG Lübeck mit dem Zweiten Staatsexamen (Volljurist), unter anderem mit Stationen bei der Hamburger Aufsichtsbehörde im Datenschutz (HmbBfDI), der Medienanstalt Hamburg-Schleswig-Holstein (MA HSH) sowie bei einer auf das IT-Recht spezialisierten Kanzlei in Hamburg.

Leo V. Dessani, B.Sc. ist Informatiker und Masterstudent am Lehrstuhl für Rechtsinformatik an der Universität des Saarlandes. Er war im Sommersemester 2022 Lehrbeauftragter an der Hochschule Reutlingen und ist ab dem Wintersemester 2022/2023 Lehrbeauftragter an der Deutschen Universität

für Verwaltungswissenschaften Speyer. Sein Forschungsinteresse liegt in den Bereichen technischer Datenschutz, Privacy-Preserving Machine Learning und Sicherheit von Rechnernetzen.

Patricia Ernst, LL. M. ist Rechtsanwältin im deutschen Büro von Morrison & Foerster in Berlin und Mitglied der Film & Entertainment, Technology Transactions und Compliance Teams. Sie berät nationale und internationale Mandanten zu allen Fragen des Immaterialgüterrechts mit Schwerpunkt im Urheber- und Medienrecht. Sie hat einen LL. M. im Bereich „Immaterialgüter- und Medienrecht" erworben. Sie ist auf die umfassende Beratung von nationalen wie internationalen Medienunternehmen, wie beispielsweise Hollywoodstudios und internationale Video-on-Demand Plattformen, im Zusammenhang mit dem gesamten Wertschöpfungszyklus audiovisueller Inhalte spezialisiert. Dies beinhaltet neben der Entwicklung, Förderung/Finanzierung und Produktion auch die Vermarkung und den Vertrieb von Filmen und TV-Serien. Patricia Ernst berät zudem TV- und Radiosender sowie Video-on-Demand Plattformen zu regulatorischen Fragen wie Jugendschutz, Werbung und Anzeigepflichten gegenüber den Medienanstalten. Im Rahmen ihrer Compliance-Tätigkeit betreut sie Mandanten insbesondere in den Bereichen digitale Compliance und interne Untersuchungen.

Dr. Ermano Geuer ist deutscher und österreichischer Rechtsanwalt und arbeitet in einer internationalen Wirtschaftskanzlei in Wien. Seine Tätigkeitsschwerpunkte sind IT- und IP-Recht und Datenschutzrecht; er publiziert regelmäßig in diesen Bereichen. Vor seiner Tätigkeit als Rechtsanwalt war er als Legal Counsel im Rechenzentrum einer österreichischen Bank und als Syndikusanwalt bei einem deutschen Handelsunternehmen tätig. Als Rechtsanwalt mit deutscher und österreichischer Anwaltszulassung, der in beiden Rechtsordnungen zuhause ist, beschäftigt ihn die unterschiedlichen Herangehensweisen an die Digitalisierung von Anwaltschaft, Justiz und Verwaltung in beiden Ländern.

Hans-Christian Gräfe, LL. M. ist Volljurist und wissenschaftlicher Mitarbeiter am Weizenbaum-Institut für die vernetzte Gesellschaft. Sein Forschungsinteresse liegt hauptsächlich im Medien- und Informationsrecht, genauer gesagt im Online-Medienrecht, insbesondere zum Einfluss von Technologie auf Kommunikation und Medien. Er betreut verschiedene Lehraufträge an Universitäten und Hochschulen, u. a. im Wirtschaftsprivatrecht sowie im Medien- und Social-Media-Recht. Parallel zur Tätigkeit am Weizenbaum-Institut ist er Gastwissenschaftler an der Universität Potsdam und absolviert den MBA Digital Media Law and Management in Kooperation der Filmuniversität Babelsberg KONRAD WOLF, der Universität Potsdam und des Erich Pommer Instituts. Seinen LL. M. hat er im Medien- und Immaterialgüterrecht an der Humboldt-Universität zu Berlin gemacht. Studiert hat Hans in Marburg, Madrid und Münster.

Dipl.-Jur. Marvin Gülker ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Medien- und Informationsrecht von Prof. Dr. Kai von Lewinski an der Universität Passau. Er forscht zu informationsrechtlichen Themen aus dem Bereich des Datenschutz- und Immaterialgüterrechts und ist in seiner Freizeit u. a. als Programmierer in der Freie-Software-Szene tätig.

Prof. Dr. Simon J. Heetkamp hat zum Wintersemester 2022/23 eine Professur für Wirtschaftsrecht, Mobilitäts- und Versicherungsrecht an der TH Köln übernommen. Dafür wurde er von seiner Richterstelle am LG Köln, wo er zuletzt in einer Baukammer tätig war, beurlaubt. Zuvor hatte Simon Heetkamp eine Zivilabteilung am AG Köln inne. Anfang 2022 initiierte er mit dem IT-Dezernenten des LG Köln, Herrn Dr. Christian Schlicht, die *digitale richterschaft*, die eine Austauschplattform zu Digitalisierungsthemen in der Justiz ist. Vor seiner richterlichen Tätigkeit war Simon Heetkamp mehrere Jahre in einer international tätigen Wirtschaftskanzlei im Bereich Litigation tätig. Neben einem Schwerpunkt im Bankrecht bearbeitete er als Teil des Leitungsteams ein Massenverfahren aus dem Automobilsektor. In diesem Zusammenhang konzipierte er ein Tool zur Verwaltung und Bearbeitung von Massenklageverfahren. Einen Schwerpunkt auf Legal Tech legte Simon Heetkamp schon im Rahmen seiner Promotion zum Thema der Online Dispute Resolution, also der außergerichtlichen Online-Streitbeilegung. An der Universität Osnabrück ist er als Lehrbeauftragter im Schwerpunktbereich Digital Law tätig.

Karla Florencia Herb arbeitet als studentische Hilfskraft in der Forschungsgruppe „Verantwortung und das Internet der Dinge“ am Weizenbaum-Institut. Sie studiert englisches und deutsches Recht am King’s College London und der Humboldt-Universität zu Berlin. Sie war Teilnehmerin der Humboldt Law Clinic Internetrecht und bereitet sich aktuell auf das 1. Staatsexamen vor. Karla interessiert insbesondere, wie KI-Technologien in Online-Medien sich auf den politischen Diskurs und demokratische Meinungsbildung auswirken.

Sarah Lena Hünting ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Öffentliches Recht, Medien- und Informationsrecht in Passau (Universität Passau, Prof. von Lewinski) und Referendarin am OLG München. Im Rahmen ihrer Promotionsforschung setzt sie sich vertieft mit dem chilenischen Datennetzwerk „Cybersyn“ und dem chinesischen „Social Credit System“ auseinander.

Prof. Dr. Dennis-Kenji Kipker ist Professor für IT-Sicherheitsrecht an der Fakultät für Elektrotechnik und Informatik der Hochschule Bremen (HSB), Legal Advisor im Competence Center Information Security und CERT des VDE, Vorstandsmitglied der Europäischen Akademie für Informationsfrei-

heit und Datenschutz (EAID) sowie Geschäftsführer der Certavo-Beratungsgesellschaft in Bremen.

Dr. Christina-Maria Leeb ist Richterin in Passau. Zuvor war sie einige Jahre als Wissenschaftliche Mitarbeiterin in einer großen mittelständischen Wirtschaftskanzlei in München tätig. Sie promovierte in Passau zum Thema „Digitalisierung, Legal Technology und Innovation – Der maßgebliche Rechtsrahmen für und die Anforderungen an den Rechtsanwalt in der Informationstechnologiegesellschaft" und hat bereits vielfach zu Fragen des IT-, Urheber-, Medien- und Datenschutzrechts publiziert und zahlreiche Vorträge gehalten. Sie ist zudem Mitherausgeberin der Zeitschrift „Recht digital (RDi)" und lehrt im Masterstudiengang Legal Tech (LL. M.) an der Universität Regensburg.

Stefanie Lefeldt ist Juristin und Leiterin Europaangelegenheiten beim Zentralverband der deutschen Werbewirtschaft (ZAW). Zuvor ha sie über 5 Jahre das Thema Influencer Martketing als stellvertretende Justiziarin und Referentin Werbung bei der Medienanstalt Berlin-Brandenburg (mabb) betreut. Im Rahmen dieser Tätigkeit war sie an der Erstellung und Weiterentwicklung der Kennzeichnungsmatrix der Landesmedienanstalten beteiligt.

Dipl.-Jur. Maximilian Leicht, LL. M. studierte Rechtswissenschaften mit wirtschaftswissenschaftlicher Zusatzausbildung an der Universität Bayreuth und ist aktuell wissenschaftlicher Mitarbeiter und Doktorand am Lehrstuhl für Rechtsinformatik an der Universität des Saarlandes. Er ist seit dem Sommersemester 2020 Lehrbeauftragter an der Deutschen Universität für Verwaltungswissenschaften Speyer. Sein Forschungsinteresse liegt im Datenschutz- und IT-Sicherheitsrecht.

Prof. Dr. Rainer Mühlhoff, Philosoph und Mathematiker, ist Professor für Ethik der Künstlichen Intelligenz an der Universität Osnabrück. Er forscht zu Ethik, Datenschutz und kritischer Sozialtheorie in der digitalen Gesellschaft. In seiner interdisziplinären Arbeit bringt er Philosophie, Medienwissenschaft und Informatik zusammen und untersucht das Wechselspiel von Technologie, Macht und gesellschaftlicher Veränderung.

Marie-Theres Neubauer ist Studierende an der Universität Potsdam mit dem abgeschlossenen Schwerpunkt Medien- und Wirtschaftsrecht und studentische Mitarbeiterin bei Schertz Bergmann Rechtsanwälte PartG mbB, Berlin.

Prof. Dr. Boris Paal, M.Jur. (Oxford), ist Inhaber des Lehrstuhls für Bürgerliches Recht und Informationsrecht, Daten- und Medienrecht, Direktor des Instituts für Medien- und Datenrecht sowie Digitalisierung an der Juristenfakultät der Universität Leipzig und Of Counsel der Rechtsanwaltskanzlei Nikol & Goetz.

Dr. Yvonne-Anne Pignolet forscht im Bereich verteilte Systeme und reicht von Design und Analyse von Algorithmen für zuverlässige und effiziente Systeme trotz Ausfällen und boshaftem Verhalten bis zur Analyse von komplexen vernetzten Systemen. Nach ihrem Doktorat an der ETH Zürich in 2009, hat sie ein PostDoc bei IBM Research Zurich und an der Ben Gurion University, Be'er Sheva absolviert. Danach arbeitete sie während 8 Jahren bei ABB Corporate Research, Schweiz, und widmete ihre Forschung den Kommunikationssystemen für industrielle und Energiesysteme, zuletzt als Principal Scientist. Parallel dazu unterrichtete sie an der EPFL eine Master-Level-Vorlesung zum Thema Industrial Automation System. Seit 2019 arbeitet sie bei DFINITY, einer Stiftung, welche sich der Förderung und Erhaltung von neuen offenen dezentralisierten Softwarearchitekturen verschrieben hat. Zurzeit leitet sie dort Forschungsgruppen und Software Engineering Teams, die den Internet Computer weiterentwickeln und verbessern.

Jun.-Prof. Dr. Hannah Ruschemeier ist Inhaberin der Juniorprofessur (Tenure) für Öffentliches Recht mit Schwerpunkt Datenschutzrecht/Recht der Digitalisierung an der FernUniversität in Hagen. Sie ist Mitherausgeberin der Zeitschrift Legal Tech im Nomos-Verlag, Vorstandsmitglied bei RAILS e. V. und assoziierte Forscherin am CAIS (Center for Advanced Internet Studies) NRW. Ihre Forschungsschwerpunkte liegen neben dem klassischen öffentlichen Recht in den rechtstheoretischen Grundlagen der Digitalisierung, dem Datenschutzrecht und den rechtlichen Aspekten von Privatheit.

Prof. Dr. Marcus Schladebach ist Professor für Öffentliches Recht, Medienrecht und Luft- und Weltraumrecht an der Universität Potsdam. Nach dem Studium der Rechtswissenschaft an der Humboldt-Universität zu Berlin, der dortigen Promotion, dem Zweiten Juristischen Staatsexamen und einem LL. M.-Studium im European Integration Law arbeitete er zwischen 2002–2013 im Landes- und im Bundesjustizministerium. Die Habilitation absolvierte er 2013 an der Universität Augsburg und erhielt die universitäre Lehrbefugnis für Öffentliches Recht, Europarecht, Völkerrecht und Luft- und Weltraumrecht. Es schlossen sich mehrere Lehrstuhlvertretungen an (u. a. Kiel, Göttingen, Düsseldorf, Potsdam), bevor er 2017 an die Universität Potsdam berufen worden ist.

Dr. Christian Schlicht wurde nach seinem Studium und Referendariat in Bonn, Berlin und New York 2015 als Richter tätig. Nach seiner Tätigkeit am LG Köln, AG Gummersbach und im Landesjustizprüfungsamt bei dem Ministerium der Justiz NRW wurde er 2018 zum Richter am LG in Köln ernannt. Seitdem ist er Prüfer in der ersten Staatsprüfung bei dem OLG Köln. Ab 2019 war er zunächst Stellvertretender IT-Dezernent, seit 2021 ist er als IT-Dezernent u. a. für die Einführung der elektronischen Akte, auch an den

acht Amtsgerichten des Bezirks, verantwortlich. Im März 2022 gründete er die *digitale richterschaft*.

Prof. Dr. Stefan Schmid ist Universitätsprofessor an der Technischen Universität Berlin, Deutschland. Er hat an der ETH Zürich promoviert, war Postdoc an der TU München und der Universität Paderborn, Senior Research Scientist bei den T-Labs in Berlin, außerordentlicher Professor an der Universität Aalborg, Dänemark, und ordentlicher Professor an der Universität Wien, Österreich. Stefan Schmid ist Experte für vernetzte und verteilte Systeme, insbesondere für Internet Architekturen und Netzwerke und deren Robustheit und Sicherheit. Er ist ein Principal Investigator am Weizenbaum-Institut und arbeitet Teilzeit fürs Fraunhofer SIT. Stefan Schmid erhielt den IEEE Communications Society ITC Early Career Award 2016 und einen ERC Consolidator Grant.

Rebecca Sieber ist Rechtsreferendarin in Berlin und ehemalige wissenschaftliche Mitarbeiterin an der Humboldt-Universität zu Berlin am Lehrstuhl von Prof. Dr. Herbert Zech. Zuvor arbeitete sie an der Freien Universität Berlin in den Arbeitsbereichen von Prof. Dr. Ruth Janal, LL. M. und Prof. Dr. Bertram Lomfeld. Seit Abschluss der ersten juristischen Prüfung 2015 studiert sie in Rahmen eines Zweitstudiums Philosophie und Japanstudien. Sie setzt sich interdisziplinär mit rechtlichen und gesellschaftlichen Fragen der Digitalisierung auseinander. Seit 2014 organisiert sie Datenschutz-Workshops, insbesondere an der Humboldt-Universität zu Berlin. Im Rahmen der Initiative #gnuHU setzt sie sich aktiv für mehr Einsatz von freier Software an der Humboldt-Universität ein. Sie wirkt selbst bei dem Betrieb einer Berliner Fediverse-Instanz mit.

Christiane Stützle ist Rechtsanwältin und Partnerin des deutschen Büros der international tätigen Anwaltskanzlei Morrison & Foerster. Sie ist Fachanwältin für Urheber- und Medienrecht und Schiedsrichterin bei der Independent Film & Television Alliance mit Sitz in Los Angeles. Christiane Stützle leitet die globale Film & Entertainment Praxis von Morrison & Foerster. Sie berät deutsche und internationale Produktionen, Plattformen und Kreative bei der Finanzierung inkl. Filmförderung, Entwicklung, Produktion und dem Vertrieb von Film- und Serienproduktionen und agiert häufig als Bindeglied zwischen USA, Asien und europäischen Partnern. Darüber hinaus berät sie an der Schnittstelle von Technologie und Recht, der digitalen Transformation und der Umsetzung von EU-Gesetzgebung. Sie ist Mitautorin des Münchener Handbuchs für Urheber- und Medienrecht (Filmrecht), veröffentlicht regelmäßig zu aktuellen Rechtsentwicklungen und ist Dozentin beim Erich Pommer Medieninstitut in den Fachgebieten Urheber-, Film- und Medienrecht.

Mireille Thierfelder, LL. B. ist Studentin der Rechtswissenschaften an der Universität Potsdam. Dort absolvierte sie den Schwerpunkt „Medien- und Wirtschaftsrecht“ und schloss ihren Bachelor ab. Sie absolvierte zudem diverse Praktika bei unterschiedlichen Kanzleien. Zu diesen zählen insbesondere Morrison Foerster, Brost Claßen und Nordemann.

Das Recht der Informationsgesellschaft in seiner Breite und Vielfalt im Jahr 2022 darzustellen, war der Anspruch der Telemedicus Sommerkonferenz 2022. Auf einer Veranstaltung in Präsenz war Platz für Ideen und Diskussionen, aber auch Updates und Austausch über die Rechtspraxis sowie nicht zuletzt für Inspiration und Vernetzung. Dies spiegelt sich im Tagungsband wider, durch hochaktuelle Beiträge zur Modernisierung des Zivilprozesses, zu NFTs sowie juristischer Ausbildung und Legal Tech.
Manche Themen lassen sich dabei am besten interdisziplinär darstellen, wie die Beiträge zu Predictive Analysis, Satelliten-Megakonstellationen und zum Metaverse zeigen. Einige Themen stammten aus einem Call for Proposals, wie die Beiträge zu Public Value, zum Influencer Marketing, zu Technologie-Souveränität, zu überindividuellen Problemen im Datenschutzrecht, zu Betroffenenrechten im eSport, zum Fediverse und zu Federated Learning oder zum Projekt Synco (Cybersyn). Die wesentlichen Themen der Konferenz dokumentieren wir in diesem Tagungsband.

Mit Beiträgen von:
Susan Bischoff, Til Bußmann-Welsch, Ertuğrul Can, Conrad Conrad, Leo Dessani, Patricia Ernst, Ermano Geuer, Hans-Christian Gräfe, Marvin Gülker, Simon Heetkamp, Karla Herb, Sarah Hünting, Dennis-Kenji Kipker, Christina-Maria Leeb, Stefanie Lefeldt, Maximilian Leicht, Rainer Mühlhoff, Marie-Theres Neubauer, Boris Paal, Yvonne-Anne Pignolet, Hannah Ruschemeier, Marcus Schladebach, Christian Schlicht, Stefan Schmid, Rebecca Sieber, Christiane Stützle und Mireille Thierfelder.

9 783800 518579

Der Verlag im Internet: www.ruw.de