CTRL

Cologne Technology Review & Law

2/22
2. Jahrgang, 2. Ausgabe
www.legaltechcologne.de/ctrl

Ethics & AI 2022 – Erfahrungen aus Helsinki

Vom Amazonas bis zum Zuckerhut – Legal Tech in Lateinamerika

Der Digital Services Act – EU zwischen Innovation und Informationskrise

LEGAL TECH LAB COLOGNE

Inhaltsverzeichnis

CTRL 2/22

Liebe Leserinnen und Leser,

wer glaubte, dass die Covid-19 Pandemie das Reiseverhalten der Menschen dauerhaft ändern würde, wurde in den letzten Wochen eines Besseren belehrt: Trotz starker Preisanstiege, chaotischer Bedingungen an vielen Flughäfen und zahlreichen Ausfällen zieht es viele wieder in die Ferne.

Dieses Fernweh hat auch uns gepackt und wir haben uns in dieser Ausgabe deshalb schwerpunktmäßig mit internationalen Entwicklungen auseinandergesetzt. Felipe Molina untersucht in seinem Aufsatz „Legal Tech in Lateinamerika am Beispiel von Kolumbien" die Entwicklung der dortigen Legal-Tech-Branche. Auch andere Staaten der Region erweisen sich bei neuen Technologien als sehr anpassungsfähig: So kürte El Salvador im Herbst des letzten Jahres als weltweit erster Staat Bitcoin zu einem offiziellen Zahlungsmittel. Christian Wengert, der sich in seinem Aufsatz mit der geldrechtlichen Einordnung von Kryptowährungen auseinandersetzt, ist indes skeptisch, ob sich dies in Europa ohne Weiteres übernehmen lässt.

All dies kann nicht davon ablenken, dass auch in Europa die regulatorische Landschaft in ständiger Bewegung ist. In seinem Aufsatz „EU Data Act - Freie Fahrt für den Datenverkehr" analysiert Hendrik Eppelmann zwei Verordnungsentwürfe, welche die Schaffung eines europäischen Binnenmarktes für Daten maßgeblich mitgestalten sollen. Michelle Duda setzt sich mit dem kürzlich vom EU-Parlament verabschiedeten Digital Services Act auseinander.

Auf deutscher Ebene zeigt sich Hans Steege in seiner Kolumne zur Datenverarbeitung beim autonomen Fahren vom Gesetzgeber enttäuscht und sieht in der StVG-Novellierung eine verpasste Chance für mehr Rechtsklarheit. Demgegenüber zeichnet Dr. Christian Deckenbrock in seinem Gastbeitrag „Legal Tech und Anwaltliches Berufsrecht" nach, wie der Gesetzgeber Legal-Tech-Anbietern durch eine schrittweise Liberalisierung des anwaltlichen Berufsrechts zunehmend größere Spielräume zugestehen.

Zuletzt noch eine Mitteilung in eigener Sache: Seit der letzten Ausgabe haben sich auch bei uns zahlreiche Änderungen ergeben. Julia Melles leitet in Zukunft das Design-Team und wird die visuelle Weiterentwicklung der CTRL vorantreiben. Tatkräftig unterstützt wird sie dabei von nun an von Larissa Pilch und Helena Sommer. Philipp Beckmann tritt der Chefredaktion als viertes Mitglied hinzu und wird die konzeptionelle Weiterentwicklung der CTRL mitgestalten. Außerdem freuen wir uns, die Errichtung eines wissenschaftlichen Beirats ankündigen zu können, der die redaktionelle Arbeit der CTRL in Zukunft begleiten und unterstützen wird.

Wir wünschen Euch viel Spaß beim Lesen dieser vierten Ausgabe der CTRL!

Mit besten Grüßen

Ferdinand Wegener
Chefredaktion

Ramon Schmitt
Chefredaktion

Philipp Beckmann
Chefredaktion

Louis Goral-Wood
Chefredaktion

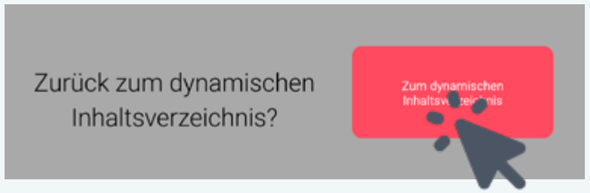
Klick mich!

Grundwissen

1 Grünes Licht für autonome Kraftfahrzeuge? – Ein Überblick über das Gesetz zum autonomen Fahren

Unser ausgabenspezifisches Inhaltsverzeichnis

Unser ausgabenspezifisches Inhaltsverzeichnis schickt euch mit einem Klick direkt zu dem Beitrag, der euch ins Auge gesprungen ist.



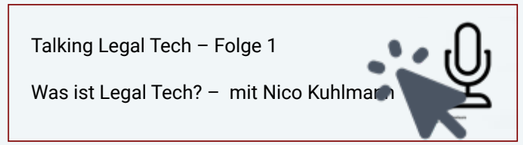
Rückverlinkungen zum dynamischen Inhaltsverzeichnis

Über einen Klick auf diesen Button springt ihr direkt zu unserem dynamischen Inhaltsverzeichnis zurück.

1 *Essig*, Ist die Redewendung „Das passt wie die Faust aufs Auge“ positiv oder negativ zu verstehen?, **hier** abrufbar (Stand: 15.12.2021).

Verlinkungen in den Fußnoten

Du findest Aspekte eines Beitrags besonders spannend? Dann lohnt sich ein Blick in unsere Fußnoten. Dort findest du hinter “hier” immer Hyperlinks hinterlegt.



Die Podcast-Verknüpfungen

Über diese Icons könnt ihr euch blitzschnell Folgen des Talking Legal Tech Podcasts anhören, die sich mit dem Thema des jeweiligen Beitrages befassen.

Über die CTRL

Die studentische Zeitschrift für Recht und Digitalisierung.

Die CTRL ist die studentische Zeitschrift des Legal Tech Lab Cologne (LTLC) für Recht und Digitalisierung, die im Format eines ePapers halbjährlich – zum Semesterende – erscheint.

Die Aufsätze für dieses ePaper werden von den Mitgliedern des LTLC verfasst, die in einführenden Grundwissens-Beiträgen die Funktionsweisen neuer Technologien verständlich erklären, die rechtlichen Implikationen dieser Technologien in Aufsätzen analysieren und Einblicke in die Veränderung des Rechtswesens durch Legal Tech ermöglichen. Darüber hinaus wird die CTRL um Gastbeiträge aus der Wissenschaft und Praxis sowie Interviews mit spannenden Persönlichkeiten aus dem Legal-Tech-Bereich ergänzt.

Über das LTLC

Das Legal Tech Lab Cologne (LTLC) ist eine studentische Initative an der Universität zu Köln, die im März 2019 gegründet wurde. Das LTLC besteht derzeit aus 50 Mitgliedern. Nebst der Veröffentlichung des ePapers findet die inhaltliche Arbeit des LTLC im Rahmen der Produktion des Podcasts Talking Legal Tech, der Organisation von Veranstaltungen (“Teaching Legal Tech”) und der Programmierung konkreter Anwendungen in Projektgruppen statt. Darüber hinaus haben Mitglieder des LTLC gemeinsam mit der Fachschaft Jura der Universität zu Köln den Sonderpreis für digitale Lehre konzipiert. Schirmherrin und wissenschaftliche Leitung der Hochschulgruppe ist Frau Prof. Dr. Dr. Frauke Rostalski.

Die Partner des LTLC

Wolters Kluwer

CMS law·tax·future

Osborne Clarke

Gateway Exzellenz Start-up Center Universität zu Köln

TRIPLIQ

Die Köpfe
hinter der Zeitschrift

Julia Melles
Head of Layout

Larissa Pilch
Layout/Social Media

Helena Sommer
Layout & Design

Greta Maria Gross
Design

Clarissa Kupfermann
Redaktion

Michelle Duda
Redaktion

Philipp Mahlow
Redaktion

Hendrik Eppelmann
Redaktion/Lektorat

Alina Rosenkranz
Social Media

Muskan Multani
Social Media

Isabel Ecker
Lektoratsleitung

Hanna Brinkmann
Lektorat

Joela Worm
Lektorat

Hendrik Scheja
Lektorat

Daniel Dischinger
Lektorat

Wir danken Christoph Pracht von der CCCP Werbeagentur ganz herzlich für sein umfassendes Engagement rund um die gestalterische Aufmachung der CTRL.

CTRL x Talking Legal Tech

Lesespaß & Hörgenuss

Das Legal Tech Lab Cologne produziert neben der CTRL den Podcast Talking Legal Tech.

Dieser beschäftigt sich, wie auch das ePaper, mit Fragen und Antworten rund um die Digitalisierung des Rechts. Er hat sich zum Ziel gesetzt, diese für jedermann zugänglich zu machen.

Dazu führt das Podcast-Team Gespräche mit bekannten Persönlichkeiten aus der Legal-Tech-Szene und befragt sie zu ihrer Perspektive auf Themen wie Digitalisierung im Jurastudium, künstliche Intelligenz oder Innovationsmanagement.

Im LTLC stehen der Podcast und das ePaper als Informationsquellen unabhängig und dennoch sich gegenseitig ergänzend nebeneinander: Die unterschiedlichen Formate ermöglichen es – entweder als Hörerinnen und Hörer oder als Leserinnen und Leser – einen Zugang zum Thema Legal Tech in all seinen Facetten zu finden.

Am Ende jedes Beitrags, der einen Bezugspunkt zu einer Folge Talking Legal Tech hat, findest du folgendes Icon mit einer Verlinkung zu der entsprechenden Folge.

Was offline illegal ist, soll es auch online sein

Grundwissen

Der Digital Services Act - Europa zwischen Innovation und Informationskrise

Michelle Duda

Michelle arbeitet und promoviert am Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtsphilosophie und Rechtsvergleichung der Universität zu Köln bei Prof. Dr. Dr. Rostalski. In diesem Kontext und auch in ihrer Freizeit setzt sie sich mit der Thematik von Digitalisierung und Recht mit einem Schwerpunkt in Cyberaggression und Datenschutz auseinander.

Open Peer Review

Dieser Beitrag wurde lektoriert von: Ramon Schmitt und Larissa Pilch

Das Internet ermöglicht eine gänzlich neuartige Form des multilateralen Austauschs. Erstmals ist es möglich, in Echtzeit mit Personen aus aller Welt zu kommunizieren, sein Leben mit einer schier unbegrenzten Zahl an Menschen zu teilen und Produkte aus aller Welt zu erwerben, sei es von einem gewerblichen oder privaten Verkäufer[1]. Das Projekt ***‚Metaverse'*** vom Unternehmen ***Meta Platforms***[2] sowie weitere VR-Welten setzen sogar erste Bausteine für die Möglichkeit eines parallelen, virtuellen Lebens ein, in dem man heiraten, Sport treiben und Freunde treffen kann.

1 Zum Zwecke der besseren Lesbarkeit wird bei personenbezogenen Hauptwörtern nur die männliche Form verwendet. Diese Begriffe sollen für alle Geschlechter gelten.
2 Bis Oktober 2021 noch als *Facebook Inc.* bekannt.

Man muss sich dafür nicht aus den eigenen vier Wänden bewegen[3] – ***Surrogates***[4] lässt grüßen. Der Alltag wird schnelllebiger und Erkenntnisgewinn ist nur noch eine Frage der Internetqualität. Das Potenzial dieser digitalen Entwicklung ist gewaltig. Und doch zeigt die Realität die dunklen Aspekte eines digitalisierten Miteinanders auf: Krisensituationen wie der aktuelle Krieg in der Ukraine, die Coronapandemie, die US-Präsidentschaftswahl 2020 oder die Vertuschungsversuche von China hinsichtlich der Gewalttaten an den Uiguren in der Region Xinjiang verdeutlichen den Krieg um Informationen. Damit sind nicht nur tatsächliche Angriffe auf Informationsinfrastrukturen gemeint, sondern auch die Frage nach der Herrschaft über Information. Wer erhält welche Informationen? Die Verbreitung von falschen oder die Unterdrückung von wahren Informationen sind häufige Probleme in bewaffneten Konflikten und Krisensituationen. Die genannten Fälle sind nur einige – aber prägnante – Beispiele der Einflussnahme von Verschwörungstheorie und der privaten und staatlichen Einflussnahme auf die Meinungsbildung.[5] Derartige Behauptungen wurden hauptsächlich über soziale Medien verbreitet, geteilt und millionenfach in vielen Sprachen angesehen, innerhalb wie auch außerhalb der EU.

Aber auch fernab von politisch motivierten Kampagnen zeigt sich die negative Kehrseite von Anonymität und Allgegenwärtigkeit des Internets. Gerade bei Betrachtung der Entwicklung in der Hochzeit der Coronapandemie, in der aufgrund diverser Lockdowns analoger Kontakt spärlich war, ließ sich ein Anstieg von Cybermobbing und damit einhergehenden psychischen Problemen beobachten.[6] Nicht selten gipfelt dies in Langzeitschäden oder gar dem Suizid der Betroffenen.[7] Auch auf das Entstehen und die Entwicklung von Essstörungen und damit verbundenen psychischen Störungen hat das Internet einen enormen Einfluss.[8] In einer Studie schätzen 65 % der Befragten das Internet als unsicher ein und sogar 90 % sind sich einig, dass Maßnahmen erforderlich sind, um die Verbreitung illegaler Inhalte online zu begrenzen.[9] Die EU setzt nun mit dem ***Digital Services Act (DSA)*** einen „***neuen Standard für die Rechenschaftspflicht von Online-Plattformen im Umgang mit illegalen und schädlichen Inhalten***“.[10] Aber wie sieht das Gesetz aus, das ein sicheres und verantwortungsvolles Online-Umfeld schaffen und verhindern soll, dass gefährliche Desinformationen viral gehen oder unsichere Produkte auf Marktplätzen angeboten werden?

> Ziel des DSA:
> „Was offline illegal ist, soll es auch online sein“

A. Kontext und Ziele des Digital Service Acts

Europa bemüht sich um eine Vorreiterstellung im digitalen Wandel.[11] Zwei hierfür heiß erwartete Verordnungen sind der ***Digital Markets Act (DMA)*** und der ***Digital Services Act (DSA)***. Während der ***DMA*** (noch) im Entwurfsstadium steckt[12] und die wettbewerbliche Regulierung von sog. ***Gatekeepern*** zum Inhalt hat,[13] erhebt der ***DSA*** den Anspruch, ein einheitliches Regelwerk zu Pflichten und Verantwortlichkeiten von Intermediären innerhalb des Binnenmarktes zu sein. Trotz Fokus auf besseren Verbraucherschutz und deren Grundrechte im Internet, sollen Innovation, Wachstum und Wettbewerbsfähigkeit sowie die Expan-

3 S. hierzu die Reportage von einem Reporter bei Funk als Selbstversuch, hier abrufbar (Stand: 24.05.2022).
4 Ein Film von 2009, in dem *Bruce Willis* als FBI-Agent Morde an besagten ‚Surrogates‘ aufklären muss. Die Menschen leben fast ausschließlich von Zuhause aus, sie steuern maschinelle Doppelgänger mit ihrem Bewusstsein und setzen sich den Gefahren eines analogen Lebens nicht mehr aus.
5 Exemplarisch seien etwa genannt: Das Trinken von Industriealkohol schütze vor dem Covid-19-Virus, 5G-Telekommunikationsmasten unterstützten die Verbreitung des Virus, häufiges Händewaschen schütze nicht vor dem Virus; in Bezug auf die Präsidentenwahl: Es habe Wahlbetrug stattgefunden, der jedoch nie belegt werden konnte und im Ergebnis in dem Sturm auf das Kapitol am 6. Januar 2021 gipfelte.
6 *Schunk/Zeh/Trommsdorff*, Computers in Human Behavior 126 (2022), hier abrufbar (Stand: 24.05.2022); *Ispas/Ispas*, Educatia 21 Journal, Iss. 21 (2021), 159.
7 *Weitzel* in Böhmer/Steffgen, Mobbing an Schulen, 131, (139-144).
8 *Grogan,* Encyclopedia of Body Image and Human Appearance, Vol. 1 (2012), 201; *Opara/Santos*, Hispanic Journal of Behavioral Science Vol. 41, iss. 3 (2019), 363 (368).
9 Eurobarometer Umfrage unter den Nutzern in ganz Europa vom 12.09.2018, hier abrufbar (Stand: 18.05.2022).
10 KOM, Presseartikel vom 25.04.2022, hier abrufbar (Stand: 18.05.2022).
11 KOM(2020)825 final, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG, 2: „*In der Entschließung wird auch für Regeln zur Untermauerung eines wettbewerbsfähigen digitalen Umfelds in Europa plädiert und davon ausgegangen, dass das Gesetz über digitale Dienste weltweit Standards setzen wird.*“
12 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte), KOM(2020)842 final, 15.12.2020.
13 S. vertiefend zum DMA-Entwurf „*Das Gesetz über digitale Märkte: für faire und offene digitale Märkte*“, KOM, hier abrufbar (Stand: 18.05.2022); *Eppelmann*, CTRL 1/2022, 123 (130 f.).

sion kleinerer Plattformen gefördert werden. Der ***DSA*** soll die ***E-Commerce-RL*** (***2000/31/EC***) von 2000[14] reformieren. Nach einem ersten Entwurf – parallel vorgelegt zu demjenigen für den ***DMA*** am 15.12.2020[15] – einigten sich das Europäische Parlament und die EU-Mitgliedstaaten nun am 23.04.2022 auf das ***Gesetz über digitale Dienste:*** Was offline illegal ist, soll es auch online sein. Doch wird es diesen eigenen hohen Ansprüchen gerecht? Welche Folgen ergeben sich für die Plattformbetreiber? Wird der Balanceakt zwischen Verbraucherschutz und Innovation erfolgreich vollzogen?

Das Gesetz richtet sich an alle Intermediäre, also vermittelnde Online-Dienste, die Dienstleistungen in der EU erbringen.[16] Gemeint sind damit Vermittlungsdienste wie Internetanbieter, Hosting-Dienste oder Online-Plattformen, die Verkäufer und Verbraucher nutzen, seien es Online-Marktplätze oder Social-Media-Plattformen (***Amazon, Youtube, Instagram*** etc.), aber auch Suchmaschinen wie ***Google***. Hinsichtlich der Pflichten der Online-Unternehmen differenziert der ***DSA*** zwischen Rolle, Größe und Auswirkung im Online-Umfeld.[17] Insbesondere sehr große Online-Plattformen und Suchmaschinen mit mehr als 10 % der 450 Millionen Verbraucher aus der EU sind anfällig für die Verbreitung illegaler Inhalte, die zu ‚Schäden' an der Gesellschaft führen können, weshalb diese gesondert reguliert werden und strengeren Anforderungen unterliegen. Ob der Intermediär innerhalb oder außerhalb der EU niedergelassen ist, ist irrelevant, solange die Dienste innerhalb des Binnenmarktes angeboten werden.[18] Die Plattformen sollen mehr Verantwortung dafür übernehmen, was auf ihnen passiert. Für kleinere Unternehmen mit weniger als 45 Millionen Nutzern im Monat soll es Ausnahmen geben.

B. Regelungsinhalt des neuen Gesetzes

Im Ergebnis betrifft der *DSA* somit zwei Gruppen:

- Online-Plattformen und Unternehmen: Sie unterliegen neuen Standards für die Rechenschaftspflicht in Bezug auf illegale und schädliche Inhalte. Der DSA soll als einheitliches Regelwerk die Grundlage für Innovation auf dem digitalen Binnenmarkt und die Expansion kleinerer Unternehmen sein.[19]

- Private Nutzer: Erhöhter Schutz und größere Beteiligungsmöglichkeiten.

Zur Bekämpfung illegaler Waren, Dienstleistungen oder Inhalte soll es Nutzern ermöglicht werden, diese Inhalte entsprechend zu kennzeichnen. Auf Seite der Plattformen soll es den Betreibern möglich sein, mit vertrauenswürdigen Hinweisgebern zusammenzuarbeiten. Ebenso sollen gewerbliche Nutzer auf Online-Marktplätzen leichter aufspürbar sein. Darüber hinaus sind stichprobenartig Überprüfungen vorgesehen, ob entsprechende Produkte oder Dienstleistungen in einer amtlichen Datenbank als illegal identifiziert wurden.

I. Pflichten der Intermediäre

Aktuell werden Nutzer mit illegalen Produkten, Inhalten und Dienstleistungen konfrontiert, deren Behandlung meist im Ermessen der Plattformen liegt. Ziel der neuen Verpflichtungen und Regularien sind unter anderem eine erleichterte Entfernung illegaler Inhalte und der Schutz der Grundrechte der Nutzer. Insbesondere Online-Plattformen, welche die 10 %-Hürde überschreiten und somit mehr als 45 Millionen Nutzer aus der EU erreichen, sehen sich aufgrund des damit erhöhten Risikos für die Gesellschaft einer Vielzahl neuer Verpflichtungen gegenüber gestellt. So haben diese Plattformen und Suchmaschinen risikobasierte Maßnahmen zu ergreifen, um den Missbrauch ihrer Systeme zu verhindern. Das entsprechende Risikomanagementsystem muss von unabhängiger Seite überprüft werden. Um das Fortschreiten von Online-Risiken nachvollziehen zu können, müssen sie außerdem den Zugriff von der Forschung auf die Kerndaten ermöglichen. Um die Plattformen bei der Ein-

14 Richtlinie 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, ABl. L 178 vom 17.07.2000, 1.
15 KOM(2020)825 final.
16 Rat der EU, Pressemitteilung vom 23.04.2022, hier abrufbar (Stand: 24.05.2022).
17 KOM, Gesetz über digitale Dienste: mehr Sicherheit und Verantwortung im Online-Umfeld, hier abrufbar (Stand: 18.05.2022).
18 KOM(2020)825 final, 7, 14.
19 *KOM*, Pressemitteilung vom 23.04.2022, hier abrufbar (Stand: 18.05.2022).

haltung der Vorschriften zu unterstützen, sind Verhaltenskodizes und technische Standards vorgesehen.

Im Sinne eines umfassenden Verbraucherschutzes wird Online-Marktplätzen eine besondere Sorgfaltspflicht gegenüber Anbietenden, die ihre Produkte oder Dienstleistungen auf ihren Online-Plattformen verkaufen, auferlegt. Hierbei müssen sie Informationen über die verkauften Produkte und Dienstleistungen erheben und zugunsten europäischer Konsumenten anzeigen.[20]

Aber auch die Mitgliedstaaten und die Kommission übernehmen einen Großteil der Verantwortung in diesem Wandel: Mit Unterstützung eines neuen europäischen Gremiums für digitale Dienste ist es an den Mitgliedstaaten, eine Aufsichtsstruktur einzurichten, die der Komplexität des Online-Raums gerecht wird. Bei sehr großen Plattformen – diejenigen, welche die 10 %-Hürde erreichen – übernimmt die Kommission selbst die Überwachung und Durchsetzung. Die Grafik soll eine Übersicht über die Aufteilung der diversen Pflichten schaffen und orientiert sich an derjenigen der Europäischen Kommission.[21]

	Vermittlungs-dienste	Hosting-Dienste	Online-Plattformen	Sehr große Plattformen
Transparenzberichte	✓	✓	✓	✓
Verpflichtung zur angemessenen Berücksichtigung der Grundrechte in Nutzungsbedingungen	✓	✓	✓	✓
Auf Anweisung Zusammenarbeit mit nationalen Behörde	✓	✓	✓	✓
Kontaktstellen und - falls erforderlich - rechtlicher Vertreter	✓	✓	✓	✓
Melde-, Abhilfe- und Informationspflichten		✓	✓	✓
Meldung von Straftaten		✓	✓	✓
Beschwerde- und Rechtsbehelfsmechanismen sowie außergerichtliche Streitbeilegungsverfahren			✓	✓
Vertrauenswürdige Hinweisgeber			✓	✓
Maßnahmen gegen missbräuchliche Meldungen und Gegendarstellungen			✓	✓
Spezielle Pflichten für Marktplätze (bspw. stichprobenartige Kontrollen)			✓	✓
Verbot von Werbung, die sich gezielt an Kinder richtet oder spzielle personenbezogene Daten nutzt			✓	✓
Transparenz der Empfehlungssysteme			✓	✓
Transparenz von Online-Werbung zugunsten der Nutzer			✓	✓
Verpflichtung zu Risikomanagement und Krisenreaktion				✓
Externe und unabhängige Prüfung, interne Compliance-Funktion und öffentliche Rechenschaftspflicht				✓
Möglichkeit für Nutzer, Empfehlungen anhand von Profiling abzulehnen				✓
Datenaustausch mit Behörden und Forschenden				✓
Verhaltenskodizes				✓
Zusammenarbeit in Krisen				✓

Darstellung des Pflichtenkatalogs für die Dienst- und Plattformbetreiber (Intermediäre).

20 Rat der EU, Pressemitteilung vom 23.04.2022, hier abrufbar (Stand: 24.05.2022).
21 Hier abrufbar (Stand: 18.05.2022).

II. Schutz und Mündigkeit der Nutzer

Eine Umfrage, die im Kontext der Beratung von *DMA* und *DSA* durchgeführt wurde, ergab, dass es unter Bürgern ein Bedürfnis nach erhöhter Transparenz der Plattformen hinsichtlich ihres Moderationsprozesses und der -ergebnisse gab.[22] Diesem Ruf nach erhöhter Transparenz wird nachgekommen. Der aktuell veröffentlichte Entwurf etwa sieht mindestens einmal jährlich klare, leicht verständliche und ausführliche Berichte über eine Moderation von Inhalten vor, die die Vermittlungsdienste im betreffenden Zeitraum durchgeführt haben.[23] Diese Berichte sollen unter anderem die Anzahl der von Behörden der Mitgliedstaaten erhaltenen Anordnungen, aufgeschlüsselt nach der Art der betroffenen illegalen Inhalte und die durchschnittliche Dauer bis zur Ergreifung der in diesen Anordnungen geforderten Maßnahmen enthalten oder auch die auf Eigeninitiative des Anbieters durchgeführte Moderation von Inhalten, aufgeschlüsselt nach der Art des Grundes und der Grundlage für das Ergreifen dieser Maßnahmen. Dies soll den Nutzern ermöglichen, die dahinterstehenden Entscheidungen anzufechten.

Auch der gezielten Werbung geht es an den Kragen: Bestimmte Arten gezielter Werbung auf Online-Plattformen sollen verboten sein, etwa wenn sie auf Kinder abzielen oder besondere personenbezogene Daten nutzen.[24] Um eine solche Art der Werbung unter Verwendung personenbezogener Daten handelt es sich etwa, wenn einer Person auf ihrem Social Media Feed Veranstaltungen oder Lokalitäten im eigenen Wohn- oder Aufenthaltsort angezeigt werden. Dabei wird der Datensatz des eigenen Wohnorts, den man etwa bei der Anmeldung angegeben hat, verwendet, um die passenden Anzeigen herauszufiltern und dem Nutzer zu präsentieren. Die Transparenzpflicht der Plattformen ist deshalb auch hinsichtlich der Algorithmen vorgesehen, welche die entsprechenden Werbevorschläge erstellen – sehr große

22 Hier abrufbar (Stand: 18.05.2022); in diesem Kontext seien insbesondere *Meta's* Bemühungen um das *Facebook Oversight Board* zu nennen, mit diesem Institut und den Grundrechtsfragen setzt sich *Beckmann*, CTRL 1/2022, 54 ff. auseinander.
23 KOM(2020)825 final, 57.
24 Art. 4 Nr. 1 DSGVO: Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Plattformen und Suchmaschinen werden Nutzern sogar ein System zur Empfehlung von Inhalten anbieten müssen, das nicht auf ihrem Profiling beruht. Wie genau dieses System aussehen soll, muss noch ausgestaltet werden. Diese Transparenzpflichten in Kombination mit einem verpflichtenden Zugang zu Streitbeilegungsmechanismen und den positiven Synergien, die aus diesen Pflichten für Nutzer entstehen, sollen neben dem sicheren Umgang mit den entsprechenden digitalen Diensten auch die Möglichkeit der freien Meinungsäußerung stärken. Indem Plattformen aktuell auf eigene Faust unangekündigt und ohne Einspruchsmöglichkeit Inhalte der Nutzer löschen können, wird diese zu stark und willkürlich eingeschränkt.[25]

Darüber hinaus sind sich die gesetzgebenden Organe einig geworden, sog. ***Dark Patterns*** (dt. ***irreführende Schnittstellen***) und Praktiken, die Nutzer in die Irre führen sollen, zu verbieten.[26] Vor dem Hintergrund aktueller Krisensituationen wie des Ukrainekrieges und der daraus folgenden, einleitend aufgezeigten Manipulation von Online-Informationen soll außerdem ein Krisenmechanismus eingeführt werden. Er wird von der Kommission auf Empfehlung des Gremiums der nationalen Koordinatoren für digitale Dienste aktiviert und ermöglicht, die Auswirkungen der Aktivität sehr großer Plattformen und Suchmaschinen auf die entsprechende Krise zu analysieren. In der Folge sollen verhältnismäßige und wirksame Maßnahmen zur Wahrung der Grundrechte ergriffen werden können.

Um diese Ziele zu erreichen, sollen die Behörden entsprechend besser ausgestattet werden.[27] Geplant ist etwa die Einrichtung einer digitalen Plattform für den Informationsaustausch zwischen den Mitgliedstaaten, dem Gremium und der Kommission sowie zur Sicherung der Funktionen und der Interoperabilität mit anderen in der Verordnung vorgesehenen Funktionen.[28] Die Mitgliedstaaten sollen zudem den entsprechenden Behörden ausreichende Befugnisse und Mittel zuweisen, um die Wirksamkeit der Untersuchungen und Durchsetzung sicherzustellen.[29]

25 Hierzu im Einzelnen bei Facebook und dem Facebook Oversight Board: *Beckmann*, CTRL 1/2022, 54 ff.
26 Rat der EU, Pressemitteilung vom 23.04.2022, hier abrufbar (Stand: 24.05.2022).
27 *KOM*, Ein Europa für das digitale Zeitalter: was sich für Nutzerinnen und Nutzer ändert, hier abrufbar (Stand: 24.05.2022).
28 KOM(2020)825 final, Anhang des Finanzbogens zu Rechtsakten, 9.
29 KOM(2020)825 final, 42.

III. Änderungen auch für Unternehmen – Grundstein für einen innovativen digitalen Binnenmarkt

Zugunsten der Förderung innovativer Online-Plattformen in der EU sollen die Normen, Verhaltenskodizes und Leitlinien Rahmenbedingung nicht nur für den dargestellten besseren Schutz der Nutzer begründen, sondern auch kleine Marktteilnehmer unterstützen. Auf dieser Grundlage soll der Binnenmarkt für digitale Dienste mit einer voraussichtlich kalkulierten Zunahme um bis zu 2 % florieren.[30]

Die kostspieligsten Verpflichtungen sollen entsprechend auch nicht die kleinen und mittleren Unternehmen betreffen, sondern nur die sehr großen Wettbewerber. Auch Unterstützung beim Wachstum ist geplant: Nachdem kleine Unternehmen die Umsatz- und Personalschwelle für Kleinunternehmen überschritten haben, soll ihnen die Steuerbefreiung für kleine Unternehmen für weitere 12 Monate zugutekommen. Zusätzlich profitieren Start-ups und andere ***KMUs*** von den erhöhten Transparenzpflichten der sog. ***Gatekeeper,*** indem sie Entscheidungen zur Anpassung ihrer Marktstrategie informierter treffen können.

KMUs (Kleine und mittlere Unternehmen; (von engl. SMUs für small and medium-sized entities) beschreiben Unternehmen, die durch gewisse Merkmale von Großunternehmen und Konzernen abgegrenzt werden. KMUs werden in diversen Gesetzen verschieden definiert. Während im deutschen Recht insb. das HGB KMUs eigenständig in § 267 HGB definiert, definiert die EU-Kommission KMUs anhand der Merkmale Mitarbeiterzahl, Umsatz und Bilanzsumme. KMUs sind in der Regulatorik ein enorm wichtiger Faktor, da sie europaweit über 99 % aller Unternehmen darstellen und etwa ⅔ aller Arbeitnehmer beschäftigen.[31]

30 *KOM*, Ein Europa für das digitale Zeitalter – was sich für Unternehmen ändert, hier abrufbar (Stand: 24.05.2022)
31 Ausführlichere Hinweise sind hier abrufbar (Stand: 12.06.2022).

Das Ziel der Innovation erfasst aber nicht nur den Gedanken größerer Beteiligung von kleinen und mittleren Unternehmen. Gemeint ist auch die Wandlung zu einem ‚ehrlicheren' Markt als Resultat aus dem Verbot illegaler Aktivitäten und Produkte im Netz.[32] Die Abschaffung von Fehlanreizen, die Implementierung einfacher und wirksamer Mechanismen zur Meldung illegaler Inhalte und Produkte, die enge Zusammenarbeit mit Plattformen durch vertrauenswürdige Hinweisgeber sowie die erweiterte Pflicht für Marktplätze zu abschreckenden Maßnahmen sollen einen kumulativen Beitrag zugunsten eines nicht nur technisch, sondern auch ideell innovativen Online-Umfeldes leisten.

C. Ausblick und Fazit

Nach dieser ersten Einigung von Europäischem Parlament und den Mitgliedstaaten kommt es nun auf die Verabschiedung des Gesetzes durch die EU-Gesetzgeber an. Die Verordnung tritt entweder am in der Verordnung selbst festgelegten oder am 20. Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.[33] Da es sich um eine Verordnung handelt, wird der ***DSA*** in der gesamten EU unmittelbar anwendbar sein und je nachdem, welcher Zeitpunkt später liegt, 15 Monate nach seinem Inkrafttreten oder ab dem 01. Januar 2024 in den Mitgliedsstaaten direkt gelten.[34] Sehr große Online-Plattformen und Suchmaschinen werden auch hier gesondert behandelt: Vier Monate nach ihrer Klassifizierung als solche haben sie sich an die Regelungen im DSA zu halten.

Für ein endgültiges Résumé wird die finale, verabschiedete Version der Verordnung abzuwarten sein. Die bisher veröffentlichten Inhalte, auf die sich das EU-Parlament und die Mitgliedstaaten inzwischen einigen konnten, lassen allerdings hoffen, dass die Ziele bei einer Regulierung des digitalen Raums – insbesondere in Kombination mit dem ***DMA*** – erreichbar werden.

> „Die bisher veröffentlichten Inhalte lassen allerdings hoffen, dass die Ziele bei einer Regulierung erreichbar werden."

Wenn es auch ein schwieriges Unterfangen wird, die Muster zu durchbrechen, die sich in der Praxis durchgesetzt haben, so überzeugt der Ansatz, sehr große Plattformen und sehr große Suchmaschinen als Kehrseite ihrer erhöhten Privilegien – der enormen Reichweite bei den Nutzern inklusive des Zugriffs auf deren Daten, der gefestigten Vorrangstellung auf dem Markt und der damit verbundene Wettbewerbsvorteil gegenüber Mitbewerbern durch Netzwerkeffekte – auch in eine verstärkte Pflicht zu nehmen. Zudem wird endlich verstärkt die Rolle des Konsumenten auf dem (digitalen) Markt gewürdigt: Indem er durch die vorgesehenen Meldemechanismen und Transparenzpflichten mündiger wird, ist er auch in der Lage, sein eigenes digitales Umfeld verstärkt mitzugestalten.

Schlussendlich bleibt abzuwarten, wie praktikabel der theoretische Ansatz ist. So muss man sich auf erste gerichtliche Entscheidungen gedulden, inwiefern sich diese Vorgehensweise tatsächlich mit den Grundrechten im Netz verträgt. Zumindest jedoch ist zu hoffen, dass Verbraucherschutz, Produktsicherheit und Innovation ausgewogener auf dem digitalen Markt koexistieren und interagieren werden.

Talking Legal Tech – Folge 28

„Regulierung & Innovation - wie lässt sich beides vereinbaren, Martin Ebers?",

32 *KOM*, Ein Europa für das digitale Zeitalter – was sich für Unternehmen ändert, hier abrufbar (Stand: 24.05.2022).
33 Letzteres ist im derzeitigen Art. 74 Abs. 1 des *DSA*-Entwurfs vorgesehen, vgl. KOM(2020)825 final, 86.
34 So wird es hinsichtlich des Geltungszeitpunkts von der EU-Kommission beschrieben, siehe *KOM*, Ein Europa für das digitale Zeitalter: Was sich für Nutzerinnen und Nutzer ändert, hier abrufbar (Stand: 24.05.2022). Allerdings sieht der *DSA*-Entwurf in Art. 74 Abs. 2 eine Geltung drei Monate nach Inkrafttreten der Verordnung vor, KOM(2020)825 final, 86.

Lust auf einen spannenden Job neben dem Studium?

Wir von Wolters Kluwer suchen regelmäßig Werkstudierende in den Bereichen Content, Produktmanagement, Marketing, Sales u. v. m.

Interesse? Dann schau gerne bei uns auf der Karriereseite vorbei!

Wolters Kluwer

careers.wolterskluwer.com

Grundwissen

Compliance goes Digital - Was versteckt sich hinter Digital Compliance?

Isabel Ecker

Open Peer Review

Dieser Beitrag wurde lektoriert von: Julia Keselj und Maria Osmakova

Isabel hat Jura an der Universität zu Köln studiert. Sie schreibt derzeit ihre Promotion im Bereich des Wirtschaftsstrafrechts u.a. zur Criminal Compliance bei Herrn Professor Waßmer und ist Promotionsstipendiatin der Studienstiftung des deutschen Volkes. Zudem ist sie Co-Head und Head of People des Legal Tech Lab Cologne e.V.

Wer aufmerksam die Berichterstattung der letzten Jahre verfolgt hat, kommt an dem Begriff der Compliance nicht vorbei. Karriere macht Compliance immer dann, wenn der nächste große Unternehmensskandal vor der Tür steht. Früher war es ***Siemens***, heute steht ***Volkswagen*** mit einem uferlos anmutenden Abgasskandal im Mittelpunkt der medialen Aufmerksamkeit. Offenbart sich ein jahrelang andauernder Unternehmensskandal, stellt sich oftmals insbesondere bei großen Unternehmen die Frage, wie konnte es so weit kommen, ohne dass jemand das Fehlverhalten bemerkt hat? Jeder, der sich diese Frage stellt, trifft den Kernpunkt, warum wir heute Vorbeugungsmaßnahmen unter dem Stichwort Compliance diskutieren.

A. Grundbegriff Compliance

Compliance zielt auf die Beherrschung von Risiken in einem Unternehmen ab, um Rechtsverstöße zu verhindern. Die verantwortlichen Führungskräfte müssen dafür sorgen, dass die (internationalen) Rechtsnormen und Vorgaben eingehalten werden, um wirtschaftliche Risiken von dem eigenen Unternehmen fernzuhalten, indem Fehlverhalten vermieden wird. Die rechtlichen Grenzen werden durch die öffentliche und private Regulierung der speziellen Bereiche festgelegt. Praktisch soll dieses Ziel durch den Einsatz vorbeugender Unternehmensorganisation wie Kontrollsysteme, Schulungs- und Meldemechanismen erreicht werden. Hierdurch sollen Regelverstöße durch Mitarbeiter und Leitungspersonen vorgebeugt werden, die zu einer ‚Strafe' führen können.

Hierbei ist Strafe nicht herkömmlich strafrechtlich zu verstehen, denn bisher gibt es in Deutschland (noch) kein Verbandssanktionenrecht. Vielmehr liegt der Fokus der Schadensvermeidung bisher vor allem in den Bereichen des Kartellrechts sowie der Vermeidung von Betrugs- und Finanzkriminalität. Dabei haftet etwa auch der Vorstand für ein mangelndes Compliance-System nach § 93 I AktG, wenn er deshalb seiner Überwachungspflichten über die unteren Ebenen des Unternehmens nicht nachgekommen ist. Eine allgemeine Legaldefinition des Compliance-Begriffs existiert bisher nicht. Allerdings hat sich die Definition aus dem Deutschen Corporate Governance Kodex zu einer allgemein anerkannten Leitlinie für den Compliance-Begriff entwickelt.

Grundsatz 4 und 5 des DCGK 2022:
Für einen verantwortungsvollen Umgang mit den Risiken der Geschäftstätigkeit bedarf es eines geeigneten und wirksamen internen Kontroll- und Risikomanagementsystems.
Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der internen Richtlinien zu sorgen und wirkt auf deren Beachtung im Unternehmen hin (Compliance).[1]

DCGK: Der Deutsche Corporate Governance Kodex ist ein von der Regierungskommission Deutscher Corporate Governance Kodex beschlossenes Sammelwerk an besten Vorgehensweisen (engl. Best Practices) für börsennotierte Aktiengesellschaften, die oft über die Anforderungen des Aktiengesetzes hinausgehen. Dabei ist die Regierungskommission ein politisch unabhängiges Gremium von Personen mit Wirtschaftserfahrung wie Vorstands-, Aufsichtsratsmitgliedern und Wirtschaftsprüfern. Da es politisch unabhängig ist, handelt es sich bei dem DCGK mangels demokratischer Legitimation nicht um ein bindendes Gesetz. Jedoch wird die Bindung der Unternehmen indirekt durch § 161 Abs. 1 AktG herbeigeführt, wonach börsennotierte Gesellschaften eine jährliche Entsprechenserklärung abgeben müssen. In dieser Erklärung müssen sie den Anteilseignern mitteilen, wenn sie einer Empfehlung nicht entsprachen und weshalb (Comply-or-Explain-Prinzip). Damit soll eine Selbstbindung ohne Rechtsbindung bewirkt werden, weshalb der DCGK häufig auch als Soft Law bezeichnet wird.

1 Grundsatz 4 und 5 des Deutschen Corporate Governance Kodex in der aktuellen Fassung von 2020, hier abrufbar (Stand: 14.06.22). Aktuell gibt es eine neue Fassung des Deutschen Corporate Governance Kodex 2022, die dem BMJ zur Prüfung vorliegt, hier abrufbar (Stand: 14.06.22). Dort sollen der 4. und 5. Grundsatz vereinigt werden, sodass es unter dem Grundsatz 5 n.F. künftig heißen soll: *„Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der internen Richtlinien zu sorgen und wirkt auf deren Beachtung im Unternehmen hin (Compliance). Das interne Kontrollsystem und das Risikomanagementsystem umfassen auch ein an der Risikolage des Unternehmens ausgerichtetes Compliance Management System."*

Um die Compliance-Risiken zu beherrschen, wird gerade in größeren Unternehmen oftmals ein Compliance-Management-System (***CMS***) implementiert. Dieses CMS besteht grundsätzlich aus mehreren Kernelementen, beginnend mit der Einschätzung des Risikos, gefolgt von der Organisation der möglichen Vorbeugungsmaßnahmen, die das Risiko beherrschen und Fehlverhalten vermeiden sollen. Hinzu kommt die kommunikative Weitergabe der Regularien an die Mitarbeiter und die Schaffung einer integren Unternehmenskultur mit gelebter Compliance.

Zu den Compliance-Maßnahmen können ganz einfache Regularien für das Verhalten von Mitarbeitern gehören, wie Vorgaben zur Annahme von Geschenken. Hinzu kommen Mechanismen, um Indizien für Fehlverhalten zu sammeln, wie etwa die Einrichtung eines Hinweisgebersystems für Whistleblower oder regelmäßige Interviews mit Mitarbeitern. Darin erschöpft sich der Bereich der Compliance jedoch bei Weitem nicht. Compliance ist vielschichtig und gestaltet sich individuell je nach Aufbau, Rechtsform und Größe eines Unternehmens. Schnittmenge der Compliance-Systeme sind die einzuhaltenden Gesetze und Regelungen.

> „Compliance zielt darauf ab, Risiken von vornherein zu minimieren und Verstöße zu vermeiden.“

Im Hinblick auf die verschiedenen zu beherrschenden Risiken lässt sich festhalten, dass die Aufgabe und das Ziel der Compliance ganz überwiegend in der Prävention liegt. Compliance-Management zielt also darauf ab, Risiken von vornherein zu minimieren und Verstöße bereits bevor es zu ihnen kommt, zu vermeiden. Hierneben gibt es einen repressiven Teil der Compliance, also Mechanismen, die greifen, sobald ein Verstoß vorliegt und aufgedeckt wurde. Darunter fallen insbesondere die unternehmensinternen Ermittlungen (engl. ***Internal Investigations***).

B. Compliance und Digitalisierung

Allerdings zeigt sich, dass die präventive Zielsetzung der Schadensvermeidung praktisch schwer umsetzbar ist. Oftmals werden trotz eingerichteter Compliance-Maßnahmen Indizien für Verstöße zu spät erkannt. Die Folge ist, dass es nicht wie geplant zu einer präventiven Aktion kommt, sondern lediglich nachgelagert zu einer Reaktion auf den Verstoß. Grund hierfür ist die Komplexität und Vielschichtigkeit der Prozesse in den Unternehmen, auf die ein analoges Compliance-Programm nicht in Echtzeit reagieren kann. Für die Überwindung des zeitlichen Auseinanderfallens von Fehlverhalten und Reaktion birgt die Digitalisierung eine Lösungsmöglichkeit.

Dieses digitale Spielfeld eröffnet sich durch die Symbiose der Begriffe ‚Compliance‘ und ‚Digitalisierung‘, im Ergebnis ‚Digital Compliance‘, wobei sich die Oberkategorie der Digital Compliance in zwei Themenblöcke unterteilen lässt: In einem ersten Schritt stellt sich die Frage, wie ein Compliance-System durch technische Tools umgesetzt werden kann (***Digitalisierte Compliance***). Ist dies beantwortet, so muss sichergestellt werden, dass das digitale Compliance-System selbst auf die eigene Compliance überprüft werden kann (***Compliance der Digitalisierung***).

I. Digitalisierung der Compliance durch technische Tools (Digitalisierte Compliance)

1. Technische Einsatzfelder

Unter den Begriff der Digital Compliance fällt der Einsatz technischer Tools in einem Compliance-Prozess. Es geht im Kern unmittelbar um die Digitalisierung von Abläufen. Während Vorbeugemaßnahmen überwiegend analog durchgeführt wurden, etwa durch Mitarbeiterschulungen und menschliche Risikobewertung, können diese Maßnahmen in vielen Bereichen technisiert und hierdurch verbessert werden. Begonnen werden kann mit einer Technisierung der Risikobewertung. Der Einsatz von Big-Data-Technologie und Algorithmen bietet die Möglichkeit, durch umfangreiche Dateneingabe Risikowahrscheinlichkeiten zu bestimmen. Eine detaillierte

Vorhersage des Risikos führt aus Unternehmenssicht zu einer besseren Skalierbarkeit und ‚Bilanzierbarkeit' des Risikos. Hierdurch können Kosten durch gezielten Einsatz in Hochrisikobereichen kanalisiert und in der Gesamtheit sinnvoll eingespart werden. Durch die ergänzende Einspeisung neuronaler Daten in das System kann die Eintrittswahrscheinlichkeit bestimmter menschlicher Verhaltensweisen anhand ausgewählter Parameter prognostiziert werden (***Predictive Analytics***[1]). Diese Ergänzung führt zu einer noch genaueren Berechnung des Risikos. Insgesamt ermöglicht eine schnelle Risikobewertung für das Unternehmen eine finanzielle Skalierbarkeit bestimmter Risikobereiche und ermöglicht die Kategorisierung der Risikogruppen für ein CMS.

Geht es um starre regulatorische Vorgaben, also beispielsweise feste Werte, die bei der Produktion eingehalten werden müssen, könnte deren Einhaltung unmittelbar durch (algorithmische) Analysetools überprüft werden. So können mehrere Daten aus parallelen Prozessen in Echtzeit erfasst, abgeglichen und bewertet sowie visualisiert und zusammengefasst werden. Wird eine Vorgabe verfehlt, kann das Analysetool den Prozess kurzzeitig unterbrechen und auf den Fehler hinweisen. Die Transparenz eines komplexen Prozesses steigt hierdurch enorm an und der Prozess lässt sich zu jeder Zeit nachverfolgen. Eine Nachverfolgbarkeit des Prozesses würde auch eine Datenspeicherung z.B. in der Blockchain garantieren.

Problematisch kann es bei dem Einsatz solcher Tools jedoch werden, sobald sich regulatorische Vorgaben des Gesetzgebers (sowohl national als auch international) ändern. In diesem Fall müssen die Daten in dem verwendeten Compliance-Tool unmittelbar angepasst werden. Durch die Vielzahl an Regelungen, die es zu beachten gilt und die stetigen inhaltlichen Weiterentwicklungen der Normen sowie der Europäisierung der Gesetze, sind die betroffenen Unternehmen ständig angehalten, ihre Compliance-Vorgaben und Systeme anzupassen. Es kommt zu immer höheren Compliance-Ausgaben für die Unternehmen.

Allerdings bietet der Einsatz digitaler Lösungen auch in diesem Bereich einen Vorteil: Für die regulatorischen Anwendungsfälle werden Softwarelösungen zur Unterstützung der Compliance entwickelt, deren Ziel es ist, sich ändernde Regularien in Echtzeit in bereits bestehende Compliance-Systeme zu integrieren (‚Regulatory Technology', kurz: ‚RegTech'). Die Vorteile einer solchen technischen Lösung liegen vor allem in der extremen Zeitersparnis. Hinzu kommt die Tatsache, dass keine Lücke im bestehenden CMS besteht. Durch die zeitliche Kohärenz zwischen einer neuen Regel und der Einbettung in das bestehende CMS wird nahtlos neuen Verstößen vorgebeugt.

Wichtig sind jedoch nicht nur die technischen Mechanismen zur Gesamtrisikominimierung im Unternehmen. Das zweite elementare Standbein einer effektiven Compliance ist das Verständnis und das Mindset der Mitarbeiter. Bisher beschränkt sich die Vermittlung der Compliance-Richtlinien oftmals entweder auf dicke Papierstapel, die nicht gelesen werden bzw. schwer verständlich sind oder auf Schulungen, die eine Bandbreite von Compliance-Themen in Form von Frontalunterricht abdecken. Hinzu kommt, dass die Zeiten für Schulungen oft starr sind und es dementsprechend an der regelmäßigen Auffrischung der wichtigen bereichsbezogenen Compliance-Vorgaben fehlt.

An dieser Stelle bietet der Einsatz von on demand E-Learning Angeboten eine Chance, den Mitarbeitern individualisiert, interaktiv und regelmäßig das für sie wichtige Wissen zu vermitteln. Durch einen enger getakteten Schulungsrhythmus kann zudem erreicht werden, dass die Thematik Compliance jederzeit fest in den Köpfen der Mitarbeiter verankert ist, was das generelle Compliance-Mindset bestärkt. Für die textuelle Aufbereitung der Richtlinien sollte auf zwei Säulen gebaut werden. Erstens müssen die Informationen kanalisiert und individualisiert werden, sodass jeder Mitarbeiter die für seinen Bereich wichtigen Informationen erhält. Ein Mitarbeiter, der beispielsweise in einem internen Verwaltungsbereich mit geringem Risiko arbeitet, benötigt nicht dieselben Compliance-Informationen, wie ein Mitarbeiter, der in einem Hochrisikobereich arbeitet, wie dem Vertrieb. Zudem sollten situationsbe-

1 Für weitere Ausführungen zu Predictive Analytics, insb. zu der Verwendung durch die deutschen Polizeibehörden, vgl. *Scholz*, CTRL 2/21, 110 ff.

zogene Compliance-Richtlinien angezeigt werden können. So könnte etwa bei einer Geschäftsreise eine automatisierte, auf das Zielland zugeschnittene, Compliance-Übersicht auf das Smartphone oder Tablet eines Mitarbeiters geschickt werden. Dieser kann sich dann auf einen Blick ins Gedächtnis rufen, was er im Folgenden zu beachten hat.

Zweitens sollte an der Darstellung der Information gearbeitet werden. Hier muss zwar eine präzise, aber dennoch verständliche Darstellung nach dem Legal-Design-Thinking-Ansatz[2] das Ziel sein. Ergänzend zu der allgemeinen Darstellung könnten in Hochrisikobereichen bei der täglichen Arbeit technische Checklisten installiert werden, die einem Mitarbeiter verständlich, übersichtlich und schnell anzeigen, welche Punkte er bedenken und beachten muss, um Verstößen bereits im Arbeits- bzw. Produktionsprozess zu begegnen.

All dies lässt sich durch die Big-Data-Technologie umsetzen. Durch Einspeisung interner Compliance-Daten sowie repräsentativer Mitarbeiterdaten, deren Bedürfnisse in verschiedenen Situationen erfasst werden, ließen sich individuelle Risikoprofile erstellen. Diese Profile können wiederum situationsabhängig eingestuft werden. Funktioniert die digitalisierte Compliance einfach, verständlich und schnell, wird die Akzeptanz der Maßnahmen durch die Mitarbeiter weiter ansteigen.

2. Vorteile des Einsatzes neuer Technologien

Die genannten Beispiele verdeutlichen einen Teil der möglichen Einsatzmöglichkeiten digitaler Compliance-Tools. Sie bieten den Unternehmen die Chance, ihre Compliance zu vereinfachen und effizienter, verständlicher sowie verlässlicher zu gestalten. Der Einsatz digitaler Technologien verhilft der Compliance letztlich erst zur Erreichung ihres tatsächlichen Ziels, nämlich der Antizipation des drohenden-Risikos verbunden mit der präventiven Vermeidung von Fehlern oder Verstößen im Gegensatz zu einer erst nachgelagerten Reaktion auf einen Verstoß.

Analoge Compliance-Mechanismen arbeiten trotz präventiver Ausrichtung oftmals zu langsam. Es fehlt an der Möglichkeit, Indizien für die Gefahr eines drohenden Verstoßes im Vorfeld zu erkennen und zu verhindern. Durch die Implementierung der neuen Technologie in bestehende CMS kann eine Überwachung in Echtzeit ablaufen und schon während des laufenden Geschäftsprozesses korrektive Wirkung entfalten.

> „Funktioniert die digitalisierte Compliance einfach, verständlich und schnell, wird die Akzeptanz der Maßnahmen durch die Mitarbeiter ansteigen.“

Zudem ist eine digitalisierte Compliance finanziell für die Unternehmen von Vorteil, da Verstöße mit immer härteren Bußgeldern einhergehen, die schlimmstenfalls in die Insolvenz führen können. Doch nicht nur die im Falle eines Verstoßes drohende finanzielle Gefahr stellt für die betroffenen Unternehmen eine Belastungsprobe dar. Hinzu kommt der drohende, erhebliche Reputationsschaden, der durch das Fehlverhalten ausgelöst wird. Es ist somit von höchstem Unternehmensinteresse, Verstöße effektiv zu vermeiden. Genau dieses Ziel kann mit einer digitalisierten Compliance besser erreicht werden.

3. Einsatzgrenzen neuer Technologien

Neben zahlreichen Vorteilen birgt eine digitalisierte Compliance allerdings neue Risiken und Hürden, die es zu bewältigen gilt. Zuvorderst bedarf es für die meisten Systemideen einer großen Menge an Trainingsdaten. Ohne diese Trainingsdaten wird die Digitalisierung im Compliance-Bereich in ihrem Keim ersticken. Die Nutzung großer Datenmengen bringt als Folge Fragen des Datenschutzrechts mit sich.

2 Zu den Hintergründen, Vorteilen und Vorgehensweisen bei Legal Design Thinking, s. *Bayzat,* CTRL 2/21, 178 ff.

Ob Big Data, Blockchain oder Algorithmen: Daten sind die Grundlage eines erfolgreichen Gelingens der Digitalisierung. Umso wichtiger wird es für Unternehmen sein, sich frühzeitig mit den komplexen Vorschriften rund um den Schutz der Daten zu befassen. Zu datenschutzrechtlichen Vorgaben kommen jedoch eine Vielzahl weiterer Vorschriften, die es zu beachten gilt. Die sich stark im Wandel befindliche, komplexe gesetzliche Struktur macht eine ständige Anpassung notwendig, was sicher eine Herausforderung für die Unternehmen darstellen wird. Die Komplexität der Regelungsmaterie wird durch die Unterschiede zwischen den Rechtsordnungen noch verstärkt, insbesondere für ein international operierendes Unternehmen. Zuletzt besteht die Gefahr von Angriffen auf die eigene IT-Sicherheit und Infrastruktur. Wer sich digital aufstellt, muss jederzeit mit Hacking-Angriffen rechnen. Diese Angriffe können neben anderen sensiblen Bereichen ebenso eine digitalisierte Compliance betreffen.

II. Compliance der eingesetzten Tools (Compliance der Digitalisierung)

Die Risiken, die der Einsatz digitaler Tools mit sich bringt, ist unmittelbarer Grund für den zweiten Themenkomplex, der unter dem Stichwort Digital Compliance diskutiert wird. Dieser erfasst solche Compliance-Maßnahmen, die Risiken managen, welche erst durch den Einsatz eines technischen Tools entstehen. Wird also z.B. Blockchain eingesetzt, müssen die Risiken, die ein Blockchain-Einsatz mit sich bringt, wiederum eingeschätzt und beherrscht werden. Überspitzt gesagt, könnte es eine Compliance für ein technisches Compliance-Tool geben. Dass für den Einsatz von Technologien selbst wiederum ein gutes Compliance-Management gefragt ist, zeigt die Auswirkung von Fehlern in diesem Bereich. Kommt es zu einem Cyber-Angriff auf das Unternehmen, ist der daraus resultierende Schaden oftmals verheerend.[3] Zudem werden für den Einsatz neuer Technologien zunehmend eigenständige Regularien geschaffen. Insbesondere der europäische Gesetzgeber ist aktiv geworden und möchte weitere Auflagen und Vorschriften für verschiedene Technologien schaffen, so zum Beispiel der Artificial Intelligence Act[4] als Regulierung Künstlicher Intelligenz. Wird somit algorithmische Analyse im Unternehmen eingesetzt, gilt es, die gesetzlichen Anforderungen an die Nutzung des Systems sicherzustellen.

C. Digitalisierte Compliance mit Maß und Verstand

Aus Unternehmenssicht lässt sich also festhalten, dass digitalisierte Compliance eine enorme Effizienzsteigerung bewirken kann. Auch aus Mitarbeitersicht ist der Nutzen digitaler Tools offenkundig. Wer zu jeder Zeit besser verstehen kann, wo sich die gesetzlichen Grenzen befinden, wird effektiv vor Fehlern oder Verstößen geschützt und wendet damit nicht nur schwere Folgen für das Unternehmen ab, sondern ebenso für sich selbst.

> „Digitalisierte Compliance bietet die Chance auf Fortschritt, darf jedoch nicht überbewertet werden.“

Weitet man den Blick, zeigt sich, dass auch die Allgemeinheit ein Interesse an funktionierender präventiver Compliance hat, um Schäden vorzubeugen. Denn von einem Skandal, wie einem solchen rund um die Abgaswerte, ist nicht nur das Unternehmen und dessen Mitarbeiter betroffen, sondern letztlich auch der Verbraucher. Digitalisierte Compliance bietet die Chance auf Fortschritt, darf jedoch

3 Durch derzeit frequentiertere Cyber-Angriffe von russischen Hackergruppen auf deutsche Unternehmen, stellen sich vornehmlich bei der Frage der Lösegeldzahlung, um die erlangten Daten zurückzuerhalten, spannende rechtliche Fragen. So kann die Zahlung von Lösegeld eine Terrorismusfinanzierung nach § 89c StGB oder eine Straftat nach § 18 AWG darstellen, wobei auch die Frage einer etwaigen Rechtfertigung nach § 34 StGB relevant wird.

4 Zum Artificial Intelligence Act im Detail: *Ecker/Mahlow*, CTRL 1/22, 118 ff.

nicht überbewertet werden. Die Komplexität vieler Situationen wird es notwendig machen, weiterhin dispositiven menschlichen Spielraum bei der Risikobewertung und -bewältigung einzuräumen. Es wird demnach weiterhin zu Regelverstößen kommen. Allerdings wird eine Verknüpfung der Digitalisierung mit verbleibenden menschlichen Einschätzungsspielräumen die Fehleranfälligkeit des Risikomanagements minimieren und Fehler bei der Umsetzung und Ausführung vermeiden. Die digitalisierte Compliance trägt hierzu bei, indem sie Fehler in Echtzeit erkennt und von vornherein verhindert. In diesem Sinne: Let's go Digital Compliance!

Weiterführende Hinweise:

Talking Legal Tech – Folge 5

„Was ist die Blockchain, Florian Glatz?", Link: https://anchor.fm/legaltech/episodes/Was-ist-die-Blockchain--Florian-Glatz-ea5blt

Talking Legal Tech – Folge 15

„Legal Design – was ist das, Lina Krawietz?", Link: https://anchor.fm/legaltech/episodes/15-Legal-Design---was-ist-das--Lina-Krawietz-edara9

Weiterführende Hinweise:

Um das Thema Digital Compliance zu vertiefen, bieten sich die im Folgenden genannten Beiträge an, die auch eine Grundlage dieses Beitrags bilden:

Generell zur Compliance s. ***Hauschka/Moosmayer/Lösler***, Corporate Compliance, 3. Auflage 2016; und ***Wieland/Steinmeyer/Grüniger***, Handbuch Compliance-Management, 3. Auflage 2020.

Deutscher Corporate Governance Kodex (Fassung von 2020), hier abrufbar (zuletzt abgerufen am 15.06.22).

Eingehend auf bereits eingesetzte Tools und deren Wirkweise im Rahmen der Digital Compliance: ***Heißner/Schaffer***, CCZ 2018, 147 ff., sowie ***Timmermann,*** Legal-Tech-Anwendungen, Berlin Diss. 2020, S. 118 ff.

Einen guten Überblick über beide Ausprägungen der Digital Compliance bietend: ***Bräutigam/Habbe***, NJW 2022, 809 ff.

Zur technischen Ausgestaltung der Tools s. ***Neufang***, IZR 2017, 249 ff.

Speziell zur digitalen Compliance-Kommunikation für Schulungen von Mitarbeitern: ***Hastenrath***, CCZ 2020, 162 ff.

LEGAL HACKATHON 2022 COLOGNE

SEPTEMBER
16. – 18. 2022

Schirmherrschaft

Bundesministerium der Justiz

Wolters Kluwer

EBNER STOLZ

Gateway
Exzellenz Start-up Center
Universität zu Köln

EXZELLENZ START-UP CENTER NORDRHEIN-WESTFALEN

LEGAL TECH LAB COLOGNE

LTO Legal Tribune Online

LEGAL TECH VERZEICHNIS
Wissen · Markt · News · Jobs

LEGAL-TECH.DE
WIE ANWÄLTE NEUE CHANCEN NUTZEN

legalhackathon.de

Kolumne

eSport-Recht: Nur Sportrecht 2.0?

Professor Dr. Martin Maties

Open Peer Review

Dieser Beitrag wurde lektoriert von: Ramon Schmitt und Philipp Beckmann

Professor Dr. Martin Maties ist Inhaber einer Professur an der Universität Augsburg und dort zugleich Gründer und Leiter der Forschungsstelle für eSport-Recht (FeSR). Er ist Kommentator der §§ 611, 611a, 612, 613 und 614 BGB im BeckOnline-Großkommentar, Autor mehrerer Lehrbücher im Zivil- und Arbeitsrecht und veröffentlicht auch sonst überwiegend im Arbeit-, Zivil- und eSport-Recht.

Wirtschaftliche und gesellschaftliche Bedeutung

Für junge Juristen tun sich stets neue Betätigungsfelder auf. Ein prosperierendes und hinsichtlich juristischer Fragen noch sehr unter beleuchtetes Gebiet stellt das eSport-Recht dar. eSport hat sich in den letzten Jahren zu einem wirtschaftlichen Erfolg entwickelt, der auch jenseits der Branche nicht mehr ignoriert werden kann. Die im eSport erreichten Umsätze der Unternehmen beliefen sich im Jahr 2021 weltweit auf 1,14 Milliarden Dollar.[1] Damit wurde ein Anstieg um 14,1 % im Vergleich zum Vorjahr verzeichnet.

Dabei nimmt eSport immer mehr Platz im Bereich der Unterhaltungsmedien ein,

1 *Tenzer*, Prognose zum Umsatz im eSports-Markt weltweit bis 2025, hier abrufbar (Stand: 01.08.2022).

aber auch im Bereich der aktiven Spieler. So werden diverse eSport-Events weltweit gestreamt und Zuschauerzahlen erzielt, die bei den meisten ‚analogen' Sportarten gar nicht erreicht werden. Die Anzahl der Personen, die sich zumindest gelegentlich eSports-Events anschauen, belief sich im Jahr 2021 auf rund 489,5 Millionen weltweit.[2]

Diese hohen Zuschauerzahlen wirken sich auch auf das Preisgeld aus: Das höchstdotierte eSport-Turnier im Jahr 2021 war das Dota-2 Turnier „*The International 2021*", bei dem Preisgelder von insgesamt 40 Millionen Dollar erspielt wurden.[3] Der Trend steigender Umsätze, Zuschauerzahlen und Preisgelder setzt sich seit Jahren kontinuierlich fort.

B. Rechtliche Einordnung

Aufgrund dessen ist es den Kennern der Szene klar, dass dieser Bereich der Digitalisierung nicht nur einen Markt darstellt, der neue Berufsfelder schafft, sondern auch zugleich ein solcher ist, in welchem sich naturgemäß aufgrund der hohen Verdienstmöglichkeiten verschiedenste Rechtsfragen auftun.

I. Verbandsstruktur vs. vertragliche Rahmenbedingungen

Während im Sport überwiegend eine Verbandsstruktur (z.B. ***FIFA, UEFA, DFL***) innerhalb der einzelnen Sportarten besteht, kann man dies für den eSport nicht in vergleichbarem Maße feststellen. Dies geht insbesondere darauf zurück, dass beim ‚analogen' Sport niemand Verwertungs- und Nutzungsrechte an der Sportart als solcher hat. So wird etwa Fußball in Bezug auf Spielfeldlänge, Torgröße, Ballgröße und Spielregeln nicht von Einzelnen bestimmt, sondern von den gewachsenen Verbandsstrukturen festgelegt, denen sich die im Verband befindlichen Mitglieder (Vereine) unterwerfen. Dies ist im eSport-Recht anders.

Beim eSport gibt es regelmäßig ein Unternehmen, das das Urheberrecht und die Verwertungsrechte am eSport-Titel hat. Dieser sogenannte Publisher hat hier eine Machtstellung inne, die es ihm ermöglicht, den Gegenstand des eSport-Titels nach seinem Belieben festzulegen.

> „Der Publisher hat hier eine Machtstellung inne, sodass er den Gegenstand des eSport-Titels nach seinem Belieben festlegen kann."

Sofern und soweit Turniere veranstaltet werden, können diese durch den Publisher oder einen sogenannten Drittanbieter durchgeführt werden. Zu diesen Turnieren melden sich entweder ***Clans*** (Vereine) als Teams oder Einzelspieler an. Da der Spielgegenstand somit aber aufgrund der absoluten Rechte vom Publisher abhängt und er den Drittanbietern nur Lizenzen für die Nutzung erteilt, liegt es allein an ihm, ob und wie sich ein eSport-Titel entwickelt. Insbesondere können sich die ***Clans*** und Spieler nicht einfach anders strukturieren und den eSport-Titel in anderer Art und Weise auf Turnierebene praktizieren.

Dementsprechend hilft eine klassische Verbandsstruktur aufgrund der herausgehobenen Stellung des Publishers nicht weiter. Aufgrund dessen liegt die Ausgestaltung der Rechtspositionen aller Beteiligten zueinander in den Händen der vertragsentwerfenden Juristen. Die Vertragsgestaltung ist damit von besonderer Bedeutung. In diesem Zusammenhang sind die Endbenutzer-Lizenzverträge (***EULA***) von herausragender Bedeutung und müssen rechtlich sauber ausgearbeitet und wirksam vereinbart sein.

2 Ebd.
3 *Tenzer*, Preisgelder der höchstdotierten eSports-Turniere weltweit bis 2022, hier abrufbar (Stand: 01.08.2022).

EULAs:

End User Licence Agreements (EULAs, dt. Endbenutzer-Lizenzverträge) räumen dem Endverbraucher ein Nutzungsrecht für die erworbene Software ein. Als AGB regeln sie, in welcher Weise der Endnutzer die Software verwenden darf, welche Rechte beim Entwickler oder Publisher verbleiben und etwaige Haftungsbeschränkungen. Man findet sie oft nach dem Download und starten einer neuen App und muss sie annehmen. Lehnt man sie ab, ist die Software nicht nutzbar.

II. Folgen der Struktur

Bereits diese Struktur macht klar, dass sich diverse Rechtsfragen auftun, die für eine ganze Generation von Juristen interessant werden können. So sind nicht nur die Verträge zwischen Publishern und Drittanbietern interessant, sondern auch die Frage, ob Turnierveranstalter Vereine und Spieler auf Basis ihrer privatautonomen Entscheidungen ausschließen können. Aufgrund der Vertragsfreiheit müsste dies den Veranstaltern freistehen, da es kein Kontrahierungszwang gibt. Andererseits kann es sein, dass die Spieler aus ihrer Tätigkeit als eSportler einen Beruf gemacht haben, der über Art. 12 I GG grundrechtlich geschützt ist. Umgekehrt kann es sein, dass Fehlverhalten von Spielern zu sogenannten Sperren und ***Bannings*** führt, die als Sanktionen für unerlaubtes Spielverhalten vom Publisher oder dem Turnieranbieter verhängt werden. Hier können also Grundrechte in mittelbarer Drittwirkung im Zivilrecht aufeinanderprallen und bei der Auslegung zu berücksichtigen sein.

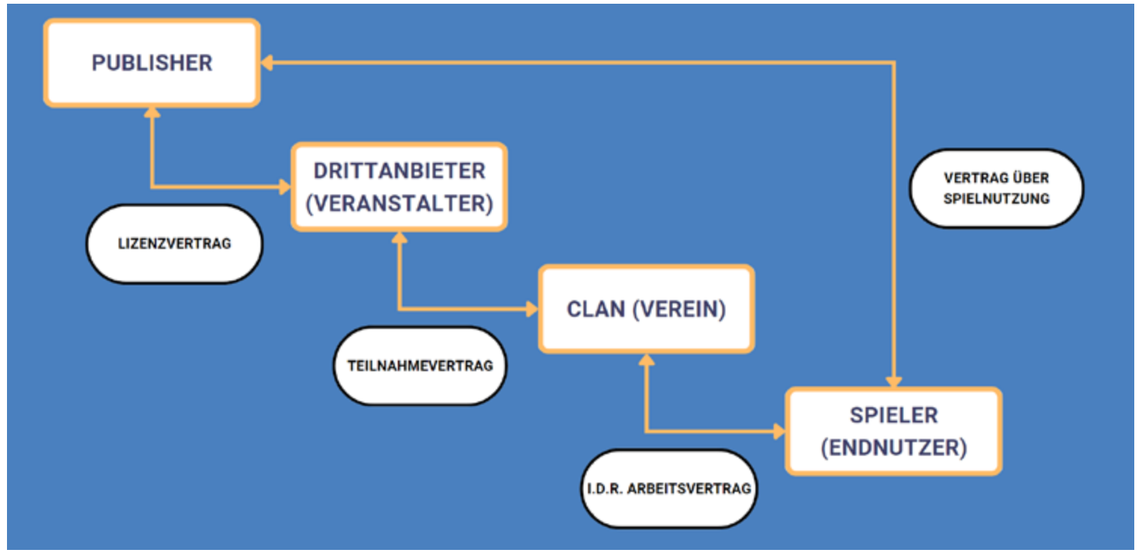
C. Querschnittsmaterie

eSportrecht tangiert nicht nur das Zivilrecht (insbesondere Vertragsgestaltung, Minderjährigen-Recht, Verbraucherschutz und Immaterialgüterrecht), sondern zieht auch diverse Fragen im Arbeits-, Straf-, Steuerrecht und vielen anderen Rechtsgebieten nach sich.

So wird beispielsweise zwischen einem Profi-eSportler und einem Verein regelmäßig ein Arbeitsvertrag (Arbeitsrecht) bestehen. Sofern und soweit (was im eSport nicht selten vorkommt) im Rahmen von Chats und andere Nachrichten ***Toxic Behavior*** (dt. beleidigendes Verhalten) vorkommt oder auch ***gecheatet*** wird (dann womöglich § 263 StGB), ist das Strafrecht betroffen.

Wenn Spieler aufgrund ihrer beruflichen Tätigkeit Einnahmen generieren (Gehälter und Preisgelder), stellt sich die Frage der Steuerpflichtigkeit; besonders umstritten ist auch die Gemeinnützigkeit im eSport, da hier diskutiert wird, ob eSport unter den Sportbegriff fällt und somit steuerrechtlich nach § 52 II Nr. 21 AO privilegiert ist.

Außerdem kann die Übertragung der Turniere im Internet das Rundfunkrecht ebenso betreffen wie das Urheberrecht. Die Einreise aus Nicht-EU-Ländern zur Turnier-Teilnahme kann das Ausländerrecht betreffen. Die Aufzählung könnte hier beliebig fortgesetzt werden.



Vertragsbeziehungen zwischen den einzelnen Parteien bei eSport-Turnieren.

D. Folgen der Unbekanntheit

Wie so häufig ist auch im eSport zu beobachten, dass eine wirtschaftlich prosperierende Materie sich rascher entwickelt als die Gesetzeslage und die Gesetzesanwendung durch Juristen.

Erschwerend kommt hinzu, dass sich die meisten Juristen, die sich mit einschlägigen Fällen befassen müssen, noch nicht mit der Materie auskennen. Wenn man bedenkt, welches wirtschaftliche Potenzial dahintersteckt und aufgrund dessen Rechtsstreitigkeiten provoziert werden, steht zu erwarten, dass wir auf Dauer – ebenso wie im Sportrecht – viele Experten im Bereich des eSports Rechts brauchen werden. Sicherlich kann man viele Parallelen zwischen eSport und Sport im Rechtlichen ziehen und Erkenntnisse übertragen. Jedoch sind auch mannigfaltige Unterschiede gegeben, da eben im eSport-Recht eine andere Struktur der ***Stakeholder*** besteht.

„Weil hier meine **Persönlichkeit** zählt“

Rouven Siegemund
Partner

Bewirb dich bei uns als

Legal Engineer (w/m/d)

und werde Teil von

#teamtomorrow

Scanne den QR-Code ein und erfahre, was hinter dieser Stelle und #teamtomorrow steckt. Wir freuen uns auf deine Bewerbung!

oder klicke hier

Grundwissen

Aussicht auf das große Geld durch die DSGVO?

David Wasilewski

Open Peer Review

Dieser Beitrag wurde lektoriert von: Joela Worm und Lisa Krebber

David studiert Rechtswissenschaften an der Universität zu Köln und ist wissenschaftliche Hilfskraft an der Kölner Forschungsstelle für Medienrecht. Er interessiert sich für Themen an der Schnittstelle zwischen Recht und neuen Technologien und arbeitet im Bereich Legal Affairs in einem DeepTech und KI Start-up.

Warum überhaupt Legal Tech?

Das Argument der Legal-Tech-Anbieterinnen ist es, jeder[1] ‚Zugang zum Recht' zu verschaffen. Es soll nicht mehr auf Spezialwissen oder die Größe des eigenen Geldbeutels ankommen. Es heißt, dass Ansprüche mit ‚kleinen' Streitwerten oftmals nicht mehr von Anwältinnen angenommen würden, da der Kosten-Nutzen-Faktor in einem unökonomischen Verhältnis stünde. Im Gegensatz dazu versuchen Legal-Tech-Anbieterinnen Forderungen oder Ansprüche von einer großen Anzahl an Per-

1 Der Beitrag wurde im generischen Femininum verfasst. Natürlich sollen alle Personen angesprochen werden.

sonen zu akquirieren, um diese dann einzufordern oder vor Gericht durchzusetzen.[2] Die Bündelung und Automatisierung von einer Vielzahl von Forderungen steigert damit die Attraktivität, Rechtsstreitigkeiten auch mit ‚geringeren' Streitwerten auszufechten. Allerdings nur, wenn diese auf einem größtenteils vergleichbaren Sachverhalt beruhen. Dies wurde in der Vergangenheit eindrucksvoll am Beispiel von Fluggastrechten, aber auch bei Hartz-IV-Bescheiden gezeigt. Je mehr Verbraucherinnen dieses Geschäftsmodell nutzen, desto größer sind die Gewinnchancen. Die Gewinnmaximierungsmöglichkeiten für Legal-Tech-Anbieterinnen steigen, wenn Unternehmen mehrfache Verstöße gegen die Rechtsordnung begangen haben und deswegen negativ in der breiten Öffentlichkeit auffallen. Deshalb werden diese Angebote auch verstärkt durch Marketingmaßnahmen angepriesen. So sollen die ‚unwissenden' Bürgerinnen auf ihre möglichen Schadensersatzansprüche aufmerksam gemacht werden. Durch die Übernahme der Kosten und Risiken der Legal-Tech-Anbieterinnen gehen diese Personen auch vermehrt auf die Angebote ein, wodurch der ‚Zugang zum Recht' mehr Menschen ermöglicht werden soll. Einen Teil der Zahlungen, die aufgrund der durchgesetzten Ansprüche geleistet werden, behalten sich die Legal-Tech-Anbieterinnen sodann als Gegenleistung ein. Teilweise lassen sich die Legal-Tech-Anbieterinnen entsprechende Ansprüche auch abtreten.

Man könnte behaupten, dass so eine Win-win-Situation geschaffen wird. Jedenfalls aus Verbraucherinnensicht. Eine breitere Masse bedient sich dem Recht und die Anbieterinnen verdienen daran. Eine nicht bediente Marktlücke wurde gefunden und wird nun zunehmend durch Legal-Tech-Anbieterinnen gefüllt.

B. Was hat das Datenschutzrecht damit zu tun?

Art. 82 I, II S. 1 DSGVO:

„Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter."

Diese Möglichkeiten der Forderungsbündelung bieten sich auch für Legal-Tech-Anbieterinnen seit dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) im Jahre 2018 im Bereich des Datenschutzrechts. Hauptgrund dafür ist, dass jeder Person nach Art. 82 DSGVO bei einem Verstoß gegen die DSGVO durch Verantwortliche oder Auftragsverarbeiterinnen ein Schadensersatzanspruch zusteht. Allerdings kann sich das Unternehmen bei fehlendem Verschulden gem. Art. 82 III DSGVO exkulpieren. Ungewöhnlich ist dabei, dass neben materiellen auch immaterielle Schäden einen Anspruch begründen. Dies führt bei Cyberangriffen zu einer potenziell großen Anzahl von möglichen Berechtigten.

Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde.

„Die Bündelung und Automatisierung von einer Vielzahl von Forderungen steigert die Attraktivität, Rechtsstreitigkeiten auch mit ‚geringeren' Streitwerten auszufechten."

2 Zu diesem Vorgehen und inwieweit dies für Rechtsanwälte möglich ist und was sich durch die große BRAO-Reform im Berufsrecht der Anwälte in Bezug auf Legal Tech ändert: *Deckenbrock*, CTRL 2/22, 86 ff.

Dies soll ein Beispiel illustrieren: Ein Unternehmen speichert unbeabsichtigt Kundinnendaten auf einem öffentlichen Server. Dadurch werden tausende von E-Mail-Adressen von Kundinnen öffentlich ins Netz gestellt. Diese Daten könnten andere Akteurinnen illegitimerweise nutzen, um eigene Zwecke zu verfolgen; beispielsweise um Werbemails an die E-Mail-Adressen zu senden. Das Unternehmen könnte hier gegen ihre Pflicht zur Sicherstellung eines angemessenen Schutzniveaus bei der Verarbeitung personenbezogener Daten gem. Art. 32 II, 5 I lit. f DSGVO verstoßen haben. Zusätzlich müsste das Unternehmen gegebenenfalls den Vorfall gem. Art. 33 I 1 DSGVO an die zuständige Aufsichtsbehörde melden. Wenn diese dann eine Geldbuße verhängt (vgl. Art. 83 DSGVO), werden diese meist auch veröffentlicht.[3] Hinzu kommt, dass in diesen Fällen gem. Art. 34 I DSGVO auch unverzüglich eine Meldung an die betroffenen Personen erfolgen muss. Dieser Vorfall wird somit durch die Behörde und der Presse einer breiten Öffentlichkeit bekannt. Dies gibt den Legal-Tech-Anbieterinnen die Möglichkeit, mit Betroffenen in Kontakt zu treten und die Durchsetzung eines Schadensersatzanspruches nach Art. 82 I DSGVO anzubieten.

In Bezug auf den Umfang des Schadensersatzanspruches aus Art. 82 I DSGVO haben deutsche Gerichte bislang sehr unterschiedlich geurteilt. Bisher erstrecken sich zugesprochene Schadensersatzansprüche – auch und gerade aufgrund von immateriellen Schäden – von 25 € bis 5.000 €. Diese Ansprüche können von den Legal-Tech-Anbieterinnen gebündelt und damit tausendfach geltend gemacht werden. Je nach Höhe des individuellen Schadenersatzes kann dies schnell zu einer existenzbedrohenden Situation für das betroffene Unternehmen führen. Bei einem bekannten Fall bezüglich eines Datenleaks aus dem Jahre 2020 wurden etwa drei Millionen Kundinnendaten offengelegt. Das Potenzial einer Bündelung von entsprechenden Schadensersatzansprüchen ist in derartigen Fallgruppen besonders groß, da alle Geschädigten vom exakt gleichen Sachverhalt betroffen sind und mittels Legal Tech oft nur der Name der Betroffenen in der Klageschrift geändert werden muss. An dieser Stelle soll nicht diskutiert werden, ob Legal-Tech-Anbieterinnen den ‚Zugang zum Recht' verbessern. Es soll vielmehr darauf eingegangen werden, ob die aufgezeigte Entwicklung in Bezug auf den immateriellen Schadensersatz begrüßenswert ist, das Recht auf Schutz personenbezogener Daten wirklich stärkt oder damit ‚nur' das große Geld verdient werden soll.

3 Vgl. für eine Übersicht *Luther*, DSGVO Bußgeldatlas, hier abrufbar (Stand: 16.06.2022).

C. Der immaterielle Schadensersatz

Deutsche Gerichte haben aufgrund der Regelung des § 253 I BGB in der Vergangenheit sehr restriktiv immaterielle Schäden anerkannt und diesen dann meist auch nur in relativ geringem Umfang stattgegeben. Anerkannte Fallgruppen sind etwa Persönlichkeitsrechtsverletzungen (dann über § 823 I BGB i.V.m. Art. 2 I, 1 I GG)[4] oder Körper- und Gesundheitsverletzungen (vgl. § 253 II BGB). Diese Beschränkungen können für die DSGVO jedoch nicht ohne weiteres gelten, da nach Art. 82 I DSGVO der immaterielle Schaden dem materiellen Schaden gleichgestellt wird. In Bezug auf Art. 82 DSGVO gibt es unterschiedliche Meinungen, wann ein immaterieller Schaden zugesprochen werden sollte und ein Urteil des EuGH dazu steht noch aus.

Wie sieht es aber in dem gerade geschilderten Fall hinsichtlich der Speicherung auf öffentlichen Servern aus? Dort sind E-Mail-Adressen abhandengekommen und andere Akteurinnen haben infolgedessen die Kundinnen mit Werbemails ‚belästigt' (vgl. § 7 I, II Nr. 2 UWG). In diesem Fall entsteht den Kundinnen kein materieller Schaden. Aufgrund von Art. 82 I DSGVO müssen die Gerichte nun entscheiden, ob, unter welchen Voraussetzungen und in welchem Umfang ein immaterieller Schaden ersatzfähig ist.

4 Hierbei handelt es sich dogmatisch nicht um einen direkten immateriellen Schadensersatzanspruch, sondern um einen von der Verfassung vorgegebenen Entschädigungsanspruch, da insb. § 253 II BGB keinen immateriellen Schadensersatzanspruch für die Verletzungen von Persönlichkeitsrechten vorsieht.

I. Vertretene Ansichten

1. Enge Auslegung

Vertreterinnen des ‚engen' Schadensbegriffs verlangen teilweise eine Erheblichkeitsschwelle. Es soll eine Bagatellgrenze für immaterielle Schäden bestehen. Grund ist, dass solche Schäden nicht grenzenlos zugesprochen werden sollen, da eine genaue Höhe des Schadens immer nur subjektiv vom jeweiligen Gericht ermittelt werden könne. Dieser Argumentationslinie hat das BVerfG jedoch einen Riegel vorgeschoben, da dies von der Rechtsprechung des EuGH weder erschöpfend geklärt, noch unmittelbar aus der DSGVO beantwortet werden könne.[5]

Außerdem müsse von der Klägerin nachgewiesen werden, dass der Schaden aufgrund einer rechtswidrigen Verarbeitung eingetreten ist. Dies wird aus dem Wortlaut des Art. 82 II DSGVO entnommen. Dementsprechend führe gerade ein Verstoß gegen die DSGVO, welcher nicht in Verbindung mit der Verarbeitung steht, nicht zu einer Haftung. Damit soll auch einem Missbrauchsrisiko unter anderem durch Legal-Tech-Anbieterinnen entgegengewirkt werden. Dem kann entgegengehalten werden, dass der Absatz 1 des Art. 82 DSGVO die Anspruchsgrundlage ist. Dieser spricht dabei nur von einem „Verstoß gegen die DSGVO." Dieser beschränkt den Anspruch also nicht nur auf die Verarbeitung.

Insgesamt besteht die Tendenz, dass eher die Zivilgerichte eine restriktive Auslegung an den Tag legen, im Gegensatz zu den Arbeitsgerichten, welche etwa im Rahmen des AGG nach § 15 II AGG – auch aus Abschreckungsgründen – höhere immaterielle Schäden zusprechen.

2. Weite Auslegung

Vertreterinnen des 'weiten' Schadensbegriffs berufen sich unter anderem auf Art. 83 III DSGVO und Erwägungsgrund 146 S. 3 der DSGVO, der auch eine Abschreckungsfunktion des Schadensersatzanspruchs beinhalte. Erwägungsgrund 146 S. 3 besagt, dass „***der Begriff des Schadens [...] weit auf eine Art und Weise ausgelegt werden [sollte], die den Zielen dieser Verordnung in vollem Umfang entspricht***". Daraus ist jedoch nicht - anders als teilweise angenommen - direkt das Ziel eines Abschreckungspotenzials des Schadensbegriffes abzulesen. Auch kann dies nicht aus systematischen Überlegungen abgeleitet werden. Im Wortlaut des Art. 83 I DSGVO wird für die Verhängung von Geldbußen durch Behörden explizit gefordert, dass diese „abschreckend" sein sollen. Die europäische Gesetzgeberin hätte dies in Art. 82 DSGVO aufnehmen müssen, wenn sie eine vergleichbare Bemessungsregel angestrebt hätte.

II. Weitere Aspekte

Im Hinblick auf Legal-Tech-Anbieterinnen kann überlegt werden, ob ein (zu) 'weit' zugesprochener Schadensersatz dazu führen würde, dass Verantwortliche oder Auftragnehmerinnen in Gefahr laufen, hohe Verluste zu erleiden. Dazu gehören, auf der einen Seite, die massenhaften Zahlungen an Betroffene (durch die massenhaft eingereichten Klagen) bei einer Niederlage vor Gericht. Auf der anderen Seite kommt ein enormer Reputationsverlust schon bei Bekanntwerden eines potenziellen Verstoßes in Betracht, welcher bei einer Verurteilung nochmals steigen würde. Darüber hinaus wird darüber gestritten, ob immaterielle Schadensersatzansprüche gem. Art. 82 I DSGVO überhaupt abtretungsfähig i.S.d. §§ 398 ff. BGB sind. Dieser sei aufgrund des höchstpersönlichen Charakters des Anspruchs nicht übertragbar.

5 *BVerfG* NJW 2021, 1005 m.w.N.

D. Fazit

Ein Schadensersatzanspruch in Bezug auf Datenschutzverstöße und insbesondere auch auf immaterielle Schäden ist längst überfällig. Dieser stellt eine wichtige Stärkung des Rechts auf Schutz personenbezogener Daten dar. In Bezug auf die Frage, wann dieser Anspruch erteilt werden sollte, ist aber genauestens darauf zu achten, wie hoch der Ersatz ausfallen sollte. Aufgrund der vergangenen Rechtsprechung des EuGH ist davon auszugehen, dass entsprechende Entscheidungen eher zugunsten des weiten Schadensersatzbegriffs ausfallen werden.

Insoweit ist zu hoffen, dass die Richterinnen eine Entscheidung treffen, die den Interessen der Betroffenen und denen der Verantwortlichen ausgewogen gerecht wird. Zu hohe Anforderungen an das Bestehen eines ersatzfähigen immateriellen Schadens könnten die DSGVO nach anfänglichem Schrecken zum zahnlosen Tiger verkommen lassen. Gleichzeitig besteht durch die Angebote der Legal-Tech-Anbieterinnen die Gefahr einer ausufernden Geltendmachung von Schadensersatzansprüchen, die für die betroffenen Unternehmen erhebliche Haftungsrisiken bergen. Deshalb müssen Unternehmen verstärkt in ihre Cybersicherheit, Compliance und Datenschutzorganisation investieren, um solche Vorfälle zu vermeiden. Es kommt somit auch zu einer immer stärkeren Verzahnung von Cybersicherheit und Datenschutz.

Weiterführende Hinweise:

Überblicksartig ***Wybitul/Leibold***, ZD 2022, 207.

Zur Rechtsprechungspraxis ***Paal/Aliprandi***, ZD 2021, 241.

Letztlich für ein weites Verständnis ***Buchner/Wessels***, ZD 2022, 251.

In Bezug auf die europarechtskonforme Auslegung ***Korch***, NJW 2021, 978.

Ausführungen zu Art. 82 DSGVO im europäischen System ***Hellgardt***, ZEuP 2022, 7.

Gegen die Abtretbarkeit von immateriellen Schäden ***Spittka***, GRUR-Prax 2019, 475.

Talking Legal Tech – Folge 1

„Was ist Legal Tech? mit Nico Kuhlmann“

Talking Legal Tech – Folge 43

„Rightmart, Flightright, Geblitzt.de & Co - Der Stand im B2C-Rechtsmarkt mit Marco Klock von Rightmart”

Talking Legal Tech – Folge 60

„UiPath - Ein Bot für alle Jurist:innen durch Robotic Process Automation (RPA), Joachim Grouven?”

Kolumne

Datenverarbeitung beim autonomen Fahren – Schafft die StVG-Novelle 2021 Rechtssicherheit bei der Datenverarbeitung?

Hans Steege

Open Peer Review

Dieser Beitrag wurde lektoriert von: Hendrik Scheja, David Wasilewski und Büsra Bayzat

Dr. Hans Steege arbeitet im Bereich Data Protection und hat einen Lehrauftrag an der Universität Stuttgart. Er ist Mitherausgeber der Zeitschrift für das Recht der digitalen Wirtschaft (ZdiW), der Zeitschrift Straßenverkehrsrecht (SVR) sowie des Handbuchs KI (Nomos).

A. Einleitung

Zunehmende Automatisierung und Vernetzung von Kraftfahrzeugen führen dazu, dass immer mehr Fahraufgaben, die klassischerweise vom Fahrer[1] bewältigt werden mussten, von automatisierten Fahrfunktionen übernommen werden. Diese Automatisierung wird international in fünf Stufen eingeteilt.[2] Aber auch auf nationaler Ebene existiert eine Klassifizierung.[3]

1 Zum Zwecke der besseren Lesbarkeit wird bei personenbezogenen Substantiven die männliche Form verwendet. Diese Begriffe sollen für alle Geschlechter gelten. Der Autor gibt in dem Beitrag ausschließlich seine persönliche Rechtsauffassung wieder.
2 *Steege*, SVR 2021, 128 (129).
3 *Steege*, PHi 2021, 210 (211 f.).

Diese technischen Einstufungen verdeutlichen zum einen, welche Fahraufgaben von der Fahrfunktion bzw. vom Fahrer ausgeführt werden müssen, und zum anderen, welche Pflichten den Fahrer treffen.

Übernimmt jedoch nicht mehr der Mensch die Fahrzeugsteuerung, sondern die automatisierte Fahrfunktion, so rücken Informationen aus der Fahrzeugumgebung in den Fokus. Die Fahrzeuge müssen hierzu ihre Umgebung wahrnehmen, Verkehrsteilnehmer, Straßen und Objekte erkennen und daraus Rückschlüsse hinsichtlich ihres Verhaltens ziehen. Dieser Vorgang wird als Perzeption (***Wahrnehmung***), Kognition (***Verarbeitung***) und Prädiktion (***Vorhersage***) bezeichnet.[4] Hierfür benötigen Fahrzeuge zahlreiche Sensoren. Zum Einsatz kommen insbesondere Kameras, Lidar, Radar, Ultraschallsensoren, Odometer sowie GPS.[5] Werden mittels dieser Sensoren Fahrradfahrer, Passanten oder Kraftfahrzeuge erfasst, so handelt es sich dabei leichthin um personenbezogene Daten i.S.d. Art. 4 Nr. 1 DSGVO. Aufgrund der Weite der Definition reicht es aus, dass eine natürliche Person (indirekt) identifizierbar ist.

Aber auch im Innenraum von Kraftfahrzeugen selbst entstehen zahlreiche Daten. Diese können etwa die Öltemperatur oder den Ladezustand der Batterie betreffen. Bei fahrerlosen, autonomen People-Movern i.S.d. § 1d StVG kann eine Innenraumüberwachung zum Schutz von Insassen erkennen, ob etwa Sicherheitsgurte angelegt sind. Daten können zudem durch die Nutzung mobiler Online-Dienste entstehen oder durch das Buchen einer Fahrt mittels App.[6]

Informationen entstehen nahezu überall im Kraftfahrzeug und damit verbunden ist die Frage, ob es sich um personenbezogene Daten i.S.d. Art. 4 Nr. 1 DSGVO handelt, sodass die Datenschutz-Grundverordnung Anwendung findet (Art. 2 Abs. 1 DSGVO).

> „Informationen entstehen nahezu überall im Kraftfahrzeug."

Ist sie anwendbar, so treffen den Verantwortlichen[7] im datenschutzrechtlichen Sinne zahlreiche Transparenz- und Informationspflichten (Art. 12-14 DSGVO). Zuerst muss eine Datenverarbeitung jedoch überhaupt rechtmäßig sein. Art. 6 Abs. 1 DSGVO nennt Bedingungen, damit die Rechtmäßigkeit der Datenverarbeitung gegeben ist.

Während es einfach ist, eine Einwilligung der Insassen eines autonomen Shuttles zur Datenverarbeitung einzuholen, so ist die Rechtsgrundlage bei der Erfassung der Fahrzeugumgebung problematisch, da von anderen Verkehrsteilnehmern regelmäßig keine Einwilligung eingeholt werden kann.[8] Des Weiteren stellt die Einhaltung der Transparenz- und Informationspflichten ebenfalls eine Herausforderung dar. Im Jahr 2021 hat der Gesetzgeber mit den §§ 1d ff. StVG das autonome Fahren in festgelegten Betriebsbereichen reguliert.[9] Mit Blick auf die datenschutzrechtlichen Herausforderungen ist es daher bedeutsam, ob durch den neuen Rechtsrahmen die bestehende Rechtsunsicherheit hinsichtlich der Rechtsgrundlage sowie der Transparenz- und Informationspflichten beseitigt wurde.

B. Regelungsgehalt des § 1g StVG

Da § 63a StVG ausschließlich für die Datenverarbeitung beim hoch- und vollautomatisierten Fahren i.S.d. § 1a StVG anwendbar ist,[10] führte der Gesetzgeber § 1g StVG für das autonome Fahren i.S.d. § 1d StVG ein. § 1g StVG regelt die Datenverarbeitung beim autonomen Fahren und verpflichtet den Halter, die in Abs. 1 Nr. 1-13 genannten Daten zu speichern.[11] Die zu speichernden Daten reichen von der Fahrzeugidentifikationsnummer über die Geschwindigkeit bis hin zu Positionsdaten.

4 *Beck*, in: Leupold/Wiebe/Glossner, MAH-IT-Recht, 4. Aufl. 2021, Teil 9.2 Rn. 23 ff.
5 *Steege*, MMR 2019, 509 (510); eingehend zur Technik autonomer Fahrzeuge *Leonhardt*, in: Chibanguza/Kuß/Steege, Künstliche Intelligenz, 2022, § 3 A.
6 Eingehend zum Personenbezug sowie zu möglichen Rechtsgrundlagen bei sog. Connected Cars *Wasilewski*, CTRL 1/2022, 43 (45).
7 Verantwortlicher ist nach Art. 4 Nr. 7 DSGVO die natürliche oder juristische Person, die allein oder gemeinsam über die Zwecke und Mittel der Datenverarbeitung entscheidet.
8 Siehe dazu *Steege*, MMR 2019, 509.
9 Ein guter Überblick zu der StVG-Novelle findet sich bei *Goral-Wood,* CTRL 1/2022, 2 ff.
10 NK-GVR/*Steege*, 3. Aufl. 2022, Anh. II zu §§ 1a-1c StVG, Rn. 44; *Stender-Vorwachs/Steege*, MMR 2018, 212 (216).
11 *Haupt*, NZV 2021, 172 (175).

Obwohl der Gesetzestext eine Widersprüchlichkeit hinsichtlich der Datenspeicherung aufweist, ist von einer anlassbezogenen Datenspeicherung in den abschließend in § 1g Abs. 2 StVG genannten Verkehrsszenarien auszugehen.[12] Dafür sprechen sowohl Sinn und Zweck des Gesetzes als auch die Autonome-Fahrzeuge-Genehmigungs- und -Betriebs-Verordnung (AFGBV) als ergänzende und konkretisierende Verordnung.[13]

Die Verpflichtung aus § 1g Abs. 1 StVG betrifft unmittelbar den Halter. Ist er Verantwortlicher im datenschutzrechtlichen Sinne und handelt es sich bei den in Nr. 1-13 genannten Daten um personenbezogene, so ist die Datenverarbeitung rechtmäßig. Denn für die Erfüllung einer rechtlichen Verpflichtung, welcher der Verantwortliche unterliegt, erkennt die DSGVO die Rechtmäßigkeit der Datenverarbeitung an (Art. 6 Abs. 1 lit. c DSGVO).

Diese Daten betreffen allerdings nicht die Fahrzeugumgebung und stellen auch keinen unmittelbaren Personenbezug zu den (einzelnen) Insassen her. Auch wenn etwa mit Blick auf die Positionsdaten ein Personenbezug angenommen wird, so kann der Verantwortliche ohne Weiteres seinen Transparenz- und Informationspflichten nachkommen, indem er in seiner App vor der Buchung der Fahrt über die Datenverarbeitung informiert.

Doch wie verhält es sich mit den Daten der Fahrzeugumgebung? Hier bestehen auch nach der StVG-Novelle 2021 nach wie vor große Hürden.[14] Einerseits stellt sich die Frage der Rechtsgrundlage und damit der Rechtmäßigkeit der Datenverarbeitung, andererseits stellt sich je nach Ausgestaltung von Speicherort, Datenzugriff sowie Datenverarbeitung die Frage der Verantwortlichkeit.

Schlussendlich ist die Einhaltung von Transparenz- und Informationspflichten gegenüber Betroffenen außerhalb des Fahrzeugs de facto eine hohe Hürde.

12 *Steege*, PHi 2022, 18 (25); *Seyda,* ZD-aktuell 2021, 0536.
13 *Steege,* SVR 2022, 161 (167); allg. zur AFGBV s.a. *Haupt,* NZV 2022, 166 ff.
14 Zur bisherigen Problematik *Steege,* MMR 2019, 509 ff.; *Bleckat,* ZdiW 2021, 40 (43).

„Bei Daten der Fahrzeugumgebung bestehen auch nach der StVG-Novelle 2021 nach wie vor große Hürden."

C. Ergebnis

Es bleibt datenschutzrechtlich bedauerlicherweise bei der Ausgangslage, die vor Inkrafttreten der StVG-Novelle 2021 bestand, weil ausschließlich die in § 1g Abs. 1 Nr. 1-13 StVG genannten Daten eine rechtliche Verpflichtung i.S.d der Datenschutz-Grundverordnung darstellen und der Katalog weitestgehend nicht Daten aus der Fahrzeugumgebung umfasst.

Hinsichtlich der Transparenz- und Informationspflichten stellt sich im Regelbetrieb die Frage, wie Halter ihren Pflichten nachkommen können. Fahrzeuge benötigen mindestens ein Labeling, das sie als Kamerafahrzeug kenntlich macht, und darüber hinaus auf eine Webseite hinweist, welche die nach der Datenschutz-Grundverordnung erforderlichen Informationen enthält. Die zu erbringenden Informationen richten sich insbesondere danach, wie die Datenverarbeitung ausgestaltet ist. Dies betrifft u.a. Speicherort sowie Datenzugriff und damit auch die (gemeinsame) Verantwortlichkeit. Je nach Umfang der Datenverarbeitung kann ein solches Labeling nebst Hinweis auf eine Homepage allerdings unzureichend sein.

Neben der Erfüllung der Informationspflichten als faktische Hürde rückt jedoch auch die Rechtsgrundlage für die Datenverarbeitung in den Vordergrund. Da sowohl Einwilligung als auch Vertragserfüllung hinsichtlich der Datenverarbeitung der Fahrzeugumgebung ausscheiden, bleibt lediglich das berechtigte Interesse des Verantwortlichen.

Neben der somit bestehenden Rechtsunsicherheit rückt abermals die Frage der Ausgestaltung der Datenverarbeitung in den Mittelpunkt. Auf die Nichtanwendbarkeit der Datenschutz-Grundverordnung kann bei gewerblicher Nutzung der Fahrzeuge nicht gehofft werden, da Art. 2 Abs. 2 lit. c DSGVO lediglich die Datenverarbeitung durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten von der Datenschutz-Grundverordnung ausnimmt.

Für den Regelbetrieb autonomer Fahrzeuge schafft die StVG-Novelle 2021 durch den neu eingefügten § 1g StVG hinsichtlich der Datenverarbeitung nur teilweise Rechtssicherheit.

Obwohl die Datenschutz-Grundverordnung unter dem Motto „***one size fits all***" stand,[15] zeigen sich erhebliche rechtliche Risiken beim Regelbetrieb autonomer Fahrzeuge. Da die Ausgestaltung der Datenverarbeitung sowohl für die Rechtsgrundlage als auch für die daraus folgenden Transparenz- und Informationspflichten sowie weiteren Pflichten der Dreh- und Angelpunkt ist, kommt der Entwicklung autonomer Kraftfahrzeuge sowie der Beachtung der Prinzipien ***Privacy by Design*** und ***Privacy by Default*** gem. Art. 25 DSGVO hohe Relevanz zu.

15 *Steege,* MMR 2019, 509 (513).

Aufsatz

Freie Fahrt im Datenverkehr? – Der Data Act und der Data Governance Act

Hendrik Eppelmann

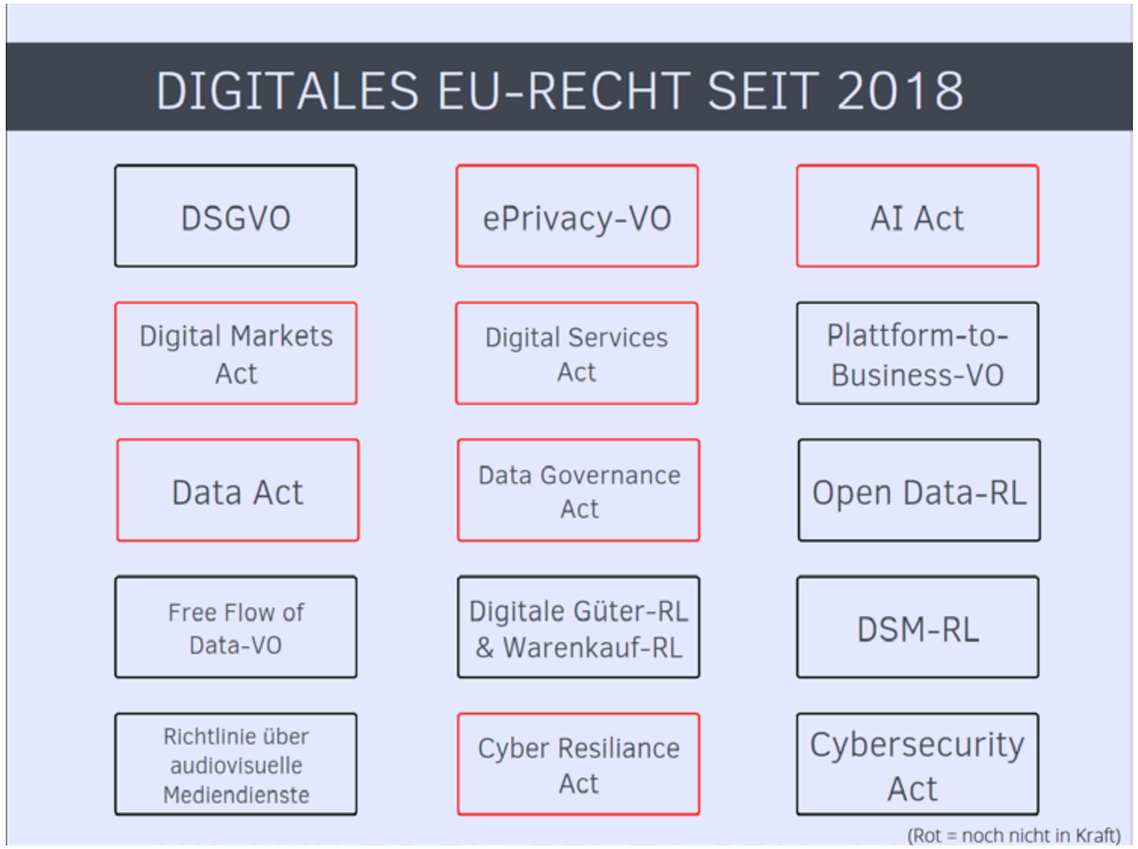
Open Peer Review

Dieser Beitrag wurde lektoriert von: Hanna Brinkmann und Daniel Dischinger

Hendrik promoviert an der Universität zu Köln zur kartellrechtlichen Beurteilung des Datenaustauschs über digitale B2B-Plattformen. Zudem ist er wissenschaftlicher Mitarbeiter in den Bereichen Kartell- und Datenschutzrecht bei Loschelder Rechtsanwälte.

Am 19.02.2020 veröffentlichte die EU-Kommission ihre „europäische Datenstrategie" und steckte damit den datenpolitischen Pfad der nächsten Jahre ab. Ambitioniertes Ziel der Kommission ist dabei nichts geringeres als die „Schaffung eines einheitlichen europäischen Datenraums, eines echten Binnenmarkts für Daten […] in dem sowohl personenbezogene als auch nicht-personenbezogene Daten […] sicher sind und in dem Unternehmen auch leicht Zugang zu einer nahezu unbegrenzten Menge hochwertiger industrieller Daten erhalten."[1] Bereits in den Jahren zuvor hat die EU einen legislativen Schwerpunkt auf die Digitalisierung und Datenwirtschaft gelegt. Zur Ausgestaltung der Datenstrategie sollen in den kommenden Jahren diverse weitere Rechtsakte folgen.

1 Kommission, COM(2020) 66 final, 5, hier abrufbar (Stand: 31.05.2022).



Ausgewählte Rechtsakte der EU zu Digital-Themen seit 2018

Auf den Umgang mit und den Fluss von Daten konzentrieren sich auch zwei aktuelle Verordnungsentwürfe: der Entwurf für den Data Governance Act[2] (DGA-E) und der Entwurf für den Data Act[3] (Data Act-E). Während der Data Act-E zurzeit noch rege diskutiert wird und vermutlich nicht vor Ende 2024 in Kraft tritt,[4] wurde der DGA-E bereits vom europäischen Parlament angenommen.[5]

2 Der offizielle deutsche Kurzname des Verordnungsentwurfs lautet "Daten-Governance-Gesetz". Bislang ist aber auch im deutschsprachigen Raum die Bezeichnung „Data Governance Act" gebräuchlicher; der letzte Entwurf ist hier abrufbar (Stand: 31.05.2022).
3 Der offizielle deutsche Kurzname des Verordnungsentwurfs lautet „Datengesetz". Bislang ist aber auch im deutschsprachigen Raum die Bezeichnung „Data Act" gebräuchlicher; der erste Entwurf ist hier abrufbar (Stand: 31.05.2022).
4 *Gerpott*, CR 2022, 271 (280), Rn. 48.
5 Europäisches Parlament, Presseerklärung vom 06.04.2022, hier abrufbar (Stand: 31.05.2022).

Doch wird die EU ihr ehrgeiziges Ziel eines Daten-Binnenmarktes mithilfe dieser Verordnungen erreichen? Geben diese Vorhaben tatsächlich grünes Licht für eine freie Fahrt im Datenverkehr oder schickt die EU die Datenwirtschaft auf eine Route voller Kurven und Baustellen? Der folgende Beitrag möchte sich diesen Fragen kritisch nähern, indem er die wesentlichen Normen der Verordnungsentwürfe zum Austausch von Daten erklärt und beleuchtet.

A. Daten im Internet of Things

Zunächst trifft der Data Act-E wesentliche Regelungen zu Daten, die im Internet of Things (‚IoT') – also dem System über das Internet vernetzter Gegenstände[6] – anfallen.

I. Zugang zu IoT Daten

Herzstück des Data Act-E ist der Zugang zu Daten aus dem IoT. Zukünftig sollen die Nutzer[7] von Produkten und verbundenen Diensten (digitale Dienste, die funktionsnotwendig in das Produkt integriert sind, Art. 2 Nr. 3 Data Act-E) einen Zugangsanspruch zu den bei der Nutzung entstandenen Daten haben. Art. 20 DSGVO sieht einen ähnlichen Anspruch bereits für personenbezogene Daten vor. Anders als dieser soll der Data Act-E aber für alle Arten von Daten, unabhängig von einem etwaigen Personenbezug, gelten. Entscheidend ist nur, dass die jeweiligen Daten durch die Nutzung eines Produktes oder eines verbundenen Dienstes erzeugt wurden.Ein solches ‚Produkt' im Sinne des Data Act-E ist ein körperlicher beweglicher Gegenstand, der Daten über seine Nutzung oder Umgebung erlangt, erzeugt oder sammelt und Daten elektronisch übermitteln kann und dessen Hauptfunktion nicht die Speicherung und Verarbeitung von Daten ist.[8] Gemeint sind letztlich alle Produkte,

6 Zum Begriff des „IoT" ausführlich: *Ye*, CTRL 1/21, 11.
7 Zum Zwecke der besseren Lesbarkeit wird bei personenbezogenen Hauptwörtern nur die männliche Form verwendet. Diese Begriffe sollen für alle Geschlechter gelten.
8 Art. 2 Nr. 2 Data Act-E.

die Teil des IoT sind, etwa Fahrzeuge, Haushaltsgeräte oder industrielle Maschinen.[9] Nicht erfasst sein sollen solche Geräte, die in erster Linie dazu dienen, Inhalte anzuzeigen, abzuspielen, aufzuzeichnen oder zu übertragen; etwa PCs, Server, Tablets, Smartphones, Kameras und Scanner. Solche Geräte erzeugen nicht nur Daten über das Nutzerverhalten, sondern erfordern einen menschlichen Beitrag zur Erstellung von Inhalten.[10] Der Data Act zielt also nur auf maschinengenerierte Daten ab, die durch die Nutzung von vernetzten Gegenständen anfallen. Interessanterweise (und schwer nachvollziehbar)[11] ausgenommen sind rein digitale Produkte wie Software.

Art. 3 I Data Act-E verpflichtet die Anbieter von IoT-Produkten dazu, die Produkte von vornherein so zu konzipieren, dass die Nutzer standardmäßig einfach, sicher und – soweit relevant und angemessen – direkt auf die bei der Nutzung erzeugten Daten zugreifen können. Man spricht hier auch von der Pflicht zum access by design.[12] Der Data Act-E verpflichtet Hersteller also zukünftig dazu, sämtliche ihrer Produkte nur noch mit entsprechenden Zugangs-Features ausgestattet zu vertreiben.

Auch, wenn der Nutzer nicht direkt mittels access by design auf die erzeugten Daten zugreifen kann, hat er einen Anspruch auf Zurverfügungstellung der Daten an sich oder Dritte. Dies muss unverzüglich, kostenlos und gegebenenfalls kontinuierlich und in Echtzeit erfolgen, soweit dies technisch machbar ist (vgl. Art. 4, 5 Data Act-E). Sind Geschäftsgeheimnisse enthalten, müssen alle erforderlichen Schutzmaßnahmen eingehalten werden (Art. 4 III Data Act-E). Erlangte Daten dürfen nicht dazu genutzt werden, Konkurrenzprodukte zu entwickeln (Art. 4 IV Data-Act).

Das Vorhaben, Datenbestände aus dem IoT für die Nutzer zu öffnen, ist zu begrüßen. Hiermit wird das Ziel einer breiten Datenverfügbarkeit aktiv gefördert. Praktisch und wirtschaftlich relevant wird dies vermutlich weniger für den einzelnen Endverbraucher, als insbesondere für Unternehmen, die bisher nicht auf alle Daten zugreifen konnten, die etwa ihre Produktionsmaschinen generiert haben.

9 Erwägungsgrund 14 Data Act-E.
10 Erwägungsgrund 15 Data Act-E.
11 *Gerpott*, CR 2022, 271 (274), Rn. 12; *Hilgendorf/Vogel*, JZ 8/2022, 380 (388).
12 Bspw.: *Klink-Straub/Straub*, ZD-Aktuell 2022, 01076; *Bomhard/Merkle*, RDi 2022, 168 (173), Rn. 39.

Herzstück des Data Act-E ist der Zugang zu Daten aus dem IoT

II. Datenlizenz

Hoch brisant und trotzdem geradezu versteckt ist Art. 4 VI Data Act-E: Hiernach darf ein Dateninhaber nicht-personenbezogene Daten, die bei der Nutzung eines IoT-Produktes oder verbundenen Dienstes erzeugt werden, nur dann nutzen, wenn er mit dem Nutzer eine entsprechende vertragliche Vereinbarung über die Nutzung geschlossen hat. Was im Datenschutzrecht als selbstverständlich erscheint, war bisher für nicht-personenbezogene Daten nicht geregelt. Zumindest in der Theorie werden damit dem Produkthersteller Steine in den Weg gelegt, wenn er die bei der Produktnutzung erzeugten Daten verarbeiten möchte. Rein praktisch gesehen dürfte sich (zumindest bei der Produktnutzung durch Endkunden) aber nicht allzu viel ändern, da diese erfahrungsgemäß bereit sind, allen möglichen Pop-up Fenstern oder ähnliches zuzustimmen, die sie von der Nutzung des Produkts abhalten.[13]

13 Vgl. *Kerber*, Governance of IoT Data: Why the EU Data Act will not fulfill its objectives, 21, hier abrufbar (Stand: 31.05.2022).

Führt man sich vor Augen, dass es eigentlich das Ziel des Data Act-E ist, die breite Nutzung von Daten zu fördern, stellt sich die Frage, ob es wirklich förderlich ist, die Nutzung nicht-personenbezogener Daten, die im IoT erzeugt werden, von einer vertraglichen Vereinbarung abhängig zu machen. Hier geht es gerade nicht um personenbezogene Daten, die grundrechtlichen Schutz genießen, sondern um nicht-personenbezogene Daten, die für die Verbesserung von Produkten und für neue Innovation genutzt werden sollen, wie etwa die Daten über Leistungsfähigkeit und Produktivität von Maschinen. Den freien Fluss solcher Daten soll der Data Act eigentlich vereinfachen.

B. Datenaustausch zwischen Unternehmen und Behörden

Im Data Act-E und DGA-E regelt die EU auch neue Fälle für den Austausch von Daten zwischen Unternehmen und öffentlichen Stellen.

I. Bereitstellung an öffentliche Stellen bei außergewöhnlicher Notwendigkeit

Zunächst definiert der Data Act-E neue Situationen, in denen Unternehmen staatlichen Behörden Daten übermitteln müssen. Man spricht dann von business to government (‚B2G').

Konkret geht es darum, dass eine öffentliche Stelle aufgrund einer „außergewöhnlichen Notwendigkeit" die Bereitstellung von Daten verlangen kann (Art. 14 I Data Act-E). Die Notwendigkeit der Datennutzung muss die öffentliche Stelle selbst nachweisen. Auch Forschungseinrichtungen wie Universitäten können solche öffentlichen Stellen sein.[14] Art. 15 Data Act-E zählt abschließend Fälle einer außergewöhnlichen Notwendigkeit auf.

Hauptfall einer solchen Notwendigkeit ist die Verhinderung und Bewältigung eines öffentlichen Notstand oder Erholung von einem solchen. Dieser ist in Art. 2 Nr. 10 Data Act-E definiert als eine außergewöhnliche Situation, die das Risiko schwerwiegender und dauerhafter Folgen für die Lebensbedingungen, die wirtschaftliche Stabilität oder wirtschaftliche Vermögenswerte in der Union birgt und sich negativ auf die Bevölkerung auswirkt. Beispiele hierfür sind Pandemien,[15] Naturkatastrophen und Umweltschäden oder große Cyberangriffe.[16] Erwägungsgrund 57 des Data Act-E legt nahe, dass es letztlich auf eine Interessenabwägung ankommen soll; auch wenn der Verordnungstext selbst dies nicht ausdrücklich hergibt.

Eine „außergewöhnliche Notwendigkeit" kann aber auch darin liegen, dass eine öffentliche Stelle aufgrund des Fehlens verfügbarer Daten eine bestimmte, gesetzlich ausdrücklich vorgesehene Aufgabe im öffentlichen Interesse nicht erfüllen kann und sich die öffentliche Stelle die Daten nicht anderweitig zeitnah besorgen oder kaufen kann bzw. dass der Verwaltungsaufwand der Dateninhaber oder anderer Unternehmen erheblich verringert werden würde.

Die öffentliche Stelle ist dann sogar dazu ermächtigt, die erlangten Daten mit anderen öffentlichen Stellen oder mit öffentlichen Aufgaben betrauten Dritten zu teilen (Art. 17 IV Data Act-E). Sie muss dies lediglich dem ursprünglichen Dateninhaber mitteilen. Freilich dürfen alle Beteiligten die erlangten Daten aber nur für die Zwecke der „außergewöhnlichen Notwendigkeit" verwenden und müssen sie vernichten, sobald sie nicht mehr für diesen Zweck erforderlich sind (Art. 19 I Data Act-E).

Wenn dies für den Zweck des Verlangens unerlässlich ist, darf die öffentliche Stelle sogar die Offenlegung von Geschäftsgeheimnissen fordern. Die Behörde muss dann aber geeignete Maßnahmen treffen, um die Vertraulichkeit dieser Informationen zu wahren (Art. 19 II Data Act-E). In diesem Bereich wird deutlich, was für ein Streitpotential den B2G-Pflichten des Data Act-E innewohnt.

14 Erwägungsgrund 56 Data Act-E.

15 Beispielhaft über die Nutzung von Daten zur Bewältigung der Corona-Pandemie: *Handelsblatt*, Wie Regierungen versuchen, das Virus mit Big Data zu bändigen, hier abrufbar (Stand: 31.05.2022).

16 Erwägungsgrund 57 Data Act-E.

ZITAT: Wenn dies für den Zweck des Verlangens unerlässlich ist, darf die öffentliche Stelle sogar die Offenlegung von Geschäftsgeheimnissen fordern

An diesen Regeln ist unter anderem durch den Europäischen Datenschutzausschuss (EDPB) und den Europäischen Datenschutzbeauftragten (EDPS) kritisiert worden, dass weder die Situationen einer „außergewöhnlichen Notwendigkeit" ausreichend präzise definiert ist, noch die genauen Kategorien von Daten spezifiziert worden sind.[17] Hier hat die Kommission noch Nachbesserungsbedarf, um dem Datenschutzbedürfnis der Bürger gerecht zu werden.

II. Weiterverwendung von Daten im Besitz öffentlicher Stellen

Der DGA-E wiederum kümmert sich um den Datenfluss in die andere Richtung, also von der Behörde zum Unternehmen (‚G2B'). Der Staat verfügt über eine Vielzahl hochwertiger Daten, die für Unternehmen von Interesse sein könnten. Beispiele hierfür sind Daten zum Straßenverkehr, Bevölkerungsstatistiken, Katasterdaten oder Daten über die Landwirtschaft.[18] Der DGA-E regelt die Weiterverwendung von Daten im Besitz öffentlicher Stellen durch Dritte.

„Wenn dies für den Zweck des Verlangens unerlässlich ist, darf die öffentliche Stelle sogar die Offenlegung von Geschäftsgeheimnissen fordern."

Bereits 2019 hat die EU eine Richtlinie über die Weiterverwendung von Daten des öffentlichen Sektors erlassen (‚Open Data RL', RL 2019/1024). Auch diese regelt Modalitäten zur Erleichterung der Weiterverwendung. Jedoch enthält sie keine Regelungen zu dem geistigen Eigentum Dritter, statistischen Geheimnissen oder Geschäftsgeheimnissen (vgl. Art. 1 II RL 2019/1024). Die zu solchen Daten offengebliebenen Fragen möchte der DGA-E beantworten.[19]

Der DGA-E hat das Ziel, zu ermöglichen, dass öffentliche Stellen entsprechend geschützte Daten zur Weiterverwendung durch Unternehmen bereitstellen können. Ausgenommen sind wiederum Daten öffentlicher Unternehmen, Daten von öffentlich-rechtlichen Rundfunkanstalten, die sich auf deren Sendeauftrag beziehen, Daten von Kultur- und Bildungseinrichtungen sowie Daten, die aus Gründen der nationalen Sicherheit geschützt sind (Art. 3 II DGA-E).

Es ist jedoch wichtig, sich stets vor Augen zu führen, was genau der DGA-E hier erreichen möchte: Es geht nicht darum, dass ein Anspruch auf Bereitstellung von Daten zur Weiterverwendung geschaffen wird.[20] Vielmehr geht es um die Schaffung von Rahmenbedingungen, unter denen auch ansonsten geschützte Daten zur Weiterverwendung bereitgestellt werden können.

Doch was heißt ‚Weiterverwendung' überhaupt? Nach Art. 2 Nr. 2 DGA-E ist hiermit jede Nutzung von Daten, die im Besitz öffentlicher Stellen sind, durch Dritte gemeint, soweit damit kommerzielle oder nichtkommerzielle Zwecke verfolgt werden, die sich vom ursprünglichen Zweck des öffentlichen Auftrags bei der Erstellung der Daten unterscheiden. Es geht also darum, dass Daten, die mittels öffentlicher Gelder erhoben wurden, in einem breiten Rahmen der Gesellschaft zugutekommen sollen.[21]

Aus Gründen der Chancengleichheit ist es den Behörden grundsätzlich verboten, die Daten nur einzelnen Unternehmen zur ausschließlichen Verwendung zur Verfügung zu stellen (Art. 4 I DGA-E). Die öffentliche Stelle kann festlegen, dass sie nur Daten herausgibt, die sie zuvor anonymisiert hat bzw. solche, bei denen Geschäftsgeheimnisse unkenntlich gemacht wurden (Art. 5 III lit. a) DGA-E). Alternativ kann sie auch dafür sorgen, dass der Datenzugang nur in kontrollierten sicheren Ver-

17 EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), Rn. 78 ff., hier abrufbar (Stand: 31.05.2022).
18 *Czychowski*, FS Taeger, 2020, 129 (130).
19 Vgl. Art. 3 Abs. 1 a.E. DGA-E; Erwägungsgrund 10 DGA-E; *Spindler*, CR 2021, 98 (100), Rn. 6; *Richter*, ZD 2022, 3 (4).
20 Erwägungsgrund 11 DGA-E.
21 Erwägungsgrund 6 DGA-E.

arbeitungsumgebungen stattfindet; entweder per Fernzugriff oder sogar nur innerhalb der physischen Räumlichkeiten (Art. 5 III lit. b), c) DGA-E). Darüber hinaus muss die öffentliche Stelle die Möglichkeit haben, die Verfahren, Mittel und Ergebnisse der Datenverarbeitung zu überprüfen, um die Verwendung dieser untersagen zu können, falls Rechte und Interessen Dritter gefährdet wären (Art. 5 IV DGA-E).

Die Erlaubnis zur Weiterverwendung der Daten müssen die Behörden aber auch nicht kostenlos gewähren. Vielmehr dürfen sie transparente, nichtdiskriminierende, verhältnismäßige und objektiv gerechtfertigte Gebühren erheben, deren Höhe sich aus den Kosten für die Bereitstellung ableiten (Art. 6 I, II, V DGA-E). Gleichzeitig sollen die Behörden hierbei aber kleinen und mittleren Unternehmen entgegenkommen, um Anreize für eine nichtkommerzielle Nutzung durch diese zu fördern (Art. 6 IV DGA-E).

Dass die neuen Regeln zur Weiterverarbeitung großen praktischen Wert haben werden, darf bezweifelt werden. Letztlich legt man den Behörden Pflichten auf (wie etwa die Löschung von Geschäftsgeheimnissen oder die Anonymisierung personenbezogener Daten) ohne sie gleichzeitig dazu zu verpflichten, auch tatsächlich aktiv zu werden und eine Weiterverwendung zu ermöglichen. Ob damit die Ziele der Verordnung erreicht werden, erscheint fraglich.[22]

C. Dienste für gemeinsame Datennutzung

Damit es zu einem regen Datenverkehr kommen kann, muss es auch eine funktionierende Infrastruktur dafür geben. Diese könnte unter anderem auf Diensten für gemeinsame Datennutzung im Sinne des Art. 10 DGA-E basieren. Darunter versteht der DGA-E vor allem Dienste, die einen Datenfluss zwischen Dateninhabern und möglichen Datennutzern vermitteln und technisch ermöglichen. Diese Angebote sollen sich an eine unbestimmte Anzahl von Nutzern richten.[23] Hoch spezialisierte Dienste, die nur auf einzelne konkrete Unternehmen ausgerichtet sind, sind daher nicht vom DGA-E erfasst. Ausgenommen sind auch bloße Vermittler von Inhalten, wie etwa Streaming Plattformen.[24] Vom DGA-E sollen nur solche Dienste erfasst sein, bei denen es wirklich darum geht, Daten zu übertragen und nicht nur Inhalte anzuzeigen. Ein breites Angebot solcher Dienste könnte den europäischen Datenaustausch sicherlich stärken, wenn die potenziellen Nutzer ein ausreichendes Vertrauen in diese haben.

Um ein solches Vertrauen zu erzeugen und aufrecht zu erhalten, sieht der DGA-E ein Anmeldeverfahren für die Diensteanbieter vor. (Wohl) nur wer seinen Dienst angemeldet hat, darf diesen auch betreiben (vgl. Art. 11 IV DGA-E).[25] Ziel ist es, dass die Diensteanbieter stets nur als neutrale Mittler auftreten.[26] Zudem unterliegen diese Dienste einer Liste an Bedingungen aus Art. 12 DGA-E. So darf der Diensteanbieter etwa die Daten nicht zu anderen Zwecken als zur Vermittlung nutzen. Die Dienste für die gemeinsame Datennutzung müssen bei einer gesonderten Rechtsperson angesiedelt sein. Das Angebot und die Preise müssen stets fair, transparent und nichtdiskriminierend sein. Zudem muss der Anbieter unter anderem über Verfahren verfügen und Maßnahmen ergreifen, die betrügerische und missbräuchliche Praktiken der Nutzer verhindern, einen garantierten Datenzugang im Insolvenzfall gewährleisten und Datentransfers verhindern, die nach anderen Gesetzen rechtswidrig wären.

Der Anbieter wird hier also in die Pflicht genommen, seinen Dienst von vornherein so zu gestalten, dass es erst gar nicht zu unerwünschten Datentransfers kommen kann. Das dürfte im Einzelfall komplexe Rechtsfragen aufwerfen. Beispielsweise soll der Anbieter gewährleisten, dass auf seiner Plattform das Wettbewerbsrecht eingehalten wird.[27] Wo die Grenze zwischen einem kartellrechtswidrigen Informationsaustausch und dem politisch erwünschten data sharing verläuft, ist eine im Detail sehr komplexe und alles andere als triviale Frage. Insofern wird dem Anbieter

22 Kritisch auch *Spindler*, CR 2021, 98 (102), Rn. 18.
23 Erwägungsgrund 28 DGA-E.
24 Vgl. Erwägungsgrund 29 DGA-E.
25 Vgl. *Spindler*, CR 2021, 98 (103), Rn. 23; *Richter*, ZEuP 2021, 634 (647 f.).
26 Erwägungsgrund 33 DGA-E.
27 Vgl. Erwägungsgrund 60 DGA-E.

eines Vermittlungsdienstes hier in Ermangelung eines abschließend klaren Rechtsrahmens eine große Verantwortung auferlegt, die mit dem hohen Bußgeldrisiko des Kartellrechts verbunden ist.[28]

Insofern birgt der Katalog der Bedingungen in Art. 12 DGA-E die Gefahr, innovative Anbieter von Diensten für die gemeinsame Datennutzung abzuschrecken. Hier sollte die Kommission mehr Klarheit schaffen oder Risiken entschärfen, um Innovationspotenzial nicht von vornherein abzuwürgen.

D. Wechsel von Cloud-Diensten & Interoperabilität

Der Data Act-E trifft Regelungen, die es ermöglichen sollen, einfach zwischen digitalen Diensten zu wechseln oder diese parallel zu nutzen.

I. Wechsel von Cloud-Diensten

Um den europäischen Datenverkehr zu fördern und die Konzentration von Datenbeständen zu verhindern, versucht der Data Act-E, den Wechsel zwischen Datenverarbeitungsdiensten (gemeint sind vor allem Cloud-Dienste) zu erleichtern. Besonders bemerkenswert ist hierbei, dass es zukünftig eine Kündigungsfrist von höchstens 30 Tagen für Datenverarbeitungsdienste geben darf (Art. 23 I lit. a) Data Act-E). Bisher sind deutlich längere Kündigungsfristen in der Praxis die Regel. Dadurch dürfte eine ganz neue Dynamik auf dem Markt für Cloud-Dienste entstehen. Inwieweit die Anbieter solcher Dienste eine derartige Schnelllebigkeit verkraften und ihre Geschäftsmodelle anpassen können, bleibt abzuwarten. Zu befürchten ist, dass Cloud-Anbieter diese Unwägbarkeiten künftig einpreisen werden.[29]

Es dürfte eine ganz neue Dynamik auf dem Markt für Cloud-Dienste entstehen.

Der Dienstleister muss zudem den Wechsel seines bisherigen Kunden zu einem anderen Dienstleister aktiv unterstützen, die Daten übertragen und einen nahtlosen kontinuierlichen Übergang gewährleisten (Art. 24 I Data Act-E). Über die ersten drei Jahre nach Inkrafttreten des Data Act sollen die Entgelte für einen solchen Wechselvorgang schrittweise abgeschafft werden und dann für den Nutzer vollständig kostenlos werden (Art. 25 I, II Data Act-E).

II. Interoperabilität

Als wichtiger Faktor für eine offene und faire Datenwirtschaft gilt die sogenannte „Interoperabilität“. Darunter versteht der EU-Gesetzgeber die Fähigkeit von zwei oder mehr Datenräumen, Kommunikationsnetzen, Systemen, Produkten, Anwen-

28 *Gellert/Graef,* The European Commission's proposed Data Governance Act: some initial reflections on the increasingly complex EU regulatory puzzle of stimulating data sharing (2021), 14, hier abrufbar (Stand: 31.05.2022); *Spindler*, CR 2021, 98 (108), Rn. 46; *Falkhofen,* EuZW 2021, 787 (790).
29 *Bomhard/Merkle*, RDi 2022, 168 (175), Rn. 56.

dungen oder Komponenten, Daten auszutauschen und zu verwenden, um ihre Funktion auszuführen (Art. 1 Nr. 19 Data Act-E). Es geht also letztlich darum, dass Systeme miteinander kommunizieren können, da sie einheitliche Formate, Verfahren und Schnittstellen benutzen. Wenn etwa Cloud-Dienste interoperabel sind, so ist der eben beschriebene Wechsel zwischen Cloud-Diensten deutlich besser zu realisieren.

Art. 28 Data Act-E legt den Betreibern von Datenräumen dafür diverse Dokumentationspflichten auf, um Informationen zu beschreiben, die für die Interoperabilität von Diensten wesentlich sind. Art. 29 Data Act-E sieht europäische Normen vor, die die Interoperabilität von Datenverarbeitungsdiensten vorantreiben sollen.

Wer für die Bereitstellung von Daten smart contracts[30] verwendet, muss gewährleisten, dass diese robust sind, sicher beendet oder unterbrochen werden können, nach Beendigung archiviert werden und über eine strenge Zugriffskontrolle verfügen (Art. 30 Data Act-E). Ob die Praxis diesen Anforderungen ausreichend nachkommen kann, wird sich zeigen.

E. Datenaltruismus

Um das volle Potenzial von Daten in der Union auszuschöpfen, setzt die Kommission zu guter Letzt auf Freiwilligkeit in Form des sogenannten ‚Datenaltruismus'. Hierunter versteht der EU-Gesetzgeber die freiwillige Bereitstellung personenbezogener oder nicht-personenbezogener Daten zur Nutzung für Ziele von allgemeinem Interesse (Art. 2 Nr. 16 DGA-E). Gemeint sind etwa die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität oder die bessere Erbringung öffentlicher Dienstleistungen.[31] Ein aktuelles Beispiel für so ein Vorgehen ist die Corona-Datenspende-App des Robert Koch-Instituts.[32]

Der Datenaltruismus soll dazu beitragen, Datenbestände zu schaffen, die umfangreiche Datenanalysen und maschinelles Lernen[33] ermöglichen.[34] Ob in der Praxis die Freiwilligkeit der Bürger ausreicht, um einen dafür ausreichend großen Datenbestand zu schaffen, darf jedoch infrage gestellt werden. Jedenfalls ist zweifelhaft, wie repräsentativ die Erkenntnisse sind, wenn dort nur die Daten derer zu finden sind, die sich dazu berufen gefühlt haben, ihre Daten freiwillig zu spenden.

Art. 17 DGA-E sieht vor, dass sich „datenaltruistische Organisationen" als solche in ein Register eintragen lassen können. Nach der Eintragung kann sie sich als „in der Union anerkannte datenaltruistische Organisation" bezeichnen und das entsprechende Logo verwenden. Die Registrierung setzt voraus, dass die Organisation Ziele von allgemeinem Interesse verfolgt, ohne Erwerbszweck tätig ist und diese Tätigkeit über eine Struktur ausübt, die von ihren anderen Tätigkeiten funktionell getrennt ist (Art. 18 i.V.m. Art. 2 Nr. 16 DGA-E). Erlaubt die Organisation die Verarbeitung des Datenbestands durch Dritte, so muss sie dies transparent dokumentieren (Art. 20 DGA-E). Zudem muss die Organisation die Datenspender über die Ziele der Verarbeitung und etwaige Verarbeitungen in Drittstaaten informieren (Art. 21 I DGA-E). Da das Erfassen von Datenspenden bei personenbezogenen Daten datenschutzrechtlich auf die Einwilligung nach der DSGVO gestützt wird,[35] stellt Art. 25 I DGA-E ein einheitliches europäisches Einwilligungsformular für den Datenaltruismus in Aussicht.

Unter dem Strich scheint die Idee des ‚Datenaltruismus' eine gute Sache zu sein. Wieso es hierzu aber neuer Regelungen neben der DSGVO bedurfte und was passieren soll, wenn eine Organisation sich nicht in das Register einträgt, bleibt unklar.[36] Erwägungsgrund 46 stellt sogar klar, dass die Eintragung keine Voraussetzung für die Ausübung datenaltruistischer Tätigkeiten ist. Es scheint sich hier vielmehr um ein reines Gütesiegel zu handeln, als dass eine Zertifizierung als „datenaltruistische Organisation" tatsächlich rechtliche Auswirkungen hätte. Ob man aber durch (rein

30 Zum Begriff des Smart Contracts siehe *Dischinger*, CTRL 1/21, 18 (19f.).
31 Art. 2 Nr. 16 DGA-E a.E.; Erwägungsgrund 45 DGA-E.
32 Infos zu der App finden sich hier (Stand: 31.05.2022).
33 Zum Begriff des maschinellen Lernens siehe *Kupfermann*, CTRL 1/21, 7.
34 Erwägungsgrund 45 DGA-E.
35 Erwägungsgrund 50 DGA-E; *Schildbach*, ZD 2022, 148 (151); *von Hagen/Völzmann*, MMR 2022, 176.
36 Vgl. *Spindler*, CR 2021, 98 (106), Rn. 41; *Schildbach*, ZD 2022, 148 (151f.).

symbolische) neue Bürokratie den Willen zur Datenspenden anregt, darf wiederum bezweifelt werden.[37]

F. Fazit

Insgesamt hinterlassen DGA-E und Data Act-E ein gemischtes Bild: Die Idee eines Binnenmarktes für Daten, in dem durch den freien Fluss großer Datenmengen Innovation erzeugt wird, scheint eine vielversprechende und zukunftsträchtige Strategie zu sein. Hier sollte die EU weiterhin Energie investieren und einen klaren Weg verfolgen.

Gleichwohl lassen einen diese beiden Verordnungs-Entwürfe auch ernüchtert zurück: Anstatt umfassender und präziser Regeln findet man gewissermaßen ein Sammelsurium an unterschiedlichsten Vorschriften. Diese sind für sich genommen (mehr oder weniger) nachvollziehbar; einen roten Faden, der die Vorschriften verbindet, sucht man jedoch vergebens. Gerade unter einer Verordnung mit dem Namen „Data Act" hätte man eine umfassende Regulierung der Datenwirtschaft erwartet. Stattdessen werden hier nur einzelne Teilgebiete in Details geregelt. Wieso man statt einer einheitlichen Verordnung zwei verschiedene (DGA und Data Act) kreiert hat, erschließt sich ebenfalls nicht ohne Weiteres. So wird die Rechtslage ohne Not verkompliziert, was letztlich der Akzeptanz und Bereitschaft der Unternehmen und Bürger zur aktiven Teilnahme am unionsweiten Datenverkehr schaden könnte. Es bleibt zu hoffen, dass die EU sich damit nicht selbst ausbremst.

Nach einem gründlichen Blick auf die Verordnungsentwürfe muss man daher feststellen, dass sich die Datenautobahn im Binnenmarkt doch noch in einem frühen Baustadium befindet. Bevor wirklich freie Fahrt im Datenverkehr herrscht, ist noch viel Arbeit zu tun – doch es wird sich sicher lohnen, den Weg weiterzugehen.

37 *Veil*, Datenaltruismus: Wie die EU-Kommission eine gute Idee versemmelt, hier abrufbar (Stand: 31.05.2022); *Steinrötter*, ZD 2021, 61 (62).

Legal Tech

Hinter den Kulissen juristischer Suchmaschinen

Christian Hartz

Open Peer Review
Dieser Beitrag wurde lektoriert von: Felipe Molina und Ramon Schmitt

Christian Hartz ist Rechtsanwalt und als Legal Engineer im Team Content Architecture & AI bei Wolters Kluwer als Product Owner für verschiedene nationale und internationale KI-Projekte verantwortlich.

„*Wissen heißt wissen, wo es geschrieben steht.*“ soll Albert Einstein gesagt haben. Ob er es wirklich gesagt hat, wissen wir nicht. Zumindest lässt es sich nur mit großem Aufwand nachprüfen. Anders sollte es bei Zitaten und Behauptungen vor Gericht sein. Doch lässt auch hier die Realität mit Falsch- und Blindzitaten auf sich warten.

Aber warum ist das so? Kann es deswegen sein, weil juristische Recherche Zeit kostet; zu viel Zeit? Kann es sein, weil die Recherche zu kompliziert oder unhandlich ist? Kann es sein, dass der Wert ordnungsgemäßen Zitierens gar nicht so hoch ist, wie manch einer zu glauben scheint? Gewinne ich einen Fall auch, ohne eine einzige Norm oder eine einzige Entscheidung zu zitieren? Die Antwort auf die letzte Frage ist ein klares: ja.

Aber wie erklärt sich dann die Existenz juristischer Recherche-Datenbanken wie ***Beck-Online***, ***juris*** oder ***Wolters Kluwer Online***? Gibt es gar eine Pflicht zur Nutzung solcher Angebote?

Die wohl herrschende Meinung sagt, dass es Pflicht der Juristen ist, zu wissen, wie der Fall gelöst wird und wie die höchstrichterliche Rechtsprechung dazu lautet.[1] Der Weg, dieses Wissen zu erlangen, wird allerdings nicht festgelegt. So steht es dem Anwalt[2] anheim, Fachzeitschriften zu lesen oder die Entscheidungssammlungen zu nutzen, um die neuste Rechtsprechung zu verfolgen und auf aktuellem Stand zu bleiben.[3] Der BGH sieht eine generelle Pflicht lediglich zum Lesen der höchstrichterlichen Entscheidungssammlungen[4] und Fachzeitschriften und selbst dort nur der ‚Mainstream-Zeitschriften'[5]. Freilich ist dies auch über eine Recherche-Datenbank möglich. In der Literatur wird diese Alternative zumindest auch diskutiert und als zulässig erachtet.[6]

> „Der BGH sieht eine generelle Pflicht zum Lesen der höchstrichterlichen Entscheidungssammlungen und Fachzeitschriften."

Was ist aber mit Entscheidungen, die (noch) gar nicht in einer amtlichen Sammlung oder in einer Zeitschrift abgedruckt sind? Besteht hier eine Pflicht, sich bei den Recherche-Datenbanken zu erkundigen?

A. Pflicht zur Nutzung von Recherche-Datenbanken?

Hier sagt die wohl (noch?) herrschende Meinung: Nein, es gibt keine Pflicht. Aber um dieser Frage und der herrschenden Ansicht auf den Grund zu gehen, muss zunächst erörtert werden, woraus sich eine Pflicht zur Nutzung von Recherche-Datenbanken für Rechtsanwälte herleiten könnte.

I. Herleitung aus dem Berufsrecht oder dem Mandatsvertrag?

Eine Pflicht zur Nutzung von Recherche-Datenbanken könnte sich möglicherweise aus § 43 S. 1 BRAO, aus § 43a VI BRAO, § 1 III BORA oder dem zugrundeliegenden Mandatsvertrag ergeben.

§ 1 BORA legt dem Rechtsanwalt, nach ständiger Rechtsprechung, die Pflicht auf, gerichtliche Fehlentscheidungen zu verhindern und „auf die rechtliche Beurteilung des Gerichts Einfluss zu nehmen".[7] Aus haftungsrechtlicher Sicht besteht zumindest die Tendenz, dass der Anwalt für ungewöhnlich schwere Fehlgriffe der Gerichte nicht zu haften hat.[8] Ein Übersehen einschlägiger Rechtsprechung aufseiten des Gerichtes stellt jedoch keinen ungewöhnlichen schweren Fehlgriff dar, der den Zurechnungszusammenhang unter-

1 Bspw. *Weinland*, in: Henssler/Gehrlein/Holzinger, Handbuch der Beraterhaftung, 1. Auflage 2018, IV. Prüfung der Rechtslage, Rn. 156.
2 Zum Zwecke der besseren Lesbarkeit wird bei personenbezogenen Hauptwörtern nur die männliche Form verwendet. Gemeint sind jedoch immer alle Geschlechter.
3 Vgl. dazu nur *Roßkothen*, AnwBl 2021, 503 (504) m.w.N.
4 *Träger*, in Weyland, Bundesrechtsanwaltsordnung, 10. Aufl. 2020, § 43a Rn. 97.
5 BGH, Urt. v. 23.09.2010 - IX ZR 26/09, Rn. 26.
6 *Weinland*, in: Henssler/Gehrlein/Holzinger, Handbuch der Beraterhaftung, 1. Auflage 2018, IV. Prüfung der Rechtslage, Rn. 196.
7 BGH, Urt. v. 04.06.1996 - IX ZR 51/95, Rn. 30.
8 *Fahrendorf/Mennemeyer*, Die Haftung des Rechtsanwalts, 10. Auflage, 2021, A. Hauptleistungspflichten aus dem Anwaltsvertrag (§ 241 Abs. 1 BGB), Rn. 58.

bricht.[9] Dies führt konsequenterweise dazu, dass der Rechtsanwalt einer Haftung unterliegt.[10] Die Recherche liegt also in seinem Interesse, aber eine Pflicht ist es nicht.

Die allgemeine Berufspflicht in § 43 S. 1 BRAO ist nach überwiegender Ansicht Auffangtatbestand und als Überleitungsvorschrift zu verstehen.[11] Die Annahme, einer Verpflichtung zur Kenntnisnahme höchstrichterlicher Rechtsprechung zur gewissenhaften Ausübung des Berufs, wie in § 43 S. 1 BRAO gefordert, ist nicht ganz fernliegend. Allerdings ist nicht festgelegt, wie diese Kenntnisnahme auszusehen hat. Gleiches gilt für § 43a BRAO, der in Abs. 6 (ab 1.8.2022 Abs. 8) eine Fortbildungspflicht statuiert, die aus der gewissenhaften Berufsausübung resultiert.[12] Auch diese postuliert eine Verpflichtung zur Kenntnis der maßgeblichen veröffentlichten Rechtsprechung. Allerding sweist auch diese Norm keine Vorgaben aus, wie der Rechtsanwalt dieser Verpflichtung nachkommen soll.[13] Letztlich lässt sich auch aus dem Mandatsvertrag eine Verpflichtung zur gewissenhaften Vornahme des Mandates und zur rechtlichen Prüfung und daher auch Kenntnis der Rechtsprechung herleiten.[14]

Somit besteht insgesamt eine allgemeine Recherche-Pflicht. Daraus folgt allerdings noch keine Pflicht zur Nutzung einer juristischen Datenbank. Lediglich bei ganz aktueller unveröffentlichter Rechtsprechung und/oder einer Veränderung der Rechtsprechung wird teilweise vertreten, dass der Rechtsanwalt sich auch aus anderen Quellen informieren müsse.[15] Kann hieraus aber bereits eine Pflicht zur Verwendung juristischer Datenbanken erwachsen?

BRAO / BORA:

Die BRAO ist die Bundesrechtsanwaltsordnung. Entgegen ihres Namens handelt es sich nicht um eine Verordnung, sondern um ein Bundesgesetz. Die BRAO legt dabei die grundsätzlichen Rechte und Pflichten für die Berufsausübung der Anwälte fest. So regelt sie etwa grundlegendes wie das Zulassungsverfahren zum anwaltlichen Beruf oder auch spezifisches wie das Verbot, dass sich an Rechtsanwaltsgesellschaften keine Nicht-Anwälte als Gesellschafter beteiligen können. Die BRAO wurde dabei vor kurzem wesentlich reformiert, sodass etwa eine anwaltliche GmbH & Co. KG zulässig sein wird. Die Änderungen treten zum 01.08.2022 in Kraft.

Die mit der BRAO nicht zu verwechselnde BORA (Berufsordnung für Rechtsanwälte) ist eine Satzung der Bundesrechtsanwaltskammer (BRAK), deren Kompetenz hierfür aus § 59b BRAO abgeleitet wird. Die Rechtsanwälte werden an die BRAO gebunden, indem jeder Anwalt einer regionalen Rechtsanwaltskammer angehören muss. Jede dieser Rechtsanwaltskammern ist wiederum Mitglied der BRAK und damit an die BRAO als Satzung gebunden.

II. Die Nutzungspflicht in der Rechtsprechung

Die Rechtsprechung befasst sich mit dieser Problematik lediglich in Haftungsfällen. Die Gerichte erhalten somit nur Sachverhalte, in welchen eine bestimmte Entscheidung nicht bekannt war, diese für den Ausgang des vom Anwalt geführten Verfahrens aber einen sehr hohen Wert hatte, das Verfahren verloren wurde und letztlich der Mandant einen weiteren Haftungsprozess gegen den Anwalt anstrebt. An der Anzahl der Voraussetzungen sieht man bereits, dass es sich eher um seltene Fälle handelt. Dass ein solcher Fall dem BGH zugetragen wird, ist eine Rarität. Offensichtlich scheint dies für das Steuerrecht etwas weniger selten zu sein, denn viele der Fälle, die durch die Rechtsprechung geklärt wurden, betreffen dieses.[16]

9 BGH, Urt. v. 18.12.2008 - IX ZR 179/07, Rn. 8.
10 So auch *Teichmann*, in: BeckOGK, 1.4.2022, BGB § 675 Rn. 1198.1.
11 *Träger*, in Weyland, Bundesrechtsanwaltsordnung, 10. Aufl., 2020, § 43 Rn. 11; so auch schon AGH Hamburg, Urt. v. 16.2.2009, I EVY 6/08.
12 *Träger*, in Weyland, Bundesrechtsanwaltsordnung, 10. Aufl., 2020, § 43a Rn. 97.
13 *Träger*, in Weyland, Bundesrechtsanwaltsordnung, 10. Aufl., 2020, § 43a Rn. 97.
14 Vgl. etwa *Seichter*, in jurisPK-BGB, 9. Aufl., 2020, § 280 Rn. 79 f.
15 BGH, Urt. v. 21.09.2000 - IX ZR 127/99, Rn. 51; so auch etwa *Seichter*, in jurisPK-BGB, 9. Aufl., 2020, § 280, Rn. 79 f.; *Träger,* in Weyland, Bundesrechtsanwaltsordnung, 10. Aufl., 2020, § 43a, Rn. 97.
16 So etwa BGH, Urt. v. 23.09.2010 - IX ZR 26/09; OLG Köln, Urt. v. 26.03.2015, 8 U 27/07.

In diesen Entscheidungen wird in der Regel darauf verwiesen, dass die in einschlägigen Zeitschriften veröffentlichte Rechtsprechung zu kennen ist.[17] Ob hierfür jedoch auch der Rückgriff auf juristische Recherchedatenbanken erfolgen muss, wurde bisher offengelassen. Die wesentliche Entscheidung des BGH hierzu stammt bereits aus dem Jahre 2010:

„Ob bei einer fortschreitenden, einen einfachen, raschen und kostengünstigen Zugriff gestattenden Informationstechnologie in Zukunft strengere Anforderungen an die Kenntnis höchstrichterlicher Entscheidungen zu stellen sind, kann vorliegend offen bleiben."[18]

III. Die Nutzungspflicht zur Datenbank in der Literatur

Die Literatur steht einer Nutzungspflicht ebenfalls (noch) überwiegend ablehnend entgegen. Teilweise wird auf die genannte Entscheidung des BGH eingegangen, verknüpft allerdings lediglich mit dem Hinweis, dass eine Pflicht zur Nutzung einer juristischen Datenbank nicht besteht. Ob sich diese – seit annähernd 12 Jahren bestehende – Lage geändert hat, wird nicht erörtert.

Seichter wagt den vorsichtigen Vorstoß, eine Abkehr von dem Verwenden von Zeitschriften hin zur Verwendung juristischer Datenbanken zu fordern. Er argumentiert damit, dass in der Praxis faktisch kein Anwalt für eine solche Recherche Zeitschriften durchliest, sondern vielmehr zur Recherche eine Datenbank verwendet.[19] Eine dogmatische Herleitung fehlt allerdings. Damit liefert ***Seichter*** einen Gegenpol zu der noch im Jahr 2007 von ***Schnabl*** vertretenen Ansicht, dass das Verwenden juristischer Datenbanken noch kein allgemeiner juristischer Standard sei.[20] Allerdings gehen sowohl ***Schnabl***[21] als auch ***Roßkothen***[22] davon aus, dass dies ein in Bewegung befindlicher Prozess sei und lediglich (noch) keine Pflicht zur Nutzung aufzuerlegen sei. Wie sieht es also nun, mehr als 10 Jahre nach der Entscheidung des BGH und 15 Jahre nach den Ausführungen von ***Schnabl*** aus? Hierzu muss man sich die Entscheidung des BGH aus 2010 genauer anschauen.

B. Die Entscheidung des BGH aus 2010

In seiner Entscheidung aus 2010 hatte der BGH folgende drei Voraussetzungen als notwendig erachtet, um von einer Nutzungspflicht (von damals noch Zeitschriften) ausgehen zu können:

(i) Kostengünstiger Zugriff;

(ii) Einfache Nutzung; und

(iii) Rascher Zugriff

Es stellt sich somit die Frage, ob juristische Datenbanken mittlerweile diese Voraussetzungen erfüllen und folglich eine Nutzungspflicht besteht.

I. Kostengünstiger Zugriff

Eine führende Zeitschrift im Baurecht ist die ***BauR***, mit einem Print-Abo-Jahrespreis von 495 €. Vergleicht man dazu das Einstiegsmodul zum Baurecht bei ***Wolters Kluwer,*** so kostet dies 888 € pro Jahr. Inhalt des Moduls ist allerdings nicht nur Rechtsprechung, sondern auch eine Vielzahl sonstiger Werke (und eben gerade auch die ***BauR***). Da es aber vornehmlich um die Rechtsprechung geht, sollte auch auf ein entsprechendes Modul abgestellt werden, welches nur Rechtsprechung beinhaltet. Das passende Modul – erneut bei ***Wolters Kluwer*** – ***„Gesetze und Rechtsprechung Flat"*** kostet 358,80 € pro Jahr. Bei ***juris*** und ***Beck-online*** gibt es lediglich

17 Vgl. nur BGH, Urt. v. 21.09.2000 - IX ZR 127/99, Rn. 51.
18 BGH, Urt. v. 23.09.2010 - IX ZR 26/09.
19 So bspw. *Seichter,* in jurisPK-BGB, Band 2, § 280, Rn. 82.
20 *Schnabl*, NJW 2007, 3025.
21 *Schnabl*, NJW 2007, 3025.
22 *Roßkothen*, AnwBl. 2012, 503.

kombinierte Produkte und keine Produkte, die nur Rechtsprechung/Normen enthalten; aber auch dort liegen die Einstiegspreise bei ca. 50 € - 110 € pro Monat (bspw. ***„NomosOnline Anwalt Basis"*** (49 €) bzw. ***„juris Professionell"*** (110 €)), somit handelt es sich um Jahrespreise zwischen 600 und 1300 €. Verglichen mit der Zeitschrift scheinen die Datenbanken – für die Kenntnisnahme von Rechtsprechung – eine kostengünstige Alternative zu sein. Wenn es um die höchstrichterliche Rechtsprechung geht, besteht allerdings für bestimmte Entscheidungen auch die Möglichkeit, völlig kostenfrei über die Seiten der Bundesgerichte auf diese Inhalte zuzugreifen. Ein „kostengünstiger Zugriff" scheint dementsprechend erfüllt zu sein.

II. Einfache Nutzung

Die meisten Recherche-Datenbanken bieten sowohl den Zugriff über ein Register oder eine Navigation als auch den Zugriff über eine Suche an. Durch die Nutzung von ***Google***, ***Bing*** oder alternativen Suchmaschinen gehört die Verwendung einer Suchmaske zum Alltag. Auch wenn juristische Recherche-Datenbanken häufig mit speziellen Stichworten gefüttert werden müssen, um das passende Ergebnis zu erhalten, sind sie dennoch vergleichsweise unkompliziert zu nutzen. Dies gerade auch deswegen, weil User-Experience-Designer die Nutzung der Datenbanken deutlich verbessert haben; Boolesche Operatoren sind keine zwingende Voraussetzung mehr.

III. Rascher Zugriff

Die Voraussetzung des Merkmals „***Rascher Zugriff***" ist mehrdeutig. Zum einen könnte es sich um die Zeit handeln, bis zu der eine Entscheidung in einer Datenbank verfügbar ist. Zum anderen um die Zeit, die benötigt wird, um die Datenbank zu nutzen und ein Ergebnis zu erhalten.

Boolesche Operatoren:

Boolesche Operatoren sind Wörter, die eine Suchmaschine mit einer logischen Funktion verknüpft hat. So können Suchmaschinen durch die Verwendung des Wortes „Und" als boolescher Operator verstehen, dass der Nutzer nur Suchergebnisse erhalten möchte, die beide durch das „Und" verknüpfte Begriffe enthält. Moderne Suchmaschinen deuten dabei häufig ein Leerzeichen als ein „Und" im Backend. Wird stattdessen ein „Oder" verwendet, so zeigt die Suchmaschine alle Ergebnisse an, die mindestens einen der Begriffe enthalten.

Insbesondere bei obergerichtlicher Rechtsprechung findet die Publikation in den Datenbanken zeitnah nach der Verkündung oder der Veröffentlichung der Gründe statt, sodass dieser Aspekt ohne Weiteres erfüllt ist.

Durch die Verfügbarkeit schnellen Internets und die Reduktion der Latenzen auf Seiten der Datenbankanbieter sind auch die Zugriffszeiten zu solchen Datenbanken minimal und vergleichbar schnell zum Öffnen und Durchblättern einer Zeitschrift.

Hinsichtlich des Auffindens der richtigen Zeitschriften-Fundstelle, verglichen mit dem Auffinden der Entscheidung in einer Datenbank, wird man wohl zugunsten der Datenbank entscheiden müssen. Allein das Heraussuchen im Index der Zeitschrift und das Aufschlagen der entsprechenden Seite wird – verglichen mit der Eingabe in die Suche der Datenbank – deutlich länger dauern.

Daher ist auch die Anforderung an den „***Raschen Zugriff***" bereits zum jetzigen Zeitpunkt erfüllt.

IV. Fazit zur Rechtsprechung des BGH

Somit sind zwischenzeitlich alle vom BGH im Jahr 2010 aufgestellten Anforderungen erfüllt, sodass man eine Pflicht annehmen kann. Bisher hat sich die Rechtsprechung jedoch hierzu noch nicht wieder äußern müssen.

Allerdings schreiten auch die Entwicklungen bei den Recherchedatenbanken voran und so steht bereits die nächste Generation vor der Tür.

Im Gegensatz zu bisherigen Datenbanken erfolgt bei der nächsten Generation eine Integration direkt in den Workflow der Juristen. Gleichzeitig nimmt auch die Verwendung künstlicher Intelligenz in den Datenbanken stark zu.

Es wird also Zeit, noch einmal zu schauen, wie juristische Recherche heute stattfindet, was die Nachteile sind und wie die Recherche der Zukunft aussehen kann.

C. Juristische Recherche heute und in der Zukunft

I. Wie funktioniert juristische Recherche heute?

Derzeit sind die meisten juristischen Recherchelösungen auf die Eingabe von Stichworten angewiesen. Diese Nutzereingabe wird dann auf verschiedene Art und Weise mit den vorhandenen Daten in der Datenbank abgeglichen, um das gesuchte Ergebnis anzuzeigen. Auf der nachfolgenden Seite ist eine schematische Darstellung abgebildet, wie eine solche Suche funktionieren kann. Diese erhebt keinerlei Anspruch auf Vollständigkeit und soll lediglich verdeutlichen, wie eine solche Suche aussehen könnte.

1. Schritt 1 – Erfassen der Nutzereingabe

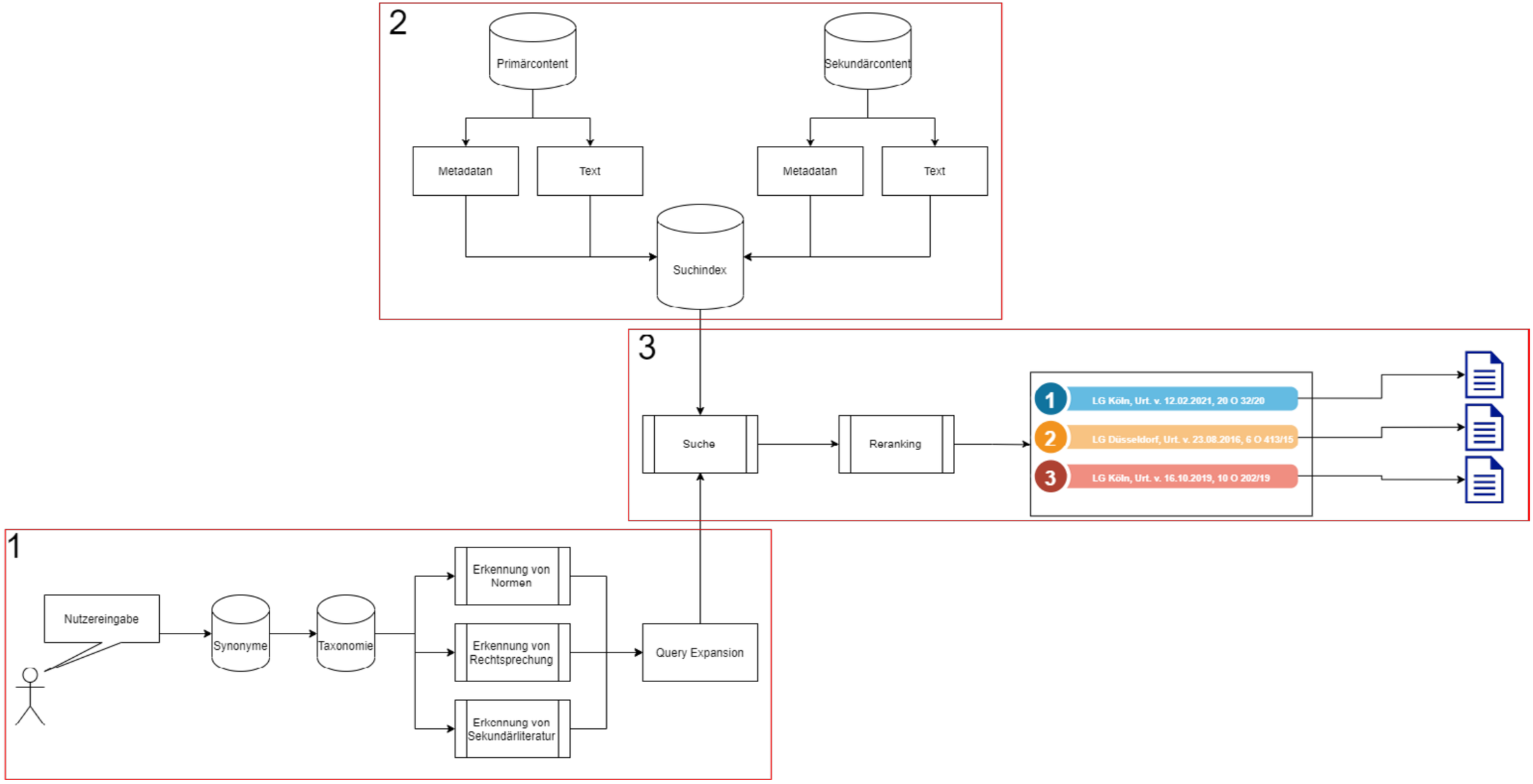
In **Schritt 1** geht es darum, die Nutzereingabe besser zu verstehen und zu erkennen, was der Nutzer gerade finden möchte.

Oftmals entspricht das gesuchte Wort lediglich einem Synonym oder einem ähnlichen Wort (die Nutzereingabe enthält bspw. Auto, es werden aber auch Dokumente mit KFZ und Fahrzeug gewünscht). Eine Taxonomie oder Ontologie kann dabei helfen, bestimmten Bestandteilen der Suche ein höheres Gewicht zu geben oder Beziehungen herzustellen.

Ein Auto ist ein engeres Konzept zum breiteren Konzept Fortbewegungsmittel; ein Fahrrad wäre auch ein Fortbewegungsmittel, sodass das Wort Fortbewegungsmittel die beiden anderen übergeordnet vereint.

Zusätzlich werden in Schritt 1 auch Normen, Entscheidungen oder Autorennamen erkannt. Wird § 433 BGB zusammen mit ***Prütting*** eingegeben, so deutet dies darauf, dass der Nutzer nicht die Norm des § 433 BGB lesen möchte oder Rechtsprechung zu dem Thema sehen möchte, sondern es gerade um die Kommentierung in dem Werk Prütting u.a. BGB geht.

Alle gefunden Informationen aus Schritt 1 werden der Nutzereingabe hinzugefügt (sog. ***Query-Expansion***) und mit dieser erweiterten Suche kann dann im Backend gesucht werden.



Schematische Darstellung der Technik einer Recherchelösung.

2. Schritt 2 – Abfrage in der Datenbank

Schritt 2 behandelt alle vorhandenen Dokumente (Rechtsprechung, Normen, Sekundärliteratur), die in einer Datenbank gespeichert wurden. Der Einfachheit halber wurden sie hier in zwei Töpfe aufgeteilt. Primärcontent (dt. ***Primärquellen***) sind Normen und Rechtsprechung, Sekundärcontent (dt. ***Sekundärquellen***) ist all das, was über diesen Primärcontent geschrieben wird, also bspw. Zeitschriften, Kommentare, Handbücher. Der Content selbst besteht aus zwei Teilen: dem Text (die Entscheidung des BGH) und der Information über das Dokument selbst, die sog. ***Metadaten***. Metadaten können etwa Gericht, Datum, Aktenzeichen, wichtigste zitierte Normen oder Informationen zur Rechtskraft sein. All diese Daten werden gemeinsam in einem Suchindex abgespeichert, um zur Laufzeit (dem Zeitpunkt, zu dem der Nutzer seine Suche absendet) abgerufen werden zu können.

3. Schritt 3 – Suche und Ranking

In **Schritt 3** findet dann die eigentliche Suche statt.

Die Eingabe des Nutzers und die daraufhin erfolgte Anreicherung mit weiteren Begriffen aus Schritt 1 (***Query***) wird mit dem Suchindex aus Schritt 2 abgeglichen und alle passenden Dokumente werden herausgesucht. Gleichzeitig werden die Informationen gewichtet, um im Ranking oder Re-Ranking die besten Informationen an die Spitze der Trefferliste zu bringen. Dieses Ranking erfolgt aufgrund von festgelegten Kriterien, die der Wichtigkeit entsprechen. Bei der Eingabe von „§ 433 BGB ***Prütting***“ würde das Ranking auf das Metadatum „Werk:Prütting“ und zusätzlich auf die Norm § 433 BGB beschränkt, sodass nur noch solche Dokumente in die Trefferliste dürfen, die aus dem Werk Prütting stammen und § 433 BGB kommentieren. Bester Treffer wäre dann wohl die Übersicht über § 433 BGB bzw. der Normtext im Kommentar. Bei Rechtsprechungsdokumenten funktioniert es genauso: Die Nutzereingabe BGH filtert auf Dokumente des BGH oder BGH wird als sehr starkes Kriterium verwendet und bringt Dokumente des BGH nach oben in die Trefferliste.

Dieser Ranking-Schritt entscheidet über die Akzeptanz des Ergebnisses, denn oftmals werden von Nutzern nur die ersten 3-5 Treffer überhaupt wahrgenommen.

II. Was sind Nachteile der derzeitigen juristischen Recherche?

Hier soll der Kürze der Darstellung wegen nur auf drei Probleme eingegangen werden: die Art der Sucheingabe, das Fehlen der Berücksichtigung semantischen Wissens und die Notwendigkeit eine Recherche aktiv durchzuführen.

Ein Nachteil der derzeitigen juristischen Recherche ist die Notwendigkeit zur Eingabe von Stichworten. In dem Fall, dass der zu recherchierende Sachverhalt gänzlich durchdrungen, die passenden Normen und Problemstellungen hinlänglich bekannt sind, stellt dies kein Problem dar. Was aber, wenn unklar ist, welche Normen relevant sind, wenn der Fachterminus nicht bekannt ist? Hier fällt die Stichwortsuche deutlich schwerer.

Ein weiterer Nachteil ist die fehlende Berücksichtigung der Semantik. Bei Semantik geht es um die Wort-, Satz- oder Textbedeutung. Die stichwortbasierte Suche gleicht den Text Wort für Wort (ggf. ergänzt um Synonyme, Komposita etc.) ab, versteht aber die dahinterliegende Semantik nicht.

Eine Unterscheidung der Phrase ‚***ist für die aberratio ictus nicht relevant***‘ und ‚***die Normen des § 16 StGB finden auf die aberratio ictus Anwendung***‘ erfolgt nicht. Dabei kann dies einen großen Unterschied machen, ob das gefundene Dokument für die Nutzereingabe relevant ist oder nicht.

Schließlich ist das Durchführen einer Recherche immer eine aktive Entscheidung und sie kann nicht nebenherlaufen, um bei der Arbeit zu unterstützen. Es muss jeweils die derzeitige Arbeit (zum Beispiel das Schreiben des Dokumentes) unterbrochen werden, um zu suchen.

III. Wie könnte die juristische Recherche in der Zukunft aussehen?

Die Recherche der Zukunft müsste in den Workflow eingebettet sein. Bei dem Schreiben eines Textes in ***Word*** wird im Dokument selbst die Rechtschreibung automatisch überprüft und Fehler werden markiert. Dadurch wird die Prüfung direkt in den Workflow integriert und ein zusätzliches Ausführen der Rechtschreibprüfung kann unterbleiben. Ähnlich sollte es mit der juristischen Recherche sein. Direkt in den Workflow eingebunden und dort unterstützend, wo Informationen benötigt werden.

Das ist allerdings nur möglich, wenn eine Abkehr von der stichwortartigen Suche stattfindet und die Semantik mit einbezogen wird. Denn nur dann kann zu einem langen Text, der gerade formuliert wird, automatisch die passende Rechtsprechung gefunden, die passende Norm angezeigt oder die Kommentar-Fundstelle, welche die eigene Argumentation stützt, eingefügt werden.

D. Wo stehen wir derzeit?

Die Entwicklungen im Bereich des maschinellen Lernens sind unglaublich schnell. Semantische Suche, die Verwendung von Wissensgrafen und juristische Sprachmodelle sind nur Teile dessen, was dazu beiträgt, dass die soeben beschriebene Integration in den Workflow keine Zukunftsmusik, sondern Realität ist.

Im englischsprachigen Raum sind solche Lösungen bereits verbreitet. In manchen Bereichen wie M&A (***Mergers & Acquisitions***, dt. ***Fusionen & Unternehmenskäufe***) wird ebenfalls intensiv mit Produkten gearbeitet, die bestimmte Arbeiten abnehmen und (teil-)automatisieren. Mit Analytics-Lösungen werden in Zukunft keine Stichworte mehr eingegeben werden müssen, sondern die Arbeit am Fall steht im Mittelpunkt. Erste Lösungen sind auch für den deutschen Markt bereits verfügbar und weisen den Weg in die Zukunft der juristischen Recherche.


© Greta Maria Gross (Illustratorin)
gretamariasgallery

Aufsatz

Es waren zwei Königskinder: zum Problem des EU-US-Datentransfers

Fabio Stark

Fabio Stark wurde 1996 in Starnberg geboren und studiert seit 2017 Rechtswissenschaften an der LMU München mit Schwerpunkt im europäischen Wirtschaftsrecht, Wettbewerbsrecht und geistigem Eigentum.

Open Peer Review

Dieser Beitrag wurde lektoriert von: Ludovica Böltling und Jens Hansen

Der Wirtschaftsverkehr zwischen der Europäischen Union und den Vereinigten Staaten von Amerika machte im Jahr 2020 42 % des Welthandels aus.[1] Dabei betrug der Wert aller Waren, die zwischen den beiden Wirtschaftsräumen ausgetauscht wurden, rund 556,2 Mrd. €.[2] Gleichzeitig flossen ca. 18 % der jeweiligen Gesamtexporte an den jeweils anderen, was bis heute eine wechselseitige Stellung als wich-

1 Infografik des Europäischen Rates zum EU-US-Handel, hier abrufbar (Stand: 25.05.2022).
2 Europäische Kommission, EU trade relations with the United States. Facts, figures and latest developments, hier abrufbar (Stand: 25.05.2022).

tigster Exportpartner[3] begründet.[4] Dass hierbei insbesondere dem Datentransfer eine herausragende Rolle zukommt, ist selbsterklärend: Im Waren- und Dienstleistungshandel müssen, von den Vertragsverhandlungen über den Leistungsaustausch bis zum Geschäftsabschluss, zwangsläufig Informationen zwischen den Geschäftspartnern fließen.[5] Dies gilt umso mehr, als Telekommunikations- und Unternehmensdienstleistungen per se zu den drei wichtigsten ‚Exportschlagern' der USA zählen.[6] Dieser Umstand hält spürbaren Einzug in unseren Alltag: jeder Post auf Twitter und Instagram, jede E-Mail, jede Suchanfrage auf Google kann hier in Deutschland getätigt werden, wird aber stets auf Unternehmensservern in den USA verarbeitet. Der Großteil der digitalen Dienste, die in Deutschland in Anspruch genommen werden, werden von US-Unternehmen angeboten. Es überrascht also keineswegs, dass die Urteile Schrems I und II, welche der EuGH 2016 und 2020 erließ, wie ein Blitz einschlugen: Ein gewichtiger Teil der Rechtsgrundlage des EU-US-Datentransfers wurde für unwirksam erklärt. Doch wie ist das möglich? In einem voran--gegangenen Artikel dieser Reihe wurden die Geschichte, die Grundsätze und die Systematik des europäischen Datenschutzes beleuchtet.[7] Nun wollen wir uns mit dem US-Datenschutz, dem US Privacy Law,[8] vor allem aber mit dem kommerziellen Datenaustausch zwischen den USA und der EU befassen. Dabei wird sich an drei Fragen orientiert:

> „Jeder Post, jede E-Mail, jede Suchanfrage kann hier in Deutschland getätigt werden, wird aber stets auf Unternehmensservern in den USA verarbeitet."

1. Was zeichnet das US Privacy Law gerade in Abgrenzung zum EU-Datenschutz grundsätzlich aus?

2. Welche rechtlichen Probleme bereitet der EU-US-Datentransfer konkret?

3. Wie kann der Datenverkehr zwischen den beiden Weltmächten rechtssicher ausgestaltet werden?

A. Der US-Datenschutz

Das US-Rechtssystem unterscheidet sich bereits in seinen Grundsätzen erheblich vom kontinentaleuropäischen. So kommt, ganz allgemein, der Rechtsgestaltung durch Rechtsprechung oder durch behördliche Dekrete eine wesentlich bedeutendere Rolle zu als hierzulande. Doch gerade der Datenschutz lässt einige besonders eklatante Differenzen erkennen, welche die Transferproblematik überhaupt erst begründen. Ein Blick auf einige dieser Grundlagen hilft, die Verschiedenheit der dahinter stehenden Wertungen besser zu verstehen und den American Approach an den Themenkomplex nachvollziehbar zu machen.

I. ‚The Right to Privacy'- Die Ausgangslage

Es war das deutsche Bundesland Hessen, das 1970 mit dem HDSG das weltweit erste Datenschutzgesetz erließ.[9] Dennoch begann die Debatte um das Konzept des Datenschutzes auf US-amerikanischem Boden: mit dem 1890 von den Juristen S. Warren und L. Brandeis im Harvard Law Review veröffentlichten bahnbrechenden Artikel „The Right to Privacy". In diesem sprachen sich die Autoren, angesichts der expandierenden Presselandschaft sowie dem Aufkommen der Fotografie, für ein

3 Zum Zwecke der besseren Lesbarkeit wird bei personenbezogenen Hauptwörtern nur die männliche Form verwendet. Diese Begriffe sollen für alle Geschlechter gelten.
4 Statistisches Monatsheft Baden-Württemberg 5/2020, Die EU, USA und China – drei Kraftzentren der Weltwirtschaft im Vergleich, 8, hier abrufbar (Stand: 25.05.2022).
5 *ECIPE*, The Economic Importance of getting Data Protection Right, 2013, 1 (7).
6 Infografik des Europäischen Rates zum EU-US-Handel, hier abrufbar (Stand: 25.05.2022).
7 *Stark*, CTRL 1/2022, 87 ff.
8 Dies dient der sauberen Abgrenzung zum Begriff der Datensicherheit, welche im Englischen stellenweise auch als Data Protection bezeichnet wird. Letzteres betrifft weniger den Individual- und Persönlichkeitsschutz als die technische Sicherheit von Daten jedweder Art, vgl. *Forbes Technology Council*, Data Privacy Vs. Data Protection: Understanding The Distinction In Defending Your Data, hier abrufbar (Stand: 25.05.2022).
9 *Stark*, CTRL 1/2022, 87 (88).

„Recht alleine gelassen zu werden“ aus.[10] Der somit erstmals rechtlich abgebildete Konflikt, zwischen dem Privatheitsinteresse des Einzelnen und einer zunehmend technisierten und bürokratisierten Allgemeinheit, wurde im Laufe des 20. Jahrhunderts nur noch schärfer. An beiden Ufern des Atlantiks wuchsen die Gefahren für die informationelle Selbstbestimmung durch technologischen Fortschritt zusehends. Entsprechend wurde der Ruf nach konkreten Datenschutzgesetzen - bald vermehrt gegen staatliche Eingriffe - ab den 1970ern auf beiden Kontinenten lauter. Auch hierbei blieben die Vereinigten Staaten lange Zeit ‚Taktgeber der Diskussion‘.[11]

Dennoch trennten sich die Herangehensweisen der beiden Rechtsräume an das gemeinsame Problem alsbald grundlegend voneinander. In Europa setzte sich ein universelles Schutzsystem durch: gekennzeichnet von Einheitlichkeit, einem möglichst weit gefassten Schutzraum und geringer Differenzierung zwischen staatlichen und privaten Stellen.[12] In den Vereinigten Staaten hingegen begann sich ein bereichsspezifischer, sog. sektoraler Ansatz abzuzeichnen, der ein weder umfassendes noch landesweit harmonisiertes Privacy Law zur Folge hatte. Heute speist sich der lückenhafte und z.T. sogar widersprüchliche US-Datenschutz teils aus Rechtsprechung, teils aus verfassungs-, bundes- und gliedstaatlichen Quellen.

II. Flickenteppich-Privacy – US-Datenschutzrechte im Überblick

1. Verfassungsrecht

Die wichtigste konstitutionelle Verankerung der Privacy Laws findet sich im vierten Amendment der US-Verfassung wieder. Dieses schützt die Privatsphäre von US-Bürgern vor unberechtigten hoheitlichen Durchsuchungen und Beschlagnahmungen.[13] Davon wird nach ständiger Rechtsprechung auch die elektronische Überwachung mittels Datenerhebungen erfasst.[14] Jede eingreifende Maßnahme verlangt demnach grundsätzlich eine gerichtliche Ermächtigung. Dies gilt jedoch nur, soweit (1) die Datenerhebung von staatlichen Stellen ausgeht, (2) der Betroffene ‚begründete Privatheitserwartungen‘ haben darf und (3) die Daten im unmittelbaren Zugriffsbereich des Betroffenen vorliegen, etwa auf seinem Server oder einem lokalen Datenträger.[15] Hat er sie bereits an einen Dritten weitergegeben, wie in Form einer E-Mail oder eines Posts bei Facebook, gelten sie als freiwillig veräußert und daher nicht länger schutzwürdig.[16]

Daneben spielen das Recht auf anonyme Meinungsfreiheit, auf Privatheit von Vereinigungen und der Schutz vor Selbstbelastung, aus dem ersten und fünften Amendment, eine untergeordnete Rolle.[17] Aus der Verfassung selbst erwächst indes keinerlei Schutz vor nicht-staatlicher Datenverarbeitung sowie vor Maßnahmen, die bei Dritten durchgeführt werden, etwa von Betreibern sozialer Netzwerke und sonstigen digitalen Dienstleistern. Und auch die Rechtfertigungsmöglichkeiten nach Eröffnung des Schutzbereichs sind bei weitem nicht so standfest wie für den europäischen Datenschutz üblich.[18]

2. Bundesrecht

Der US-Kongress erließ ab 1974 dutzende Regulierungen, welche Privacy zumindest als Bestandteil enthalten.[19] Allerdings wurden durch diese entweder nur bestimmte

10 *Warren/Brandeis*, The Right to Privacy, in Harvard Law Review, 1890, hier abrufbar (Stand: 25.05.2022).
11 Zit. *Lewinski*, Was Europa und die USA in Sachen Datenschutz unterscheidet, hier abrufbar (Stand: 25.05.2022); zur Entwicklung des Datenschutzes zudem Kühnl, Persönlichkeitsschutz 2.0: Profilbildung und -nutzung durch soziale Netzwerke am Beispiel von *Facebook* im Rechtsvergleich zwischen Deutschland und den USA, 2016, 215.
12 Zur Geschichte und Dogmatik des europäischen Datenschutzes *Stark*, CTRL 1/2022, 87 ff.
13 Wörtlich: *„The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.“*, hier abrufbar (Stand: 25.05.2022).
14 *Swire* in: Svantesson/Kloza, Transatlantic data privacy relations as a challenge for democracy, 2017, 89.
15 *Kühnl*, Persönlichkeitsschutz 2.0: Profilbildung und -nutzung durch soziale Netzwerke am Beispiel von Facebook im Rechtsvergleich zwischen Deutschland und den USA, 2016, 227 ff.
16 Zur sog. Third Party Doctrine: U.S. vs. Golden Valley Elec., Assn.689 F.3d 1108 1116 (9th Circ. 2012); *Wittmann*, Der Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen durch die US-amerikanische Bundesverfassung, 2014, 181.
17 *Solove/Schwartz*, Privacy Law Fundamentals, 2019, 3.
18 Dies wird maßgeblich durch das Erfordernis der begründeten Privatheitserwartungen bedingt, vgl. *Kühnl*, Persönlichkeitsschutz 2.0: Profilbildung und -nutzung durch soziale Netzwerke am Beispiel von Facebook im Rechtsvergleich zwischen Deutschland und den USA, 2016, 229.
19 Übersicht zu sämtlichen Bundesgesetzen mit Datenschutzbezug: ebd., 4 f.

Informationstypen (Kredit[20]- oder Gesundheitsdaten[21] etc.) oder besondere Personengruppen wie beispielsweise Minderjährige[22] geschützt. Damit zeichnet sich das US Privacy Law durch einen im Schwerpunkt mehr verbraucherschützenden als abwehrrechtlichen Charakter aus.

Die Überwachung vieler dieser Vorschriften sowie insbesondere der Einhaltung von Selbstverpflichtungen obliegt der 1914 gegründeten Federal Trade Commission (FTC). Ihr kommt eine besondere Rolle im US Privacy Law zu, zumal vertragliche Abreden einen gewichtigen Anteil des geltenden Schutzstandards ausmachen.[23] Als Verbraucherschutz- und Wettbewerbsaufsicht gewährleistet sie die Durchsetzung entsprechender Rechte aufgrund Anträge von Betroffenen. Jedoch beschränkt sich dies zumeist auf Aufklärungspflichtverletzungen.[24] Mit einer europäischen Datenschutzbehörde ist die FTC daher nicht vergleichbar.

Wichtigstes abwehrrechtliches Datenschutzgesetz ist der Privacy Act von 1974. Als parlamentarische Antwort auf den Watergate-Skandal räumt er US-Bürgern gegenüber Bundesbehörden ein Recht auf Zugang und Kopie bereits erhobener persönlicher Daten sowie auf Korrektur von Falschinformationen ein. Auch der hierzulande bekannte Minimierungsgrundsatz sowie das Erforderlichkeitsgebot für Datenverarbeitungen hielten Einzug; wesentlich mehr Zugriffseinschränkungen gelten indes nicht.[25] Damit reichen die Betroffenenrechte des Privacy Acts nicht an den europäischen Standard heran.

Insoweit erscheint der Electronic Communications Privacy Act (ECPA) von 1986, zur Einschränkung elektronischer Überwachung von US-Bürgern durch Bundesbehörden, schon wirkmächtiger.[26] Im Unterschied zum Privacy Act verbietet Letzterer den Zugriff von Bundesbehörden auf Bürgerdaten unter bestimmten Voraussetzungen gänzlich. Und zwar, im Gegensatz zum vierten Amendment, auch dann, wenn sie an Dritte weitergegeben wurden. Allerdings nur, soweit sie u.a. nicht länger als sechs Monate gespeichert wurden. Vor allem deshalb ist der ECPA wiederholt scharfer Kritik ausgesetzt.[27]

3. Gliedstaatliche Rechte

Während das Bundesrecht also weiterhin nur vereinzelte und unvollständige Regelungen zum Datenschutz enthält, zeichnet sich auf bundesstaatlicher Ebene seit 2018 eine Kehrtwende ab.[28] Zum Zeitpunkt der Veröffentlichung dieses Artikels haben bereits vier Bundesstaaten eigene allgemeine Verbraucherdatenschutzgesetze verabschiedet, in zwölf weiteren Staaten werden entsprechende Regelungen vorbereitet.[29] Allen gemein ist der Anspruch, sämtliche personenbezogenen Daten von Verbrauchern vor möglichst vielen privaten Organisationen zu schützen. In den einzelnen Bestimmungen sind jedoch erhebliche Unterschiede feststellbar. So weist der Vorreiter Kalifornien in seinem California Consumer Privacy Act (CCPA) ein der DSGVO noch ähnliches Schutzkonzept auf. Neben einem Anspruch auf Zugang und Löschung persönlicher Daten gegenüber den Verarbeitern sieht er auch eine Opt-Out-Lösung vor. Demnach hat der Betroffene, nachdem er über die Verarbeitungen seiner Daten (verpflichtend) informiert worden ist, das Recht, diese abzulehnen.[30] Auch der Schutzbereich ist über den verwendeten Datenbegriff nahezu

20 So im Gramm-Leach-Bliley Act (GLBA) von 1999 als Verbraucherschutzregelungen im Bank- und Finanzwesen, hier abrufbar (Stand: 25.05.2022); sowie im Fair Credit Reporting Act (FCRA) von 1970 zum Datenschutz bei Verbrauchermeldezentren, hier abrufbar (Stand: 25.05.2022).
21 Insb. im Health Insurance Portability and Accountability Act (HIPAA) von 1996 zum Schutz von Gesundheitsdaten bei medizinischen Dienstleistern, mehr Informationen hier abrufbar (Stand: 25.05.2022).
22 Geregelt im Children's Online Privacy Protection Act (COPPA) von 2000 zum Schutz persönlicher Daten von Minderjährigen unter dreizehn Jahren, hier abrufbar (Stand: 25.05.2022).
23 So verhängte die *FTC* 2012 gegen *Facebook* eine Geldbuße i.H.v. 5 Mrd. USD, nachdem unrichtige Angaben über die Datenlimitation sowie weitere Verarbeitungspraktiken gemacht wurden, vgl. hier abrufbar (Stand: 25.05.2022).
24 *Kühnl*, Persönlichkeitsschutz 2.0: Profilbildung und -nutzung durch soziale Netzwerke am Beispiel von Facebook im Rechtsvergleich zwischen Deutschland und den USA, 2016, 248 ff.
25 Dazu, aber auch als allgemeine Einführung ins US Privacy Law *Green*, Complete Guide to Privacy Laws in the US, hier abrufbar (Stand: 25.05.2022).
26 *Solove/Schwartz,* Privacy Law Fundamentals, 2019, 41 ff.
27 So *Kravets*, Aging ‚Privacy' Law Leaves Cloud E-Mail Open to Cops, hier abrufbar (Stand: 25.05.2022); oder *Kerr*, The Next Generation Communications Privacy Act, hier abrufbar (Stand: 25.05.2022).
28 So etwa die eBook-Regulierungen Missouris hier abrufbar (Stand: 25.05.2022); oder der Illinois Biometric Information Privacy Act (BIPA), hier abrufbar, (Stand: 25.05.2022).
29 Vgl. zur aktuellen Entwicklung den US State Privacy Legislation Tracker der *International Association of Privacy Professionals* (*IAPP*), hier abrufbar (Stand: 25.05.2022).
30 In Abgrenzung zum Erlaubnisvorbehalt der DSGVO (Opt-In-Lösung), vgl. *Klosowski*, The State of Consumer Data Privacy Laws in the US (And Why It Matters), hier abrufbar (Stand: 25.05.2022).

"europäisch" weit gefasst.[31] Andere Staaten wie Virginia wiederum bieten ein geringeres Schutzniveau, vor allem hinsichtlich der Massenverarbeitung von Daten.[32] Interessanterweise führte insbesondere die Frage nach der Klagebefugnis Privater in der jüngsten Vergangenheit regelmäßig zu Konflikten und sogar gescheiterten Gesetzesvorhaben.[33] All dies hat letztlich einen noch laufenden gesetzgeberischen Wettbewerb innerhalb der USA zur Folge, in welchem sich auf der einen Seite ein bürgerrechtlicher und auf der anderen ein freiheitlicher Ansatz gegenüberstehen. Der Ausgang dessen bleibt ungewiss.

4. Zwischenergebnis

Das sektorale US-Datenschutzrecht weist zumindest den potenziellen Vorteil einer einzelfallgerechteren Regelungsmöglichkeit auf. Während die DSGVO mitunter für die rigorose Gleichbehandlung von Ungleichem kritisiert wird, trifft das US-Recht spezifische Entscheidungen für unterschiedliche Adressaten, Daten- und Verarbeitungsformen. Dadurch räumt das Rechtssystem auch mehr Freiraum für den modernen Datenverkehr ein. Gleichzeitig entstehen durch den lückenhaften Datenschutz nicht nur erheblich mehr Risiken für die informationelle Selbstbestimmung der Betroffenen, sondern auch große Rechtsunsicherheit. Das unübersichtliche Dickicht bestehender bundesrechtlicher Vorschriften wird dabei zunehmend durch teils grundverschiedene einzelstaatliche Gesetze zusätzlich verkompliziert. Noch weniger eingeschränkt bleiben indes die staatlichen Eingriffsmöglichkeiten. Auch der aktuelle Gesetzgebungstrend auf Bundesstaatsebene bleibt dem Verbraucherschutzkonzept des US Privacy Laws unverändert treu.

	DSGVO	CCPA	VCPA
1. **Verarbeitung mit Einwilligungsvorbehalt (Opt-In)**	+	−	+
2. **Verarbeitung mit Widerrufsoption (Opt-Out)**	−	+	−
3. **Recht auf Auskunft über die Verarbeitung**	+	+	+
4. **Recht auf Zugang**	+	+	+
5. **Recht auf Löschung**	+	+	+
6. **Technische u. organisatorische Maßnahmen**	+	+	−
7. **Recht auf Berichtigung falscher Daten**	+	−	+
8. **Adressiert private Stellen**	+	+	+
9. **Adressiert staatliche Stellen**	+	−	−
10. **Klagebefugnis Privater**	+	+	−
11. **Finanzielle Höchststrafen**	**20 Mio €** oder **4 %** des weltweiten Jahresumsatzes	**2.500 $** bei fahrlässiger Verletzung **7.500 $** vorsätzlicher Verletzung	**7.500 $**

Rechtsvergleich zwischen der DSGVO, dem CCPA und dem VCPA im Überblick

III. Datenstrom mit Hindernissen - die Problematik des EU-US-Datentransfers

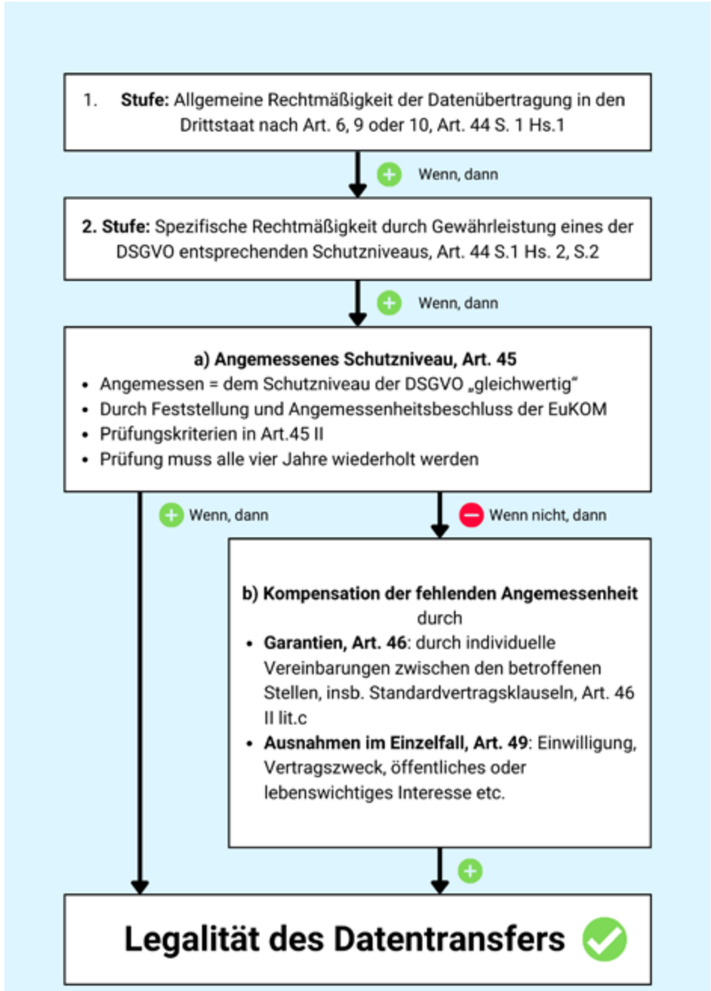
Es wird deutlich, dass bereits die generelle Systematik des US Privacy Laws in einem scharfen Kontrast zum hiesigen Datenschutz steht.[34] In der Literatur wird auch zwischen einem würde- und einem freiheitsbasierten Ansatz differenziert. Ersterer verweist auf den grundrechtlichen Charakter des europäischen Datenschutzes, der einen umfassenden und effektiven Schutz des Einzelnen in seinem Persönlichkeitsrecht verlange. Letzterer stelle wiederum nicht nur die Dispositionsfreiheit des US-Bürgers selbst, sondern auch die Freiheit der dortigen Gesellschaft und dritter Akteure in den Vordergrund, an persönlichen Daten schrankenlos teilhaben zu können.[35] Dass dieser Dissens in Zeiten des globalen Datenverkehrs zu Konflikten führen muss, ist bereits für sich genommen erwartbar. Zwei konkrete Besonderheiten verschärfen dies jedoch umso mehr.

31 Geschützt werden als personal informations „information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.", vgl. hier (Stand: 16.05.2022).
32 *Rippy*, Virginia passes the Consumer Data Protection Act, hier abrufbar, (Stand: 25.05.2022).
33 *Klosowski,* The State of Consumer Data Privacy Laws in the US (And Why It Matters), hier abrufbar (Stand: 25.05.2022).
34 Zur europäischen Dogmatik *Stark*, CTRL 1/2022, 87 ff.
35 Zur Unterscheidung *Lewinski,* Was Europa und die USA in Sachen Datenschutz unterscheidet, hier abrufbar (Stand: 25.05.2022).

1. General Protection vs. General Surveillance - die Ausgangslage

Wie bereits die Datenschutz-Richtlinie von 1995[36] (DS-RL) enthalten auch die geltenden Vorschriften Bestimmungen zum Transfer personenbezogener Daten in Nicht-EU-Länder, sog. Drittstaaten, Art. 44 ff.[37] Dabei gelten folgende Regeln: Mit dem Grundsatz der Gewährleistung eines angemessenen Schutzniveaus verlangt die DSGVO Geltung über die Grenzen der EU hinaus.[38] Statt der üblichen Lösung zwischenstaatlicher Rechtskollisionen über völkerrechtliche Vereinbarungen diktiert sie Drittstaaten ihren eigenen Datenschutzstandard als Maßstab. Dies entspricht zwar der generell protektiven Konzeption des EU-Datenschutzes, stellt aber den kommerziellen Datenverkehr vor erhebliche Herausforderungen.[39] Schließlich drohen bei Verstößen gegen die Art. 44 ff. Geldstrafen bis zu 20 Mio. € bzw. für Unternehmen bis zu 4 % des weltweit erzielten Jahresumsatzes, Art. 83 V lit. c.

Die andere Besonderheit liegt im US-Nachrichtendienstwesen. Im Gegensatz zur Inlandsüberwachung unterliegen auslandsnachrichtendienstliche Aktivitäten nicht den Anforderungen des vierten Amendments und auch nicht des ECPA. Rechtsgrundlage bezüglich der behördlichen Verarbeitung von Nicht-US-Bürgerdaten in den USA, und damit vor allem für die Überwachungsprogramme PRISM und UPSTREAM, ist der 1978 erlassene Foreign Intelligence Surveillance Act (FISA). Bereits seinerzeit mit großzügigen Eingriffsrechten der Behörden ausgestattet, erfuhr der FISA insbesondere nach 2001 noch weitere Anpassungen, welche die staatlichen Überwachungsbefugnisse erheblich ausgedehnt haben. Dass Dauer und Intensität der FIS-Eingriffe zumindest dem Zweck nach erforderlich und angemessen sein müssen, bleibt dabei die wichtigste materiellrechtliche Einschränkung.[40]



Zulässigkeitsprüfung der Drittstaatenübermittlung nach Art. 44-49 DSGVO

Nach Section 702 des FISA sind US-Telekommunikationsunternehmen gegenüber US-Sicherheitsdiensten ganz ohne richterliche Anordnung zur bedingungslosen Auskunft verpflichtet. Damit ist auch die Freigabe persönlicher Daten von Nicht-US-Bürgern aus Drittstaaten gemeint, soweit sie in die USA gelangen.[41] Zwar erfordern FIS-Maßnahmen die Zustimmung des FIS-Courts: einer Kammer aus unabhängigen Bundesrichtern, denen die US-Behörden gegenüber auskunftspflichtig sind. Allerdings genehmigt dieses Gericht nur die generelle Durchführung von Maßnahmen zu bestimmten Zwecken (zum Beispiel das Sammeln von Kontaktdaten deutscher Staatsbürger, die in Verbindung zu einem mutmaßlichen Terroristen stehen), nicht hingegen jede Datenerhebung oder -auswertung im Einzelfall.[42] Noch weitreichender zeigt sich die 1981 erlassene Executive Order 12333

36 Art. 25 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.
37 Alle Art. ohne weitere Bezeichnung sind solche der DSGVO.
38 Dieser heute in Art. 44 II kodifizierte Grundsatz ist dem EuGH-Urteil Schrems I geschuldet (s.u.). Art. 25 DS-RL zielte mit seiner *„Angemessenheit"* noch nicht auf die Gleichwertigkeit des Schutzniveaus ab, sondern ließ Qualitätsunterschiede der herrschenden Auslegung zufolge noch durchaus zu, vgl. *Rüpke/v. Lewinski /Eckhardt*, Datenschutzrecht. Grundlagen und europarechtliche Neugestaltung, 2018, 266 Rn. 13.
39 *Schweighofer*, Principles for US-EU Data Flow Arrangements, in: *Svantesson/Kloza*, Transatlantic data privacy relations as a challenge for democracy, 2017, 35.
40 *Solove/Schwartz*, Privacy Law Fundamentals, 2019, 57 ff.
41 *Karthäuser,* Und jetzt?, hier abrufbar (Stand: 25.05.2022).
42 CRS Report, EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield, 2021, 8 ff.

(EO 12333).[43] Präsident Reagan regelte darin die umfassenden Zugriffsrechte der US-Geheimdienste auf Nicht-US-Bürgerdaten außerhalb der USA. Denn dort entfaltet der FISA keine Wirkung und somit auch nicht seine Rechtsschutz- und Beschränkungsbestimmungen. Folglich ist der Zugriff auf persönliche Daten von Nicht-US-Bürgern, die auf dem Weg in die USA‘ sind, legal. Zudem ist er weniger Rechtsstaatsprinzipien unterworfen: Die EO 12333 kennt weder einen richterlichen Vorbehalt noch Einschränkungen über den Minimierungsgrundsatz hinaus.[44]

2. Transferabkommen, die Erste – Safe Harbor

Ihren ersten Angemessenheitsbeschluss i.S.d. heutigen Art. 45 I, III hinsichtlich den USA traf die Europäische Kommission im Jahr 2000, mit ihrer sog. Safe-Harbor-Entscheidung.[45] Dieser gingen jahrelange Verhandlungen mit der US-Administration voraus, weshalb auch von einem Abkommen die Rede ist. Einen völkerrechtlich verbindlichen Vertrag hat es indes nie gegeben.[46]

Nach Safe Harbor verpflichteten sich US-Unternehmen freiwillig, sieben bestimmte, an die Standards der DS-RL angelehnte Kriterien (‘Grundsätze’), sowie fünfzehn FAQs zu erfüllen und sich dabei der Kontrolle der FTC bzw. des US-Handelsministeriums zu unterstellen.[47] Dogmatisch erscheint es vertretbar, diese Bedingungen der Entscheidung als Garantie i.S.d. Art. 46 II[48] zu deuten.[49] Jedenfalls stellte die EuKOM die Angemessenheit des US-Datenschutzes bereits seinerzeit nicht bedenkenlos fest, ohne besondere Bedingungen an den Datentransfer zu stellen.

Bereits vor Schrems I wurde scharfe Kritik an der Entscheidung laut. Konkrete Anknüpfungspunkte waren maßgeblich die mangelhafte Überprüfung der Pflichtentreue[50], sowie die Tatsache, dass die Bestimmungen jedenfalls in der Praxis keine sonderliche Beachtung fanden.[51] Ganz erhebliche Kopfschmerzen bereitete, spätestens ab dem PRISM-Skandal 2015, zudem Abschnitt B des 4. Anhangs der Safe-Harbor-Abkommen. Dieser sah vor, dass “Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen (in den USA)“ stets Vorrang vor den Grundsätzen des Abkommens gehabt hätten. Dies bedeutet, dass US-Organisationen zur Datenweitergabe an US-Behörden verpflichtet blieben, auch wenn dies den Safe-Harbor-Anforderungen widersprach.[52] Oder ‚in a nutshell’: FISA brach Safe Harbor. Der EuGH traf in seinem Schrems I Urteil, angelehnt an Art. 25 DS-RL, nur wenige Aussagen zu den allgemeinen Anforderungen an ein Transferabkommen. Zunächst beschied er, dass ein “angemessenes Schutzniveau” zwar kein dem Unionsrecht identisches, wohl aber ein “der Sache nach Gleichwertig(es)” verlange, wobei die DS-RL sowie die GRCh als Maßstab gelten.[53] Diesem strengen Grundsatz folgend stellte er weiter fest, dass in Safe Harbor weder der Angemessenheit noch der Gewährleistung des Schutzniveaus Genüge getan wurde. Unangemessen

> „In a nutshell’:
> FISA brach Safe Harbor.“

erschienen die unbegrenzten US-dienstlichen Eingriffsrechte, welche das Abkommen sogar gänzlich verdrängen konnte.[54] Für eine ausreichende Gewährleistung fehle es wiederum sowohl an wirksamen Überwachungs- und Kontrollmechanismen bzgl. der praktischen Einhaltung der Selbstverpflichtungen,[55] als auch an hinrei-

43 Executive Order 12333, United States Intelligence Activities, hier abrufbar (Stand: 25.05.2022).
44 Übersicht zu den Ermächtigungen und Einschränkungen der EO 12333 hier abrufbar (Stand: 25.05.2022); zum verringerten Schutzniveau ggü. FIS-Maßnahmen vgl. EuGH, C-311/18, „Schrems II“, (Rn. 63, 183), hier abrufbar (Stand: 25.05.2022).
45 Dieser bezog sich, wie Privacy Shield, auf den Datentransfer privater Stellen. Der Datenaustausch zwischen Ermittlungsbehörden wurde in weiteren Abkommen wie dem Umbrella-Agreement v. 2015, dem PNR-Agreement v. 2016 sowie dem SWIFT-Agreement v. 2010 geregelt. Ersteres setzt zwar hohe Anforderungen, findet jedoch keine Anwendung auf privaten, insb. kommerziellen Datenverkehr, vgl. *Schweighofer,* Principles for US-EU Data Flow Arrangements, in *Svantesson/Kloza,* Transatlantic data privacy relations as a challenge for democracy, 2017, 38-40.
46 Ebd., 36.
47 *Paal/Pauly*, DSGVO u. BDSG, 3. Aufl. 2021, Rn. 9.
48 Zum Zeitpunkt des Safe-Harbor-Beschlusses geregelt in Art. 26 II DS-RL 95/46/EG.
49 So *Lewinski,* EuR 2016, 405 (408).
50 Mitteilung der Europäischen Kommission vom 27.11.2013, KOM (2013) 847 final(5).
51 BeckOK DatenschutzR BDSG aF/*Schantz,* § 4b, Rn. 32; *Schweighofer*, Principles for US-EU Data Flow Arrangements, in *Svantesson/Kloza*, Transatlantic data privacy relations as a challenge for democracy, 2017, 41.
52 EuGH, C-362/14, „Schrems I“, (Rn.86), hier abrufbar (Stand: 25.05.2022).
53 EuGH, C-362/14, „Schrems I“, (Rn.73), hier abrufbar (Stand: 25.05.2022).
54 EuGH, C-362/14, „Schrems I“, (Rn.86), hier abrufbar (Stand: 25.05.2022).
55 EuGH, C-362/14, „Schrems I“, (Rn.81), hier abrufbar (Stand: 25.05.2022).

chenden Rechtsschutzmechanismen bei bereits erfolgten, insbesondere staatlichen Eingriffen.[56] Generell habe die Kommission keine ausreichende Prüfung des US-Rechts vorgenommen. Diese Annahme genügte dem Gericht, um die Entscheidung der EuKOM, und damit die Rechtsgrundlage für einen beträchtlichen Teil des EU-US-Datentransfers, für insgesamt unwirksam zu erklären.[57]

3. Transferabkommen, die Zweite - Privacy Shield

Unter entsprechendem Druck trat, nur wenige Monate nach Schrems I und wiederholten Verhandlungen mit US-Vertretern, am 12.07.2016 das Privacy-Shield-Abkommen in Kraft. In sechs Artikeln, sieben Annexen und 155 Erwägungsgründen bemühte man sich, die wenigen Vorgaben aus Schrems I zufriedenstellend umzusetzen. Dabei hielten auch zahlreiche Erklärungen von US-Regierungsvertretern Einzug, die als mehr oder weniger verbindliche Versprechen gedeutet werden konnten. Während die materiellen Anforderungen Safe Harbors nunmehr als „Principles" in Privacy Shield weitestgehend übernommen wurden,[58] erfuhren Kontrolle und Rechtsschutz einige Erweiterungen. Dies entsprach der Gewichtung des Urteils. Hierfür war zum einen eine dem US-Außenministerium unterstellte Ombudsperson[59] vorgesehen, die auf Antrag europäischer Stellen hin tätig werden und mögliche Rechtsverletzungen prüfen sollte.[60] Zum anderen wurde ein verschärftes Kontrollrecht des US-Handelsministeriums und der FTC zugesichert, sowie eine beschränkte Klagebefugnis für Nicht-US-Bürger eingeführt.[61] Darüber hinaus wurden schriftliche Zusicherungen von US-Sicherheitsbehörden beigefügt, die Überwachungsaktivitäten gegenüber EU-Bürgern einzuschränken. Dabei spielte insbesondere ein Verweis auf die Presidential Policy Directive 28 (PPD-28) eine gewichtige Rolle. In letzterer wies der damalige Präsident Obama die US-Sicherheitsdienste unter anderem an, Ausländerüberwachungen nur auf einer rechtlichen Grundlage gestützt, auf das erforderliche und notwendige Maß beschränkt und nicht zu Zwecken der Diskriminierung von Meinungen und Personengruppen durchzuführen.[62]

Doch auch damit zeigte sich der bereits vor dem Erlass angerufene EuGH nicht zufrieden. Dabei wurde er in seiner Begründung zwar ausführlicher, in der Sache blieben die Kritikpunkte jedoch identisch. Erwartbar war die Bemängelung jener Klauseln, die den Sicherheitsinteressen der USA wiederholt Vorrang vor Privacy Shield einräumten. Diese fanden sich, trotz Schrems I, nahezu unverändert im neuen Abkommen wieder.[63] Auch gewährleiste der FISA zu wenig Einschränkungen der Datenzugriffs- und -verarbeitungsrechte und lege weder den Umfang noch die Tragweite der Überwachung fest. Damit fehlte es wiederholt an der Angemessenheit des Schutzniveaus.[64] Dies könne auch nicht durch die PPD-28 kompensiert werden: Zum einen räume diese betroffenen EU-Bürgern keine eigenen Rechte ein, wie es die Angemessenheit nach Art. 45 II lit. a verlange. Zum anderen gestatte sie Massendatenerhebungen, die einen hinreichenden Individualschutz erst gar nicht ermöglichen würden.[65] Auch der Ombudsmechanismus wurde bemängelt: Der Ombudsmann könne schon aufgrund seiner Abhängigkeit vom US-Außenministerium und der fehlenden Weisungsbefugnis gegenüber den Sicherheitsdiensten keinem gerichtlichen Kontrollorgan gleichkommen, wie es die DSGVO vorsehe.[66] Die altbekannte Folge: Unwirksamkeit des gesamten Beschlusses.[67]

4. Letzte Bastion - Standardvertragsklauseln

Ist nun jeder Datentransfer von hier nach Übersee rechtswidrig? Nein. Wie aus Abbildung 2 hervorgeht, verbleiben zwei Rechtfertigungsmöglichkeiten trotz Fehlen eines wirksamen Angemessenheitsbeschlusses. Art. 46 I erlaubt die genehmigungsfreie Übermittlung, soweit die EU-ansässigen Verantwortlichen in Kooperation mit ihren Partnern im Drittland geeignete Garantien schaffen, die

56 EuGH, C-362/14, „Schrems I", (Rn.89), hier abrufbar (Stand: 25.05.2022).
57 EuGH, C-362/14, „Schrems I", (Rn.98, 105), hier abrufbar (Stand: 25.05.2022).
58 Hier abrufbar (Stand: 16.05.2022).
59 Ombudsman ist eine unparteiische Schiedsperson; vgl. auch *Heinzke*, GRUR-Prax 2022, 436, 437.
60 *Brauneck*, EuZW 2020, 933, 935, hier abrufbar (Stand 25.05.2022).
61 Durch den 2016 erlassenen „Judicial Redress Act" (JRA), der jedoch nur gilt, soweit es um Strafverfolgungen geht, vgl. *Lewinski,* EuR 2016, 405 (414).
62 Auswahl von Maßnahmen des US-Gesetzgebers und der US-Regierung in Bezug auf die Überwachungstätigkeit der US-Geheimdienste seit Sommer 2013, BT-WD 3 - 3000- 150/15, S.6, hier abrufbar (Stand 25.05.2022).
63 EuGH, C-311/18, „Schrems II", (Rn.163 f.), hier abrufbar (Stand: 25.05.2022).
64 EuGH, C-311/18, „Schrems II", (Rn.176, 180), hier abrufbar (Stand: 25.05.2022).
65 EuGH, C-311/18, „Schrems II", (Rn.181, 183 f.), hier abrufbar (Stand: 25.05.2022).
66 EuGH, C-311/18, „Schrems II", (Rn.190 ff.), hier abrufbar (Stand: 25.05.2022).
67 EuGH, C-311/18, „Schrems II", (Rn.199), hier abrufbar (Stand: 25.05.2022).

das mangelhafte gesetzliche Schutzniveau vertraglich kompensieren. Um nun nicht jedwede Verantwortung auf die Verarbeiter abzuwälzen, hat die EuKOM bereits vor langem Musterverträge, sog. Standardvertragsklauseln (SVK) i.S.d. Art. 6 II lit c, vorgegeben.[68] Durch sie verpflichten sich die Verarbeiter dies- und jenseits des Atlantiks, freiwillig Datenschutzmaßnahmen einzuhalten, die den strengen Anforderungen der DSGVO genügen. Andernfalls drohen Unterlassungs- und Schadensersatzansprüche. So gilt nach Klausel 8 der SVK bspw. das Zweckbindungs-, Transparenz- und Richtigkeitsgebot.[69]

Die gute Nachricht: der EuGH hat die SVK in ihrer bestehenden Form grundsätzlich für zulässig erklärt.[70] Allerdings sei der Verantwortliche verpflichtet, vorab das Schutzniveau des Drittlands nach den Umständen des Einzelfalls zu überprüfen. Sollte er zu dem Ergebnis kommen, dass es nicht angemessen sei, habe der Datenexporteur den Transfer auszusetzen, der Importeur die bereits übermittelten Daten sogar zu vernichten.[71] Ende 2021 erneuerte daraufhin die EuKOM die SVK und führte Klausel 14 und 15 ein. Letztere sieht vor, dass der Datenimporteur im Falle eines Auskunftsersuchens von US-Behörden diese auf ihre Rechtmäßigkeit hin zu prüfen, den Exporteur und den Betroffenen zu informieren und gegen das Ersuchen vorzugehen hat. In Klausel 14 ist wiederum die oben genannten Prüfungspflicht statuiert, das sog. Transfer Impact Assessment (TIA). In dieser sind die geltenden Rechtsvorschriften und Gepflogenheiten des Drittstaates zu berücksichtigen. Dabei legen Wortlaut und Begründung[72] nahe, dass auch eine evidenzbasierte Risikoberechnung erfolgen darf. Es könnte also genügen, dass nur die Wahrscheinlichkeit eines behördlichen Datenzugriffs nachweislich gering ist, auch wenn er rechtlich möglich ist.[73] Hierfür wurden bereits eigene mathematische Verfahren entwickelt, um eben diese Risikobestimmung zu ermöglichen.[74] Neben erheblichen praktischen Problemen der Quantifizierung stellt sich dabei aber die drängende Frage, ob dies als "der Sache nach gleichwertig" zum europäischen Schutzniveau gelten darf. Denn auch das geringe Risiko eines nach der DSGVO unrechtmäßigen Zugriffs wird, so er nach US-Recht legal wäre, dem Unionsrechtsstandard nicht gerecht. Eben diese Streitfrage bietet echtes Potenzial für ein Schrems-III-Urteil.[75] Zudem können EU-Aufsichtsbehörden SVKs jederzeit kippen, sollten ihnen Zweifel am angemessenen Schutzniveau aufkommen.[76]

Ohne SVK verbleibt nur noch die ausnahmsweise Rechtfertigungen nach Art. 49, der jedoch für spezifische Einzelfälle konzipiert wurde und daher für den relevanten Massendatenverkehr keine geeignete Rechtsgrundlage darstellt.

B. Über den Nutzen globaler Regeln auf globalen Märkten - Conclusion

Es ist unumstößlich: Der EU-US-Datentransfer benötigt einen wirksamen Angemessenheitsbeschluss der EuKOM. Eine Abwälzung von Prüfungspflicht und Haftung auf Verantwortliche i.S.d. DSGVO mittels Standardvertragsklauseln geht nicht nur mit einer erheblichen Belastung für zahlreiche Private, insb. kleine u. mittelständische Unternehmen, einher: Sie steht auch, wie gezeigt, auf tönernen Füßen. Dies gilt vor allem dann, wenn es um die hochrelevanten Massendatenübermittlungen an Dienstleister wie Meta Platforms (früher: Facebook) oder Alphabet geht. Denn gerade diese Unternehmen unterliegen nach FISA Section 702 und der EO 12333 jenen staatlichen Zugriffsrechten, die nicht nur nach US-Recht durchaus möglich, sondern nur schwerlich vertraglich abdingbar sind. Von der prinzipiellen Kontrollproblematik unüberschaubarer Datenströme mal ganz zu schweigen. Eine Unterbrechung der Datentransfers hätte wiederum ungeahnte wirtschaftliche Schäden zur Folge.[77] Was also ist die Lösung des Problems? Hält man die aufgezeigten Widersprüche zwischen dem EU-Datenschutz und dem US-Privacy-Kon-

68 *Scholl*, Die neuen Standardvertragsklauseln: Eine Bestandsaufnahme, hier abrufbar (Stand: 25.05.2022).
69 Aktuelle Fassung hier abrufbar (Stand: 25.05.2022).
70 EuGH, C-311/18, „Schrems II", (Rn. 148), hier abrufbar (Stand: 25.05.2022).
71 EuGH, C-311/18, „Schrems II", (Rn. 142 ff.), hier abrufbar (Stand: 25.05.2022).
72 *„Zur Ermittlung der Auswirkungen derartiger Rechtsvorschriften und Gepflogenheiten auf die Einhaltung dieser Klauseln können in die Gesamtbeurteilung verschiedene Elemente einfließen. Diese Elemente können einschlägige und dokumentierte praktische Erfahrungen im Hinblick darauf umfassen, ob es bereits früher Ersuchen um Offenlegung seitens Behörden gab, die einen hinreichend repräsentativen Zeitrahmen abdecken, oder ob es solche Ersuchen nicht gab. […] Sofern anhand dieser praktischen Erfahrungen der Schluss gezogen wird, dass dem Datenimporteur die Einhaltung dieser Klauseln nicht unmöglich ist, muss dies durch weitere relevante objektive Elemente untermauert werden."*, vgl. hier (Stand: 25.05.2022).
73 Zur Deutung der Begründung *Diercks/Roth*, Data Transfer to unsafe Third Countries, hier abrufbar (Stand: 16.05.2022).
74 *Kötter*, Drittland Übermittlung: Leitfaden zu Transfer Impact Assessments, hier abrufbar (Stand: 25.05.2022).
75 So in: EU-Kommission verabschiedet DSGVO-Standardvertragsklauseln, hier abrufbar (Stand: 25.05.2022).
76 *Karthäuser*, Und jetzt?, hier einsehbar (Stand: 25.05.2022).
77 Nach einer Studie des *ECIPE* aus 2013 hätte das BIP der EU seinerzeit durch eine Unterbrechung des kommerziellen Datentransfers in die USA um bis zu 1,3 % zusammenbrechen können, vgl. *ECIPE*, The Economic Importance of getting Data Protection Right, 2013, 3.

zept für unüberwindbar, verbleibt nur noch eine Option: eine ausschließlich auf europäischem Boden stattfindende Verarbeitung von EU-Bürgerdaten, gänzlich umschlossen vom Schutzbereich der DSGVO. So fordern es auch Schrems und seine Organisation NOYB.[78] Ob dieser radikale Einschnitt indes erforderlich ist, erscheint zweifelhaft. Zunächst einmal ist festzustellen, dass sowohl die USA als auch die EU demokratische Rechtsstaaten sind.[79] Wenn schon die Kollision zwischen diesen beiden Rechtsräumen nicht gelöst werden kann, wie soll es dann erst mit anderen Handelspartnern, insbesondere aus Südostasien gelingen, denen der westliche Persönlichkeitsschutz oftmals gänzlich fremd ist?[80] Solche Begegnungen sind jedoch in Zeiten des notwendigerweise globalen Datenverkehrs unvermeidbar. Dies wirft die Frage auf, ob die strenge Angemessenheitskontrolle des EuGH bezüglich Drittstaaten überhaupt weiter Bestand haben kann oder sollte.[81] Auch empirische Erhebungen zur wirtschaftlichen Wirkung des Datenschutzes zeigen, dass strengere Regeln den Freihandel sowie die Produktivität insbesondere mittelständischer Unternehmen erheblich beeinträchtigen.[82]

Reformbedarf besteht also hier wie da. Einige Probleme sind, wie aufgezeigt, systemspezifisch. In den USA sind dies vor allem die Unvollständigkeit des Datenschutzes, die damit eröffnete Möglichkeit der anlasslosen staatlichen Massenüberwachung und Rechtsunsicherheiten aufgrund des sektoralen Ansatzes, sowie die in den einzelnen Bundesstaaten divergierenden Rechtslagen. In der EU bereiten wiederum mangelnde Flexibilität, teils enorme bürokratische Anforderungen sowie die Wachstums- und Wettbewerbsbeeinträchtigung durch die DSGVO Kopfschmerzen.[83] Ob nun nach europäischer Opt-In- oder kalifornischer Opt-Out-Lösung: in beiden Fällen handeln Betroffene, Studien zufolge, alles andere als rational. Meistens sind sie von Datenschutzaufklärungen überfordert und widersprechen in ihren Handlungen den zuvor angegebenen Intentionen.[84] Man denke nur an die eigenen Erfahrungen mit sog. ‘Cookie-Bannern’ auf diversen Webseiten.

Die wirksamste Lösung für alle genannten Herausforderungen wäre also die Einführung eines gemeinsamen, optimierten Datenschutzstandards. Durch diesen würden nicht nur endlich Rechtssicherheit und wettbewerbsfreundliche Bedingungen zwischen den USA und der EU geschaffen werden.[85] Man könnte dies zum Anlass nehmen, die in beiden Rechtsregimen bekannten rechtlichen und tatsächlichen Mängel anzugehen. Hierbei könnten die USA von der EU lernen, wie Einheitlichkeit, effektive Kontrolle und auch Abwehrrechte im Datenschutz gewährleistet werden können. Umgekehrt kann die US-amerikanische Ausdifferenzierung des Datenbegriffs mehr Flexibilität in die starre DSGVO bringen. Gemeinsam könnten Konzepte entwickelt werden, die die gemeinsamen Probleme der Effektivität und der ungewollten Folgen lösen. Traumtänzerei muss dies langfristig nicht bleiben: der zunehmende Druck des EuGH, die weiterhin enorme wirtschaftliche Bedeutung des transatlantischen Handels und nicht zuletzt die Internationalität des Datenverkehrs per se lassen einen multilateralen Standard naheliegend erscheinen. Die Hürden bleiben indes hoch: hier wie da müssten mittels umfangreicher Reformen gesetzgeberische Kompromisse gemacht werden. Der Wille dazu ist auf beiden Seiten noch nicht erkennbar. Naheliegender erscheint ein bilateraler Vertrag, der die DSGVO-Anforderungen bindend erfüllt, ohne die Substanz des US-Rechts zu tangieren. Auf diesem Weg könnten gezielt für persönliche Daten von EU-Bürgern verbindliche völkerrechtliche Vertragsrechtsstandards eingeführt werden, die (auch) die USA zu berücksichtigen haben. Diese könnten überdies, im Gegensatz zum Administrativrecht der US-Regierung (wie im Privacy Shield vorgesehen) nicht ohne weiteres aufgehoben werden und wären daher erheblich standfester als die bisherigen Regelungen.[86]

78 So Schrems gegenüber *WELT* am 16.07.2020, hier abrufbar (Stand 25.05.2022).
79 So auch *Swire,* US Surveillance Law, Safe Harbour and Reforms since 2013, in *Svantesson/Kloza,* Transatlantic data privacy relations as a challenge for democracy, 2017, 86 ff.; sowie: Why U.S. Surveillance Law Protections Are Better Than Europe Thinks, 2015, hier abrufbar (Stand: 25.05.2022).
80 So auch *Lewinski*, Was Europa und die USA in Sachen Datenschutz unterscheidet, hier abrufbar (Stand: 25.05.2022).
81 Derzeit gewährleisteten nach Feststellung der Europäischen Kommission nur Andorra, Argentinien, die Schweiz, die Färöer-Inseln, Guernsey, Isle of Man, Jersey, Neuseeland und Uruguay sowie eingeschränkt Kanada und Israel das nach Art. 45 I erforderliche Schutzniveau, vgl. *Kühling/Klar/Sackmann:* Datenschutzrecht. 5. Aufl. 2021, 251 Rn. 59; andererseits geht die Theorie des sog. Brussels Effect davon aus, dass sich internationale Rechtsordnungen zunehmend dem Standard des EU-Rechts anpassen werden, *vgl. Bradford,* The Brussels Effect, 107 Nw. U. L. Rev.1-67, 2012.
82 *ECIPE,* The Cost of Data Protection, 2018, hier abrufbar (Stand 25.05.2022).
83 Dazu *Stark,* CTRL 1/2022, 95 ff.
84 *Acquisti/Grossklags,* Privacy and Rationality, in: Strandburg/Raicu, Privacy and Technologies of Identity, 2008, 15, 17 f, 27; *Nissenbaum*, Privacy in Context, 2010, 129 ff.
85 So auch, wenngleich auf die Regulierung von Profilbildung- und nutzung durch soziale Netzwerke beschränkt, *Kühnl,* Persönlichkeitsschutz 2.0: Profilbildung und -nutzung durch soziale Netzwerke am Beispiel von Facebook im Rechtsvergleich zwischen Deutschland und den USA, 2016, 314 f., 316.
86 So *Schweighofer,* Principles for US-EU Data Flow Arrangements, in Svantesson/Kloza, Transatlantic data privacy relations as a challenge for democracy, 2017, 44 f.

Am 25. März 2022 erklärten US-Präsident Biden und EU-Kommissionspräsidentin von der Leyen in einer gemeinsamen Pressekonferenz in Brüssel, dass ein neues Datentransferabkommen abgeschlossen worden sei.[87] Die Ausgestaltung ist derzeit noch unbekannt. Zwei Erfahrungssätze aber haben die Parteien aus dem bisher Geschehenen in jedem Fall zu berücksichtigen: beschränkt verbindliche Transferabkommen mit Hintertüren für US-Nachrichtendienste und beeinträchtigtem Rechtsschutz werden nach Unionsrecht auch künftig unwirksam bleiben. Zum anderen: sollte eine – durchaus wünschenswerte – Reform des Datenschutzrechts dies- oder jenseits des Atlantiks doch einmal zur Debatte stehen, führen wir sie am besten gemeinsam.

Talking Legal Tech – Folge 28

„Regulierung & Innovation - wie lässt sich beides vereinbaren, Martin Ebers?“

87 Vgl. die Erklärung der Präsidentin *von der Leyen* mit US-Präsident Biden vom 25.03.2022, hier abrufbar (Stand: 25.05.2022).

Aufsatz

Digitale Dokumentation der strafgerichtlichen Hauptverhandlung

Maria Osmakova

Maria Osmakova hat kürzlich ihr Studium der Rechtswissenschaften mit strafrechtlichem und kriminologischem Schwerpunkt an der Universität zu Köln beendet. Sie ist wissenschaftliche Mitarbeiterin bei Heuking Kühn Lüer Wojtek im Dezernat Arbeitsrecht.

Open Peer Review

Dieser Beitrag wurde lektoriert von: Isabel Ecker und Hanna Brinkmann

Die digitale Dokumentation der strafgerichtlichen Hauptverhandlung wird kommen.[1] Dies hat der Bundesjustizminister Dr. Marco Buschmann in einer Rede vom April 2022 erneut bestätigt.[2] Die Möglichkeit oder Pflicht zur audiovisuellen Aufzeichnung der Hauptverhandlung im Strafprozess ist schon seit Jahren in Diskussion,[3] in der Umsetzung ist man jedoch noch nicht weit gekommen. Dies soll sich nun durch

1 *Mosbacher,* ZRP 2021, 180 (180): es gehe nicht mehr um das „Ob", sondern nur noch um das „Wie".
2 Video-Grußwort des Bundesministers der Justiz Dr. Marco Buschmann vom 28. April 2022, hier abrufbar (Stand: 31.05.2022).
3 Siehe nur *Barthel,* StV 2018, 678 ff.; *von Galen,* StraFo 2019, 309 ff.; *Schmitt,* NStZ 2019, 1 ff.; *Traut/Nickolaus,* StraFo 2020, 100 ff., *Traut/Nickolaus,* StraFo, 2022, 55 ff.; *Mosbacher,* ZRP 2019, 158 ff., *Mosbacher*, ZRP, 2021, 180 ff. mwN; *Fischer, Thomas*, Dient die Aufzeichnung im Gericht der Wahrheitsfindung? in: Legal Tribune Online, 22.06.2022, hier abrufbar (Stand 01.07.2022).

eine Reform ändern, die darauf abzielt Strafprozesse „effektiver, schneller, moderner und praxistauglicher“[4] zu machen. Ein Gesetzesentwurf des Bundesministeriums der Justiz (BMJ) wurde für Mitte dieses Jahres angekündigt.[5] Wie genau die Aufzeichnung der strafgerichtlichen Hauptverhandlung ausgestaltet werden kann und welche Chancen und Risiken sie birgt, wird im folgenden Beitrag näher beleuchtet.

A. Stand der Digitalisierung im Prozessrecht

Zunächst lohnt sich ein allgemeiner Blick auf den Stand der Digitalisierung in den verschiedenen Gerichtssälen Deutschlands.

I. Im Strafverfahren

Die Digitalisierung hat im Strafverfahren derzeit nur marginal Einzug gefunden. Es wäre angemessener von einer Technologisierung zu sprechen, nämlich von der Durchführung des Strafverfahrens mit technischen Hilfsmitteln.

Im Ermittlungsverfahren kann die Vernehmung des Beschuldigten durch Richter[6], Polizei oder Staatsanwaltschaft in Bild und Ton aufgezeichnet werden, §§ 136 Abs. 4 S. 1, 163a Abs. 4 S. 2 StPO. Eine Pflicht zur Aufzeichnung besteht, wenn dem Ermittlungsverfahren der Verdacht eines vorsätzlichen Tötungsdeliktes zugrunde liegt und weder äußere Umstände noch die besondere Dringlichkeit der Vernehmung entgegenstehen, § 136 Abs. 4 S. 2 Nr. 1 StPO.[7] Wird gegen den Beschuldigten Anklage erhoben, kann die Aufzeichnung in der Hauptverhandlung nur zum Zwecke der Beweisaufnahme über ein Geständnis oder, wenn ein Widerspruch zu einer früheren Aussage nicht anders festgestellt werden kann, vorgeführt werden, § 254 StPO. Ansonsten muss der Angeklagte aufgrund des Unmittelbarkeitsgrundsatzes nach § 250 StPO direkt vernommen werden, wobei seine Aussage nicht durch die Aufzeichnung aus dem Ermittlungsverfahren ersetzt werden darf.[8]

Auch Zeugenvernehmungen können audiovisuell aufgezeichnet werden, §§ 58a, 58b StPO. Dabei kann die persönliche Vernehmung in der Hauptverhandlung grundsätzlich nicht durch das Abspielen der Aufnahme ersetzen werden, § 255a Abs. 1, §§ 250 – 253 StPO.[9] Ausnahmsweise ist die Aufzeichnung einer Zeugenvernehmung gem. § 58a Abs. 1 S. 2 Nr. 1 StPO zur Wahrung von schutzwürdigen Interessen Minderjähriger, die durch eine schwere Straftat[10] verletzt worden sind, verpflichtend. Eine solche Aufzeichnung kann die erneute persönliche Vernehmung in der Hauptverhandlung ersetzen, § 255a Abs. 2 StPO.[11] Besteht die Gefahr eines schwerwiegenden Nachteils für das Wohl des Zeugen, kann er physisch getrennt, also in einem anderen Raum, vernommen werden, wobei die Vernehmung zeitgleich in Bild und Ton in den Sitzungssaal übertragen wird, § 247a StPO.[12]

Aufzeichnungspflichten bestehen somit nur in Einzelfällen. Darüber hinaus können technische Hilfsmittel zwar eingesetzt werden; es macht jedoch wenig Sinn von ihnen Gebrauch zu machen, wenn sie meist eine erneute Aussage im Prozess nicht zu verhindern vermögen. Eine rechtliche Grundlage für eine umfassende Aufzeichnung der gesamten Hauptverhandlung zum Zwecke der Dokumentation und Sicherung der Aussagen und des Prozesses besteht zurzeit nicht, weder auf freiwilliger noch verpflichtender Basis.

4 Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP, „Mehr Fortschritt wagen“, S. 85, hier abrufbar (Stand 31.05.2022).
5 Video-Grußwort des Bundesministers der Justiz Dr. Marco Buschmann vom 28. April 2022, hier abrufbar (Stand: 31.05.2022).
6 Zum Zwecke der besseren Lesbarkeit wird bei personenbezogenen Hauptwörtern nur die männliche Form verwendet. Umfasst sind Menschen jeglicher Geschlechtsidentität.
7 Sie muss auch dann aufgezeichnet werden, wenn die schutzwürdigen Interessen von Beschuldigten, die erkennbar unter eingeschränkten geistigen Fähigkeiten oder einer schwerwiegenden seelischen Störung leiden, durch die Aufzeichnung besser gewahrt werden können, § 136 Abs. 4 S. 2 StPO.
8 Vgl. KK-StPO/*Diemer*, 8. Aufl., § 250 Rn. 4.
9 Vgl. *Schork*, in: Dölling/Duttge/König/Rössner, Gesamtes Strafrecht StPO, 4. Aufl., § 255a Rn. 3.
10 §§ 58a Abs. 1 S. 2 Nr. 1, 255a Abs. 2 S. 1 StPO: Straftaten gegen die sexuelle Selbstbestimmung (§§ 174-184k StGB), gegen das Leben (§§ 211-212 StGB), gegen die persönliche Freiheit (§ 232-233a StGB) und Missbrauch von Schutzbefohlenen (§ 225 StGB).
11 Eine ergänzende Vernehmung des Zeugen bleibt jedoch zulässig, § 255a Abs. 2 S. 4 StPO.
12 Vollständigkeitshalber sei auf die komplementäre Norm für das Ermittlungsverfahren hingewiesen, § 168e StPO.

II. Andere Rechtszweige

Zwar können Tonaufnahmen gemäß § 169 Abs. 2 S. 1 GVG bei allen Gerichtsverhandlungen zu wissenschaftlichen und historischen Zwecken zugelassen werden, wenn es sich um ein Verfahren von herausragender zeitgeschichtlicher Bedeutung für die Bundesrepublik Deutschland handelt. Unabhängig davon, dass diese Vorschrift in der Praxis kaum Anwendung findet, ist sie auch nicht zielführend, da die Aufzeichnungen gemäß § 169 Abs. 2 S. 3 GVG kein Akteninhalt werden und nicht für Zwecke des aufgenommenen Verfahrens verwendet werden dürfen.[13] Das bedeutet, dass die Aufzeichnungen den Verfahrensbeteiligten im laufenden Prozess nicht zugänglich sind, sondern lediglich zu geschichtlichen Archivierungszwecken angefertigt werden.

In den anderen Rechtszweigen, also der Zivil-, Sozial-, Arbeits- Verwaltungs-, und Finanzgerichtsbarkeit können Aussagen der Parteien durch Tonaufnahmen dokumentiert werden.[14] Von einer solch auditiven oder audiovisuellen Dokumentation des Gerichtsprozesses bei Anwesenheit aller Beteiligten sind virtuelle Gerichtsverhandlungen zu unterscheiden, in denen sich die Parteien per Videostream in den Gerichtssaal zuschalten. Prozesse per Videokonferenz erfreuen sich seit der Corona-Pandemie immer größerer Beliebtheit. Grundlage hierfür ist § 128a ZPO.[15] Eine ausschließlich digital geführte Verhandlung ist im Strafverfahren nicht vorgesehen und würde mit dem Unmittelbarkeits- und Mündlichkeitsgrundsatz nach §§ 250, 261 StPO konfligieren. Bevor die Option einer Online-Hauptverhandlung diskutiert wird, sollte zunächst das Niveau der Digitalisierung im Strafverfahren auf den europäischen Standard angehoben werden.

13 *Traut/Nickolaus*, StraFo 2020, 100 (102).
14 Näher *Mosbacher*, ZRP 2019, 158 (158).
15 Zur Vertiefung empfiehlt sich der Beitrag *Paschke*, CTRL 1/22, S. 80 ff.

III. Strafprozesse im Ausland

Eine digitale Dokumentation der Hauptverhandlung ist im europäischen Ausland überwiegend Alltag. In Dänemark, Estland, Frankreich, Irland, Litauen, Rumänien und Tschechien ist die akustische Aufzeichnung der Hauptverhandlung erst ab zweiter Instanz verpflichtend. In den meisten Fällen erfolgt eine automatische Transkription, die den Staatsanwälten und Verteidigern teils unverzüglich, teils erst nach Einlegung von Rechtsmitteln zur Verfügung gestellt wird. In Spanien und Lettland ist die akustische und visuelle Aufzeichnung Pflicht. Gerichte in Schweden müssen ihre Verhandlungen entweder akustisch oder audiovisuell dokumentieren. In Portugal, Slowenien und der Slowakei besteht die Möglichkeit einer akustischen oder audiovisuellen Aufzeichnung, die zumindest bei größeren Verhandlungen öfters genutzt wird. Erstaunlich ist, dass die Digitalisierung des Strafprozesses im Ausland kein neues Phänomen ist und die Pflicht zur digitalen Dokumentation teilweise schon 2001 eingeführt wurde. Lediglich in Belgien, Deutschland[16] und Griechenland findet keine Aufzeichnung oder Transkription der gesamten Hauptverhandlung statt.[17]

B. Wann kommt endlich die Reform?

Die Frage, wann Hauptverhandlungen in Deutschland automatisch digital dokumentiert werden, ist somit mehr als berechtigt. Die Einführung technischer Aufzeichnungspflichten der Hauptverhandlung wurde in den vergangenen Legislaturperioden, trotz einiger Gesetzesentwürfe und Expertenkommissionen[18] versäumt. Dieses Versäumnis will die neue Ampel-Koalition nun nachholen. Im Koalitionsvertrag der Ampel-Parteien heißt es: „Wir machen Strafprozesse noch effektiver, schneller, moderner und praxistauglicher, ohne die Rechte der Beschuldigten und deren Verteidigung zu beschneiden."[19] Laut dem Bundesjustizminister folgt daraus unter anderem die Vorführung von aufgezeichneten Zeugenvernehmungen aus dem

16 Zur Situation in Deutschland siehe D. I.
17 *Von Galen*, StaFo 2019, 309 (311 ff.).
18 Ebd., S. 316; siehe auch Fn. 3.
19 Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP, „Mehr Fortschritt wagen", S. 85, hier abrufbar (Stand 31.05.2022).

Ermittlungsverfahren in der Hauptverhandlung und die digitale Dokumentation der Hauptverhandlung.[20] Einen entsprechenden Gesetzesentwurf kündigte Bundesjustizminister Marco Buschmann für Mitte des Jahres 2022 an.[21]

Wie genau die digitale Dokumentation im Gesetzesentwurf ausgestaltet wird, bleibt abzuwarten. Der im Koalitionsvertrag vorgesehene Digitalpakt für die Justiz beinhaltet eine Pflicht zur Aufzeichnung von Vernehmungen und Hauptverhandlung in Bild und Ton, also audiovisuell.[22] Ob das Gesprochene zusätzlich transkribiert werden soll, ist unklar. Alternativ könnte der Entwurf die Empfehlung der Expertengruppe,[23] welche 2020 vom BMJV eingesetzt wurde, umsetzen und die Pflicht zu einer bloßen auditiven Aufzeichnung ohne Bild mit automatischer Transkription einführen. Zusätzlich kann die Aufzeichnung flächendeckend oder nur für Verfahren vor dem Landgericht und/oder dem Oberlandesgericht eingeführt werden.

C. Die digitale Dokumentation der Hauptverhandlung

Wieso ist eine digitale Dokumentation der strafgerichtlichen Hauptverhandlung notwendig und wichtig?

I. Notwendigkeit

Einfach ausgedrückt: Die Handgelenke der Richter sollen entlastet werden. Oder die Finger, falls sie sich beim Mitschreiben eines Laptops bedienen. Denn so sieht es zurzeit an den Landgerichten und Oberlandesgerichten in Deutschland aus. Richter schreiben jede Aussage handschriftlich mit, um bei der Urteilsfindung die Aussagen der Zeugen zu berücksichtigen oder sich auf sie stützen zu können. Die Richter haben anderweitig keine Möglichkeit nachzuvollziehen, was zu welchem Zeitpunkt von welcher Person ausgesagt wurde. Dahinter steckt ein strukturelles Problem: Das Protokoll der Hauptverhandlung muss nach § 273 Abs. 1 StPO den Gang und die Ergebnisse der Hauptverhandlung wiedergeben. Davon sind allerdings nicht die Ergebnisse der Beweisaufnahme, also unter anderem die Aussagen von Zeugen oder des Angeklagten, erfasst[24], sondern nur die wesentlichen Verfahrensvorgänge[25]. Ein Wortprotokoll gibt es nicht.[26] Bei Verfahren vor dem Amtsgericht, also solche Verfahren mit einer Straferwartung von maximal zwei Jahren, wird immerhin ein sog. Inhaltsprotokoll angefertigt, in dem die wesentlichen Ergebnisse der Zeugenaussagen zusammengefasst werden, § 273 Abs. 2 StPO.[27] Bei Verfahren vor dem Landgericht und Oberlandesgericht wird nur das sog. Ereignisprotokoll nach § 273 Abs. 1 StPO angefertigt. Darin findet sich nicht mehr als der Hinweis „Der Zeuge sagte zur Sache aus“.[28] Somit fehlt es derzeit an einer lückenlosen Dokumentation der Hauptverhandlung, in der Aussagen von Zeugen zuverlässig und objektiv dokumentiert werden.[29] Dieser Missstand führt dazu, dass wenn sich Richter bei ihrer Urteilsbegründung auf die Aussage eines Zeugen oder des Angeklagten stützen wollen, sie die Details der Aussage in ihren selbst verfassten Notizen nachlesen müssen. Dass die Mitschrift der Richter von Unvollständigkeiten geprägt sein kann, erscheint nur menschlich. Dabei geht es nicht nur um Probleme der Vollständigkeit, sondern auch um subjektive Wahrnehmungen. Da es nicht möglich ist die Aussagen wortgleich mitzuschreiben, muss sie in den Notizen verkürzt oder zusammengefasst niedergeschrieben werden. Diese können von anderen Richtern im Spruchkörper, oder dem Richter selbst zu einem späteren Zeitpunkt im Verfahren anders interpretiert werden als zum Zeitpunkt der Mitschrift. Bei allem Bemühen um Objektivität, gestaltet sich die Mitschrift als Aufgabe, bei der sich Fehler und selektive Wahrnehmungen aus der Natur des Menschen und aus der erforderlichen Teilung der Aufmerksamkeit nicht immer vermeiden lassen.[30]

20 Video-Grußwort des Bundesministers der Justiz Dr. Marco Buschmann vom 28. April 2022, hier abrufbar (Stand: 31.05.2022).
21 Ebd.
22 Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP, „Mehr Fortschritt wagen“, S. 85, hier abrufbar (Stand 31.05.2022).
23 Bericht der Expertinnen- und Expertengruppe zur Dokumentation der strafgerichtlichen Hauptverhandlung, S.16, hier abrufbar (Stand: 31.05.2022); siehe zusammenfassend auch *Mosbacher,* ZRP, 2021, 180 (180).
24 *Schmitt,* NStZ 2019, 1 (2).
25 Siehe näher MüKO-StPO/*Valerius*, 1. Aufl., § 273 Rn. 7, 25 ff.
26 *Traut/Nickolaus*, StraFo 2022, 55 (56).
27 *Schmitt*, NStZ 2019, 1 (2); *Traut/Nickolaus*, StraFo 2022, 55 (56).
28 *Schmitt*, NStZ 2019, 1 (2).
29 *Traut/Nickolaus*, StraFo 2022, 55 (56).
30 *Schmitt,* NStZ 2019, 1 (5); zum „confirmation bias“ und „hindsight bias“ siehe *Traut/Nickolaus,* StraFo 2020, 100 (103).

II. Chancen

Eine Aufzeichnung würde also eine objektivere Grundlage der Dokumentation des Beweisverfahrens schaffen. Dabei würden nicht nur die Richter entlastet werden, indem sie ihre volle Aufmerksamkeit auf das Geschehen lenken können.[31] Die Aufzeichnungen oder/und die Transkriptionen wären auch für die übrigen Verfahrensbeteiligten wie Staatsanwaltschaft und Verteidigung bei der Vorbereitung weiterer Verhandlungstage oder Rechtsmittel hilfreich. Denn auch sie haben keine Möglichkeit im laufenden Verfahren oder im Nachgang die Aussagen zu rekonstruieren außer durch ihre eigenen Mitschriften. Eine Aufzeichnung bietet ebenfalls eine objektive Grundlage für Vorhalte, die direkt im Verfahren erhoben werden könnten, sodass widersprüchliche Aussagen oder Missverständnisse schneller und einfacher aufgeklärt werden können.[32]

Die durch das BMJ eingesetzte Expertengruppe bestehend aus Vertretern der Justiz und Verbänden der Anwaltschaft sieht die technische Dokumentation der Hauptverhandlung als verbesserte Grundlage für die Nachvollziehbarkeit der Hauptverhandlung im Hinblick auf die richterliche Überzeugungsbildung.[33] Sie trage dazu bei, kognitiv bedingte Fehler zu vermeiden und diene so der Wahrheitsfindung. Man könnte die Einführung sogar als eine aus rechtsstaatlicher Sicht gebotene Reform bezeichnen.[34]

Auf die für sich genommen schon kuriose Praxis des Mitschreibens trifft eine weitere strukturelle Eigenheit des deutschen Strafprozessrechts: Bei Verbrechen, die in erster Instanz vor dem LG oder OLG verhandelt werden, also Schwerstkriminalität wie Totschlag, Mord oder Staatsschutzdelikten fehlt es an einer zweiten Tatsacheninstanz. Eine Berufung ist grundsätzlich nicht möglich, es bleibt allein die Revision zum BGH. Beim BGH findet keine zweite Beweiserhebung statt, er befasst sich nur mit Rechtsfragen. Auf diese Weise gewinnt die Aufzeichnung solcher Verfahren nicht nur mit Blick auf die Dauer des Prozesses und der Vielzahl an Zeugenaussagen mehr Relevanz, sondern auch dadurch, dass die Tatsachen im ersten Urteil endgültig festgestellt werden.[35]

III. Risiken

Die Hauptverhandlung könnte durch die Aufzeichnung eine Menge an Qualität hinzugewinnen. Doch welche Risiken birgt sie? Zunächst ist es sinnvoll zwischen dem Ob und dem Wie zu unterscheiden. Mögliche Konflikte mit Persönlichkeitsrechten und dem Revisionsverfahren lassen sich durch Optimierung von Details des Konzepts einer Dokumentation lösen (dazu sogleich). Zuerst müssen Zweifel aus dem Weg geräumt werden, die gegen eine technische Dokumentation an sich sprechen.

Vorbehalte von Praktikern, insbesondere von Richtern gegen eine technische Dokumentation der Hauptverhandlung sind grundsätzlicher Natur. Befürchtet wird ein Mehraufwand an Arbeit und eine Verkomplizierung des Verfahrens.[36] Dies liegt zum einen daran, dass die Justiz schlecht ausgestattet sei, sodass Technik im Gerichtssaal oft als etwas erfahren werde, was mehr Probleme schafft, als sie lösen kann. Zum anderen sei die Justiz und die in ihr tätigen Juristen „struktur konservativ“[37] und hielten gerne am Bewährten fest, nach dem Motto, es hätte ja bisher auch gut geklappt. Nicht zuletzt werde die Reformbestrebung zur Aufzeichnung der Hauptverhandlung auch als Kontrolle der Arbeit wahrgenommen, da nicht nur die Zeugenaussagen, sondern jeglicher Wortbeitrag mitgeschnitten werde. Man kann sich gut vorstellen, wie die marginale Ausstattung der Gerichtssäle durch ständige Unterfinanzierung der Justiz die Bereitschaft und Motivation um Einsatz technischer Hilfs-

31 *Traut/Nickolaus,* StraFo 2020, 100 (105); *Barthel,* StV 2018, 678 (680); vgl. *Fischer, Thomas*, Dient die Aufzeichnung im Gericht der Wahrheitsfindung? in: Legal Tribune Online, 22.06.2022, hier abrufbar (Stand 01.07.2022).

32 *Mosbacher*, ZRP 2019, 158 (160); *Traut/Nickolaus,* StraFo 2020, 100 (102); vgl.*Fischer, Thomas*, Dient die Aufzeichnung im Gericht der Wahrheitsfindung? in: Legal Tribune Online, 22.06.2022, hier abrufbar (Stand 01.07.2022).

33 Bericht der Expertinnen- und Expertengruppe zur Dokumentation der strafgerichtlichen Hauptverhandlung, S.15, hier abrufbar (Stand: 31.05.2022).

34 *Traut/Nickolaus,* StraFo 2020, 100 (102). Ähnlich auch *Fischer, Thomas*, Dient die Aufzeichnung im Gericht der Wahrheitsfindung? in: Legal Tribune Online, 22.06.2022, hier abrufbar (Stand 01.07.2022): Die Aufzeichnung würde zwar nicht grundlegend die Schwierigkeit der Rekonstruktion längst vergangener “Wahrheiten” ändern, jedoch Willkürgefahren beseitigen und Rationalisierung voranbringen.

35 Vgl. *Ebd.; Mosbacher,* ZRP 2019, 158 (158).

36 *Prof. Dr. Ali B. Norouzi,* in: Dokumentation der Hauptverhandlung das Revisionsrecht; FAZ Einspruch Folge 207, ab 38:35, hier abrufbar (Stand: 31.05.2022).

37 Ebd., ab 38:55.

mittel hemmt. Es wird eine Zeit zur Eingewöhnung brauchen, sowohl seitens der Technik und eventueller Installationsprobleme, als auch der Verfahrensbeteiligten. Der Aufwand wird sich dennoch lohnen und darf nicht als Ausrede dienen, um Einschnitte in der Rechtsstaatlichkeit des Strafverfahrens hinzunehmen. Es braucht gerade solcher Reformbestrebungen, um das Strafverfahren zeitgemäß zu gestalten und das Ziel der Wahrheitsfindung noch besser zu erreichen.

D. Auswirkungen einer Dokumentationspflicht

Eine technische Dokumentation der Hauptverhandlung ist somit notwendig. Ob diese auditiv, audiovisuell oder/und mit automatischer Transkription erfolgen sollte, ergibt sich aus der Betrachtung der Auswirkungen der Dokumentationspflicht auf das Strafverfahren.

I. Rechtliche Folgen

1. Revisionsrecht

Die wohl beliebteste Frage in der Diskussion um die Dokumentationspflicht ist die der Auswirkungen auf das Revisionsrecht. Mit der Inbegriffsrüge kann im Revisionsverfahren gerügt werden, dass die im Urteil getroffenen Feststellungen sich nicht aus dem Inbegriff der Hauptverhandlung, also aus der Beweisaufnahme ergeben.[38] Dies ist zum Beispiel der Fall, wenn das Urteil den Wortlaut einer verlesenen Urkunde, verlesenen Aussage oder eine nach § 255a StPO vorgeführte Aufzeichnung falsch, unvollständig oder gar nicht wiedergibt.[39] Die Inbegriffsrüge kann jedoch nur dann fruchten, wenn die Unstimmigkeit dokumentiert ist, da die Revisionsinstanz keine zweite Beweisaufnahme durchführt. Urkunden oder Protokolle können nur unter den Voraussetzungen der §§ 251 ff. StPO eingebracht und damit Teil der Akte werden, die das Revisionsgericht erhält. Zeugenaussagen werden, wie zuvor erläutert, praktisch nie dokumentiert. Ergibt sich die Unstimmigkeit also aus der Vernehmung eines Zeugen oder des Angeklagten, kann das Revisionsgericht diese nicht nachprüfen, ohne zu versuchen die Beweisaufnahme selbstständig zu rekonstruieren, was unzulässig wäre (sog. Rekonstruktionsverbot).[40] Es gibt demnach keine Möglichkeit des Rechtsschutzes, wenn eine Verurteilung auf der Vernehmung des Zeugen X basiert, die Aussage jedoch im Urteil inhaltlich falsch wiedergegeben wurde.

Mit der Dokumentation der Hauptverhandlung könnten solche Rügen nun inhaltlich nachgeprüft werden. Es wird daher befürchtet, dass sich Inbegriffsrügen häufen werden und das Revisionsgericht sich durch Sichtung der Aufzeichnung zu einer zweiten Tatsacheninstanz entwickelt.[41] Bei der Einlegung der Revision in Form einer Inbegriffsrüge muss begründet werden, welcher Teil der Vernehmung eines Zeugen nicht mit den Feststellungen im Urteil übereinstimmt.[42] Das bedeutet, dass die Revisionsrichter sich nicht die gesamte Aufzeichnung der Hauptverhandlung ansehen müssen bzw. dürfen. Ein Blick auf einen Ausschnitt der Transkription dürfte dabei ausreichen. Für die Rüge, dass ein Zeuge unglaubwürdig war, bedürfe es einer genauen Sichtung von audiovisuellen Aufzeichnungen. Solche Rügen sind jedoch nach der Rechtsprechung unzulässig, da die Bewertung der Glaubhaftigkeit eines Zeugen eine Frage der Beweiswürdigung gem. § 261 StPO darstellt, die allein den Tatrichtern vorbehalten ist.[43]

Es mag also zu bezweifeln sein, dass der BGH mit einer Flut von Revisionen überrannt wird.[44] Eine Missbrauchsgefahr besteht zwar immer. Jedoch wird die objektive digitale Dokumentation zu weniger Widersprüchen, also zu weniger begründeten Inbegriffsrügen führen.[45] Selbst, wenn es zu mehr Revisionsanträgen kommen

38 *Schmitt,* NStZ 2019, 1 (8).
39 BGH NStZ-RR 2011, 214; vgl. auch KK-StPO/*Gericke*, 8. Aufl., § 337 Rn. 26a.
40 KK-StPO/*Ott*, 8. Aufl., § 261 Rn. 197.
41 *Mosbacher,* ZRP 2021, 180 (181).
42 *Prof. Dr. Ali B. Norouzi,* in: Dokumentation der Hauptverhandlung das Revisionsrecht; FAZ Einspruch Folge 207, ab 38:35, hier abrufbar (Stand: 31.05.2022).
43 Ebd., ab 42:47; BeckOK StPO/*Graf*, 43. Edit., § 337 Rn. 61.
44 So auch *Schmitt,* NStZ 2019, 1 (1) und Bericht der Expertinnen- und Expertengruppe zur Dokumentation der strafgerichtlichen Hauptverhandlung, S.17, hier abrufbar (Stand: 31.05.2022).
45 *Schmitt,* NStZ 2019,1 (8); vgl. *Traut/Nickolaus,* StraFo 2020, 100 (103).

wird, wären die Anträge „qualitativ kein Systembruch, sondern lediglich eine konsequente Fortführung bereits vorhandener Judikatur“[46]. Eine solch konsequente Weiterführung des Rechtsschutzes ist insbesondere bei Verfahren mit hoher Straferwartung mit nur einer Tatsacheninstanz wünschenswert. Insgesamt können durch den Vorzug einer auditiven Aufzeichnung mit automatischer Transkription gegenüber einer audiovisuellen Risiken wie Mehrarbeit, Umgehung des Rekonstruktionsverbots und Entwicklung zur zweiten Tatsacheninstanz minimiert werden.

2. Persönlichkeitsrechte

Bei der digitalen Dokumentation der Hauptverhandlung müssen die Persönlichkeitsrechte der Betroffenen, genauer das Recht am gesprochenen Wort und das Recht am eigenen Bild nach Art. 2 Abs. 1 GG i. V .m. Art. 1 Abs. 1 GG berücksichtigt werden. Der Eingriff durch die Aufzeichnung des Gesprochenen mit anschließender Transkription ist grundsätzlich durch das Ziel der verbesserten Wahrheitsfindung gerechtfertigt.[47] Die Auffassung der Expertengruppe, dass eine auditive Aufzeichnung einer Bild-Ton Aufzeichnung vorzuziehen ist, da sie ihr nicht nachsteht, jedoch ihre Risiken und Nachteile vermeidet, ist überzeugend.[48] Eine audiovisuelle Aufzeichnung greift mehr in diese Persönlichkeitsrechte der Betroffenen ein als eine rein auditive.[49] Gleichzeitig reicht die auditive Aufzeichnung mit automatischer Transkription zur Wahrheitsfindung aus und steht der Videoaufzeichnung somit kaum nach.[50] Dies trifft insbesondere zu, wenn man sich daran erinnert, dass die Aufzeichnung weder für die Richter der Tatsacheninstanz noch für die der Revision als Mittel zur Einschätzung der Glaubhaftigkeit dienen soll, sondern zur Gedächtnisstütze und als Beweis des Inhalts der Aussage. Insofern ist die auditive Aufzeichnung gleich geeignet und milder als die audiovisuelle, sodass eine audiovisuelle Aufzeichnung nicht erforderlich scheint.

46 Schmitt, NStZ 2019, 1 (8).
47 Vgl. Bericht der Expertinnen- und Expertengruppe zur Dokumentation der strafgerichtlichen Hauptverhandlung, S. 87, hier abrufbar (Stand: 31.05.2022).
48 Ebd., S. 16.
49 Ebd., S. 87.
50 *Mosbacher,* ZRP 2021, 180 (181).

Insgesamt muss die Aufzeichnung möglichst persönlichkeitsrechtschonend ausgestaltet werden.[51] Dafür müssen Detailfragen wie die der Akteneinsicht, Speicherung und Weiterverwendung im Rahmen anderer Verfahren[52] geklärt werden.

II. Tatsächliche Folgen

1. Mehraufwand für die Richter

Wie zuvor erwähnt ist mit einem erheblichen Anstieg der Arbeit für Richter nach einer Phase zur Eingewöhnung insbesondere bei der bisher präferierten auditiven Aufzeichnung der Hauptverhandlung nicht zu rechnen. Dafür müssen jedoch einige rechtliche Eckpunkte gegeben sein: Zum einen soll das Tatgericht seine Verhandlung bei Aufzeichnungsmängeln nicht unterbrechen müssen.[53] Ein Ausfall der Technik oder technische Mängel dürften keine absoluten Revisionsgründe darstellen.[54] Außerdem müsste die Aufzeichnung als bloßes Beweismittel qualifiziert werden, auf das gegebenenfalls zurückgegriffen werden kann, sodass die Richter die Aufzeichnung und die Transkription am Ende nicht auf Fehler überprüfen und bestätigen müssen.[55]

2. Kosten

Die Einführung einer technischen Dokumentation wird wie erwartet erhebliche Kosten mit sich bringen.[56] Die Expertengruppe sieht sich erst nach Vorlage eines

51 Bericht der Expertinnen- und Expertengruppe zur Dokumentation der strafgerichtlichen Hauptverhandlung, S. 87, hier abrufbar (Stand: 31.05.2022).
52 Ebd., S. 87.
53 Ebd., S. 16.
54 Ebd., S. 17.
55 *Prof. Dr. Ali B. Norouzi,* in: Dokumentation der Hauptverhandlung das Revisionsrecht; FAZ Einspruch Folge 207, ab 40:10, 37:27, hier abrufbar (Stand: 31.05.2022).
56 Bericht der Expertinnen- und Expertengruppe zur Dokumentation der strafgerichtlichen Hauptverhandlung, S. 19, hier abrufbar (Stand: 31.05.2022).

genauen Anforderungsprofils zu einer exakten Benennung der Kosten in der Lage.[57] Positiv feststellen lässt sich, dass eine auditive oder audiovisuelle Aufzeichnung mit anschließender Transkription rein technisch möglich ist, so wie auch zu erwarten war.[58] Dabei betont die Expertengruppe jedoch, dass eine fehlerfreie Transkription von keinem System zu leisten ist.[59] Diese Fehlerfreiheit kann auch aus den zuvor erläuterten Gründen nicht der Anspruch sein. Als Paradebeispiel der technischen Ausstattung gilt der IStGH: Die Verhandlungen werden mittels neun Kameras und Sitzplatz Mikrofonen aufgezeichnet, während Stenografen ein Wortprotokoll erstellen und dieses sofort über Monitore im Saal gestreamt wird.[60] Das Budget von 1,4 Millionen pro Saal kann von Deutschland nicht gestemmt werden.[61] Allerdings muss diese Ausstattung nicht der Anspruch sein. Ein großer Schritt wäre schon getan, wenn jeder Saal im LG und OLG mit funktionierenden Mikrofonen, Kameras und automatischer Transkriptionssoftware ausgestattet wäre. Dass dabei die audiovisuelle Aufzeichnung zu höheren Kosten führen wird als die auditive, erklärt sich von selbst.[62]

E. Fazit

Eine digitale Dokumentation der strafgerichtlichen Hauptverhandlung beim Landgericht und Oberlandesgericht muss kommen. Die Verfahren sind längst nicht mehr zeitgemäß und weisen insbesondere im Vergleich zum europäischen Standard hohe Defizite in der Rechtsstaatlichkeit auf.[63] Klar ist auch, dass es eine Pflicht zur Aufzeichnung geben muss, da zu befürchten ist, dass die Technik als freiwillige Option nicht genutzt wird. Insgesamt überwiegen die Chancen und Vorteile ganz klar die Risiken. Die Bedenken können durch eine präzise Ausarbeitung des Rahmens und der Details aus dem Weg geräumt werden. Die Einführung einer auditiven Aufzeichnungspflicht ist als milderes Mittel im Vergleich zur audiovisuellen Aufzeichnung vorzuziehen. Daraus ist aber nicht zwangsläufig zu schließen, dass die Aufzeichnung in Bild und Ton nicht ebenfalls realisiert werden kann. Auch hierbei wird es auf Detailfragen ankommen. Eine automatische Transkription, die allen Verfahrensbeteiligten unmittelbar zur Verfügung gestellt wird, ist bei beiden Optionen unabdingbar.

Es wird noch einige Jahre dauern, bis digitale Verhandlungssäle Alltag werden. Die Expertengruppe empfiehlt erste Pilotprojekte ab 2026.[64] Dennoch wecken die Pläne der neuen Regierung Hoffnung. Einen Beitrag zur Prozessdigitalisierung leistet beispielsweise das Forschungsprojekt „Elektronischer (Straf-)Gerichtssaal der Zukunft“ geleitet von Frau Professorin Rostalski, das sich mit den rechtlichen und technischen Rahmenbedingungen von Digitalisierungsprozessen im Strafgerichtssaal beschäftigt.[65] Gespannt wird der erste Prototyp eines elektronischen Gerichtssaal erwartet, welcher durch den angekündigten Gesetzesentwurf hoffentlich bald in den Gerichten realisiert werden kann.

57 Ebd., S. 19.
58 Ebd., S. 20.
59 Ebd., S. 20.
60 Ebd., S. 153; zur Dokumentation der Hauptverhandlung am IStGH *Mosbacher,* NStZ 2019, 1 (4 ff.).
61 Bericht der Expertinnen- und Expertengruppe zur Dokumentation der strafgerichtlichen Hauptverhandlung, S. 153, hier abrufbar (Stand: 31.05.2022).
62 Ebd., S. 19.
63 Zum Vergleich mit dem europäischen Standard siehe *von Galen,* StraFo 2019, 309-318.
64 Bericht der Expertinnen- und Expertengruppe zur Dokumentation der strafgerichtlichen Hauptverhandlung, S. 20, hier abrufbar (Stand: 31.05.2022).
65 Weitere Informationen zum Forschungsprojekt finden sich hier (Stand: 14.06.2022).

Aufsatz

Wie die Blockchain das Gesellschaftsrecht revolutionieren könnte

Ludovica Bölting

Open Peer Review

Dieser Beitrag wurde lektoriert von: Hendrik Eppelmann und Joela Worm

Ludovica studiert Jura an der Universität zu Köln. Sie hat einen LL.M. in deutsch-italienischen Rechtswissenschaften (Köln/Florenz) abgeschlossen und arbeitet zurzeit studienbegleitend bei der Deutschen Gesellschaft für Geldwäscheprävention.

Der digitale Wandel zeichnet sich vor allem dadurch aus, dass er gleichzeitig viele verschiedene Sphären beeinflussen kann: von der Privat- über die Arbeits- bis hin zur Rechtssphäre. Das Recht, das seit jeher ein eng mit der Gesellschaft verbundenes Phänomen ist, bleibt nicht abgeschieden gegenüber neuen Ereignissen, die bisher unbekannte Rechtsfragen aufwerfen. In der Tat stellt sich die Aufgabe, diese innovativen Neuheiten regulatorisch zu berücksichtigen, indem zunächst versucht wird, sie unter bereits bekannte Rechtskategorien zu subsumieren. Insbesondere um ihre Nutzung sicherer zu machen und damit die Verbraucher/Nutzer[1] selbst zu schützen. Eine IT-Revolution, die seit dem vergangenen Jahrzehnt eine zentrale

1 Zum Zwecke der besseren Lesbarkeit wird bei personenbezogenen Hauptwörtern nur die männliche Form verwendet. Diese Begriffe sollen für alle Geschlechter gelten.

Rolle gespielt hat, ist zweifellos das Aufkommen der Blockchain[2]. Diese Erscheinung, die in erster Linie mit der Entstehung von Bitcoin zusammenhängt, hat sich seitdem auf unendlich viele verschiedene Bereiche ausgeweitet, welche weit über Kryptowährungen allein hinausgehen. Dabei ist ein Sachgebiet, das unter unterschiedlichen Aspekten von der Blockchain-Technologie beeinflusst werden könnte, das Gesellschaftsrecht. Im folgenden Beitrag soll ein Überblick gegeben werden, welche Bereiche ganz besonders von der Blockchain verändert werden und eventuell davon profitieren könnten. Zu diesem Zweck wird auf der Grundlage der Funktionsweise der Blockchain (Kapitel A) die Vorteile für das Gesellschaftsrecht dargestellt (Kapitel B) und hierbei speziell die Auswirkungen auf die Register beleuchtet (Kapitel C). Anknüpfend wird zusätzlich die Thematik der Zusammenwirkung von Blockchain und Corporate Governance (*dt. Unternehmensführung*) (Kapitel C.) erläutert.

A. Überblick über die Funktionsweise des Blockchain-Systems

Die Einführung der Blockchain hat es ermöglicht, Daten auf transparente,eindeutige und zuverlässige Weise zu verwalten und zu speichern. Als Grundlage dafür dient ein System, das Informationen auf verteilte, unabhängige Knoten (sog. ***Nodes***) speichert, die zusammengefügt einen einheitlichen Rahmen bilden. Dieses dezentral geführte „verteilte Knotenbuch" (***distributed ledger***), bildet das zentrale Merkmal der Distributed-Ledger-Technologien (***DLT***). DLTs zeichnen sich dadurch aus, dass es keine zwischengeschaltete oder zentrale Behörde bzw. Unternehmen gibt, das für die Pflege, Aktualisierung und Gewährleistung der Gültigkeit der gespeicherten Informationen zuständig ist. Sie basieren auf einem verteilten Netzwerk, in dem jeder Computer eine Kopie des Ledgers unterhält, auf die er frei zugreifen kann. Dieses Netzwerk wird als Peer-To-Peer-Netzwerk (***P2P-Netzwerk***) bezeichnet. Bei diesem sind einzelne Computer permanent über das Internet miteinander verbunden und die Informationen innerhalb der Blockchain werden automatisch auf individueller Software an verschiedenen Orten gespeichert.[3]

> „Kernelement der klassischen Blockchain ist, dass alle Daten in einer chronologischen Reihenfolge gespeichert werden müssen."

Die Blockchain ist eine DLT mit eigenen, spezifischen Merkmalen. Es ist wichtig zu unterstreichen, dass nicht alle DLTs auch Blockchains sind. Hauptmerkmal des Blockchain-Systems ist das Vorhandensein einer genau definierten Abfolge von ***‚Blöcken'***, die zusammen eine unveränderliche ***‚Kette'*** bilden. Daher leitet sich auch der Name des Systems ab. Jeder Block innerhalb der Abfolge beinhaltet die Informationen des vorhergehenden und wird somit sicher und unwiderruflich in die Kette eingebunden.[4] Kernelement der klassischen Blockchain ist also, dass alle Daten in einer chronologischen Reihenfolge gespeichert werden müssen.

Um die Authentizität der eingegebenen Informationen zu gewährleisten, ist jeder Nutzer im Besitz eines Paares kryptografischer Schlüssel: eines öffentlichen und eines privaten. Diese bilden ein asymmetrisches Verschlüsselungssystem.[5] Einerseits wird der öffentliche Schlüssel mit allen Knoten des Systems geteilt und soll somit die Identifizierung des Benutzers ermöglichen. Andererseits wird der private Schlüssel verwendet, um Nachrichten auf der Blockchain zu entschlüsseln oder um die Integrität von Daten durch eine digitale Signatur zu überprüfen.[6] Möchte ein Nutzer etwa Informationen auf der Blockchain (zum Beispiel eine Transaktion) speichern, kann er durch Verwendung seines individuellen private Keys signalisieren, dass die Information von ihm stammt. Durch eine kryptografi-

2 Für die Grundlagen der Funktionsweise einer Blockchain, s., CTRL 1/21, 15 ff.

3 Vgl. *Kaulartz*, CR 2016, 474 (475).
4 Um die Funktionsweise und die technischen Aspekte der Blockchain zu vertiefen, s. *Schrey/Thalhofer*, NJW 2017, 1431 (1431 ff.); *Frink*, CTRL 1/21, 15 ff.
5 Vgl. *Hornung/Schallbruch,* IT-Sicherheitsrecht, 1. Aufl. 2021, § 14 Rn. 10.
6 Vgl. *Rehmani,* Blockchain systems and communication networks: from concepts to implementation, 2021, 45.

sche Funktion und der Nutzung des öffentlichen Schlüssels kann das Netzwerk überprüfen, dass die Information von der Person stammt, die den privaten Schlüssel hat. Das Bemerkenswerte hieran ist, dass das Netzwerk gerade nicht den privaten Schlüssel, sondern nur den öffentlichen kennen muss.

Im Großen und Ganzen sind die DLTs dadurch gekennzeichnet, dass sie auf einem gemeinsamen, verteilten, replizierbaren, gleichzeitig zugänglichen, dezentralen Register auf kryptografischer Basis aufbauen.

B. Warum gerade die Blockchain Technologie für Gesellschaften so verlockend ist

Die Blockchain zeichnet sich grundsätzlich durch vier Haupteigenschaften aus. Erstens gewährleistet sie ein hohes Maß an Transparenz, da die Informationen dezentral verfügbar und für alle Teilnehmer einsehbar sind. Zweitens bleibt sie im Laufe der Zeit unverändert, aufgrund der besonderen Verkettung der Informationsblöcke. Drittens weist sie ein hohes Maß an Zuverlässigkeit auf, da sie auf kryptografischen Schlüsseln basiert. Viertens können einzelne Informationsketten nachverfolgt werden, was die eingegebenen Daten nachvollziehbar macht All diese Merkmale machen die Blockchain zu einer sehr sicheren, effizienten und verlässlichen Datenbank. Trotz fehlender Kontrollinstanz wird somit Manipulationssicherheit gewährleistet.[7] Grundsätzlich ist sie damit für Gesellschaften eine praktische Lösung, um mit niedrigen Kosten und geringem Zeitaufwand eine Datenbank zu führen, die als Register genutzt werden kann. In dieser dezentralen und transparenten Datenbank könnten die Gesellschafter einfach und eindeutig gespeichert werden. Denn innerhalb des Systems wären Gesellschaftsanteile direkt verfolgbar, insbesondere dank den verknüpften Blöcken.[8] Beispielsweise könnte ein Aktionärswechsel durch das Hinzufügen eines neuen Blocks abgebildet werden.[9] Ein Blick in die Datenbank würde dann ausreichen, um allen Beteiligten die aktuellen Gesellschafterstellungen vorzulegen.

7 Vgl. *Hecht*, MittBayNot 2020, 314 (317).
8 Grundsatz „*know your shareholder*“, vgl. *Möslein/Omlor/Urbach*, ZIP 2020, 2149 (2154).
9 Vgl. *Möslein*, FS Windbichler, 2020, 889 (894).

Somit wird nicht nur der Identifikation gedient, sondern gleichzeitig sichergestellt, wer zur Wahrnehmung der Aktionärsrechte befugt ist.[10] Aktuell wird zu diesem Zweck bei Namensaktien ein Aktienregister bei der Gesellschaft geführt und bei Inhaberaktien muss ein Depotauszug in Textform von der Depotbank des Aktionärs ausgestellt werden, §§ 123 IV, 67c III AktG. Außerdem kann die Blockchain auch für interne Vorgänge innerhalb der Gesellschaft genutzt werden und diese womöglich erleichtern. Grundsätzlich steht es einer Gesellschaft frei, die eigene Versammlung durch die Nutzung der Blockchain-Technologie effizienter zu gestalten.[11] Die Blockchain ermöglicht kurzum eine Mitgliederverwaltung in Echtzeit.

Durch die Datenbankeigenschaften der Validierung und Einfügung neuer Transaktionen wird sie beispielsweise den Anforderungen an ein Handelsregister gerecht.[12] Dank der typischen Struktur der aufeinander aufbauenden Blöcke garantiert sie einen höheren Grad an Sicherheit als andere DLT-Systeme.

> „Die Blockchain ermöglicht kurzum eine Mitgliederverwaltung in Echtzeit.“

Zusätzlich lässt sich die Blockchain ziemlich genau auf die Bedürfnisse des konkreten Lebenssachverhaltes zuschneiden. In diesem Zusammenhang sind zwei

10 Grundsatz „*traceable shares*“, s. *Möslein/Omlor/Urbach*, ZIP 2020, 2149 (2154).
11 Bspw. indem die Abstimmung auf der Blockchain durchgeführt wird, vgl. *Maume*, NZG 2021, 1189 (1193). Mehr dazu in diesem Artikel unter D.
12 Vgl. *Hecht,* MittBayNot 2020, 314 (317).

Arten von Blockchains zu nennen, die sich in Bezug auf die Schreibrechte unterscheiden. In der ***permissionless Blockchain*** haben alle Nutzer im Netzwerk die gleichen Zugangs- und Schreibrechte.[13] Bei einer ***permissioned Blockchain*** hingegen werden diese Rechte nur einem bestimmten Kreis von Nutzern zugeteilt. Diese Differenzierung ermöglicht es, den Grad an Dezentralisierung einer Blockchain nach den eigenen Wünschen zu gestalten. Eine Gesellschaft kann durch eine ***permissioned Blockchain*** Zugangs- und Schreibrecht der Nutzer einschränken, um somit u.a. auch datenschutzrechtlichen Vorgaben nachzukommen.[14]

C. Blockchain-Technologie als mögliche Weiterentwicklung für das Aktienregister und Unternehmensregister

Die Tatsache, dass die Blockchain sich optimal für die Speicherung von Daten eignet, eröffnet die Möglichkeit, diese Technologie auch für die Führung von Registern zu nutzen. Im Rahmen des Gesellschaftsrechts stehen das Aktien- und das Handelsregister im Vordergrund.

I. Aktienregister goes Blockchain?

Das Aktienregister (§ 67 AktG) ist ein Dokument, das die Gesellschaft zunächst privat führen muss, sobald sie Namensaktien oder Zwischenscheine[15] ausgibt.[16] § 67 AktG regelt auch, welche Angaben im Register eingetragen werden müssen. Grundsätzlich zählen dazu Name, Adresse und Geburtsdatum der Aktionäre (sofern sie natürliche Personen sind). Das Aktienregister dient dazu, die Identität der Aktionäre für die AG zu erfassen und diese für Stimmrechte und Dividendenausschüttung zu legitimieren.[17] Im Gegensatz zum Handelsregister (§ 15 HGB) oder zum Grundbuch (§ 892 Abs. 1 BGB) ist das Aktienregister kein öffentliches Register.[18] Dadurch sind auch die Prüfungsanforderungen niedriger, was die mögliche Blockchain-Anwendung erleichtert.[19] Eine bestimmte Form, in der das Aktienregister geführt werden muss, ist nicht vorgeschrieben. Die Verwendung des Begriffs ***„Aktienregister"*** deutet darauf hin, dass es auf elektronischem Wege erstellt werden kann.[20] Diese Möglichkeit wird in der Unternehmenspraxis weitgehend genutzt: Die meisten Aktienregister werden in elektronischer Form geführt und von spezialisierten Dienstleistungsunternehmen verwaltet.[21] Bei der Führung des Aktienregisters auf einer Blockchain würde die Dezentralität der Registerführung im Mittelpunkt stehen. Grundsätzlich würde einer solchen Führung des Registers nichts im Wege stehen, da der Vorstand keine Pflicht hat, das Register operativ selbst zu betreiben.[22] Insbesondere wenn es um die Identifizierung von einzelnen Aktionären geht, könnte die Blockchain-Registerführung große Vorteile mit sich bringen. Aktuell genießt das Aktienregister keine große Rechtssicherheit, da es nicht permanent aktualisiert wird und somit nicht auf den neuesten Stand gebracht wird.[23] Die Identifizierung der Aktionäre erfolgt sehr mühsam und aufwendig. Hauptsächlich weil die Gesellschaft für die Ermittlung der Informationen auf Intermediäre (meistens Banken) innerhalb der Verwahrungskette zurückgreifen muss.[24] Diese Führung einzelner selbständiger Register hindere den Informationsfluss und treibe auch die Kosten nach oben. Eine Lösung könnte darin besteht, dass innerhalb der Blockchain Intermediäre selbst einzelne Knoten des Netzwerkes abbilden würden und somit die Informationen direkt auf der Blockchain speichern könnten. Auch Aktionäre würden von schnellen Eintragungen in das Register profitieren. Damit wären sie in der Lage Handelsaktivitäten der Gesellschaft in Echtzeit nachzuvollziehen, etwa auch Transaktionen, da diese innerhalb weniger Minuten schon registriert werden. Gleichzeitig steht eine schnelle Eintragung der Aktionäre in das Register ohnehin in deren Eigeninteresse, weil die mitgliedschaftlichen Rechte (Dividendenansprüche, Teilnahmerechte) erst mit Eintragung in das Aktienregister geltend gemacht werden können, § 67 II AktG. Zudem können datenschutzrechtli-

13 Typisches Beispiel einer permissionless und public Blockchain ist die von Bitcoin.
14 Vgl. *Maume*, NZG 2021, 1189 (1190).
15 Zwischenscheine sind Anteilspapier, die auf den Namen lauten, §§ 10 III, 8 VI AktG. Sie können als temporärer Vorläufer der Aktienurkunden an die Aktionäre ausgegeben werden, falls etwa die Herstellung der Aktienurkunden längere Zeit benötigen sollte.
16 Vgl. *Heinrich* in: *Heidel*, Aktien und Kapitalmarktrecht, Nomoskommentar, 5. Aufl., § 67 Rn. 11.
17 Vgl. *Lieder*, NZG 2005, 159 (159 ff.).
18 *Mayer/Albrecht vom Kolke* in: Hölters/Weber, Aktiengesetz Kommentar, 4. Aufl., § 67 Rn. 3.
19 *Schubert*, Beiträge zum transnationalen Wirtschaftsrecht, 2019, 5 (12).
20 Mit einer Gesetzesänderung ersetzte der Gesetzgeber den bis dahin verwendeten Begriff „Aktienbuch" mit „Aktienregister", um den Begriff des Buches zu streichen, der eine Schriftform vermuten ließ, vgl. dazu *Koch* in: ders., Aktiengesetz Beck'sche Kurz-Kommentare, 16. Aufl., § 67 Rn. 4.
21 Bspw. von der *Deutsche Börse Systems AG*. Für weitere Beispiele s. *Bayer* in: MüKoAktG Nachtrag ARUG II, 5. Aufl., § 67 Rn. 13.
22 Ebd., Rn. 15.
23 *Zetzsche*, AG 2019, 1 (13).
24 Ebd.

che Problematiken grundsätzlich durch die weiten Gestaltungsmöglichkeiten einer ***permissioned Blockchain***, die schon oben erwähnt wurden, behoben werden. So könnten Einsichtsrechte seitens der Gesellschaft beschränkt und nur für bestimmte Nutzer und Aktionäre genehmigt werden. Auch die Einsichtnahme der Identifikation der einzelnen Aktionäre, mit den dazugehörigen persönlichen Daten, könnte auf den Vorstand und Aufsichtsrat begrenzt werden.

II. Handelsregister 2.0

Das Handelsregister hingegen unterscheidet sich grundsätzlich vom Aktienregister wegen der öffentlichen Zugänglichkeit. Es muss für jedermann besonders wichtige wirtschaftliche Verhältnisse von Kaufleuten und Handelsgesellschaften offenlegen.[25] Um dies zu gewährleisten, muss das Handelsregister besondere Funktionen erfüllen, insbesondere die Publizitäts- und Kontrollfunktion.[26] Die Blockchain als Trägerin von beliebigen Informationen könnte sich natürlich auch für die Speicherung von Registerinhalten eignen. In diesem Zusammenhang sind jedoch bestimmte Gesichtspunkte zu beleuchten, die im Rahmen eines Blockchain-Handelsregisters genau geregelt werden sollten. Als Erstes muss bestimmt werden, wer gültige Inhalte innerhalb des Systems einfügen darf. Eine ***permissioned Blockchai***n ließe es zu, nur einen bestimmten, eingeschränkten Nutzerkreis für die Erstellung von Inhalten zu legitimieren. Somit wäre die Berechtigung schon von Anfang an eingeschränkt.[27] Jedoch könnte auch eine Blockchain öffentlicher Art verwendet werden. In diesem Fall müsste bestimmt werden, welche Einträge als rechtsverbindlich gelten.[28] Da jeder Eintrag eine elektronische Signatur beinhaltet, wäre man auch in der Lage diesen zuzuordnen. Somit könnte innerhalb der öffentlichen Plattform zwischen berechtigten und nicht berechtigten Einträgen differenziert werden, ohne den Nutzerkreis von Beginn an eingrenzen zu müssen. Eine andere Lösung, die der jetzigen Funktionsweise des Handelsregisters näher käme, wäre die, eine Signatur seitens einer vertrauenswürdigen öffentlichen Stelle für jede Registereintragung vorzusehen.[29] Diese Signatur könnte durch einen Notar oder durch das Registergericht getätigt werden. Als Zweites muss festgelegt werden, ab welchem Zeitpunkt die Publizitätswirkung des Handelsregisters bei Eintragung auf die Blockchain gilt. Durch die Publizitätswirkung soll vergewissert werden, dass der Rechtsverkehr auf die Korrektheit und Vollständigkeit des Handelsregisters vertrauen kann. § 15 HGB regelt grundsätzlich die Folgen der unterbliebenen, der richtigen und der unrichtigen Eintragung und Bekanntmachung.[30] Bei einem Blockchain-Handelsregister wäre es sinnvoll, auf den Moment abzustellen, in dem die Eintragung für den Leser innerhalb der Plattform als valide gilt.[31] Im Vorfeld müsste aber für die Nutzer festgestellt werden, welche eingegebenen Informationen eine sogenannte Eintragung darstellen würden.

Die auftauchenden Fragen sind zahlreich, insbesondere weil noch kein Handelsregister derzeit komplett auf Blockchain-Basis geführt wird. Es gibt zwar ein paar wenige Anwendungsbeispiele in anderen Ländern, aber in keinem wird die Blockchain als komplette Grundlage für das Handelsregister genutzt. Ein Beispiel dafür ist Estland, das die Blockchain als Mechanismus nutzt, um die Informationen ihres digitalen Registers zusätzlich abzuspeichern.[32] Diese ‚doppelte Speicherung' auf der Blockchain soll hauptsächlich vor Manipulationen schützen. Ein weiteres Beispiel ist Malta. Die ‚Blockchain-Island' hat eigentlich vor, ihr Handelsregister komplett Blockchain-basiert zu gestalten. Dies wäre das erste vollständig zirkulierende Handelsregister auf einer DLT-Plattform.[33]Es muss betont werden, dass nicht alle technologischen Veränderungen, einschließlich der Nutzung der Blockchain, einen Fortschritt darstellen. Allein die abstrakte Möglichkeit, das Handelsregister auf Blockchain-Basis führen zu können, genügt als Selbstzweck nicht, um tiefgründige technologische und rechtliche Änderungen vorzunehmen. Der Mehrwert der Blockchain liegt grundsätzlich in den Bereichen Manipulationssicherheit und Transparenz. Wobei auch hier differen-

25 *Krafka* in: MüKoHGB, 5. Aufl., § 12 Rn. 1.
26 *Preuß* in: Oetker, Handelsgesetzbuch Kommentar, 7. Aufl., § 8 Rn. 4 f.
27 Vgl. *Paal*, ZGR 2017, 590 (611).
28 Vgl. *Knaier/Wolff*, BB 2018, 2253 (2257).
29 Diese qualifizierten Nutzer werden als ‚Oracles' bezeichnet, die Ereignisse aus der Außenwelt verifizieren und diese im Nachhinein in der Blockchain integrieren, vgl. *Sattler*, BB 2018, 2243 (2245).
30 Zur Vertiefung s. hierzu *Krebs* in: MüKoHGB, 5. Aufl., § 15 Rn. 1 ff.
31 Vgl. *Knaier/Wolff,* BB 2018, 2253 (2258).
32 Ebd., (2259).
33 Durch den Technology Arrangements und dem Services Bills, vgl. *Laurence*, Introduction to Blockchain Technology, 1. Aufl. 2019, 140.

ziert werden muss. Eine Blockchain hat einen sehr hohen Grad an Manipulationssicherheit, jedoch nur, wenn diese eine ausreichende Größe und Rechenleistung erreicht hat. Vorwiegend in der Anfangszeit einer staatlich geführten Blockchain wird man nicht von einer großen Rechenleistung ausgehen können, was mit einem höheren Risiko für Hackerangriffe und Manipulationen einhergeht.[34] Auch die Datenübermittlung wird nicht vom Schutz der Blockchain erfasst. Heute wird dieser Vorgang meistens sicher von Notaren durchgeführt. Wie aber externe Daten an das Blockchain-Handelsregister sicher weitergegeben werden könnten, müsste noch geregelt werden.[35] Außerdem muss man sich vor Augen führen, dass durch ein Blockchain-Handelsregister wichtige und spezifische staatliche Aufgaben einem dezentralen und grundsätzlich nicht kontrollierbaren Netzwerk übergeben werden. Es kann jedenfalls bezweifelt werden, ob dann Sinn und Zweck eines Handelsregisters noch erhalten blieben. Auch die ehemalige Bundesregierung äußert sich in diesem Zusammenhang eher skeptisch: *„Beispielsweise scheint eine Sinnhaftigkeit nicht gegeben, wenn öffentliche Register auch der inhaltlichen rechtlichen Prüfung durch staatliche Stellen dienen (vor allem Grundbuch und Handelsregister) […]"*.[36]

Es bleibt dabei: Nicht jeder Schritt zur Digitalisierung vieler rechtlichen Bereiche muss grundsätzlich mit Begeisterung begrüßt werden. Vielmehr soll stets auf der Grundlage objektiver Kriterien und unter Berücksichtigung des tatsächlichen Nutzens eines Kurswechsels entschieden werden.

D. Corporate Governance und Blockchain

Ein weiterer Zweig, der weitgehend von der Blockchain-Technologie profitieren könnte, ist die Unternehmensführung, besser bekannt als Corporate Governance[37]. Hauptziel der Corporate Governance ist es, das Unternehmen mit einer effizienten Struktur auszustatten, die in der Lage ist, die Qualität der Unternehmensführung in

> „Allein die abstrakte Möglichkeit, ein Register auf Blockchain-Basis führen zu können, genügt als Selbstzweck nicht."

Bezug auf Ziele und Leistung zu kontrollieren und zu maximieren.[38] Im Mittelpunkt stehen dabei vor allem die Beziehungen zwischen dem Vorstand, dem Aufsichtsrat und den Aktionären. Eines der Hauptthemen innerhalb der Corporate Governance ist der Versuch, die Vorstandsmitglieder zu motivieren, im Interesse ihrer Aktionäre und Stakeholder zu handeln. Zu diesem Zweck werden oft vertragliche Lösungen im Dienstvertrag formuliert.[39] Die Prozesse zur Verbesserung der Governance befinden sich in einem ständigen Wandel: Einerseits soll die Beteiligung der Anleger am Unternehmensgeschehen durch die Ausübung der Stimmrechte kontinuierlich gefördert werden. Andererseits wird eine stetige Rechenschaftspflicht der Aktiengesellschaften angestrebt, insbesondere im Hinblick auf die Vergütungspolitik.[40] Die Fragen, die für die Anleger von großem Interesse sind, entsprechen im Allgemeinen den bereits erwähnten Themen: in erster Linie die Notwendigkeit eines hohen Maßes an Transparenz, vorwiegend in Bereichen, in denen die Stimmrechte der Anleger ausgeübt werden sollen. Darüber hinaus besteht ein wachsender Bedarf an einem verstärkten Dialog innerhalb des Unternehmens; auch über nicht-finanzielle Themen. Zusammenfassend lässt sich sagen, dass es drei Bereiche gibt, in denen die Corporate Governance verbessert werden könnte: Zugänglichkeit und Transparenz von Informationen, aktive und informierte Beteiligung von Aktionären an Entscheidungen des Vorstands und ein verstärkter Dialog mit der Unternehmensleitung.

34 *Berger*, DVBl 2017, 1271 (1272).
35 Vgl. den Vorschlag von *Knaier/Wolff*, BB 2018, 2253 (2259).
36 So *Bundesregierung,* Blockchain-Strategie der Bundesregierung: Wir stellen die Weichen für die Token-Ökonomie 2019, 19, hier abrufbar (Stand: 27.05.2022).
37 Für die wesentlichen Aspekte der Digital Compliance als Teil der Corporate Governance, vgl. *Ecker*, CTRL 2/22, 1 ff.-.
38 Vgl. *Blemus/Guégan*, Capital Markets Law Journal 2020, 191 (193).
39 Vgl. *Lafarre/Van Der Elst*, Tilburg Law School Research Paper 2018, 1 (3).
40 Vgl. *Bianconi/Surace*, Corporate Governance and Research & Development Studies, 2019, 9 (9).

I. Vorteile der Blockchain im Corporate-Governance-Bereich

Es bedarf neuer Ansätze, um die Qualität der derzeitigen Corporate Governance weiterzuentwickeln und gleichzeitig den oben genannten Bedürfnissen gerecht zu werden. Dabei könnte die Blockchain eine geeignete Technik sein, um diese Bedürfnisse zu befriedigen.[41] Die Zukunft der Corporate Governance scheint daher in gewisser Hinsicht mit der Entwicklung und Nutzung der Blockchain-Plattform verflochten zu sein. Es lohnt sich, genauer zu untersuchen, auf welche Argumente sich diese Annahme stützt. Die Blockchain kann einen großen Einfluss auf die Transparenz von Informationen innerhalb der Gesellschaft haben. Damit werden eine verstärkte Berichterstattung, Kommunikation und komplette Einsichtnahme in die Informationen erfasst. Denn allzu oft leiden Gesellschaften unter einer hohen Informationsasymmetrie, obwohl alle Beteiligten grundsätzlich die gleichen Rechte auf Einsichtnahme haben.[42] Durch die Nutzung der Blockchain stünden allen Stakeholdern im Netzwerk die gleichen aktuellen Informationen zur Verfügung. Eine angemessene Informationsgrundlage ist der Startpunkt, um Aktionäre und Stakeholder zur Teilnahme am Unternehmensleben zu ermutigen.[43] Darüber hinaus könnte die Blockchain die traditionelle Buchhaltung obsolet machen. Bei einer automatischen Buchführung ist von ‚Real-time Accounting' die Rede: Die Buchungseinträge werden automatisch erfasst, mit einem Zeitstempel versehen und sind damit nicht mehr modifizierbar.[44] Mal davon abgesehen, dass die ganze Buchführung digital abbildbar und in Echtzeit aktualisierbar wäre, würden sich auch die Kosten für die Gesellschaft extrem senken. Insbesondere könnte aber die Führung der Hauptversammlung revolutioniert werden, mit besonderem Augenmerk auf die Abstimmungen. Diese sind von zentraler Bedeutung für die interne Willensbildung der Gesellschaft.[45]

41 Vgl. u.a. Yemark, Review of Finance 2017, 7 (7 ff.); Kaal, Blockchain-Based Corporate Governance, 4 f., hier abrufbar (Stand: 27.05.2022).
42 Sutter-Rüdisser/Germann/Letsch, Corporate Governance 2021, 165 (166).
43 Vgl. Esposito De Falco/Cucari/Canuti/Modena, Corporate Governance: Search for the Advanced Practices 2019, 102 (103 ff.). Es ist von „real time accounting, corporate voting, turnout rate e record ownership" die Rede.
44 Kein Dritter müsste nämlich die Buchungen kontrollieren und zusammenführen, vgl. Sutter-Rüdisser/Germann/Letsch, Corporate Governance 2021, 165 (168).
45 Vgl. *Spindler*, ZGR 2000, 420 (440).

II. Hauptversammlung und Abstimmungen mittels Blockchain

Es ist keine Neuigkeit, dass die Stimmabgabe oft mit schwerwiegenden Mängeln behaftet ist, wie z. B. Unsicherheiten über die Wahlberechtigung, unvollständige Wahlzettel und einseitige Wahlentscheidungen.[46] Außerdem ist es nicht selten, dass die Anwesenheit während den Versammlungen sehr gering ist.[47] Von zentraler Bedeutung für die Wahl ist es, dass die eigene Stimme anonym, überprüfbar und manipulationssicher abgegeben werden kann. Die Wahl mithilfe von einem sog. ***Blockchain-enabled e-voting*** (***BEV***) kann diesen Anforderungen grundsätzlich gerecht werden.[48] Bei der Abstimmung auf einem Blockchain-System wird die Irreversibilität der eigenen Stimme gewährleistet, damit können jegliche Zweifel an der Richtigkeit der Stimme behoben werden.[49] Zudem müssen Stimmberechtigte nicht bei der Versammlung anwesend sein, sondern können direkt von zu Hause aus an der Abstimmung teilnehmen. Eine Möglichkeit, die nicht nur Reisekosten vermeiden würde, sondern auch diejenigen Aktionäre zur Abstimmung veranlassen könnte, die im ‚Normalfall' nicht teilgenommen hätten.[50] Durch die simple und kostengünstige Teilnahme könnten auch Kleinaktionäre dazu angeregt werden, kontinuierlich an den Abstimmungen teilzunehmen. Eine breite Wahlbeteiligung und Willensbildung wirkt sich positiv auf die Mitwirkung der Aktionäre aus und schafft es, deren Interessen in der Unternehmensführung stärker einzubinden.[51]

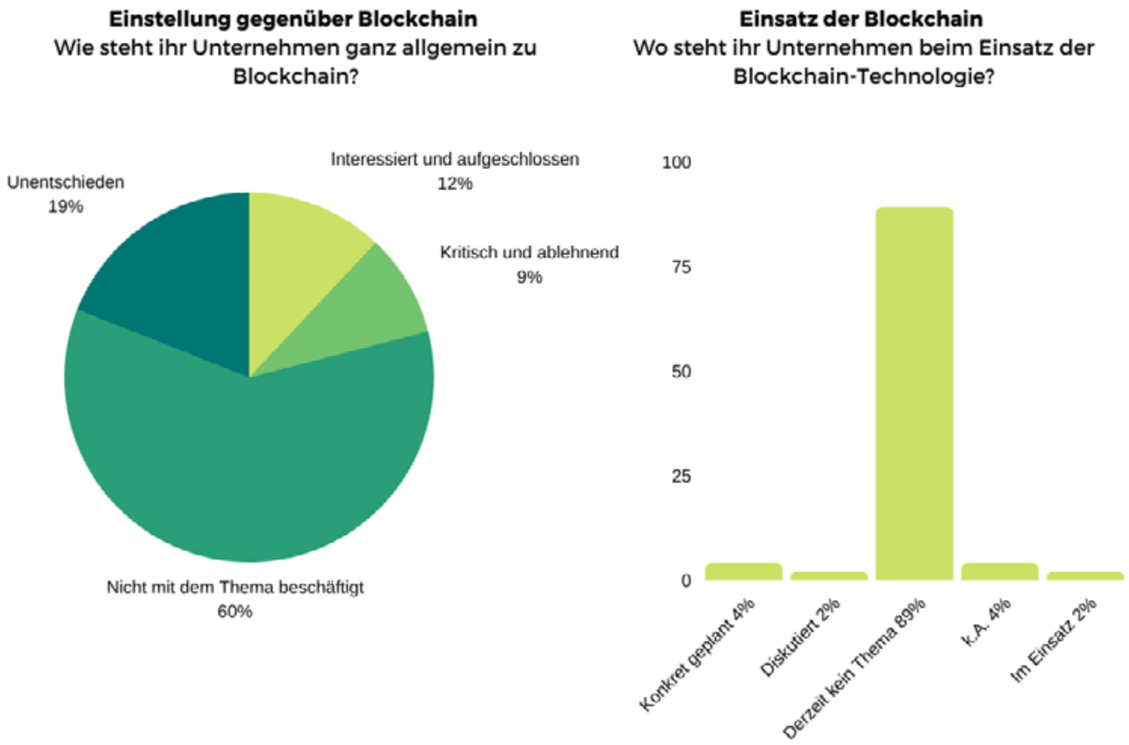
Das Votum wäre auch überprüfbar, da jede Stimme eine einzigartige Adresse hat, die im Nachhinein erkannt und nachträglich kontrolliert werden könnte.[52] Außerdem erhält jeder nach elektronischer Abgabe der Stimme, eine Kopie der erfolgten Registrierung auf der Blockchain. Die Abstimmung mittels BEV ist nicht auf virtuelle Versammlungen begrenzt, sondern kann problemlos auch in Präsenz genutzt werden. Damit könnte man auf jegliche Vertrauensinstanzen verzichten, die ansonsten für

46 Vgl. *Schubert,* Beiträge zum transnationalen Wirtschaftsrecht 2019, 5 (17).
47 Bei Aktiengesellschaften sind meistens nur 30 % bis 40 % des stimmberechtigten Grundkapitals anwesend. Kleinaktionäre nehmen fast nie teil, vgl. dazu *Teichmann*, ZfPW 2019, 247 (260).
48 Für eine Vertiefung zur Funktionsweise des BEV s. *Kschetri/Voas*, IEEE Software, 35/2018, 95 ff.
49 Vgl. *Sutter-Rüdisser/Germann/Letsch*, Corporate Governance, 2021, 165 (169).
50 Bspw. aus Kostengründen, pandemiebedingt oder wegen der zu großen Distanz, vgl. *Sutter-Rüdisser/Germann/Letsch,* Corporate Governance 2021, 165 (169).
51 Vgl. *Schubert*, Beiträge zum transnationalen Wirtschaftsrecht 2019, 5 (17).
52 Vgl. *Maume*, NZG 2021, 1189 (1194).

die Organisation und Durchführung der Abstimmung verantwortlich sind.[53] Somit wären auch die Kostenvorteile für das Unternehmen nicht unwesentlich. Um solche BEV-Systeme nutzen zu können, könnte das Unternehmen selbst eine solche Plattform konzipieren, was mit viel Arbeit und Kosten verbunden wäre. Eine Alternative liegt darin, bereits existierende Blockchains zu nutzen, um die Abstimmung durchzuführen. Als Beispiel existiert bereits ***DecentraVote***. Ein Dienstleister, der die nötige Technologie für die Unternehmen zur Verfügung stellt.[54]

III. Kritische Gesichtspunkte und Herausforderungen einer „Governance of Blockchain"

Allerdings ist die Blockchain-Technik noch kein großes Thema in der Unternehmensleitung. Zwar haben Unternehmen allgemein eine positive und aufgeschlossene Einstellung zur Digitalisierung. Jedoch wird es aufgrund mangelnder Vorbereitung in den Aufsichtsräten nicht kontinuierlich behandelt. Dies spiegelt sich wiederum in dem Einsatz der Blockchain innerhalb der Unternehmen wider, der sehr gering ist (vgl. Abbildung 1).[55] Damit fehlt dem Thema ein praktischer Bezug innerhalb der Unternehmensrealität. Im Rahmen eines groß angelegten Blockchain-Einsatzes, wie im Fall einer Hauptversammlung, sollte der Aspekt der Auswirkung auf die Umwelt nicht vergessen werden. Seit 2015 hat die Bedeutung des Klimawandels für Investitionsentscheidungen exponentiell zugenommen. Befragte Investoren nennen den Klimawandel als entscheidenden Faktor für ihr Engagement in einem Unternehmen.[56] Die größte Auswirkung der Blockchain auf die Umwelt ist der immense Energieverbrauch: Für jeden Verifizierungsprozess wird eine riesige Menge an Strom benötigt.[57] Dies macht die Vereinbarkeit mit den Anforderungen der unternehmerischen Nachhaltigkeit fraglich, was die Handlungen von Investoren maßgeblich beeinflusst. Dieses Problem wird jedoch bereits durch die Verfügbar-



Basis: Alle befragten Unternehmen ab 50 Mitarbeiter (1.004)
Quelle: Bitkom Research 2018

Eine Befragung von ca. 1000 Unternehmen hinsichtlich ihrer Einstellung und Nutzung der Blockchain.
Quelle: Bitkom Research 2019, hier abrufbar S. 17 f.

keit anderer Konsensmechanismen neben dem bisher üblichen Proof-of-Work, wie dem Proof-of-Stake[58] angegangen. Unter Berücksichtigung der großen Anreize, die die Blockchain-Technologie im Bereich der Transparenz, der Partizipation und der Kosten mit sich bringt, kann sie allgemein als ***„[...] new best practice in the digital transformation of corporate governance***" angesehen werden.[59]

53 Vgl. *Schubert,* Beiträge zum transnationalen Wirtschaftsrecht 2019, 5 (16).
54 *DecentraVote* wird bspw. vom *Blockchain-Bayern e.V.* genutzt, um deren Beschlussfassungen elektronisch durchzuführen.
55 Vgl. *Bitkom Research*, Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen, 17, hier abrufbar (Stand: 27.05.2022).
56 Vgl. *Morrow Sodali*, Institutional Investor Survey 2021, S. 11, hier abrufbar (Stand: 30.05.2022).
57 Nach Angaben einiger Analysten ist der Energieverbrauch pro Bitcoin-Transaktion im Jahr 2019 auf 635 kWh gestiegen, was dem Stromverbrauch von etwa 21 US-Haushalten für einen Tag entspricht, vgl. European Environment Agency, Blockchain and the environment 2020, hier abrufbar (Stand: 27.05.2022). Die Bitcoin-Blockchain verbraucht mit ca. 100 TWh etwa so viel wie der gesamte Bankensektor, wobei hierbei Bau und Instandhaltung der Infrastruktur nicht berücksichtigt sind, vgl. *Göbe*l, Blockmagazin 02, 104 (105).
58 Um die Funktionsweise und die Unterschiede zwischen Proof-of-Work und Proof-of-Stake zu vertiefen s. *Frink*, CTRL 1/22, 22.
59 Vgl. *Esposito De Falco/Cucari/Canuti/Modena,* Corporate Governance: Search for the Advanced Practices 2019, 102 (113).

E. Fazit

Die Möglichkeiten, die die Blockchain für Gesellschaften eröffnet, sind zahlreich und wirken sich auf viele Bereiche aus. Die tatsächlichen Anwendungen sind aber noch sehr gering. Der gesamte Prozess steckt noch in einer Entwicklungs- und Erforschungsphase.

Der zukünftige Anwendungsumfang der Blockchain hängt unmittelbar damit zusammen, ob die Risiken und Skepsis behoben bzw. gemindert werden können.[60]

Die Cyberkriminalität ist etwa ein Problem, das stärker im Vordergrund stehen wird, wenn die Technologie angewendet wird. Ein Unternehmen muss sich gegen Cyberangriffe wappnen. Jedoch ist bei einer Blockchain nicht nur der Cyberschutz des Unternehmens wichtig, sondern auch der Schutz aller dezentralen Knoten des Systems. Das Unternehmen wird nicht in der Lage sein, für alle Knoten den angemessenen Schutz zu gewährleisten und diesen im besten Fall sogar zu kontrollieren. Außerdem kann nicht davon ausgegangen werden, dass die Nutzer in der Lage sein werden, einen solchen Schutz zu installieren. Damit steigen die Risiken weiter.

Im Großen und Ganzen zeichnet sich die Blockchain durch ein hohes Maß an Transparenz aus. Doch Transparenz steht oft in einem Spannungsverhältnis mit datenschutzrechtlichen Vorgaben. Zwar sind die Informationen auf der Blockchain nicht unmittelbar mit persönlichen Angaben des Nutzers verbunden, jedoch kann nicht ausgeschlossen werden, dass ein Bezug zwischen dem kryptografischen Schlüssel und dem Nutzer hergestellt wird.[61] Es gibt innerhalb der Blockchain keinen Adressaten bzw. keine Stelle, die sich mit datenschutzrechtlichen Pflichten auseinandersetzt und diese befolgt.[62] Außerdem bleibt es fraglich, wie das Recht auf Löschung der Daten (Art. 17 DSGVO) befolgt werden kann.[63] Denn die Kette der Blockchain kennzeichnet sich dadurch aus, dass kein Datenblock verändert und gelöscht werden kann, was die Durchsetzung dieses Anspruches grundsätzlich unmöglich macht.[64] Was den Datenschutz anbelangt, ist folglich bei der Blockchain noch Luft nach oben; eine Regulierung und Einflussnahme seitens des Gesetzgebers ist notwendig.[65]

Trotz alledem sind die bereits hervorgehobenen großen Vorteile einer Blockchain-Anwendung nicht außer Acht zu lassen. Die Buchhaltung könnte insbesondere einen großen Sprung nach vorne machen, weit entfernt von der doppelten Buchführung, die bereits vor Jahrhunderten eingeführt wurde.[66] Die Unternehmensführung könnte grundlegende Veränderungen erfahren: Durch die komplette Einsehbarkeit von Geschäften und Transaktionen wäre es grundsätzlich unmöglich, Geschäfte zu verschleiern. Doch auch hier muss beachtet werden, dass das Unternehmen abseits von gesetzlichen Pflichten entscheiden kann, welche Daten es transparent auf einer Blockchain speichert. Insoweit schafft die Blockchain an sich noch keine erhöhte Transparenz, wenn das Unternehmen die Daten vorher selektiert.

Der Bereich der Corporate Governance könnte am meisten vom Einfluss der Blockchain profitieren. Denn eine schlechte Corporate Governance war in den letzten

„Außerdem bleibt es fraglich, wie das Recht auf Löschung der Daten (Art. 17 DSGVO) befolgt werden kann.“

60 Vgl. *Schubert,* Beiträge zum transnationalen Wirtschaftsrecht 2019, 5 (23).
61 Vgl. *Hecht*, MittBayNot 2020, 314 (319).
62 Vgl. *Schrey/Thalhofer*, NJW 2017, 1431 (1433 f.).
63 *Hecht*, MittBayNot 2020, 314 (319).
64 Vertiefend zu diesem Thema: *Tröber*, CTRL 2/21, 151 (154 f.).
65 Vgl. *Bechtolf/Vogt*, ZD 2018, 66 (69); *Schrey/Thalhofer,* NJW 2017, 1431 (1433 ff.); *Schubert*, Beiträge zum transnationalen Wirtschaftsrecht 2019, 5 (25).
66 Vgl. *Yemark*, Review of Finance, 21/2017, 7 (30).

Jahren stets einer der zentralen Auslöser für Unternehmensskandale und Finanzkrisen.[67] Es bleibt abzuwarten, ob Unternehmen in der Lage sind, diesen großen technischen Schritt zu wagen und ob sie überhaupt Interesse an einer stärkeren Demokratisierung der Unternehmensentscheidungen haben. Ein zentraler Akteur in diesem Prozess ist zweifellos der Gesetzgeber, der einen sicheren und eindeutigen gesetzlichen Rahmen für den Gebrauch der Blockchain schaffen sollte.

Im Allgemeinen besteht kein Zweifel daran, dass wir uns heute in einer experimentellen Phase rund um die Blockchain-Anwendung im Gesellschaftsrecht befinden. Ob es ein Experiment bleibt oder weitreichende Änderungen nach sich zieht, bleibt abzuwarten.

Weiterführende Hinweise:

Talking Legal Tech – Folge 59

“Notarity - Digitale Beglaubigung, Beurkundung, GmbH-Gründung und Vollmachtserteilung - wie geht das, Jakobus Schuster?”

Talking Legal Tech – Folge 28

„Regulierung & Innovation - wie lässt sich beides vereinbaren, Martin Ebers?“,

Talking Legal Tech – Folge 5

“Was ist Blockchain, Florian Glatz?“

67 Vgl. *OECD,* Blockchain Technology and Corporate Governance 2018, (25), hier abrufbar (Stand: 27.05.2022).

Geld ist „eines der großartigsten Werkzeuge der Freiheit, die der Mensch je erfunden hat.“

– Nach Friedrich von Hayek, 1944

Abbildung 1, Quelle: https://pxhere.com/de/photo/1196883

Aufsatz

Nicht alles, was zahlt, ist Geld! – Zur geldrechtlichen Einordnung von Kryptowährungen

Christian Wengert

Christian hat Jura an der Albert-Ludwigs-Universität Freiburg studiert. Er verfasst zurzeit seine Dissertation an der Philipps-Universität Marburg bei Prof. Dr. Sebastian Omlor, LL.M. (NYU), LL.M. Eur. zu Kryptowährungen im Schuldrecht und arbeitet begleitend als wissenschaftlicher Mitarbeiter in einer Kanzlei in Frankfurt.

Open Peer Review

Dieser Beitrag wurde lektoriert von: Jens Hansen und Santeri Schenk

Friedrich von Hayek bezeichnete einmal Geld *„als eines der großartigsten Werkzeuge der Freiheit, die der Mensch je erfunden hat.“*[1]

Die Kryptowährungen werden häufig als Fortführung der Ideen der österreichischen Schule der Ökonomie gedeutet, zu der ***von Hayek*** gehörte.[2] Auch wenn er womöglich Bitcoin als einen Anstoß zur Weiterentwicklung dieser großartigen Erfindung gesehen hätte, stellt sich bei einer rechtlichen Perspektive die Frage, ob eine Einordnung von Kryptowährungen unter den Geldbegriff möglich ist. Faktisch werden die Kryptowährungen als Zahlungsmittel verwendet und bezeichnen sich oft selbst

1 *Von Hayek*, Der Weg zur Knechtschaft, 95.
2 *Herrmann*, Währungshoheit, Währungsverfassung und subjektive Rechte, 59: Sieht schon 2008 exemplarisch in der gescheiterten virtuellen Währung E-Gold, einen Auftrieb der österreichischen Schule durch das Internet; *Lerch*, ZBB 2015, 190 (203).

als alternatives Geld.[3] Juristisch richtig ist jedoch, dass Geld ein Zahlungsmittel ist, aber nicht jedes Zahlungsmittel auch automatisch Geld.[4] Unabhängig von der Selbstbezeichnung ist daher entscheidend, ob Kryptowährungen überhaupt Geld im Rechtssinne sind. Dies erschöpft sich nicht in einer rein abstrakten Rechtsfrage. Schon bei der Einordnung in die BGB-Vertragstypologie wird relevant, ob mit Currency Token überhaupt ein ***Kaufpreis*** im Sinne von § 433 Abs. 2 BGB bezahlt werden kann. Außerdem bereitet die Beantwortung den Weg für die schuldrechtliche Behandlung von Kryptowährungen: Kryptowährungsschulden sind womöglich am nicht unmittelbar anwendbaren Geldschuldrecht zu messen. Insgesamt stellt sich somit die Frage, ob Kryptowährungen auch im Rechtssinne eine Fortführung der nach ***Hayek*** großartigsten Erfindung der Menschheit sind?

A. Ausgangsproblem

Die Diskussion um die Definition des Geldes ist keine historische Neuheit und weiterhin nicht eindeutig entschieden. Als Sinnbild der wirtschaftlichen Potenz prägt das Geld unseren Alltag und unsere Entscheidungen. Neben den Rechtswissenschaften spielt der Geldbegriff auch in den Wirtschaftswissenschaften, der Philosophie, der Psychologie und der Theologie eine bedeutende Rolle.[5] Aus der juristischen Perspektive führte das über lange Zeit zur Konkurrenzfrage zwischen Rechts- und Wirtschaftswissenschaften mit dem Ziel einer einheitlichen Definition.[6] Wer bestimmt also, was Geld ist? Ist eine solche Entscheidung überhaupt möglich und wenn ja, was bedeutet sie für die anderen Disziplinen?

I. Definitionsversuche

Hierzu haben sich unzählige Definitionsversuche herausgebildet. Möglich wäre eine Kategorisierung zwischen Ansätzen der Rechtswissenschaften und solchen der Wirtschaftswissenschaften. Allerdings zeigt sich schon an ***Knapp'schers*** Geldtheorie, dass einer der bekanntesten Definitionsansätze eines Ökonomen die Perspektive des Rechts wählt. Sinnvoll scheint daher, nach dem Inhalt der Definition und somit der Bestimmungsperspektive einzuteilen.

1. Geld als rechtliches Konstrukt

Folgenden Versuchen ist inhärent, dass sie Geld für ein Konstrukt des Rechts halten. Die Eigenschaft eines Guts als ***Geld*** bestimmt sich durch den Blick des Gesetzes. Wegweisend hierfür war die Ansicht von ***Knapp***. Nach seiner staatlichen Theorie ist die Geldeigenschaft eine Schöpfung der Rechtsordnung[7] und bestimmt sich durch hoheitliche Verleihung dieser Qualifikation.[8] Als kennzeichnendes Merkmal entsteht für ihn daraus die Chartalität.[9] Der Wert des Geldes entsteht unabhängig vom Trägermedium und nur im Rückgriff auf das geltende Recht. Darauf aufbauend werden viele Variationen des rechtlichen Charakters vertreten. Von diesen lassen sich einige zur Exemplifizierung darlegen:

Auch ***Mann*** hielt an der staatlichen Verleihung der Qualifikation als Geld fest und fügte die funktionellen Voraussetzungen der Eignung als Universaltauschmittel und der Stückelung als Rechnungseinheiten hinzu.[10] Weiter modifiziert wurde die Theorie von ***Münch***, der die Anforderungen an den anerkennenden staatlichen Rechtsakt abschwächt und daher einen Annahmezwang nicht für notwendig hielt.[11]

3 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 1: *„a […] version of electronic cash"*; *Butterin*, Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 1: bezeichnet ETH als eigene Währung; so auch für Ripple bei *Schwartz/Young/Britto,* The Ripple Protocol Consensus Algorithm, 1.
4 *Omlor,* ZHR 183 (2019), 294 (311).
5 Als Beispiel dienen der Philosoph F*ichte*, Der geschlossene Handelsstaat, 68 der sich *Knapp* anschließt, wenn er kundtut, dass ein *„Staat […] zu Gelde machen [kann], schlechthin was er will"*; aus Blick der Theologie ist das Wort Geld in der Bibel häufig zu finden, hervorgehoben sei die Einschränkung als Universaltauschmittel in Apostelgeschichte 8, 20: *„Daß* [sic!] *du verdammt werdest mit deinem Gelde, darum daß* [sic!] *du meinst, Gottes Gabe werde auch durch Geld erlangt!"*.
6 *Schmidt*, Geldrecht, Vorbem. zu § 244, Rn. A1; *Omlor*, Geldprivatrecht, 69.
7 *Knapp*, Staatliche Theorie des Geldes, 1.
8 Die Verleihung richtet sich danach, wie Schulden insb. gegen den Staat also Steuern erfüllt werden können. Maßgeblich ist also die Rezeption durch den Staat und nicht die Emission: *Knapp*, Staatliche Theorie des Geldes, 42, 85.
9 Das zeigt sich in seiner (verwirrenden) Definition von Geld: *„Geld bedeutet stets chartales Zahlungsmittel; jedes chartale Zahlungsmittel heißt bei uns Geld. Die Definition des Geldes ist: chartales Zahlungsmittel."*, *Knapp*, Staatliche Theorie des Geldes, 31.
10 *Mann,* Das Recht des Geldes, 5.
11 *Münch*, Das Giralgeld in der Bundesrepublik Deutschland, 100 ff.

Gerber und ***Jung*** befassen sich übereinstimmend mit der Beschaffenheit der auch für sie notwendigen rechtlichen Anerkennung. Sie stehen dabei im Widerspruch, nach welchem Rechtsgebiet dies zu geschehen hat. Für ***Gerber*** ist das Geld als gesetzliches Zahlungsmittel rechtlich bestimmte Wirtschaftssache, die sich durch ihre Diensthaftigkeit für die Lebensgestaltung der gesamten Gemeinschaft aus dem Verfassungsrecht ergibt.[12] Unabhängig von der staatlichen Bestimmung lassen sich weitere Ansätze mit Blick auf die geltenden Rechtsvorschriften finden. Zu nennen sei hier zunächst exemplarisch ***Wolf,*** der Geld in Anlehnung an § 91 BGB als vertretbare Sache sieht, die in ihrem Verwendungsgebiet ein Tauschwert hat.[13] Damit geht zwingend ein Verkörperungserfordernis einher.

Weitaus abstrakter erfassten ***Hartmann, Frauenfelder*** und ***Burckhardt*** den auch ihrer Meinung rechtlichen Charakter des Geldes. Danach ist es das ***zwangsweise Solutionsmittel*** eines jeden Anspruchs, das im modernen Rechtssystem den umfassenden Zugriff auf das Schuldnervermögen gibt und einen Schadensersatz bestimmen lässt.[14] Geld wird dadurch charakterisiert, dass alle Forderungen subsidiär darauf vollstreckbar sind.

Am unteren Spektrum einer rechtlichen Konstruktion befinden sich ***Hahn*** und ***Häde*** fast wortgleich mit ***Siebelt***. Nach ihnen ist zwar weiter legislatives Handeln konstitutiv, aber nicht mehr ausreichend, da erst im Zusammenspiel mit der Gesellschaft ein Tauschmittel als Geld geschaffen werden kann.[15]

Übereinstimmend ist allen Ansätzen trotzdem die Anknüpfung an die jeweilige Rechtsordnung. In den Anforderungen und Grundlagen variieren sie von der bloßen Rechtsschöpfung über privatrechtliche Rechtsgestaltung hin zu einem bloßen Zusammenspiel mit dem Verkehr. Was bleibt, ist das pointierte Ergebnis: ohne staatliches Handeln kein Geld!

12 *Gerber*, Geld und Staat, 57, 71, 89 f.
13 *Wolf,* Lehrbuch des Schuldrechts, § 4 D II a), 148.
14 *Hartmann,* Über den rechtlichen Begriff des Geldes und den Inhalt von Geldschulden, 50, 52; *Frauenfelder,* Das Geld als allgemeiner Rechtsbegriff, 153.; *Burckhardt,* Das Geld, Zeitschrift des Bernischen Juristenvereins, 1935, 3 (11).
15 *Hahn/Häde*, Währungsrecht, § 3 Rn. 10; Siebelt, Der juristische Verhaltensspielraum der Zentralbank, 263.

„Im Ergebnis: ohne staatliches Handeln kein Geld."

2. Geld als wirtschaftliches Konstrukt

Diametral hierzu stehen Theorien, die rechtlich abgelöst Geld als ein rein wirtschaftliches Konstrukt betrachten. Was für die vorgenannten Ansichten knapp ist, ist für die Ökonomen der prägende Satz: *„money is what money does"*[16]. Hieran orientiert wird die Geldeigenschaft vielfach ausschließlich an den Funktionen des Geldes geprüft.[17] Das Geld ist nur einer Bestimmung zugänglich, wenn man dessen Funktionen bestimmt. Alles, was als Geld qualifiziert werden will, muss diese erfüllen. Als Geldfunktionen wird klassischerweise dreigliedrig auf Universaltauschmittel, Recheneinheit und Wertaufbewahrung verwiesen,[18] wenn auch abweichend vertreten wird, dass sich zumindest die Wertaufbewahrung oder sogar die Eignung als Recheneinheit unter die des Tauschmittels einordnen lassen.[19] Diesen funktionsfokussierten Ansatz zeigt etwa ***Simitis,*** wenn er – in Rückgriff auf ***Wolff*** und ***v. Savigny*** – hierfür den Begriff der abstrakten unkörperlichen

Darstellung der klassischen drei Geldfunktionen

16 Dieser Satz wird vielfach verwendet, vgl. *Spahn*, Money as a social Bookkeeping device – From Mercantilism to General Equilibrium Theory, 1. Die Herkunft ist nicht unbedingt geklärt, wird aber auf den Satz *„That which the money-work is the money-thing"* von *Walker,* Political Economy, 123 (Rn. 163) zurückgeführt.
17 *Schilcher,* Geldfunktionen und Buchgeldschöpfung, 35; *Helfferich,* Das Geld, 260; Budge, Lehre vom Geld, 10.
18 *Ohler,* JZ 2008, 317 (318); *Grothe* in Hau/Poseck, BeckOK, § 244 Rn. 2; *Ibold,* ZJS 2019, 95 (97) m.w.N.
19 Die Konzentrierung auf die Tauschmittelfunktion vertritt Wieser in *Elster/Weber/Wieser,* Handwörterbuch der Staatswissenschaften Bd. 4, 686 f.; *Omlor* plädiert hingegen auf die Beibehaltung der Funktion als Recheneinheit und reduziert nur um die Wertaufbewahrung als in Zukunft gerichteten Tausch: *Omlor* in v. Staudinger/Höpfner/Kaiser, BGB, vor § 244, Rn. A38 ff.; *Omlor,* Geldprivatrecht, 57.

Vermögensmacht benutzt.[20] Damit sollten schlicht die Funktionen in einem Begriff zusammengefasst und umschrieben werden. ***Nussbaum*** versucht Geld hingegen als Bruchteil einer ideellen Einheit, also dass es im Verkehr gegeben und genommen wird, zu verstehen.[21] Damit stimmt er mit ***Knapp*** überein, lässt sich aber dennoch von der Funktion des Geldes als „Einheit" leiten. Dem zieht ***Reinhardt*** gleich, wenn er die Definition in einem Kaufkraftträger durch gesellschaftliche Anerkennung finden will.[22] Einen weiteren Grad an Abstraktion erhält der Geldbegriff, wenn man ihn wie ***Elster*** in der ***„Beteiligung am Sozialprodukt"***[23] oder wie ***Forstmann*** in der ***„allgemein anerkannte[n] und jederzeit aktivierbare[n] anonymen Forderungslegitimation an das nationale Güter- und Leistungsvolumen"***[24] sehen will. Auch bei solch einer volkswirtschaftlichen Perspektive orientiert man sich an den Funktionen. Allen Ansätzen ist gemein, dass weit unabhängig von rechtlicher Konstruktion das Geld als wirtschaftliches Gebilde gesehen wird, welches sich auf seine Funktionen reduzieren lässt.

„Eine inhaltliche Auseinandersetzung mit jeder einzelnen Theorie, um DIE Definition des Geldes zu finden, hilft nicht weiter."

20 *Simitis,* AcP 159 (1960/1961), 406 (428 f., 443) fordert, dass Geld von seiner Aufgabe her zu erfassen; *Wolff* in Ehrenberg, Handbuch des gesamten Handelsrechts Band IV 1, 569; die Funktionsorientierung wird vor allem bei *v. Savigny*, Das Obligationenrecht als Theil des heutigen römischen Rechts, 406 deutlich, der in dem Begriff der Vermögensmacht die Funktionen Wertmesser, Wertträger und Eintauschbarkeit in alle Gegenstände vereinen will.
21 *Nussbaum,* Das Geld in Theorie und Praxis des deutschen und ausländischen Rechts, 6.
22 *Reinhardt,* Vom Wesen des Geldes und seiner Einfügung in die Güterordnung des Privatrechts, in FS für Gustav Boehmer, 66 f.
23 *Elster,* Die Seele des Geldes: Grundlagen und Ziele einer allgemeinen Geldtheorie, 59.
24 *Forstmann,* Geld und Kredit, 72.

II. Der rechtliche Geldbegriff

1. Perspektive und Zweck der Definition

Unter historischem Rückblick ließen sich bekannte Versuche zur begrifflichen Bestimmung des Geldes darlegen. Diese sind zwar dualistisch in ihrer definitorischen Perspektive kategorisierbar, eine Tendenz oder gar ein eindeutiges Ergebnis resultieren daraus aber nicht. Übereinstimmend ist allen Ansätzen hingegen das Bestreben einer umgreifenden Begriffsbestimmung.[25] Eine inhaltliche Auseinandersetzung mit jeder einzelnen Theorie, um **DIE** Definition des Geldes zu finden, hilft nicht weiter. Förderlich ist hingegen die Erörterung des Zwecks einer Definition. Zu bestimmen ist der Begriff „Geld" im rechtlichen Sinne, um ihn hier hauptsächlich für die Behandlung von Geldschulden, aber auch bei jeglicher anderer normativer Verwendung greifbar zu machen. Es ist mithin ein Rechtsbegriff, der der jeweiligen normativen Teleologie gerecht werden muss. Richtigerweise ist deshalb nicht zwingend der ökonomische Begriff inkludiert und von diesem zu trennen.[26] Das Ziel einer reinen Definition für das Recht reduziert den Geltungsdrang und lässt eine passgenaue und weniger umgreifend abstrakte Definition zu. Wenngleich erfolgt diese nicht im Sinne von ***Knapp*** rein rechtlich. Die bloße Schöpfung des Rechts geht mit der Erwartung einer Legaldefinition einher, die nicht zu finden ist.[27] Das Recht regelt außerdem Lebenssachverhalte und ist daher deskriptiver Natur, was sich im Telos vieler Normen niederschlägt.[28] Eine Abstraktion von den tatsächlichen Funktionen wäre lebensfremd. Deutlich wird dies am Beispiel des Schadensrechts. Wird nach § 249 Abs. 2 S. 1 BGB der erforderliche ***Geld***betrag gezahlt, dient dies der Restitution des schadensfreien Zustands.[29] Ermöglicht wird das durch Geld als Universaltauschmittel. Bei § 433 Abs. 2 BGB wird neben der Vereinbarung zum Ein-

25 Vgl. in etwa *Gerber,* Geld und Staat, 2, 88; *Simitis*, AcP 159 (1960/1961), 406 (418); *Nussbaum,* Das Geld in Theorie und Praxis des deutschen und ausländischen Rechts, 13.
26 Differenzierung zwischen rechtlichem und wirtschaftlichem Begriff schon bei: *Helfferich,* Das Geld, 321; *Lütge,* Einführung in die Lehre vom Gelde, 13.; *Liefmann,* Geld und Gold, 95; *Forstmann,* Geld und Kredit, 65 f.; *Simitis*, AcP 159 (1960/1961), 406 (418) sieht dies und versucht trotzdem Geld als *„gesellschaftliche Kategorie"* einheitlich zu definieren.
27 *Herrmann,* Währungshoheit, Währungsverfassung und subjektive Rechte, 59.
28 *Schmidt,* Geldrecht, Vorbem. zu § 244, Rn. A 1; *Omlor* in v. Staudinger/Höpfner/Kaiser, BGB, vor § 244, Rn. A63.
29 *Flume* in Hau/Poseck, BeckOK, § 249, Rn. 3; *Rüßmann* in Herberger/Martinek/Rüßmann/u.a., BGB, § 249, Rn. 1; *Teichmann* in Jauernig BGB, § 249, Rn. 1; *Dörner* in Schulze, BGB, § 249, Rn. 1.

satz als Tauschmittel die Recheneinheitsfunktion deutlich. Die Parteien können in Ausübung der Privatautonomie die Kaufsache beziffern und sich so auf einen Preis einigen. Zu bestimmen ist somit (nur) die Definition für die rechtliche Behandlung, die der normativen Verwendung des Begriffes Geld gerecht wird. Ein ökonomischer Begriff verfolgt andere Bedürfnisse. Ein Gleichlauf mit rechtlicher Anschauung ist denkbar, aber nicht zwingend.

2. Relativität des Begriffes „Geld" – Zweigliedrigkeit

Orientierung bietet deshalb die rechtliche Verwendung des Begriffs. Nur so kann dem Zweck der einzelnen verwendenden Normen gerecht werden. Unumstritten ist, dass dieser in der deutschen Rechtsordnung nicht einheitlich benutzt wird.[30] Das wird schon durch einen systematischen Blick auf das BGB deutlich. Bei den §§ 935 Abs. 2, 1007 Abs. 2 S. 2 BGB kann es sich durch die Stellung im Sachenrecht nur um körperliche Gegenstände im Sinne von § 90 BGB handeln. Auch in § 698 BGB muss es sich durch Verortung im Normkomplex der Verwahrung nach § 688 BGB um eine bewegliche Sache handeln. Wortlaut und Systematik setzen das Erfordernis einer Verkörperung bei der Verwendung in den §§ 700 Abs. 1, 702 Abs. 3 S. 1 BGB fort. Entgegen steht eine Vielzahl von Normen, die nicht auf eine bewegliche Sache Bezug nehmen. Zuvor wurde die Orientierung des § 249 Abs. 2 S. 1 BGB an der Tauschmittelfunktion des Geldes dargelegt. Nach Sinn und Zweck setzt der Geldbegriff in den §§ 249 Abs. 2 S. 1, 250, 251 Abs. 1 und 253 Abs. 1 BGB durch diesen Funktionsbezug keine zwingende Verkörperung voraus. Das Erfordernis wird auch bei § 488 Abs. 1 BGB durch den nicht sachenrechtlichen Wortlaut und im Umkehrschluss zu § 607 BGB verneint.[31] Zuletzt dient die Verwendung in § 270 Abs. 1 BGB als Beispiel. Die Norm ist bei der Schuld von bestimmten gegenständlichen Geldstücken nicht anwendbar,[32] was eine weitere Definition als die der sachenrechtlich fokussierten Normen erfordert.

Es ergibt sich eine relative Bedeutung des Geldbegriffs im BGB.[33] Relativ ist der Begriff, weil er von seiner jeweiligen Verwendung abhängt. Hiervon lässt sich eine zweigliedrige Definition ableiten.[34] Dadurch kann der jeweiligen normativen Verwendung Rechnung getragen werden und dennoch abweichend von einer reinen Einzelfallentscheidung eine systematische Betrachtung stattfinden.

Darstellung der Zweiteilung des relativen Geldbegriffs

a) Funktionsbezogener Begriff

Auf der einen Seite der Zweigliedrigkeit steht ein funktionsbezogener Begriff. Dieser ist im Wesentlichen durch die klassischen Geldfunktionen geprägt und vom Erfordernis der Verkörperung freigestellt.[35] Dadurch wird der Immaterialisierung im Geldverkehr Rechnung getragen, ohne den tradierten gegenstandsbezogenen Normen den Boden zu nehmen. Sie werden auf die andere Seite der zweiteiligen Definition verwiesen. Der Begriff erschöpft sich nicht darin und ist mithin nicht identisch mit

30 *Isele*, AcP 129 (1928), 129 (184); *Thywissen,* BB 1971, 1347 (1348 f.); mangelndes Bewusstsein hierfür weist *Skauradszun,* AcP 221 (2021), 354 (369) auf, der die Bedeutung im Rahmen der §§ 935 Abs. 2 BGB, 146 ff. StGB verallgemeinert, obwohl das zweite referenzierte Urteil (BGH: NJW 1984, 1311 (1311)) ausdrücklich auf die Geltung im Sinne der Strafrechtsnorm verweist.
31 *Omlor,* Geldprivatrecht, 69.
32 *Krüger* in Säcker/Rixecker/Oetker/u.a., Münchener Kommentar zum BGB, § 270, Rn. 3; *Kerwer* in Herberger/Martinek/Rüßmann/u.a., BGB, § 270, Rn. 5; *Bittner/Kolbe* in v. Staudinger/Höpfner/Kaiser, BGB, § 270, Rn. 7.
33 Schon: *Isele*, AcP 129 (1928), 129 (184); *Simitis,* AcP 159 (1960/1961), 406 (408); *Nussbaum*, Das Geld in Theorie und Praxis des deutschen und ausländischen Rechts, 3; *Veit,* Reale Theorie des Geldes, 56 will davor bewahren den theoretischen Geldbegriff zu fassen.
34 Schon bei *Liefmann*, Geld und Gold, 95, wenn auch zwischen ökonomisch und rechtlichem Begriff; explizit im rechtlichen Sinne: *Schmidt,* Geldrecht, Vorbem. zu § 244, Rn. A 11; *Omlor,* Geldprivatrecht, 98; *Omlor* in v. Staudinger/Höpfner/Kaiser, BGB, vor § 244, Rn. A62; hingegen vertritt *Herrmann,* Währungshoheit, Währungsverfassung und subjektive Rechte, 78 eine Einzelfallentscheidung bei jeder Norm, wobei von einem „*vorrechtlichen Geldbegriff*" ausgegangen wird. Damit wird zwischen einem ökonomischen und juristisch vielgliedrigen Begriff unterschieden. Dies verhindert eine Systematisierung der geldrechtlichen Normen und ist daher abzulehnen.
35 *Omlor,* Geldprivatrecht, 98; Schmidt, Geldrecht, Vorbem. zu § 244, Rn. A 14, 18.

den volkswirtschaftlichen Theorien, die sich in einer Gleichstellung mit den klassischen Funktionen begrenzen. Als Rechtsbegriff ist eine zumindest rudimentäre Anerkennung durch die Rechtsordnung erforderlich und dient als Indiz der Geldeigenschaft.[36] Es scheint widersprüchlich, etwas als Geld im rechtlichen Sinne einer Norm zu behandeln, wenn die normative Ordnung einer solchen Behandlung nicht offensteht. Eine tatsächliche Übung des Verkehrs genügt nicht.

b) Gegenstandsbezogener Begriff

Der funktionsbezogene Geldbegriff ermöglicht, diesem einen gegenstandsbezogenen Begriff im engeren Sinne zur Seite zu stellen, der einer strengeren normativen Verwendung gerecht wird. Darunter sind bewegliche Sachen zu verstehen, die allgemein als Tauschmittel dienen und als gesetzliches Zahlungsmittel mit einem Annahmezwang versehen sind.[37] Dieser Begriff spiegelt das historische Verständnis eines staatlichen Sachgelds wider. Es ist zur Handhabung der zuvor genannten Normen mit gegenständlichem Bezug relevant.

Entsprechend ***Knapp*** folgt hieraus ein chartales Zahlungsmittel, dessen Wert also nicht aus dem Stoff des Gegenstandes, sondern aus der staatlichen Anerkennung folgt.

III. Subsumtion der Kryptowährungen

Ob Kryptowährungen als Geld im Sinne des deutschen Rechts qualifiziert werden können, ist anhand der zwei obigen Begriffe zu messen. Mangels einer Verkörperung der Token kann eine Einordnung unter den gegenstandsbezogenen Begriff schnell abgelehnt werden. Dies wird durch die alleinige Anerkennung des Euro als gesetzliches Zahlungsmittel in Deutschland gem. Art. 10 S. 2 VO (EG) Nr. 974/98 und dem wortgleichen § 14 Abs. 1 S. 2 BBankG weiter gestützt. Ein Annahmezwang für Kryptowährungen besteht nicht. Somit steht die fehlende Einordnung als bewegliche Sache und die fehlende Eigenschaft als gesetzliches Zahlungsmittel entgegen, um Currency Token als Geld in einem gegenständlichen Sinne zu qualifizieren. Eröffnet und begrifflich näher ist die funktionsbezogene Definition. Diese setzt sich aus den Geldfunktionen und der rechtlichen Anerkennung zusammen.

1. Funktionstrias

a) Universaltauschmittel

Aus der Trias [Universaltauschmittel, Wertaufbewahrung, Rechnungseinheit, siehe Abbildung 1] stellt die Eigenschaft als Universalttauschmittel die Hauptfunktion dar.[38] Als Treiber der Arbeitsteilung ist es so möglich, zu umgehen, dass der Tauschpartner nicht nur das Gewollte anbietet, sondern auch das ihm Angebotene will (sog. doppelte Bedarfskoinzidenz).[39] Ansonsten besteht die Schwierigkeit, eine Übereinstimmung zu finden: Es muss am gleichen Ort und zur gleichen Zeit Interesse am jeweiligen Gut bestehen. Das Tauschmittel umgeht diese unmittelbare Bedarfsbefriedigung, da es zeitlich, räumlich und gegenständlich mittelbar für das jeweilige Interesse eingesetzt werden kann. Der universale Charakter verbürgt den nicht nur begrenzten Einsatz. Um die Erfüllung dieser Eigenschaft bei Kryptowährungen zu betrachten, muss evaluiert werden, inwieweit diese vor allem im Handel eingesetzt werden können. Bitcoin ist die am weitesten verbreitete Kryptowährung.[40] Zunächst etablierte sich dieser als Tauschmittel am bekannten Beispiel der Plattform ***Silk Road*** vorwiegend für illegale Geschäfte im Internet. Durch den Kursanstieg und die damit einhergehende gesellschaftliche Bekanntheit wurde Bitcoin in den letzten Jahren

36 *Omlor* in v. Staudinger/Höpfner/Kaiser, BGB, vor § 244, Rn. A67; *Omlor*, JZ 2017, 754 (759); *Schmidt,* Geldrecht, Vorbem. zu § 244, Rn. A 2 macht dies am Beispiel der *„Zigarettenwährung"* nach dem Zweiten Weltkrieg deutlich; *Hahn/Häde*, Währungsrecht, § 3 Rn. 10 fordern eine Verankerung im staatlichen Recht; wird auch weitestgehend in der Kommentarliteratur vorausgesetzt: *Grundmann* in Säcker/Rixecker/Oetker/u.a., Münchener Kommentar zum BGB, § 245, Rn. 10; *Martens* in Grunewald/Maier-Reimer/Westermann, Erman, § 244, Rn. 3; *Toussaint* in Herberger/Martinek/Rüßmann/u.a., BGB, § 244, Rn. 5.

37 *Schmidt*, Geldrecht, Vorbem. zu § 244, Rn. A 12; Omlor, Geldprivatrecht, 100 ff.; *Omlor* in v. Staudinger/Höpfner/Kaiser, BGB, vor § 244, Rn. A84 ff.

38 *Spiegel*, Blockchain-basiertes virtuelles Geld, 27 m.w.N.

39 *Herrmann*, AcP 218 (2018), 285 (388).

40 Siehe Fn. 25.

primär zum Anlageobjekt.[41] Im Internet lassen sich einige Anbieter finden, die bereit sind Waren oder Dienstleistungen gegen Kryptowährungen und damit vor allem Bitcoin zu veräußern. Auch außerhalb des E-Commerce sind zuweilen Angebote zu finden.[42] Diese beschränken sich jedoch meist auf spezielle Dienstleistungen. Mit Bitcoin bezahlbare Güter zum allgemeinen Lebensbedarfs werden in Deutschland vergeblich gesucht. Die geringe Verbreitung steht der Voraussetzung einer universellen Einsetzbarkeit entgegen. Es wäre kaum mit dem Telos von Normen wie den §§ 249 ff. BGB vereinbar, Bitcoin so unter den dort verwendeten Geldbegriff zu subsumieren. Eine Restitution des Status Quo ist nicht denkbar, denn Kryptowährungen sind nur über den Umtausch in andere Zahlungsmittel frei einsetzbar. Dann kann nicht von einer Lösung der doppelten Bedarfskoinzidenz die Rede sein, wenn vor allem im alltäglichen Leben die Einsatzmöglichkeit die Ausnahme darstellt. Die geldtechnische Hauptfunktion wird entsprechend weitestgehend abgelehnt.[43]

b) Wertaufbewahrung

Auch am Vorliegen der Funktionen der Wertaufbewahrung und der Recheneinheit lässt sich aufgrund der Volatilität zumindest zweifeln.[44] Bei den originären Kryptowährungen, die keine ***Asset-Backed-Stablecoins*** sind, bilden historisch betrachtet Kurssprüngen von 100 % Zugewinn oder 50 % Verlust innerhalb eines Monats keine Seltenheit.[45] Dies führt zur beschriebenen Bewegung vom Zahlungsmittel hin zum Anlage- und Spekulationsobjekt. Sinn der Wertaufbewahrung besteht im Transfer von Kaufkraft in die Zukunft.[46] Ein möglicher starker Kursabfall steht der durch die relative Wertstabilität verbürgten Sicherheit des künftigen Einsatzes als Tauschmittel entgegen. Das Individuum kann sich nicht sicher sein, ob die betreffende Kryptowährung in naher Zukunft ein Tausch gegen Waren auf ähnlichem Niveau zulässt. Dabei verfängt sich der Vergleich mit der Inflation bei staatlichen Währungen:[47] Zwar stellt deren Inflation ebenfalls einen Verlust der in die Zukunft transferierten Kaufkraft dar, allerdings beschränkt sich dieser in westlichen Staaten oft auf einen mittleren einstelligen Prozentsatz, der regelmäßig voraussehbar ist. Kryptowährungen sind häufig in der Anzahl ausgegebener Token begrenzt und daher ab einem bestimmten Zeitpunkt nicht mehr inflationär oder bei steigender Nachfrage sogar deflationär.[48] Der Wert richtet sich allein nach Angebot und Nachfrage. Dies führt zu teils unkontrollierbarem und sehr hohem Wertverfall bis hin zur totalen Wertlosigkeit. Weil dies meist nicht voraussehbar ist, kann dies m.E. nicht mit dem Wertverlust staatlicher Währungen durch das Fehlen einer Kontinuität verglichen werden. Sieht man die Wertaufbewahrung als bloßes Element der Qualifikation als Tauschmittel,[49] liegt die erstgenannte Funktion a maiore ad minus nicht vor. Können Kryptowährungen nicht universal eingetauscht werden, ist auch ein gestreckter Tausch durch Wertaufbewahrung nicht möglich.

c) Rechnungseinheit

Die letzte der drei Funktionen, die der Rechnungseinheit, führt dazu, dass Preise und Schulden in einer Einheit ausdrückbar sind und dadurch Güter über diesen Referenzwert vergleichbar werden.[50] Der Wert des einen Gutes kann in Geld ausgedrückt und mit dem des anderen Gutes in Relation gesetzt werden. Eine Bejahung dieser Funktion erfolgt mit Blick auf die Kryptowährungen größtenteils rein theoretisch durch deren Stückelung.[51] Die Token bilden keine untrennbare Einheit, son-

41 *Sorge/Krohn-Grimberghe*, DuD 2012, 479 (481); *Omlor*, ZHR 183 (2019), 294 (312).
42 So auch schon EuGH: MMR 2016, 201 (203, Rn. 52); als Übersicht hierzu dient visuell, hier abrufbar: von größeren Anbietern akzeptiert bis jetzt nur Lieferando die Zahlung mit Bitcoin, hier abrufbar; hingewiesen sei weiterhin auf das neu auftretende Phänomen der sog. Krypto-Kreditkarten, die jedoch bei Verwendung zur Bezahlung eine Umwandlung in die entsprechende FIAT-Währung durchführen.
43 *Grothe* in Hau/Poseck, BeckOK, § 244 Rn. 2; *Schäfer/Eckhold* in Assmann/Schütze/Buck-Heeb, Hdb. des Kapitalanlagerechts, § 16a, Rn. 33; *Omlor,* JZ 2017, 754 (760); *Omlor,* ZHR 183 (2019), 294 (314); a.A.: *Beck,* NJW 2018, 580 (583) charakterisiert als „*überindividuell anerkanntes Tauschmittel*"; *Freitag* in Gsell/Krüger/Lorenz/Reymann, BeckOGK, § 244, Rn. 28; *Spindler/Bille,* WM 2014, 1357 (1361); *Lerch*, ZBB 2015, 190 (199).
44 *Grundmann* in Säcker/Rixecker/Oetker/Limperg, Münchener Kommentar zum BGB, § 245, Rn. 10; *Spiegel*, Blockchain-basiertes virtuelles Geld, 33; *Langenbucher,* Digitales Finanzwesen, AcP 218 (2018), 285 (394).
45 Übersicht der historischen Kursverläufe ist hier abrufbar.
46 *Mankiv,* Macroeconomics, 80; *Hahn/Häde*, Währungsrecht, § 1 Rn. 36; *Grundmann* in Säcker/Rixecker/Oetker/u.a., Münchener Kommentar zum BGB, § 245, Rn. 2; *Langenbucher,* AcP 218 (2018), 285 (388).
47 *Beck*, NJW 2018, 580 (584); *Lerch,* ZBB 2015, 190 (199); *Spindler/Bille*, WM 2014, 1357 (1361),
48 Bei Bitcoin beträgt die Anzahl 21 Millionen. und soll im Jahre 2140 erreicht sein: *Nakamoto,* Bitcoin – A Peer-to-Peer Electronic Cash System, 4; bei Ethereum ist die Anzahl zwar nicht begrenzt, die Neuemission sinkt aber exponentiell und geht auf lange Sich gen 0: *Buterin,* Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 31.
49 Siehe Fn. 20.
50 *Mankiv,* Macroeconomics, S. 80; *Grundmann* in Säcker/Rixecker/Oetker/u.a., Münchener Kommentar zum BGB, § 245, Rn. 4.
51 *Spiegel*, Blockchain-basiertes virtuelles Geld, 37; Omlor, JZ 2017, 754 (759); Lerch, ZBB 2015, 190 (199).

dern lassen sich in mehrere Dezimalstellen untergliedern.[52] Ein Wert kann dadurch passgenau durch die Kryptowährung ausgedrückt werden. Kritisch könnte wiederum die einleitend erläuterte Volatilität sein. Rein theoretisch können Güter über die Dezimalstellen der Kryptowährungen in Relation gesetzt werden. Praktisch stößt dies bei hohen Preisschwankungen auf Schwierigkeiten. Will man nun Werte genau vergleichen, ist zusätzlich zur Einheit in Kryptowährungen ein Referenzzeitpunkt für dessen eigene Wertbestimmung nötig. Die wirtschaftliche Koordination wird ineffizient[53] und ein theoretischer Referenzwert bildet wenig Mehrwert.

2. Rechtliche Anerkennung

Letztendlich steht der Qualifikation als Geld im Rechtssinne nicht nur die Skepsis der Funktionserfüllung, sondern auch die de lege lata fehlende rechtliche Anerkennung entgegen. Die Deklarierung zum staatlichen Zahlungsmittel, wie es in El Salvador oder der Zentralafrikanischen Republik zuletzt geschehen ist,[54] muss hierzu nicht erfolgen. Der abstrakte Geldbegriff ist funktionsgetrieben im Gegensatz zum gegenstandsbezogenen, welcher am Annahmezwang festhält. Der Token ist als solcher ein rechtlich nicht speziell geschütztes Immaterialgut, er ist also schlichtweg im Zivilrecht nicht geregelt. Daran ändert sich auch nichts, wenn die BaFin Kryptowährungen als Rechnungseinheit i.S.v. § 1 Abs. 11 S. 1 Nr. 7 KWG einstuft.[55] Als Handeln der Exekutive sagt es nichts über die legislative Öffnung aus und bezieht sich bereichsspezifisch nur auf das Kreditwesen. Ebenso ist es mit der mehrfachen Nennung von ***virtuellen Währungen*** in der 5. Geldwäscherichtlinie (RL (EU) 2018/843). Der deutsche Gesetzgeber verwendet hingegen den Begriff der ***Kryptowerte*** (z.B. in §§ 1 Abs. 29, 30; 10 Abs. 3 Nr. 2 c), … GWG) und nicht den europarechtlich angetragenen Begriff mit seiner geldrechtlichen Konnotation. Außerdem ist unzweifelhaft eine Kenntnisnahme der geldwäscherechtlichen Relevanz nicht als rechtliche Anerkennung der Geldeigenschaft im normativen Sinne zu interpretieren. Den Kryptowährungen mangelt es an einer eigenständigen rechtlichen Anerkennung.[56] Es bleibt nur ein Rückgriff auf die Einordnung unter bereits rechtlich anerkanntes. Hierbei sind die Kategorien des Buchgeldes und des E-Geldes relevant. Die rechtliche Anerkennung von Buchgeld folgt aus dem detailliert normierten Zahlungsdiensterecht der §§ 675c ff. BGB.[57] Die Rechtsordnung zeigt sich offen für solch ein entmaterialisiertes Geldphänomen. Buchgeld ist eine Geldforderung gegen ein Kreditinstitut, die in Guthaben dargestellt ist und jederzeit zu Zahlungszwecken eingesetzt werden kann.[58] Dem liegt als Forderung ein abstraktes Schuldversprechen des jeweiligen Kreditinstituts zugrunde.[59] Hinsichtlich des E-Geldes verweist der § 675c Abs. 3 BGB auf die Definition aus § 1 Abs. 2 S. 3 ZAG. Es ist *„**jeder elektronisch, darunter auch magnetisch, gespeicherte monetäre Wert in Form einer Forderung an den Emittenten, der gegen Zahlung eines Geldbetrags ausgestellt wird*** […]“. Aufgrund der parallelen Struktur durch die Darstellung einer Forderung wird E-Geld als

§ 1 XI 4 KWG:

„Kryptowerte im Sinne dieses Gesetzes sind digitale Darstellungen eines Wertes, der von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen aufgrund einer Vereinbarung oder tatsächlichen Übung als Tausch- oder Zahlungsmittel akzeptiert wird oder Anlagezwecken dient und der auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann.“

52 Ein Bitcoin lässt sich in Einheiten auf 8 Dezimalstellen (sog. Satoshis) unterteilen. Bei Ethereum ist diese Unterteilung sogar auf 18 Dezimalstellen in die kleinste Einheit „*Wei*“ möglich.
53 *Issing, Hayek* – currency competition and European Monetary Union, 4.
54 *Patz*, BKR 2021, 725 (Fn. 7); *Müller,* Zentralafrikanische Republik erklärt Bitcoin zum offiziellen Zahlungsmittel.
55 LG Berlin: BeckRS 2017, 152022; außerdem justizierte das KG Berlin dem widersprechend in KG Berlin: NJW 2018, 3734 (3734).
56 *Spindler/Bille*, WM 2014, 1357 (1361); *Martens* in Grunewald/Maier-Reimer/Westermann, Erman, § 244, Rn. 7; *Lerch,* ZBB 2015, 190 (200) kommt zum Ergebnis, dass Kryptowährungen daher nur privates Geld sind, ohne Hinweis auf daraus folgende Auswirkungen; *Omlor,* JZ 2017, 754 (760).
57 *Omlor,* ZHR 183 (2019), 294 (312).
58 *Martens* in Grunewald/Maier-Reimer/Westermann, u.a., § 244, Rn. 5; *Toussaint* in Herberger/Martinek/Rüßmann/u.a. BGB, § 244, Rn. 10; *Omlor* in v. Staudinger/Höpfner/Kaiser, BGB, vor § 244, Rn. A149.
59 *Haug* in Schimansky/Bunte/Lwowski, Bankrechts-Handbuch § 123, Rn. 52.

Buchgeld mit elektronischer Speicherung verstanden.[60] Gemein ist beiden mithin die Forderung gegen einen Emittenten. Kryptowährungen sind durch die Dezentralität gekennzeichnet. Mangels einer zentralen Instanz handelt es sich bei Token um keine Forderung. Damit fallen sie auch nicht unter das Buchgeld oder die Unterform des E-Geldes. Es lässt sich für eine rechtliche Anerkennung auch nicht auf bestehende Kategorien nach §§ 675c ff BGB zurückgreifen. Die Rechtsordnung ist schlicht nicht offen für die Einstufung von Kryptowährungen als Geld im rechtlichen Sinne.

IV. Auswirkung

So lässt sich im Ergebnis festhalten, dass zum jetzigen Zeitpunkt keine Kryptowährungen unter einen der Geldbegriffe fällt. Diese Einstufung wäre auf der einen Seite bezüglich der jeweiligen Kryptowährung eine universelle Einsatzmöglichkeit und begrenzte Volatilität nötig. Außerdem erfordert es – unabhängig von deren Gestaltung und Akzeptanz – eine rechtliche Anerkennung nach zukünftigen Recht. Bis dahin gilt: Kein Token ist Geld! Dies führt zunächst zum naheliegenden Ergebnis, dass Geldschulden ohne anderweitige Vereinbarung nicht in Kryptowährungen gem. § 362 Abs. 1 BGB erfüllbar sind. Eine Erfüllungswirkung braucht neben der tatsächlichen Übertragung einer Annahme an Erfüllung statt, § 364 Abs. 1 BGB. Da der Gläubiger hierzu nicht verpflichtet ist, kann er die Annahme verweigern und gerät nicht nach §§ 293 ff. BGB in Verzug. Weiter verschließen sich die Normen des Geldschuldrechts einer direkten Anwendung. Die Auswirkung und womöglich privatautonome Übertragbarkeit bedürfen einer tiefgehenden Untersuchung.

Es bleibt festzuhalten: Juristisch richtig sind Kryptowährungen zwar Zahlungsmittel, aber kein Geld.

B. Währung

Die geldrechtliche Einordnung des Currency Tokens lässt noch eine verwandte terminologische Richtigstellung zu. An den Begriff des Geldes schließt sich derjenige der Währung an. Im Verlauf des Aufsatzes war häufig von Krypto***währungen*** die Rede. Dies resultiert aus der alltäglich vorherrschenden Nomenklatur für Currency Token, soll aber nicht über die rechtliche Bedeutung hinwegtäuschen. Allein die bisherige Verwendung impliziert nicht, dass es sich bei der Gesamtheit solcher Coins um eine Währung im Rechtssinne handelt. Es verdeutlicht nur die vor allem im Alltag häufige Begriffsvermischung mit dem Begriff des Geldes.[61] Richtigerweise wird rechtlich unter der Währung die Geldverfassung eines Staates als Gesamtheit der Regeln und die ideelle Rechnungseinheit derselben verstanden.[62] Diesen Begriff legt auch das Währungsrecht zugrunde, da es seinem Inhalt nach um die Abgrenzung hoheitlicher Geldverfassungen geht.[63] In ihrem Ideal sind Kryptowährungen unabhängig von einer zentralen Instanz und daher ein Gegenkonstrukt zu staatlichen Währungen. Sie sollen zu einem dezentralen Zahlungsverkehr ohne fremde Einflussnahme durch Geldpolitik führen. Diese staatliche Unabhängigkeit sorgt nicht nur für Probleme im rechtlichen Umgang, sondern lässt sie auch aus dem rechtlichen Währungsbegriff herausfallen. Richtigerweise dürfte juristisch nicht von einer Kryptowährung die Rede sein.[64] Allerdings prägt dieser Begriff den alltäglichen Diskurs und wird für alle Currency Token verwendet. Der alltägliche Sprachgebrauch passt sich dieser Verwendung an, ist aber frei von rechtlicher Wertung.

C. Ergebnis

Blickt man zurück auf ***Hayeks*** Zitat, so sind Kryptowährungen bis dato wohl nicht die erhoffte Weiterentwicklung des großartigsten Werkzeugs der Freiheit. Verwendet das Gesetz die Terminologie „Geld“, so folgt dies aus einer rechtlichen Perspektive. Über die wirtschaftswissenschaftliche Einordnung von Kryptowährungen ist

60 *Freitag* in Gsell/Krüger/Lorenz/u.a., BeckOGK, § 244, Rn. 17; *Omlor* in v. Staudinger/Höpfner/Kaiser, BGB, vor § 244, Rn. A152.

61 *Herrmann*, Währungshoheit, Währungsverfassung und subjektive Rechte, 73.
62 *Helfferich*, Das Geld, 412; *Reinhuber,* Grundbegriffe und internationaler Anwendungsbereich von Währungsrecht, § 1 6; *Vischer,* Geld- und Währungsrecht im nationalen und internationalen Kontext, 29 Rn. 45; *Seiler* in Epping/Hillgruber, BeckOK GG, Art. 73, Rn. 14; *Herrmann,* Währungshoheit, Währungsverfassung und subjektive Rechte, S. 78; *Omlor,* ZHR 183 (2019), 294 (307), *Samm, „Geld“* und *„Währung“* – begrifflich und mit Blick auf den Vertrag von Maastricht, 235 f..
63 *Schäfer/Eckhold* in Assmann/Schütze/Buck-Heeb, Hdb. des Kapitalanlagerechts, § 16a, Rn. 34; *Omlor,* ZHR 183 (2019), 294 (307).
64 Häufig ist daher die Rede von Kryptowerten.

damit keine Aussage getroffen. Die Verwendung lässt sich wiederum in einen relativen, zweigliedrigen Geldbegriff teilen. Kryptowährungen erfüllen keine der beiden Definitionen. Schädlich ist letztendlich die mangelnde Offenheit der Rechtsordnung und ein Fehlen der klassischen Geldfunktionen. Obwohl mit Kryptowährungen auch bezahlt werden kann, sind sie kein Geld! Und mangels Staatlichkeit auch keine Währung!

„Obwohl man mit Kryptowährungen zahlen kann, sind sie kein Geld und mangels Staatlichkeit auch keine Währung!“

Weiterführende Hinweise:

Talking Legal Tech – Folge 5

“Was ist die Blockchain, Florian Glatz?”

ETHICS x AI in Helsinki 2022 – Ein Veranstaltungsbericht

Legal Tech

„ETHICS x AI“ in Helsinki 2022 – Ein Veranstaltungsbericht

Louis Goral-Wood

Open Peer Review

Dieser Beitrag wurde lektoriert von: Ramon Schmitt

Louis hat an der Universität zu Köln Jura mit dem Schwerpunkt Völker- und Europarecht studiert. Er bereitet aktuell seine Promotion an der Schnittstelle zwischen internationalem Investitionsschutzrecht und Cybersicherheitsrecht vor.

Am 13. Mai 2022 fand in Helsinki die internationale Konferenz „***ETHICS x AI – Putting ethical AI into practice***“, seit 2019 die nunmehr dritte Veranstaltung der Reihe „***ETHICS x AI***“, statt. Ausgerichtet wurde die Veranstaltung von der ***Deutschen Botschaft in Helsinki***, der ***Deutschen Gemeinde in Finnland***, der ***Außenhandelskammer Finnland*** und dem ***Goethe-Institut Finnland***. Im Zuge der eintägigen Veranstaltung entstand ein reger Diskurs zwischen Akteuren aus Wirtschaft, Forschung, Recht, Kunst und Religion mit spannenden Gedankenanstößen zur praktischen Implementierung ethischer Standards für Künstliche Intelligenz.

Eine Aufzeichnung der „***ETHICS x AI***“ 2022 kann hier abgerufen werden.

A. KI und Ethik in Helsinki? – Finnland als treibende Kraft europäischer KI-Entwicklung

Die finnische Hauptstadt Helsinki eignet sich, vor dem Hintergrund der Bemühungen Finnlands um eine Förderung des Einsatzes von KI in Wirtschaft, Forschung und Staat, hervorragend als Austragungsort für eine Veranstaltung zu KI und Ethik: Bereits im Jahr 2017 stellte die finnische Regierung mit ihrer nationalen Strategie für Künstliche Intelligenz 200 Mio. € für Investitionen in finnische KI-entwickelnde Unternehmen und Forschungseinrichtungen bereit. Dabei bemüht man sich auch um eine Stärkung der Digitalkompetenz finnischer Bürger: Die Informatikfakultät der ***Universität Helsinki*** entwickelte die Online-Schulungsreihe „***Elements of AI***“, die Finnen die technischen Grundlagen Künstlicher Intelligenz vermittelt. Im Zuge der finnischen Ratspräsidentschaft 2019 wurde dieses Angebot auf die gesamte EU ausgeweitet und allen Unionsbürger in sämtlichen Amtssprachen der EU zur Verfügung gestellt (hier kann „Elements of AI“ in deutscher Sprache abgerufen werden). Die diesjährige „***ETHICS x A***I“ unterteilte sich in zwei Abschnitte. Sie startete in den Vormittag mit vier Keynotes zu unterschiedlichen Perspektiven der praktischen Umsetzung ethischer KI.

Die einzelnen Keynote-Speaker diskutierten anschließend gemeinsam im Rahmen einer Podiumsdiskussion ihre Ansätze. Am Nachmittag folgten Workshops, eine künstlerische Darbietung und Vorträge sowie ein Fireside-Chat.

B. Kurzweilige Keynotes zu Künstlicher Intelligenz und Ethik

Maxime Lebrun vom *European Centre of Excellence for countering hybrid threats* (***hybrid COE***) hielt die erste Keynote zum Thema „***The power to foresee society, an imperative for AI systems accountability***“. Unter Bezugnahme auf den Cambridge Analytica Skandal und den Sturm auf das US-Kapitol durch Trump-Anhänger am 6. Januar 2021, beleuchtete er die Fähigkeit von KI-Systemen Vorhersagen über individuelles und gesamtgesellschaftliches Verhalten zu treffen.

Maxime Lebrun **trägt zu „*The power to foresee society, an imperative for AI systems accountability*“ vor.**

Michael Hanf **(Moderation),** ***Taina Kalliokoski*****,** ***Nitin Sawhney*****,** ***Meeri Haataja*** **und** ***Maxime Lebrun*** **(von links nach rechts) diskutieren ihre unterschiedlichen Ansätze zu Implementierung ethischer Leitlinien in der praktischen KI-Entwicklung.**

Dieser Fähigkeit von KI-Systemen wohne, so ***Lebrun***, die Gefahr einer Erosion der Grundstrukturen freiheitlicher Demokratien inne. KI könne genutzt werden, um einzelne gesellschaftliche Gruppen zu radikalisieren und nachhaltig den gesamtgesellschaftlichen Zusammenhalt zu zerstören. Nach seiner Ansicht kann diesem Bedrohungspotenzial in dreifacher Weise entgegengewirkt werden: Es bedarf eines „***technology ownership***", d.h. die Zuweisung von Verantwortung für KI-Systeme durch die Etablierung rechtlich durchsetzbarer Kontrollmechanismen, stets eines „***human in the loop***" (d.h. einer menschlichen Aufsicht) und der Entwicklung hinreichender technischer Ansätze, welche die Erklärbarkeit von KI (engl. „***explainability***") gewährleisten.

Welche Auswirkungen der Einsatz von KI auf gesamtgesellschaftliche Entwicklungen haben könnte, war auch Gegenstand des sich daran anschließenden Vortrags von Dr. ***Taina Kalliokoski***, einer Wissenschaftlerin der Theologischen Fakultät der Universität Helsinki. Sie stellte in ihrem Vortrag „***Merciful Community in the Age of AI***" Überlegungen dazu an, ob und wie der zunehmende Einsatz Künstlicher Intelligenz das soziale Miteinander beeinflussen könnte.

Professor ***Nitin Sawhney***, Leiter der ***Critical AI and Crisis Interrogatives*** (***CRAI-CIS***) Forschungsgruppe an der Fakultät für Informatik der ***Universität Aalto*** in Finnland beschäftigte sich in seiner Keynote mit dem Thema „***Civic agency in the age of AI***". Er fokussierte sich auf die Frage, wie gesellschaftliche Randgruppen in KI-Entwicklungsprozesse miteinbezogen werden könnten. Zudem stellte er dar, wie – aus der Perspektive eines Informatikers – ethische Leitlinien auf den unterschiedlichen Stufen der KI-Entwicklung praktisch implementiert werden können.

Daran schloss die letzte Keynote des Vormittags von ***Meeri Haataja*** an. ***Meeri Haataja*** ist Geschäftsführerin und Mitgründerin des finnischen Startups ***Saidot***. ***Saidot*** hat eine Plattform entwickelt, die KI-entwickelnden Unternehmen dabei hilft, Leitlinien verantwortungsvoller KI in ihre Entwicklungsprozesse zu implementieren. In ihrem Vortrag trug sie zum Thema „***Is there business in AI Ethics?***" vor und stellte das sich neue entwickelnde Geschäftsfeld von Beratungsunternehmen mit einer Spezialisierung auf KI und Ethik dar.

Im Anschluss wurden alle vier Perspektiven der Vortragenden in einer Podiumsdiskussion zusammengeführt. Die Diskussion fokussiert sich dabei insbesondere auf die bisher unzureichende Berücksichtigung der Perspektiven gesellschaftlicher Randgruppen im Rahmen der Entwicklung von KI und die Einbindung ethischer Leitlinien in die tatsächliche KI-Entwicklung. Dabei kamen alle Keynote Speaker einhellig zu dem Ergebnis, dass es nicht die „***eine***" Blaupause ethischer Leitlinien für KI-Entwicklung gebe, sondern das KI und Ethik kontextspezifisch verstanden werden muss.

C. Fireside-Chat: *„Regulation vs. Innovation — Two Mutual Exclusives?"*

Am Nachmittag fand ein Fireside-Chat zum Thema *„Regulation vs. Innovation – Two Mutual Exclusives?"* statt.

Die Ausgangshypothese: Häufig wird jede Form der Regulierung, insbesondere im Tech-Sektor, als solche – unabhängig von ihrem Inhalt – als innovationshindernd betrachtet. Vor dem Hintergrund des Kommissionsentwurfs für den Artificial Intelligence Act (AIA) diskutierten ***Philipp Mahlow***, Mitglied des ***Legal Tech Lab Cologne*** und der ***CTRL***-Redaktion, und ***Galith Nadbornik***, Regional Vice President Nordic bei der IT-Unternehmensberatung ***Gartner***, zum Spannungsverhältnis zwischen Regulierung und Innovationsförderung.

Philipp Mahlow **und** ***Galith Nadbornik*** **(von links nach rechts) tauschen Ihre Gedanken zum Verhältnis zwischen Regulierung und Innovationsförderung aus.**

Dabei kamen beide übereinstimmend zu dem Ergebnis, dass Regulierung nicht per se etwas Schlechtes sei. Gute KI-Regulierung könne aber nur dann gelingen, wenn die Perspektiven derjenigen hinreichende Berücksichtigung finden, die KI selbst entwickeln. Insoweit wurde aber gerade der Entwurf des AIA, u.a. mit der vorgesehenen technischen Konkretisierung über harmonisierte Normen sowie der Möglichkeit der Einsetzung von Regulatory Sandboxes, positiv gesehen.

Galith Nadbornik wies auf die Gefahr hin, dass eine ausufernde KI-Regulierung die Gefahr berge, die KI-Wettbewerbsfähigkeit der EU – insbesondere im Verhältnis zu den USA und China – zu unterlaufen. Es bestünde aber auch die Möglichkeit, soweit der EU am Ende ein hinreichend differenziertes Regelwerk gelinge, dass sie eine regulatorische Vorbildfunktion einnimmt und sich – ähnlich wie bereits im Rahmen der DSGVO – für KI-Regulierung ein *„Brussels Effect"* einstelle.

D. Workshop *"Case Study: The Dilemma of Responsible AI"*: Praktische Einblicke in den Umgang mit ethischen Dilemmata im Rahmen der KI-Entwicklung

Am Nachmittag fanden Workshops zu folgenden Themen statt:

- *„Case Study: The dilemma of responsible AI"*
- *„Ethics of shared Data and AI: How to manage the rights and responsibilities in company networks"*
- *„Translation, Ethics and digital spaces"*
- *„AI Ethics in Health and Diagnostics"*
- *„Feminist Frameworks for Equitable AI"*

Vincent Hofmann **(links) und** ***Susanna Mäkelä*** **(rechts) mit einer Workshop-Teilnehmerin (Mitte).**

Alle Workshops gaben den Teilnehmern die Möglichkeit diverse Einblicke in die praktische Implementierung ethischer Leitlinien in den KI-Entwicklungsprozess zu erhalten. Besonders spannend: der Workshop zu *„Case Study: the dilemma of responsible AI"*. ***Susanna Mäkelä***, Senior Director of Government Affairs bei ***Microsoft Finnland*** und ***Vincent Hofmann***, wissenschaftlicher Mitarbeiter am ***Humboldt Institute for Internet and Society*** in Berlin, stellten anhand des aktuellen ***Microsoft*** Forschungsprojekts *„**PeopleLens**"* (sog. ***Project Tokyo***) vor, mit welchen ethischen Dilemmata KI-Entwickler im Rahmen der Entwicklung einer Augmented-Reality-Brille, die soziale Interaktionen für blinde Menschen erleichtern soll, konfrontiert waren.

Mithilfe der in der Brille eingebauten Sensoren kann die Software bekannte Gesichter erkennen und deren Entfernung und Position durch akustische Hinweise wie Klicks, Töne und gesprochene Namen vermitteln. So ertönt zum Beispiel ein leises Klopfgeräusch, wenn der Kopf des Benutzers in die Richtung einer Person zeigt, und wenn sich diese Person in einem Umkreis von etwa drei Metern befindet, wird der Name der Person genannt. Dann hilft eine Reihe aufsteigender Töne dem Benutzer, seine Aufmerksamkeit auf das Gesicht der Person zu lenken.

Die Workshop-Teilnehmer wurden – genauso wie die Entwickler bei ***Microsoft*** im Zuge der Entwicklung der ***PeopleLens*** – mit einem ethischen Dilemma konfrontiert: Wie kann die ***PeopleLens*** einerseits ihr integratives Potenzial realisieren, indem sie blinden Menschen soziale Interaktionen ermöglicht, während ihre Nutzung andererseits die Privatsphäre Dritter wahrt, die mit der ***PeopleLens*** in Kontakt kommen. Gefordert waren insoweit keine originär (datenschutz-)rechtlichen Überlegungen, die sich bei Einsatz einer solchen ***PeopleLens*** naturgemäß auch stellen. Vielmehr sollten die Workshop-Teilnehmer anhand gezielter Fragen, eine Abwägung zwischen dem Entwicklungsziel der Inklusionsförderung und dem Schutz der Privatsphäre Dritter vornehmen. Dabei stellten sich viele schwierige Probleme im Hinblick darauf, welche Informationen die ***PeopleLens*** dem sehbehinderten Nutzer zur Verfügung stellen darf. Zum Beispiel: Soll die KI hinter der ***PeopleLens*** so entwickelt werden, dass sie erkennt, ob die erfasste Person ein religiöses Zeichen trägt? Schnell wurden sich die Workshop-Teilnehmer bewusst, welche Herausforderung nicht nur dieser Abwägungsprozess als solcher, sondern auch seine Integration in den eigentlichen Prozess der Entwicklung der Software darstellt.

Mehr Informationen zum ***Project Tokyo*** gibt es hier. Hier gibt es Näheres zum *„**Responsible AI Program**"* von ***Microsoft***.

Vom Zuckerhut zum Amazonas: 7 Gedanken zu Legal Tech in Lateinamerika

Vom Zuckerhut zum Amazonas: 7 Gedanken zu Legal Tech in Lateinamerika

Felipe Molina

Open Peer Review
Dieser Beitrag wurde lektoriert von: Theodor Himmel und Lisa Krebber

Felipe hat an der Universität zu Köln das Studium der Rechtswissenschaften absolviert. Derzeit arbeitet er als Produktmanager bei der rightmart Group. Daneben betreut er als Host den Podcast des Legal Tech Lab Cologne e.V. "Talking Legal Tech".

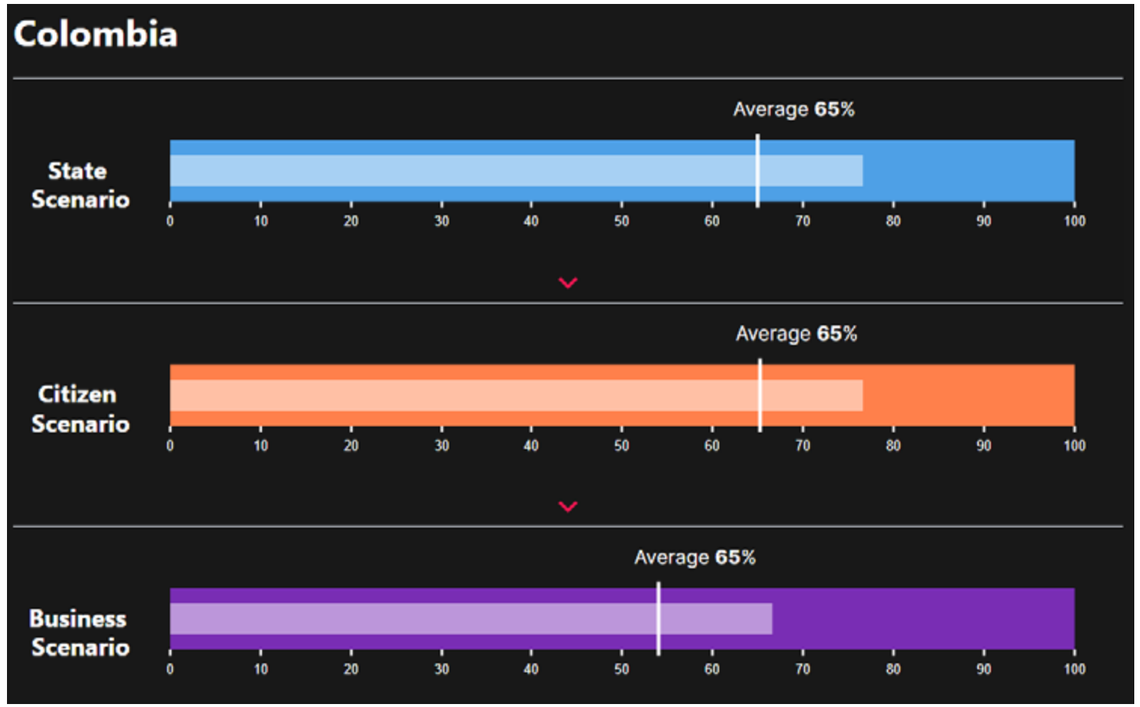
Grünes Licht für die digitale Justiz in Kolumbien" heißt es auf der kolumbianischen Seite impacto TIC.[1] Dabei ist es allerhöchste Zeit, dass sich Lateinamerika mit der Veränderung seines Rechtsmarktes und der Digitalisierung der Justiz beschäftigt, denn der Zugang zum Recht steht auf dem Spiel. Zwar wird der fehlende Zugang zum Recht auch in Europa häufig als Grund für die Entwicklung von neuen Rechtsdienstleistungen herangezogen, aber hier liegen die Probleme an anderer Stelle. Die europäischen Verbraucher:innen setzen mehrheitlich ihre Rechte nur nicht durch, weil aus ihrer Perspektive der Aufwand und die Kosten der Rechtsverfolgung außer Verhältnis zum Wert des Anspruchs stehen (rationales Desinteresse). Dies

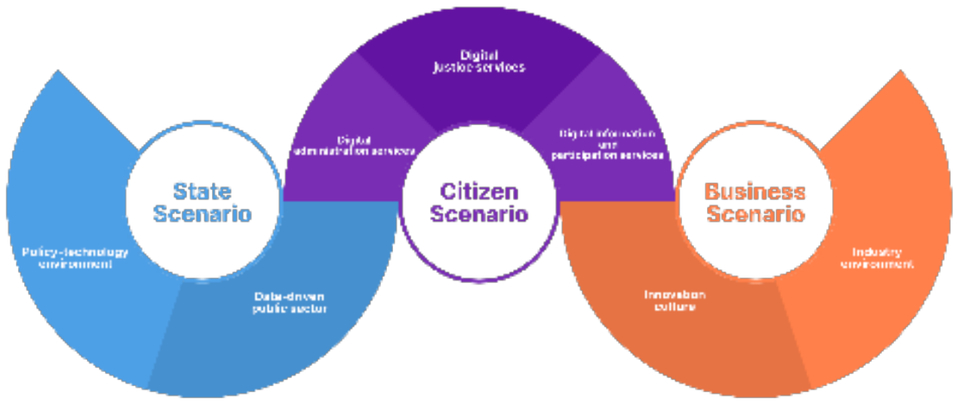
1 Impacto TIC - Luz verde a la justicia digital en Colombia, se buscan talentos globales en Tecnología y mas- hier abrufbar (Stand: 17.06.2022).

ist wenig vergleichbar mit der Situation in Lateinamerika. Dort ist zwar das rationale Desinteresse auch ein Grund für die fehlende Rechtsdurchsetzung, allerdings spielen Themen wie die Überlastung der Justiz und Korruption eine deutlich bedeutendere Rolle. Dieser Beitrag soll sich mit einigen Gedanken um den Stand des Zugangs zum Recht im gesamten lateinamerikanischen Markt beschäftigen. Gleichzeitig wird ein besonderer Fokus auf das Land Kolumbien gelegt. Es werden sieben, voneinander selbstständige Gedanken geschildert, die den Status Quo skizzieren und einen Ausblick wagen.

#1 Status Quo - Potenzial in einem jungen, fragmentierten und wenig entwickelten Markt

Wie steht es aktuell um die digitale Rechtsdurchsetzung in Lateinamerika und insbesondere in Kolumbien? Damit hat sich das Projekt „*Legal Tech Index*“ - geleitet durch die Anwältin Eluisa Helbig-Marchena - beschäftigt. Das Ziel der Studie war es, standardisierte, vergleichbare Indikatoren zu erstellen, die dabei helfen, den Grad der





Die Studie ist hier abrufbar (Stand: 17.06.2022).

Bereitschaft lateinamerikanischer Länder für disruptive Veränderungen durch Legal Tech aufzuzeigen. Dazu wurden auf unterschiedliche Szenarien eingegangen, die auf drei verschiedenen Perspektiven auf Rechtsstaatlichkeit basieren: die Regierung (State Scenario), die Öffentlichkeit (Citizen Scenario) und der Unternehmenssektor (Business Scenario - sowohl B2B als auch B2C).

Der Index stellt somit sowohl den Status quo als auch das Potenzial von Legal Tech im Zusammenhang mit der Rechtsstaatlichkeit in Lateinamerika dar. Je höher der prozentuale Wert, desto besser entwickelt ist das jeweilige Land in dem jeweiligen Bereich.

Das Ergebnis der Studie: Die Strukturen in allen Ländern sind sehr jung und noch wenig geformt, das Potenzial ist entsprechend groß. Legal Tech in Lateinamerika hat gegenüber dem Legal-Tech-Markt in Europa einen wichtigen Vorteil: die Einheitlichkeit der Sprache. Von 640 Millionen Menschen, die in Lateinamerika

leben, spricht der Großteil Spanisch als Muttersprache. Das vereinfacht die Implementierung von Systemen um ein Vielfaches. Der Markt an verschiedenen Angeboten im Bereich B2B (für Kanzleien oder Unternehmen) und im Bereich B2C (für Verbraucher:innen) wächst stetig. Es existieren eine ganze Reihe von Angeboten, beispielsweise solche, die das Notariat digitalisieren sollen, aber auch Datenbanken für juristisches Fachpersonal oder Plattformen für Verbraucherrechte.[2][3] Allerdings spiegeln jene Angebote nicht die Ansprüche wider, die Dienstleistungen für eine moderne kundenzentrierte Rechtsdienstleistung fordern. Eine Herausforderung bleibt dabei weiterhin trotz der einheitlichen Sprache: Fragmentierte Länder und Regionen, Korruption und durch bürokratisierte Vorgänge.

#2 Digitale Justiz ist in Lateinamerika ein sehr wichtiges Thema

Der Zugang zur Rechtsdurchsetzung ist weiterhin sehr stark von bürokratischen Vorgängen geprägt. Soweit so gut. Das Problem ist auch in Deutschland bekannt. Ein großes Problem in dem Prozess ist allerdings, dass die staatlichen Institutionen in Deutschland, nachdem ein Fall bei Gericht eintrifft, verhältnismäßig gut und schnell reagieren. Anders in Kolumbien. Dort sind gravierende Probleme klar erkennbar. Die nationale Erhebung über den Rechtsbedarf aus dem Jahr 2021 zeigt, dass 56 % der Bürger:innen im Land nicht in der Lage sind, ihre rechtlichen Fragen mit den zuständigen Behörden zu klären.[4] Ein Grund dafür besteht in der ineffizienten Arbeitsweise der Justiz. Daneben besteht eine enorme Überlastung der Justiz. Die effektive Überlastungsrate der Gerichte liegt bei 50,7 %.[5] Die Überlastung wird auch dadurch erkennbar, dass die Anzahl der Richter:innen weit unter dem OECD-Standard liegt. Derzeit kommen auf 100.000 Einwohner nur 11 Richter:innen, die sich sehr unterschiedlich über das Staatsgebiet von Kolumbien verteilen.[6] Dies führt zu erheblichen Unterschieden bei dem Zugang zu Gerichten zwischen Bevölkerungsgruppen und Gebieten. Zusätzlich dazu tritt das Problem, dass allein ein Zugang zum Gericht nicht ausreicht. Es bedarf einer schnellen (oder schnelleren) Durchsetzung der Ansprüche. Gerade diesen Problemen kann durch technologische Lösungen begegnet werden. Hierzu gibt es derzeit in Kolumbien erste Versuche.

> „Derzeit kommen in Kolumbien auf 100.000 Einwohner nur 11 Richter:innen."

Als wichtigstes Projekt im Bereich digitaler Justiz kann das Projekt ***PretorIA*** gesehen werden.[7] ***PretorIA*** ist ein System der künstlichen Intelligenz, mit dem das Auswahlverfahren für Tutelas beim Verfassungsgericht verbessert werden soll.

Eine Tutela ist ein Rechtsinstrument, wodurch Bürger:innen staatliche Rechtsverletzungen in Bereichen der Grund- und Menschenrechte vor einem ordentlichen Gericht in der ersten Instanz anzeigen können. Dadurch sollen Minderheiten geschützt werden. Alle Tutelas sollen danach, um eine einheitliche Rechtsprechung zu gewährleisten, durch das Verfassungsgericht überprüft werden. Von den 600.000 Urteilen aufgrund von Tutelas pro Jahr werden etwa 1.000 Urteile von einem Gerichtssenat in einem freien Annahmeverfahren ausgewählt. Die Nachfrage nach Tutelas hat dabei in den vergangenen 20 Jahren rasant zugenommen und gefährdet das Rechtsinstrument und die Arbeitsweise der Gerichte.[8] Die Auswahl der Verfahren, mit denen sich der Verfassungsgerichtshof beschäftigt, soll mittels technologischer Unterstützung verbessert werden.

Hier soll ***PetorIA*** helfen. Das System soll die erste Analyse der Urteile vornehmen und durch eine standardisierte Verarbeitung der Daten danach dazu führen, dass Menschen den nachfolgenden Auswahlprozess besser durchführen können. Die wichtigste Funktion ist die Klassifizierung der Urteile nach den Kriterien des Verfassungsgerichtshofs.

2 *LexBase* - hier abrufbar (Stand: 17.06.2022); *Legis Analitica* - hier abrufbar (Stand: 17.06.2022); Data *Juridica* - hier abrufbar (Stand: 17.06.2022).
3 *Juzto* - hier abrufbar (Stand: 17.06.2022).
4 Die Ergebnisse der Erhebung sind hier abrufbar (Stand: 10.06.2022).
5 Das Wahlprogramm von *Sergio Fajardo* ist hier abrufbar (Stand: 10.06.2022).
6 *Jueces*, fiscales y defensores públicos por cada 100.000 habitantes en Colombia - hier abrufbar (Stand: 10.06.2022).
7 Alle Informationen zu *PretorIA* findet man hier (Stand: 10.06.2022).
8 Das kolumbianische Verfassungsgericht stärken - Hier (Stand: 10.06.2022).

Die Technologie, entwickelt durch ein Forschungsteam der juristischen Fakultät in Buenos Aires, Argentinien, gilt als eines der Vorzeigeprojekte im Bereich der digitalen Justiz in Lateinamerika und ist ein anschauliches Beispiel für länderübergreifende Kooperation und die Vorteile der gemeinsamen Sprache.[9] Allerdings äußern sich immer wieder Expert:innen mit Zweifeln an der Adaptierbarkeit der Systeme auf andere Anwendungsfelder. Insofern fehlt es an den großen, erfolgreichen Leuchtturmprojekten im Bereich der digitalen Justiz, die eigentlich dringend gebraucht werden. Denn anders als beispielsweise in Deutschland, wo ein tatsächlicher Zugang zum Recht besteht, die Rechte aber häufig nicht durchgesetzt werden, fehlt in Kolumbien schon der tatsächliche Weg zum Recht. Dadurch steht für Kolumbien das Justizsystem auf dem Spiel.

#3 Die Korruptionsbekämpfung nimmt einen hohen Stellenwert ein

Ein Grund, weswegen der Zugang zu rechtlicher Hilfe auf staatlicher Ebene nicht auf der ersten Stelle steht, kann die Vielfalt an anderen wichtigen Themen sein, die das politische Geschehen, insbesondere in Kolumbien, bestimmen. Gerade im Thema Rechtsstaatlichkeit dominieren die Themen Korruptionsbekämpfung[10] und die Durchsetzung des Friedensvertrags aus dem Jahr 2016 zwischen der Regierung und den FARC-Rebellen[11]. Dieser Gedanke bestätigt sich auch, wenn man sich die Programme der Kandidaten der aktuell laufenden Präsidentenwahl in Kolumbien ansieht. Einzig das Programm der mittlerweile aus dem Präsidentschaftswahlkampf ausgeschiedenen ***Federico Gutierrez*** und ***Sergio Fajardo*** beschäftigten sich auch nur ansatzweise mit digitaler Justiz.

9 Mehr Informationen zu *Prometea* findet man hier und hier (Stand: 10.06.2022).
10 *Spiegel* - Kommt in Kolumbien das erste Mal in 200 Jahren ein Linker an die Macht?, hier abrufbar; Wahlprogramm von *Rodolfo Hernandez*, hier abrufbar (Stand: 10.06.2022).
11 *Deutschlandfunk*, Kolumbien geht polarisiert in die Wahl, abrufbar hier (Stand: 10.06.2022).

#4 Die digitale Justiz in Kolumbien: Viele gut gemeinte Insellösungen ohne Einfluss

Die Betrachtung der Programme hilft dabei, den Status quo der Justiz besser zu verstehen und einen kleinen Blick in die Glaskugel zu ermöglichen.

Sowohl ***Gutierrez***[12] als auch ***Fajardo***[13] forderten eine zentrale Anlaufstelle für die Bürger:innen und für die digitale zentrale Verteilung der Verfahren[14], das Stärken von virtuellen Interaktionen, die Interoperabilität von Justizsystemen zur Bekämpfung von technischen Insellösungen, die Modernisierung der Informationsverwaltung und die Förderung alternativer, digitaler Streitbeilegungsmechanismen. Zuletzt wurde auch die Rolle der ***LegalApp*** im Programm von ***Fajardo*** in den Vordergrund gestellt. Die ***LegalApp*** ist ein Serviceportal für den offenen und kostenlosen Zugang zu Mechanismen zur Lösung von Rechtsfragen in Kolumbien.[15] Was nach einer guten Idee klingt und sogar in der Challenge des World Justice Project als Finalistin weltweit ausgezeichnet wurde[16], wird in der Realität kaum gepflegt und noch weniger genutzt, sodass es sich - derzeit noch - um eine gut gemeinte Insellösung handelt, die weder gut integriert noch in der Bevölkerung bekannt ist. Gute Lösungsansätze werden oft nicht weit genug bekannt, um tatsächlich eine Verbesserung bei den Bürger:innen zu erreichen. Für den weiteren Verlauf der Wahlen bleibt abzuwarten, inwiefern und ob sich die verbleibenden Kandidat:innen zu der Digitalisierung des Rechts äußern werden. Es wäre wünschenswert, dass diese einen Blick in die Wahlprogramme der hier genannten ausgeschiedenen Kandidaten werfen.

#5 Rechtsberatung per WhatsApp? - Ein erkennbarer Trend

Was können wir aus Lateinamerika lernen? Beratung per ***WhatsApp***. Gerade der Rechtsmarkt hinkt aufgrund hoher regulatorischer Anforderungen anderen Märkten und dem Verbraucherverhalten klassischerweise hinterher. In Lateinamerika ist

12 Das Wahlprogramm von *Federico Gutierrez* ist hier abrufbar (Stand: 10.06.2022).
13 Das Wahlprogramm von *Sergio Fajardo* ist hier abrufbar (Stand: 10.06.2022).
14 Eine der Kernziele der Kampagne von *Gutierrez* war, dass neue Gerichtsverfahren bis ins Jahr 2026 100 % digital bearbeitet werden sollten.
15 Informationen zur *LegalApp* findet man hier und hier (Stand: 10.06.2022).
16 Die Ergebnisse der *World Justice Challenge* findet man hier (Stand: 10.06.2022).

WhatsApp DAS Kommunikationsmittel. Seit langem kann man alles über ***WhatsApp*** bestellen und jeden Service über ***WhatsApp*** buchen. Kein Geschäft, weder in der Stadt noch auf dem Land, hat eine Internetseite, sondern man kauft direkt über den ***WhatsApp***-Katalog. Der Trend des Conversational Commerce dominiert sowohl in Asien als auch in Lateinamerika.

Daneben hat kein Medium in Lateinamerika eine so große Durchschlagskraft wie ***WhatsApp***.[17] So ist es auch keine Überraschung, dass die Rechtsberatung über ***WhatsApp*** ein wichtiges Thema ist. Beispiele dafür gibt es noch wenige, aber vereinzelt bieten Kanzleien diesen Service schon an. Eine breitflächige Beratung könnte sich im Hinblick auf das Kundenverhalten in naher Zukunft entwickeln.

Eine solche Entwicklung könnte auch dazu führen, dass der Zugang zu rechtlichen Informationen an Personengruppen gelangt, die davor keinen Zugriff darauf hatten. Das wird auch dadurch unterstrichen, dass immer mehr Banken - wie Nubank - versuchen über ***WhatsApp*** ihre Kund:innen zu erreichen.[18]

#6 Der Aufstieg von Nubank - Wo ist Nulaw? Ideen von den “Unbanked” für die “Unlawed”

In Lateinamerika hat sich in den letzten Jahren ein großer Player in den Finanzsektor geschlichen. Die Rede ist von ***Nubank***. Seit 2021 an der New York Stock Exchange gelistet und bekannt als “das Fintech-Investment” des legendären Investors ***Warren Buffett***.[19]

Wichtiger ist allerdings das Problem, das ***Nubank*** zu lösen versucht. Das Eröffnen eines Bankkontos ist sehr komplex und das Finanzsystem von nur wenigen Banken beherrscht.

> „Welchen Zweck hat das Recht, wenn man nicht von seinen eigenen Rechten weiß oder seine Rechte nicht durchsetzen kann.“

Daneben ist das Kundenerlebnis bei lateinamerikanischen Banken erschreckend schlecht. Der Abschluss des Bankvertrages ist komplex und die Bankgebühren zu hoch, insbesondere für internationale Überweisungen von im Ausland arbeitenden Familienmitgliedern, auf die viele Familien angewiesen sind. Kein Erlebnis, das einem den Weg zur Bank einfach macht.

Dementsprechend möchte ***Nubank*** den Sektor der Finanzdienstleistungen revolutionieren und eine Personengruppe in Lateinamerika ansprechen, die derzeit kein Bankkonto hat. In Brasilien handelt es sich dabei ungefähr um 55 Millionen Menschen, in ganz Südamerika mehr als 200 Millionen. Sie werden die “Unbanked” genannt. Bei diesem Ansatz kann nun eine Parallele zum Rechtsmarkt gezogen werden. So wie ***Nubank*** den “Unbanked” geholfen hat, kann ein ähnlicher Ansatz den “Unlawed” helfen. Denn Nubank hat gelernt in einem hoch regulierten Markt mit wenigen Konkurrenten und einem schlechten Kundenerlebnis, mit geringen Kundenakquisekosten aufgrund von starkem organischen Wachstum durch Word-Of-Mouth-Effekte[20], niedrigen Margen[21] und einen kundenzentrierten Ansatz[22] den Zugang zu Finanzdienstleistungen zu verbessern. Der kundenzentrierte Ansatz wird beispielsweise dadurch erkennbar, dass ***Nubank*** den Kund:innen keine Gebühren auferlegt. Es wurde eine Kostenstruktur geschaffen, die keine andere Bank in Lateinamerika aufweisen konnte.[23]

Ein ähnliches Problem besteht in den nicht durchgesetzten Rechten vieler Lateinamerikaner:innen. So wie der Ansatz von ***Nubank*** erfolgreich dazu geführt hat, den “Unbanked” einen Zugang zu allgemeinen Finanzdienstleistungen zu ermöglichen, ist dies im Rechtsdienstleistungsmarkt denkbar.

17 Wharton FinTech Podcast - Building a Customer-Centric Culture with *David Velez*, Founder and CEO of Nubank, hier abrufbar (Stand: 10.06.2022).
18 Ebd.
19 FINANCEFWD - *Warren Buffett* investiert in Nubank - Was steckt hinter seiner Fintech-Wette?, hier abrufbar (Stand: 10.06.2022).
20 TechCrunch - *Nubank´s* IPO filing gives us a peek into neobank economics, abrufbar hier (Stand: 10.06.2022).
21 FINANCEFWD - *Nubank* gewinnt seine Kunden für 5 Dollar, hier abrufbar (Stand: 10.06.2022).
22 Der kundenzentrierte Ansatz zahlt sich auch aus. Der NPS (*Net Promoter Score*) von *Nubank* liegt bei 90. Dies kann man hier nachhören. (Stand: 10.06.2022).
23 Den Ansatz kann man hier nachhören. (Stand: 10.06.2022).

Welchen Zweck hat das Recht, wenn man nicht von seinen eigenen Rechten weiß oder seine Rechte nicht durchsetzen kann? Warum also kein Nulaw?

#7 Lateinamerika ist nicht nur ein Markt, der unsere Modelle kopiert.

Die abschließende Erkenntnis ist, dass Lateinamerika auch im Bereich Legal Tech ein spannender Entwicklungsmarkt bleibt. Viele Aspekte wirken chaotisch und unausgereift. Allerdings ist in Lateinamerika auch viel unternehmerisches und digital affines Talent vorhanden und es bleibt viel Raum für unternehmerische Kreativität und neue Lösungsansätze. Insbesondere das anwaltliche Berufsrecht und die Regulierung von Rechtsdienstleistung ist in den meisten Ländern Lateinamerikas noch kaum ausgeprägt. Somit stehen die Marktbedingungen günstig und die Innovation hat freie Fahrt. Es leuchtet ein grünes Licht für Legal Tech in Lateinamerika.

Weiterführende Hinweise:

Talking Legal Tech – Folge 18

“Legal Tech in Afrika mit Cord Brügmann”

43

Talking Legal Tech – Folge 43

“Rightmart, Flightright, Geblitzt.de - Der Stand im B2C mit Marco Klock von Rightmart”

Talking Legal Tech – Folge 57

„Digitale Instrumente für eine moderne Ziviljustiz - Was kann die Ziviljustiz von Flightright lernen, Yannek Wloch?”

Talking Legal Tech – Folge 55

„Warum der CONNY-Gründer Daniel Halmer ohne Legal Tech den Rechtsstaat gefährdet sieht”

Legal Tech

SEO – Effektivere Mandantenwerbung

Björn Decker und Theodor Himmel

Open Peer Review

Dieser Beitrag wurde lektoriert von: Philipp Beckmann und Lisa Krebber

In seinem Jura-Studium an der Universität zu Köln waren überzeugende Formulierungen entscheidend. Als examinierter Jurist schreibt Theodor Himmel (links) bei der Online-Marketing-Agentur OMmatic GmbH Texte für die ADVOmatic-Plattform. So verhilft er Anwälten bei der Generierung neuer Mandanten.

Mit mehr als 20 Jahren Erfahrung in Daten- und Wissensmodellierung, als auch Projektmanagement entwickelt Björn Decker (rechts) die ADVOmatic-Plattform, mit der die verschiedensten Online-Marketing-Kanäle zur Generierung von Mandanten abgestimmt und optimiert werden.

SEO – Die Idee, wie Mandanten zu Ihnen kommen. Wer heute einen Anwalt braucht, der sucht zuerst auf ***Google***. Auf Suchmaschinen, wie ***Google, Yahoo, oder Bing*** werden deutschlandweit jeden Monat Anwälte weit mehr als 570.000-mal gesucht.[1] Dem stehen 51.900 Kanzleien in Deutschland gegenüber,[2] eine schier unendliche Auswahl an Anwälten. Um bei dieser Angebotsflut nicht unterzugehen, müssen Sie als Rechtsanwalt im Internet sichtbar sein. Die Möglichkeiten des Online-Marketings sind mannigfaltig. Zum Beispiel können Sie in sozialen Netzwerken wie ***YouTube*** oder ***Instagram*** Beiträge veröffentlichen, um Ihre eigene Kom-

1 Hier können Sie eine Übersicht von mehr als 570.000 Suchanfragen einsehen, die sich auf 760 Keywords aufteilen, die für einen Rechtsanwalt relevant sind. *Google* macht mit circa 90 % den Bärenanteil aus. Dadurch lässt sich auch erklären, warum die Suchoptimierung auf *Google* angepasst wird (Stand: 01.08.2022). Zusätzlich gibt es im deutschen Raum noch Suchmaschinen wie *bing* mit ca. 5 % und *Ecosia* mit ca. 1 % Marktanteil, wie Sie hier nachlesen können. (abgefragter Zeitraum 01.06.2021-31.05.2022; Stand: 01.08.2022).

2 Die Statistik über die Anzahl der Kanzleien finden Sie hier (Stand: 01.08.2022).

petenz sichtbar zu machen. Eine andere häufig genutzte Möglichkeit ist es, kostenpflichtig Anzeigen in Suchmaschinen (*SEA = Search Engine Advertising*) oder auf gängigen Webseiten (sogenannte *Display Werbung*) zu platzieren. Einträge in lokale Branchenbücher – allen vorweg *Google myBusiness* – sind weitere Möglichkeiten im Online-Marketing. In diesem Artikel fokussieren wir uns auf die Suchmaschinenoptimierung (*SEO = Search Engine Optimization*) der eigenen Kanzleiwebseite, da dies der ideale Ausgangspunkt für weitere Online-Marketing-Aktivitäten ist. SEO hilft den eigenen Internetauftritt präsenter zu machen und schließlich mehr Mandanten zu gewinnen.

Das Ziel: Mehr Mandate

Das Hauptziel der Suchmaschinenoptimierung ist es, dass Sie auf Ihrer Webseite durch verstärkte Sichtbarkeit bei Suchmaschinen neue Mandanten gewinnen. Die Kundengewinnung hängt von zwei Faktoren ab: Qualität und Quantität der Werbung. **Der Online-Nutzer soll Ihre Leistung finden und von ihr überzeugt sein**. Das Zusammenspiel von Weite und Tiefe der Werbemaßnahmen ist entscheidend. Ihre Webseite kann tausendmal geklickt werden; aber kein Besucher wurde mangels überzeugender Werbung zum Mandanten. Ebenso kann Ihre inhaltlich stark aufgestellte Webseite keinen überzeugen, wenn sie keine Besucher hat. Das Ziel einer „mandatengenerierenden" Webseite lässt sich also auf zwei Aspekte aufteilen: zum einen die Sichtbarkeit, zum anderen den Inhalt.

„Jemand, der Fragen zum Steuerrecht hat, den interessiert das Angebot eines Familienrechtsanwalts nicht."

Ohne Sichtbarkeit geht's nicht

Unter Sichtbarkeit *(visibility)* versteht man die Rate, wie viele Nutzer eine Seite in einem Zeitraum sehen. Ein wichtiges Kriterium ist hier die möglichst hohe Positionierung der eigenen Seite auf den Suchergebnisseiten (***Search Engine Results Page, SERP***): je besser die Sichtbarkeit, desto mehr Mandanten. Während die Seite auf der ersten Position, also das oberste nicht bezahlte Ergebnis, fast von 40 % der Nutzer besucht wird, so sind es ab Position 6 nur noch unter 2 %.[3] Diese Sichtbarkeit ist hart erarbeitet durch ständige zeitintensive Pflege und Weiterentwicklung der Seite. Wie in jedem Marketing geht es auch im Onlinemarketing darum, die eigenen (begrenzten) Ressourcen sinnvoll einzusetzen. Egal ob Marketingbudget, investierte Arbeitszeit oder der Umfang des Seiteninhalts: All das wird unnötig verschwendet, wenn die Werbemaßnahmen darauf abzielen, seine Rechtsdienstleistungen jedem einzelnen Nutzer zu präsentieren. Kurz gesagt: Jemand, der Fragen zum Steuerrecht hat, den interessiert das Angebot eines Familienrechtsanwalts nicht, sondern das eines Steuerrechtsanwalts, der sich auf sein spezielles Rechtsproblem spezialisiert hat. Das Nebenziel lautet also, seine Webseite punktuell zu platzieren.

Auch andere Online-Marketing-Ansätze profitieren von verständlichen Inhalten: Suchmaschinenwerbung (SEA – Search Engine Advertising) ermöglicht es, auf die (bezahlte) erste Position der Suchergebnisseite zu gelangen. Da dies Kosten – im Anwaltsbereich von 2 bis 3 € pro Seitenaufruf – erzeugt, ist es hier umso wichtiger, den potenziellen Mandanten auf der Webseite durch ansprechendes Design und schlagfertige Texte zu überzeugen.)

3 Statistiken finden Sie hier (Stand: 01.08.2022).

Verständliche Inhalte formulieren

Findet ein Nutzer eine Webseite, ist der Seitenbetreiber, also der Rechtsanwalt, noch nicht am Ziel. Erst wenn der Besucher auch von der angebotenen Rechtsdienstleistung überzeugt ist, hat sich die Suchmaschinenoptimierung gelohnt. Dabei gehen Überzeugungskraft und SEO zusammen, denn die Algorithmen, nach denen die Suchmaschine die Webseite einordnet, orientieren sich auch an inhaltlichen Faktoren. Wichtig ist also, dass der Rechtsanwalt den Rechtssuchenden mit seiner Kompetenz ‚überredet'. Hierzu ist es notwendig, die Reichweite, welche man erreicht hat, auch entsprechend zu bedienen. Im Gegenteil schadet es, wenn potenzielle Mandanten die Webseite aufrufen, aber sie aufgrund uninteressanter Ansprache sofort wieder verlassen. Um unser Beispiel von eben aufzugreifen: Jemand, der auf der Webseite eines Steuerrechtsanwalts landet, wird nicht von einer mageren Auflistung von Mandaten, sondern von einer detaillierten Beschreibung, wie sein Rechtsproblem zu lösen ist, angeregt. Das Nebenziel lautet also, seine Webseite überzeugend zu formulieren. Beide Ziele beeinflussen sich gegenseitig – zugkräftige Suchbegriffe müssen auf der Webseite für den potenziellen Mandanten klar verständlich erklärt werden und so aufbereitet sein, dass die Suchmaschine die Inhalte ebenfalls ‚versteht'.

A. Welche Hürden bestehen und was muss ich beachten?

Auf dem Weg zu mehr Mandaten über das Internet, stehen Ihnen drei Hindernisse im Weg, die es zum Ziel des erfolgreichen Auftritts zu beseitigen gilt.

I. Wollen:

Zunächst verkennen viele Anwälte das Potenzial von Onlinemarketing. Ihre Unwissenheit zahlt sich teuer in nicht gewonnenen beziehungsweise verpassten Mandaten aus. Aus Unwissenheit beschäftigt man sich nicht damit. Dabei darf „Online" im modernen Rechtsdienstleistungsmarkt nicht ignoriert werden.

II. Können:

Des Weiteren besteht ein Hemmnis gegenüber Onlinemarketing. Sei es aus genereller IT-Skepsis der älteren Generation, deren erste Legal-Tech-Erfahrungen der Ausdruck einer E-Mail über einen Schriftsatz war oder sei es das fehlende Wissen, wie man sein eigenes Angebot an Rechtsdienstleistungen im Internet „an den Kunden bringen" kann. Wichtig ist daher, sich zu informieren oder professionelle Unterstützung zu holen.

> „Das Internet ändert sich stetig, wichtig ist es daher, sich nicht auf einer Website im Windows '98-Stil auszuruhen."

III. Optimieren:

Auch wenn ein Anwalt, der eine Webseite betreibt und daraus monatlich zwei Mandate generiert, bereits Onlinemarketing nutzt, schöpft er damit nicht das volle Potenzial aus. Das Internet ändert sich stetig, wichtig ist es daher, sich nicht auf einer Website im Windows '98-Stil auszuruhen.

B. Die Umsetzung – wie sichtbarer werden

Die Suchmaschinen funktionieren nach einem definierten Algorithmus, welcher die Hervorhebung der Suchergebnisse in Form einer organischen Auflistung (sog. ***natural list***) auf eine Suchanfrage hin bestimmt. Der jeweilige Algorithmus ist ein Geschäftsgeheimnis der Suchmaschinen und wird stetig angepasst. Für die bei der Positionierung in der Suchergebnisliste relevanten Faktoren gibt es zumindest Anhaltspunkte. Als goldene Regel gilt: Eine für den Nutzer relevante Seite ist auch für die Suchmaschinen relevant.

I. Die richtigen Keywords finden

Diese Relevanz zu steigern, fängt mit den richtigen Keywords an, die im Text auf Ihrer Webseite häufig auftreten müssen. Es sollten häufig verwendete Keywords oder Phrasen (sogenannte ***long-tail Keywords***) abgedeckt werden. Dabei darf der

Text nicht wahllos so formuliert sein, dass möglichst viele Keywords auftauchen. Dieses Spammen von Keywords (sogenanntes ***Keyword-Stuffing***) wird durch Suchmaschinen erkannt und mit weniger Sichtbarkeit bestraft. Der Hintergrund ist, dass bei dem Spammen von Keywords nicht angenommen wird, dass diese in einem vernünftigen Kontext stehen. Maßgeblich ist nicht nur das Keyword an sich, sondern auch die sinnvolle Verwendung im Text. Ein Nutzer, der eine bestimmte Frage hat, bekommt von der Suchmaschine Seiten mit gewissen Wörtern vorgeschlagen. Landet man dann auf der Seite, wird dazu der spezifische Absatz markiert. Auch enthält die Suche in der Regel verwandte Suchbegriffe und damit sowohl Keywords als auch Fragen, die im Text beantwortet werden sollten.

Um dem Ziel der Kompetenzvermittlung zu entsprechen ist es wichtig, dass Sie beim Verfassen der Texte darauf achten, mit Fachvokabular den Leser zu überzeugen. Fachvokabular sollte im Text auch erklärt werden. Zum einen ist der Leser nicht mit dem ‚Juristendeutsch' vertraut. Zum anderen entspricht das Fachvokabular selten den gesuchten Keywords. Beispielsweise gibt es im Verkehrsrecht unzählig viele Anfragen zum „Führerschein verloren" (9.900 Suchanfragen) wobei das Gesetz nur den „Entzug der Fahrerlaubnis" (720 Suchanfragen) kennt.

Versetzen Sie sich in die Rolle des Mandanten und suchen Sie eine Rechtsdienstleistung, die Ihre Kanzlei bedient. So erhalten Sie einen Eindruck, wie die eigene Webseite positioniert ist. Einen weiteren Einblick in die Keywords und ihre Funktionsweise erhalten Sie bei ***Google,*** etwa auf den ***Google Trends***[4]**.** Mit diesem kostenlosen Online Tool können Sie nach Suchbegriffen Ihrer potenziellen Mandanten suchen – zum Beispiel „Rechtsanwalt Strafrecht München" – und sich die prozentuale Verteilung der Suchen über einen Zeitraum anzeigen lassen.

Einen detaillierten Einblick und eine weitergehende Recherche nach Keywords bieten Ihnen SEO-Tools. Die meisten dieser Tools bieten kostenfreie Probeabos oder Funktionen an, mit denen Sie Ihre eigenen Erfahrungen sammeln können.

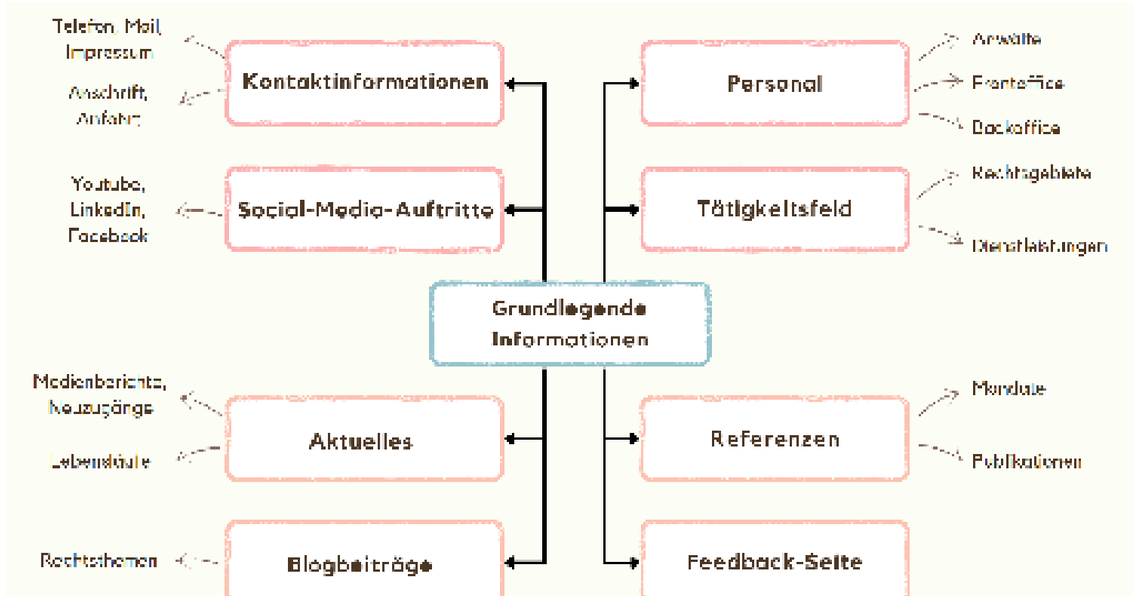
Auf dieser Abbildung sehen Sie die Anzahl der Suchen des Begriffs „Rechtsanwalt Strafrecht München" in einem einjährigen Zeitraum.

Für alle Tools gelten folgende Grundregeln: Aufgrund des stetigen Wandels im Internet ist es unerlässlich, dass der Internetauftritt ständig angepasst wird. Durch kontinuierliche Überprüfung (Monitoring) der Position in den Suchergebnislisten können Maßnahmen eingeleitet werden, die Webseite anzupassen und so aktuell zu halten. Aus diesem Grund sind die Angebote der Marketingdienstleistungen meist auch als Abonnement aufgebaut.

II. Webseite aufbauen

Der Aufbau Ihrer Seite und des Textes soll den Leser bei der Orientierung helfen. Er sollte dazu nutzerorientiert und intuitiv sein. Wichtig ist auch zu beachten, dass Texte im Web in der Regel ‚gescannt', also kursorisch gelesen werden. Eine klare visuelle Strukturierung durch Absätze und Layout hilft dem zukünftigen

4 *Google Trends* können Sie hier ausprobieren (Stand: 01.08.2022).



Die wichtigsten grundlegenden Informationen über eine Kanzlei, die auf der Webseite prägnant vorhanden sein sollten.

Mandanten, sich von der Kompetenz um dem Fähigkeitsprofil des Rechtsanwalts zu überzeugen. Der Text sollte auch funktionieren, wenn er linear von oben nach unten gelesen wird. Die klare Betitelung einzelner Abschnitte einer Webseite hilft bei der Orientierung. Dies wird auch von der Suchmaschine erkannt und durch eine verbesserte Sichtbarkeit belohnt. Es ist daher entscheidend, dass die grundlegenden Informationen der Kanzlei direkt einzusehen sind. Diese grundlegenden Informationen über die Kanzlei finden sich in Abbildung 2. Diese Informationen sollten auf der Webseite jederzeit leicht auffindbar sein. Eine themenbezogene Bebilderung ist ein weiterer Baustein einer ansprechenden Gestaltung. Durch interne Verlinkungen wie Querverweise oder ‚Zurück an den Anfang'-Buttons wird die Orientierung des Nutzers auf einer Seite unterstützt.

III. Technische Überprüfung

Neben den inhaltlichen Aspekten wird auch die technische Umsetzung bei den Suchanbietern durch die Positionierung auf der Suchseite berücksichtigt. Die technische Optimierung beruht auf zwei wesentlichen Faktoren: Darstellung und Geschwindigkeit.

1. Darstellung

Mit Darstellung ist gemeint, wie die Webseite auf verschiedensten Endgeräten angezeigt wird. Dies betrifft den herkömmlichen PC, das Mobiltelefon und die Unterstützungshilfen für Menschen mit Einschränkungen (***Accessibility***). Die Nutzung von Smartphones hat in den letzten Jahren stetig zugenommen. Seit März 2021 gilt bei der ***Google***-Suche ***‚mobile first'.*** Das heißt, nur noch die mobile Webseite ist relevant für die Positionierung in den Suchergebnissen. Es ist daher ratsam, bei der Gestaltung der Webseite die Darstellung auf mobilen Endgeräten als Ausgangspunkt zu nehmen.

2. Geschwindigkeit

Google berücksichtigt auch die Ladegeschwindigkeit[5] der Webseite; jedoch unter erschwerten Bedingungen. Nach Angabe einer URL erhalten Sie eine umfassende Bewertung der Ladegeschwindigkeiten und an welchen Stellen Verbesserungspotenziale umgesetzt werden können.

Pagespeed Insights simuliert eine langsame 3G-Verbindung und ein langsames Endgerät. Die Logik dahinter: eine Webseite, die unter diesen ungünstigen Bedingungen schnell ist, ist es auch mit LTE und dem neuesten ***iPhone.*** Aus diesem Grund hilft es auch nicht die Webseite auf einem schnellen Server zu betreiben, da die tatsächliche Geschwindigkeit nicht berücksichtigt wird.

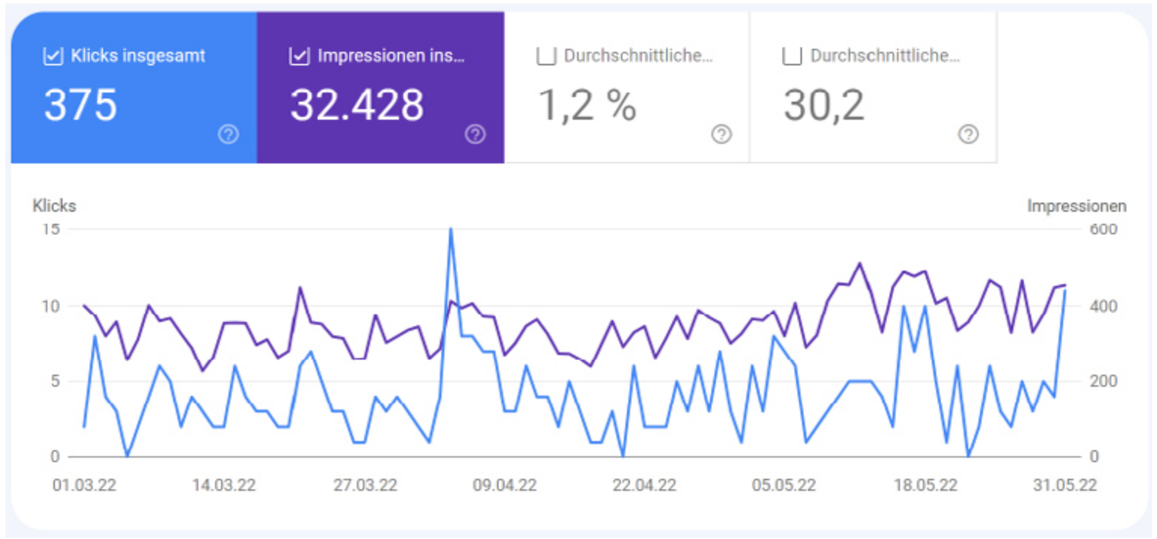
Auch die Indexierbarkeit der Seite durch die Suchmaschine ist wichtig. ***Google*** überprüft beispielsweise, ob die Webseite indexiert werden darf und ob die Struktur

5 Die Ladegeschwindigkeit können Sie selbst über Page Speed Insight testen (Stand: 01.08.2022).

der Webseite klar strukturiert und in Form eines Inhaltsverzeichnisses vorhanden ist. Auch sogenannte Meta-Informationen der Seite wie Öffnungszeiten oder die Kurzbeschreibung werden überprüft.

3. Kontinuierliche Optimierung

Nach dem initialen Aufsetzen der Webseite gilt es, das Erreichte zu verbessern. Insbesondere sollte die aktuelle Position in den Suchergebnislisten überprüft werden. Damit ermitteln Sie den Ausgangspunkt, um den Effekt von Änderungen – zum Beispiel Anpassungen im Text – beobachten zu können. Sie erkennen vornehmlich, wenn die Positionierung bei relevanten Suchen abfällt und können geeignete Gegenmaßnahmen einleiten. Die gängigen Suchmaschinen bieten Betreibern von Webseiten auch Werkzeuge an, um dies zu überprüfen. Für ***Google*** ist dies die sogenannte ***Search Console***. Damit sich nur der Inhaber der Webseite über die Suchergebnisse informieren kann, muss hier zuerst ein Code (sog. ***Property***) auf der Webseite hinterlegt werden. Danach kann der Benutzer sich ein umfassendes Bild darüber verschaffen, wie die Webseite in den Suchergebnissen sichtbar ist. Auch führt die ***Search Console*** kontinuierlich die bereits erwähnten technischen Überprüfungen aus. Dazu gehören zum Beispiel lange Ladezeiten oder welche Inhalte nur unzureichend berücksichtigt werden. So können Gegenmaßnahmen eingeleitet werden, da diese Faktoren ebenfalls bei der Suchposition berücksichtigt werden.



Auszug einer Search-Console-Suche für eine Website.

Schlussbemerkung

Wie Sie gesehen haben, ist SEO und die Gestaltung der eigenen Webseite ein weites Feld. Allerdings bieten die kostenlosen Tools (insb. ***Search Console*** von ***Google***) der Suchmaschinen eine gute Möglichkeit, sich damit ein wenig vertraut zu machen. So können Sie selbst entscheiden, ob Sie den dafür nötigen Aufwand selbst bewältigen wollen. Wenn Sie die Pflege der Webseite und deren SEO-Optimierung auslagern möchten, haben Sie einen guten Eindruck darüber, auf welche Punkte es ankommt. So können Sie mit Dienstleistern auf Augenhöhe kommunizieren. Mit Ihrer SEO-optimierten Webseite erhalten Sie einen soliden Ausgangspunkt für Ihre weiteren Online-Marketing-Aktivitäten wie Suchmaschinenwerbung, Werbung in Verzeichnisdiensten oder sozialen Netzwerken.

Unabhängig von Ihrer Entscheidung: Ihre Mandanten werden Sie im Internet suchen!

Legal Tech und anwaltliches Berufsrecht

Dr. Christian Deckenbrock

Open Peer Review

Dieser Beitrag wurde lektoriert von: Ramon Schmitt und Philipp Beckmann

Dr. Christian Deckenbrock ist Akademischer Oberrat am Institut für Anwaltsrecht der Universität zu Köln (Geschäftsführender Direktor Prof. Dr. Martin Henssler). Er ist Autor zahlreicher Publikationen und Fachbeiträge zum anwaltlichen Berufsrecht und Rechtsdienstleistungsrecht.

Die Liberalisierung des Rechtsdienstleistungsmarkts

Zum 1. Juli 2008 ist das grundlegend neu konzipierte Rechtsdienstleistungsgesetz in Nachfolge des früheren Rechtsberatungsgesetzes in Kraft getreten.[1] Auch wenn einige weitreichende Öffnungen (etwa wenn Rechtsdienstleistungen unentgeltlich erbracht werden) erfolgt sind, hat der Gesetzgeber für den Bereich entgeltlicher Rechtsdienstleistungen grundsätzlich am Anwaltsmonopol festhalten wol-

1 Vom 12.12.2007, BGBl. 2007 Bd. I, S. 2840. Überblick bei *Henssler/Deckenbrock*, DB 2008, 41 ff.; bei diesem Aufsatz handelt es sich um die mit Fußnoten versehene Fassung eines Beitrags, den der Verfasser zuerst auf der Webseite der *Legal University* hat (und dort auch künftig aktuell halten wird), hier abrufbar (Stand: 01.08.2022). Der Verfasser dankt für die Genehmigung des Zweitabdrucks.

len. Nur Anwältinnen und Anwälte sind die berufenen unabhängigen Berater und Vertreter des Rechtsuchenden in allen Rechtsangelegenheiten (§ 3 Absatz 1 Bundesrechtsanwaltsordnung [BRAO]). Damit soll der Schutz der Rechtsuchenden, des Rechtsverkehrs und der Rechtsordnung vor unqualifizierten Rechtsdienstleistungen gewährleistet werden (§ 1 Absatz 1 Satz 2 Rechtsdienstleistungsgesetz [RDG]), nicht aber der Schutz der Anwältinnen und Anwälte vor unliebsamer Konkurrenz.[2] Trotz dieses grundsätzlichen Bekenntnisses zum Anwaltsmonopol ist in jüngerer Vergangenheit auf dem Rechtsdienstleistungsmarkt viel Bewegung entstanden. Neuartige Geschäftsmodelle, die oft unter dem Stichwort „Legal Tech" diskutiert und von Nicht-Anwältinnen und Anwälten angeboten werden, sind entstanden und inzwischen – unter Nutzung verbliebener Spielräume, die das Rechtsdienstleistungsgesetz eröffnet – sogar höchstrichterlich gebilligt worden.

So wird die Erstellung eines Vertragsentwurfs mithilfe eines digitalen Rechtsdokumentengenerators, bei dem anhand von Fragen und vom Nutzer auszuwählender Antworten standardisierte Vertragsklauseln abgerufen werden, nicht einmal als erlaubnispflichtige Rechtsdienstleistung angesehen.[3] Die Rechtsprechung qualifiziert einen solchen Generator als die digitale Variante eines Formularhandbuchs, weil die über den üblichen Fall hinausgehenden individuellen Verhältnisse des Anwenders keine Berücksichtigung fänden. Es fehle daher an einer rechtlichen Prüfung des konkreten Falls und liege deshalb schon keine Rechtsdienstleistung im Sinne des § 2 Absatz 1 RDG – die Norm bestimmt die Schwelle, ab der eine Tätigkeit nicht mehr jedermann eröffnet ist – vor.

B. Legal-Tech-Inkasso als neues Phänomen

Sehr weitgehende Kompetenzen sind inzwischen auch sogenannten Legal-Tech-Unternehmen, die sich als Inkassodienstleister registriert haben, eingeräumt worden. Nach dem Rechtsdienstleistungsgesetz kann für die Einziehung fremder oder zum Zweck der Einziehung auf fremde Rechnung abgetretener Forderungen, wenn die Forderungseinziehung als eigenständiges Geschäft betrieben wird, eine spezielle Erlaubnis erteilt werden (§ 2 Absatz 2 Satz 1, § 10 Absatz 1 Satz 1 Nummer 1 RDG). Genauso wie in den Bereichen „Rentenberatung" und „Rechtsdienstleistungen in einem ausländischen Recht", für die ebenfalls eine Registrierung möglich ist, ist der Gesetzgeber davon ausgegangen, dass die anwaltliche Versorgung die bestehende Nachfrage der Rechtsuchenden nicht vollständig befriedigen kann. Er hat Inkassounternehmen sogar als unverzichtbar für unser Wirtschaftsleben bezeichnet.[4]

Dabei hat er ursprünglich aber an solche Dienstleister gedacht, die für gewerbliche Unternehmen Forderungseinziehung betreiben (etwa für ein Mobilfunkunternehmen offene Forderungen von Kunden einziehen). Neben diesen „klassischen" Inkassodienstleistern finden sich heute auch zahlreiche Angebote am Markt, bei denen registrierte Unternehmen Forderungen von Verbraucherinnen und Verbrauchern nach einem standardisierten Prozess geltend machen und einzuziehen versuchen (sog. ***Verbraucherinkasso***).

Die Portale, die etwa mit dem Einzug von Fluggastrechteentschädigungen oder der Geltendmachung von Rückzahlungsansprüchen im Zusammenhang mit der sogenannten Mietpreisbremse (notfalls auch auf gerichtlichem Wege) werben, bieten ihre Leistungen gegen Zahlung einer nicht unerheblichen Erfolgsprovision an, versprechen aber zugleich, dass im Misserfolgsfall dem Kunden keinerlei Kosten entstehen. Nach Auffassung des ***BGH*** ist der Begriff „Inkassodienstleistung" weit zu begreifen. Auch wenn hierunter ursprünglich vor allem der Forderungseinzug im herkömmlichen, stärker von Mahn- und Beitreibungsmaßnahmen geprägten Sinne verstanden worden sei, sei er „***unter Berücksichtigung der vom Gesetzgeber mit dem Rechtsdienstleistungsgesetz […] verfolgten Zielsetzung einer grundlegenden, an den Gesichtspunkten der Deregulierung und Liberalisierung ausgerichteten, die Entwicklung neuer Berufsbilder erlaubenden Neugestaltung des Rechts der außergerichtlichen Rechtsdienstleistungen nicht in einem zu engen Sinne zu verstehen***".[5]

2 BT-Drucks. 16/3655, S. 45; *Deckenbrock*, in: Deckenbrock/Henssler, RDG, 5. Aufl. 2021, § 1 Rn. 2 ff.
3 BGH, Urteil vom 9.9.2021 – I ZR 113/20, NJW 2021, 3125; vgl. zum Problemkreis *Deckenbrock*, AnwBl Online 2020, 178 ff.
4 Entwurf eines Gesetzes zur Neuregelung des Rechtsberatungsrechts, BT-Drucks. 16/3655, 40 f.
5 BGHZ 224, 89 = NJW 2020, 208.

Einem Inkassodienstleister sei es daher gestattet, zugunsten von Verbraucherinnen und Verbrauchern ein umfassendes Servicepaket anzubieten, das die rechtliche Forderungsprüfung, eine substanzielle Beratung der Kunden über den Forderungsbestand und auch die Durchführung von Maßnahmen, die zur Begründung der Forderung notwendig sind (so muss etwa eine Mieterin oder ein Mieter, die beziehungsweise der einen Teil der Miete wegen Verstoßes gegen die Bestimmungen der Mietpreisbremse zurückfordern möchte, dies zunächst gegenüber der Vermieterin beziehungsweise dem Vermieter rügen) beinhaltet.

C. Sammelklage-Inkasso als weiteres neuartiges Geschäftsmodell

Diese Rechtsprechung hat der ***BGH*** inzwischen fortentwickelt und geklärt, dass der Inkassobegriff auch Geschäftsmodelle, die ausschließlich oder vorrangig auf eine gerichtliche Einziehung der Forderung abzielen, einschließt.[6] Dies gilt auch im Fall des sog. „***Sammelklage-Inkasso***“. Damit ist es registrierten Inkassodienstleistern erlaubt, Forderungen verschiedener Parteien gegen ein Unternehmen einzusammeln und gebündelt geltend zu machen. Am Markt bekannt sind etwa Geschäftsmodelle,

- die Forderungen von Autokäufern im Zusammenhang mit dem Dieselskandal gegen die ***Volkswagen AG***,
- Ansprüche von Anlegern auf Schadensersatz gegen ein Wirtschaftsprüfungsunternehmen anlässlich der ***Wirecard***-Insolvenz oder
- Kartellschadensersatzansprüche von Kunden gegen LKW-Hersteller, die unter Verstoß gegen die europäischen Wettbewerbsregeln Preisabsprachen getroffen haben,

zum Gegenstand haben.

6 BGHZ 230, 255 = NJW 2021, 3046; vgl. nun auch BGH, Urt. v. 13.6.2022 – VIa ZR 418/21 (zum EInzug ausländischer Forderungen).

Die gebündelte Durchsetzung von Forderungen verschiedener Parteien begründe keinen relevanten Interessenkonflikt. Vielmehr seien die Interessen der klagenden Inkassodienstleister und der Kunden, die dem Inkassounternehmen ihre Forderung zur Einziehung überlassen, untereinander gleichgerichtet. Ziel sei jeweils, eine möglichst hohe Befriedigung aller Forderungen zu erhalten. Zwar sei nicht auszuschließen, dass der einzelne Kunde durch einen Vergleichsschluss möglicherweise das Risiko übernehme, dass der auf ihn entfallende Anteil der Vergleichssumme gering ausfällt, weil der Inkassodienstleister die Forderung des Kunden mit Forderungen mit niedrigerer Durchsetzungsaussicht (***heterogen***) gebündelt geltend gemacht hat. Diesem Risiko stünden jedoch erhebliche Vorteile einer gebündelten Geltendmachung im Vergleich zu einer jeweils individuellen Anspruchsdurchsetzung gegenüber. Insoweit zählt der ***BGH*** beispielhaft die Nutzbarmachung der Gebührendegression bzw. -deckelung, die Streuung des Kostenrisikos einer etwaig vorausgegangenen Beweisaufnahme und die erhebliche Stärkung der Verhandlungsposition gerade im Hinblick auf einen Vergleichsschluss auf. Zudem könne das Inkassounternehmen Unterschieden hinsichtlich der Durchsetzungsaussichten durch eine entsprechende (möglichst ***homogene***) Gruppierung der Ansprüche weitgehend Rechnung tragen.[7]

D. Legal-Tech-Angebote als Beitrag zum Zugang zum Recht

Die neuartigen Geschäftsmodelle nicht-anwaltlicher Legal-Tech-Dienstleister sind ein wichtiger Beitrag zum Zugang zum Recht. Denn sie nehmen Forderungen in den Blick, die ansonsten von den Verbraucherinnen und Verbrauchern mit Blick auf das Prozesskostenrisiko (im Unterliegensfall sind Gerichtskosten und die Kosten von bis zu zwei Anwältinnen und Anwälten zu bezahlen) oft – gerade, wenn es an einer Rechtsschutzversicherung fehlt – nicht realisiert würden.

7 Auch noch nach der BGH-Entscheidung vom 13.7.2021 zum Sammelklage-Inkasso (BGHZ 230, 255 = NJW 2021, 3046) halten manche Instanzgerichte – nicht überzeugend – bestimmte Geschäftsmodelle von Legal-Tech-Inkasso für unzulässig, vgl. etwa OLG Schleswig, BeckRS 2022, 385 Rn. 34 ff.; LG Stuttgart, BeckRS 2022, 1731 Rn. 17 ff.; LG Stuttgart, BeckRS 2022, 362 Rn. 76 ff. m. krit. Besprechung *Heinze*, NZKart 2022, 193 ff.; LG Stuttgart, BeckRS 2022, 10278 m. ablehnender Anm. *Deckenbrock*, EWiR 2022, 349 ff., sowie (zum Einzug ausländischer Forderungen) OLG Braunschweig, BeckRS 2021, 29486 Rn. 12 ff. m. ablehnender Anm. *Deckenbrock*, EWiR 2021, 703 f. (nunmehr aufgehoben durch BGH, Urt. v. 13.6.2022 – VIa ZR 418/21).

„Die neuartigen Geschäftsmodelle nicht-anwaltlicher Legal-Tech-Dienstleister sind ein wichtiger Beitrag zum Zugang zum Recht.“

Durch solch niedrigschwellige Angebote wird sichergestellt, dass berechtigte Ansprüche auch tatsächlich und erfolgversprechend geltend gemacht werden. Das aufseiten der Rechtsuchenden bestehende rationale Desinteresse wird auf diese Weise überwunden. Aber auch für Unternehmer wird die Hemmschwelle, die das Kostenrisiko begründet, beseitigt, sodass es insgesamt zu einer konsequenteren Durchsetzung von Ansprüchen kommt. Der Preis, den die Rechtsuchenden dafür zu tragen haben, ist freilich der, dass ihnen nicht die vollständige Forderungssumme ausgekehrt wird, sondern sie einen Abzug der mit dem Inkassounternehmen vereinbarten Erfolgsprovision hinnehmen müssen. Das ist ein entscheidender Unterschied zur klassischen anwaltlichen Forderungsdurchsetzung, die allerdings – wenn eine Rechtsschutzversicherung nicht besteht – den Preis der Übernahme des Prozesskostenrisikos hat.

E. Das Dilemma: Die Ungleichbehandlung von Anwälten und Inkassodienstleistern

Auf der anderen Seite steht der Erfolg dieser Legal-Tech-Inkasso-Angebote auch im Zusammenhang mit den seit jeher strengen Regeln des anwaltlichen Berufsrechts. Denn die berufsrechtliche Regulierung der registrierten Inkassodienstleister ist im Vergleich zur Rechtsanwaltschaft weniger streng ausgestaltet. So war es etwa Rechtsanwältinnen und Rechtsanwälten lange Zeit berufsrechtlich - von engen Ausnahmen abgesehen - weder gestattet, mit ihren Mandantinnen und Mandanten ein Erfolgshonorar zu vereinbaren (§ 49b Absatz 2 Satz 1 BRAO alte Fassung [a.F.]) noch den Mandantinnen und Mandanten im Fall einer Erfolglosigkeit der Inkassotätigkeit eine Freihaltung von den entstandenen Kosten zuzusagen (§ 9b A bsatz 2 Satz 2 BRAO a.F.). Der Grund für diese strengen Vorgaben des anwaltlichen Berufsrechts war die Befürchtung, dass bei Vereinbarung eines Erfolgshonorars eine spezifische Gefährdung der anwaltlichen Unabhängigkeit drohe. Weil durch ein Erfolgshonorar und die Übernahme der Prozessfinanzierung eine weitgehende Parallelität der wirtschaftlichen Interessen von Rechtsanwalt und Mandant herbeigeführt werde, könnte deshalb die zur Wahrung der Unabhängigkeit gebotene kritische Distanz des Rechtsanwalts zum Anliegen des Auftraggebers Schaden nehmen. Es sei zu befürchten, dass mit der Vereinbarung einer erfolgsbasierten Vergütung für unredliche Berufsträger ein zusätzlicher Anreiz geschaffen würde, den Erfolg ‚um jeden Preis‘ auch durch Einsatz unlauterer Mittel anzustreben. Zudem seien der Schutz der Rechtsuchenden vor einer Übervorteilung durch überhöhte Vergütungssätze und die Sicherung der prozessualen Waffengleichheit mit Blick darauf, dass der Gegner womöglich nicht in der Lage ist, sein Kostenrisiko auf vergleichbare Art zu verlagern, legitime Ziele des Gesetzgebers.

Inkassounternehmen sind dagegen seit jeher weder an ein Erfolgshonorar noch an ein Prozessfinanzierungsverbot gebunden. Sie können gegenüber ihren Kunden ihr Dienstleistungspaket ‚kostenfrei‘ anbieten, weil die geschuldete Provision nur im Erfolgsfall anfällt.[8] Dies gilt mangels berufsrechtlicher Bindung auch in Fällen, in denen das Inkassounternehmen selbst Anwältinnen und Anwälte beauftragen muss, um die streitigen Forderungen auch vor Gericht durchzusetzen (Inkassounternehmen sind in streitigen gerichtlichen Verfahren selbst nicht postulationsfähig). Es fehlte daher an einem ‚level-playing-field‘, weil das strenge anwaltliche Berufsrecht Anwältinnen und Anwälten das Angebot von Geschäftsmodellen untersagte, die von Inkassodienstleistern massenhaft erfolgreich am Markt platziert werden konnten.

8 BGH, NJW-RR 2022, 376 Rn. 49 ff.

Dieser Wertungswiderspruch bedingte aber nicht die Unzulässigkeit der Tätigkeit der Inkassodienstleister, sondern beruhte – wie der ***BGH*** mehrfach betont hat – auf einer bewussten Entscheidung des Gesetzgebers im Rahmen der Reform des 2008 in Kraft getretenen Rechtsberatungsrechts. Sie wurde auch mit Blick darauf, dass Inkassounternehmen im Gegensatz zu Rechtsanwältinnen und Rechtsanwälten keine unabhängigen Organe der Rechtspflege sind, getroffen.[9] Nur die Rechtsanwältin und der Rechtsanwalt haben ihre Mandantinnen und Mandanten als unabhängige Berater und Vertreter in allen Rechtsangelegenheiten vor Rechtsverlusten zu schützen, rechtsgestaltend, konfliktvermeidend und streitschlichtend zu begleiten, vor Fehlentscheidungen durch Gerichte und Behörden zu bewahren und gegen verfassungswidrige Beeinträchtigung und staatliche Machtüberschreitung zu sichern. Diese der Anwaltschaft besonders zugewiesenen Rolle und ihrer Einbindung in das Rechtspflegesystem im Sinne einer im Gemeinwohl liegenden Funktion der Anwaltschaft bedingt, dass Rechtsanwältinnen und Rechtsanwälte einem besonderen Berufsrecht unterliegen. Ihre Einstufung als unabhängige Organe der Rechtspflege grenzt sie deutlich von sonstigen Dienstleistungsberufen ab. Diese rechtsstaatsspezifische Tätigkeit ist zugleich Grundlage der Anwaltsprivilegien wie dem Zeugnisverweigerungsrecht und dem Beschlagnahmeverbot, aber auch der besonderen Pflichtenstellung in Form weitere spezifischer Berufspflichten. Hierdurch wird das Vertrauensverhältnis zwischen Anwalt und Mandant gegen Störungen abgesichert.[10]

F. Der Versuch einer gesetzlichen Regelung

Man muss dem Gesetzgeber aber zugutehalten, dass die vielfältigen Formen sog. Verbraucherinkassos 2008 beim Inkrafttreten des Rechtsdienstleistungsgesetzes noch keine Rolle spielten, die damit verbundenen Probleme also gar nicht zu erkennen waren. Auch deshalb fühlte sich der Gesetzgeber 2021 dazu veranlasst, einen kohärenten Regelungsrahmen für Inkassodienstleistungen zu schaffen.

Mit dem Gesetz zur Förderung verbrauchergerechter Angebote im Rechtsdienstleistungsmarkt vom 10. August 2021[11] hat der Gesetzgeber mit Wirkung zum 1. Oktober 2021 sich den unterschiedlichen rechtlichen Rahmenbedingungen für Inkassounternehmen auf der einen und Anwältinnen und Anwälten auf der anderen Seite angenommen.

Zum einen hat der Gesetzgeber Inkassodienstleister strikter reguliert und ihnen unter anderem neue umfangreiche Darlegungs- und Informationspflichten bei Inkassodienstleistungen für Verbraucherinnen und Verbraucher auferlegt (§ 13b RDG). Falls ein Erfolgshonorar vereinbart werden soll, müssen Verbraucherinnen und Verbraucher künftig etwa einen Hinweis darauf erhalten, welche anderen Möglichkeiten zur Durchsetzung der Forderung bestehen – insbesondere, wenn diese es der Verbraucherin oder dem Verbraucher im Erfolgsfall ermöglichen, die Forderung in voller Höhe zu realisieren. Geschuldet ist auch ein Hinweis auf die mit dem Prozessfinanzierer im Hinblick auf die Prozessführung getroffenen Vereinbarungen. Außerdem sind, falls der Inkassodienstleister berechtigt sein soll, mit dem Schuldner einen Vergleich zu schließen, die Folgen eines solchen Vergleichs näher zu erläutern.

Der Gesetzgeber hat sich aber nicht mit einer stärkeren Regulierung der Inkassodienstleister begnügt, sondern zugleich das bislang recht strikte Verbot anwaltlicher Erfolgshonorare liberalisiert. Nunmehr ist Anwältinnen und Anwälten die Vereinbarung eines Erfolgshonorars möglich, wenn eine Inkassodienstleistung außergerichtlich oder in gerichtlichen Mahnverfahren bis zur Abgabe an das Streitgericht erbracht wird (§ 4a Absatz 1 Satz 1 Nummer 2 Rechtsanwaltsvergütungsgesetz [RVG]). Soweit solche Inkassodienstleistungen betroffen sind, können Rechtsanwältinnen und Rechtsanwälte auch Vereinbarungen treffen, durch die sie sich verpflichten, Gerichtskosten, Verwaltungskosten oder Kosten anderer Beteiligter zu tragen (§ 49b Absatz 2 Satz 2 BRAO). Auf diese Weise soll zugunsten der Anwalt-

9 Vgl. BT-Drs. 16/3655, 67; BGHZ 224, 89 Rn. 173 = NJW 2020, 208; BGH, NJW-RR 2022, 376 Rn. 47.
10 BVerfGE 110, 226, 252 = NJW 2004, 1305, 1307; BVerfG, NJW 2015, 2949 Rn. 38.
11 BGBl. 2021 Bd. I, 3415; s. dazu die Einführung von *Kilian*, MDR 2021, 1297 ff.

schaft ein kohärenter Gleichlauf der den registrierten Inkassodienstleistern eröffneten Möglichkeiten erreicht werden.[12] Zudem ist es Anwältinnen und Anwälten unabhängig von einem Forderungseinzug möglich, ein Erfolgshonorar zu vereinbaren, wenn sich der Auftrag auf eine Geldforderung von höchstens 2.000 € bezieht. Erfolgshonorare sind bei solchen ‚Kleinstforderungen' damit auch gestattet, wenn die Anwältin oder der Anwalt mit der Abwehr eines solchen Anspruchs beauftragt ist (§ 4a Absatz 1 Satz 1 Nummer 1 RVG). Auch ist eine derartige Vereinbarung mit Bezug zum gerichtlichen Verfahren möglich. Die Prozessfinanzierung bleibt der Anwaltschaft in dem Anwendungsbereich dieser Ausnahme dagegen entgegen den ursprünglichen Plänen der Bundesregierung[13] verwehrt.[14]

Auch wenn durch diese Reform zweifelsohne der Rechtsrahmen, den Anwältinnen und Anwälten auf der einen und Inkassounternehmen auf der anderen Seite bei der Erbringung von Inkassodienstleistungen beachten müssen, angeglichen worden ist, bedeutet dies nicht, dass die rechtlichen Regeln nun dieselben sind. Eine Ungleichbehandlung besteht zunächst im Bereich des gerichtlichen Forderungseinzugs weiter. Während Inkassodienstleister ihren Kunden die Freihaltung von sämtlichen Kosten auch im Fall eines Rechtsstreits vor Gericht versprechen können (sie müssen freilich eine Anwältin oder einen Anwalt für die Vertretung vor Gericht beauftragen, da sie dort außerhalb des vorgeschalteten gerichtlichen Mahnverfahrens nicht selbst tätig werden dürfen), dürfen Anwältinnen und Anwälte ein solch umfassendes Paket nicht anbieten (wenn sie selbst das Klageverfahren durchführen wollen). Ihnen ist ein Erfolgshonorar im gerichtlichen Bereich nur für Forderungen bis zu einem Gegenstandswert von 2.000 Euro erlaubt, die Übernahme der Gerichtskosten oder der gegnerischen Anwaltsvergütung ist ihnen sogar vollständig untersagt.

> „Die Prozessfinanzierung bleibt der Anwaltschaft entgegen den ursprünglichen Plänen verwehrt"

Außerdem bleiben Anwältinnen und Anwälte an das strenge Fremdkapitalverbot gebunden: Gesellschafterinnen und Gesellschafter einer anwaltlichen Berufsausübungsgesellschaft können nur aktiv tätige Berufsträgerinnen und Berufsträger sein, die zudem in der Gesellschaft einen freien Beruf ausüben müssen. Berufsfremde Investoren sind dagegen unerwünscht, reine Kapitalbeteiligungen zum Schutz der anwaltlichen Unabhängigkeit unzulässig. Zudem kennen Inkassodienstleister auch ansonsten nicht ein so strenges Berufspflichtenprogramm wie Rechtsanwältinnen und Rechtsanwälte. So unterliegen nur Anwältinnen und Anwälte einer berufsrechtlichen und zudem strafbewehrten Verschwiegenheitspflicht.

G. Nach der Reform ist vor der Reform?

Möglicherweise wird sich der Bundestag bereits in der neuen, gerade begonnenen Legislaturperiode erneut diesem Thema widmen. Denn gemeinsam mit der Verabschiedung des Gesetzes zur Förderung verbrauchergerechter Angebote im Rechtsdienstleistungsmarkt wurde auch ein Entschließungsantrag gebilligt, mit dem die Bundesregierung aufgefordert wird, weiter offene Fragen zu klären. Insbesondere wird die Bundesregierung aufgefordert, bis zum 30. Juni 2022 einen Gesetzentwurf vorzulegen, der die Aufsicht über registrierte Inkassodienstleister auf eine zentrale Stelle auf Bundesebene übertragen soll.[15] Diesem Beschluss Rechnung tragend hat das ***Bundesministerium der Justiz*** Anfang Mai 2022 nun einen Referentenentwurf eines Gesetzes zur Stärkung der Aufsicht bei Rechtsdienstleistungen und zur Änderung weiterer Vorschriften des Rechts der rechtsberatenden Berufe vorgestellt.[16]

12 Entwurf eines Gesetzes zur Förderung verbrauchergerechter Angebote im Rechtsdienstleistungsmarkt, BT-Drs. 19/27673, 1 f.
13 BT-Drs. 19/27673, 7, 30 f.
14 Vgl. auch BT-Drs. 19/30495, 15 (Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz zu BT-Drs. 19/27673).
15 Vgl. BT-Drucks. 19/30495, 8.
16 Hier abrufbar (Stand: 01.08.2022).

Dem Petitum des Bundestags folgend soll die Aufsicht über Inkassodienstleister künftig beim ***Bundesamt für Justiz*** zusammengeführt werden – bislang sind hierfür die Landesjustizverwaltungen zuständig, die ihrerseits nachgeordnete Gerichte und Behörden mit der Aufsicht betraut haben. Mithilfe der geplanten Zentralisierung beim ***Bundesamt für Justiz*** soll eine einheitliche, qualitativ verbesserte Aufsicht gewährleistet werden.[17]

Weitere Änderungen bleiben denkbar, wird doch auch im Koalitionsvertrag das Thema Legal Tech angesprochen. Dort heißt es: „***Wir erweitern den Rechtsrahmen für Legal Tech-Unternehmen, legen für sie klare Qualitäts- und Transparenzanforderungen fest und stärken die Rechtsanwaltschaft, indem wir das Verbot von Erfolgshonoraren modifizieren und das Fremdbesitzverbot prüfen.***“[18] Kritiker, hierzu zählt vor allem die ***Bundesrechtsanwaltskammer***, halten dagegen eine weitere Liberalisierung des anwaltlichen Berufsrechts mit dem Ziel einer weiteren Angleichung an die geringen Vorgaben, die für Inkassounternehmen greifen, für nicht angezeigt. Vielmehr müsse das hohe Schutzniveau, das das anwaltliche Berufsrecht zur Sicherung der anwaltlichen Unabhängigkeit und im Interesse der Rechtsuchenden vermittle, aufrechterhalten bleiben. Richtigerweise seien vielmehr die Kompetenzen von Inkassounternehmen zu beschneiden.[19]

Das letzte Wort ist daher noch nicht gesprochen. Sicher bleibt Raum für weitere vorsichtige Öffnungen des anwaltlichen Berufsrechts, möglicherweise auch für eingeschränkte Ausnahmen vom Fremdfinanzierungsverbot. Wer aber für eine völlige Deregulierung des anwaltlichen Berufsrechts plädiert, übersieht, dass die Pflichten, die Anwältinnen und Anwälte treffen, in erster Linie nicht Bürde, sondern ein Vorzug sind, die sie wohltuend als „unabhängiges Organ der Rechtspflege“ von den anderen Anbietern auf dem Rechtsdienstleistungsmarkt abgrenzen.[20]

Legal Tech University:

Dieser Beitrag ist parallel auf der digitalen juristischen Lernplattform Legal Tech University veröffentlicht worden. Die interdisziplinäre Legal Tech University (https://www.legaltech.university/) stammt aus der Feder der studentischen Initiative eLegal e.V. und stellt ein europaweit einzigartiges Format zur Vermittlung von Grundlagenwissen über die digitalen Veränderungen innerhalb der Rechtsbranche dar. Die Inhalte der kostenlosen Plattform umfassen etwa die Themen Dokumentenautomatisierung, Künstliche Intelligenz, Vertragsanalyse, Blockchain, Gerichte und Verwaltung, Online Dispute Resolution, Anwaltliches Berufsrecht und viele mehr.Methodisch wurde auf einführende Texte, Original-Praxisbeispiele für den Einsatz von Legal-Tech-Lösungen, Videos und Demo-Tools zurückgegriffen, sowie mit rund 30 führenden Expert/innen aus Kanzleien, Rechtsabteilungen, Start-ups, Gerichten und Universitäten zusammengearbeitet. Das Projekt ist am 01. Februar 2022 nach anderthalb Jahren Arbeit gelauncht worden.

eLegal e.V. ist eine im April 2019 gegründete studentische Initiative, die sich aus Student/innen, Referendar/innen, wissenschaftlichen Mitarbeiter/innen und Anwält/innen mit über 150 Mitgliedern aus ganz Deutschland zusammensetzt. Die Initiative hat sich zum Ziel gesetzt, angehenden Jurist/innen die Möglichkeit zu geben, sich mit der Zukunft der Rechtsbranche zu beschäftigen.

17 S. dazu *Deckenbrock*, NJW-aktuell 22/2022, 3.
18 Koalitionsvertrag 2021 – 2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90 / Die Grünen und den Freien Demokraten (FDP), Mehr Fortschritt wagen: Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, 89, hier abrufbar (Zugriff: 17.06.2022).
19 BRAK-Stellungnahme 2/2022.
20 *Jaeger*, NJW 2004, 1, 6; vgl. auch § 1 BRAO.

Impressum

Chefredaktion

Philipp Beckmann, Louis Goral-Wood, Ramon Schmitt, Ferdinand Wegener

E-Mail: ctrl@legaltechcologne.de

Redaktion

Lektoratsleitung: Isabel Ecker, Daniel Dischinger, Hendrik Eppelmann, Philipp Mahlow, Hendrik Scheja

Layout & Design: Julia Melles, Helena Sommer, Larissa Pilch

Illustration: Greta Maria Gross, designer_pals @ fiverr.

Marketing: Larissa Pilch, Hendrik Scheja, Joela Worm

Social Media: Muskaan Multani, Alina Rosenkranz, Michelle Duda

IT: Alexander Adlmüller, Simon Damschen, Daniel Dischinger

Schreib uns einen Leserbrief!

Die CTRL ist eine studentische Zeitschrift. Als Studierende schreiben wir teilweise zum ersten Mal über komplexe Fragestellungen zu Recht und Digitalisierung. Wir sind daher auf Dein Feedback und Deine kritischen Anmerkungen angewiesen. Darüber hinaus würden wir uns über den inhaltlichen Austausch mit Euch, liebe Leserinnen und Leser, freuen.

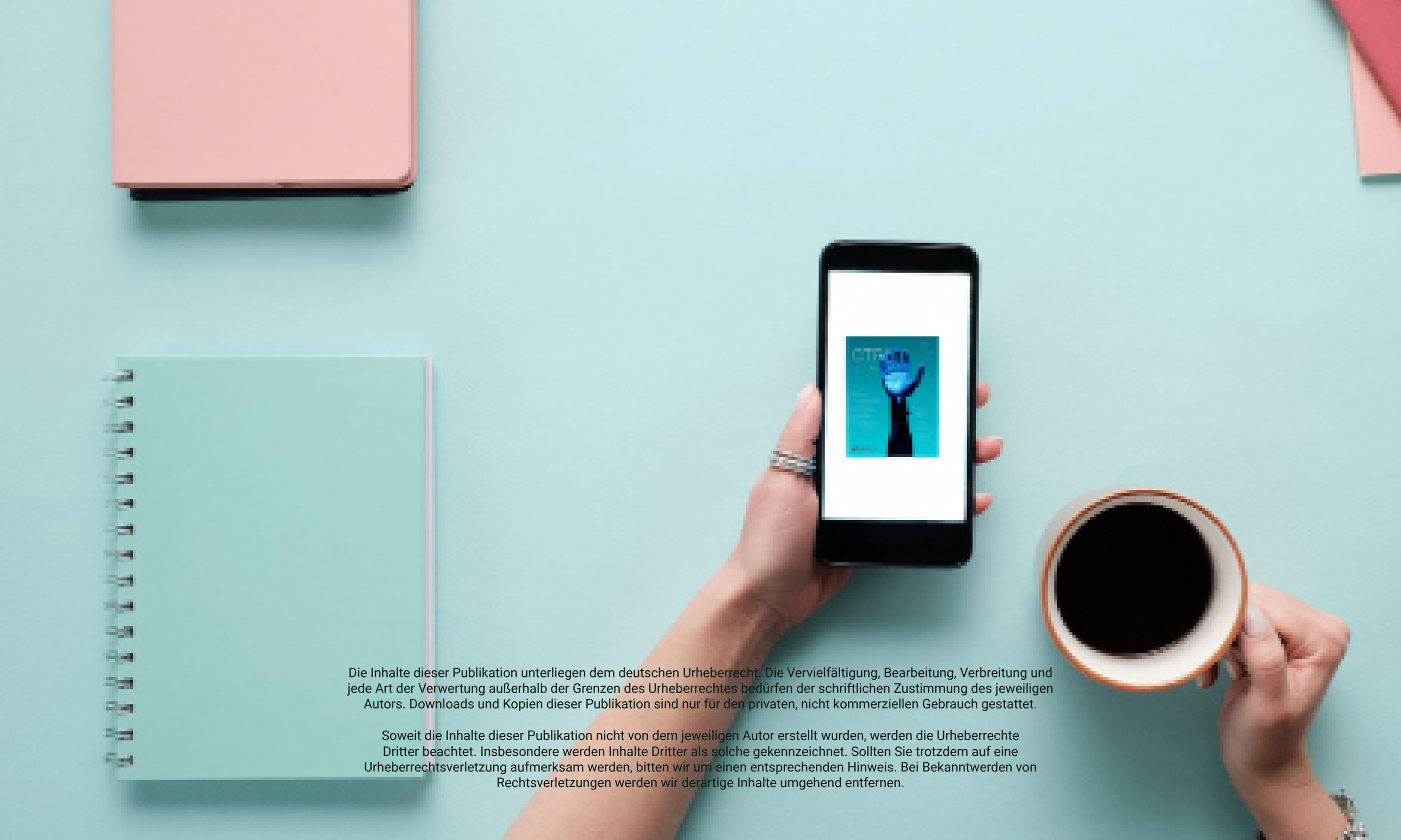
Schreib uns. Wir freuen uns!

Deinen Leserbrief kannst Du

per E-Mail an ctrl@legaltechcologne.de schicken

oder

Du nutzt das hierfür vorgesehene Typeform auf unserer Website.



LEGAL TECH LAB
COLOGNE