CTRL

1/23

3. Jahrgang,1. Ausgabe
www.legaltechcologne.de/ctrl

Cologne Technology
Review & Law

Grundwissen
Wie Digitalisierung das Risiko von Blackouts verringert

Streitgespräch
DSGVO: Ignorieren statt kooperieren?

Deepfakes als Gefahr für die Demokratie – eine rechtliche Einordnung

LEGAL TECH LAB COLOGNE

Cologne Technology
Review & Law

Liebe Leserinnen und Leser,

Im Zuge des technologischen Fortschritts verschwimmen die Grenzen zwischen Realität und Fiktion immer mehr. Mit dem Aufkommen von Deepfakes, virtueller Realität und KI-Sprachmodellen wie *ChatGPT* wird es immer schwieriger, Fakten von Fiktion zu unterscheiden. Diese Tools ermöglichen es uns, Inhalte auf eine Weise zu erstellen und zu erleben, die früher unvorstellbar war, aber sie stellen auch neue Herausforderungen an unsere Fähigkeit, zu erkennen, was real ist und was nicht.

Hast Du etwa gemerkt, dass der erste Absatz von *ChatGPT* geschrieben und von *DeepL* übersetzt wurde? Nein? Deshalb haben wir uns entschlossen, die damit einhergehenden rechtlichen Herausforderungen in den Mittelpunkt unserer neuen Ausgabe zu stellen. In ihrem Aufsatz „Wenn Videomanipulationen zu einer Gefahr für die Demokratie werden: Eine rechtliche Bewertung von Deepfakes“ analysieren Anna Dungel und Eva Beute die strafrechtliche Verantwortlichkeit derer, die Deepfakes verbreiten, um politisches Aufsehen zu erregen. Der Philosoph *David Chalmers, NYU*, greift in seinem neusten Buch *Reality+* diese Entwicklung auf und denkt sie weiter: „Within a century we will have virtual realities that are indistinguishable from the non-virtual world. In centuries to come we may face the decision: ‘Should we move our lives to a virtual world?’ The reasonable answer may often be yes”. *Hannah Wissler* setzt sich in ihrem Grundwissensbeitrag mit der Frage auseinander, welche Rechte Kinder in solchen digitalen Welten haben (sollten).

Die Grenzen zwischen Realität und Fiktion will auch zunehmend das Unternehmen Meta verschwimmen lassen: Allerdings versucht die *Europäische Union* mit der Verabschiedung des Digital Services Act (DSA) solche Plattformbetreiber stärker in die Pflicht zu nehmen. In ihrem Aufsatz „Der DSA auf dem Prüfstand - zwischen Grundrechten und Regulierung“ zeigen *Alexander Niebler* und *Sofian Djebbar* jedoch auf, dass der Umsetzung dieses Gesetzes noch zahlreiche offene Fragen entgegenstehen. Der DSA wäre dabei nicht der erste EU-Rechtsakt, dessen Umsetzbarkeit fraglich ist. Die Datenschutzexperten und Rechtsanwälte *Lutz Martin Keppeler* und *Alan Dahi* diskutieren in einem Streitgespräch die Praktikabilität und Umsetzbarkeit der DSGVO. Nachdem *Christian Kuß* in der CTRL 1/2022 das Konzept der Einwilligung im Datenschutz kritisiert hat, hält *Inka Knappertsbusch* in ihrer Kolumne „Die Einwilligungserklärung - Der Stein der Weisen!“ dagegen und verweist insbesondere auf die Rechtsunsicherheiten alternativer Ansätze.

Zuletzt noch einige Ankündigungen in eigener Sache: Wir freuen uns sehr, dass die CTRL ab dieser Ausgabe einen wissenschaftlichen Beirat hat, der die Weiterentwicklung der Zeitschrift begleiten und die wissenschaftliche Ausrichtung der CTRL stärken wird. Die Mitglieder sind: *Frau Prof. Dr. Dr. Frauke Rostalski* (Strafrecht, Universität zu Köln), *Herr Prof. Dr. Erich Hölter* (Wirtschaftswissenschaften, Technische Hochschule Köln), *Herr Prof. Dr. Florian Möslein* (Handels- und Wirtschaftsrecht, Universität Marburg), *Herr Prof. Dr. André Niedostadek* (Sozialrecht, Hochschule Harz), *Herr Prof. Dr. Markus Ogorek* (Öffentliches Recht, Universität Köln), *Herr Prof. Dr. Sebastian Omlor* (Bürgerliches Recht, Universität Marburg), sowie *Frau Prof. Dr. Louisa Specht-Riemenschneider* (Informations- und Datenschutzrecht, Bürgerliches Recht, Universität Bonn).

Zudem tritt *Julia Melles* der Chefredaktion als fünftes Mitglied hinzu und wird den Bereich Design und Layout führen.

Wir wünschen Euch allen einen angenehmen Frühling und viel Spaß beim Lesen dieser fünften Ausgabe der CTRL.

Ferdinand Wegener
Chefredaktion

Ramon Schmitt
Chefredaktion

Philipp Beckmann
Chefredaktion

Louis Goral-Wood
Chefredaktion

Julia Melles
Chefredaktion

Inhaltsverzeichnis

Grundwissen

9 Die Stromversorgung revolutionieren: Wie Digitalisierung das Risiko von Blackouts verringert

16 Digitale Kinderrechte: Eine Idee steckt in den Kinderschuhen

25 Legal Tech - Darf man das?

Aufsätze

40 Deepfakes als Gefahr für die Demokratie — eine rechtliche Einordnung

55 Der DSA auf dem Prüfstand Zwischen Grundrechten und Regulierung

Kolumne

77 Das Orakel-Problem oder: Warum Blockchains keine guten Notare sind

83 Wie begeistert man für Legal Tech? Start-up-Förderung mit dem Legal Tech Colab

90 Die Einwilligungserklärung Der Stein der Weisen!

Digitalisierung done right

32 Digitalisierung des Handelsregisters: Was kostet kostenlos?

Interview

66 DSGVO: Ignorieren statt kooperieren?

Legal Tech

93 Data Science meets BGB: Eine Einführung in die juristische Datenvisualisierung

110 Der Legal Hackathon 2022 Cologne: Zwischen innovativem Zukunftsgeist, Massagen und Networking

Klick mich!

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.

Grundwissen

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

Unser ausgabenspezifisches Inhaltsverzeichnis

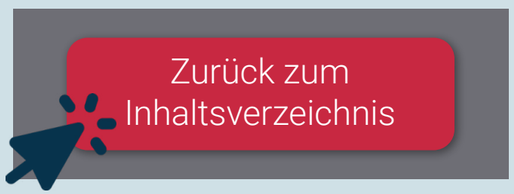
Unser ausgabenspezifisches Inhaltsverzeichnis schickt euch mit einem Klick direkt zu dem Beitrag, der euch ins Auge gesprungen ist.

Talking Legal Tech – Folge 1

Was ist Legal Tech? – mit Nico Kuhlmann

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.



Rückverlinkungen zum dynamischen Inhaltsverzeichnis

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

Über die

Cologne Technology Review & Law

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

LEGAL TECH LAB COLOGNE

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 Solutions

Gateway Exzellenz Start-up Center Universität zu Köln

Die Köpfe
hinter der Zeitschrift

Clarissa Kupfermann
Redaktion

Philipp Mahlow
Redaktion

Hendrik Eppelmann
Redaktion/Lektorat

Alina Rosenkranz
Social Media

Larissa Pilch
Social Media

Helena Sommer
Layout & Design

Michelle Duda
Layout

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.

Grundwissen

Die Stromversorgung revolutionieren:
Wie Digitalisierung das Risiko von Blackouts verringert

Jonas Neubert

Open Peer Review

Dieser Beitrag wurde lektoriert von:
Alexander Niebler & Sofian Djebbari

Jonas studiert Rechtswissenschaften an der Universität zu Jena. Darüber hinaus absolviert er das Zertifikatsstudium Energierecht am Institut für Energiewirtschaftsrecht in enger Zusammenarbeit mit der Stiftung Umweltenergierecht. Er arbeitet aufgrund seiner Interessen an den Themen Energie und Digitalisierung im Energiewirtschaftsbereich von Rödl & Partner.

In den letzten Jahren und insbesondere in den vergangenen Monaten haben sich Berichte über unkontrollierte und flächendeckende Stromausfälle (*Blackouts*) gehäuft. Der Grund hierfür ist die verschärfte europäische Energiekrise.

Diese wurde durch den russischen Angriffskrieg gegen die Ukraine und die Ausfälle von europäischen Energieerzeugern intensiviert. Die im Kern zugrunde liegende

Ursache für die langfristig zunehmende Belastung der Stromnetze liegt in der zunehmenden Komplexität der Energienetze und der europäischen Integration der nationalen Energiesysteme. Die Transformation von fossilen zu erneuerbaren Energiequellen und die fortschreitende Elektrisierung aller Lebensbereiche sind gewaltige Verschiebungen in der Energiewirtschaft. Um diese Herausforderungen erfolgreich zu meistern, spielt die Digitalisierung innerhalb der Energiewirtschaft eine entscheidende Rolle. Sie kann dazu beitragen, das Energiesystem zukunftsfähiger und nachhaltiger zu gestalten und die Energieversorgungssicherheit zu erhöhen.

„A world without electric power“ by DALL-E

A. Grundbegriff: Blackout

Eine zuverlässige Stromversorgung ist das Fundament einer modernen Industriegesellschaft. Das Risiko bei langanhaltenden, unkontrollierten und flächendeckenden Ausfällen des Stromnetzes ist, dass in kürzester Zeit andere essenzielle Infrastrukturen wie Transportsysteme, Wasserversorgung und -entsorgung, das Gesundheitswesen, sowie Informations- und Kommunikationssysteme empfindlich gestört oder sogar vollständig zum Erliegen kommen.Blackouts entstehen, wenn die dynamische Balance zwischen der nachgefragten und der vorhandenen Energiemenge gestört wird.

Die Netzfrequenz, die in unseren Breitengraden bei 50 Hertz liegen sollte und nur minimal schwanken darf, gibt diesen Zustand wieder. Die Netzfrequenz kann aufgrund von technischen Störungen oder Naturkatastrophen unterbrochen werden, wodurch eine Unter- oder Überversorgung von Energie entstehen kann, abhängig davon, ob zu viel oder zu wenig Strom in die Netze eingespeist wird. Nach § 11 Absatz 2 Satz 1 EnWG sind die Netzbetreiber verpflichtet, eine zuverlässige Energieversorgung für jedermann bereitzustellen.

„Brownouts“ werden eingesetzt, um Blackouts aufgrund von Unterversorgung zu verhindern. Im Gegensatz zu einem Blackout ist ein Brownout ein kontrollierter Stromausfall, orchestriert von den Netzbetreibern selbst, der immer dann notwendig wird, wenn die produzierte Menge an Strom nicht ausreicht, um die Nachfrage zu decken. Dies wird z.B. aufgrund von Engpässen in der Energieerzeugung, wie Brennstoffmangel oder nicht verfügbaren Energieerzeugungsanlagen, erforderlich. Um die Stromversorgung stabil und zuverlässig aufrechterhalten zu können, muss die Nachfrage in solchen Fällen durch gezielten Lastenabwurf (Abschaltung von energieintensiven Verbrauchern) gemäß § 13 Absatz 2 EnWG reduziert werden, damit das Angebot wieder vollständig die Nachfrage decken kann. Mit anderen Worten: Die Stromnachfrage wird von den Stromversorgern gezielt verringert, indem einzelne Verbraucher nicht mehr mit Strom beliefert werden, um einen das ganze System betreffenden Blackout zu verhindern.

Das Ziel muss sein, dass das Stromnetz stabil und zuverlässig funktioniert, um das Stressszenario eines Blackouts, das verheerende humanitäre und wirtschaftliche Schäden verursachen kann, zu vermeiden. In jüngster Zeit haben sich aktuelle Entwicklungen als erhöhte Gefahr für Blackouts erwiesen, wie die zunehmende Schwankung der Netzfrequenzen. Diese Schwankungen können auf die Integration erneuerbarer Energien in den Strommix zurückgeführt werden, die aufgrund ihrer Natur schwankende Energiequellen sind. Um diese Schwankungen auszugleichen,

Auswirkungen eines Blackouts

sind vermehrt technische Eingriffe erforderlich, wie der sogenannte „Redispatch" nach § 13 Absatz 1 Nr. 2 EnWG, bei dem Energie von einem Bereich des Netzes in einen anderen umgeleitet wird.

Darüber hinaus zeigen Forderungen seitens der EU, der Bundesregierung, von Energieversorgern und von Netzbetreibern, Strom einzusparen, um die Belastung des Stromnetzes zu verringern, wie angespannt die Energiesicherheit derzeit ist. Die Netzstabilität wird immer komplexer, je mehr sich Europa in Richtung 100 % erneuerbarer Energien bewegt. Nach Artikel 2 EU-Klimaverordnung muss dieser Zustand bis zum Jahr 2050 erreicht sein. Die steigende Nutzung von erneuerbaren Energien könnte vorrangig durch den Einsatz von Digitalisierung und technischen Innovationen erreicht werden.

Art. 2 Abs. 1 der EU-Klimaverordnung: „Die unionsweiten im Unionsrecht geregelten Treibhausgasemissionen und deren Abbau müssen in der Union bis spätestens 2050 ausgeglichen sein, sodass die Emissionen bis zu diesem Zeitpunkt auf nett null reduziert sind, und die Union strebt danach negative Emissionen an."

B. Digitalisierung der Energiewirtschaft

I. Die Auswirkungen der Digitalisierung auf das Energiesystem

Die Digitalisierung hat einen tiefgreifenden Einfluss auf fast alle Bereiche der Wirtschaft und Gesellschaft, einschließlich der Energieversorgung. Die Umstrukturierung des Energiesystems hin zu dezentralen Erzeugungsanlagen und erneuerbaren Energien sowie die zunehmende Nutzung von Strom für Elektrofahrzeuge und Wärmebedarf stellen eine große Herausforderung dar. Das Zusammenspiel von verschiedenen Elementen innerhalb eines vernetzten Energiesystems trägt wesentlich zu einer erfolgreichen Transformation bei. Der Betrieb, die Steuerung von Erzeugungsanlagen, sowie das Stromnetz und die Integrationsrate erneuerbarer Energien in das System müssen optimiert werden, um die Anpassung an eine variable Stromnachfrage zu ermöglichen. Durch die Vernetzung und Automatisierung von Anwendungen und Prozessen, sowie das Verbinden von Objekten der physikalischen Welt mit dem Internet werden länderübergreifende Netzwerkdaten und künstliche Intelligenz (KI) für Entscheidungen eingesetzt. Die Digitalisierung bietet somit die Möglichkeit, das Energiesystem zukunftsfähiger und nachhaltiger zu gestalten.

In der Energieversorgung gibt es eine zunehmende Verbindung durch Informations- und Kommunikationstechnologien (IKT). Der Ausbau der Smart-Meter-Infrastruktur gemäß §§ 42 ff. MsbG (Messstellenbetriebsgesetz) stellt ein großes Potenzial für die Digitalisierung der Energieversorgung dar, indem sie als sichere Infrastruktur für die Steuerung von dezentralen Anlagen (etwa Solaranlagen einzelner Verbraucher) dient. Digitalisierung und IKT umfassen viel mehr als nur Hardware und Kommunikationsnetze, sondern auch Software. Die zunehmende Verfügbarkeit von großen Datenmengen und die stetige Verbesserung der Echtzeitverarbeitung führen zu einer erhöhten Notwendigkeit der Automatisierung von Verteilnetzen. Dies ist erforderlich, um die Integrierbarkeit der wachsenden Menge an variabler Erzeugung aus erneuerbaren Energieanlagen sicherzustellen.

II. IT/OT-Konvergenz und ihr Einfluss auf die Energiewirtschaft

Die Konvergenz von IT (*Information Technology*) und OT (*Operational Technology*) schafft Mehrwerte, indem sie die Interaktion zwischen den Bereichen erhöht, die früher strikt voneinander getrennt waren. Beispielsweise können Daten aus der OT genutzt werden, um Entscheidungen über die erforderliche Wartung von Maschinen und Anlagen zu treffen. Auf der anderen Seite haben OT-Systeme auch Schnittstellen zu anderen Systemen, um bei Schalthandlungen die Auswirkungen auf die Lebensdauer von Betriebsmitteln, wie zum Beispiel von elektrischen Bauteilen, in Betracht zu ziehen und somit die ökonomische Effizienz zu steigern. Die IT/OT-Konvergenz bietet das Potenzial, die Zusammenarbeit zwischen administrativen und produktionsbezogenen Prozessen zu verbessern und die Effizienz von Netzbetreibern zu erhöhen.

Eine weitere Fähigkeit von der IT/OT-Konvergenz ist das Sammeln und Analysieren von Daten über Maschinen und Anlagen in Echtzeit. Dies kann dazu beitragen, die Zuverlässigkeit und Verfügbarkeit von Anlagen zu erhöhen und somit Ausfallzeiten zu minimieren. Die Planbarkeit von Bedarfen entlastet die Stromnetze erheblich.

Durch die Digitalisierung entstehen neue Akteure der Energiewirtschaft, welche digitale Produkte oder Plattformen für die Energieversorgung anbieten, wie beispielsweise Smart-Home-Anwendungen oder Marktplattformen für den Energiehandel. Perspektivisch werden gemäß § 14a EnWG viele Konsumgeräte – von Beleuchtungen bis hin zu Kühlschränken – mit dem Internet verbunden sein. Dies wird auch als das *„Internet der Dinge"* (IoT) bezeichnet. Branchenfremde Anbieter vertreiben

„A city in a blackout" by DALL-E

Smart-Home-Lösungen, die Geräte automatisiert steuern können. Um die Auswirkungen der Digitalisierung zu verstehen, reicht es nicht aus, nur technische und betriebliche Prozesse zu betrachten. Es ist auch erforderlich, die veränderte gesellschaftliche und ökonomische Dynamik zu berücksichtigen.

C. Digitalisierung der Energiewirtschaft als Maßnahme zur Prävention von Blackouts

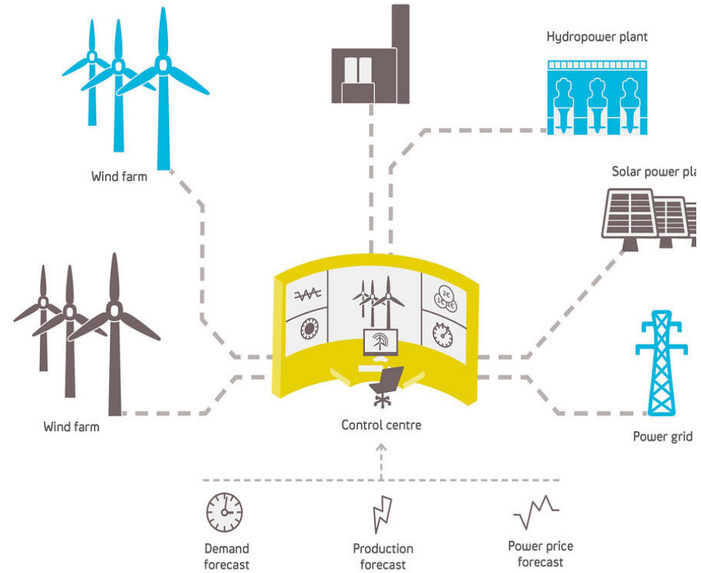
Die Digitalisierung der Energiewirtschaft bietet eine Vielzahl von Möglichkeiten, um Blackouts zu verhindern. Durch die Anwendung von intelligenten Messsystemen und Bereitstellung von Regelenergie nach § 22 Absatz 2 EnWG können Schwankungen im Stromverbrauch besser ausgeglichen werden, um die Stabilität des Systems zu verbessern. Die strategische Integration erneuerbarer Energien und der Einsatz von Batteriespeichern sind ein zusätzlicher Baustein, um die Stromversorgung flexibler und anpassungsfähiger zu gestalten. Die Digitalisierung ermöglicht es, den Zustand von Stromversorgungsanlagen zu überwachen und aufkommende Probleme frühzeitig zu erkennen und zu beheben.

Eine weitere Präventionsmaßnahme, die durch die Digitalisierung eröffnet wird, ist die Etablierung von *„Smart Grids"*. Diese ermöglichen es, den Stromverbrauch in Echtzeit zu überwachen und die Stromproduktion und -verteilung entsprechend nach § 14a EnWG anzupassen, um den Bedarf an Strom effektiver abzustimmen. Smart Grids können auch dazu beitragen, Stromausfälle durch Wetterbedingungen oder andere Ereignisse zu minimieren, indem sie die Integration erneuerbarer Energien steigern und somit die dynamische Balance stabilisieren.

Die Förderung der Zusammenarbeit zwischen verschiedenen Akteuren im Energiesektor ist ein entscheidender Faktor bei der Prävention von Blackouts durch vernetzte und dezentralisierte Energieerzeugung. Die Netzbetreiber, Stromproduzenten und -verbraucher werden mittels digitaler Informationskanäle enger zusammenarbeiten und miteinander kommunizieren, um die Stromversorgung zu stabilisieren. So können etwa Verbraucher, die über eine Fotovoltaikanlage verfügen, ihren selbst erzeugten Strom ins Netz nach § 11 Absatz 1 EEG einspeisen und damit zur Stabilisierung beitragen. Durch die Zusammenarbeit und Kommunikation aller Akteure können Blackouts effektiver verhindert werden.

Die Netzresilienz ist die Fähigkeit eines Netzwerks, Störungen zu überwinden und eine zügige Wiederherstellung der Soll-Leistung zu erreichen, um die Verfügbarkeit und Zuverlässigkeit von Netzwerken und Diensten zu gewährleisten. Die Digitalisierung befähigt Netzbetreiber, die Netzresilienz zu optimieren, indem sie die Überwachung und Steuerung des Netzes intensivieren und kollektiv auf Störungen reagieren. Die Integration von redundanten Systemen und die Nutzung von *„Microgrids"* sind zusätzliche Puzzleteile, um die Stromversorgung zuverlässiger zu gestalten. Praktisch wird die Netzresilienz auch mittels monetärer Anreize wie nach § 6 EEG gestärkt.

Die Anwendung von *„Predictive Maintenance"* ist eine technische Innovation, Blackouts zu verhindern. Predictive Maintenance ist das Monitoring von Stromversorgungsanlagen mit der Analyse von möglichen Problemen, bevor diese zu Störungen im Netz führen. Durch die Verwendung von hochsensiblen Sensoren und Machine-Learning-Technologien, können Netzbetreiber mögliche Ausfälle frühzeitig erkennen und entsprechende Maßnahmen, wie z.B. Brownouts ergreifen, um Blackouts zu verhindern.



Zusammensetzung von Virtual Power Plants

Ein immer beliebteres Tool sind *„Virtual Power Plants"* (VPPs). Dieses Konstrukt fasst dezentrale Energieerzeugungseinheiten, wie Fotovoltaikanlagen oder Batteriespeicher, zu einem virtuellen Kraftwerk zusammen. Das daraus resultierende,

optimierte Kraftwerk dient als Ersatz für konventionelle Kraftwerke. Die Nutzung von VPPs wird die Stromversorgung für Netzbetreiber flexibler, anpassungsfähiger und dezentraler gestalten. Im Ergebnis ermöglicht dies daher eine weitere Steigerung der Stabilität des Netzbetriebes.

D. Risiken der Digitalisierung in der Energiewirtschaft

Der Einsatz digitaler Technologien in der Energiewirtschaft birgt aus der Natur der Sache eine Reihe von Risiken, die es zu berücksichtigen gilt.

Eines dieser Risiken ist die Abhängigkeit von digitalen Systemen. Wenn das Energiesystem auf gewisse Technologien angewiesen ist, kann ein Ausfall dieser Systeme die Energieversorgung unterbrechen. Auch Sicherheitsbedenken spielen eine Rolle, insbesondere im Hinblick auf die Cyber-Sicherheit. Angriffe auf digitale Systeme können dazu führen, dass die Energieversorgung gestört wird oder Daten gestohlen werden.

„Wenn das Energiesystem auf gewisse Technologien angewiesen ist, kann ein Ausfall dieser Systeme die Energieversorgung unterbrechen."

Hinzu kommt das Risiko von fehlerhafter Software oder von deren unsachgemäßer Nutzung. In einem digitalisierten Energiesystem, das sich auf die Energiewende und die Verteilung von Energie konzentriert, wird der Wiederaufbau der Versorgung zudem komplexer.

„A city shrouded in darkness" by DALL-E

Es ist daher wichtig, Maßnahmen zur Absicherung digitaler Systeme in der Energiewirtschaft zu treffen, um die Sicherheit der Energieversorgung zu gewährleisten. Dazu gehören beispielsweise regelmäßige Sicherheitsüberprüfungen, die Einführung von Sicherheitsstandards, Kraftwerk- und Notfallreserven und die Schulung von Mitarbeitern in Sachen Cyber-Sicherheit.

Insgesamt überwiegen jedoch die Vorteile der Digitalisierung der Energiewirtschaft, um Blackouts zu verhindern und die Stromversorgung zu verbessern, etwa durch die Anwendung von Smart Grids, intelligenten Messsystemen und der Regelenergie. Die Befähigung der technischen Integration erneuerbarer Energien und der Einsatz von Batteriespeichern verbessert zunehmend die Netzresilienz.

Im Ergebnis scheint eine klimaneutrale und energiesichere Zukunft ohne Blackouts dank der Fortschritte in der Digitalisierung bis Mitte des Jahrhunderts realisierbar.

Weiterführende Literatur

- Ergebnisse des zweiten Stresstests zum Stromsystem
  BMWK – Veröffentlichung der Langfassung der Ergebnisse des zweiten Stresstests zum Stromsystem
  Bundesamt für Bevölkerungsschutz informiert Stromausfall (bund.de)
  Innovationsbericht 2022 Amperion – Digitalisierung für klimaneutrales Energiesystem

- Amprion-Innovationsbericht.pdf
  Jahresmagazin 2020 von 50 Hertz
  Digitalisierung – 50Hertz – Jahresbericht 2020 (jahresmagazin-50hertz.com)

Zurück zum Inhaltsverzeichnis

Grundwissen

Digitale Kinderrechte:
Eine Idee steckt in den Kinderschuhen

Hannah Wißler

Open Peer Review

Dieser Beitrag wurde lektoriert von: Hendrik Scheja

Hannah hat Jura an der Freien Universität Berlin studiert und arbeitet als wissenschaftliche Mitarbeiterin bei Hausfeld Rechtsanwälte LLP. Sie war während ihres Studiums als studentische Hilfskraft im Bereich Datenschutz tätig und hat sich mit künstlicher Intelligenz und Algorithmen in der Strafverfolgung auseinandergesetzt.

Die neue Generation Alpha (ca. 2010 - 2025) wächst vollständig im digitalen Zeitalter auf. Fast jeder Aspekt des Lebens von Kindern hat nun eine Online-Dimension. Dadurch gibt es keine klare Trennung zwischen ‚Offline' und ‚Online' mehr. Bereits vor der Geburt können Kinder digitale Spuren hinterlassen, zum Beispiel, wenn Eltern das Ultraschallbild oder den Namen des Kindes auf sozialen Medien wie *Instagram*, *Facebook* oder *TikTok* veröffentlichen (sog. *Sharenting*).

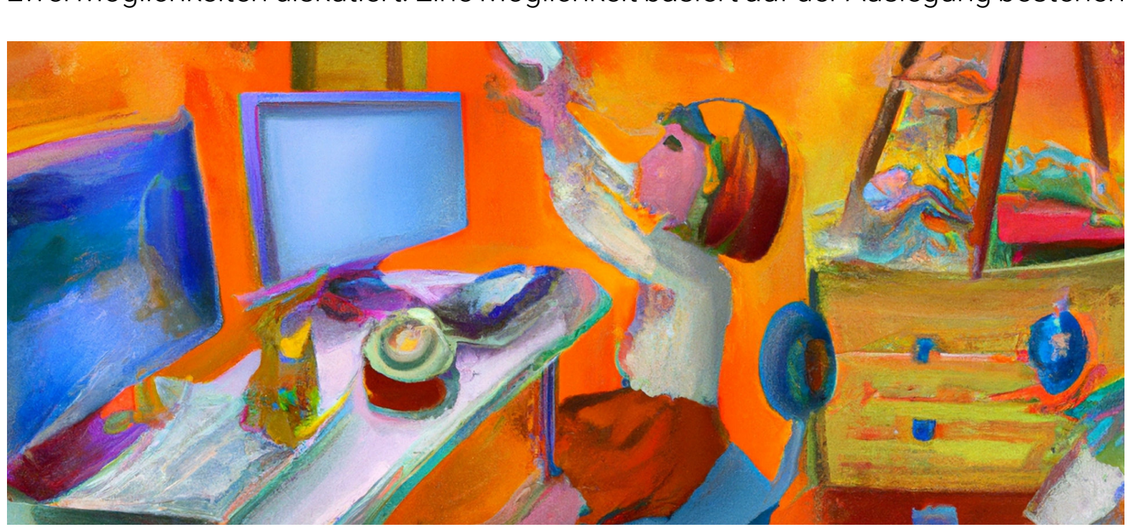
Den ersten eigenen Kontakt mit der digitalen Welt können Kinder im sehr jungen Alter spielerisch über das Interagieren mit sog. *Smart Toys* haben. Der Begriff *Smart Toys* bezeichnet kurz gesagt das Internet der Dinge für Kinder. Intelligentes Spielzeug erkennt seine Umgebung und interagiert mit dieser, etwa durch Gesichts- oder Spracherkennung. Kinder können das Spielzeug unter anderem per App oder über die Sprachschnittstelle verwenden. Eltern sind ebenfalls in der Lage, auf das Spielzeug zuzugreifen und damit die Aktivitäten des Kindes zu beobachten.[1] Ein bekanntes Beispiel ist *Hello Barbie*, eine Barbie, die Gespräche aufzeichnet, verarbeitet und passende Antworten generieren kann.[2]

Ein Großteil der Kommunikation findet in der Online-Welt über Text, Fotos oder Videos statt. Bereits ab sechs Jahren oder jünger können Kinder spezielle Angebote von bekannten Diensten wie *YouTube Kids* oder *Messenger Kids* nutzen. Dort können Eltern unter anderem den Zugang zu bestimmten Inhalten beschränken und die Aktivitäten ihres Kindes über ihr eigenes Konto nachverfolgen.[3] In fortgeschrittenem Alter registrieren sich Kinder und Jugendliche selbst auf Plattformen wie *Instagram*, *Snapchat* oder *TikTok*.

Die digitale Welt wurde ursprünglich nicht für Kinder und Jugendliche entwickelt.[4] Das führt unter anderem dazu, dass sie im Internet mit den gleichen Inhalten und Problemen konfrontiert werden wie Erwachsene. Die digitale Welt bringt somit nicht nur Vorteile mit sich. Zu den Nachteilen zählen insbesondere Fake News[5] und das Sammeln von Daten mit dem Ziel der Erstellung eines Persönlichkeitsprofils, um personalisierte Inhalte zu präsentieren. Bei Kindern und Jugendlichen besteht bei der Erstellung von Persönlichkeitsprofilen die Besonderheit, dass Daten von Geburt an gesammelt werden können. Dadurch werden die Persönlichkeitsprofile viel detaillierter, wodurch sich die Gefahr von Identitätsdiebstahl und Betrug erhöht.

Weitere Problematiken sind die Konfrontation mit unpassenden Inhalten wie Gewaltverherrlichungen oder die Kommunikation mit gefährlichen Kontakten, die – in den schlimmsten Fällen – zu sexueller Ausbeutung, Gewalt oder dem Beitritt einer extremistischen oder sogar terroristischen Gruppe führen können.

Damit Kinder die Möglichkeiten der Digitalisierung nutzen können, müssen die Risiken und Gefahren minimiert werden. Digitale Kinderrechte haben die Aufgabe, Kindern zum einen die Vorteile der Digitalisierung zu ermöglichen und sie zum anderen vor den Risiken hinreichend zu schützen. Bei der rechtlichen Ausgestaltung werden zwei Möglichkeiten diskutiert: Eine Möglichkeit basiert auf der Auslegung bestehen-



der Kinderrechte (vgl. Kapitel A), um sie auf die digitale Umgebung anzuwenden. Als andere Idee wird die Formulierung spezifischer digitaler Kinderrechte vorgeschlagen (vgl. Kapitel C).

1 Bundesamt für Sicherheit in der Informationstechnik, Smarte Spielzeuge – Lernhilfen oder Spione, hier abrufbar (Stand: 15.1.2023).
2 Biselli, Abhörpuppen im Kinderzimmer: und wer ist eigentlich dafür verantwortlich?, hier abrufbar (Stand: 15.1.2023).
3 *YouTube*, AGB, hier abrufbar (Stand: 15.1.2023); ***Messenger Kids,*** Webseite, hier abrufbar (Stand: 15.1.2023).
4 ***UN-Kinderrechtsausschuss***, General Comments No. 25 (2021) on children's rights in relation to the digital environment, Rn. 12.
5 Zu dem Problem von Deep Fakes in sozialen Medien wird auf den Beitrag von ***Beute/Dhunge***l in dieser Ausgabe der CTRL verwiesen.

A. Auslegung bestehender Kinderrechte

Im Jahr 1989 hat *Tim Berners-Lee* den Programmiercode veröffentlicht, der die Grundlage des Internets bildet. Im selben Jahr verabschiedeten die *Vereinten Nationen (UN)* die Kinderrechtskonvention (UNCRC). Es handelt sich dabei um den am meisten ratifizierten Menschenrechtsvertrag in der Geschichte der *UN*.[6] Sie besteht aus drei Säulen: Schutzrechte, Förderungsrechte und Beteiligungsrechte. Die Kinderrechtskonvention erkennt das Kind als Träger eigener Rechte an und definiert vier Grundprinzipien, die in der digitalen Welt von Bedeutung sein können. Die heutigen Herausforderungen der digitalen Lebensumstände von Kindern und Jugendlichen waren damals nicht Teil der Überlegungen. Dementsprechend stellt sich die Frage, ob die Rechte der UNCRC in der digitalen Welt effektiv zur Anwendung kommen können. Als Antwort auf diese Frage hat der *UN-Kinderrechtsausschuss*[7] am 24.3.2021 den *„General Comment No. 25 (2021) on children's rights in relation to the digital environment"* veröffentlicht.[8] Danach müssen die Rechte jedes Kindes im digitalen Umfeld beachtet, geschützt und erfüllt werden.

Bei einem *General Comment* handelt es sich um eine Auslegungshilfe. Er bietet eine offizielle Interpretation, wie Staaten ihren in der UNCRC definierten Verpflichtungen im Zuge der Digitalisierung gerecht werden können. Er ist – anders als Zusatzprotokolle – kein Teil des Vertrages und somit für die Vertragsparteien nicht rechtlich bindend (sog. *soft law*).

„Ein General Comment ist für die Vertragsparteien rechtlich nicht bindend."

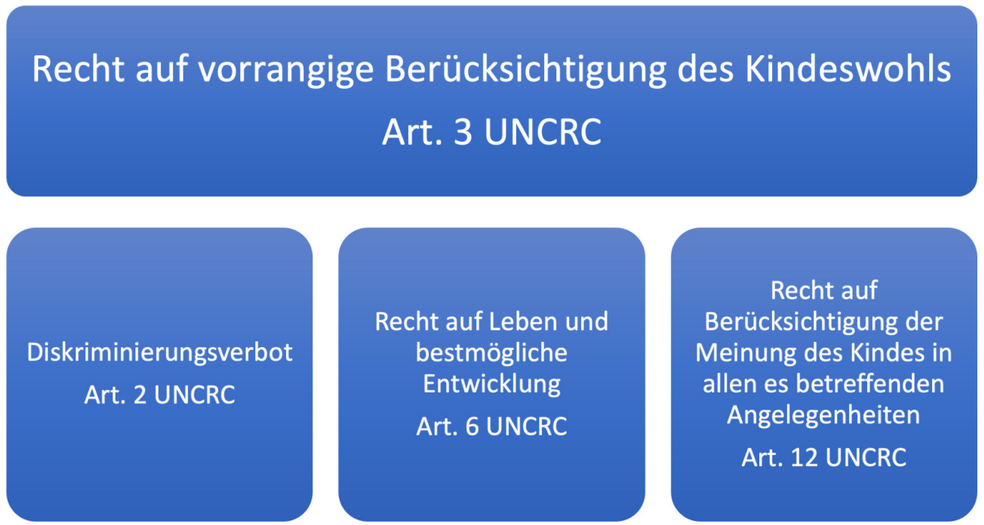
I. Was ist eigentlich rechtlich ein Kind?

Die Definition des Kindes und somit des personellen Schutzbereichs berührt bereits einen Kernpunkt digitaler Kinderrechte. Der *UN-Kinderrechtsausschuss* bespricht diesen Punkt indirekt in seinem *General Comment* unter dem Begriff der *„evolving capacities"* (dt.: sich entwickelnde Fähigkeiten). Hiernach haben Kinder unterschiedliche digitale Entwicklungsfähigkeiten. Ein vierjähriges Kind erfährt erste spielerische Erfahrungen mit Spracherkennung über seinen *SmartToy-Bear*, während ein siebenjähriges Kind bereits über Messaging-Dienste auf seinem eigenen Smartphone kommuniziert. Die zu entwickelnden Fähigkeiten können sich nicht nur anhand des Alters unterscheiden, sondern anhand anderer Parameter wie dem Wohnort oder dem Geschlecht. Die Unterschiede in Bezug auf einzelne Fähigkeiten zeigen, dass die gleichen Maßnahmen, die Kinder allgemein betreffen, nicht die gleiche Wirkung entfalten können. Eine Zugangsbeschränkung zu bestimmten Inhalten kann ein Kind mit niedrigen digitalen Fähigkeiten zunächst einmal schützen, während es ein Kind mit hohen digitalen Fähigkeiten in der Entwicklung aufhalten kann.

Art. 1 I UNCRC: Im Sinne dieses Übereinkommens ist ein Kind jeder Mensch, der das achtzehnte Lebensjahr noch nicht vollendet hat, soweit die Volljährigkeit nach dem auf das Kind anzuwendenden Recht nicht früher eintritt.

Zur Berücksichtigung der *„evolving capacities"* in der Praxis, schlägt der Kinderrechtsausschuss vor, Eltern und andere Erziehungspersonen auf die unterschiedlichen Fähigkeiten aufmerksam zu machen. Damit Eltern und andere Erziehungspersonen Kinder angemessen unterstützen können, sollen sie selbst digitale Kompetenzen erlernen und über die Wichtigkeit von Autonomie und Privatsphäre aufgeklärt werden.

6 Die UN-Kinderrechtskonvention wurde am 20.11.1989 von der UN-Generalversammlung angenommen und trat am 2.9.1990 in Kraft. Die Konvention wurde von allen Staaten, mit Ausnahme der USA, unterzeichnet.
7 Bei dem UN-Kinderrechtsausschuss handelt es sich um einen Fachausschuss der UN (sog. Vertragsorgan), der die Umsetzung und Einhaltung der Konvention beobachtet. Er nimmt in periodischen Abschnitten die Berichte der Vertragsstaaten entgegen und wertet diese aus.
8 UN-Kinderrechtsausschuss, General Comment No. 25 (2021) on children's rights in relation to the digital environment, hier abrufbar (Stand: 15.1.2023).



Der Kinderrechtsausschuss geht jedoch nicht so weit, sich mit der grundsätzlichen Definition des Begriffes Kind auseinanderzusetzen. Nach Art. 1 UNCRC sind Kinder Personen unter 18 Jahren. Bei der Ausgestaltung von digitalen Kinderrechten ist es in Anbetracht der unterschiedlichen digitalen Fähigkeiten (*evolving capacities*) essenziell, dass der UNCRC-Begriff des Kindes dieser Unterscheidung zugänglich ist.

II. Die vier Grundprinzipien

Im Fokus der Kinderrechtskonvention stehen vier Grundprinzipien, wobei Art. 3 UNCRC handlungsleitend über den anderen Rechten steht. Insgesamt unterscheidet die UNCRC die vier in Abbildung 2 dargestellten Grundprinzipien

Der Kinderrechtsausschuss legt diese vier Grundprinzipien vor dem Hintergrund der digitalen Umgebung aus. Ein wichtiges Ziel im Zusammenhang mit dem Diskriminierungsverbot nach Art. 2 UNCRC sei die Verhinderung der digitalen Ausgrenzung. Zunächst müsse die Bereitstellung des digitalen Angebotes gewährleistet werden. Dafür sei es erforderlich, dass Staaten jedem Kind den gleichen Zugang zur digitalen Welt gewährleisten. Kinder sollten digitale Kompetenzen erlernen und ausbauen können. Nicht nur Kinder, sondern Eltern, Erziehungspersonen und Lehrer:innen müssten ebenfalls digitale Kompetenzen stärken, um diese an Kinder und Jugendliche weitergeben zu können.

Art. 3 I UNCRC: Bei allen Maßnahmen, die Kinder betreffen, gleich viel ob sie von öffentlichen oder privaten Einrichtungen der sozialen Fürsorge, Gerichten, Verwaltungsbehörden oder Gesetzgebungsorgangen getroffen werden, ist das Wohl des Kindes ein Gesichtspunkt, der vorrangig zu berücksichtigen ist.

Auf einer weiteren Stufe müssten Kinder auch bei der Nutzung des Angebotes vor Diskriminierungen geschützt werden. Diskriminierungen könnten bei der Nutzung zum Beispiel hinsichtlich der Sicherheit im Internet oder durch einen Datenbias erfolgen. Zur Verhinderung dieser Diskriminierungen fordert der Kinderrechtsausschuss das Ergreifen von proaktiven Maßnahmen.

Vor dem Hintergrund des Rechts auf Leben und bestmögliche Entwicklung erkennt der Kinderrechtsausschuss an, dass die Digitalisierung der Entwicklung von Kindern viele Möglichkeiten eröffne. Es sei die Aufgabe des Staates, Risiken zu minimieren, damit die Entwicklung sicher und frei möglich ist. Das Recht auf Leben überschneide sich mit der Digitalisierung vor allem in Krisensituationen; zum Beispiel durch Verbreitung von Informationen in Zeiten von Corona.

Die Auslegung der Grundprinzipien durch den Kinderrechtsausschuss verdeutlicht, dass eine konsequente Umsetzung der Rechte aus der Konvention auch bedeutet, dass Kinderrechte in der digitalen Welt zur Anwendung kommen. Staaten haben dies durch verschiedene Maßnahmen sicherzustellen. Einen wichtigen Beitrag könnte der von der *EU* geplante *Digital Services Act (DSA)* leisten. Der *DSA* plant eine ausdrückliche Anerkennung der Kinderrechte und nimmt Bezug auf die Kinderrechtskonvention und den *General Comment*.[9]

B. Nationale Umsetzung in Deutschland

Internationale Standards dienen dazu, gleiche Voraussetzungen für alle Kinder zu schaffen. Die Umsetzung im Einzelnen erfolgt jedoch durch die Vertragsstaaten. Der Kinderrechtsausschuss nimmt in seinem *General Comment* die Vertragsstaaten in die Pflicht, Maßnahmen umzusetzen, die dem Schutz der Kinderrechte in der digitalen Umgebung dienen. Es lohnt sich daher, einen Blick auf die nationale Ebene zu werfen.

Die Kinderrechtskonvention gilt seit der Ratifizierung des Vertrages im Jahr 1992 in Deutschland verbindlich als Rang eines einfachen Bundesgesetzes, Art. 59 Abs. 1 S. 1 GG. Aufgrund der völkerrechtsfreundlichen Auslegung des Grundgesetzes, ist die Kinderrechtskonvention zur Auslegung der Grundrechte heranzuziehen. Damit ist noch nicht geklärt, wie die Anwendung der Rechte auf die digitale Umgebung in Deutschland stattfinden wird. Es ist umstritten, ob der Grundsatz der völkerrechtsfreundlichen Auslegung auch solche *General Comments* umfasst, die lediglich eine nicht bindende Auslegungshilfe darstellen.[10] Das Grundgesetz trifft weder Aussagen zu Kinderrechten, noch gibt es ein ausdrückliches Grundrecht mit digitalem Bezug. Im deutschen Grundrechtssystem spielen Kinder nur eine passive Rolle. Der Schutz der Kinder wird Art. 6 II 1 GG[11] und Art. 2 I GG entnommen. Bei Art. 6 II 1 GG sind jedoch die Eltern Träger des Grundrechtes und nicht das Kind selbst. Eltern steht ein Abwehrrecht gegenüber staatlichen Eingriffen in Fragen der Kindererziehung zu (sog. *Elternrecht*). Komplementär dazu begründet Art. 6 II 1 GG eine Grundpflicht der Eltern auf Inanspruchnahme für Pflege und Erziehung des Kindes. Das Kindeswohl soll dabei die Grundlage aller Entscheidungen darstellen.[12] Im Gegensatz dazu zeigt die finnische Verfassung, wie ein subjektives Kinderrecht ausformuliert sein kann: *„Die Kinder sind gleichberechtigt als Individuen zu behandeln und sie sollen auf die Angelegenheiten, die sie betreffen, entsprechend ihrer Entwicklung einwirken dürfen."*

> „Im deutschen Grundrechtssystem spielen Kinder nur eine passive Rolle."

Auch der Kinderrechtsausschuss empfahl Deutschland, Kinderrechte im Grundgesetz zu verankern. Die Gesetzesinitiative zur Ergänzung des Art. 6 II GG im Jahr 2021 erhielt im parlamentarischen Verfahren jedoch nicht die erforderliche zwei-drittel Mehrheit.[13] Digitale Grundrechte lassen sich in Deutschland nur aus der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) ableiten. 2008 hat das BVerfG das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme als spe-

9 Hier abrufbar (Stand 15.1.2023); eine ökonomische Analyse des DSA findet sich bei Niebler/Djebarri in dieser Ausgabe der CTRL.
10 Siehe hierzu Reiling, ZaöRV 78 (2018).
11 „Pflege und Erziehung der Kinder sind das natürliche Recht der Eltern [Hervor. d. Verf.] und die zuvörderst ihnen obliegende Pflicht.", Art. 6 II 1 GG.
12 Uhle, in: BeckOK Grundgesetz, 53. Edition, Art. 6 Rn. 48.
13 Bundesministerium für Familie, Senioren, Frauen und Jugend, Kinderrechte ins Grundgesetz, hier abrufbar (Stand: 15.1.2023); Vorschlag zur Ergänzung des Art. 6 II GG: „Die verfassungsmäßigen Rechte der Kinder einschließlich ihres Rechts auf Entwicklung zu eigenverantwortlichen Persönlichkeiten sind zu achten und zu schützen. Das Wohl des Kindes ist angemessen zu berücksichtigen. Der verfassungsrechtliche Anspruch von Kindern auf rechtliches Gehör ist zu wahren. Die Erstverantwortung der Eltern bleibt unberührt."

zielle Ausprägung des allgemeinen Persönlichkeitsrechts entwickelt. Das Gleiche gilt für das Recht auf informationelle Selbstbestimmung. Es kann daher von einer Unsichtbarkeit digitaler Grundrechte gesprochen werden.[14]

„Es kann von der Unsichtbarkeit digitaler Grundrechte gesprochen werden."

C. Neuformulierung von spezifischen digitalen Kinderrechten

I. Leitlinie des Europarates

Im Gegensatz zum deutschen Gesetzgeber hat sich der Europarat bereits 2018 mit dem Thema digitale Kinderrechte auseinandergesetzt und konkrete *Leitlinien zur Achtung, zum Schutz und zur Verwirklichung der Rechte des Kindes im digitalen Umfeld* verabschiedet.[15] Die Leitlinien nehmen ebenfalls Bezug auf die vier Grundprinzipien der Kinderrechtskonvention. Folgende Leitlinien sollen die Mitgliedstaaten auszugsweise bei der Gestaltung einer digitalen Welt für Kinder unterstützen:

- Recht auf Zugang zu Geräten, Netzanbindung, digitalen Diensten und digitalen Inhalten.

- Kinder haben das Recht auf den Schutz ihrer persönlichen Daten und die Vertraulichkeit ihrer Kommunikation. Dabei sollte der Grundsatz der Datenminimierung (vgl. Art. 5 DSGVO) eingehalten werden. Kindern sollten Informationen über Datenschutz zur Verfügung stehen, die sie verstehen.

- Ein weiteres Thema betrifft die Sicherheit von Kindern vor Gewalt. Staaten sollen Maßnahmen zur Bewältigung von Risiken (etwa Altersverifikationssysteme) schaffen. Der Europarat hebt dafür die Konzepte *Privacy by Design*[16] und *Security by Design*[17] hervor.

Die Leitlinien des Europarats sind mit dem *General Comment* des *UN-Kinderrechtsausschusses* vergleichbar. Es handelt sich jedoch erneut lediglich um Empfehlungen, die keine rechtsverbindliche Wirkung entfalten.

„Die aktuelle passive Rolle des Kindes in der deutschen Rechtsordnung muss sich verändern."

II. Vorschlag für eine digitale Kinderrechts-Charta

Brauchen wir ausformulierte digitale Kinderrechte?

Einerseits beweisen die generell gefassten Rechte aus der Kinderrechtskonvention große Innovationskraft für die Anwendung im digitalen Umfeld. Die Online- und Offline-Welt lassen sich im Alltag häufig nicht voneinander trennen. Man kann deshalb

14 Leuschner, Eine „Charta der Grundrechte für die digitale Zeit", und warum wir sie brauchen, hier abrufbar (Stand: 15.1.2023).
15 ***Europarat***, Leitlinien zur Achtung, zum Schutz und zur Verwirklichung der Rechte des Kindes im digitalen Umfeld, hier abrufbar (Stand: 15.1.2023).
16 ***Privacy by Design*** bedeutet, dass die Privatsphäre der Nutzer:innen bei Online-Diensten so weit wie möglich geschützt wird, indem die Konten von Kindern bspw. nicht öffentlich sind oder die Menge der gesammelten Daten minimiert wird. ***Beobachtungsstelle für gesellschaftspolitische Entwicklung in Europa,*** Kinderrechte im Digitalen Raum, S. 5, hier abrufbar (Stand: 15.1.2023).
17 ***Safety by Design*** bedeutet, dass Online-Dienste so entworfen werden, dass sie die Sicherheit von Benutzer:innen so weit wie möglich gewährleisten, indem etwa standardmäßig sichere Einstellungen für Konten von Kindern voreingestellt werden oder verhindert wird, dass Erwachsene minderjährige Nutzer:innen kontaktieren können, ebd.

argumentieren, es bei digitalen Kinderrechten genauso zu halten: Die Rechte der Offline-Welt müssen die Online-Welt repräsentieren. Deutlich wird dies durch den *General Comment* des Kinderrechtsausschusses.

Andererseits überwiegen die Gründe, die für eine ausformulierte digitale Kinderrechts-Charta sprechen. Dadurch erlangt das Thema mehr Sichtbarkeit, wodurch die gesellschaftliche Debatte belebt wird. Ausdrücklich formulierte Gesetze können für die betroffenen Akteure, also private Unternehmen, Eltern und Kinder, mehr Rechtssicherheit schaffen. Die aktuelle passive Rolle des Kindes in der deutschen Rechtsordnung muss sich verändern.

Bei der Schaffung von digitalen Kinderrechten darf nicht nur der Schutz im Fokus stehen, sondern es müssen auch Förderungs- und Beteiligungsrechte eine gewichtige Rolle spielen: Kindern müssen zur Berücksichtigung der *evolving capacities* als eigenes subjektives Rechtssubjekt mehr Handlungsautonomie zustehen. Das Kind als Träger eigener Rechte anzuerkennen, bedeutet, es in die Lage zu versetzen, autonom über die Art seiner Lebensgestaltung zu entscheiden.[18] Die alleinige Entscheidungsmöglichkeit und die damit einhergehende Verantwortung darf nicht vollständig auf Eltern oder andere Betreuungspersonen übertragen werden.

Ein Vorschlag zur gesetzlichen Ausgestaltung digitaler Kinderrechte könnte wie folgt lauten:

1. Jedes Kind hat das Recht auf fairen Zugang zur digitalen Welt.
Es ist die Aufgabe von Staaten zu gewährleisten, dass jedes Kind den gleichen Zugang zur digitalen Welt hat. Davon umfasst ist unter anderem der freie Zugang zum Internet. Im Internet hat jedes Kind das Recht auf gleichen Zugang zu Informationen aus verschiedenen glaubwürdigen Quellen, die zur Not vom Staat bereitzustellen sind, sowie zu qualitativ guten online Angeboten. Eine Möglichkeit zur Umsetzung des Rechts wäre die Schaffung von kommerziell und politisch unabhängigen Suchmaschinen, die Inhalte kinderspezifisch filtern und anzeigen. Der Zugang darf nur eingeschränkt werden, wo er für das Kindeswohl schädlich ist. Ein Eingriff darf nur aufgrund eines Gesetzes erfolgen und muss die widerstreitenden Interessen in Einklang bringen.

18 Sauerteig, in: Schierer/Rabe/Groner, Institutionelle und personenbezogene Zugänge zum Kinderschutz: Prävention – Kinderschutz – Kinderrechte, 2022, 203 (205).

2. Jedes Kind hat das Recht auf digitale Bildung.
Kinder müssen die Möglichkeit haben, digitale Kompetenzen in der Schule lernen und ausbauen zu können. Damit das Recht praktisch umgesetzt wird, müssen auch Lehrer:innen digitale Kompetenzen erlernen, um diese an Kinder weitergeben zu können. Dem Recht auf Förderung digitaler Kompetenzen kommt eine fundamentale Bedeutung zu, da es eine Ergänzungsfunktion zu den weiteren digitalen Kinderrechten hat.

3. Jedes Kind hat das Recht darauf, dass seine digitalen Fähigkeiten berücksichtigt werden.
Bei Förderungs- und Schutzmaßnahmen haben Staaten darauf zu achten, dass die Maßnahmen die verschiedenen Fähigkeiten und Kompetenzen von Kindern berücksichtigen (*evolving capabilities*). Staaten müssen sich mit dem Thema laufend auseinandersetzen und Studien erheben, um mehr über Unterschiede unter anderem aufgrund von Alter, Wohnort oder Geschlecht herauszufinden. Eine einmalige Studie ist nicht ausreichend, da sich digitale Kompetenzen von Kindern stetig verändern.

4. Jedes Kind hat das Recht vor Online-Gefahren geschützt zu werden.
Die digitale Umgebung muss für Kinder sicher sein, damit sie das volle Potenzial nutzen können. Entscheidend hierbei ist, dass Staaten nicht zu pauschalen Schutzmaßnahmen greifen, sondern die spezifischen Online-Gefahren für Kinder identifizieren und darauf basierend passende Maßnahmen erlassen.

Das Internet ist kein rechtsfreier Raum. Staaten müssen sicherstellen, dass das geltende Recht zum Schutz von Kindern im Internet durchgesetzt wird, bevor weitere – möglicherweise freiheitsbeschränkende – Maßnahmen erlassen werden.

5. Jedes Kind hat das Recht auf digitale Selbstbestimmung und Selbstdarstellung.
Das Recht dient der freien Entwicklung der Persönlichkeit. Kinder sollen selbstständig bestimmen, wie sie online auftreten wollen. Das bedeutet auch, dass Entscheidungen rückgängig gemacht werden können. Von Bedeutung sind insbesondere das Recht auf Berichtigung und Vergessenwerden.

6. Jedes Kind hat das Recht auf Beteiligung bei der Ausarbeitung von Maßnahmen hinsichtlich der Umsetzung digitaler Kinderrechte.
Kinder kennen sich in der digitalen Umgebung oft besser aus als Erwachsene und wissen, was ihnen wichtig ist. Staaten müssen bei der Ausarbeitung von Maßnahmen, die zur Umsetzung digitaler Kinderrechte dienen, vorab Kindern die Möglichkeit eröffnen, sich zu beteiligen. Staaten könnten diesbezüglich Umfragen oder Abstimmungen erstellen und Kinder über diese informieren.

7. Jedes Kind hat das Recht darauf, dass die Ausübung ihrer Rechte in der digitalen Umgebung gewährleistet wird.
Das Internet gewährleistet die Ausübung vieler Rechte. Staaten müssen die Ausübung der Rechte gewährleisten und fördern. Die Umsetzung digitaler Kinderrechte darf nicht zur unverhältnismäßigen und willkürlichen Einschränkung der Rechte von Kindern führen. Kontrollmaßnahmen oder Überwachungen stellen dabei nur eine ultima ratio dar.

8. Vor dem Erlass von Maßnahmen ist das Prinzip Kindeswohl durch Design zu berücksichtigen.
Bereits vor Erstellung eines digitalen Produktes oder eines Gesetzes zur Umsetzung digitaler Kinderrechte oder anderer Maßnahmen müssen die Auswirkungen auf das Kindeswohl analysiert und in das Design implementiert werden. Staaten

müssen sicherstellen, dass auch private Akteure den Grundsatz *Kindeswohl by Design* umsetzen.

D. Fazit

Die Auslegung der *UN-Kinderrechtskonvention* durch den *Kinderrechtsausschuss* und die Leitlinien des *Europarates* erkennen die Herausforderungen und Chancen, denen Kinder in einer digitalen Welt begegnen. Sie präsentieren Staaten Vorschläge für Maßnahmen, um darauf angemessen reagieren zu können. Es obliegt nun den Vertragsstaaten, den *General Comment* und die Leitlinien des Europarates umzusetzen, damit Kinder als aktive Nutzer:innen von der digitalen Welt profitieren können. Die Verabschiedung von ausformulierten – und für den jeweiligen Vertragsstaat verbindlichen – digitalen Kinderrechten würde dabei mehr Rechtssicherheit schaffen.

Weiterführende Hinweise

- Livingstone / Third, Children and young people's rights in the digital age: an emerging agenda, New Media and Society, hier abrufbar (Stand: 15.1.2023)
- Initiative der Zeit-Stiftung: Charta der digitalen Grundrechte der Europäischen Union hier abrufbar (Stand: 15.1.2023)
- Hofmann / Donath, Gutachten bezüglich der ausdrücklichen Aufnahme von Kinderrechten in das Grundgesetz nach Maßgabe der Grundprinzipien der UN-Kinderrechtskonvention, Schriftenreihe des deutschen Kinderhilfswerkes 2017, hier abrufbar (Stand: 15.1.2023)
- Noller, Kinderrechte by Design: Kinderrechte und digitale Produkte, hier abrufbar (Stand: 15.1.2023)
- Andresen / Dreyer, Die Rolle der Eltern bei der datenschutzrechtlichen Einwilligung für ihre Kinder, DuD 6/2022, 361

Talking Legal Tech, Folge 41: "Meta – wie entwickelt man den weltweit ersten Antidiskriminierungschatbot, Said Haider & Meryem Can?"

Talking Legal Tech, Folge 28: "Regulierung & Innovation – wie lässt sich beides vereinbaren, Martin Ebers?"

Zurück zum Inhaltsverzeichnis

Grundwissen

Legal Tech – darf man das?

Lucas Schönborn

Open Peer Review

Dieser Beitrag wurde lektoriert von: Ferdinand Wegener & Joela Worm

Lucas Schönborn ist Doktorand an der Universität zu Köln, wissenschaftlicher Mitarbeiter bei Linklaters und betreibt den Legal-Tech-Blog lawtomise.com.

Inkasso - ein Begriff, der den meisten Verbrauchern Schweiß auf die Stirn treibt. Welche Rechnung wurde nicht gezahlt? Was habe ich vergessen? Diese negative Assoziierung könnte sich jedoch in Zukunft ändern. Seit einigen Jahren gibt es Inkasso-Anbieter, die dafür sorgen, dass geringwertige Ansprüche gegen Fluggesellschaften, Vermieter und Co durchgesetzt werden, sodass der Durchsetzung des

Verbraucherschutzes endlich die Bedeutung zukommt, die ihm gebührt. Dem haftet jedoch ein kleines Problem an: Ist das Geschäftsmodell überhaupt von der Inkasso-Lizenz umfasst? Schließlich gibt das Rechtsdienstleistungsgesetz (RDG) vor: Das Monopol der außergerichtlichen Rechtsberatung liegt gem. § 3 RDG bei der Anwaltschaft. Eine Ausnahme stellen Inkassodienstleister dar. Der Schwerpunkt von solchen Geschäftsmodellen liegt jedoch mehr auf dem Eintreiben der Forderung als der Prüfung, ob ein solcher Anspruch überhaupt besteht. Eine signifikante Abweichung von der Tätigkeit diverser Legal-Tech-Anbieter, die unter der Inkassolizenz operieren. Nach mannigfaltigen Auseinandersetzungen in der Literatur (die naturgemäß in ihrer Breite nicht dargestellt werden kann) hat schließlich auch der BGH seine Pfähle eingerammt. Dies hat den Gesetzgeber dazu bewogen, auch mal ein Wörtchen mitzureden.

A. Schutzcharakter des RDG

Nach § 1 I RDG soll das RDG wie sein Vorgängergesetz, das RBerG[1], Rechtssuchende, den Rechtsverkehr und die Rechtsordnung vor unsachgemäßer Beratung schützen. Diese Schutzzweckbestimmung ist vor allem für die Auslegung des Gesetzes relevant. Sie dient dazu, eine an den Schutzzwecken des RDG orientierte Würdigung des Einzelfalles zu finden.

B. Ausnahme des Inkassobegriffs

Eine Ausnahme vom Beratungsmonopol wurde in § 10 I RDG für den Fall der Inkassodienstleistung normiert. Dieser verweist auf § 2 II 1 RDG, der eine Legaldefinition des Inkassobegriffs enthält. Eine Inkassodienstleistung ist dadurch geprägt, dass man aufgrund einer Inkassoermächtigung Forderungen einzieht, die jedoch gleichzeitig wirtschaftlich und formal fremd bleiben. Rechtlich wird dies über eine Empfangs- (§ 362 II, 185 BGB) und Einzugsermächtigung (§ 185 BGB) für die Forderung bewerkstelligt. Ob jedoch Legal-Tech-Angebote von diesem Ausnahmetatbestand umfasst sind, erschien lange Zeit sehr fraglich. Die Tätigkeit solcher Legal-Tech-Unternehmen unterscheidet sich wesentlich von denen der klassischen Inkassounternehmen: Schließlich liegt der Schwerpunkt hier weniger auf dem Eintreiben der Forderung als der rechtlichen Prüfung, ob ein derartiger Anspruch überhaupt besteht.

> „Vor dem Urteil war nicht vorhersehbar, ob einem Legal Tech-Unternehmen, in das Millionen investiert wurden, plötzlich von Gerichten der Riegel vorgeschoben wird."

Eine nicht zu unterschätzende Rechtsunsicherheit. Diese wirkt rechtshemmend und verschreckt Investoren und Unternehmen. Schließlich ist nicht vorhersehbar, ob ein Unternehmen, in das Millionen investiert wurden, plötzlich von Gerichten der Riegel vorgeschoben wird. Dies würde gravierende Konsequenzen zur Folge haben. Diese Unsicherheit hat der BGH mit einem liberalen Urteil teilweise beseitigt. Ferner hat der Gesetzgeber durch eine Reform des RDG den Legal Tech-Geschäftsmodellen unter der Inkassolizenz grundsätzlich seinen Segen erteilt.

Welche Fragen wurden jedoch genau vom BGH verhandelt und welche Antwort hat der Gesetzgeber gefunden?

1 Das Rechtsberatungsgesetz wurde 1935 verabschiedet. Sinn und Zweck war es unter anderem, jüdische Mitbürgerinnen und Mitbürger aus der Anwaltschaft auszuschließen. Dass das RBerG somit aufgrund des Unrechtscharakters historisch ohnehin belastet war, versteht sich von selbst.

C. BGH-Urteil *LexFox*

Nachdem bereits zwischen verschiedenen Kammern des LG Berlin Uneinigkeit dahingehend bestanden hatte, ob Legal-Tech-Unternehmen unter der Inkasso-Erlaubnis nach §§ 10 I 1, 2, II 1 RDG zulässig operierten,[2] hat der BGH am 27. November 2019 ein lang erwartetes Grundsatzurteil verkündet.[3]

I. Hintergrund

Klägerin war die ***LexFox GmbH*** (ehemals ***wenigeremiete.de***). Sie machte Ansprüche aus abgetretenem Recht des Mieters gegen die Vermieterin wegen eines behaupteten Verstoßes gegen die Mietpreisbremse nach § 556d BGB geltend. Die Klägerin bietet softwarebasiert die Möglichkeit an, die entsprechenden Rahmenbedingungen einzugeben und automatisiert festzustellen, ob ein Verstoß gegen die Mietpreisbremse vorliegt. Bei Vorliegen eines Verstoßes kann der Rechtssuchende einen entgeltlichen Geschäftsbesorgungsvertrag mit der Klägerin abschließen und ihr die Ansprüche gegen ein Erfolgshonorar abtreten. Die ***LexFox GmbH*** bemüht sich anschließend, die Ansprüche außergerichtlich einzutreiben. Ist dies nicht erfolgreich, kann die Klägerin mit Zustimmung des Rechtssuchenden einen Vertragsanwalt mit der gerichtlichen Durchsetzung beauftragen. Als Vergütung erhält die Klägerin im Erfolgsfall einen Teil der enthaltenen Rückzahlung in Höhe eines Drittels der Ersparnisse eines Jahres.

Der Mieter trat seine Ansprüche an die Klägerin ab. Mit Schreiben vom 20.03.2017 rügte die Klägerin den Verstoß gegen die Mietpreisbremse. Die Miete habe bei Beginn in dem vorliegenden Fall 24,76 € höher gelegen, als sie aufgrund der ortsüblichen Vergleichsmiete hätte sein dürfen. Das AG Berlin-Lichtenberg hat der Klage grundsätzlich stattgegeben. Hinsichtlich der vorgerichtlichen Rechtsverfolgungskosten i.H.v. 166,90 € hat es den Rechtsstreit jedoch für erledigt erklärt und die Berufung zugelassen. Das LG Berlin hat die Berufung zurückgewiesen, da bereits die Aktivlegitimation der Klägerin nicht vorläge. Die Forderung sei bereits aufgrund eines Verstoßes gegen das Verbot des Erbringens unerlaubter Rechtsdienstleistung nach §§ 2 I, 3, 5, 10 RDG i.V.m. § 134 BGB nichtig. Der Schwerpunkt der Tätigkeit der Klägerin liege hier auf dem Gebiet der Rechtsberatung und nicht auf dem Eintreiben der Forderung, was die Inkassolizenz nach §§ 10 I Nr. 1, 2, II 1 RDG überschreite. Dies sei mit dem RDG unvereinbar und führe im Ergebnis zu einer Nichtigkeit der Abtretung. Die vom Berufungsgericht zugelassene Revision hatte im Ergebnis Erfolg.

II. Entscheidung

Mit einem liberalen Urteil, das den Legal Tech-Anbietern den Rücken stärkt, hat der BGH die ablehnende Entscheidung des LG Berlin aufgehoben und betont, dass die Aktivlegitimation der Klägerin zu Unrecht verneint wurde.[4] Die Voraussetzungen der Nichtigkeit der Abtretung i.S.d. § 398 BGB nach § 3 RDG i.V.m. § 134 BGB liegen nicht vor. Die Befugnis zum Erteilen einer Rechtsdienstleistung ist hier nach den §§ 10 I Nr. 1, 2 Abs. 2 S. 1 RDG von der Inkassolizenz (noch) umfasst. Damit halten sich die Tätigkeiten der Klägerin noch im Rahmen dessen, was ihr durch die Inkassolizenz erlaubt ist. Ein hinreichend enger sachlicher Zusammenhang der rechtlichen Prüfung der Forderung mit der eigentlichen Eintreibung liegt vor.

Einen ersten Argumentationsschwerpunkt legt der BGH auf die Frage, ob überhaupt Raum für eine Nichtigkeit der Abtretung nach § 2 RDG i.V.m. § 134 BGB ist, wenn der Dienstleister entsprechend registriert ist. Eine Auffassung in der Literatur, dass die Abtretung nur dann gem. § 3 RDG i.V.m. § 134 BGB nichtig ist, wenn der Inkassodienstleister nicht entsprechend nach § 10 I Nr. 1 RDG registriert ist, wird jedoch abgelehnt. Konsequenz dieser Auffassung wäre, dass das einzige Sanktionsregime für registrierte Inkassodienstleister die §§ 13, 14a RDG sein würden. Wäre ein Dienstleister registriert, käme eine Nichtigkeit der Abtretung nicht mehr in Betracht. Eine solche weitgehende Zulässigkeit würde – so der BGH – den Schutzzweck

2 Vgl. LG Berlin, Urt. v. 24.01.2019 - 67 S 277/18; LG Berlin, Beschl. v. 26.07.2018 - 67 S 157/18.
3 BGHZ 224, 89 ff.
4 Vgl. dazu auch *Deckenbrock*, CTRL 2/2022, 117 (118 f.).

des § 3 RDG jedoch verfehlen. Ferner bedient sich der BGH im Rahmen der Auslegung dem Wortlautargument: dieses spricht im Rahmen von § 3 RDG („*nur in dem Umfang zulässig*“) ebenfalls dafür, registrierte Inkassodienstleistungen als umfasst anzusehen.

Auch hat der Gesetzgeber in den Gesetzesmaterialien dargelegt, dass er an der bereits unter dem RBerG geltenden Rechtslage festhalten wolle. Insofern stellt der Charakter des § 3 RDG als Verbotsgesetz i.S.d. § 134 BGB die wichtigste Sanktionsfolge dar. Sich lediglich auf Maßnahmen nach den §§ 13a, 14 RDG zu beschränken, würde dem Schutzcharakter nicht hinreichend Rechnung tragen. Ein hinreichender Vertrauensschutz wird ebenfalls nicht begründet, da das Geschäftsmodell vor Eintragung als Inkassodienstleister nicht hinreichend auf seine rechtliche Zulässigkeit überprüft wird. Das Vertrauen kann nicht weiter gehen als das Register es rechtfertigt.

Eine Nichtigkeit der Abtretung nach § 3 RDG i.V.m. § 134 BGB liegt hingegen dann vor, wenn bei einer „*umfassenden Würdigung der Gesamtumstände aus der objektivierten Sicht eines verständigen Auftraggebers [ein Verstoß] eindeutig vorliegt und unter Berücksichtigung der Zielsetzung des [RDG], die Rechtsuchenden, den Rechtsverkehr und die Rechtsordnung vor unqualifizierten Rechtsdienstleistungen zu schützen (§ 1 I 2 RDG), in ihrem Ausmaß als nicht nur geringfügig – etwa auf Randbereiche beschränkt – anzusehen ist.*“[5] Dem Verbraucher wird also eine eigene Einschätzung aufgebürdet, wenngleich sich diese auf Evidenz beschränkt. Wo genau jedoch diese Trennlinie des Offensichtlichen zum Geringfügigen verlaufen soll, führt der BGH nicht weiter aus.

Die Tätigkeit der Klägerin ist nach BGH noch als Inkassotätigkeit zu sehen, da die Eintreibung von Forderungen im Vordergrund steht. Es wird also ein weites Verständnis des Inkassobegriffs offenbart. Grundsätzlich lässt sich dennoch für die Frage, ob die Registrierung nach § 10 I Nr. 1 RDG überschritten ist, was nach § 3 RDG i.V.m. § 134 BGB zur Nichtigkeit der Abtretung führt, „kein allgemeingültiger Maßstab aufstellen“. Maßgebend ist eine an den Schutzgütern des RDG orientierte Auslegung, wobei auch Wertentscheidungen des Gesetzgebers hinreichend berücksichtigt werden müssen. Dies sind namentlich etwa Art. 12 GG des Inkassodienstleisters und die vom Schutz des Art. 14 GG umfassten Forderungen der Kunden. Der BGH betont, dass andernfalls die infrage stehenden Forderungen wahrscheinlich aufgrund ihrer Geringwertigkeit gar nicht durchgesetzt würden *(rationales Desinteresse*). Die von Art. 14 GG geschützte Forderung wäre faktisch wertlos, was nicht im Sinne der Eigentumsgarantie sein kann.

> „Ohne Inkassodienstleister wäre aufgrund von rationalem Desinteresse die von Art. 14 GG geschützte, aber geringwertige Forderung faktisch wertlos, was nicht im Sinne der Eigentumsgarantie sein kann.“

Ein weiteres Argument des BGH ist, dass die Inkassodienstleister lediglich im außergerichtlichen Bereich tätig sind. Die Funktionsfähigkeit der Rechtspflege ist bei einer solchen, auf außergerichtliche Eintreibung gerichteten Tätigkeit noch nicht berührt. Ferner lehnt der BGH einen Verstoß gegen § 4 RDG ab, da keine Gefahr der Interessenkollision besteht. Grundsätzlich hat der BGH mit seinem Urteil Legal Tech-Anbietern, die unter der Inkassolizenz operieren, zwar keinen „Freibrief für ausufernde Rechtsberatung“ erteilt, aber das Geschäftsmodell der ***LexFox GmbH*** „gerade noch“

5 BGHZ 224, 89 Rn. 91.

für zulässig erklärt. Weiterhin unklar bleibt dennoch, wo die genaue Trennlinie zwischen zulässiger Rechtsberatung durch Inkassodienstleister und dem Kerngeschäft der Anwaltschaft verläuft, das vom anwaltlichen Rechtsberatungsmonopol noch vollumfänglich geschützt ist. Dies ist dann Gegenstand künftiger Einzelfallbetrachtung, wie der BGH auch in seinem Urteil mehrfach betont hat.

„Mit dem Urteil hat der BGH keinen „Freibrief für ausufernde Rechtsberatung“ erteilt, aber das Geschäftsmodell „gerade noch“ für zulässig erklärt.“

D. Gesetzgeberische Reaktion

2021 hat der Gesetzgeber als Anlass auf das Urteil ‚***wenigermiete***‘ des BGH das RDG entsprechend reformiert und das ‚Legal-Tech-Gesetz‘ verabschiedet. Dieses trat am 01.10.2021 in Kraft. Die Reform kann hier insofern als anlassbezogen bezeichnet werden, als dass der Gesetzgeber vor Erlass des Urteils noch keinen Reformbedarf gesehen hat. Er hielt die vorherige Rechtslage für hinreichend sicher und ausgeglichen. Dies geht aus einer kleinen Anfrage der FDP-Fraktion an die Bundesregierung hervor. Das neue Gesetz hat vor allem zum Ziel, den Rechtsrahmen der verschiedenen Akteure anzupassen, für hinreichende Transparenz am Markt zu sorgen und adäquate Vorschriften für den Verbraucherschutz zu schaffen. Der Inkassobegriff des § 2 II 1 RDG wird insofern erweitert, als neben der Einziehung auch die „auf die Einziehung bezogene rechtliche Prüfung und Beratung“ umfasst wird. Die Erweiterung bezieht sich jedoch nur auf den Umfang, in dem es für die Einziehung der konkreten Forderung erforderlich ist. Eine weitergehende Tätigkeit ist hingegen nicht mehr zulässig. Dennoch dürfte es noch von dem neuen Inkassobegriff umfasst sein, eine mietrechtliche Rüge und den entsprechenden Auskunftsanspruch geltend zu machen. Derartige außergerichtliche Instrumentarien sind schließlich auf die Geltendmachung der konkreten Forderung bezogen.

Der Inkassobegriff wird somit einerseits erweitert, indem nun ausdrücklich auch die Prüfung des Bestehens der Forderung umfasst ist. Andererseits wird jedoch klargestellt, dass eine weitergehende Tätigkeit nicht mehr davon umfasst ist.

„Mit der Reform des RDG und der Verabschiedung des ‚Legal Tech-Gesetzes’ ist die Auseinandersetzung rund um die Vereinbarkeit solcher Legal Tech-Dienstleistungen mit der Inkassolizenz ist somit beigelegt.“

Die Auseinandersetzung in Literatur und Rechtsprechung rund um die Vereinbarkeit solcher Legal Tech-Dienstleistungen mit der Inkassolizenz ist somit beigelegt. Legal-Tech-Anbieter operierten, wie jetzt entschieden, zulässig unter der Inkassolizenz. Aufgrund etwaiger Unsicherheiten hat der Gesetzgeber solchen Geschäftsmodellen ausdrücklich seinen Segen erteilt und die entsprechenden Vorschriften reformiert.

Weiterführende Literatur

- Anfrage der FDP an die Bundesregierung: Drucksache Bundestag 19/5438, hier abrufbar.
- BGHZ 224, 89, NJW 2020, 208 ff.
- Legal Tech Gesetz Drucksache BT 19/27673, hier abrufbar.
- Deckenbrock, Legal Tech und anwaltliches Berufsrecht, CTRL 2/2022, 117
- Fries, de minimis curat mercator – Legal Tech wird Gesetz, NJW 2021, 2537.

Zurück zum Inhaltsverzeichnis

„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

Osborne Clarke

Digitalisierung des Handelsregisters: Was kostet kostenlos?

Ramon Schmitt

Ramon hat sich vor seiner Zeit als Referendar am OLG Köln vertieft als wissenschaftlicher Mitarbeiter mit Gesellschafts- und Kartellrecht auseinandergesetzt. Er ist Vorstandsmitglied im Legal Tech Lab Cologne und verantwortet die interne Compliance.

Open Peer Review

Dieser Beitrag wurde lektoriert von: Maria Osmakova & Joela Worms

Deutsche Justiz‘ und ‚fortschrittliche Digitalisierung‘ sind zwei Begriffe, die man selten im selben Kontext hört. Neben wiederkehrenden Problemen mit dem besonderen elektronischen Anwaltspostfach (*beA*)[1] und der häufigen Ablehnung von Anträgen für Gerichtsverhandlungen per Videokonferenz nach § 128a ZPO aufgrund von fehlender IT Ausstattung des Gerichts,[2] wird auch die fehlende Konsistenz bei der Digitalisierung kritisiert. Es erscheint zum Beispiel inkonsequent

1 Fun Fact: Einer E-Mail an ein Gericht kann im beA maximal 100 MB angehängt werden. Bei Schriftsätzen, die gerne eine dreistellige Seitenanzahl übersteigen und viele eingescannte Anhänge haben, wird eine Übersendung deshalb häufiger problematisch.

2 Vgl. weiterführend hierzu *Paschke*, CTRL 1/22, 81 ff., die sich im nächsten Schritt mit der Frage einer digitalisierten Gerichtsöffentlichkeit befasst. Weiterführend zu dem Themenkomplex der digitalen Dokumentation einer strafgerichtlichen Hauptverhandlung siehe Osmakova, CTRL 2/22, 69 ff.

und fast schon amüsant, dass seit 2022 nach § 130d S. 1 ZPO Rechtsanwälte zwar Schriftsätze elektronisch an Gerichte übersenden müssen, diese aber dann bei Gericht ausgedruckt werden, um zur Akte gelegt werden zu können. Denn die Pflicht zur elektronischen Aktenführung wird es für die Justiz flächendeckend erst ab 2026 geben.[3] Ein Hinweis des Gesetzgebers, dass auch er der Justiz in Sachen Digitalisierung keine schnelle Umsetzung zutraut? Dennoch gibt es neben diesen Stolpersteinen auch Digitalisierungserfolge innerhalb der Justiz wie etwa die erste Versteigerung der in einem Strafverfahren sichergestellten Bitcoins[4] oder Pilotprojekte wie der KI-gestützte Frankfurter Urteilskonfigurator ***Frauke***[5], der Gerichte in ähnlich gelagerten Flugverspätungsverfahren unterstützen soll. Der Richter gibt ***Frauke*** den Tenor und die Kosten vor und anhand dessen schlägt es Textbausteine zur Begründung des Urteils vor. Zu diesen Erfolgen gesellt sich nun auch ein Digitalisierungsfortschritt im Gesellschaftsrecht: Zum August 2022 werden auf der Webseite des Handelsregisters alle Registerauszüge aus dem Handels-, Genossenschafts-, Vereins- und Partnerschaftsregister sowohl kostenfrei als auch ohne die Notwendigkeit eines Benutzerkontos digital zum Download bereitgestellt. Aber bevor im Detail darauf eingegangen wird, was sich im Register geändert hat, wer die Kosten jetzt trägt (C.II.) und ob diese Änderungen wirklich einen Digitalisierungserfolg darstellen (D.), werden zunächst die Fragen beantwortet, wieso es das Handelsregister überhaupt gibt (A.) und wie es aufgebaut ist (B).

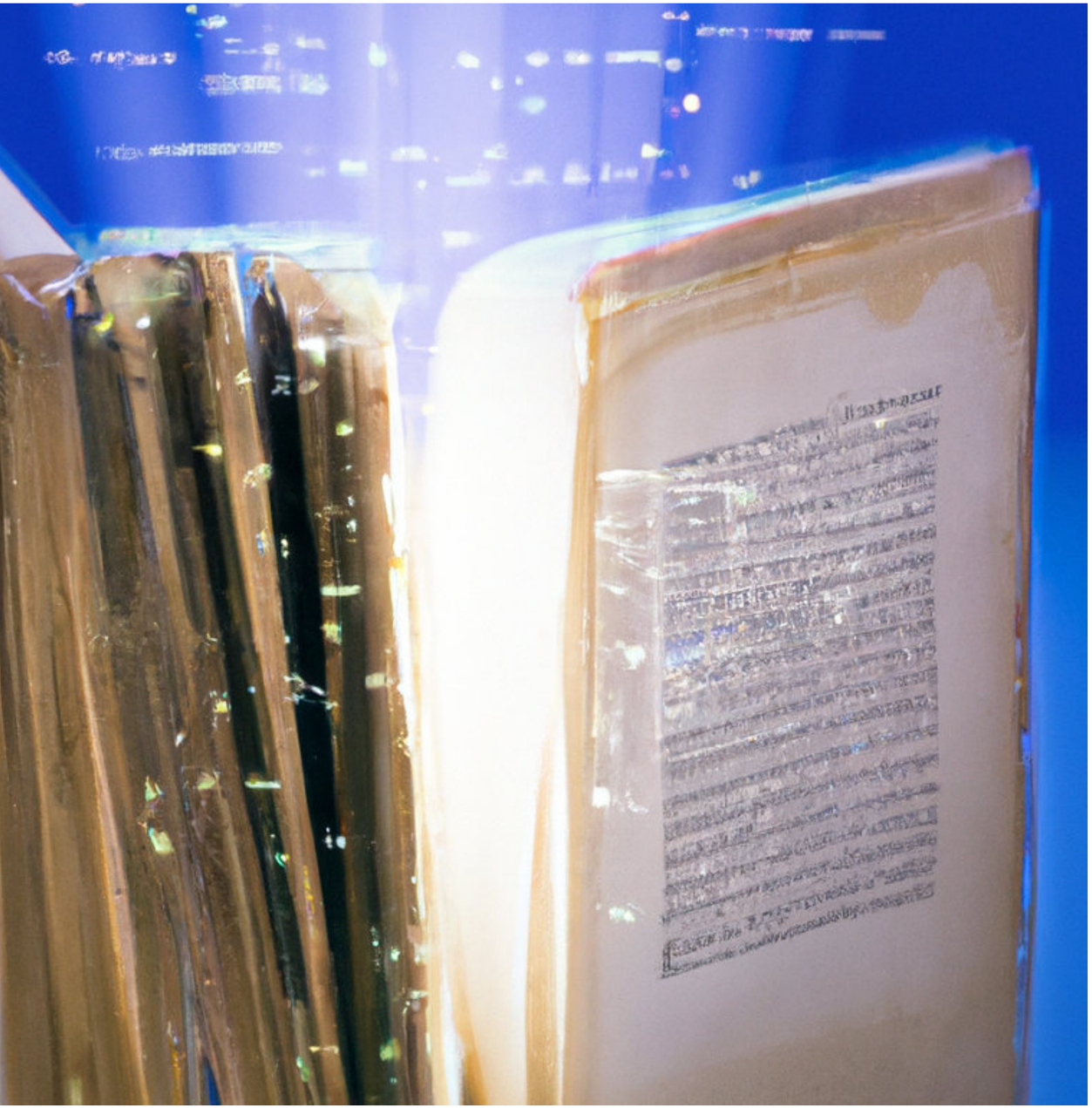
A. Zweck des Handelsregisters

Studierende kommen häufig zum ersten Mal in Berührung mit dem Handelsregister im Kontext der „***negativen Publizität***" des § 15 I HGB. Was der Jurist hiermit auf komplizierte Weise ausdrücken möchte, ist ganz einfach: Was in das Handelsregister eingetragen werden muss und nicht eingetragen ist, muss ein potenzieller Vertragspartner auch nicht gegen sich gelten lassen. Aufgrund der Regelung des § 15 I HGB muss zwangsläufig die tatsächliche (materielle) Rechtslage von der im Handelsregister eingetragenen (formellen) Rechtslage unterschieden werden, wobei sich letztere ‚durchsetzt'. So kann etwa eine Prokura nach § 49 HGB – wie jede andere rechtsgeschäftliche Vollmacht – grundsätzlich jederzeit nach §§ 168, 167 I BGB widerrufen werden. Dieser Widerruf ist jedoch nach § 53 II HGB in das Handelsregister einzutragen. Der juristische Witz ist nun, dass nach dem Widerruf die Prokura materiell tatsächlich erlischt, so dass der ehemalige Prokurist nun Geschäfte als nicht vertretungsberechtigter Vertreter abschließt, § 179 BGB. Da der Widerruf der Prokura aber nicht in das Handelsregister eingetragen wurde, gilt er formell weiter als Prokurist, wenn der Vertragspartner sich auf das fehlerhafte Handelsregister berufen möchte.

> **§ 15 I HGB:** „Solange eine in das Handelsregister einzutragende Tatsache nicht eingetragen und bekanntgemacht ist, kann sie von demjenigen, in dessen Angelegenheiten sie einzutragen war, einem Dritten nicht entgegengesetzt werden, es sei denn, daß [sic!] sie diesem bekannt war."

Diese Differenzierung zwischen der tatsächlichen Rechtslage und den Eintragungen im Handelsregister ergibt sich aus dessen Zweck: Es soll umfassende Rechtssicherheit und Transparenz schaffen. Steht etwas nicht im Handelsregister, so kann sich der Geschäftspartner hierauf berufen und dementsprechend darauf vertrauen, dass das Register auf dem aktuellen Stand ist. Die enorme Wichtigkeit und Notwendigkeit dieser vermittelten Rechtssicherheit lässt sich leicht durch ein Beispiel belegen: Der tüchtige CTRL-Leser A vertreibt gewerbsmäßig Computerspiele. Er möchte eine große Anzahl an Exemplaren im Wert von 10 Millionen Euro an das DAX-Unternehmen und den Elektronikfachhändler Jupiter veräußern. Hierzu möchte er einen Vertrag mit Jupiters Prokurist

3 Vgl. im Einzelnen das „Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs", hier abrufbar (Stand: 01.01.2023).
4 Diese Versteigerung darstellend und durch eine wirtschaftliche Analyse Verbesserungsvorschläge aussprechend: Schmitt/Wegener, CTRL 1/22, 34 ff.
5 Weitere Informationen zu *Frauke* sind hier abrufbar (Stand: 01.01.2023).



B abschließen. Das Bestehen der Prokura ist für A nun enorm wichtig und keine Selbstverständlichkeit, weil die Prokura eine jederzeit widerrufbare rechtsgeschäftliche Vollmacht darstellt, welche nur hinsichtlich ihres Umfangs gesetzlich normiert ist. Ist B jedoch kein Prokurist, haftet nur dieser persönlich nach § 179 BGB. Eine Privatperson wird selten ein Vermögen von 10 Millionen Euro erreichen. Gäbe es kein Handelsregister, müsste A jetzt selbst herausfinden, ob die Prokura tatsächlich (noch) besteht. Er müsste etwa beim Geschäftsführer des Unternehmens anrufen und dies erfragen. Jedoch besteht selbst dann noch keine Gewähr dafür, dass die Prokura nicht durch Widerruf – beispielsweise durch einen anderen Geschäftsführer – erloschen ist. Ein solcher Prozess ist dem A auch im Hinblick auf die Schnelllebigkeit des Geschäftsverkehrs nicht zumutbar.

Durch das Handelsregister kann sich A gewiss sein, dass Jupiter die Prokura des B gegen sich gelten lassen muss, solange sie im Handelsregisterauszug der Jupiter eingetragen ist. Somit kann sich A gemütlich zurücklehnen und die 10 Millionen Euro in Kryptowährungen investieren.

B. Aufbau und Inhalt des Handelsregisters

Das Handelsregister ist in zwei Abteilungen aufgeteilt: Abteilung A für Einzelkaufleute und Personengesellschaften wie die OHG und KG (HRA-Nummern) und Abteilung B für Kapitalgesellschaften wie GmbHs und AGs (HRB-Nummern). Jedes Handelsgewerbe erhält somit abhängig von der jeweiligen Rechtsform also eine HRA- oder HRB-Nummer.

In beiden Abteilungen sind dabei folgende drei Ausdrucke für den Geschäftsverkehr am relevantesten: Zunächst gibt es einen aktuellen Auszug, der Eintragungen im Handelsregister in Bezug auf Firmennamen, Stammkapital, Geschäftsanschrift, Unternehmensgegenstand, vertretungsberechtigte Personen und Gesellschafter bei Personengesellschaften wiedergibt. Hingegen stellt der chronologische Handelsregisterauszug alle Änderungen dieser Fakten ab ca. 2005 in einer laufenden

Abbildung 2: Die Landingpage des Online-Handelsregisters

Tabelle dar, so dass man auch frühere Eintragungen nachvollziehen kann. Für alle Eintragungen vor 2005 ist ein historischer Auszug erforderlich, da diese Daten nicht in das elektronische Handelsregister übernommen wurden.

Daneben finden sich noch weitere wichtige Dokumente wie die Satzungen von GmbHs und AGs und die Gesellschafterliste einer GmbH. Gesellschafterlisten der AGs hingegen werden nicht aufgeführt, da hier der Handel von Aktien so einfach wie möglich gestaltet sein soll. Sollte allerdings ein einziger Aktionär mehr als 3% einer AG erwerben, greifen §§ 33, 40 WpHG, wonach die betroffene AG dies zu veröffentlichen hat, sodass die Aktionärsstruktur auf der Webseite der AG oftmals im Bereich 'Investor Relations' eingesehen werden kann.[6]

6 Beispielsweise: Die Aktionärsstruktur der Volkswagen AG ist hier abrufbar (Stand: 01.01.2023).

Vereinsregister des Amtsgerichts Köln	Wiedergabe des aktuellen Registerinhalts Abruf vom 29.12.2022 21:06	Nummer des Vereins: **VR 20777**
Abdruck	Seite 1 von 1	

1. **Anzahl der bisherigen Eintragungen:**

   3

2. **a) Name:**

   Legal Tech Lab Cologne e.V.

   b) Sitz:

   Köln

3. **a) Allgemeine Vertretungsregelung:**

   Jedes Vorstandsmitglied vertritt einzeln. Zu Rechtshandlungen, welche den Verein vermögensrechtlich zu Leistungen von mehr als 2.500,00 € verpflichten, bedarf es der Zustimmung aller Vorstandsmitglieder.

   b) Vertretungsberechtigte und besondere Vertretungsbefugnis:

   Vorstand: Breuer, Konstantin, Köln, *09.01.1996
   Vorstand: Ecker, Isabel, Köln, *25.03.1996
   Vorstand: Lihotzky, Isabel, Köln, *21.02.1999
   Vorstand: Pilch, Larissa, Hamburg, *14.05.1992
   Vorstand: Scheja, Hendrik, Köln, *18.05.1994
   Vorstand: Schenk, Santeri Konstantin, Mainz, *18.01.2000
   Vorstand: Schmitt, Ramon, Köln, *16.03.1997
   Vorstand: Tröber, Erik Christian, Münster, *12.12.1999
   Vorstand: Wegener, Ferdinand, Köln, *14.10.1997

Abbildung 3: Der aktuelle Vereinsregisterauszug des Legal Tech Lab Cologne e.V.

In der Praxis wird das Handelsregister hauptsächlich für drei Zwecke verwendet: Erstens wird überprüft, ob der Vertreter des Unternehmens als organschaftlicher Vertreter (Geschäftsführer oder Vorstand) oder Prokurist im Handelsregister eingetragen ist, um nicht in die Gefahr des § 179 BGB zu geraten. Zweitens werden

die Auszüge genutzt, um die Gesellschafterstrukturen einzelner Gesellschaften oder großer Konzerne nachzuvollziehen. Drittens und nicht zu vernachlässigen ist die Information über die Höhe des Stammkapitals einer GmbH (bzw. das Grundkapital einer AG oder die Einlagen von Kommanditisten). Das ist vor allem für Kreditinstitute bei der Vergabe von Krediten relevant: Je höher dieses Kapital ist, desto höher ist wahrscheinlich die Haftungsmasse der Gesellschaft. Die Höhe des Stammkapitals hat maßgeblichen Einfluss auf die Kreditkonditionen und -linien, welche die Bank der Gesellschaft einräumt.

C. Die Umsetzung

I. Die Neuheit

Das übergeordnete Handelsregisterportal gibt es bereits seit vielen Jahren im Internet. Bis zum 01.08.2022 benötigte man allerdings zum Abruf der Dokumente sowohl ein Benutzerkonto als auch eine hinterlegte Zahlungsmethode.

Die Dokumente kosteten je nach gewünschtem Datenformat und -typ zwischen 1,50€ und 4,50 Euro. Dies stellte zwar schon damals eine niedrige Einstiegshürde dar, allerdings führte aber dazu, dass das Handelsregister als Informationsquelle weniger genutzt wurde. So wurde es von Privatpersonen fast nie genutzt, obwohl auch sie ein Interesse an den Informationen hatten. Etwa macht es als Mieter Sinn bei der Vermietung durch eine Gesellschaft zu überprüfen, ob der Handelnde überhaupt Vertretungsmacht hat und wie viel Grund- bzw. Stammkapital der Gesellschaft zur Verfügung steht. Aber auch bei Kanzleien war der Abruf der Auszüge immer mit einem zeitlichen und administrativen Mehraufwand verbunden, da man intern die Kosten einem Mandat zuweisen musste, um sie später dem Mandanten in Rechnung stellen zu können. Dies hat sich nun mit dem Gesetz zur Umsetzung der Richtlinie 2019/1151 (DiRUG[7]) und der zugehörigen Richtlinie 2019/1151 (Digitalisierungsrichtlinie[8]) geändert. Die Digitalisierungsrichtlinie sollte eigentlich schon bis August 2021 umgesetzt werden, aber Deutschland hat von einer in der Richtlinie vorgesehenen Verlängerungsoption bis zum August 2022 Gebrauch gemacht.

Das DiRUG ist bekannt für seine Möglichkeit der Online-Gründung von GmbHs über Online-Termine mit einem Notar. Die weniger bekannte Änderung betrifft das Handelsregister: Alle Handelsregisterauszüge und Dokumente aus dem Vereins-, Partnerschafts- und Genossenschaftsregister sind jetzt sowohl völlig kostenlos als auch ohne ein Benutzerkonto abrufbar. Dies erhöht selbstverständlich die Transparenzfunktion des Handelsregisters, aber die interessante Frage bleibt: Wer bezahlt für die Möglichkeit eines kostenlosen Handelsregisters? Bei wem bleiben die Kosten hängen?

II. Das Problem der Finanzierungsfrage

1. Die Ausgangslage

Vor der Gesetzesänderung durch das DiRUG war die Frage nach der Finanzierung dem Grunde nach ziemlich klar: Der Abrufende trug die Kosten. Die Gebühren, welche ein Unternehmen bei der Anmeldung zahlen musste, umfassten die Kosten der Bereitstellung und Abrufbarkeit auf der Webseite nicht. Insoweit stellte § 1 I der Handelsregistergebührenverordnung (HRegGebV)[9] klar, dass die Gebühren vornehmlich nur die „*Eintragung*" sowie „*Prüfung und Aufbewahrung*" betrafen. Dass die Gebühren nicht die Kosten des Onlineregisters umfassten, wurde zudem mit einem Blick auf die Gebührentabelle deutlich: So zahlte eine AG im Zusammenhang mit einer erstmaligen Eintragung wegen einer Umwandlung

7 Das Änderungsgesetz ist hier abrufbar (Stand: 01.01.2023).

8 Die Digitalisierungsrichtlinie ist hier in deutscher Sprache abrufbar (Stand: 01.01.2023).

9 Die HRegGebV ist hier abrufbar (Stand: 01.01.2023).

nach dem Umwandlungsgesetz[10] mit 660 Euro eine mehr als doppelt so hohe Gebühr als eine GmbH. Diese Mehrkosten können sich nur aus dem Mehraufwand hinsichtlich des erhöhten Prüfungsaufwandes des Registergerichts bei der AG[11] ergeben und gerade nicht aus höheren administrativen Kosten aufgrund des Online-Handelsregisters.

Zusätzlich konnte man nach der alten Rechtslage die Frage der Angemessenheit der Abrufkosten pro Dokument bemängeln. Gerade im Hinblick auf den Transparenz- und Verkehrsschutzgedanken des Handelsregisters wäre es völlig ungerechtfertigt gewesen, wenn die Gebühren wesentlich höher gewesen wären als die tatsächlich anfallenden Kosten. Zum Betreiben des Onlineregisters fallen dem Staat natürlich Kosten in Bezug auf die notwendige Infrastruktur für Server sowie die interne Übermittlung und das Einfügen der Informationen in die Datenbanken an. Jedoch wird der Ausdruck und die Übermittlung eines Handelsregisterauszuges kaum Kosten in Höhe von 4 Euro verursachen, da automatisiert eine Kopie einer schon hinterlegten PDF angefertigt wird. Dass hier pro Datei wirklich ein monetärer Aufwand von 4 Euro entstand, war fragwürdig.

Aber wie sieht es mit den Kosten seit der Einführung des kostenlosen Registers im August 2022 aufgrund des DiRUG aus?

III. Finanzierung des neuen Systems

Das Onlineregister kostet auch nach der Gesetzesänderung weiterhin Geld. Die Erhaltung der Infrastruktur ist nicht plötzlich kostenfrei geworden. Die Frage ist somit, auf wessen Kosten das Handelsregister nun kostenfrei geworden ist. Wird das Handelsregister etwa jetzt ausschließlich durch Steuergelder querfinanziert?

Die Finanzierungsfrage beantwortet das DiRUG, welches auch die HRegGebV anpasste: In dem neuen Absatz 2 des § 2 HRegGebV heißt es inzwischen, dass auch für die „Bereitstellung von Registerdaten oder Dokumenten zum Abruf" eine Gebühr bei der Anmeldung anfällt. So ist nach Teil 6 der HRegGebV bei jeder Eintragung nochmals der anfallenden Gebühr zu entrichten. Im obigen Beispiel hat die AG bei der Eintragung neben den bereits fälligen 660 Euro zusätzlich für die abstrakte Bereitstellung im Onlineregister schlappe 220 Euro zu zahlen. Die GmbH müsste für den gleichen Vorgang ca. 86 Euro zusätzlich zahlen.

10 Das Umwandlungsgesetz bietet einen geordneten Prozess für verschiedene Rechtsformen an, um die Rechtsform zu ändern. Hierbei wird ein abschließender Katalog angeboten, der Verschmelzungen von Rechtsträgern, Spaltung eines Rechtsträgers, Vermögensübertragung und den Formwechsel eines Rechtsträgers vorsieht. Das Gesetz ist hier abrufbar (Stand: 01.01.2023).

11 Vergleiche hierzu etwa § 146 II UmwG, wonach bei der Abspaltung und Ausgliederung einer AG weitere Dokumente - wie der Spaltungs- und Prüfungsbericht - bei der Anmeldung einzureichen sind.

Nach der neuen Gesetzesregelung drängt sich die Frage der Angemessenheit der Kostenhöhe noch stärker auf. Dass die Bereitstellung der Dokumente in der Online-Datenbank des Handelsregisters auf unbestimmte Zeit wirklich 220 Euro kostet, ist sehr fragwürdig. Noch merkwürdiger als die Höhe der Kosten ist ihr Anknüpfungspunkt: Die Kosten knüpfen an die Grundgebühr des jeweiligen Vorgangs an (zum Beispiel $^1/_3$ der Kosten für die Eintragung der Umwandlung einer AG). Die Höhe dieser Grundgebühr wurde vom Gesetzgeber maßgeblich wegen des jeweiligen Prüfungsaufwands des Registergerichts bei der Anmeldung festgesetzt. Je umfassender die Prüfung des Gerichts, desto mehr sollte es kosten. Hieran die Kosten für die Online-Bereitstellung anzuknüpfen, erscheint bizarr, denn ein höherer Prüfungsaufwand führt nicht zwangsläufig zu höheren Kosten bei der Bereitstellung der Dokumente in der Online-Datenbank des Handelsregisters. Zuzugeben ist, dass ein höherer Prüfungsaufwand des Registergerichts oftmals mit einer höheren Anzahl an Dokumenten einhergeht, die in das Register einzupflegen sind. Allerdings rechtfertigt dies eine so hohe prozentuale Koppelung (der Grundgebühr) noch nicht. Weshalb eine GmbH knapp 150 Euro weniger für die Online-Bereitstellung als eine AG für den gleichen Umwandlungsvorgang zahlen muss, erschließt sich nicht.

Man mag jetzt einwenden, dass die nun um erhöhten Anmeldungsgebühren bei einer Kapitalgesellschaft nicht ins Gewicht fallen, jedoch wird dabei die Auswirkungen auf die Start-up-Szene übersehen. Ein gewichtiges Problem des deutschen Gesellschaftsrechts sind schon seit langem die hohen Gründungskosten von Gesellschaften. Hier hat der Gesetzgeber mit der Einführung der Gesellschaftsform der Unternehmergesellschaft und Bereitstellung von Mustersatzungen[12] bereits die Kosten der Gründung gesenkt.

Die Gründungskosten einer UG mit Mustersatzung beginnen bei ca. 300 Euro. Allerdings sind die Gründungskosten weiterhin wesentlich höher als bei ausländischen Rechtsformen wie der britischen Limited, die lediglich eine Eintragung in das 'englische Handelsregister' für ca. 30 Euro benötigt. Die neue - zusätzlich zu den 300 Euro anfallende - Bereitstellungsgebühr beläuft sich bei der Gründung einer UG mit Mustersatzung auf ca. 50 Euro und ist damit ein nicht unerheblicher Kostenpunkt, der Gründungen in Deutschland noch weniger attraktiv werden lässt. Schließlich ist das Onlineregister zum 01.08.2022 keineswegs kostenfrei geworden, sondern der Kostenschuldner wurde schlicht ausgetauscht. Statt der Zahlung einer Gebühr pro konkreten Abruf ist eine – zu hohe – Pauschale normiert worden.

Unternehmensgesellschaft (UG): Die UG ist eine in § 5a GmbHG geregelte Sonderform der GmbH. Es handelt sich um eine vollwertige GmbH, die aber ein Anfangsstammkapital unter 25.000 Euro haben kann. Dadurch können UGs mit einem Stammkapital ab 1 Euro gegründet werden, sodass nicht mehr eine erhebliche Liquidität zur Gesellschaftsgründung notwendig ist. Nachteilig ist, dass ein Viertel des Jahresüberschusses nicht an die Gesellschafter ausgezahlt werden darf, § 5a III GmbHG.]

§ 2 II HRegGebV: „Gebühren für die Bereitstellung von Registerdaten oder Dokumenten zum Abruf werden neben den Gebühren für Eintragungen im Register oder für Entgegennahmen zum Register gesondert erhoben."

Jedenfalls ist im Hinblick auf den Verkehrsschutz und die Transparenz, welche vom Handelsregister ausgehen soll, die Idee, dass das anmeldende Unternehmen und nicht der Abrufende die Mehrkosten tragen sollte, völlig richtig. Nur so können die Hürden zur Einsichtnahme in das Handelsregister auf der Nutzerseite völlig beseitigt

12 Die Mustersatzung ist eine im Anhang des GmbHG (hier abrufbar, Stand: 01.01.2023) vorhandene Vorlage, die man zur Gründung einer Gesellschaft mit bis zu drei Gesellschaftern nutzen kann. Sie führt dazu, dass der Notar (auch wegen einer zwingenden Bargründung) einen geringeren Prüfungsaufwand hat und führt auch bei dem Register zu geringeren Kosten, weil die Satzung etwa auch als Gesellschafterliste gilt.

werden. Ob aber die Höhe dieser Kostenverlagerung angemessen ist, erscheint mindestens zweifelhaft.

D. Fazit

Im Kern sind die Änderungen durch das DiRUG zu begrüßen. Je weniger Hürden es für die Einsicht in das Handelsregister für den Endnutzer bestehen, desto besser wird der Transparenzgedanke des Handelsregisters verwirklicht.

Problematisch sind allerdings die hohen Kosten der abstrakten Online-Bereitstellung. Die zusätzlichen Gebühren erreichen dabei mit $^1/_3$ der jeweiligen Grundgebühr eine Höhe, die ernsthaft einen negativen Einfluss auf die Gründungsbereitschaft deutscher Start-ups haben kann. Letztlich muss man jedoch sagen, dass das Handelsregister hinsichtlich der Digitalisierung nun auf einem lobenswerten Stand ist, der eine umfassende Nutzungsmöglichkeit zulässt.

Insoweit erscheint es zweifelhaft, ob eine weitere Digitalisierung des Handelsregisters – etwa mittels einer Blockchain – noch sinnvoll wäre, da diese Blockchain ohnehin nur über wenige Nodes dezentralisiert und permissioned betrieben werden würde. Welcher Mehrwert hier im Hinblick auf Sicherheit und Nutzerfreundlichkeit durch eine solche Blockchain im Backend erreicht werden könnte, muss kritisch hinterfragt werden.[13]

In diesem Sinne: Wenn einer Deiner Bekannten sich mal wieder als Gesellschafter, Geschäftsführer oder Gründer eines Start-ups auf LinkedIn vermarktet, dann schau doch mal ins Handelsregister, ob das wirklich stimmt und wie viel (Stamm)Kapital in dem Projekt steckt! Einem geschenkten Handelsregister schaut man dann mal gerne ins ‚Maul'!

13 Ausf. über die Blockchain im Gesellschaftsrecht: *Ludovica*, CTRL 2/22, 77 ff.

Notarity: Digitale Beglaubigung, Beurkundung, GmbH-Gründung & Vollmachtserteilung

Was ist die Blockchain, Florian Glatz

Was ist Legal Tech? mit Nico Kuhlmann

Zurück zum Inhaltsverzeichnis

Aufsatz

Deepfakes als Gefahr für die Demokratie — eine rechtliche Einordnung

Eva Beute & Anna-Katharina Dhungel

Open Peer Review

Dieser Beitrag wurde lektoriert von:
Hannah Wissler & Hendrik Scheja

Sind Sie es leid, dass Politiker die Öffentlichkeit jedes Mal anlügen, wenn sie den Mund aufmachen? Möchten Sie in der Lage sein, das Gesicht einer Person auf den Körper einer anderen Person zu bearbeiten? Stellen Sie sich vor, jeder hätte die Möglichkeit, das Gesicht von jedem, den er will, so aussehen zu lassen, wie er will. Dieser Tag ist da. Diese Technologie wird ‚Deepfake' genannt. In einem Deepfake-Video werden die Form, die Größe und das Gewicht einer Person verwendet, um ein überzeugendes, dreidimensionales Abbild des Gesichts der Zielperson zu erstellen. Das bedeutet, dass ein gutes Deepfake über genügend Informationen verfügt, um eine überzeugende Nachbildung der Gesichtszüge einer Person zu erstellen.

Deepfakes sind aus Gründen, die man sich gut vorstellen kann, gefährlich. Vielleicht wird es benutzt, um Politiker zu erpressen. Vielleicht wird es genutzt, um politische Gegner zu schikanieren. Vielleicht wird es von Kriminellen verwendet, um ihre Opfer zu terrorisieren oder, wenn sie clever genug sind, um den Opfern vorzugaukeln, dass sie es mit anderen Personen zu tun haben. Vielleicht wird es eingesetzt, um die Öffentlichkeit zu täuschen oder sie etwas Falsches glauben zu lassen.

Der Text, den Du soeben gelesen hast, ist nicht ‚echt', sondern wurde von einer Maschine über die Plattform ***InferKit*** erzeugt.[1] Lediglich das Schlagwort ‚Deepfake' wurde eingegeben, der restliche Inhalt ist von einem System der künstlichen Intelligenz (KI) geschrieben worden. Anschließend wurde der Text – ebenfalls von einer KI, der Anwendung ***DeepL*** – vom Englischen in das Deutsche übersetzt.[2] Ähnlich ist es bei den Autorenbildern[3], hierbei handelt es sich nicht um die Autorinnen, sondern vielmehr existieren die abgebildeten Personen gar nicht. Es sind von künstlichen neuronalen Netzen hergestellte Fotos von nicht existierenden Personen, die über eine Website abgerufen werden können.[4]

A. Aufbau dieses Beitrags

Neben Texten und Bildern, die von KI-Systemen generiert werden, entsteht momentan eine neue Dimension der künstlich erzeugten Medien: Deepfakes. Ebenso wie von Maschinen erzeugte Texte und Bilder für echt gehalten werden können, ist es mittlerweile möglich, Videos zu generieren, die nie geschehene Sachverhalte täuschend echt inszenieren. Ziel dieses Beitrags ist es, die Erstellung und Verbreitung von Deepfakes rechtlich zu analysieren und zu bewerten. Der Fokus liegt dabei auf solchen Deepfakes, die zur Manipulation der öffentlichen Meinung und zur gezielten Beeinflussung von politischen Prozessen eingesetzt werden. Zu diesem Zweck wird zunächst eine Definition von Deepfakes und deren Funktionsweise vorgestellt sowie der aktuelle Stand der Forschung erörtert (vgl. Kapitel B). Hierauf aufbauend wird analysiert, welche Gefahren sich für eine Demokratie aus der Verbreitung von Deepfakes ergeben, unter welche Straftatbestände solche Fälle subsumiert werden können und welche weiteren Lösungsansätze für diese neue Herausforderung in Betracht kommen (siehe Kapitel C). Der Beitrag schließt mit einem Ausblick (siehe Kapitel D).

> „Dass online gerne Wirklichkeiten verdreht, aus dem Kontext gerissen oder verfälscht dargestellt werden, ist bekannt."

B. Ein Überblick

I. Kann man noch glauben, was man sieht?

Auf ***TikTok*** führt ein vermeintlicher ***Tom Cruise*** einen Zaubertrick vor oder zeigt, wie man seine Hände korrekt wäscht.[5] Im Film ***Star Wars: Rogue One*** taucht die verstorbene Schauspielerin ***Carrie Fisher*** plötzlich in einer Szene auf und in einem Video auf der Plattform ***Vimeo*** erklärt eine Person, die wie ***Kim Kardashian*** aussieht: „***I genuinly love the process of manipulating people online for money***."[6]

1 Hier abrufbar (Stand: 01.08.2022).
2 Hier abrufbar (Stand: 01.08.2022).
3 Zum Zwecke der besseren Lesbarkeit wird bei den personenbezogenen Hauptwörtern nur die männliche Form verwendet. Diese Begriffe sollen für alle Geschlechter gelten.
4 Hier abrufbar (Stand: 01.08.2022).
5 Hier abrufbar (Stand: 01.08.2022).
6 Black/Fullerton, Digital Deceit: Fake News, Artificial Intelligence, and Censorship in Educational Research, in: Open Journal of Social Sciences 08 (07): 71-88, hier abrufbar (Stand: 01.09.2022); Posters, 'When there's so many haters…', hier abrufbar (Stand: 19.08.2022). Der Künstler hat diverse Deepfake Videos erstellt, neben denen von Kim Kardashian auch u.a. von Mark Zuckerberg oder Boris Johnson, hier abrufbar (Stand: 01.09.2022).

Nicht immer entspricht das, was in einem Video suggeriert wird, der Wahrheit. Dass online gerne Wirklichkeiten verdreht, aus dem Kontext gerissen oder verfälscht dargestellt werden, ist mittlerweile bekannt. Der ***Duden*** nahm die Begrifflichkeit „***Fake News***“ 2017 auf und versteht darunter: „***in den Medien und im Internet, besonders in sozialen Netzwerken, in manipulativer Absicht verbreitete Falschmeldungen***“.[7] Welche gesellschaftlichen Auswirkungen diese Fake News haben können, zeigt etwa der Fall ‚***Pizzagate***‘: Während der US-Präsidentschaftswahl 2016 verbreitete sich online der Verschwörungsmythos[8], dass ***Hillary Clinton*** aus dem Keller einer Pizzeria in Washington D.C. einen internationalen Pädophilen-Ring leiten würde. Nachrichten rund um diese Theorie verbreiteten sich in den sozialen Medien rasant und führten schließlich dazu, dass sich ein bewaffneter Mann Zugang zu der besagten Pizzeria verschaffte, um die vermeintlich dort anzutreffenden Kinder zu retten. Er feuerte Schüsse auf Türen und einen Computer ab, musste dann jedoch feststellen, dass die Pizzeria noch nicht einmal über einen Keller verfügte.[9]

Eine neue Art der Fake News sind Deepfakes, deren gesellschaftliche Folgen sich bisher nur erahnen lassen. Was passiert, wenn in den oben genannten Fake-Videos nicht ***Tom Cruise***, ***Carrie Fisher*** oder ***Kim Kardashian*** zu sehen wären, sondern ein Afroamerikaner, der von einem weißen Polizisten brutal zusammengeschlagen wird oder ein Soldat, der einen Gefangenen foltert? Dass solche Videos enorme gesellschaftliche Auswirkungen haben können, zeigen vergleichbare (reale) Videos, etwa das der Tötung von ***George Floyd*** – welches in den USA landesweite Demonstrationen hervorrief und kürzlich mit dem Pulitzerpreis ausgezeichnet wurde[10] – oder die Foto- und Videoaufnahmen rund um die Folterungen durch US-Soldaten im irakischen Abu Ghraib, welche international für Entsetzen sorgten.[11]

Doch wie ist es nun ersichtlich, wann der Inhalt eines Videos ‚echt‘ ist, welche Folgen hat es, wenn Inhalte generell angezweifelt werden und welche rechtlichen Möglichkeiten hat ein Staat, um einer negativen gesellschaftlichen Entwicklung entgegenzuwirken?

7 Hier abrufbar (Stand: 17.08.2022).
8 Information zur Unterscheidung zwischen Verschwörungsmythos und Verschwörungstheorie hier abrufbar (Stand: 13.10.2022).
9 Bis heute gibt es Anhänger dieser Theorie, siehe beispielsweise Kalenberg, Wieso Menschen weiterhin an „Pizzagate“ glauben, hier abrufbar (Stand: 17.08.2022).
10 Spanhel, Der Kampf gegen Rassismus geht weiter, hier abrufbar (Stand: 18.08.2022); Häntzschel, George-Floyd-Video bei Pulitzer-Preisen gewürdigt, hier abrufbar (Stand: 17.08.2022).
11 Wittwer, Abu Ghraib: Es kann jeden Tag wieder passieren, hier abrufbar (Stand: 19.08.2022).

II. Definition Deepfake

Westerlund definiert Deepfakes als *„hyper-realistic videos digitally manipulated to depict people saying and doing things that never actually happened."*[12] Zum Teil wird dies näher konkretisiert: *„In a deepfake video, a person's face, emotion or speech are replaced by someone else's face, different emotion or speech, using deep learning technology."*[13] Der Wörter-Zusammenschluss entsteht aus *„deep learning"* und *„fake"*, wobei ersteres eine spezielle Form der künstlichen Intelligenz meint: Deep Learning umschreibt künstliche neuronale Netze, die mittlerweile in vielen Anwendungen zum Einsatz kommen, etwa bei der Bild- und Spracherkennung, bei Zeitreihenanalysen oder beim Entdecken von Betrugsfällen. Im Rahmen von Deepfakes lernt ein künstliches neuronales Netz anhand großer Datenmengen die Mimik, Stimme, Tonlage und Eigenarten von zwei Personen, um das Gesicht der einen Person in einem Video für das originäre Gesicht auszutauschen.[14]

Teilweise werden Deepfakes zusätzlich kategorisiert in die Klassen *face-swap*, *lip-sync* und *puppet-master*.[15] Beim *Face-Swap* wird das Gesicht der einen Person auf den Kopf einer anderen Person transferiert. Eine besonders bekannte App für *Face-Swaps* ist beispielsweise *Snapchat*, aber auch andere Anbieter wie etwa *Instagram* bieten den Tausch und Transfer von Gesichtern an. Beim *Lip-Sync* wird in einem Video der gesprochene Inhalt einer Person mit einem neuen Audio hinterlegt und anschließend werden die Lippen- und Mundbewegungen dementsprechend angepasst. Bei dieser Methode lässt es sich in der Regel leichter erkennen, dass es sich um eine Fälschung handelt, weil die Lippenbewegungen nicht immer zur restlichen Gestik und Mimik der Person passen. Bei der *Puppet-Master-Methode* wird das Gesicht und der Körper der Zielperson im Video beibehalten, die Gesichtsbewegungen können jedoch komplett manipuliert werden. Sowohl die Stimme, als auch die Mimik können somit in Einklang gebracht werden.[16] *Wagner* und *Blewer* betonen, dass ein Deepfake mehr ist als ein Video, welches mittels Software entsteht. Vielmehr ist gerade das Besondere an Deepfakes, dass ein KI-System die Proportionen der Gesichter und deren Ausdrücke lernt und es somit möglich ist, neuen Inhalt mit diesen Gesichtern zu erstellen bzw. das Gesicht der einen Person durch das der anderen Person in beliebig vielen neuen Situationen auszutauschen.[17]

> „In a deepfake video, a person's face, emotion or speech are replaced by someone else's face, different emotion or speech, using deep learning technology."

Erstmals kamen Deepfakes in das öffentliche Bewusstsein, als ein Nutzer auf der Plattform *Reddit* 2017 ein Video teilte, in dem er das Gesicht der Schauspielerin *Gal Gadot* in pornografische Videos transferiert hatte.[18] Die Erstellung von gefälschter Pornografie ist eine der häufigsten Einsatzszenarien.[19] Es wird geschätzt, dass es sich bei rund 96 % aller Deepfakes um nicht einvernehmlich erstellte Pornografie handelt.[20] Daneben werden Deepfakes häufig in sozialen Netzwerken veröffentlicht, weil sie sich dort rasant verbreiten können und Nutzer dazu neigen, häufig geteilten Inhalten mehr zu glauben. Parallel dazu führt eine andauernde Informa-

12 Westerlund, 2019, The Emergence of Deepfake Technology: A Review, in: Technology Innovation Management Review 9 (11), 39 (40).
13 Mitra, Mohanty u.a., A Machine Learning based Approach for DeepFake Detection in Social Media through Key Video Frame Extraction, in: SN Computer Science, 2, 1.
14 Westerlund, 2019, The Emergence of Deepfake Technology: A Review, in: Technology Innovation Management Review 9 (11), 39 (40).
15 Agarwal, Farid u.a., Detecting Deepfake Videos from Appearance and Behavior, in: IEEE International Workshop on Information Forensics and Security (WIFS), New York, 1 (3), hier abrufbar (Stand: 17.08.2022).
16 Semaan, Die Demokratisierung von Deepfakes, hier abrufbar (Stand: 17.08.2022).
17 Wagner/Blewer, "The Word Real Is No Longer Real": Deepfakes, Gender, and the Challenges of AI-Altered Video, in: Open Information Science 3, 36.
18 Hier abrufbar (Stand: 13.10.2022).
19 *Hancock/Bailenson,* The Social Impact of Deepfakes, in: Cyberpsychology, Behaviour, and Social Networking 24 (3), 149 (150).
20 *Ajder, Patrini u.a.,* The State of Deepfakes: Landscape, Threats, and Impact, hier abrufbar (Stand 13.10.2022).

tionsüberflutung dazu, dass Nutzer quellenunabhängig alle Informationen anzweifeln und das Vertrauen in Medien signifikant sinkt – es sei denn, die Inhalte bestätigen eigene Meinungen und Weltansichten. In diesem Fall sind Personen sogar bereit, Inhalten zu glauben, selbst wenn es deutliche Hinweise auf einen Fake gibt.[21]

Screenshot eines Deep Fakes von Barack Obama / Jordan Peele

Das in der Abbildung referenzierte Video „***You Won't Believe What Obama Says In This Video!***" wurde von dem US-amerikanischen Medienunternehmen ***BuzzFeed*** 2018 auf ***YouTube*** veröffentlicht und verbreitete sich über die sozialen Netzwerke innerhalb kürzester Zeit.[22] Es zeigt zunächst nur ***Barack Obama***, der einige ungewöhnliche und überraschende Sätze sagt. Nach 35 Sekunden wird neben ihm der Schauspieler ***Jordan Peele*** eingeblendet und es wird deutlich, dass er die Stimme des ehemaligen US-Präsidenten ist. Das Video wurde auf ***YouTube*** über 9,1 Millionen Mal aufgerufen (Stand September 2022) und es war bereits Grundlage für wissenschaftliche Forschung.[23]

21 Westerlund, The Emergence of Deepfake Technology: A Review, in: Technology Innovation Management Review 9 (11), 39 (40).
22 Hier abrufbar (Stand: 17.08.2022).
23 Vaccari, Cristian; Chadwick, Andrew, Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News, in: Social Media + Society January-March, 1-13.

III. Funktionsweise und Erstellung

Bei den für Deepfakes genutzten künstlichen neuronalen Netzen handelt es sich konkret um sogenannte ***Generative Adversarial Networks*** (***GAN***). Diese bestehen aus zwei miteinander agierenden Systemen: dem ***Generator*** und dem ***Discriminator***. Beide trainieren mit denselben Datensätzen. Der Generator versucht ein Video zu erstellen, das so gut ist, dass der Discriminator es nicht als Fake erkennt. Wenn dieser den Fake erkennt, gibt er diese Information zurück und der Generator versucht erneut ein besseres Deepfake zu erstellen. Dieser Vorgang wird fortgesetzt, bis optimale Ergebnisse erreicht werden und der Discriminator das gefälschte Video als real einstuft.[24] Je mehr Zeit und Rechenkapazitäten vorhanden sind und je besser die Datenqualität ist, desto realistischer kann das Deepfake aussehen. Das System erstellt beim Training 3D-Modelle der Personen und ist dadurch in der Lage, auch Gesichtsausdrücke der Personen abzubilden, die vorher nicht im Datenbestand gespeichert waren. Basierend auf diesen Modellen wird für jedes Einzelbild des originalen Videos der Ausdruck der originären Person analysiert und dementsprechend wird das Gesicht der anderen Person angepasst und in das Video integriert.[25]

Das Angebot an Software, um qualitativ hochwertige Deepfakes zu erstellen, erhöht sich fortlaufend.[26] Teilweise wird eine leistungsfähige Grafikkarte benötigt, ansonsten liegen aber keine technischen Hindernisse vor – eine Entwicklung ist mittlerweile auf einem handelsüblichen Laptop möglich. Es gibt bereits Anwendungen wie die chinesische App ***ZAO,*** mit der man selbst auf einem Smartphone Deepfakes erzeugen kann – und das mit nur einem Foto und mit einer Schnelligkeit, die selbst Experten überrascht.[27] Häufig sind die Anwendungen frei verfügbar und ermöglichen es

24 Westerlund, The Emergence of Deepfake Technology: A Review, in: Technology Innovation Management Review 9 (11), 39 (41).
25 Wagner/Blewer, "The Word Real Is No Longer Real": Deepfakes, Gender, and the Challenges of AI-Altered Video, in: Open Information Science 3, 32 (36).
26 Eine anschauliche Übersicht der aktuell verfügbaren Software zur Erstellung von Deepfakes findet sich bei Nguyen, Nguyen u.a., Deep Learning for Deepfakes Creation and Detection: A Survey, 1 (3).
27 Der Standard, Zao: Aufregung um neue Deepfake-App, die erschreckend gute Resultate erzeugt, hier abrufbar (Stand: 16.08.2022).

auch Nutzern mit geringen technischen Fähigkeiten, Videos zu erstellen, bei denen die ausgetauschte Person äußerst überzeugend in der Gestik, den Gesichtszügen und der Stimme ist.[28]

IV. Status zur Identifikation von Deepfakes

Weltweit wird nicht nur an der Erstellung, sondern auch an der Identifikation von Deepfakes gearbeitet und geforscht. Allerdings wird das Verhältnis der Anzahl an Personen, die an der Erstellung von Deepfakes arbeiten, gegenüber der Anzahl an Personen, welche an deren Erkennung und Identifizierung arbeiten, als 100 zu eins geschätzt.[29] Ein Experte beschreibt die Situation wie folgt: *„We are witnessing an arms race between digital manipulations and the ability to detect those, and the advancements of AI-based algorithms are catalyzing both sides."*[30]

	2018	2019	2020	2021	2022*
Science Direct	2	2	5	21	28
Scopus	0	27	151	329	212
IEEE Xplore	3	18	82	126	16
JSTOR	3	20	75	21	20
arXiv	4	11	62	97	100

*Stand September 2022

Anzahl wissenschaftlicher Veröffentlichungen über Deepfakes pro Jahr

Im Bereich der digitalen Multimediaforensik wird seit etwa Mitte der 2000er Jahre intensiv geforscht, wie man die Echtheit medialer Inhalte verifizieren kann. Häufig geht es dabei jedoch um vergleichsweise einfache Manipulationen medialer Daten. Die per künstlichen neuronalen Netzen erzeugten Deepfakes stellen eine neue Herausforderung dar, weil sie sich nicht mit bisherigen Methoden identifizieren lassen.[31] Derzeit entsteht ein eigener Forschungszweig, in welchem ebenfalls mithilfe solcher Netze nach Möglichkeiten gesucht wird, Deepfakes zu erkennen. In Tabelle 1 wird die Anzahl relevanter Studien seit 2018 dargestellt, die sich mit dem Thema Deepfakes beschäftigen.[32]

> „We are witnessing an arms race between digital manipulations and the ability to detect those, and the advancements of AI-based algorithms are catalyzing both sides."

Schaut man sich die Zahlen rund um wissenschaftliche Veröffentlichungen zu KI an, so kann bei Deepfakes als Teilanwendungsbereich von KI die Kritik geäußert werden, dass das Thema wissenschaftlich vernachlässigt oder sogar ignoriert wird. Eine der Schwierigkeiten im Bereich Deepfakes ist aus Forschungssicht die schwache Datenlage. Während es für Bildmanipulationen zahlreiche Datensätze gibt, sind größere Deepfake-Datensätze bisher rar. Nennenswert sind bis dato nur zwei Datensätze von ***Google*** und ***Facebook's*** Mutterkonzern ***Meta Platforms***.[33] ***Google*** hat gemeinsam mit der konzerneigenen Tochtergesellschaft ***Jigsaw*** einen

28 Westerlund, The Emergence of Deepfake Technology: A Review, in: Technology Innovation Management Review 9 (11), 39 (40).
29 Galston, Is seeing still believing? The deepfake challenge to truth in politics, hier abrufbar (Stand: 17.08.2022).
30 Hao Li, zitiert nach Knight, Will, A New Deepfake Detection Tool Should Keep World Leaders Safe—for Now, hier abrufbar (Stand: 17.08.2022).
31 Mitra/ Mohanty u.a., A Machine Learning based Approach for DeepFake Detection in Social Media through Key Video Frame Extraction, in: SN Computer Science, 2, 1 (4).
32 Anschauliche Übersichten zu aktuellen Studien finden sich bei: Nguyen/Nguyen u.a., Deep Learning for Deepfakes Creation and Detection: A Survey, 1 (2); Mitra/Mohanty u.a., A Machine Learning based Approach for DeepFake Detection in Social Media through Key Video Frame Extraction, in: SN Computer Science, 2, 1 (9).
33 Mitra/Mohanty u.a., A Machine Learning based Approach for DeepFake Detection in Social Media through Key Video Frame Extraction, in: SN Computer Science, 2, 1 (10).

großen Datensatz an authentischen und manipulierten Videos zusammengestellt.[34] ***Meta Platforms*** hat in Zusammenarbeit mit ***Microsoft*** und mehreren Universitäten aus den USA, dem Vereinigten Königreich, Deutschland und Italien im Jahr 2019 die ***Deepfake-Detection-Challenge*** gestartet und stellte im Rahmen davon einen Datensatz mit über 100.000 Deepfake-Videos bereit. Über 2.000 Forschende reichten ihre Ergebnisse ein, wobei die besten Lösungen circa 80 % der Deepfakes in dem Datensatz identifizieren konnten.[35] Daneben gibt es etliche einzelne Lösungsansätze; einige dieser Ansätze werden im Folgenden kurz vorgestellt.

Auf der ***IEEE Conference on Computer Vision and Pattern Recognition*** stellten ***Agarwal, Farid u.a.*** eine Möglichkeit vor, hochrangige Politiker vor Deepfakes zu schützen.[36] Sie erstellten Pseudo-Modelle über die Art und Weise, wie diese Personen sprechen und erzeugten damit eine Art Fingerabdruck über die individuelle Gestik und Mimik. Grundsätzlich liefert das Modell gute Ergebnisse, die Fehlerrate nimmt allerdings zu, wenn die Person in dem Video nicht direkt in die Kamera blickt. Außerdem ist dieser Detektor nur für Deepfakes von Personen relevant, die besonders schutzwürdige Positionen besetzen. Es fehlen ferner Angaben darüber, wie aufwändig es ist, diese Pseudo-Modelle zu erstellen.[37] ***Microsoft*** stellte im September 2020 seinen ***Video-Authenticator*** vor. Dieser gibt eine Wahrscheinlichkeit an, nach der es sich bei dem vorliegenden Video um künstlich manipulierten Inhalt handelt.

Auch wenn das Thema in der Wissenschaft langsam an Bedeutung zunimmt, wird es politisch bisher noch größtenteils vernachlässigt, obwohl es bereits eine Studie gibt, in der ein politischer Einfluss von Deepfakes nachgewiesen wurde.[38] Innerhalb der ***Europäischen Union*** sind Projekte rund um das Thema Fake News personell stark unterbesetzt und der ***EU*** wird regelmäßig vorgeworfen, dass sie sich zwar mit Fake News beschäftige, aber kaum mit dem Thema Deepfakes.[39] Ein Bericht im Auftrag des ***Europäischen Parlaments*** lässt sich jedoch finden, in welcher der aktuelle Status, die Chancen und Risiken sowie politische Handlungsmöglichkeiten zusammengefasst werden.[40] ***Europol*** hat in einem aktuellen Bericht die Herausforderungen von Deepfakes ausführlich beschrieben. Danach würde der Einsatz von Deepfakes bei Kriminellen immer beliebter. Eines der Ziele sei es dabei, die öffentliche Meinung zu manipulieren und falsche Informationen zu verbreiten.[41] ***Europol*** stellt fest: „***The increase in use of deepfakes will require legislation to set guidelines and enforce compliance***."[42]

34 Dufour/Gully, Contributing Data to Deepfake Detection Research, hier abrufbar (Stand: 18.08.2022).
35 Skibba, Accuracy Eludes Competitors in Facebook Deepfake Detection Challenge, in: Engineering, 6 (12), 1339 (1339-1340).
36 Agarwal/Farid u.a., Detecting Deep-Fake Videos from Appearance and Behavior, in: IEEE International Workshop on Information Forensics and Security (WIFS), New York, 1 (3), hier abrufbar (Stand: 17.08.2022).
37 Solsman, Deepfake Debunking Tool May Protect Presidential Candidates. For Now. Sometimes, hier abrufbar (Stand: 18.08.2022).
38 *Dobber, Metoui u.a.,* Do (Microtargeted) Deepfakes Have Real Effects on Political Attitudes?, The International Journal of Press/Politics, 26 (1), (69–91).
39 *Bressan*, Can the EU Prevent Deepfakes From Threatening Peace?, hier abrufbar (Stand: 18.08.2022).
40 *EPRS (European Parliamentary Research Service), Scientific Foresight Unit (STOA),* "Tackling deepfakes in European policy, hier abrufbar (13.10.2022).
41 Europol, Facing reality? Law enforcement and the challenge of deepfakes. An Observatory Report from the Europol Innovation Lab. Publications Office of the European Union, 1 (10), hier abrufbar (Stand: 16.08.2022).
42 Europol, Facing reality? Law enforcement and the challenge of deepfakes. An Observatory Report from the Europol Innovation Lab. Publications Office of the European Union, 1 (22), hier abrufbar (Stand: 16.08.2022).

C. Deepfakes und Rechtswissenschaften

Die Entwicklung und Verbreitung von immer hochwertigeren Deepfakes führt zwangsläufig zu der Frage, wie das Recht diesem Phänomen begegnen kann. Was ist, wenn Deepfakes eingesetzt werden, um parlamentarische Entscheidungen zu manipulieren oder Wahlen zu beeinflussen, indem man versucht, Politiker zu diskreditieren? Was ist, wenn sie Mittel zum Zweck werden, um Menschen gegeneinander aufzuhetzen oder populistische Strömungen zu verstärken? Ist das Recht für solche Szenarien gewappnet?

I. Gefahren für die Staatssicherheit und die Demokratie

Aktuelle Beispiele zeigen, dass Deepfakes inzwischen zur politischen Destabilisierung und Manipulation der Meinungsbildung eingesetzt werden. Im Russland-Ukraine-Krieg wird derzeit nicht nur mit echten, sondern auch mit medialen Waffen gekämpft. Ende März 2022 tauchte in den sozialen Medien ein Video auf, in dem der ukrainische Präsident ***Wolodymyr Selenskyj*** ukrainische Soldaten dazu aufruft, sich zu ergeben: Der Krieg sei verloren. Das Video ist eine Fälschung, was der ***Facebook***-Konzern ***Meta Platforms*** schnell bemerkte.[43] Selbst wenn das Video nur kurze Zeit online war, dürfte es in der angespannten Kriegssituation für weitere Verunsicherungen bei einigen Ukrainern gesorgt haben.

Auch Wahlen könnten zukünftig durch verfälschte Videos beeinflusst werden. Angenommen, kurz vor einer Wahl taucht ein Deepfake eines Spitzenkandidaten auf, in welchem er sich vermeintlich rassistisch oder sexistisch äußert. Klar ist, dass die Folgen für den Spitzenkandidaten verheerend wären. Eine Rehabilitation innerhalb kürzester Zeit erscheint fast aussichtslos. Zumindest für die betreffende Wahl wäre der Kandidat de facto ausgeschlossen. Deepfakes können damit zu einer großen Bedrohung für die Demokratie und die Gesellschaft werden.

43 Metzger/Schneider, Wie Deepfakes im Ukraine-Krieg genutzt werden, hier abrufbar (Stand: 16.08.2022).

II. Rechtliche Herausforderungen

1. Status Quo: Welche Gesetze finden Anwendung?

Die gesamte Materie der Künstlichen Intelligenz unterliegt bislang noch keinem eigenen Regelungsregime. Daher ist es nicht verwunderlich, dass Deepfakes als spezielle Form von Künstlicher Intelligenz dem deutschen Recht völlig unbekannt sind. Natürlich gibt es Vorschriften im deutschen Recht, die auch ‚Deepfake-Fälle' erfassen. Speziell auf Künstliche Intelligenz und damit auch Deepfakes zugeschnittene Regelungen fehlen jedoch bislang.

Die Bundesregierung hält vor allem die Stärkung der Medienkompetenz, insbesondere der Nachrichten- und der digitalen Informationskompetenz, für entscheidend, um gegen Desinformation im Allgemeinen und Deepfakes im Besonderen gewappnet zu sein.[44] Nationale Gesetze zur Regulierung von Deepfakes scheinen daher nicht geplant zu sein. Problematisch ist dies vor allem für Deepfakes, die zu politischen Zwecken eingesetzt werden. Denn während pornografische und vermögensschädigende Deepfakes unter mehrere Straftatbestände subsumiert werden könnten,[45] ist dies bei politisch motivierten Deepfakes häufig nicht der Fall.

a) § 201a Abs. 2 StGB

In Betracht kommt zunächst § 201a Abs. 2 StGB.

> **§ 201a Abs. 2 StGB:** „Ebenso wird bestraft, wer unbefugt von einer anderen Person eine Bildaufnahme, die geeignet ist, dem Ansehen der abgebildeten Person erheblich zu schaden, einer dritten Person zugänglich macht."

44 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Manuel Höferlin, Frank Sitta, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP – Drs. 19/15210 Beschäftigung der Bundesregierung mit Deepfakes, 5, hier abrufbar (Stand: 23.08.2022).
45 Nähere Ausführungen hierzu in: Lantwin, MMR 2020, 78 ff.

Hier könnte bereits fraglich sein, ob ein Deepfake eine Bildaufnahme im Sinne des § 201a Abs. 2 StGB darstellt. Unter den Begriff der „Bildaufnahme" fallen hauptsächlich Fotos und Videos. Erforderlich ist, dass eine andere Person aufgenommen wird. Daher sind Karikaturen, Zeichnungen oder auch rein computergenerierte Bilder – wie beispielsweise die Fake-Bilder unserer Autorinnen – nicht erfasst.[46] Bei Deepfakes wird eine Person nicht im klassischen Sinne aufgenommen. Ein Deepfake erschafft aber gerade eine solche Bildaufnahme. Denn im Ergebnis erscheint es so, als sei die betroffene Person aufgenommen worden, da Deepfakes es ermöglichen, täuschend echt nie geschehene Sachverhalte zu inszenieren. Da der Gesetzgeber mit der Einführung des § 201a StGB der technischen Entwicklung und der damit einhergehenden Bedrohung des allgemeinen Persönlichkeitsrechts entgegentreten wollte, und ein Deepfake im besonderen Maße eine Gefahr für das von § 201a StGB geschützte Rechtsgut darstellt, wird man Deepfakes daher unter den Begriff subsumieren können. Weiter setzt der Tatbestand eine Ansehensschädigung voraus. Es geht um solche Aufnahmen, welche die abgebildete Person in einer peinlichen, ihre Würde verletzenden Situation zeigen. Im Hinblick auf die Zugänglichmachung von pornografischen Deepfakes wird der Tatbestand regelmäßig zu bejahen sein. Nicht einvernehmlich erstellte pornografische Inhalte dürften geeignet sein, dem Ansehen der abgebildeten Person erheblich zu schaden.[47] Das kann für politische Deepfakes aber nicht so pauschal bejaht werden. Denn nach der Gesetzesbegründung sollen insbesondere Aufnahmen erfasst werden, bei denen nach allgemeiner gesellschaftlicher Bewertung angenommen werden kann, dass ein Interesse daran besteht, die Aufnahmen nicht Dritten zugänglich zu machen.[48] Damit wollte der Gesetzgeber unter anderem ein Signal gegen das immer stärker um sich greifende Cybermobbing setzen und hatte ganz offensichtlich einen anderen Anwendungsfall als politische Deepfakes im Blick.

46 Eisele, in: Schönke/Schröder, Strafgesetzbuch, 30. Aufl. 2019, § 201a Rn. 6.
47 ebd., 79.
48 Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Umsetzung europäischer Vorgaben zum Sexualstrafrecht, BT-Drucks. 18/2601, 37.

Deepfakes, die mit dem Ziel eingesetzt werden, die Meinungsbildung zu beeinflussen oder für politische Unruhen zu sorgen, werden sich daher nur selten unter den Tatbestand subsumieren lassen. Bei dem Deepfake des ukrainischen Präsidenten beispielsweise geht mit der Äußerung, der Krieg sei verloren, keine Ansehensschädigung einher. § 201a Abs. 2 StGB schützt nämlich nicht das Ansehen selbst. *„Denn es gibt […] kein Recht des Einzelnen auf einen bestimmten Grad der Wertschätzung seiner Person durch Dritte."*[49] Gleiches gilt etwa für den vermeintlichen Aufruf, nicht wählen zu gehen. Allein diese Äußerungen zeigen eine Person nicht in einer peinlichen, ihre Würde verletzenden Situation. *„Die Eignung zur Schädigung muss nach dem Wortlaut des § 201a Abs. 2 StGB aber allein aus der Bildaufnahme resultieren; es genügt nicht, dass das Ansehen erst durch die Art und Weise des Zugänglichmachens, etwa durch hämische Kommentare, geschädigt werden kann."*[50] Trotz der Schädigung des politischen Ansehens scheidet in solchen Fällen eine Strafbarkeit nach § 201a Abs. 2 StGB aus. Die politische Integrität und Karriere des Geschädigten werden von § 201a Abs. 2 StGB somit nicht an sich geschützt.

b) §§ 185 ff. StGB

Die Straftatbestände der §§ 185, 186 und 187 StGB bezwecken den Schutz der persönlichen Ehre. Politische Deepfakes enthalten jedoch häufig keine ehrverletzenden Äußerungen, da sie regelmäßig nicht den Zweck verfolgen, einzelne Personen zu diffamieren, sondern vielmehr eine politische Destabilisierung herbeizuführen. Das tatbestandsmäßige Verhalten in § 185 StGB wird als *„Beleidigung"* beschrieben, ohne diesen Begriff näher zu erläutern. Nach ständiger Rechtsprechung des BGH liegt eine solche bei einem Angriff auf die Ehre einer Person durch Kundgabe von Missachtung oder Nichtachtung vor.[51] *„Als Äußerungsdelikt erfordert die Beleidigung also die Kundgabe der ehrverletzenden Tatsachenbehauptung bzw. des herabwürdigenden Werturteils."*[52] Bei politischen Deepfakes, wie dem des ukrainischen

49 Altenhain, in: Matt/Renzikowski, 2. Aufl. 2020, StGB, § 201a Rn. 21.
50 Eisele/Sieber, Strafverteidiger 2015, 312 (315).
51 BGHSt 11, 67; BGHSt 36, 145.
52 Valerius, in: BeckOK, StGB, 52. Ed., § 185 Rn. 17.

Präsidenten, fehlt es an einer solchen Kundgabe. Der Ersteller dieses Deepfakes bringt weder seine Miss- oder Nichtachtung zum Ausdruck, noch nutzt er ihn, um seine Missachtung gegenüber einer anderen Person kundzutun. Vielmehr bezweckt der Täter, den Rezipienten zu täuschen und damit deren Willensbildung zu manipulieren. Ein ehrverletzender Sinn lässt sich der vermeintlichen Äußerung des Präsidenten, die Soldaten sollen ihre Waffen niederlegen, nicht beimessen.

Die Straftatbestände der §§ 186, 187 StGB setzen voraus, dass Tatsachen geäußert werden, die geeignet sind, den Betroffenen verächtlich zu machen oder in der öffentlichen Meinung herabzuwürdigen. Hierbei kann auf die Rechtsprechung zu ‚Fake News' zurückgegriffen werden. Danach ist das ‚In-den-Mund-Legen' von politischen Statements nur dann strafbar, wenn die Zuschreibung des Zitats ehrverletzenden Charakter hat. „*Die bisherige Rechtsprechung deutet darauf hin, dass Äußerungen, die zwar in Teilen der Bevölkerung Empörung gegen den Betroffenen auslösen, aber im Einklang mit der Rechtsordnung stehen, in der Regel nicht die Grenze zur Ehrverletzung überschreiten. Damit ist die Beeinträchtigung etwa der öffentlichen Reputation eines Politikers nicht geschützt – trotz möglicherweise gravierender Schäden für die persönliche politische Karriere oder den Wahlerfolg der betroffenen Partei.*"[53]

> „Für den Wähler ist es aufgrund der Qualität der Deepfakes aber schlicht unmöglich, ein solches Video als Fake zu identifizieren."

53 Hoven/Krause, JuS 2017, 1167 (1169).

c) § 108a StGB

Besonderes Gefahrenpotenzial entfalten Deepfakes kurz vor einer Wahl. Denn hier kann die Manipulation unmittelbar Wirkung entfalten. Sehen Wähler in dieser Situation Deepfakes, wie die von ***Boris Johnsen*** und ***Jeremy Corbyn***[54], in denen die beiden den jeweils anderen als nächsten Premierminister empfehlen, kann sich dies auf die Willensbildung der Wähler auswirken. Sie könnten hierdurch zu einer Wahlentscheidung bewegt werden, welche sie sonst nicht getroffen hätten.

Für den Wähler ist es aufgrund der Qualität der Deepfakes aber schlicht unmöglich, ein solches Video als Fake zu identifizieren. Strafrechtliche Sanktionen für den Ersteller ergeben sich allerdings auch aus § 108a StGB nicht.

Nach § 108a StGB wird bestraft, wer durch Täuschung bewirkt, dass jemand bei der Stimmabgabe über den Inhalt seiner Erklärung irrt oder gegen seinen Willen nicht oder ungültig wählt. § 108a StGB schützt jedoch nur vor einer Täuschung beim Akt der Wahl selbst, das heißt bei der Stimmabgabe.[55] Dadurch wird die Entscheidungsfreiheit des Wählers, nicht aber seine Willensbildungsfreiheit vor Täuschung geschützt. Unwahre Wahlpropaganda wird folglich nicht vom Tatbestand erfasst.[56]

d) Strafrechtliche Nebengesetze

§ 33 Kunsturhebergesetz (KUG) stellt die Verbreitung und öffentliche Zurschaustellung eines Bildnisses entgegen den §§ 22, 23 KUG unter Strafe. Fraglich ist bereits, ob ein Deepfake ein Bildnis in diesem Sinne darstellt. Ein Bildnis im Sinne des KUG ist ein Personenbildnis. Das heißt die Darstellung einer oder mehrerer Personen, welche die äußere Erscheinung der Abgebildeten in einer für Dritte erkennbaren Weise wiedergibt.[57] Schutzgut des KUG ist das Selbstbestimmungsrecht der abgebildeten Person. „*Erfasst werden soll die Freiheit des Menschen, ausschließlich selbst über*

54 Hier abrufbar (Stand: 09.09.22).
55 Kühl, in: Lackner/Kühl, Kommentar zum Strafgesetzbuch, 29. Aufl. , § 108a Rn.1.
56 v. Heintschel-Heinegg, in: BeckOK, StGB, 52. Ed., § 108a Rn. 1.
57 Götting, in: Schricker/Loewenheim, Kommentar zum Urheberrecht, 6. Aufl., § 22 Rn. 14.

sein dem höchstpersönlichen Lebensbereich zuzuordnendes Erscheinungsbild zu bestimmen."[58] Nach Ansicht von ***Hartmann*** soll dem Einzelnen aber kein allgemeines Verfügungsrecht über die eigene Darstellung zustehen. Deepfakes sind aus seiner Sicht „***keine Derivate des Selbstdarstellungsrechts, sondern originäre Fremddarstellung***." Damit unterliegen sie seiner Ansicht nach nicht dem KUG.[59]

„Eine Ausgestaltung als Antragsdelikt ist bei politisch motivierten Deepfakes zudem wenig zweckmäßig."

Soweit man Deepfakes entgegen dieser Ansicht die Eigenschaft als Bildnis zuerkennt, dürfte diese Norm politisch motivierte Deepfakes erfassen. Denn eine Einwilligung in die Verbreitung und öffentliche Zurschaustellung wird regelmäßig nicht vorliegen und eine Ausnahme im Sinne des § 23 KUG dürfte zumindest aufgrund von Abs. 2 ebenfalls zu verneinen sein. Gemäß § 23 Abs. 2 KUG erstreckt sich die Befugnis nämlich nicht auf eine Verbreitung und Schaustellung, durch die ein berechtigtes Interesse des Abgebildeten verletzt wird. So kann insbesondere die Veröffentlichung von manipulierten Aufnahmen unzulässig sein, wenn der Aussagegehalt der Abbildung verfälscht worden ist.[60] „***Insoweit kann es an dem legitimen Informationsinteresse der Öffentlichkeit fehlen, weil unrichtige Informationen grundsätzlich nicht als schützenswertes Gut anzusehen sind***."[61] Die als Antrags- und Privatklagedelikt ausgestaltete Norm hat in der Praxis bislang jedoch so gut wie keine Bedeutung.[62]

58 Herrmann, in: BeckOK, InfoMedienR, 35. Ed., KunstUrhG § 22 Rn. 3.
59 Hartmann, Kommunikation & Recht 2020, 350 (353).
60 BVerfG, NJW 2005, 3271 (3273).
61 LG Frankfurt am Main, ZUM-RD 2020, 329 (335).
62 Specht-Riemenschneider, in: Dreier/Schulze, Kommentar zum Urheberrechtsgesetz, 7. Aufl., KUG, §§ 33-50 Rn. 3.

Der Schutz des KUG kommt zudem nur für solche Deepfakes in Betracht, die uneingeschränkt sichtbar für alle sind. Das heißt nur in solchen Fällen, in denen das Deepfake-Video auf einer öffentlich zugänglichen Plattform hochgeladen wird und damit einem nicht begrenzten Personenkreis zugänglich gemacht wird. Wird das Video hingegen in einer Benutzergruppe geteilt, unterfällt es der Norm nicht. Unsicherheiten bestehen zudem in Hinblick auf den Begriff des Bildnisses. „***Als adäquate Sanktionsfolgen für die Ahndung von Persönlichkeitsrechtsverletzungen eignen sich diese Instrumentarien daher nur teilweise.***"[63]

Im Hinblick auf §§ 106, 108 Urheberrechtsgesetz (UrhG) und § 42 Bundesdatenschutzgesetz (BDSG) dürften politische Deepfakes nicht anders zu behandeln sein als pornografische und vermögensschädigende Deepfakes, sodass eine Strafbarkeit zu bejahen ist. Gerade für politische Deepfakes wird der Ersteller auf fremdes Bild und Videomaterial zurückgreifen müssen, sodass die §§ 106, 108 UrhG einschlägig sind. „***Zudem stellen die Gesichtszüge einer Person personenbezogene Daten i.S.d. Art. 4 Nr. 1 DS-GVO dar, weswegen sich eine Strafbarkeit in Einzelfällen aus Datenschutzstrafrecht ergeben kann.***"[64] Zu beachten ist allerdings, dass insbesondere bei politisch motivierten Deepfakes häufig auf allgemein zugängliches Bildmaterial zurückgegriffen wird, sodass eine Strafbarkeit aus § 42 Abs. 2 Nr. 1 BDSG nur selten in Betracht kommt.

Folglich eignen sich diese Vorschriften aus dem Nebenstrafrecht regelmäßig nicht als Instrumentarien für die Ahndung von Persönlichkeitsrechtsverletzungen zur Verhütung von Manipulation und politischer Destabilisierung. Straftaten aus dem Urheberrecht sind ebenfalls ‚nur' Antragsdelikte, § 109 UrhG. Es sind nur dann Offizialdelikte, wenn gewerbsmäßiges Handeln vorliegt, § 108 a, § 108 b Abs. 2, 3 UrhG. § 42 BDSG ist sogar ein absolutes Antragsdelikt. Damit unterliegen sie einer kurzen Frist im Hinblick auf die Strafantragstellung und ein Strafantrag darf nur von der verletzten Person gestellt werden. Trotz der Gefahren für die Demokratie hat der

63 Heuchemer, in: BeckOK, 52. Ed., Der strafrechtliche Schutz des Persönlichkeitsrechts, StGB, Rn. 18.
64 Insoweit wird auf den bereits zitierten Aufsatz von Lantwin verwiesen.

Staat damit nur sehr eingeschränkt die Möglichkeit, diese Taten zu sanktionieren. Eine Ausgestaltung als Antragsdelikt ist bei politisch motivierten Deepfakes zudem wenig zweckmäßig. Straftatbestände, die sich auf Eingriffe in die Privatsphäre des

§ 106 Abs. 1 UrhG: „Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft."

Verletzten oder Verletzung von Rechtsgütern mit ausgeprägtem Persönlichkeitsbezug beziehen, sind in der Regel als Antragsdelikte ausgestaltet, weil der Verletzte oftmals ein Interesse daran hat, dass der Fall nicht in einem Strafverfahren erörtert wird. Dadurch wird der auf der Tat beruhende Verletzungseffekt häufig nur noch verstärkt.[65] Bei politisch motivierten Deepfakes besteht ein solches Interesse des Verletzten in der Regel jedoch gerade nicht. Solche Deepfakes wurden bereits regelmäßig der breiten Öffentlichkeit zugänglich gemacht. Durch ein anschließendes Strafverfahren kommt es daher nicht mehr zu einer Verstärkung des Verletzungseffekts. Vielmehr wird ein gerichtliches Verfahren die einzige Möglichkeit für die Rehabilitation der Verletzten sein.

2. Mögliche Lösungsansätze

Das vorige Kapitel zeigt, dass für die Zukunft noch Regelungsbedarf für Deepfakes besteht. Allerdings wird eine strafrechtliche Sanktionierung allein nicht ausreichen, um die Erstellung und Verbreitung von Deepfakes zu verhindern. Um den freien Diskurs und die Meinungsbildung zu schützen, sind weitere Maßnahmen erforderlich, die nachfolgend diskutiert werden.Da die Verbreitung von Falschnachrichten in der Regel kein schützenswertes Verhalten darstellt, kommt eine weitergehende Pönalisierung grundsätzlich in Betracht.[66] Vom Schutzbereich des Art. 5 Abs. 1 Satz 1 GG ausgeschlossen sind nach ständiger Rechtsprechung[67] bewusst unwahre Tatsachenbehauptungen („***bewusste Lüge***") und solche, deren Unwahrheit bereits im Zeitpunkt der Äußerung unzweifelhaft feststeht.[68] Dennoch ist es für den Gesetzgeber eine schmale Gratwanderung zwischen rechtsstaatlicher Selbstbehauptung und totalitären Tendenzen. Es wird nur schwer möglich sein, den gesamten öffentlichen Meinungsbildungsprozess zu schützen, ohne den Bürger in seiner Meinungsfreiheit einzuschränken. Im Hinblick auf den Schutz des staatlichen Willensbildungsprozesses könnte aber der Vorschlag von ***Mafi-Gudarzi*** ein geeignetes Mittel darstellen.[69] So wäre eine Ergänzung von § 108a StGB (Wählertäuschung) oder die Schaffung eines neuen § 108f StGB in Bezug auf die Verbreitung falscher Tatsachen, die geeignet sind, den Wählerwillen zu beeinflussen, zu erwägen.[70]

> „Dennoch ist es für den Gesetzgeber eine schmale Gratwanderung zwischen rechtsstaatlicher Selbstbehauptung und totalitären Tendenzen."

In der ***Europäischen Union*** wird ebenfalls nicht über ein Verbot nachgedacht. Der Vorschlag der EU-Kommission zur ***Festlegung harmonisierter Vorschriften für***

65 Mitsch, JA 2014, 1 (2).

66 Mafi-Gudarzi, ZRP 2019, 65 (67).
67 BVerfGE 61, 1 (8); 99, 185 (197).
68 Holznagel, MMR 2018, 18 (20).
69 Mafi-Gudarzi, ZRP 2019, 65 (68).
70 Mafi-Gudarzi verweist diesbezüglich auf § 264 Abs.1 des österreichischen StGB gegen die Verbreitung falscher Nachrichten bei Wahlen: „Wer öffentlich eine falsche Nachricht über einen Umstand, der geeignet ist, Wahl- oder Stimmberechtigte von der Stimmabgabe abzuhalten oder zur Ausübung des Wahl- oder Stimmrechts in einem bestimmten Sinn zu veranlassen, zu einer Zeit verbreitet, da eine Gegenäußerung nicht mehr wirksam verbreitet werden kann, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen."

Künstliche Intelligenz sieht für den Einsatz von Deepfakes sogar nur minimale Transparenzpflichten vor.[71] Der Ersteller des Deepfakes muss lediglich darauf hinweisen, dass es sich um ein Deepfake handelt. Vielversprechender erscheint da der ***Gestärkte Verhaltenskodex für Desinformation***.[72] Vertreter von Online-Plattformen, führenden Technologieunternehmen und Akteuren der Werbebranche haben sich erstmals weltweit und auf freiwilliger Basis auf Selbstregulierungsstandards zur Bekämpfung von Desinformation geeinigt. Unterzeichner des Kodex müssen danach Maßnahmen zur Eindämmung von Desinformation ergreifen. Der Verhaltenskodex erfasst explizit auch neue manipulative Verhaltensweisen wie Deepfakes. Der ***Verhaltenskodex für Desinformation*** soll mit dem ***Gesetz über digitale Dienste*** (***Digital Services Act***)[73] verknüpft werden. Unternehmen, die ihren Verpflichtungen im Rahmen des aktualisierten Kodex nicht nachkommen, müssten dann mit Geldstrafen von bis zu 6 % ihres weltweiten Umsatzes rechnen.

Eine weitere Idee wäre, die Verbreitung von Deepfakes mit technologischen Mitteln einzuschränken, etwa durch effektive Erkennungsprogramme, welche manipulierte Videos identifizieren und diese sichtbar als solche markieren. Wie jedoch bereits in Kapitel B. IV. angesprochen, liefern sich die Entwickler von Deepfakes mit denen, die an deren Identifizierung forschen, ein unausgeglichenes Wettrennen, bei dem Erstere klar im Vorsprung sind. Der KI-Forscher und Unternehmer ***Hao Li*** geht davon aus, dass man zeitnah in der Lage sein wird Deepfakes zu erzeugen, die weder von Menschen noch von Maschinen erkannt werden können.[74] ***David Doermann***, Professor für Medienforensik an der ***Buffalo Universität***, bezeichnet die Entwicklung als „***cat-and-mouse game***".[75] Dies hat zur Folge, dass aktuelle Lösungen zur Identifikation von Deepfakes mittelfristig weniger zuverlässig sind. Da es sich bei Deepfakes um ein verhältnismäßig neues Phänomen handelt, gibt es viele Menschen, denen diese Technik noch völlig unbekannt ist. Eine Stärkung der Medienkompetenz – insbesondere mit Blick auf die kritische Reflektion von Online-Informationen und der Erkennung von manipulierten Videos – ist zwar keine rechtliche Lösung, kann jedoch dazu beitragen, den möglichen Schaden von Deepfakes zu begrenzen.

„Deepfakes haben ein beispielloses Potenzial zu manipulieren, da sie erfundene Informationen leicht mit Autoritätsquellen kombinieren können."

D. Ausblick

Deepfakes haben ein beispielloses Potenzial zu manipulieren, da sie erfundene Erzählungen und Informationen leicht mit Autoritätsquellen kombinieren können. Das macht die Enttarnung der Fehlinformation für den Rezipienten sehr schwer. Zugleich vermuten die wenigstens Menschen bei der Betrachtung eines Videos eine Falschmeldung. Videos und Audioaufnahmen halten die meisten Menschen noch immer für manipulationsfest und erkennen sie als unumstößliche Beweise an.

Neben dem großen Potenzial für Falschinformationen besteht zudem die Gefahr, dass die Menschen das Interesse an der Wahrheit verlieren. Menschen bevorzugen als Quelle der Gewissheit das, was sie selbst gesehen haben vor dem, was sie bloß von anderen gehört oder irgendwo gelesen haben.[76] Dieses Vertrauen kann

71 Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz, Titel IV, KOM(2021)206 final, hier abrufbar (Stand: 01.08.2022).
72 The Strengthened Code of Practice on Disinformation 2022, hier abrufbar (Stand: 17.08.2022).
73 Mehr Informationen hier abrufbar (Stand: 18.08.2022); Duda, Der Digital Services Act – EU zwischen Innovation und Informationskrise, CTRL 2/22, 10 ff.
74 Laaff, Deepfakes: Hello, Adele – bist du's wirklich?, hier abrufbar (Stand: 18.08.2022).
75 Solsman, Deepfake Debunking Tool May Protect Presidential Candidates. For Now. Sometimes, hier abrufbar (Stand: 18.08.2022).
76 Rini, Deepfakes Are Coming. We Can No Longer Believe What We See., hier abrufbar (Stand: 17.10.2022).

durch Deepfakes stark erschüttert werden. Dies werden sich Menschen in Zukunft vermutlich zunutze machen. Es ist damit zu rechnen, dass bei Gerichtsverfahren immer häufiger der Einwand erhoben wird, die vorgelegte Video-, Bild- oder Tondatei sei ein Deepfake . Bei entsprechend substantiierten Vortrag wird regelmäßig die Bestellung eines Sachverständigen (mit entsprechender Expertise) erforderlich sein.[77]

Um den Gefahren, die mit der Verwendung von Deepfakes einhergehen, in Zukunft Einhalt gebieten zu können, ist es wichtig, dass dieses Thema mehr in den Fokus politischer Aufmerksamkeit gerückt wird. Die Verwendung von Deepfakes wird zunehmen; vor allem im politischen Kontext. Hierauf müssen sich auch die Bürger, die Plattformen und der Gesetzgeber einstellen. Die rasante Entwicklung von Deepfake-Software darf nicht unterschätzt werden. Der Gesetzgeber muss sich überlegen, wie er diese Technologie regulieren will. Bislang ist er überwiegend untätig geblieben, doch damit wird sich das Problem der missbräuchlichen Verwendung von Deepfakes sicher nicht in den Griff bekommen lassen. Begrüßenswert ist, dass das Thema Deepfakes bei der Frühjahrskonferenz der Justizminister im Juni 2021 auf der Tagesordnung stand. Es bleibt abzuwarten, ob der Vorschlag des bayerischen Justizministers zur Schaffung einer Regelung in einem neuen § 141 des StGB bei der Bundesjustizministerin Gehör finden wird.[78]

Eva ist wissenschaftliche Mitarbeiterin am Lorenz-von-Stein-Institut für Verwaltungswissenschaften an der CAU Kiel (gf.) und am Institut für Multimediale und Interaktive Systeme an der Universität zu Lübeck. Sie beschäftigt sich vor allem mit der Wirkung neuer Technologien auf das Recht und die Gesellschaft.

Anna ist wissenschaftliche Mitarbeiterin am Institut für Multimediale und Interaktive Systeme an der Universität zu Lübeck. In ihrer Forschung beschäftigt sie sich mit dem Einsatz von intelligenten Systemen für Richterinnen und Richter im Strafprozess.

77 Kuhlmann, Realität, Fiktion und das Problem, sie vor Gericht zu kriegen, hier abrufbar (01.09.22).
78 Pressemitteilung der Bayerischen Staatsregierung vom 16. Juni 2021, hier abrufbar (Stand: 01.08.2022).

Folge 25

Künstliche Intelligenz – was ist das eigentlich, Manuela Lenzen?

Folge 28

Regulierung & Innovation – wie lässt sich beides vereinbaren, Martin Ebers?

Folge 40

CTRL-KI als Rechtssubjekt, Transitional Justice & Legal Tech und das Internet der Dinge – Was ist die Cologne Technology Review & Law?

Zurück zum Inhaltsverzeichnis

Aufsatz

Der DSA auf dem Prüfstand – Zwischen Grundrechten und Regulierung

Alexander Niebler und Sofian Djebbari

Open Peer Review

Dieser Beitrag wurde lektoriert von:
Hendrik Eppelmann & Lea Heyder

Alexander ist wissenschaftliche Hilfskraft am Institut für Öffentliches-, Völker- und Europarecht von Professor Daniel Erasmus-Khan an der Universität der Bundeswehr München. Er hat im Juli 2021 in Frankreich die Licence en droit abgelegt.

Sofian ist wissenschaftliche Hilfskraft am Max-Planck-Institut für Innovation und Wettbewerb sowie studentische Hilfskraft am Lehrstuhl für Privates, Europäisches und Internationales Wirtschaftsrecht an der LMU München. Er hat im Juli 2021 in Frankreich die Licence en droit abgelegt.

Am 28.10.2022, einen Tag nachdem der Gründer und CEO von ***Tesla***, ***Elon Musk***, den Kurznachrichtendienst ***Twitter*** endgültig erworben hatte, twitterte dieser – in Anspielung an das Logo des Unternehmens – dass der „***Vogel befreit wurde***“.[1] Der europäische Kommissar für den Binnenmarkt, ***Thierry Breton***, reagierte schnell und antwortete in einem „***Retweet***“, dass „***in Europa der Vogel nach den europäischen Regeln fliegen wird***“.[2]

1 Hier abrufbar (Stand: 10.11.2022).
2 Hier abrufbar (Stand: 10.11.2022).

Der ***EU***-Kommissar spielt damit auf den Versuch der ***Europäischen Union*** an, den großen Digitalunternehmen mit europäischer Regulierung entgegenzutreten und illegalen Aktivitäten, die in der analogen Welt strafbar sind, auch in der digitalen Welt einen Riegel vorzuschieben.[3]

Die ***Europäische Union*** hat sich mit der europäischen Digitalstrategie zum Ziel gesetzt, der fortschreitenden Digitalisierung regulatorisch entgegenzutreten. Im Mittelpunkt stehen dabei zwei Legislativpakete, welche die ***Europäische Kommission*** am 15. Dezember 2020 vorgestellt hat: der Digital Markets Act (im Folgenden DMA)[4] und der Digital Services Act (nachfolgend DSA)[5]. Während der DMA die Regulierung spezifischer Verhaltensformen von sogenannten ***Gatekeepern*** vorsieht[6], möchte der DSA Anbieter digitaler Dienste wegen illegaler Inhalte stärker in die Verantwortung nehmen.[7] Damit geht die Verordnung deutlich über die 20 Jahre alte E-Commerce-Richtlinie (ECRL) hinaus.[8]

1996 haben die ***Vereinigten Staaten von Amerika*** mit Section 230 des Communication Decency Acts einen Rechtsakt erlassen, der als ***Magna Charta*** des Internets gilt.[9] Das dort kodifizierte Haftungsprivileg für Plattformbetreiber[10] wurde nicht nur in Art. 14 der E-Commerce-Richtlinie übernommen, sondern steht auch weiterhin im Mittelpunkt der Regulierung des DSA.[11]

> Art. 14 I E-Commerce-Richtlinie: „Die Mitgliedstaaten stellen sicher, dass im Fall eines Dienstes der Informationsgesellschaft, der in der Speicherung von durch einen Nutzer eingegebenen Informationen besteht, der Diensteanbieter nicht für die im Auftrag eines Nutzers gespeicherten Informationen verantwortlich ist, sofern folgende Voraussetzungen erfüllt sind […].“

Das Ziel des DSA ist es, ein „***level playing field***“ der Mitgliedstaaten im Digitalmarkt zu schaffen und damit die nationalen Abweichungen der E-Commerce-RL zu harmonisieren.[12] Es sollen um diese ***Magna Charta*** der Digitalwirtschaft herum neue, fundamentale Regelungen eingeführt werden, deren Ausmaß für manche Autoren bereits als ***„Grundgesetz“*** der Digitalwirtschaft bezeichnet werden.[13]

In diesem Beitrag wird zunächst eine Positionierung des DSA in der Digitalstrategie der EU vorgenommen (Kapitel A) bevor auf den persönlichen Anwendungsbereich eingegangen wird (Kapitel B). Dann werden die neuen Regelungsinhalte sowie deren Vollziehbarkeit vertieft dargestellt (Kapitel C). Abschließend wird die Durchsetzung des neuen Gesetzes aus rechtspolitischer Sicht analysiert (Kapitel D).

Zum DSA wurden durch den Bericht des ***Ausschusses für Binnenmarkt und Verbraucherschutz*** im ***Europäischen Parlament*** (***„DSA-E-Schaldemose“***) vom 20.12.2021 wichtige Änderungsvorschläge formuliert. Am 22.04.2022 haben sich ***Rat***, ***Europäisches Parlament*** und ***Europäische Kommission*** im Rahmen des fünften Trilogs über den DSA auf eine vorläufig endgültige Fassung. Das ***Europäische Parlament*** hat in erster Lesung am 05.07.2022 seinen Standpunkt verabschiedet. Der ***Rat*** hat am 04.10.2022 den Entwurf final erörtert. Am 19.10.2022 wurde der DSA im Amtsblatt der Europäischen Union veröffentlicht. Bereits zum 16.11.2022 traten erste

3 Mitteilung der Kommission, KOM(2020) 67 endgültig, 11; Mitteilung der Kommission, Digitaler Kompass 2030: der europäische Weg in die digitale Dekade, KOM (2021) 118 endgültig/2 vom 9.3.2021, 15; siehe ErwGr. 3, 27 ff., 57 DSA.
4 Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte).
5 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), im Folgenden DSA.
6 Eppelmann, CTRL 2/21, 123 ff.
7 *Duda*, CTRL 2/2022, 10 ff.; *Gielen/Uphues*, EuZW 2021, 627 (632).
8 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 (Richtlinie über den elektronischen Geschäftsverkehr); *Schmid/Grewe*, MMR 2021, 279; *Berberich/Seip*, GRUR-Prax 2021, 4.
9 *Langvardt* 106 Geo. L. J. 2018, 1353 (1373); *Gielen/Uphues*, EuZW 2021, 627 (632).
10 *„No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.“*
11 *Gielen/Uphues*, EuZW 2021, 627 (632).
12 ErwGr. 7 DSA; *Berberich/Seip*, GRUR-Prax 2021, 4.
13 *Schmid/Grewe*, MMR 2021, 279.

Inhalte der Verordnung in Kraft, der Großteil der Regelungen wird jedoch erst ab dem 17.02.2024 anwendbar sein.[14] Die publizierte Verordnung bildet die Grundlage für die Bearbeitung des vorliegenden Beitrags.[15]

A. Der DSA als Teil der Digitalstrategie der EU

Zu Beginn ihrer Amtszeit betonte Kommissionspräsidentin ***Ursula von der Leyen***, dass Europa auf dem Weg in eine neue digitale Welt international die Führungsrolle übernehmen müsse und erklärte die Digitalpolitik zu einer Priorität ihrer Amtszeit.[16] Dazu präsentierte die ***Kommission*** am 09.03.2021 ein allumfassendes digitalpolitisches Programm; den ***digitalen Kompass***.[17] In diesem formuliert die ***Kommission*** ihre Zielvorstellung für den digitalen Wandel in Europa bis 2030 und benennt konkrete Ziele in den Bereichen digitale Kompetenzen, Aufbau digitaler Infrastrukturen, Digitalisierung der Unternehmen und Digitalisierung öffentlicher Dienste.[18] Dieses Programm wurde mit leichten Änderungen in Form eines Beschlusses des Parlaments und des Rates am 14.12.2022 verabschiedet.[19]

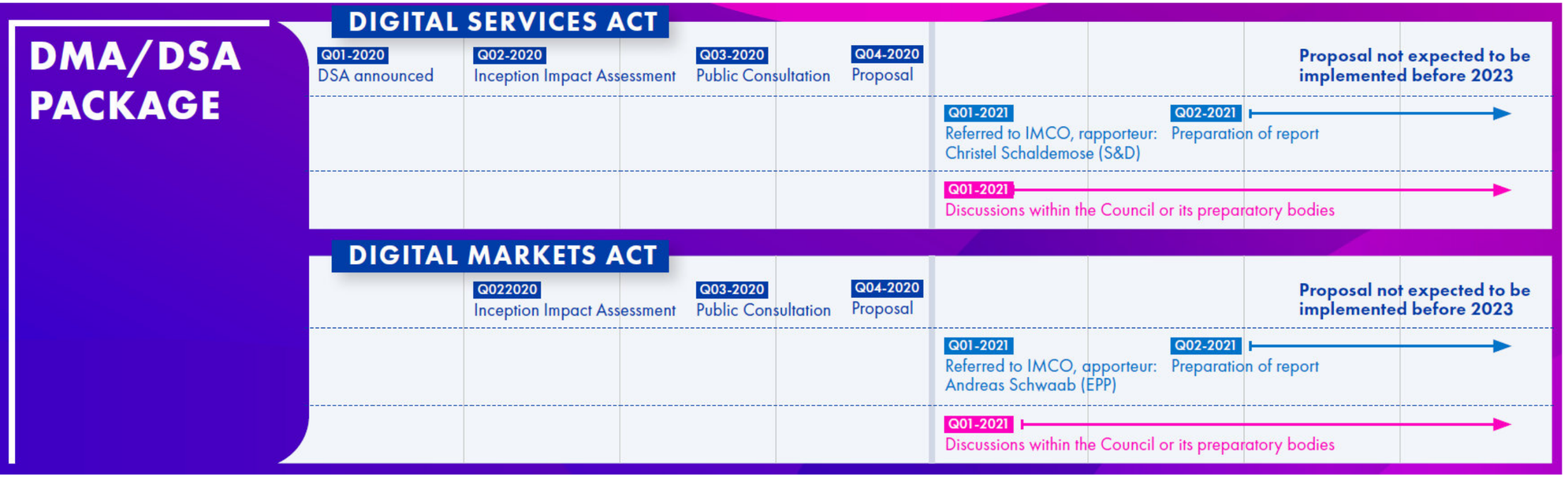
Auf der gesetzgeberischen Ebene hat die ***Kommission*** am 19.02.2020 eine Strategie zur Gestaltung der digitalen Zukunft Europas vorgelegt.[20] Dieses Konzept der ***EU*** stützt sich auf drei Säulen und möchte mit der Digitalstrategie auf Technologie im Dienste der Menschen (1), eine faire und wettbewerbsfähige digitale Wirtschaft (2) und eine offene, demokratische und nachhaltige Gesellschaft (3) hinarbeiten.[21] Der DSA ist inhaltlich zu großen Teilen der dritten Säule zuzuordnen und stellt eine von mehreren Schlüsselmaßnahmen dar, mit welchen die ***Kommission*** europäische Werte und ethische Regeln sowie die sozialen und ökologischen Standards auch im digitalen Raum durchsetzen möchte.[22] Das erklärte Regelungsziel des DSA ist gemäß den Erwägungsgründen 1, 3, 4 und 9 die Wahrung der in der Charta garantierten Grundrechte und eines funktionierenden Binnenmarkts im Online-Umfeld sicherzustellen.

> Erwägungsgrund 3 des DSA [paraphrasiert]: „Damit das Online-Umfeld sicher, berechenbar und vertrauenswürdig ist und Bürger der Union die ihnen in der Charta der Grundrechte der Europäischen Union garantierten Grundrechte ausüben können, insbesondere das Recht auf Meinungs- und Informationsfreiheit und die Erreichung eines hohen Verbraucherschutzniveaus, ist unbedingt ein verantwortungsvolles Verhalten der Anbieter von Vermittlungsdiensten erforderlich."

Erwähnenswert in diesem Zusammenhang ist neben dem DSA insbesondere die europäische Datenstrategie, die ebenfalls am 19.02.2020 veröffentlicht wurde und sich zum Ziel gesetzt hat, Europa eine globale Führungsrolle in der von Daten geprägten Wirtschaft zu verschaffen.[23] Als Kernmaßnahmen der Datenstrategie hat die Kommission am 25.11.2020 einen Vorschlag für den Data-Governance-Act vorgelegt, der am 16.05.2022 final vom Rat beschlossen wurde.[24] Der Rechtsakt schafft Regeln für die erleichterte Wiederverwendung und Teilung geschützter Daten des öffentlichen Sektors.[25] Am 23.02.2020 hat die ***Kommission*** ferner einen Vorschlag für eine Richtlinie über harmonisierte Regeln zum gerechten Zugang und Nutzen von Daten (Data Act) vorgelegt, der aktuell vom Rat und zukünftig vom Parlament diskutiert wird.[26]

14 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste). In: Amtsblatt der Europäischen Union. L 277, 27. Oktober 2022, S. 1–102, Art. 93 Abs. 2 S. 2 DSA.
15 Alle nicht anderweitig benannten ErwGr. und Artikel sind solche des DSA–E.
16 Politische Leitlinien für die künftige Europäische Kommission 2019–2024, hier abrufbar (Stand: 02.06.2022).
17 Mitteilung der Kommission, Digitaler Kompass 2030: der europäische Weg in die digitale Dekade, KOM (2021) 118 endgültig vom 09.03.2021; Vorschlag für einen Beschluss des Europäischen Parlaments und des Rates über das Politikprogramm für 2030 „Weg in die digitale Dekade", KOM (2021) 574 endgültig.
18 Beschluss (EU) 2022/2481 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Aufstellung des Politikprogramms 2030 für die digitale Dekade.
19 Hier abrufbar (Stand: 31.12.2022).
20 Mitteilung der Kommission, KOM(2020) 67 endgültig.
21 Ebd., 2.
22 Ebd., 11.
23 Mitteilung der Kommission, Eine europäische Datenstrategie, KOM(2020) 66 endgültig.
24 Verordnung über europäische Daten-Governance und die Anpassung der Verordnung (EU) 2018/1724 (*Data Governance Act*).
25 Rat der Europäischen Union, Pressemitteilung vom 16. Mai 2022, 441/22 ; *Eppelmann*, CTRL 2/21, 123 ff.
26 Vorschlag für eine Richtlinie über harmonisierte Regeln zum gerechten Zugang und Nutzen von Daten (*Data Act*), KOM(2022) 68 endgültig.

Die Vielzahl der genannten Rechtsakte, insbesondere hinsichtlich ihrer Parallelität zum DMA sowie der Umstand, dass – wie Erwägungsgründe 10 ff. und Art. 2 II, III DSA explizit normieren – der DSA andere Rechtsakte der Union als ***lex specialis*** unberührt lassen soll, macht eine genaue Eingrenzung des persönlichen Anwendungsbereichs des DSA notwendig.



Quelle: EU-Komission

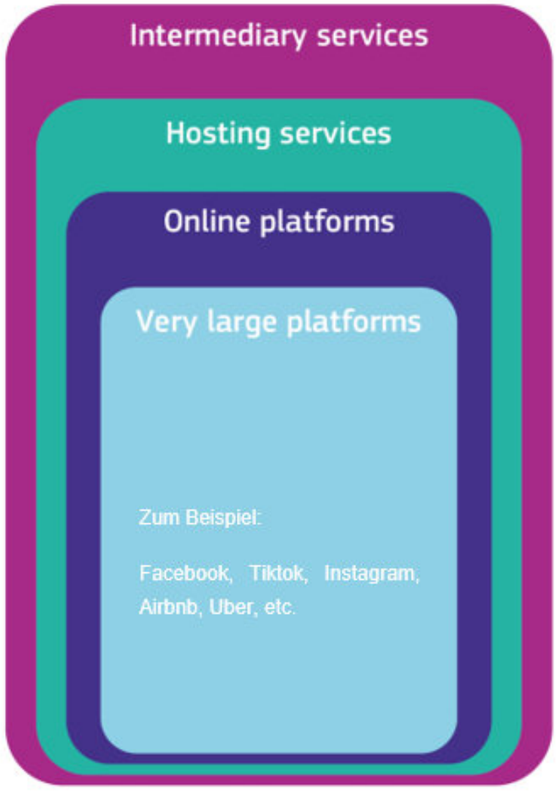
B. Der Begriff der Anbieter digitaler Dienste im DSA-E

Gemäß Art. 2 I gilt die Verordnung grundsätzlich für alle Vermittlungsdienste, die für Nutzer angeboten werden, welche ihre Niederlassung in der EU haben. Dabei ist der Niederlassungsort des Dienstanbieters grundsätzlich unbeachtlich.[27] Der Oberbegriff der Vermittlungsdienste wird in Art. 3 g) näher beschrieben. Dieser definiert Vermittlungsdienste als kommerzielle, in der Regel gegen Entgelt erbrachte Dienstleistungen der Informationsgesellschaft, die in Form der ***„reinen Durchleitung"*** (Art. 3 g) i)), der ***„Caching"***-Leistung (Art. 3 g) ii)) oder in Form von ***„Hosting"***-Diensten erbracht werden können.[28] Insbesondere mit Blick auf die systematisch abgestufte Regulierung des DSA, die neben allgemeinen Regelungen für alle Vermittlungsdienste auch zusätzliche besondere Regelungen für ***„Host-Provider"*** und ***„Online-Plattformen"***, sowie ***„sehr große Online-Plattformen"*** vorsieht, ist eine Abgrenzung dieser vier Adressatenkategorien erforderlich.[29] Um das Verhältnis der vier Begriffe ***„Vermittlungsdienste"***, ***„Host-Provider"*** und ***„Online-Plattformen"*** bzw. ***„sehr große Online-Plattformen"*** untereinander zu verdeutlichen, ist der bildliche Vergleich zur Matroschka-Puppe hilfreich[30]: Der DSA sieht die Kategorie der ***„Vermittlungsdienste"*** als Überbegriff an, zu dem unter anderem auch ***„Host-Provider"*** gehören und gemäß Art. 3 i) sind ***„Online-Plattformen"*** wiederum als Unterkategorie von ***„Host-Providern"*** zu qualifizieren. Für die Kategorie der „Online-Plattformen" sieht die abgestufte Regulierung des DSA dann zuletzt noch besondere Vorschriften für sogenannte ***„besonders große Online-Plattformen"*** vor. Das heißt, der Begriff der ***„Vermittlungsdienste"*** umfasst noch die meisten Dienstleister, während die Kategorie ***„besonders große Online-Plattformen"*** die wenigsten Dienstleister betrifft (zur visuellen Darstellung der Begriffe vgl. Abbildung 2).

27 *Raue/Heesen*, NJW 2022, 3537 (3538).

28 *Spindler*, GRUR 2021, 545 (547); ErwGr. 5.
29 Vgl. *Schmidt/Grewe*, MMR 2021, 279 (279).
30 Vgl. *Gielen/Uphues*, EuZW 2021, 627 (634).

Als „*Host-Provide*r“ definiert Art. 3 g) iii) einen Dienst der Informationsgesellschaft, der darin besteht, die von einem Nutzer bereitgestellten Informationen in dessen Auftrag zu speichern. Es handelt sich somit regelmäßig um Plattformen, auf denen Nutzer ihre Inhalte hochladen, speichern und der Öffentlichkeit zur Verfügung stellen können, wobei die Inhalte in Abgrenzung zu den sogenannten „*Access-Providern*“ nicht nur ‚durchgeleitet‘ werden.[31] Bedeutsam ist dabei, dass es sich bei den Inhalten nicht um eigene Inhalte der Dienstleister handelt, sondern um die der Nutzer und es aus Sicht des „*Host-Provide*r“ also fremde Drittinhalte sind.[32]



Der Zusammenhang zwischen den Begriffsdefinitionen im DSA (Quelle: EU-Komission)

Gemäß Art. 3 i) sind „*Online-Plattformen*“ eine Unterkategorie von „*Host-Providern*“, die im Auftrag eines Nutzers Informationen speichern und öffentlich verbreiten; etwa Online-Marktplätze oder soziale Netzwerke.[33] Mit Blick auf das Merkmal der erforderlichen öffentlichen Verbreitung der Inhalte, stellt sich die Frage, ob Messenger-Dienste wie *WhatsApp* und *Telegram* als „*Online-Plattformen*“ im Sinne des DSA qualifiziert werden können oder vom Anwendungsbereich ausgenommen werden.

Denn diese Messenger stellen die Nachrichten der Nutzer nur einem Kontakt oder einer bestimmten Anzahl von Kontakten in Gruppenchats zur Verfügung. Art. 3 k) definiert die „*öffentliche Verbreitung*“ als Bereitstellung der Informationen für eine potenziell unbegrenzte Zahl von Dritten im Auftrag des Nutzers. Damit sind beispielsweise klassische Sprachanrufe, E-Mails oder Privat- bzw. Gruppenchats grundsätzlich nicht erfasst, da die relevanten Informationen nur an bestimmte Dritte bereitgestellt werden.[34] Anders sind jedoch solche Messenger-Dienste und Gruppenchats zu behandeln, bei denen die Anzahl der Gruppenteilnehmer unbegrenzt ist und für mögliche neue Nutzer keine Zutrittshindernisse bestehen, also sogenannte „*öffentliche Gruppen*“ oder „*offene Kanäle*“.[35] In diesen Fällen, in denen der Absender den Empfängerkreis nicht vorab konkret bestimmt hat, kann wieder von einer „*öffentlichen Bereitstellung*“ ausgegangen werden und der entsprechende Dienst unterliegt erneut dem Anwendungsbereich des DSA.[36] Zuletzt ist noch auf die vierte und restriktivste Unterkategorie der „*sehr großen Online-Plattformen*“ hinzuweisen. Gemäß Art. 33 I sind Online-Plattformen mit einer durchschnittlichen monatlichen Anzahl von mindestens 45 Mio. Nutzern in der *EU* als „*sehr große Online-Plattformen*“ einzustufen, für die der DSA-E noch weitere, spezifischere Regulierungen vorsieht.

C. Die gestufte Regulierungsregime des DSA aus rechtsökonomischer Sicht

Der DSA sieht in Fortführung der Grundentscheidung aus der ECRL ein allgemeines Haftungsregime sowie hinsichtlich des dargestellten Definitionsmodells (vgl. Kapitel B und Abbildung 2) ein abgestuftes Modell der Regulierung vor.[37]

I. Beibehaltung der alten Haftungsregelungen

Im ersten Abschnitt des DSA (insb. Art. 4 bis 10) werden beinahe identisch die Haftungsprivilegierungen der Art. 12 bis 15 ECRL übernommen, welche für alle Vermittlungsdienste i.S.d. Art. 3 g – also Access- und Host-Provider sowie Caching-Dien-

31 Hier abrufbar (Stand: 30.12.2022).
32 Ebd.
33 Vgl. *Gielen/Uphues*, EuZW 2021, 627 (634).
34 Vgl. ebd., 634.
35 Erwägungsgrund. 14.
36 Vgl. *Gielen/Uphues*, EuZW 2021, 627 (634).
37 *Duda*, CTRL 2/2022, 10 (12 ff.); *Berberich/Seip*, GRUR-Prax 2021, 4.

ste – gelten. Hierbei handelt es sich um die Übermittlung oder Abrufung der von Nutzern bereitgestellten Informationen, also fremder Inhalte.[38] Für diese Nutzer-Inhalte soll der Diensteanbieter grundsätzlich nicht haften. Eine Ausnahme hiervon gilt gem. Art. 6 III für Host-Provider, wenn aus Sicht eines Verbrauchers der Eindruck entsteht, dass die angebotene Information als Leistung vom Host-Provider selbst oder ihm unterstellten Nutzern bereitgestellt wird.[39] Dies erinnert an die vom EuGH entwickelte Rechtsprechung der ***„aktiven Rolle***, nach welcher eine Haftung des Host-Providers dann geboten ist, wenn er sich nicht darauf beschränkt, die Dienstleistungen auf neutrale Weise und durch die bloße technische und automatische Verarbeitung der vom Nutzer bereitgestellten Informationen zu erbringen, sondern vielmehr eine ***„aktive Rolle***" einnimmt.[40] Dies wirft jedoch die Frage nach der Reichweite der Ausnahme, insbesondere außerhalb des Verbrauchsgüterrechts, auf.[41] Neu ist ebenso Art. 7, demzufolge freiwillige Untersuchungen zur Erkennung und Entfernung rechtswidriger Inhalte die Privilegierungen der Art. 4 ff. nicht entfallen lassen.[42] Wenn ein Vermittlungsdienstleister ohne rechtliche Verpflichtung solche Maßnahmen anwendet, dann soll er nicht schlechter stehen als ein Dienstleister, der dies unterlässt.

II. Regelung des Umgangs mit rechtswidrigen Inhalten

Neuland betritt der DSA durch Auflagen zum Vorgehen gegen rechtswidrige Inhalte nach Art. 9 f. Wie Art. 8 klarstellt, wird es keine allgemeine Pflicht zur Überwachung der übermittelten Informationen auf rechtswidrige Inhalte geben. Jedoch haben Vermittlungsdienste neuerdings auf Grundlage einer behördlichen Anordnung gegen rechtswidrige Inhalte vorzugehen und darüber Auskunft zu geben (Art. 9, 10). Solche Inhalte sind gem. Art. 3 h alle Informationen, die nicht im Einklang mit Unionsrecht sowie mitgliedstaatlichem Recht stehen.[43] Bemerkenswert ist hierbei zunächst, dass die Einordnung, welche Inhalte rechtswidrig sind, ohne Differenzierung erfolgt und in großem Maße an die Mitgliedstaaten abgegeben wird.[44] Aus deutscher Sicht ist anzumerken, dass diese Definition deutlich über § 1 Abs. 3 NetzDG hinausgeht, welche sich nur auf strafbare Inhalte bezieht.[45] Jedoch werden damit schädliche Inhalte, mithin Desinformationen, sofern diese nicht rechtswidrig sind, nicht erfasst. [46] Hierbei wird auch weiterhin ein Selbstregulierungsansatz der Plattformen verfolgt.[47]

> „Wie Art. 8 DSA klarstellt, wird es grds. keine allgemeine Pflicht zur Überwachung der Nutzer-Informationen auf rechtswidrige Inhalte geben."

Die Transparenzregeln der Art. 11 ff. sollen zukünftig die Kommunikation zwischen den Behörden und den Dienstanbietern durch Einrichtung von „single ***points of contact***" erleichtern (Art. 11, 12). Anbieter von Vermittlungsdiensten haben bei fehlender Niederlassung in der Union einen rechtlichen Vertreter zu benennen, der für Pflichtverstöße gegen den DSA unmittelbar haftet (Art. 13 III).[48] Intermediäre haben nach Art. 15 ferner jährliche Transparenzberichte mit Informationen über gelöschte und gesperrte Inhalte zu veröffentlichen. Interessant ist, dass diese Regelungen, im Unterschied zu den weitreichenderen Verpflichtungen für ***sehr große Online-Plattformen*** und ***Suchmaschinen***, keine Regelungen zur Vereinbarkeit dieser Offenlegungspflichten mit der Wahrung von Geschäftsgeheimnissen vorsehen.[49]

38 Ebd.
39 *Schmid/Grewe*, MMR 2021, 279 (280).
40 Explizit ErwGr. 18; EuGH GRUR 2010, 445 Rn. 114 ff. – Google France; *Berberich/Seip*, GRUR-Prax 2021, 4; ähnlich auch die vom BGH entwickelte Rechtsprechung des „Zu-eigen-machens" (BGH MMR 2010, 556 m. Anm. *Engels*).
41 *Schmid/Grewe*, MMR 2021, 279 (280).
42 Ebd.
43 Ebd.
44 *Gielen/Uphues*, EuZW 2021, 627 (634).
45 Ebd.
46 ErwGr. 106; Art. 45 ff.; *Kühling*, ZUM 2021, 461 (470).
47 Ebd.
48 *Berberich/Seip*, GRUR-Prax 2021, 4.
49 Ebd.

III. Einführung von Melde- und Abhilfeverfahren

Herzstück des DSA bildet die Fortentwicklung des „***Notice-and-takedown***"-Verfahrens hin zu einem „***Notice-and-action***"-Verfahren.[50] Hosting-Dienste und Plattformen müssen demnach Verfahren schaffen, nach denen Nutzer rechtswidrige Inhalte einfach melden können, der Eingang von Meldungen bestätigt wird, diese zeitnah, sorgfältig und objektiv bearbeitet werden und eine begründete Rückmeldung über die Entscheidung gegeben wird (Art. 16 und 17).[51] Sie können Meldungen vollständig automatisiert bearbeiten.[52] Nach Art. 16 III begründet eine berechtigte Meldung Kenntnis im Sinne des Art. 6, sodass ab diesem Zeitpunkt der Diensteanbieter für die Löschung des Inhalts haftet.[53] Dabei bleibt offen, ob dies eine unwiderlegliche Fiktion oder eine Vermutungsregel darstellt.[54] Dies erinnert an den US-amerikanischen Digital Millennium Copyright Act (***DMCA***), welcher jedoch ergänzend eine Haftungsfreistellung für Anbieter, die ihnen als rechtswidrig notifizierte Inhalte rechtskonform löschen, vorsieht.[55] Damit normiert der DSA keine explizite Löschpflicht, weswegen einige kritisieren, dass das Schutzniveau unter demjenigen des NetzDG absinken könnte und ergänzende Bußgelder fordern, um bei den Host-Providern Druck zum Löschen zu erzeugen.[56]

Als Gegenargumente werden diesbezüglich stets die Einschränkung der Meinungsfreiheit sowie die Gefahr des Overblocking von kritischen Meinungen vorgebracht.[57] Besonders die Vielzahl unbestimmter Rechtsbegriffe wie der Entscheidungsmaßstab „***sorgfältig, frei von Willkür und objektiv***" in Art. 16 VI lässt den Plattformen großen Freiraum für Wertentscheidungen, die nach Stimmen der Literatur aufgrund der Grundrechtsrelevanz der Materie eigentlich vom europäischen Gesetzgeber geregelt werden müssten.[58] Art. 18 verpflichtet Anbieter darüber hinaus, bei Kenntnis Strafverfolgungsbehörden den Verdacht von Straftaten mitzuteilen.[59]

IV. Besondere Regeln für Online-Plattformen

Die Art. 19 ff. normieren für Online-Plattformen weitergehende Pflichten. Demnach stehen privaten Nutzern (Art. 3 b) bei Löschung ihrer Beiträge oder Sperrung ihres Nutzerkontos gegen die Plattform ein Recht auf ein internes Beschwerdeverfahren beim Plattformbetreiber[60] (Art. 20) und eine außergerichtliche Streitbeilegung (Art. 21) zu. Bemerkenswert ist hierbei, dass gem. Art. 22 V Online-Plattformen in Vorleistung zu treten haben und selbst im Falle ihres Obsiegens bei einer außergerichtlichen Streitbeilegung ihre Gebühren und Auslagen nicht ersetzt bekommen.[61] Ferner werden Online-Plattformen zusätzliche Transparenz- und Berichtspflichten auferlegt (Art. 24 ff.). Dies betrifft etwa Online-Werbung wie ***targeted advertising***[62] oder ***Microtargeting***, wobei Nutzer künftig bei jeder angezeigten Werbung in klarer, präziser Art und in Echtzeit erkennen können müssen, ob und um wessen Werbung es sich handelt und was die Hauptparameter für die Ausspielung an ihre Zielgruppen sind (Art. 26 I).[63] Art. 26 III normiert ferner ein Verbot von Profiling.

V. Regeln für sehr große Online-Plattformen und -Suchmaschinen

Am stärksten verpflichtet der DSA sehr große Online-Plattformen und Suchmaschinen (Abschnitt 5 DSA).[64] Als solche gelten gem. Art. 33 I, IV solche Plattformen und Suchmaschinen, die durchschnittlich monatlich mindestens 45 Millionen aktive Nutzer in der ***EU*** haben und als solche von der ***Kommission*** per Beschluss benannt wurden. Auf solche Diensteanbieter kommen zukünftig erhöhte Transparenz-, Audit- und Publizitätspflichten zu (Art. 34 ff.).[65] Der DSA sieht in deren Reich-

50 Ebd., 5; *Schmid/Grewe*, MMR 2021, 279 (280); *Spindler*, GRUR 2021, 545 ff.
51 *Berberich/Seip*, GRUR-Prax 2021, 5.
52 Art. 16 VI 2; *Raue/Heesen*, NJW 2022, 3537 (3540).
53 *Schmid/Grewe*, MMR 2021, 279 (280).
54 Ebd., Rn. 9.
55 Ebd.
56 *Eisenreich*, RDi 2021, 289 (290 f.).
57 *Eisenreich*, RDi 2021, 289, 291; Zum NetzDG *Liesching*, Netzwerkdurchsetzungsgesetz, 1. Online-Auflage 2018, § 3 NetzDG, Rn. 8 ff., m. w. N. zum Meinungsstand.
58 *Eisenreich*, RDi 2021, 289 (292).
59 *Raue/Heesen*, NJW 2022, 3537 (3541).
60 Zu dem spannenden Konflikt zwischen dem *Facebook Oversight Board* und der Meinungsfreiheit siehe bereits *Beckmann*, CTRL 1/22, 54 ff.
61 *Schmid/Grewe*, MMR 2021, 279 (281), eine Ausnahme besteht bei Böswilligkeit des Nutzers.
62 *Schmid/Grewe*, MMR 2021, 279 (281).
63 *Berberich/Seip*, GRUR-Prax 2021, 5.
64 Ebd.
65 *Spindler*, GRUR 2021, 653 (658 f.).

weite die Gefahr potenzieller gesellschaftlicher Risiken, welche zusätzliche Pflichten und insbesondere Compliance-Maßnahmen für die Bewertung systemischer Risiken begründen (Art. 34 f.).[66] Zu diesen Risiken zählen gem. Art. 34 I a – d die Verbreitung rechtswidriger Inhalte sowie potenziell nachteilige Auswirkungen auf die gesellschaftliche Debatte, Wahlprozesse[67] und die öffentliche Sicherheit.[68] Um diesen entgegenzutreten, werden Diensteanbieter dazu verpflichtet, die Moderation von Inhalten, Werbesystemen sowie Algorithmen entsprechend anzupassen (Art. 35). Hinzu kommen die Pflicht zur Einrichtung eines Krisenreaktionsmechanismus (Art. 36), einer jährlichen unabhängigen Prüfung (Art. 37) und weitgehende Transparenzanforderungen an Online-Werbung (Art. 39). Letztere werden durch den Aufbau spezifischer, leicht zugänglicher Verzeichnisse, in denen Informationen zur Art der Werbung, den Werbetreibenden und der Ausspielung verfügbar sind, sichergestellt.[69] Darüber hinaus entstehen zusätzliche Compliance- (Art. 41) und Transparenzberichtspflichten (Art. 42). Einige Stimmen in der Literatur befürchten, dass diese zusätzlich veröffentlichten Informationen nicht zu einer tatsächlich erhöhten Transparenz, sondern nur ***„zu weiteren Texten führen, die von den Konsumenten nicht gelesen werden"***.[70]

Noch weitgehender sind die Verpflichtungen des Art. 40 I, welche die Diensteanbieter verpflichten, den Koordinatoren für digitale Dienste (Art. 3 n) oder der ***Kommission*** Zugang zu den Daten, die zur Überwachung der Pflichten aus dem DSA notwendig sind, zu gewähren. Diese Möglichkeit steht gem. Art. 40 IV ff. bei begründetem Verlangen nunmehr auch zugelassenen Forschern offen. Damit soll der Forschung ermöglicht werden, Plattformen zukünftig besser zu untersuchen.[71] Diese Offenlegungspflichten teils wettbewerblich sensitiver Informationen stellt einen als sehr weitreichenden Eingriff in das – grundrechtlich geschützte – Geschäftsgeheimnis der Diensteanbieter dar.[72] Diesbezüglich räumt der DSA den Anbietern nunmehr lediglich unter Berufung auf die Sicherheit des Dienstes oder dem Schutz von Geschäftsgeheimnissen die Möglichkeit der Unterbreitung eines Alternativvorschlags ein (Art. 40 V, VI).[73] Mit Stimmen der Literatur ist festzustellen, dass insbesondere die Regelungen zum Zugang von Daten des DSA neben einer wirtschaftspolitischen auch eine gesellschaftspolitische Zielrichtung erkennen lassen.[74]

VI. Zwischenfazit

Unter rechtsökonomischen Gesichtspunkten sieht der DSA für Plattformen eine bislang ungekannte Regulierung vor. Die spärlichen Regelungen zum Schutz von Geschäftsgeheimnissen, fehlende Haftungsfreistellungen wie aus dem DMCA bekannt, die Kostentragungsregelungen sowie die Pflicht zum weitreichenden Zugang zu sensiblen Daten lassen aufhorchen und nehmen große Plattformen und Suchmaschinen klar in die Pflicht. Fraglich ist insoweit, wie durch diese Regelungen der Schulterschluss zu den USA gelingen kann.[75] Hierbei einen gemeinsamen Rechtsrahmen aufzubauen, ist immerhin die Absicht der ***Kommission***.[76]

D. Die geteilten Durchsetzungsbefugnisse aus rechtspolitischer Perspektive

I. Das geteilte Zuständigkeitsregime des DSA

Die Durchsetzung der Verpflichtungen des DSA erfolgt primär durch europäische Aufsichtsbehörden sowie durch Selbstverpflichtung der Vermittlungsdienste.[77] Jedoch wurde auf Vorschlag des Parlaments der in Art. 54 normierte Schadensersatz eingefügt, der privaten Nutzern bei Verstößen der Vermittlungsdienste gegen nutzerbezogene Pflichten nach den Vorschriften des nationalen Rechts eine ***„Ent-***

66 Ebd.; ErwGr. 75 f.
67 Zur derzeit bereits bestehenden Problematik von Deepfakes in großen sozialen Medien, vgl. *Beute/Dhungel* in dieser Ausgabe der CTRL.
68 *Berberich/Seip*, GRUR-Prax 2021, 6; *Raue/Heesen*, NJW 2022, 3537 (3542).
69 Ebd.
70 *Kuß/Lehmann*, DB 2021, 605 (609); *Gielen/Uphues*, EuZW 2021, 627 (636).
71 Schmid/Grewe, MMR 2021, 279 (281), ErwGr. 97.
72 So u.a. *Spindler*, GRUR 2021, 653 (660); *Berberich/Seip*, GRUR-Prax 2021, 6; *Gielen/Uphues*, EuZW 2021, 627 (636).
73 *Gielen/Uphues*, EuZW 2021, 627 (636).
74 *Schmid/Grewe*, MMR 2021, 279 (281).
75 Umfassend zum derzeit bestehenden Problem des EU-US-Datentransfers *Stark*, CTRL 2/22, 58 ff.; *Gielen/Uphues*, EuZW 2021, 627 (637).
76 Ebd.; so die Präsidentin der EU-Kommission in ihrer Rede in Davos, hier abrufbar (Stand: 31.12.2022).
77 *Raue/Heesen*, NJW 2022, 3537 (3542).

schädigung" einräumt.[78] Die behördliche Durchsetzung erfolgt durch von den Mitgliedstaaten geschaffene Behörden, die sog. ***„Koordinatoren für digitale Dienste"*** (Art. 49 ff.).[79] Diese Koordinatoren werden nach Art. 51 durch die Mitgliedstaaten mit Auskunfts-, Durchsuchungs- und Ermittlungsbefugnisse ausgestattet, die sich zwar aus dem nationalen Recht ergeben, jedoch in Art. 51 einen europarechtlich determinierten Mindeststandard finden.[80] Die Koordinatoren haben gem. Art. 52 III ferner die Kompetenz, Geldbußen von bis zu 6 % des jährlichen Umsatzes zu verhängen.[81] In Hinsicht auf die örtliche Zuständigkeit der Koordinatoren verfolgt Art. 56 I das Herkunftslandprinzip, nach dem der Mitgliedstaat, in dem sich die Hauptniederlassung des Vermittlungsdienstes befindet, für die Durchsetzung zuständig ist.[82] Teile der Literatur sehen hierbei die Gefahr eines standortpolitischen ***„race to the bottom"***.[83] Es besteht die Gefahr, dass die Vermittlungsdienste ihre Hauptniederlassungen in das Land verlegen, welches die Befugnisse nach Art. 51 im höchstmöglichen Mindestmaß umsetzt. Für die Überwachung sehr großer Online-Plattformen und Suchmaschinen ist gem. Art. 65 ff. die ***Kommission*** selbst zuständig. Dabei kann sie selbständig tätig werden oder zu einer Untersuchung aufgefordert werden.[84] Der ***Kommission*** stehen darüber hinaus umfangreiche Untersuchungs- , Anordnungs- und Sanktionsbefugnisse zu, die sich aus dem DSA selbst ergeben (Art. 67 ff., 74).[85] Diese Befugnisse erinnern dabei an die Kompetenzen der Kommission in Kartellverfahren, insbesondere aus Art. 11 III, VI VO 1/2003/EG.[86] Vor allem die erweiterten Kommissionskompetenzen lassen für einige eine effizientere Rechtsdurchsetzung erwarten. Wie beim DMA lassen jedoch begrenzte (Personal-) Ressourcen auch hier potenziell daran zweifeln, ob dies so einfach gelingen wird.[87]

78 Ebd.; ErwGr. 121.
79 *Schmid/Grewe*, MMR 2021, 279 (281).
80 Ebd., 282.
81 *Raue/Heesen*, NJW 2022, 3537 (3543).
82 *Schmid/Grewe*, MMR 2021, 279 (282).
83 Ebd.; *Berberich/Seip*, GRUR-Prax 2021, 6.
84 *Raue/Heesen*, NJW 2022, 3537 (3543).
85 *Schmid/Grewe*, MMR 2021, 279 (282); *Spindler*, GRUR 2021, 653 (661 f.).
86 *Schmid/Grewe*, MMR 2021, 279 (282); VO 1/2003/EG des Rates v. 16.12.2002 zur Durchführung der in den Art. 81 und 82 des Vertrags niedergelegten Wettbewerbsregeln.
87 So *Djebbari/Niebler*, rescriptum studentische Rechtszeitschrift (im Erscheinen).

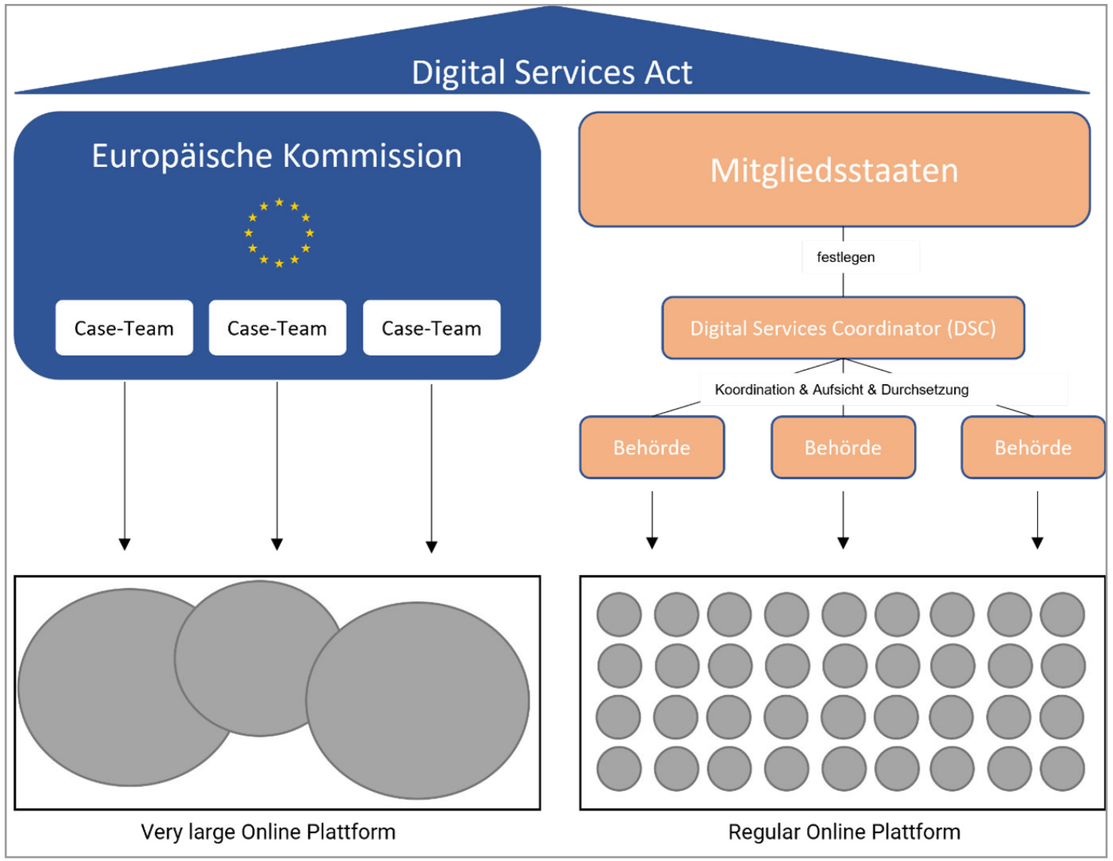
„Die spärlichen Regelungen zum Schutz von Geschäftsgeheimnissen und dem Zugang zu sensiblen Daten nehmen die großen Plattformen klar in die Pflicht."

II. Vereinbarkeit mit bestehenden nationalen Regelungen

Der DSA wurde seitens der EU als Verordnung erlassen, welche Anwendungsvorrang vor entsprechenden nationalen Regelungen genießt (Art. 288 II AEUV). Jedoch ordnet Art. 2 III, IV an, dass andere europäische Rechtsakte als Spezialvorschriften unberührt bleiben.[88]

Wie beim DMA, der es Mitgliedstaaten verbietet, Gatekeepern zusätzliche Verpflichtungen aufzuerlegen (Art. 1 V DMA), harmonisiert der DSA die Regulierung von Vermittlungsdiensten abschließend (Erwägungsgrund 9), sodass nationale Regelungen wie das NetzDG, die über den DSA hinausgehen, allenfalls in europarechtskonformer Auslegung noch angewandt werden können (Erwägungsgrund 9).[89] Nicht unbegründet ist, dass hierbei einige Autoren ein Absinken des Schutzniveaus befürchten.[90] Für das deutsche Recht stellt hier insbesondere die Anzeigepflicht des Art. 18 einen Rückschritt zur aktuellen Gesetzeslage dar, wonach eine Anzeigepflicht nur für eine Straftat besteht, die eine ***„Gefahr für das Leben oder die Sicherheit einer Person oder von Personen darstellt***". Diese Regelung verdrängt den

88 *Gielen/Uphues*, EuZW 2021, 627 (633).
89 *Raue/Heesen*, NJW 2022, 3537 (3542).
90 So insb. *Eisenreich*, RDi 2021, 289 (290 f.).



Das geteilte Durchsetzungskonzept des DSA (Quelle: EU-Komission)

wesentlich bestimmteren § 3a NetzDG zwar in Hinsicht auf schwere staatsgefährdende Straftaten wie die Verbreitung von Propagandamitteln verfassungswidriger Organisationen aus § 86 StGB aufgrund Erwägungsgrund 9 nicht vollständig, lässt aber gewisse Schutzlücken bestehen.[91] So könnte beispielsweise bei älterem kinderpornografischem Material in Einzelfällen fraglich sein, ob noch eine „***Gefahr***" für die Sicherheit des Opfers und somit eine Anzeigepflicht besteht.[92]

91 *Dregelies,* MMR 2022, 1033 (H. 12/2022); *Raue/Heesen*, NJW 2022, 3537 (3541).
92 *Eisenreich*, RDi 2021, 289 (293).

Schlussendlich besteht für die Strafverfolgungsbehörden im Falle der Löschung von Inhalten das Bedürfnis, für einen ausreichenden Zeitraum zu Beweiszwecken auf die Informationen auch nach der Löschung zugreifen zu können.[93] Dies ist aber im DSA nicht explizit geregelt.[94]

E. Fazit

Insbesondere in Hinsicht auf den Vollzug lässt der DSA noch viele Fragen offen. Inwieweit die angeführten Durchführungs- und Vollzugsbestimmungen eine effektive Regulierung durchsetzen werden, ist zum aktuellen Zeitpunkt sehr fraglich.

Zusammenfassend lässt sich auf jeden Fall anführen, dass die Verordnung durch ihren weiten Anwendungsbereich, das abgestufte Regulierungsregime und die neu zu schaffenden Durchsetzungsautoritäten regulatorisches Neuland betritt.[95] Ob der DSA im schwierigen Umfeld zwischen der Verwirklichung von Grundrechten und Regulierung das richtige Maß trifft, bleibt abzuwarten.

93 Ebd.; *Bundesrat*, BR-Drs. 96/21B, Ziff. 39.
94 *Eisenreich*, RDi 2021, 289 (293).
95 So auch *Raue/Heesen*, NJW 2022, 3537 (3543).

Welche digitalen Klagewege es aktuell schon gibt, erklärt der hier verlinkte CTRL-Podcast. Einfach mal reinhören!

Zurück zum Inhaltsverzeichnis

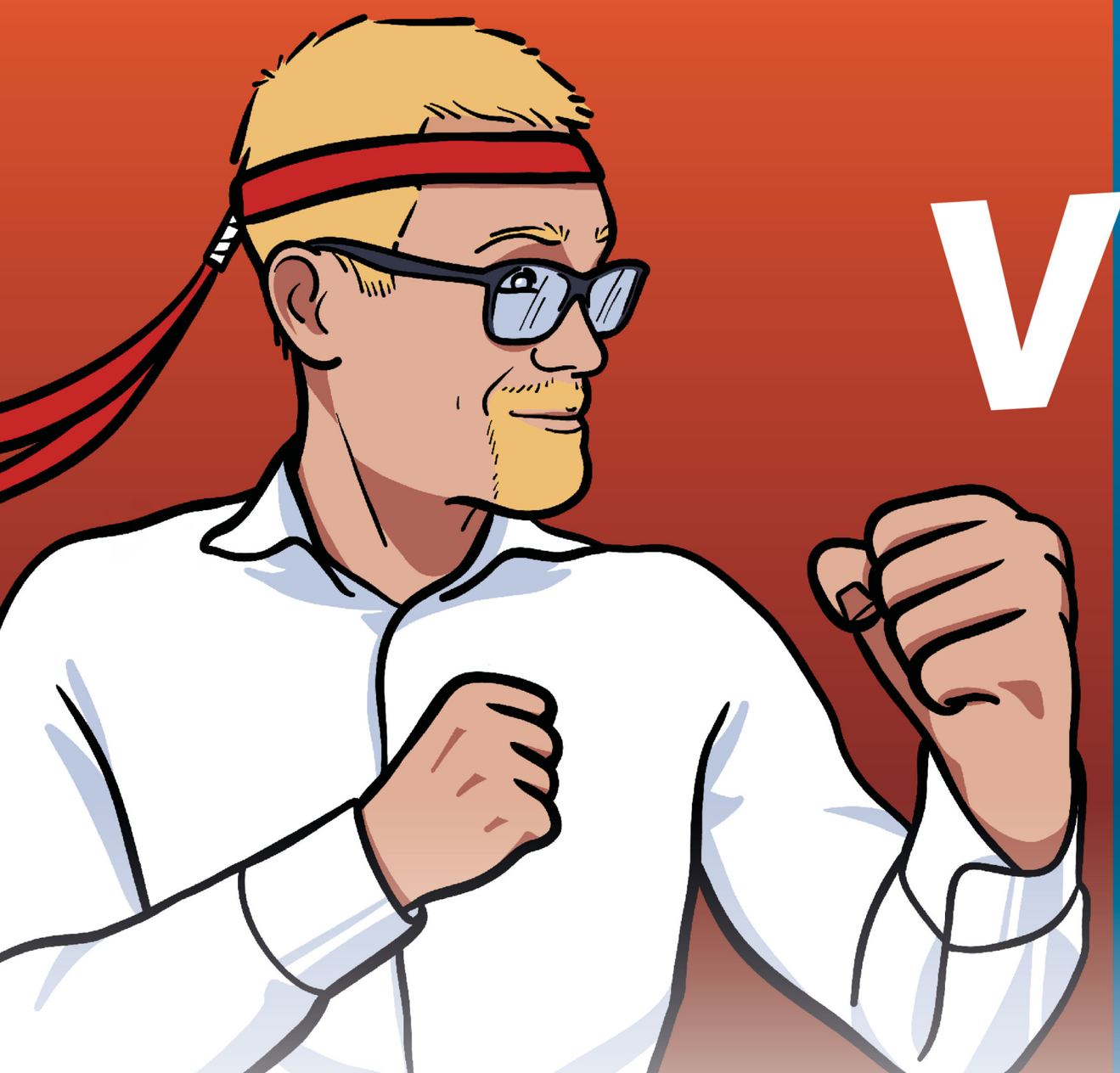
P1

Keppeler

P2

Dahi

Vs.



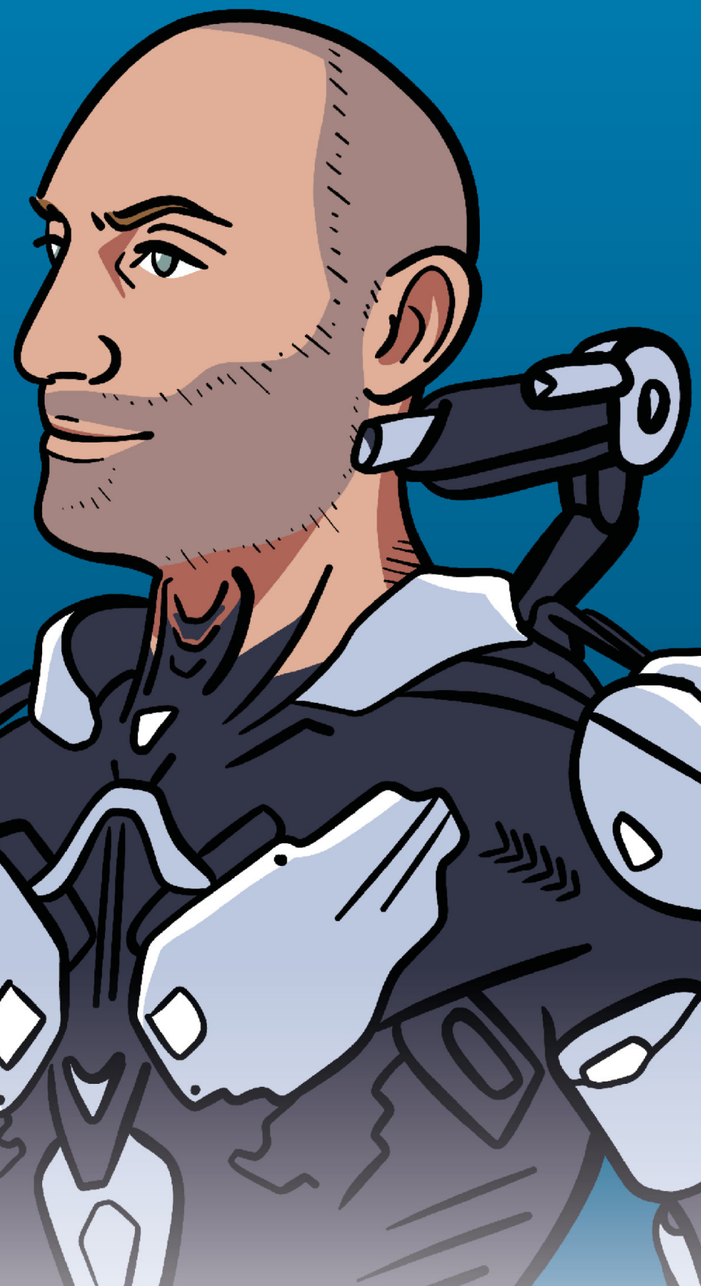


Illustration: Helena Sommer || fr.wntr

Dr. Lutz Martin Keppeler ist Partner bei der überregionalen Kanzlei Heuking Kühn Lüer Wojtek und Lehrbeauftragter für Datenschutzrecht an der TH Köln. Er berät Mandanten zu allen Fragen des IT- und Datenschutzrechts. Dabei berät er Mandaten an der Schnittstelle zwischen Technik und Recht, in den Gebieten IT-Sicherheitsrecht, Telekommunikationsrecht, Open Source Lizenzrecht und Datenschutzrecht.

Alan Dahi ist Berater für Datenschutzrecht, externer Datenschutzbeauftragter und Gutachter. U.a. ist er als Berater für die britische Kanzlei AWO tätig. Zudem ist er Gastdozent am Institut für Rechtsinformatik der Universität Hannover. Bei noyb – European Center for Digital Rights in Wien war er bis 2022 zuständig für Projekte in den Bereichen biometrische Suchmaschinen, Pur-Abos und Cookie-Banner sowie Datenschutz durch Technikgestaltung.

Streitgespräch

DSGVO: Ignorieren statt kooperieren?

David Wasilewski, Ferdinand Wegener, Philipp Beckmann

Open Peer Review

Dieser Beitrag wurde lektoriert von:
Anna Misera

Herr Dr. Keppeler, Sie haben auf der Future Fair 2022 Aufsehen erregt, als Sie erklärten,[1] dass es aufgrund des geringen Enforcement-Risikos und den hohen Kosten für die Umsetzungen von datenschutzrechtlichen Vorgaben für viele Unternehmen keinen Sinn ergibt, die Datenschutz-Grundverordnung (DSGVO) flächendeckend umzusetzen. Ist das langfristig eine sinnvolle Strategie?

1 Ein Videoausschnitt des Gesprächs ist hier abrufbar (Stand: 29.01.2023).

Dr. Keppeler: Ich stehe für eine pragmatische Umsetzung der Datenschutz-Vorgaben. Eine langfristige Nichtumsetzung ist aber sicherlich nicht empfehlenswert. Ich meine dennoch, dass jeder Geschäftsführer die Kosten und Vorteile der DSGVO-Umsetzung auf Basis der in der Praxis tatsächlich existierenden Risiken abwägen sollte. Täglich gibt es europaweit nach meiner Einschätzung deutlich mehr Datenschutzverstöße als Straßenverkehrsunfälle. Manch ein Unfall zieht ein Bußgeld oder einen Schadensersatzanspruch nach sich. Bei der Vielzahl der (unentdeckten und offen zutage tretenden) Datenschutzverstöße ist dies in viel geringerem Umfang der Fall (wobei die Schadensersatzklagen erheblich zunehmen – dazu sogleich).

„'Compliance' ist sehr oft gesellschaftlich wichtig und erwünscht.“

Herr Dahi, Ihr Kollege Herr *Dr. Keppeler* erklärte jüngst auf einer Konferenz, dass es aufgrund des niedrigen Enforcement-Risikos für viele Unternehmen keinen Sinn ergebe, die DSGVO umzusetzen. Hat er recht?

Dahi: Nehmen wir an, ich bin ein Lebensmittelunternehmen. Soll ich mich nur dann an die zahlreichen lebensmittelrechtlichen Vorgaben halten, falls es ein hohes Enforcement-Risiko gibt? Oder soll ich mich rechtskonform verhalten, weil die Bestimmungen grundsätzlich Sinn ergeben und wir daher unbesorgt im Supermarkt und auf dem Wochenmarkt einkaufen können?

Dieses Beispiel zeigt, dass „*Compliance*“ sehr oft gesellschaftlich wichtig und erwünscht ist. Das gilt auch für den Datenschutz, der nicht nur verbraucherschutzrechtliche, sondern auch gesellschaftsschutzrechtliche Elemente hat. Erwägungsgrund 4 S. 1 und 2 der DSGVO fasst es schön zusammen:

„Die Verarbeitung personenbezogener Daten sollte im Dienste der Menschheit stehen. Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden.“

Den genauen Kontext der Aussage von Herrn *Dr. Keppeler* kenne ich nicht. Die DSGVO ist wahrlich kein perfektes Gesetz. Aber pauschal zu behaupten, dass es keinen Sinn ergibt, die DSGVO aufgrund des niedrigen Enforcement-Risikos umzusetzen, halte ich für verfehlt.

Nach einer Bitkom-Umfrage behaupten 40 % der befragten Unternehmen, dass die DSGVO kein relevanter Wettbewerbsvorteil für sie sei.[2] 30 % sprechen sogar von gar keinem Wettbewerbsvorteil. Glauben Sie, dass Unternehmen einen Wettbewerbsvorteil haben, wenn Sie die DSGVO umsetzen?

Dahi: Es kommt auf den Sektor an. Wie datengetrieben ist der Sektor, wie reguliert, welche Erwartungen haben die Kunden? In meiner Beratungspraxis Pilleum sehe ich, dass erfolgreicher Datenschutz für viele technologienahe Unternehmen durchaus ein Wettbewerbsvorteil ist. Der Datenschutz spielt in vielen Ausschreibungen eine sehr wichtige Rolle und selbst Informationssicherheitszertifizierungen wie die ISO 27001 überlappen zum Teil mit den Anforderungen aus der DSGVO.[3]

2 *Streim/Weiß*, DS-GVO bringt nur den wenigsten Unternehmen Wettbewerbsvorteile, hier abrufbar (Stand: 29.01.2023).

3 Eine ISO 27001-Zertifizierung ist ein dokumentierter Nachweis, dass ein Informationssicherheits-Managementsystem mit den Anforderungen der Informationssicherheit konform ist. Ein solches System schützt u.a. Unternehmen und Organisationen, Risiken bzgl. Cyberangriffen und Datendiebstählen zu senken.

Dr. Keppeler: Einzelne Unternehmen sicher schon. Wer das Gleiche anbietet, wie alle anderen, nur eben datenschutzkonform, der hat einen Vorteil. Jedenfalls, wenn es um ein datenlastiges Business geht und nicht um – sagen wir – das Schreinern von Möbeln. Ich bin in dieser Hinsicht aber marktgläubig: Wenn die Umsetzung von Datenschutzvorgaben tatsächlich ein riesiger Vorteil wäre, würden Unternehmen dies von ganz allein machen.

Private-Enforcement-Risiko: Birgt die massenhafte Durchsetzung von Ansprüchen durch Legal-Tech-Anbieter, die Verbrauchern ihre Schadensersatzansprüche wegen DSGVO-Verletzungen abkaufen und durchsetzen, ein wesentliches Mittel zur Sicherstellung einer flächendeckenden Einhaltung der DSGVO? Oder sehen Sie in dieser Praxis auch Risiken?

Dr. Keppeler: Wenn die Möglichkeit von Schadensersatzansprüchen nach jeder DSGVO-Verletzung (und nicht nur nach einer *gravierenden* Verletzung) durch den EuGH akzeptiert wird (ein Urteil dazu ist dieses Jahr zu erwarten), steigt das DSGVO-Risiko sämtlicher Unternehmer (und sämtlicher öffentlicher Stellen – inklusive Universitäten) sofort rasant. Dann muss plötzlich jeder Amts- und Landrichter ganz schnell die DSGVO lernen und wir brauchen tausende neue Datenschutzprofis. Dies würde vermutlich zu einer wesentlich intensiveren Beschäftigung der Unternehmen mit einer systematischen Umsetzung der Anforderungen der DSGVO führen. Das wäre an sich eine gute Sache. Aber die Aufsichtsbehörden haben in der Vergangenheit auch an gesellschaftlich erwünschten Stellen beide Augen zugekniffen. So haben wir alle in der Pandemie viele Cloud-Tools genutzt, um unsere Arbeit fortzuführen. Ich selbst habe eine Datenschutz-Vorlesung über Zoom abgehalten (ein „*Widerspruch in sich, wie ein Kollege sagte …*"). Die ganze Digitalisierung mit verfügbaren Cloud-Tools wäre durch ein Datenschutzbußgeld erledigt gewesen. Wenn Anfang 2020 die große Welle der Schadensersatzansprüche schon so weit gewesen wäre wie jetzt, hätte die Nutzung von Cloud-Tools in der Pandemie zahlreiche Ansätze hierfür geboten. Dies ist das Risiko.

Hervorragend ist übrigens, dass wir dank der vielen Schadensersatzansprüche nun endlich viel Rechtsprechung zu interessanten Streitfragen bekommen.

Dahi: Grundsätzlich begrüße ich die Entwicklung. Das ist genauso wie bei Fluggastrechten. Entweder verbringe ich als betroffene Person unverhältnismäßig viel Zeit mit der Verfolgung und Durchsetzung meiner Rechte, oder ich trete diese an einen effizienten Dienstleister ab. Das entlastet Gerichte, das entlastet betroffene Personen, das kann sogar in gewissen Fällen Unternehmen entlasten — sofern tatsächliche und sinnige Ansprüche professionell durchgesetzt werden und das System nicht missbraucht wird.

Halten Sie das (neue) EU-Bußgeldmodell[4] der Aufsichtsbehörden für angemessen im Hinblick auf die Kopplung an den Unternehmensumsatz? Beispielhaft: In Rede steht ein relativ hohes Bußgeld gegen einen Großkonzern, das „*nur*" auf formelle Verstöße gestützt ist. Grund für die Höhe sei die Anknüpfung an den hohen Unternehmensumsatz (etwa das Millionenbußgeld für Datenschutzverstöße von VW in Niedersachsen)[5].

Dahi: Die Berücksichtigung des Unternehmensumsatzes beim Bußgeld im Datenschutz ist m.E. gesetzlich festgelegt (vgl. Art. 83 IV, V DSGVO) und daher keine neue Entwicklung an sich. Neu ist, dass die verschiedenen nationalen Aufsichtsbehörden nun ein Modell zur Vereinheitlichung der Bußgelder haben. Damit dürfte es nicht mehr zu so großen Unterschieden zwischen den Mitgliedstaaten kommen, wenn es um die Höhe der Bußgelder geht. Weil letztlich auch andere Elemente in die Bußgeldbemessung einfließen, sehe ich kein grundsätzliches Problem mit dem Modell. Das Modell hat sich im Übrigen auch in anderen Rechtsbereichen bewährt, so z.B. im Wettbewerbsrecht und auf eine gewisse Weise auch im Personenstrafrecht (vgl. die vorgesehenen Tagessätze des § 40 II StGB).

4 S. Guidelines 04/2022 on the calculation of administrative fines under the GDPR, hier abrufbar (Stand: 29.01.2023).
5 Vgl. dazu: 1,1 Millionen Euro Bußgeld gegen Volkswagen, hier abrufbar (Stand: 29.01.2023).

Art. 83 V DSGVO: „Bei Verstößen gegen die folgenden Bestimmungen werden (…) Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist"

Dr. Keppeler: Immerhin wird das Bußgeldmodell zu einer europaweiten Vereinheitlichung der Bußgeldhöhen in der Praxis führen. Man muss anerkennen, dass selbst *„nur formelle"* Themen in der DSGVO horrend sanktioniert werden können. Insoweit wird das Konzept durch den Bußgeldrahmen der DSGVO gedeckt. Entsprechend hohe Bußgelder hätten also bereits im Juni 2018 – kurz nach dem Beginn der Anwendbarkeit der DSGVO – erlassen werden können. Meine Beobachtung ist, dass die Anzahl der hohen Bußgelder von über 1. Mio. EUR in Deutschland immer noch überschaubar ist. Ich tippe, daran wird sich auch durch das Bußgeldkonzept nicht viel ändern.

Inwieweit hemmt es Unternehmen, dass es 18 Aufsichtsbehörden in Deutschland gibt und somit auch in jedem Bundesland die Auslegung der DSGVO anders erfolgen kann?

Dahi: Ich glaube nicht, dass die Anzahl der Aufsichtsbehörden und eine gegebenenfalls unterschiedliche Auslegung der DSGVO wirkliche Hemmnisse für eine erfolgreiche Umsetzung der DSGVO sind — weder in Deutschland noch in der EU, wo jeder Mitgliedsstaat eine eigene Aufsichtsbehörde hat. Die Grundanforderungen der DSGVO sind klar. Schließlich ist es auch kein wirkliches Hemmnis für Unternehmen, dass Oberlandesgerichte in Deutschland das Recht zum Teil unterschiedlich auslegen.

Dr. Keppeler: Jeder, der während der Corona-Zeit seine Maske im Zug in Bundesland X absetzen durfte und in Bundesland Y wieder aufsetzen musste, kann nachvollziehen, zu wie viel komplexer Unerklärbarkeit gut gemeinter Föderalismus führen kann. Ausländischen Unternehmen und Investoren ist dies kaum zu vermitteln.

„Auch der Datenschutz braucht eine gute Öffentlichkeitsarbeit."

In welchem Maße halten Sie die (mögliche) Gefahr für relevant, dass durch sog. Pur-Abonnements vieler Medienwebseiten eine Art Zweiklassengesellschaft entstehen könnte? (Einerseits diejenigen, die es sich leisten können und wollen, für jeden Beitrag zu zahlen, damit sie nicht getrackt werden. Andererseits diejenigen, die in ein Tracking *„einwilligen"* (müssen), damit keine Entgeltkosten entstehen.)

Dr. Keppeler: Dies führt ja nur zu einer Zweiklassengesellschaft von Personen, die passende Werbung angezeigt bekommen und Personen, die mit aller Macht Werbung verhindern wollen und die als Ergebnis unpassende Werbung erhalten. Gemessen daran, dass die wesentlichen Zeitungen (auch die der Qualitätspresse) ganz maßgeblich von Onlinewerbung leben, ist dies aus meiner Sicht nicht dramatisch.

Dahi: Egal ob reich oder arm, ich glaube kaum, dass sich irgendjemand stets die Mühe machen wird, für jede besuchte Seite ein Konto anzulegen und Zahlungsdetails einzugeben, *„nur"* damit die Person nicht getrackt wird. Das dauert zu lange und es gibt viel einfachere und billigere Methoden, Tracking zu umgehen.

Beispielsweise kann man ein Virtuelles Privates Netzwerk (VPN) mit Tracking-Blocker verwenden oder einen Browser wie Brave, wo ebenfalls Tracking unterbunden wird. Daher würde ich die Frage eher umformulieren: Sind Pur-Abonnements überhaupt rechtmäßig? Irgendwann wird sich wohl der Europäische Gerichtshof (EuGH) mit der Frage auseinandersetzen.

Die Sinnhaftigkeit des Einwilligungserfordernisses wurde in Wissenschaft und Praxis in den vergangenen Jahren zunehmend hinterfragt.6 Halten Sie die Einwilligung noch für ein geeignetes Instrument, um das Recht auf Schutz der Sie betreffenden personenbezogenen Daten (Art. 8 I GRCh) ausüben zu können?

Dahi: Die Einwilligung ist in gewissen Situationen ein geeignetes Instrument, in sehr vielen aber auch nicht. Liegt beispielsweise eine vertragliche Notwendigkeit der Verarbeitung vor, ist eine Einwilligung schlicht und einfach die falsche Rechtsgrundlage. Es fehlt an der Freiwilligkeit; die Verarbeitung ist für den Vertragszweck erforderlich.

Doch angenommen, dass die Einwilligung für einen Verarbeitungszweck tatsächlich die geeignete Rechtsgrundlage ist. In den allermeisten Fällen gehe ich davon aus, dass eine betroffene Person durchaus in der Lage sein wird, die Verarbeitung ausreichend zu verstehen, um darin einzuwilligen. Das Problem liegt eher an der mangelnden Aufklärungsarbeit, die gegenüber der betroffenen Person erbracht werden sollte.

Als Beispiel sei ein einfaches Cookie-Banner auf einer Webseite genannt. Den wenigsten Nutzern wird bekannt sein, dass eine Einwilligung oft nicht nur Auswirkungen auf die ersuchende Webseite haben wird, sondern dass mit einer *„Einwilligung“* das Internet-Verhalten des Nutzers auf zahlreichen Seiten und sogar geräteübergreifend erfasst, analysiert und für Werbezwecke an unzählige Unternehmen wortwörtlich versteigert wird. Das könnte man natürlich dem Webseitenbesucher klarmachen. Man will es aber nicht. Denn die allermeisten Nutzer würden dann zwischen den Knöpfen *„Akzeptieren“* und *„Ablehnen“* letzteren wählen.

Dr. Keppeler: Die Kritik und das Thema sind wichtig und richtig. Aber die Lösung besteht nicht im *„entweder-oder“*, sondern aus sehr vielen Schattierungen. Sonst könnte mit der gleichen Begründung auch niemand mehr in seine medizinische Operation einwilligen. Ich meine, es sollte hier vor allem auf die *„Angemessenheit“* ankommen. Je weniger sensibel die Daten sind, in deren Verarbeitung eingewilligt werden soll, um so größere Informationsdefizite sind beim Einwilligenden hinzunehmen. Eine Cookie-ID und eine IP-Adresse sind zum Beispiel – nach meiner Ansicht – sehr wenig sensibel. Es sollte daher ein ganz geringer Informationsgehalt genügen, um darüber wirksam per Einwilligung zu verfügen. Bei einer strengen Anwendung der höchsten Anforderungen an die Einwilligungserklärung, welche die Deutsche Rechtsprechung maßgeblich anhand von §7 _ entwickelte, müsste man eigentlich weite Teile des Internets für deutsche Nutzer sperren. Hier dürfen täglich deutlich über eine Millionen Verstöße feststellbar sein.

> „Bei einer strengen Anwendung der höchsten Anforderungen an die Einwilligungserklärung müsste man eigentlich weite Teile des Internets für deutsche Nutzer sperren.“

Um nicht auf eine Einwilligung ausweichen zu müssen, versuchen Verantwortliche aufgrund eines Vertrages (Art. 6 I 1 lit. b DSGVO) die Verarbeitung zu legitimieren. Sind Sie der Ansicht, man könnte über eine *„geschickte“* Vertragsgestaltung nahezu sämtliche Verarbeitungen legitimieren oder wird dadurch die Einwilligung ausgehöhlt?

6 Vgl. dazu etwa *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2016.

Dr. Keppeler: Man kann das versuchen, aber dem sind Grenzen gesetzt und es kann *„nach hinten“* losgehen. Die Grenzen kommen in Deutschland aus dem AGB-Recht. Ein Abweichen vom Leitbild des Gesetzgebers führt zur Unwirksamkeit der Klausel. Hierüber kann leicht stolpern, wer sich seine AGB nur noch nach Datenschutzgesichtspunkten entwirft. Zudem geht man auf diesem Weg häufig Verpflichtungen ein, die man im Nachhinein selbst lieber nicht mehr als echte einklagbare Verpflichtung sehen möchte. Das Instrument der kreativen Vertragsanpassung aus Datenschutzgesichtspunkten ist daher kein Allheilmittel, aber im Einzelfall eine interessante Gestaltungsoption.

Dahi: Eine solche Legitimierung wird in den seltensten Fällen möglich sein. Den Grund kann man meines Erachtens auch aus dem allgemeinen Vertragsrecht ableiten. Dort gibt es Haupt- und Nebenleistungspflichten. Deren Einordnung hängt vom Kern der vertraglichen Leistung ab, welche objektiv bestimmt wird.

Die vertragliche Erforderlichkeit einer datenschutzrelevanten Verarbeitung hängt ebenfalls vom Kern der zugrundeliegenden vertraglichen Leistung ab.

Verwende ich einen E-Mail-Provider wie Google Mail oder Hotmail, so ist, objektiv gesehen, die Erbringung von E-Mail-Dienstleistungen der Kern der vereinbarten Leistung. Eine *„geschickte“* Vertragsgestaltung kann das Schalten von personalisierter Werbung nicht in eine Kernleistung verwandeln, die nun vertraglich verpflichtend sein soll.

Stichwort *„Rechtsmissbrauch“*: Glauben Sie, dass der Auskunftsanspruch (Art. 15 DSGVO) ein wichtiges Instrument ist, um seinem Grundrecht nachzukommen oder *„verkommt“* dieses nur als *„Druckmittel“*, um bei Vertragspartnern zusätzliche Kosten zu verursachen? Immerhin wird das Recht auf Auskunft ausdrücklich in Art. 8 II GRCh genannt.

Dahi: Selbstverständlich ist der Auskunftsanspruch ein wichtiges Instrument. Ohne zu wissen, welche Daten über mich verarbeitet werden, kann ich zum einen viele andere Datenschutzrechte nicht ausüben. Zum anderen kann ich mit dem Auskunftsrecht oft den Grund für Störungen im Vertragsverhältnis ausfindig machen.

Ein Beispiel: über Monate hinweg erhielt ich von einem Paketdienst regelmäßig eine Mahnung wegen einer angeblich nicht bezahlten Rechnung. Ich habe mich unzählige Male an den Kundendienst gewandt, sowohl telefonisch als auch schriftlich. Ich erklärte dem Kundendienst, dass die Rechnung beglichen wurde und legte dafür Beweise vor. Es tat sich nichts. Also habe ich mich schlussendlich an den Datenschutzbeauftragten des Unternehmens mit einer Mischung aus dem Recht auf Auskunft und auf Berichtigung gewandt. Innerhalb kürzester Zeit war das Problem gelöst.

Dieser Streit bezieht sich auf die Auslegung des Art. 6 I 1 lit. b DSGVO. Nach dieser Norm ist eine Datenverarbeitung zulässig, wenn sie zur Erfüllung eines Vertrags oder einer vorvertraglichen Pflicht “erforderlich” ist. Insoweit wird vertreten, dass grundsätzlich erstmal alles in den Vertrag geschrieben werden kann und danach mittels einer AGB-Kontrolle gem. §§ 305 ff. BGB (wie von Keppeler ausgeführt) die Rechtmäßigkeit ermittelt wird. Die andere Ansicht (wie von Dahi ausgeführt) will den „Wesensgehalt” des Vertrags ermitteln und daraus schließen, welche personenbezogenen Daten erforderlich sind, um den Vertrag zu erfüllen.[1]

1 Für die erste Ansicht: *Engeler*, ZD 2018, 55 (57); für die zweite Ansicht: *Golland*, MMR 2018, 130 (131) jeweils m.w.N.

Dr. Keppeler: Ich halte den Auskunftsanspruch für legitim und ich freue mich über die fast 300 Urteile, die Juris (Stand: Dezember 2022) zu Art. 15 DSGVO angibt. Hierbei gilt: Jedes wichtige Recht wird auch einmal *„missbraucht“* (wobei dies immer

eine Frage der Perspektive ist). Das gilt auch für Art. 15 DSGVO. Die sorgfältige Beantwortung von Betroffenenrechten führt bei Unternehmen zu viel Arbeit, aber damit muss jedes Unternehmen leben, welches massenhaft die Daten von Verbrauchern verarbeitet.

Der von der EU-Kommission vorgeschlagene Entwurf eines Data-Acts7 soll die Bereitstellung von Daten ermöglichen, währenddessen die DSGVO Daten unter ein Erlaubnisvorbehaltsverbot stellt. Sehen Sie hier einen Zielkonflikt, insb. durch den Grundsatz der Datenminimierung der DSGVO?

Dr. Keppeler: Es stimmt, der Data-Act soll den freien Datenaustausch fördern und insoweit besteht ein Widerspruch zur gesamten DSGVO. Dennoch regelt der Data-Act ein wichtiges Thema, denn dauernd fragen mich Mandanten: „*Wem gehören denn jetzt die Daten?*“ und „*Habe ich ein Recht, die Daten zu nutzen?*“. Die faire Nutzung von Daten für europäische Entwicklungen im Bereich Künstlicher Intelligenz (KI) halte ich beispielsweise für wichtig. Nur so viel zu dem bislang nicht final erlassenen Data-Act.

Dahi: Auf den ersten Blick sehe ich keinen Konflikt zwischen den Gesetzen. Die DSGVO soll ja auch weiterhin Anwendung finden, wenn es um personenbezogene Daten geht. Das Datengesetz regelt nicht nur personenbezogene Daten, sondern auch nicht-personenbezogene Daten.

Drittlandtransfers: Sind Sie zuversichtlich, dass die neue „*Executive Order to Implement the European Union-U.S. Data Privacy Framework*“ diesmal halten wird, um den Transfer von personenbezogenen Daten in die USA zu legitimieren? Oder wird dieses Abkommen abermals vom EuGH für nichtig erklärt werden?

Dr. Keppeler: Um genau zu sein: Die „*Executive Order*“ ist ein Puzzlestück des neuen „EU-US-Privacy Frameworks“. Die sogenannte „***Adequacy decision***“ (Angemessenheitsbeschluss) der EU-Kommission ist ein wesentlich wichtigerer Puzzlestein (jedenfalls aus europäischer Sicht).[8] Liegt beides vor, wird ein EU-US Datentransfer wieder vollständig legitim sein. Dann darf jeder endlich wieder sorgenfrei Google Fonts dynamisch einbinden und Zoom verwenden. Auf mittlerer Sicht sehe ich das Risiko, dass man auch an dem EU-US-Privacy Frameworks wieder ausreichend kritisieren kann – wenngleich man bei einem strengen Maßstab Kritikpunkte bei einem Datentransfer in viele Rechts- und Unrechtsstaaten sehen kann. Ich halte es daher mit einer Wahrscheinlichkeit von 50 % für möglich, dass man auch das aktuelle Abkommen wieder vor dem EuGH kippen könnte. Allerdings ist es bis dahin ein jahrelanger Weg.

Dahi: Das Abkommen behebt nur oberflächlich die vom EuGH genannten Mängel.[9] Daher tippe ich darauf, dass der EuGH es kippen wird.

Wird Ihrer Meinung nach “*Datenschutz*“ in der Bevölkerung als Verhinderer angesehen?

Dr. Keppeler: Ja, das ist der Fall. Es gibt ein erstes Datenschutz-Comedy-Programm. Man kann überspitzt sagen: Die DSGVO sei an sich ein einziges großes Comedy-Programm, weil sie zu so viel Realsatire führt.

Wenn man dies ändern wollte, müsste man die Geltung der DSGVO für Handwerksbetriebe und Vereine und ähnliches aufheben und stattdessen täglich und mit aller Macht gegen die großen US-Datenkraken und ihre Nachahmer in Deutschland vorgehen. Aber nur dort, wo einzelne Datenverarbeitungsschritte wirklich als „*Skandal*“ empfunden werden. Mit dem Erfolg der Aufsichtsbehörden käme die Anerkennung der DSGVO.

7 S. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), COM(2022)68 final, ausf. dazu: *Eppelmann*, CTRL 2/2022, 37 f.

8 Im Dezember 2022 hat die Kommission einen ersten Entwurf dazu veröffentlicht. Dieser ist hier abrufbar (Stand: 29.01.2023).

9 Krit. auch Gorski, The Biden Administration’s SIGINT Executive Order, Part II: Redress for Unlawful Surveillance, hier abrufbar (Stand: 29.01.2023).

Dahi: Leider sehe ich im Bekanntenkreis tatsächlich, wie Datenschutz als Verhinderer angesehen wird. Schwachsinnige Cookie-Banner, die man eh nicht ablehnen kann, ohne in die Untiefen des Banners vordringen zu müssen, um nervige Einzeleinstellungen vorzunehmen. Überall einen Haken für die stets erforderliche *„Einwilligung“* zu setzen, obwohl man keine Wahl hat, die Einwilligung nicht zu erteilen. Schwierigkeiten bei der Nutzung von Daten für gesellschaftsförderliche Zwecke, zum Beispiel für ***Smart Cities*** oder ***Cognitive Cities***.

Meines Erachtens gibt es unterschiedliche Gründe dafür. Blickt man auf Cookies oder Einwilligungs-Haken, dann liegt das zum einen an einer schlechten Beratung von Anwälten und Beratern, die solche *„Lösungen“* empfehlen. Zum anderen muss man auch eine gewisse Schuld bei den Aufsichtsbehörden sehen, die nicht immer bestimmt genug handeln, sei es in der Durchsetzung oder in veröffentlichten Leitfäden und Orientierungshilfen.

„Man kann überspitzt sagen: Die DSGVO sei an sich ein einziges großes Comedy-Programm, weil sie zu so viel Realsatire führt.“

Der Laie sieht sich im Alltag mit den (End-)Ergebnissen dieser Mängel konfrontiert und schiebt naturgemäß alles auf den Datenschutz. Woher soll ein Laie wissen, dass vielleicht nicht das Gesetz das Problem ist, sondern diejenigen, die mit dem Gesetz arbeiten?

Wie ist das Problem anzugehen?

Klar ist, dass sich die Qualität des angewandten Datenschutzes erhöhen muss, sowohl juristisch als auch technisch. Dadurch wird der von Laien im Alltag erlebte Datenschutz positiver erfahren. Juristen und Techniker müssen sich auch zusammensetzen, damit innovative technische Lösungen (Stichwort: *„Datenschutz durch Technikgestaltung“*, Art. 25 DSGVO) vorangetrieben werden. Dadurch kann bei komplexeren Verarbeitungsprozessen ein Datenschutz umgesetzt werden, der sowohl im Dienste der Menschheit als auch des Menschen steht. Es würde auch helfen, den Nutzen des Datenschutzes besser zu kommunizieren. Auch der Datenschutz braucht eine gute Öffentlichkeitsarbeit.

„Woher soll ein Laie wissen, dass vielleicht nicht das Gesetz das Problem ist, sondern diejenigen, die mit dem Gesetz arbeiten?“

Wie denken Sie, wird sich und sollte sich die DSGVO weiterentwickeln? Ist die DSGVO bereit für neue Entwicklungen der Digitalisierung?

Dr. Keppeler: Die DSGVO ist neutral geschrieben. Man spricht ganz offiziell von *„Technikneutralität“*. In Wahrheit löst man dies über sehr abstrakte Generalklauseln. Dies führt dann faktisch zu einer Art *„Regelungsneutralität“* der DSGVO. So wie die DSGVO jetzt geschrieben ist, müsste sie sich in 100 bis 1000 Jahren nicht ändern, da bin ich mir sicher. Aus dem gleichen Grund, aus dem man §§ 138, 242 und 826

BGB nicht zu ändern braucht: Die Generalklauseln lassen es zu, dass eine sich entwickelnde Rechtsprechung neue Technologien, aber auch eine „***Änderung des Zeitgeistes***“ berücksichtigt.

Wenn man die DSGVO sinnvoll weiterentwickeln will, müsste man beginnen, einzelne Regelungsbereiche wie z.B. „***Videoüberwachung***“ oder „***Onlinemarketing***“ zu konkretisieren. Ich sehe aber nicht, dass es Bestrebungen in diese Richtung gibt.

Dahi: Zunächst müssen die bestehenden verfahrensrechtlichen Probleme in grenzüberschreitenden Beschwerden angegangen werden.[10] Ich bin zuversichtlich, dass wir diesbezüglich demnächst eine potenzielle Lösung sehen werden.

Materiell rechtlich wird sich in naher Zukunft wohl nicht viel tun. Der endgültige Text der DSGVO war hart umkämpft und man will das Gesetz nicht wieder „***öffnen***“. Die Gerichte werden jedoch die vielen noch offenen Auslegungsfragen Stück für Stück klären.

Entwicklungen der Digitalisierung werden vornehmlich wohl mit neuen Gesetzen geregelt werden, wie beispielsweise das Gesetz über Künstliche Intelligenz (KI-Act) und das Datengesetz (Data-Act). Die DSGVO und diese Gesetze werden sich ergänzen. Europa ist für Digitalisierung bereit!

„Europa ist für Digitalisierung bereit!“

Die Beratung Pilleum hat einen datenschutzrechtlichen Fokus und umfasst Dienstleistungen wie Rechtsgutachten, die datenschutzrechtliche Begleitung von Projekten wie Produktentwicklungen, Datenschutz-Folgenabschätzungen, Trainings und Fortbildungen, sowie die Tätigkeit als externer Datenschutzbeauftragter. Zudem werden betroffene Personen bei Beschwerden wegen Datenschutzverletzungen unterstützt.

10 Vgl. dazu: EDSA nimmt „Wunschliste“ verfahrensrechtlicher Aspekte, das erste EU-Datenschutzsiegel und eine Erklärung zum digitalen Euro an, hier abrufbar (Stand: 29.01.2023).

Weiterführende Hinweise

- Übersicht zu DSGVO-Bußgeldern und Schadensersatz: CMS, GDPR Enforcement Tracker, hier abrufbar (Stand: 29.01.2023)
- *Wybitul*/Jacquemain, DSGVO Schadensersatztabelle, hier abrufbar (Stand: 29.01.2023)

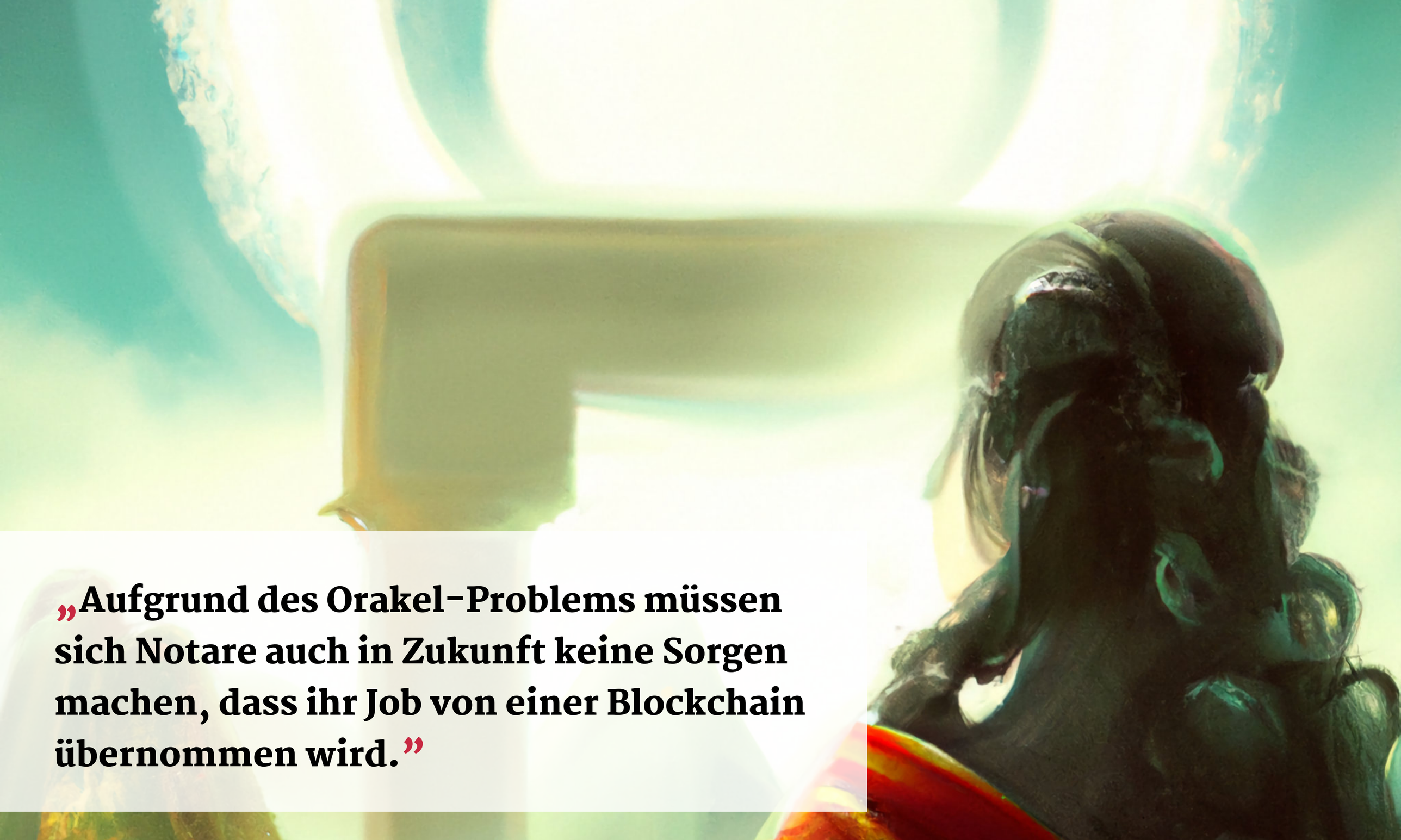
Zurück zum Inhaltsverzeichnis



Ferdinand ist Jurastudent an der Universität zu Köln und Head of CTRL im LTLC. Neben dem Studium beschäftigt er sich insbesondere mit Technologien wie Blockchain, KI und IoT sowie ihren rechtlichen und regulatorischen Implikationen.

Philipp studiert Jura an der Universität Freiburg und hat den Schwerpunkt Grundlagen des deutschen, europäischen und internationalen öffentlichen Rechts absolviert. Er interessiert sich besonders für öffentliches Recht, Rechtstheorie und Rechtsvergleichung sowie Völkerrecht.

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.



„Aufgrund des Orakel-Problems müssen sich Notare auch in Zukunft keine Sorgen machen, dass ihr Job von einer Blockchain übernommen wird."

Kolumne

Das Orakel-Problem oder: Warum Blockchains keine guten Notare sind

Roman Reher

Open Peer Review

Dieser Beitrag wurde lektoriert von:
Ferdinand Wegener & Jonas Neubert

Roman Reher (auch bekannt als ‚Blocktrainer') ist ein deutscher Informatiker, Bitcoin-Educator und Content-Creator. Sein YouTube-Kanal ‚Blocktrainer' ist mittlerweile einer der weltweit größten Kanäle mit Bitcoin-Fokus.

René Ackermann ist bei Blocktrainer.de für die Inhalte der Seite verantwortlich. Er verfasst News- und Wissensbeiträge, moderiert einen Podcast und berät Privatpersonen und Unternehmen zu allen Bereichen rund um Bitcoin.

„*Vergesst Bitcoins – die Zukunft heißt Blockchain.*"
„Man muss nicht an den Bitcoin glauben, um in die Blockchain zu investieren". „Bitcoin ist veraltet, es gibt ja schon neuere Blockchains". Solche und ähnliche Sprüche hat vermutlich jeder, der sich mit Distributed Ledger Technologies oder sogenannten Kryptowährungen beschäftigt, schon mehrfach gehört.

Bereits seit einigen Jahren und besonders in den beiden ‚Hype-Phasen' in den Jahren 2017/2018 und 2020/2021 konnte man zahlreichen Medien entnehmen, dass die Erfindung der Blockchain-Technologie unsere Welt verändern wird und dass diese gekommen ist, um zu bleiben. Egal ob Tech-Branche, Finanzindustrie oder sogar die Rechtswissenschaften, die Blockchain wird alle Bereiche unseres Alltags erfassen, so waren sich die Experten einig. Es brach eine regelrechte Blockchain-Manie aus.

Einige Unternehmer nutzten diesen Hype, ähnlich wie die ***Dotcom-Bubble*** in den 2000ern, direkt zu ihrem geschäftlichen Vorteil aus. So etwa der Eistee-Produzent ***Long Island Iced Tea Corp.*** aus New York. Die Führungsetage der Firma erkannte den Wahn, der von dem Buzzword ‚Blockchain' in vielen Menschen ausgelöst wird und benannte sich kurzerhand in ***Long Blockchain Corp***. um.[1] Der gewünschte Effekt ließ nicht lange auf sich warten. Der Aktienwert des Unternehmens stieg zwischenzeitlich um fast 500 %, obwohl sich an den Geschäftsprozessen oder Verkaufszahlen nichts geändert hatte.

A. Bitcoin statt Blockchain

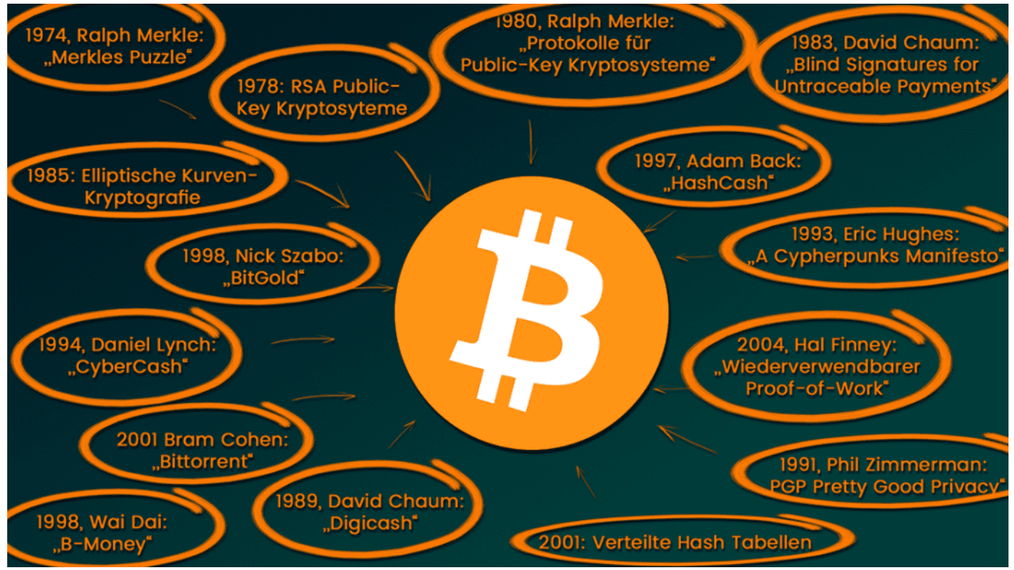
Während für viele Menschen der Begriff ‚Blockchain' eng mit ‚Bitcoin' verknüpft ist und teilweise sogar synonym verwendet wird, gibt es andere, die aus voller Überzeugung behaupten: „***Bitcoin ist eine veraltete Technologie, aber Blockchain wird die Welt verändern***". Interessanterweise wird das Wort ‚Blockchain' im berühmten Bitcoin-Whitepaper[2] kein einziges Mal erwähnt und nicht überall wo ‚Blockchain' draufsteht, ist auch wirklich ‚Blockchain' drin.

Weiter macht aber auch nicht in jedem Fall, in dem eine Blockchain für die Umsetzung einer Anwendung verwendet wird, dies tatsächlich Sinn. Blockchains sind hergebrochen im Grunde langsame Datenbanken, deren Technologie weder neu noch bahnbrechend ist. Tatsächlich gehen die ersten Überlegungen dazu bis in die 1970er Jahre zurück.

„Nicht in jedem Fall, in dem eine Blockchain für die Umsetzung einer Anwendung verwendet wird, macht dies tatsächlich Sinn."

Oft wird Bitcoin als die erste Blockchain, das erste digitale Geld oder auch die erste Kryptowährung betitelt. Genau genommen ist dies aber nicht korrekt, da bereits in den 1990er Jahren erste Kryptowährungen konzipiert wurden. Leider hatten diese aber mit verschiedenen Problemen zu kämpfen, die deren Sicherheit und Nutzbarkeit beeinflussten. ***Satoshi Nakamoto***, dem Erfinder von Bitcoin, gelang es im Jahr 2008 jedoch, diese Probleme zu beheben und Bitcoin zum ersten sicheren und limitierten digitalen Gut der Welt zu machen. Er verknüpfte geschickt bekannte Konzepte und ihm gelang es durch einen Energieaufwand in der physischen Welt eine digitale Knappheit zu erzeugen. Dies ist der eigentliche Durchbruch, der mit dem Start des Bitcoin-Netzwerks einherging.

1 *Gründerszene*, Eistee-Hersteller nennt sich in Blockchain um und lässt Aktie explodieren, hier abrufbar (Stand: 29.01.2023).
2 *Satoshi Nakamoto* (Pseudonym), Bitcoin: A Peer-to-Peer Electronic Cash System, hier abrufbar (Stand: 29.01.2023).



Bitcoin ist eine Komposition aus vielen älteren Konzepten. Quelle: blocktrainer.de

Die Erzeugung von digitaler Knappheit dient allerdings der Lösung von Problemen in einem sehr spezifischen Anwendungsfall, der Schaffung eines monetären Systems im virtuellen Raum. Diese Knappheit, und damit die technische Umsetzung über die Blockchain, wird in vielen anderen Fällen aber überhaupt nicht gebraucht und kann im Gegenteil zur Zweckerreichung sogar hinderlich sein.

Oft werden Zensurresistenz und Unveränderbarkeit ebenfalls als zentrale Eigenschaften von Blockchains genannt. Einmal davon abgesehen, dass man diese auch ohne eine Blockchain sicherstellen könnte, läuft man bei der Verknüpfung von der physischen und der digitalen Welt aber immer in das sogenannte ‘Orakel Problem’.

B. Was ist das Orakel-Problem?

Das Orakel-Problem bezieht sich auf die Herausforderung, wie man in eine Blockchain vertrauenswürdige Informationen von außerhalb, also aus der ‚realen Welt’, einspeisen kann. Grundsätzlich bezeichnet ein Orakel, lateinisch von ***oraculum*** für ‚Götterspruch’, eine Offenbarung oder Erkenntnis, die mittels der Befragung einer höheren Instanz – etwa einer Gottheit – gewonnen wurde.

Ein Orakel ist in diesem modernen Fall ein Mittelsmann, der entweder eine externe Datenquelle abfragt oder eine externe Schnittstelle aufruft, um aktuelle Informationen zu erhalten. Es muss jedoch sichergestellt werden, dass dieses Orakel, sei es eine staatliche oder private Quelle, vertrauenswürdig ist und dass die gelieferte Informationen wirklich unverfälscht und korrekt sind.

Das berühmteste Beispiel ist das antike Orakel von Delphi am Hang des Berg Parnass in Griechenland

Ein Anwendungsbeispiel könnte etwa ein Smart Contract sein, der auf Basis der Durchschnittstemperatur in einer Region die monatlichen Raten anpasst, die Kunden einer Versicherung für den Schutz vor Sturmschäden zahlen müssen. Selbst wenn dieser Smart Contract nun vollständig auf der Blockchain abgebildet wäre, so müsste er sich bei der Umsetzung externer Wetterdaten bedienen, die außerhalb der Blockchain stehen. Diese Wetterdaten müssten von Wetterstationen geliefert werden, auf die sich der Smart Contract und seine Nutzer wiederum verlassen müssten.

Einige Lösungen für das Orakel-Problem beinhalten die Verwendung von mehreren Orakeln, welche ihre Ergebnisse miteinander vergleichen und abstimmen, bevor sie bestätigt werden. Dies ist zwar für einige Anwendungsfälle eine zufriedenstellende, aber für wirklich wichtige Daten keine gute Lösung, denn auch hier ist Verfälschung möglich und Vertrauen in die Verlässlichkeit der Orakel notwendig. Bis dato ist es nicht möglich, Daten aus der Realwelt völlig vertrauensfrei in die digitale Welt und dementsprechend auch in Blockchains zu übertragen.

C. Die Blockchain als Notar?

Das Orakel-Problem ist auch der Grund dafür, warum sich beispielsweise Notare keine Sorgen machen müssen, dass ihr Job bald von einer (staatlichen) Blockchain übernommen wird. Unter dem Begriff ‚Tokenisierung' träumen einige Blockchain-Enthusiasten davon, dass bald Grundstücke und Immobilien, aber auch Vermögenswerte wie Kunst, Uhren oder Oldtimer in Form von sogenannten Nicht-Fungiblen-Token (NFTs) auf einer Blockchain dargestellt und repräsentiert werden können. Wer Halter des jeweiligen Tokens ist, soll dann auch automatisch Eigentümer des Vermögenswertes in der realen Welt sein. Wird ein Token über die Blockchain auf einen anderen Eigentümer übertragen, dann werden die Eigentumsverhältnisse überprüfbar verändert, so zumindest die Wunschvorstellung.

> „Notare müssen sich keine Sorgen machen, dass ihr Job bald von einer (staatlichen) Blockchain übernommen wird."

Einmal davon abgesehen, dass das deutsche Rechtssystem ohnehin noch nicht dafür ausgelegt ist und Notare, Grundbuchämter und Co. noch weitere Aufgaben (z.B. Beratungs- und Warnfunktion) erfüllen, stößt man bei der Tokenisierung von realen Objekten wieder auf das Orakel-Problem. Wer garantiert, dass die Daten zu einem Haus oder Grundstück auch tatsächlich korrekt sind, wenn sie in die Blockchain aufgenommen werden? Was passiert, wenn Token-‚Besitzer' ihre sogenannten ‚privaten Schlüssel',[3] also den Zugang zum jeweiligen Token verlieren? Muss das tokenisierte Haus dann abgerissen werden? Was ist, wenn mein Eigenheim-NFT durch einen Hack gestohlen wird? Muss ich dann ausziehen? Schlussendlich muss man sich bei all diesen Fragen wieder auf zentrale Instanzen verlassen. Den Blockchain-Hokuspokus hätte man sich demnach von Anfang an sparen können. Die erhoffte Disruption der Grundbuch- und Immobilienbranche wird wohl noch lange Zeit ein Traum bleiben und damit der Beruf des Notars auch in den kommenden Jahren sicher vor digitaler Konkurrenz sein.

3 *Blocktrainer*, Was sind Private & Public Keys?, hier abrufbar (Stand: 29.01.2023).

Roman fasst komplexe technische und ökonomische Sachverhalte in leicht verständliche Worte zusammen. Er war zudem mehrfach als Experte für diverse Medienformate tätig. Der ***Blocktrainer*** und sein Team stellen kontinuierlich aktuelle Bitcoin-Inhalte für ein deutschsprachiges Publikum bereit.

BLOCKTRAINER

YouTube

Reinhören lohnt sich:
Der Blocktrainer Bitcon Podcast

Zurück zum Inhaltsverzeichnis

Kolumne

Wie begeistert man für Legal Tech? – Start-up-Förderung mit dem Legal Tech Colab

Victor Monsees

Open Peer Review

Dieser Beitrag wurde lektoriert von:
Ferdinand Wegener & Jonas Neubert

Victor Monsees ist Diplom-Jurist und arbeitet als Venture Manager für das Legal Tech Colab. Zudem studiert er Legal Technology (M. Sc.) an der University of Law und verfasst derzeit seine Masterarbeit über die Regulierung von KI-Modellen in der Rechtsbranche.

Wie begeistert man Studierende für Legal Tech? – Diese zentrale Frage, stellte ich mir, als ich am 20. September 2022 die Aufgabe bekam, für unser neues ***Legal Tech Colab*** die erste Legal Tech Challenge zu veranstalten. Erst eine Woche zuvor war das ***Legal Tech Colab*** feierlich eröffnet worden.

Das **Legal Tech Colab** unterstützt als domainspezifischer Inkubator innovative Start-ups, deren Geschäftsmodell sich im Kern mit Verträgen, (Vermögens-) Rechten, Normen oder gesetzlich determinierten Abläufen befasst. Wir unterstützen dabei ausschließlich Start-ups, deren Geschäftsmodell auf neuester Technologie basiert und skalierbar ist.

Wir helfen den Teams in ihrer Pre-Seed- und Seed-Phase: Von der Analyse der Kundenbedürfnisse und des jeweiligen Markts, der Entwicklung eines Prototyps, Matching mit passenden Co-Gründenden, bis hin zur Finanzierung des Start-ups mit Venture-Capital. Die Start-ups können auf eine in dieser Form einmalige Natural-Language-Processing-Plattform zugreifen, die speziell mit deutschen Rechtsdokumenten trainiert wird und erhalten ein Stipendium sowie Arbeitsplätze. In Netzwerkveranstaltungen bringt das **Legal Tech Colab** Start-ups aus anderen Branchen zusammen und stellt ihnen Mentor:innen von Venture-Capital-Fonds, Großkanzleien oder Unternehmen an die Seite.

Die Gründenden profitieren von dem Know-how aus 20 Jahren Entrepreneurship- und Tech-Förderung von UnternehmerTUM, Europas größtem Zentrum für Innovation und Gründung. Georg Eisenreich, Tech-Enthusiast und bayerischer Justizminister, initiierte 2022 den Inkubator und fand mit **UnternehmerTUM** [hier] einen perfekten Partner für die Gründung des **Legal Tech Colabs**, welches seither auch maßgeblich durch das Bayerische Staatsministerium für Justiz [hier] gefördert wird.

Jedes Semester organisiert ***UnternehmerTUM***, Europas erfolgreichstes Gründungs- und Innovationszentrum, sog. Tech Challenges, bei denen Studierende die Möglichkeit erhalten, in interdisziplinären Teams eine ihnen gestellte Herausforderung in verschiedenen Sektoren wie Robotics, Aerospace oder Biotech eigenständig zu lösen. Die Challenges werden von den jeweiligen Industriepartnern und zusammen mit den domainspezifischen Inkubatoren von ***UnternehmerTUM*** gestellt und betreut. Hier ist neben den ***TUM Venture Labs*** auch das ***Legal Tech Colab*** einer dieser domainspezifischen Inkubatoren. In dem dreimonatigen Programm lernen die Teilnehmenden einerseits, als Team zu agieren und andererseits das unternehmerische Handwerkszeug. Am Ende wird ein Siegerteam gekürt und es winken neben einem Preis auch vor allem die Förderung des jeweiligen Inkubators. Wir als ***Legal Tech Colab*** würden nun also zum ersten Mal solche Challenges veranstalten. Dabei fühlte sich unser Inkubator für mich selbst noch wie ein Start-up an. Es existierten keine festgefahrenen Strukturen, was uns die seltene Chance gab, alles neu zu denken und die Tech Challenge nach unserer Vision zu formen.

Beim Kickoff der Tech Challenge pitcht jeder Inkubator den Studierenden ihre spezifische Challenge und versucht sie davon zu überzeugen, sich dieser die nächsten drei Monate zu widmen. Meine erste Aufgabe war es also, mir zwei möglichst interessante und passende Legal Tech Challenges zu überlegen. Eine kurze Recherche ergab ehemalige Challenges wie “3D Printing of Houses” oder “Iron Man Suit”. Dagegen würden unsere Legal Tech Challenges wohl ankommen müssen. Bisher hatten stets vor allem Studierende aus technischen Fachrichtungen wie Informatik oder Maschinenbau teilgenommen. Meine Aufgabe war es also, auch Studierende ohne rechtlichen Bezug für die Digitalisierung und Automatisierung der Juristerei zu begeistern.

Die erste Idee für eine Challenge steuerte unser Managing Director Stefan Blenk bei: „Digitalize legal aid“, also die Digitalisierung des Prozesskostenhilfeantrags. Der derzeitige Prozesskostenhilfeantrag ist völlig überfrachtet, nur auf Deutsch und vor allem ausschließlich analog beantragbar. Gerade jene, die Prozesskostenhilfe am nötigsten haben, um für ihre eigenen Rechte zu kämpfen, kann das abschrecken und an einer erfolgreichen Beantragung hindern. Dies zu ändern, war das Ziel der ersten Challenge.

Während ich nach geeigneten Themen für die zweite Challenge suchte, fiel mir ein, dass es bezüglich der in Deutschland begangenen Straftaten immer noch eine hohe Dunkelziffer gibt. Die deutsche Anzeigenstatistik, die ich daraufhin studierte, zeigte deutlich, wie groß die Diskrepanz zwischen den begangenen und den angezeigten Straftaten derzeit noch ist.[1] Besonders frappierend ist die Lücke bei Sexualdelikten und Delikten, die im Internet begangen werden. Über die Gründe gab die Studie ebenfalls Auskunft: Mangel an Wissen und Deutschkenntnissen sowie Scham waren häufig der Grund, sich nicht an die Polizei oder Staatsanwaltschaft zu wenden. Ich war mir sicher, dass Technologie hier das Potenzial hat, Opfer zu unterstützen und dabei zu bestärken, sich für Hilfe an den Staat zu wenden. Damit lautete der Titel der zweiten Challenge: „*Low-threshold for victims of crime*", also ein niederschwelliger digitaler Assistent für Opfer von Straftaten.

Einige Tage nachdem ich bei der Kickoff-Veranstaltung unsere Challenges vorgestellt hatte, wurde zu unserer Überraschung klar, dass über 25 % der Teilnehmenden unsere beiden Challenges gewählt hatten und bereit waren, sie zu lösen. Das Interesse an Legal Tech war also erheblich.

A. Wie also begeistert man Studierende für Legal Tech?

Ich glaube, die Antwort ergibt sich aus den Gemeinsamkeiten unserer beiden Challenges. Erstmal haben beide einen sozialen Mehrwert. Technik kann genutzt werden, um den Zugang zum deutschen Rechtssystem für alle zu verbessern. Mangelnde Kenntnisse oder Sprachvermögen können durch digitale Anträge überwunden werden. Anonyme digitale Assistenten können Opfern von Straftaten den Mut und das Wissen geben, um ihre Rechte selbstbewusst zu verfolgen.

Außerdem ist der deutsche Legal Tech Markt noch in seinen Anfängen. Es bietet sich deshalb die Möglichkeit, der oder die erste zu sein und etwas völlig Neues zu schaffen, während dies in anderen Branchen oft nur noch selten möglich ist.

1 Sicherheit und Kriminalität in Deutschland – SKiD 2020, hier abrufbar (Stand: 31.01.23).

B. Wie wird aus einer Idee ein Prototyp?

Damit begannen wir also unsere Tech Challenges. Gleich zu Anfang wurde klar: Nahezu niemand, der oder die unsere Legal Tech Challenges gewählt hatte, verfügte über einen juristischen Hintergrund. Zudem waren viele Teilnehmende ausländische Masterstudierende, die bisher keinen persönlichen Bezug zum deutschen Rechtssystem gehabt hatten.

Ich entschloss mich also, für die ersten Treffen mit den Teams eine kurze, allgemeine Einführung in das deutsche Rechtssystem vorzubereiten. Dinge, die mir durch das lange Jurastudium zur Selbstverständlichkeit geworden sind, erschienen mir dabei plötzlich in neuem Licht. Wie funktioniert der juristische Syllogismus? Wie wird eine Meinung zur herrschenden und warum ist das wichtig? Was unterscheidet unsere

Abb. 1: Phasen der Tech Challenge (Quelle: Legal Tech Colab)

Codex Tradition mit ihren umfassenden Gesetzen vom angelsächsischen Common Law, das vor allem auf Case Law basiert?

Als ich begann zu erzählen, dass man Prozesskostenhilfeanträge nur auf einem deutschen Papierformular per Post (oder zu Protokoll bei der Geschäftsstelle) einreichen kann, erntete ich ungläubige Gesichter – ich merkte mal wieder: Die deutsche Verwaltung hat noch viel Digitalisierung aufzuholen. Schon kurz danach begannen die Studierenden bei verschiedenen Workshops gemeinsam das Gründungshandwerk zu erlernen (vgl. Abb. 1). Ihr erstes Ziel war es, bis zu den "Midterm-Meetings", die einen Monat später folgen würden, als Team zu funktionieren und ihre Konzepte für den späteren Prototyp festzulegen.

Da die Justiz und der Rechtsbereich im Ganzen von außen nur schwer zu verstehen und einzuschätzen sind, entschloss ich mich, für die Studierenden vorher noch ein „Expertenmeeting" zu veranstalten. Um ihnen die Möglichkeit zu geben, Experten aus der Praxis Fragen zu stellen und dabei ihre Konzepte zu validieren. Dafür konnte ich die zwei erfahrenen Mitglieder der Justiz und Legal Tech-Enthusiasten Johannes Obenauf und Dr. Derk Strybny gewinnen.

Die Experten-Meetings lieferten den Studierenden Erkenntnisse, die sich nur aus dem Kontakt zur Praxis ergeben können. So zum Beispiel, dass für die digitalen Assistenten wie Chatbots sichergestellt werden muss, dass diese nicht durch Suggestivfragen die Aussagen der Opfer beeinflussen, bevor sie mit der Polizei sprechen. Ebenso wichtig war für die Teams das Bewusstsein, dass gerade die Menschen, denen wir mit beiden Challenges helfen wollen, oft keine Laptops oder Desktop-PCs besitzen, sondern meist ausschließlich Handys. Anwendungen müssen also mobil erreichbar sein, am besten über Browser-Anwendungen. Beide Experten verwiesen immer wieder darauf, dass nicht nur der Inhalt wichtig ist, sondern vor allem auch der Tonfall. Empathische und einfach verständliche Sprache kann einen zentralen Beitrag leisten, dass juristische Anwendungen tatsächlich für jeden nutzbar werden.

Begleitet von diesen Eindrücken stellten mir die Teams schon einige Tage später ihre Konzepte in den Midterm-Meetings vor. Immer wieder war ich dabei verblüfft, wie tief die Teams in den wenigen Wochen in das Thema eingestiegen waren und wie weit sie bereits gekommen waren. Viele hatten zum Beispiel schon umfangreiche Interviews mit Betroffenen geführt. Besonders faszinierte mich damals, in welch verschiedene Richtungen sich die Konzepte entwickelt hatten. Für den digitalen Assistenten für Opfer von Straftaten hatte sich ein Team auf Stalking-Opfer spezialisiert, ein anderes auf internationale Studierende, wieder ein anderes hatte sich auf eine beachtliche strafrechtliche "Subsumptionsmaschine" konzentriert. Auch bezüglich der Prozesskostenhilfeanträge gab es verschiedene Lösungswege. Einige hatten sich auf die Bedürfnisse von Anwält:innen fokussiert, wieder andere auf die der Gerichte.

Nach den Midterm-Meetings begannen die Teams, ausgehend von ihren Konzepten und wieder unterstützt von den ***UnternehmerTUM*** Coaches, ihre Prototypen für das Finale Ende Januar auszuarbeiten.

C. Wer überzeugt in der Pitch Night?

Am Ende der drei Monate, war es dann schließlich so weit: Jedes Team stellte der Jury, in der neben mir auch die Experten Derk Strybny und Johannes Obenauf saßen, seinen finalen Pitch vor und präsentierte dabei seinen Prototypen. Für die Teams ging es um viel, jeweils winkten 1.000 Euro Preisgeld sowie eine besondere Unterstützung durch das ***Legal Tech Colab***.

Jedes Team hatte auf seine Weise Tolles erreicht. Sie bewiesen mit ihren kreativen Pitches, wie das Thema Legal Tech mit Leben gefüllt werden kann. Dadurch machten sie es uns als Jury jedoch besonders schwer, eine Entscheidung zu treffen. Am nächsten Tag diskutierten Johannes Obenauf und ich am Telefon derart lange über die Bewertungen, dass wir fast zu spät zu der für den Abend geplanten Abschlussfeier gekommen wären.

An diesem Abend kamen alle 26 Teams der verschiedenen Challenges in den Räumen von ***UnternehmerTUM*** zusammen. Nacheinander stellten alle Partner ihre jeweiligen Challenges vor und verkündeten die Siegerteams. Die Teams erfuhren erst in diesem Moment von ihrem Sieg und hatten dann die Gelegenheit, in einem Elevator Pitch das Publikum von Ihrem Prototyp zu überzeugen, um den "Audience-Award" für den besten Pitch des Abends zu gewinnen.

Nachdem die Teams drei Monate auf diesen Moment hingearbeitet hatten, war die Aufregung bei Teams deutlich zu spüren und endlich durfte auch ich unsere Gewinner:innen verkünden: Die erste Challenge "Digitalize legal aid" gewann Team ***LegalAiders***: Ihre Lösung leitet die Nutzer:innen durch eine intelligente Fragenliste, an deren Ende ein vollständig ausgefülltes Antragsformular als PDF ausgegeben wird und die nötigen Nachweise bereits mit anhängt. Die App lässt sich in Deutsch, Englisch, Türkisch und Ukrainisch bedienen. Neben dem funktionierenden Prototyp überzeugte uns insbesondere auch die Energie des Teams. Als das ***ZOOM***-Meeting für den finalen Pitch losging, stand das ganze Team bereits gemeinsam in einem Raum vor der Kamera. Wir merkten sofort, sie brannten darauf, endlich loszulegen.

Bei unserer zweiten Challenge "Digital assistant for victims of crimes" gewann Team ***Rannstein*** mit ihrer App "Lilo". Die Anwendung führt mit empathischer Sprache durch eine erste rechtliche Einschätzung der Lage. Sie gibt daraufhin Hilfestellungen zum anstehenden Polizeiprozedere und erinnert im Fall von Gewalt-/Sexualdelikten an wichtige Schritte, wie nach Möglichkeit frühzeitig zur Beweissicherung eine:n Ärzt:in aufzusuchen. Außerdem beinhaltet die Anwendung eine Datenbank von Hilfsorganisationen wie dem ***Weißen Ring***, damit Opfer auch anderweitig Betreuung und Unterstützung finden können. Bei dem finalen Pitch merkten wir, wie sehr sich das Team in die tatsächlichen Bedürfnisse der Opfer eingefüllt hatte, diese Empathie und Praxisnähe überzeugten uns.

Beiden Teams war ihre Freude und Überraschung deutlich anzusehen, als sie sich für ihre Sieger-Pitches vor der Menge sammelten. Entsprechend sprühten beide Pitches dann auch noch ein letztes Mal vor Enthusiasmus. Für mich wurde nochmal richtig deutlich, dass Legal Tech trotz seiner Abstraktheit und Komplexität eben oft sehr menschliche Themen betrifft.

Am Ende des Abends dann noch einmal große Spannung: das Publikum wählte aus allen Pitches den besten aus. Auf dem Bildschirm stiegen die gezählten Stimmen unaufhörlich nach oben. Am Ende wurde klar: ***LegalAiders*** gewinnt den Audience-Award! Ihre Energie hatte nicht nur uns als Jury, sondern auch das Publikum angesteckt – besser hätte unsere erste Tech Challenge des ***Legal Tech Colab*** nicht enden können.

Abb. 2: Team LegalAiders (Quelle: Legal Tech Colab)

Abb. 3: Team Rannstein (Quelle: Legal Tech Colab)

D. Was mich die Studierenden über den Stand von Legal Tech in Deutschland gelehrt haben

Die Arbeit mit den Studierenden hat mir stark verdeutlicht, wie wichtig die Arbeit des ***Legal Tech Colab*** ist. Die deutsche Justiz und Rechtsbranche hängt in der Digitalisierung deutlich hinterher. Ausländische Studierende können nicht fassen, dass wichtige Anträge per Post erledigt werden müssen. Ich bin froh, ihnen nicht noch erklären zu müssen, dass bis vor kurzem Faxgeräte in deutschen Gerichten noch der Standard war. Auch wird mir bewusst, dass für viele Studierende in technischen Bereichen der Begriff "Legal Tech" höchstens am Rande bekannt ist und sie diesen Bereich vorher noch nicht in Betracht gezogen haben. Das ist schade, da gerade der Legal Tech Bereich ein faszinierendes Testfeld für neueste Technologien wie Natural-Language-Processing oder Blockchain-Anwendungen bietet.

Gleichzeitig hat mich unsere Tech Challenge sehr optimistisch bezüglich der Zukunft der deutschen Rechtsbranche gestimmt. Die Studierenden sind engagiert und voller Elan. Sozialer Nutzen ist für sie bedeutsam bei der Frage, welchen Projekten sie ihre Zeit widmen. Sobald die Berührungsängste zum Thema Legal Tech abgebaut sind, entzündet sich große Begeisterung für die schier unendlichen Anwendungsalternativen von Technologie zur Lösung rechtlicher Probleme bei den Studierenden. Viele der Studierenden fragten mich nach dem Finale, welche Möglichkeiten unser ***Legal Tech Colab*** bietet, um aus den Projekten echte Start-ups werden zu lassen.

Dass eines unserer Teams mit einem Pitch über juristische Antragsverfahren gegen Software zu selbstfahrenden Autos oder smartem Städtebau, vor einem jungen Publikum nicht nur bestehen, sondern sogar gewinnen konnte, macht für mich eines besonders klar: Die Absolvent:innen der Tech Challenge haben sowohl den Willen als auch das Potenzial zur Disruption der deutschen Rechtsbranche.

Ihr möchtet Teil dieses Wandels werden und an der nächsten Tech Challenge teilnehmen? Ihr seid an einer Gründung interessiert oder bereits selbst Gründer:in? Ihr würdet gerne als Mentor:in unsere Start-ups unterstützen oder ihr wollt einfach mehr über Legal Tech erfahren?

Dann meldet euch bei mir unter: victor.monsees@unternehmertum.de oder besucht unsere Webseite.

Zurück zum Inhaltsverzeichnis

LEGAL REVOLUTION
EMPOWERING LEGAL PROS
3. + 4. Mai 2023 NürnbergMesse

EUROPAS WEGWEISENDE KONGRESSMESSE FÜR DIE GESAMTE RECHTS- UND COMPLIANCE BRANCHE

#LEGALREVOLUTION #LEGALTECH #LR23

Hochkarätige Keynotes, Expertenvorträge und Workshops
Hotspot für alle Experten entlang der gesamten Wertschöpfungskette
Erleben Sie auf der Messe die neuesten Innovationen der Branche

3. + 4. Mai in der NürnbergMesse

edra MEDIA

+49 69 3487 920-92
info@legal-revolution.com

Tickets und weitere Informationen unter
www.LEGAL-REVOLUTION.com

Kolumne

Die Einwilligungserklärung – Der Stein der Weisen!

Dr. Inka Knappertsbusch

Open Peer Review

Dieser Beitrag wurde lektoriert von: David Wasilewski & Jagjit Sahota

Dr. Inka Knappertsbusch LL.M. ist Senior Associate bei CMS Hasche Sigle in Köln. Sie berät Mandanten insbesondere in arbeits- und datenschutzrechtlichen Themen im Rahmen internationaler Restrukturierungen. Als Mitherausgeberin des Buches „Arbeitswelt und KI 2030“ und Mitglied der Robotics & AI Law Society bildet auch Künstliche Intelligenz im Arbeitsumfeld einen Ihrer Beratungsschwerpunkte.

Jeder und jede ist im Alltag häufig mit datenschutzrechtlichen Einwilligungen konfrontiert. Kuß[1] hat in seiner Kolumne die Probleme der Einwilligung und die damit verbundenen praktischen und rechtlichen Herausforderungen – wie etwa das Desinteresse der Betroffenen bei der Vielzahl an erforderlichen Einwilligungserklärungen im Internet – dargestellt.

1 Kuß, CTRL 1/22, 10.

Gleichwohl lässt sich aber unter Berücksichtigung dieser Herausforderungen gerade in Beschäftigungsverhältnissen ein praktisches Bedürfnis für die Einwilligung nicht leugnen.[2] Dies gilt besonders in Betrieben ohne Betriebsrat, so dass eine Betriebsvereinbarung als Rechtsgrundlage der Datenverarbeitung ausscheidet. Im Vergleich zu den anderen Erlaubnistatbeständen der Datenschutzgrundverordnung (DSGVO) bietet die Einwilligung besondere Vorteile, die sowohl Beschäftigte als auch Arbeitgeber zu schätzen wissen. Um deren Interessenlagen in Bezug auf die Einwilligung verstehen zu können, wird im Folgenden ein Überblick über die Vorzüge der Einwilligung gegeben.

Art. 7 Abs. 1 DSGVO: „Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.“

A. Hohes Maß an Rechtssicherheit

Die Einwilligung eignet sich vor allem deswegen als Mittel für die Rechtfertigung der Datenverarbeitung, weil sie für alle Beteiligten ein vergleichsweise hohes Maß an Rechtssicherheit schafft. Da die Möglichkeit von hohen Bußgeldern bei Datenschutzverstößen besteht, liegt es im besonderen Interesse des Verantwortlichen (im Beschäftigungsverhältnis des Arbeitgebers), Rechtssicherheit in Bezug auf die Wirksamkeit der Verarbeitung zu gewährleisten. Auch die Beschäftigten haben ein Interesse daran, dass ihre personenbezogenen Daten rechtmäßig verarbeitet werden. Eine rechtssichere Lösung schützt also auch ihre Interessen. Bei einer Einwilligung können sie die Rechtmäßigkeit durch die Reichweite ihrer Einwilligungserklärung und einem etwaigen Widerruf dabei vergleichsweise einfach kontrollieren.

2 Riesenhuber, RdA 2011, 257 (265).

Trotz der Möglichkeit dieses Widerrufs kann die Einwilligung als rechtssicher angesehen werden.[3] Denn bei einer wirksamen Einwilligung kommt es – anders als bei den anderen Erlaubnistatbeständen – nicht auf eine Erforderlichkeitsprüfung an.[4] Bei einer Erforderlichkeitsprüfung besteht die Gefahr, dass die Verhältnismäßigkeitsabwägung fehlerhaft durchgeführt wird.[5] Wird ein solcher Fehler begangen, ist die Datenverarbeitung unwirksam, wenn sich der Verantwortliche nicht auf eine andere Verarbeitungsgrundlage berufen kann.

„Die Einwilligung eignet sich vor allem, weil sie für alle ein hohes Maß an Rechtssicherheit schafft.“

Der Widerruf ist – gerade im Beschäftigungsverhältnis – nur von geringer Relevanz. Denn in der Regel werden die Beschäftigten die Einwilligung nur dann widerrufen, wenn das Beschäftigungsverhältnis beendet wird oder die Gründe, die zur Einwilligung führten, nicht mehr vorliegen. Abgesehen davon fehlt es an Motiven, die Einwilligung zu widerrufen. Die Anzahl der widerrufenen Einwilligungen wird daher im Vergleich zu der Gesamtzahl der erklärten Einwilligungen nur einen sehr kleinen Anteil ausmachen.

3 Buchner/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, DSGVO Art. 7 Rn. 9; Schmidt, Datenschutz, S. 298; Forst, RDV 2010, 150 (154); Hoeren, VersR 2005, 1014 (1018).
4 Albers/Veit, in: Wolff/Brink, BeckOK-DatenSR, DSGVO Art. 6 Rn. 22; Golland, MMR 2018, 130; Veil, NJW 2018, 3337 (3344).
5 Vgl. Buchner/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, DSGVO Art. 7 Rn. 17.

B. Legitimation weitreichender Datenverarbeitungen

Zudem ermöglicht die Einwilligung die Legitimation von weitreichenden Datenverarbeitungen, die sich anhand von abstrakt-generellen Tatbeständen nur schwierig rechtfertigen lassen. So stellt nur die Einwilligung nicht auf die Erforderlichkeit der Datenverarbeitung ab (Art. 6 Abs. 1 UAbs. 1 DSGVO). Die Einwilligung kann mithin auch sehr weitreichende Formen der Datenverarbeitung legitimieren, bei denen mangels Erforderlichkeit keine anderen Erlaubnistatbestände einschlägig wären.[6] Noch deutlicher wird dies bei der Verarbeitung besonderer Kategorien personenbezogener Daten (etwa: Gesundheitsdaten, ethnische Herkunft oder Gewerkschaftszugehörigkeit), die nur bei Vorliegen von sehr engen Voraussetzungen erfolgen darf (Art. 9 Abs. 2 DSGVO).[7] Diese Voraussetzungen werden bei Arbeitsverhältnissen oft nicht vorliegen, so dass in diesen Fällen häufig nur die Einwilligung die Datenverarbeitung legitimieren kann.

C. Entscheidungshoheit des Betroffenen

Darüber hinaus liegt nur bei der Einwilligung die Entscheidungshoheit über die Legitimation der Datenverarbeitung bei dem Betroffenen selbst: Er hat die Wahl, ob er sich mit seiner Erklärung für die Verarbeitung entscheidet.[8] Die Rechtmäßigkeit der Datenerhebung hängt also vom Willen des Betroffenen ab und kann von ihm kontrolliert werden.[9]

Auch wenn andere Rechtsgrundlagen fehlen, kann die Datenverarbeitung in einer Vielzahl von Fallgestaltungen vom Beschäftigten gewünscht sein. Als mögliche Interessen nennt das Bundesdatenschutzgesetz (BDSG) rechtliche oder wirtschaftliche Vorteile sowie gleichgelagerte Interessen mit denen des Arbeitgebers

6 Kühling, in: Wolff/Brink, BeckOK-DatenSR, BDSG 2003 [aK], § 4a Rn. 1; Schild, in: Wolff/Brink, BeckOK-DatenSR, DSGVO Art. 4 Rn. 125; vgl. Pohl, Einwilligung, S. 134; vgl. Kollmar/El-Auwad, K&R 2021, 73; Veil, NJW 2018, 3337 (3342).
7 Bühr, K&R 2021, 221 (222).
8 Vgl. auch Sydow, in: Sydow, DSGVO, Einleitung Rn. 74, der vom „zentralen Gestaltungselement der Betroffenen" spricht; Bunnenberg, Datenschutzrecht, S. 164.
9 Schulz, in Gola, DS-GVO, Art. 7 Rn. 3; vgl. Kollmar/El-Auwad, K&R 2021, 73; Veil, NJW 2018, 3337 (3342); Hanloser, DB 2009, 663 (664).

> „Nur bei der Einwilligung liegt die Entscheidungshoheit bei dem Betroffenen selbst."

(§ 26 Abs. 2 S. 2 BDSG). Schon aus dem Wortlaut der Vorschrift (*„kann"*, *„insbesondere"*) ergibt sich dabei, dass es auch darüber hinaus legitime Interessen des Beschäftigten geben kann.[10] Es handelt sich also um eine Art von Regelbeispielen.[11]

D. Fazit

Da die anderen Erlaubnistatbestände der DSGVO im Beschäftigungskontext häufig an der Erforderlichkeit scheitern bzw. die dort erforderliche Verhältnismäßigkeitsprüfung Rechtsunsicherheiten hervorruft, ist die Einwilligung in vielen Fällen die einzige Möglichkeit, eine Datenverarbeitung zu legitimieren. Überdies ist sie aufgrund ihrer weiteren Vorteile die naheliegende Grundlage für die Datenverarbeitung in Beschäftigungsverhältnissen.

Zurück zum Inhaltsverzeichnis

10 Klausch/Grabenschröer, PinG 2018, 135 (139); Wybitul, NZA 2017, 413 (416).
11 LfDI BW, Tätigkeitsbericht 2018, S. 40; *Riesenhuber,* in: Wolff/Brink, BeckOK-DatenSR, BDSG § 26 Rn. 47; *Klausch/Grabenschröer,* PinG 2018, 135 (139).

Data Science meets BGB: Eine Einführung in die juristische Datenvisualisierung

Ihar Nestsiarenia und Christian Hartz

Open Peer Review

Dieser Beitrag wurde lektoriert von:
Ferdinand Wegener & Louis Goral-Wood

Ihar Nestsiarenia ist Lead Machine Learning Engineer, spezialisiert auf die Anwendung und Implementierung von KI-Algorithmen. Er arbeitet für EPAM Systems und entwickelt für Wolters Kluwer. In seiner Verantwortlichkeit liegt die Anwendung von Machine Learning zur Lösung von Information-Retrieval-Problemen.

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

Gesetze sind abstrakt und daher teilweise schwer verständlich. Referenzen auf andere Normen machen dies noch komplizierter. Was passiert aber, wenn man gerade diese Referenzen aus mathematischer Sicht betrachtet und sie visualisiert? Dieser Beitrag widmet sich der Visualisierung aller Zitierungen des BGB und zeigt, dass beide Seiten – sowohl Jurist:innen als auch Informatiker:innen – gewinnen, wenn sie zusammenarbeiten.

In der juristischen Ausbildung als auch in der täglichen Arbeit von Jurist:innen dreht sich vieles um Text: Gerichtliche Entscheidungen oder Kommentare durchgehen, Schriftsätze lesen und verfassen oder der berühmte Blick ins Gesetz.

Auch wenn es auf den ersten Blick nicht so scheint: Alle diese Texte haben gemeinsam, dass sie nicht linear sind. Es gibt Beziehungen innerhalb und außerhalb der Texte. Ein Schriftsatz zitiert eine wichtige BGH-Entscheidung, einen Kommentar oder eine Norm. Eine Entscheidung zitiert eine andere Entscheidung. Normen zitieren andere Normen innerhalb und außerhalb desselben Gesetzes. All diese Verknüpfungen bleiben oftmals unberücksichtigt, weil sie sich hinter dem Text verstecken. Schaut man sich die Bücher des BGB mit einem mathematischen Hintergrund an, so sticht einem die Verwendung der Graphentheorie ins Auge. In der Mathematik ist ein Graph eine mathematische Struktur, die dazu verwendet wird, Verbindungen paarweiser Informationen herzustellen. Jede Beziehung zwischen Objekten in der Welt kann so modelliert und als Graph dargestellt werden. Ein Beispiel hierfür ist ein soziales Netzwerk, bei dem jede Person ein Knoten darstellt und mit anderen Personen Beziehungen eingeht. Wenn wir diese Beziehungen visualisieren, erhalten wir einen Graphen. Sofern Beziehungen zwischen allen Knoten bestehen, nennt man dies ein Netzwerk. Auch Gesetze können als Graph dargestellt werden.

Versuchen wir uns einmal ein Gesetz als Graph vorzustellen:

Im ersten Schritt kann man sich das Inhaltsverzeichnis des Gesetzes anschauen. Diese Informationen können in einer Baumstruktur abgebildet werden. Auch das ist eine Art Graph. Gehen wir einen Schritt weiter: Zwar hilft uns das Inhaltsverzeichnis dabei, zu verstehen, wie das Gesetz aufgebaut ist, aber wir haben noch keine Ahnung, ob und wie Beziehungen der Normen untereinander aussehen.

In Gesetzen gibt es eine Vielzahl von Referenzen. Zitiert eine Norm eine andere Norm oder ein Konzept aus dieser Norm, so kann eine Beziehung zwischen diesen beiden Normen hergestellt werden. Wenn wir alle Beziehungen aller Normen herstellen, so erhalten wir einen Graphen; genauer gesagt, einen gerichteten Graphen (sog. directed Graph). Gerichtet meint hier, dass wir die Richtung des Informationsflusses visualisieren. Im Falle der Norm also: Norm A zitiert Norm B (ausgehend), bzw. Norm C wird von Norm D zitiert (eingehend). Durch diese Unterscheidung und Visualisierung des Informationsflusses kann gezeigt werden, in welche Richtung der Verweis und damit das Einbinden der Information statt findet.

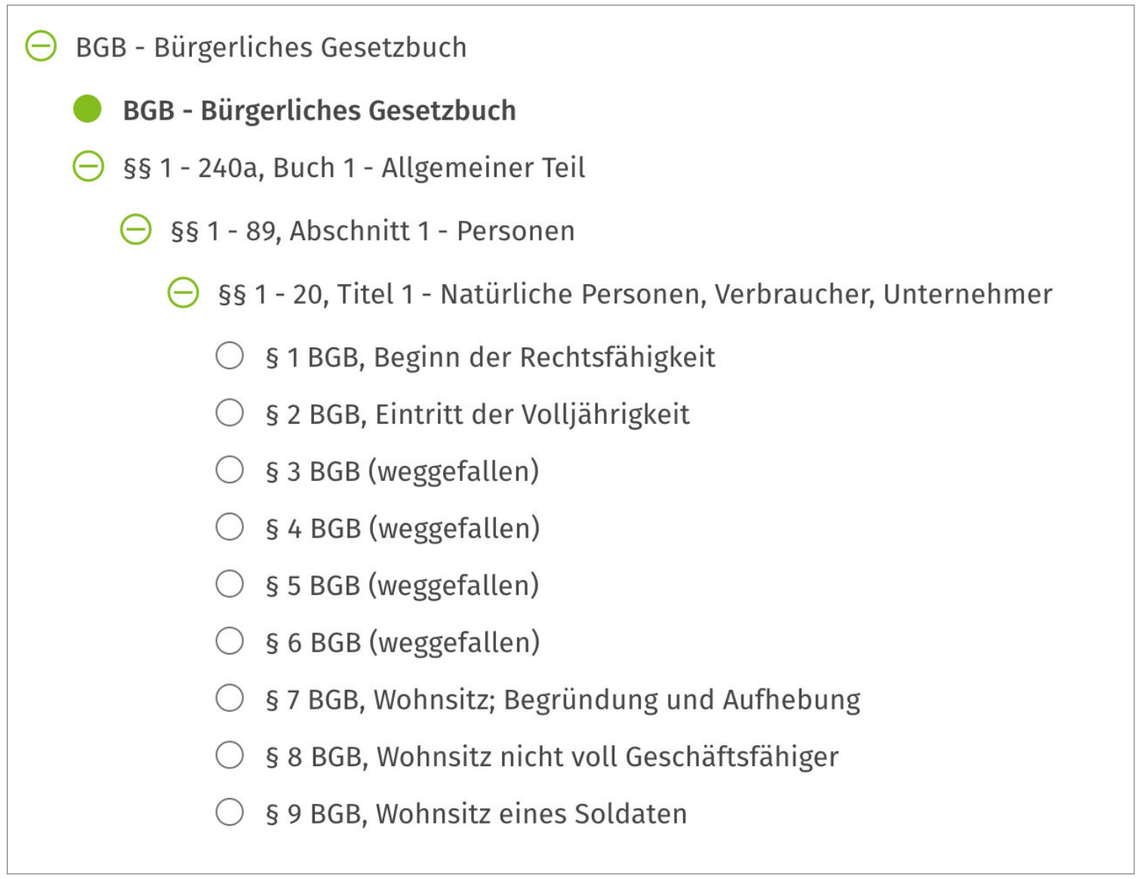


Abb. 1: Inhaltsverzeichnis des BGB aus Wolters Kluwer Online als Baumdiagramm.

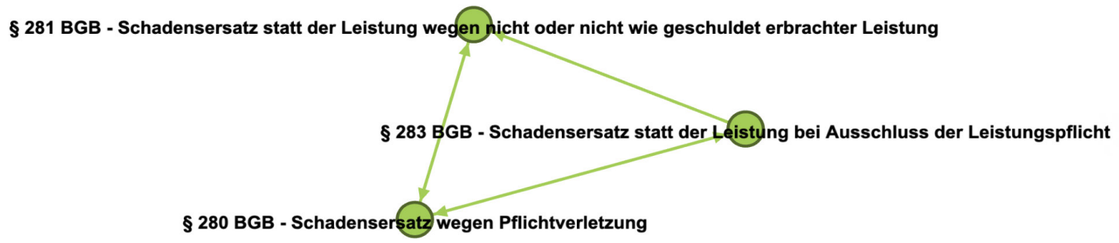


Abb. 2: Dieser Graph stellt dar, dass sowohl § 281 BGB (Knoten) als auch § 283 BGB (Knoten) direkt auf § 280 BGB (Knoten) verweisen (Kanten). § 280 BGB hingegen verweist selbst auch auf § 281 BGB und § 283 BGB. § 281 BGB hingegen verweist nicht auf § 283 BGB.

Hier sieht man eine einfache Visualisierung einer Norm, die selbst zitiert wird (§ 280 BGB). Die Norm wird als Kreis dargestellt und wird in der Regel als Knoten oder Ecke bezeichnet. Die Verbindungslinien, die bei einem gerichteten Graphen als Pfeil dargestellt werden, sind die sog. Kanten. Diese verbinden wiederum die anderen Normen mit der Norm, die sie zitieren. Wir haben allerdings nicht nur die Verlinkung von einzelnen Normen berücksichtigt, sondern auch von ganzen Büchern, Kapiteln, Titeln etc.; diese nennen wir strukturelle Knoten.

Nachdem wir zunächst erklären wollen, was Datenvisualisierung ist, warum wir sie verwenden (siehe Kapitel A.) und wie das technisch aussehen kann (Kapitel A. I.), wollen wir im zweiten Teil das Bürgerliche Gesetzbuch (Kapitel B.) etwas näher beleuchten.

A. Was ist Datenvisualisierung und warum verwenden wir sie?

Ausgangspunkt für die Analyse von Daten ist oftmals eine sogenannte Explorative Datenanalyse (EDA). Hierbei geht es nicht nur darum, Erkenntnisse zu erlangen, sondern auch ein Gefühl für die Daten zu erhalten. Mittel hierfür können statistische Auswertungen oder aber Visualisierungen sein. Dabei meint Visualisierung nicht nur die hier verwendete Darstellung der Beziehungen in Netzwerken, sondern es kann auch ein einfaches Balken- oder Tortendiagramm sein.

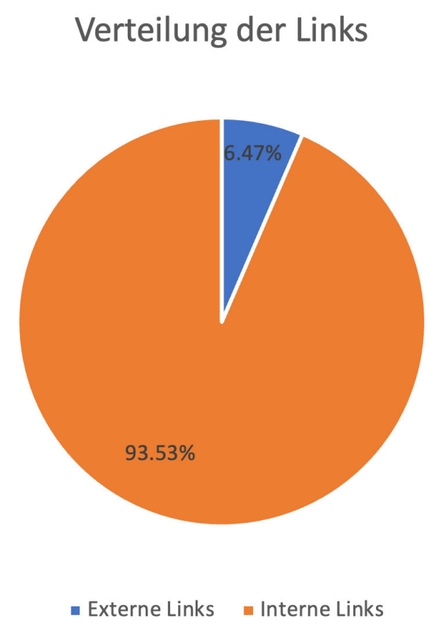


Abb. 3: EDA in Form eines Tortendiagramms, das alle Verweisungen des BGB auf andere Regelungen im BGB (interne Links; orange) und des BGB auf andere Gesetze (externe Links; blau) visualisiert.

Würde man beispielsweise alle Verweise des BGB einzeln in einer Tabelle ausgeben, wäre es bei der Anzahl an Verweisen (insgesamt 1932 Verweise, wovon 125 Externe und 1807 Interne sind) eine schier unüberschaubare Anzahl an Informationen. Mittels der Datenvisualisierung kann eine aggregierte Version erstellt werden (vgl. Abbildung 3).

Diese erlaubt es uns, auf Besonderheiten zu stoßen, die bei der Betrachtung einzelner Elemente nur sehr schwer erfolgen kann. So erkennt man etwa bestimmte Häufungen von Informationen an einem bestimmten Punkt (sog. Cluster) in einer Datenvisualisierung deutlich einfacher.

Schauen wir uns nun die technische Umsetzung etwas näher an.

Das Erstellen einer Graph-Visualisierung erfolgt in zwei Schritten: 1. Erzeugen des Graphen und 2. Auffinden des besten Weges zur Visualisierung. Die Ausgangsdaten für unsere Visualisierung stammen aus dem BGB in einem strukturierten XML-Format von ***Wolters Kluwer***. In diesem Format sind alle Schlüsselelemente enthalten: Titel, Text und die Referenzen.

Wir nutzen in einem ersten Schritt einen einfachen Ansatz, indem wir verschiedene Farben verwenden, um die unterschiedlichen Bücher des BGB zu unterscheiden. Gleichzeitig nutzen wir auch bestimmte Farben, um Strukturknoten, wie bspw. Abschnittsüberschriften, zu kennzeichnen.

Schließlich verwenden wir den ***ForceAtlas2***-Algorithmus, um die Lage der Knoten zu bestimmen. Die Idee hinter dem ***ForceAtlas2***[1] Algorithmus ist es, ein physikalisches System zu simulieren, das Netzwerke räumlich zuordnet.

Aus praktischer Sicht bedeutet dies, dass in der Mitte der Visualisierung mehrere Ansammlungen (Cluster) von verbundenen Normen zu sehen sind. Im Außenbereich der Visualisierung sammeln sich Einzelnormen oder kleine Cluster. Je mittiger der Knotenpunkt (Norm) in der Darstellung also ist, desto öfter wird dieser von anderen Knotenpunkten referenziert und je näher die Knotenpunkte räumlich sind, desto öfter referenzieren sich Knotenpunkte, sodass Cluster entstehen (vgl. Abbildung 4).

Um die Visualisierung noch aussagekräftiger zu machen, können Parameter zur Festlegung der Anziehungskraft verändert werden. Je nachdem, wie der Parameter gewählt wird, wird eine gedrungene oder weitläufige Visualisierung erstellt. Auch kann es hilfreich sein, Überlappungen zu verhindern und Knotenpunkte (sog. Hubs) zu separieren, wodurch die Visualisierung deutlich lichter wird. Dieser Ansatz erzeugt wunderbare Visualisierungen, um ein grundsätzliches Gefühl für die Daten und die Verknüpfung der Normen zu erhalten. Gleichwohl ist es jedoch ungleich schwerer, hierdurch auch konkrete Fragen zu beantworten. Daher ist es praktisch unmöglich, eine einzige Visualisierung zu erstellen, mit der alle Fragen beantwortet werden können.

Um den Graph sinnvoll nutzen zu können, wird ein Programm benötigt, mit dem die Visualisierung einfach verändert und an konkrete Fragen angepasst werden kann.

Wir begannen unsere Suche nach einer solchen Lösung mit komplett auf ***Python*** basierenden Bibliotheken;[2] diese sind allerdings allesamt nicht interaktiv. Sodann wechselten wir zu Web-basierter Technologie wie ***sigma.js*** und ***D3***. Allerdings waren diese auch nicht ausreichend genug, um einfache Veränderungen vorzunehmen; es musste jeweils neuer Code verfasst werden.

1 Für mehr Informationen über die Funktionsweise des ForceAtlas2-Algorithmus, ist das Entwicklungspapier zu empfehlen, hier abrufbar (Stand: 20.02.2022).

2 Bibliothek meint hier eine Sammlung von extra Modulen, die für eine Programmiersprache von Dritten entwickelt wurde und die es Programmierern erlaubt, unkompliziert und einfach auf bereits existierende Funktionen zurückzugreifen und diese in ihr Programm zu inkorporieren.

Letztlich entschieden wir uns, Gephi zu verwenden. ***Gephi***[3] ist eine Open-Source Bibliothek mit einem sehr breiten Funktionsspektrum.

Im Verlauf des Artikels sind verschiedene Visualisierungen zu finden, welche wir zur Beantwortung spezifischer Fragen oder zur Ermöglichung neuer Perspektiven erstellt haben. Hier eine Übersicht über Tipps und Tricks, die wir verwendet haben, um diese Repräsentationen zu erstellen:

- Knotengröße: hilfreich, um wichtige Knoten hervorzuheben. Normalerweise visualisiert die Knotengröße die Anzahl der Beziehungen. Wir nutzen verschiedene Ansätze zur Berechnung der Knotengröße: der Knoten ist größer, wenn er mehr eingehende Beziehungen hat (in-Degree), der Knoten ist größer, wenn er mehr ausgehende Beziehungen hat (out-Degree) oder eine Kombination aus ein- und ausgehend (Degree).

- Knotenfarbe: eine großartige Möglichkeit, um bestimmte Knoten hervorzuheben. Wir haben dies bspw. durchgängig verwendet, um die verschiedenen Bücher des BGB zu visualisieren.

- Kantenfarbe: kann verwendet werden, um verschiedene Arten von Referenzen hervorzuheben. Wir verwenden lediglich eine Farbe zur Kenntlichmachung der Zitate der Normen. In manchen Visualisierungen haben wir die Kantenfarbe identisch mit der Knotenfarbe gewählt, um einfacher zu verdeutlichen, von wo die Beziehung ausgeht.

- Kantengewicht: kann hilfreich sein, um die Visualisierung zu vereinfachen. Wenn beispielsweise ein Knoten mehrere Referenzen zu einem anderen Knoten hat, dann kann dies einfach durch das Kantengewicht und bspw. eine stärkere Linie hervorgehoben werden.

- Filter: diese können auch helfen, die Visualisierung zu vereinfachen. Bspw. dann, wenn wir nur Knoten mit ganz bestimmten Eigenschaften betrachten wollen.

Somit ist es ganz einfach, einen Graphen zu erstellen. Allerdings gilt es zu beachten, dass zur Beantwortung besonders spezifischer Fragen viele Parameter verändert werden müssen, um eine gute Visualisierung zu erhalten. Betrachten wir nun ein paar Beispiele:

B. Die einzelnen Fragestellungen und ihre Visualisierung

I. Die Fragestellungen und ihre Bedeutung

Eine Datenvisualisierung erfolgt in der Regel mit einem bestimmten Ziel. Das Ziel unserer Datenvisualisierung ist es, Fragestellungen aus dem BGB nachzugehen. Diese Fragestellungen kann man teilweise bereits vorab formulieren oder aber sie ergeben sich im Laufe des Prozesses der Erstellung. In unserem Fall lassen sie sich in zwei Gruppen unterteilen: allgemeine und spezielle Fragestellungen. Die allgemeinen Fragestellungen betreffen das ganze BGB, während die spezifischen Fragestellungen nur ganz bestimmte Ausschnitte oder Bezüge betreffen.

Allgemeine Fragestellungen und Ausgangshypothesen:

- Gibt es Auffälligkeiten hinsichtlich der Verweise? Hypothese: bestimmt, aber wir haben zum Startzeitpunkt (noch) keine Ahnung, was es ist.

- Gibt es bestimmte andere Gesetze, die besonders häufig zitiert werden? Hypothese: ja, bspw. das Einführungsgesetz zum BGB.

- Gibt es bestimmte Bereiche des BGB, die besonders häufig zitiert werden? Hypothese: ja, vermutlich der vor die Klammer gezogene Allgemeine Teil.

3 Hier abrufbar (Stand: 29.11.2022).

- Gibt es bestimmte Normen des BGB, die besonders häufig zitiert werden? Hypothese: ja, vermutlich eine Norm aus dem Allgemeinen Teil.

Spezifische Fragestellungen:

- Gibt es Normen, die als Zwischenschritt ganze Bücher des BGB verbinden?
- Gibt es Normen, die eine Vielzahl anderer Normen verbinden?
- Gibt es abgeschlossene Bereiche, die nur untereinander referenzieren?

Dies stellt nur eine Auswahl an Fragen dar, mit denen wir gestartet sind.

II. Allgemeine Fragestellungen

1. Gibt es Auffälligkeiten?

Die erste Visualisierung zeigt das BGB in seiner Gesamtheit. Visualisiert sind nur Verbindungen zwischen Normen innerhalb des BGB. Verschiedene Bücher sind farblich unterschiedlich markiert. Wenn es eine Verbindung zwischen den Büchern gibt, so wird sie durch eine Linie angezeigt. Auffällig sind die beiden Cluster in der Mitte. Insbesondere das lila Cluster hat einige sehr lange Verkettungen von Normen, die von Mitte unten (lila) bis Oben rechts (blau) reichen.

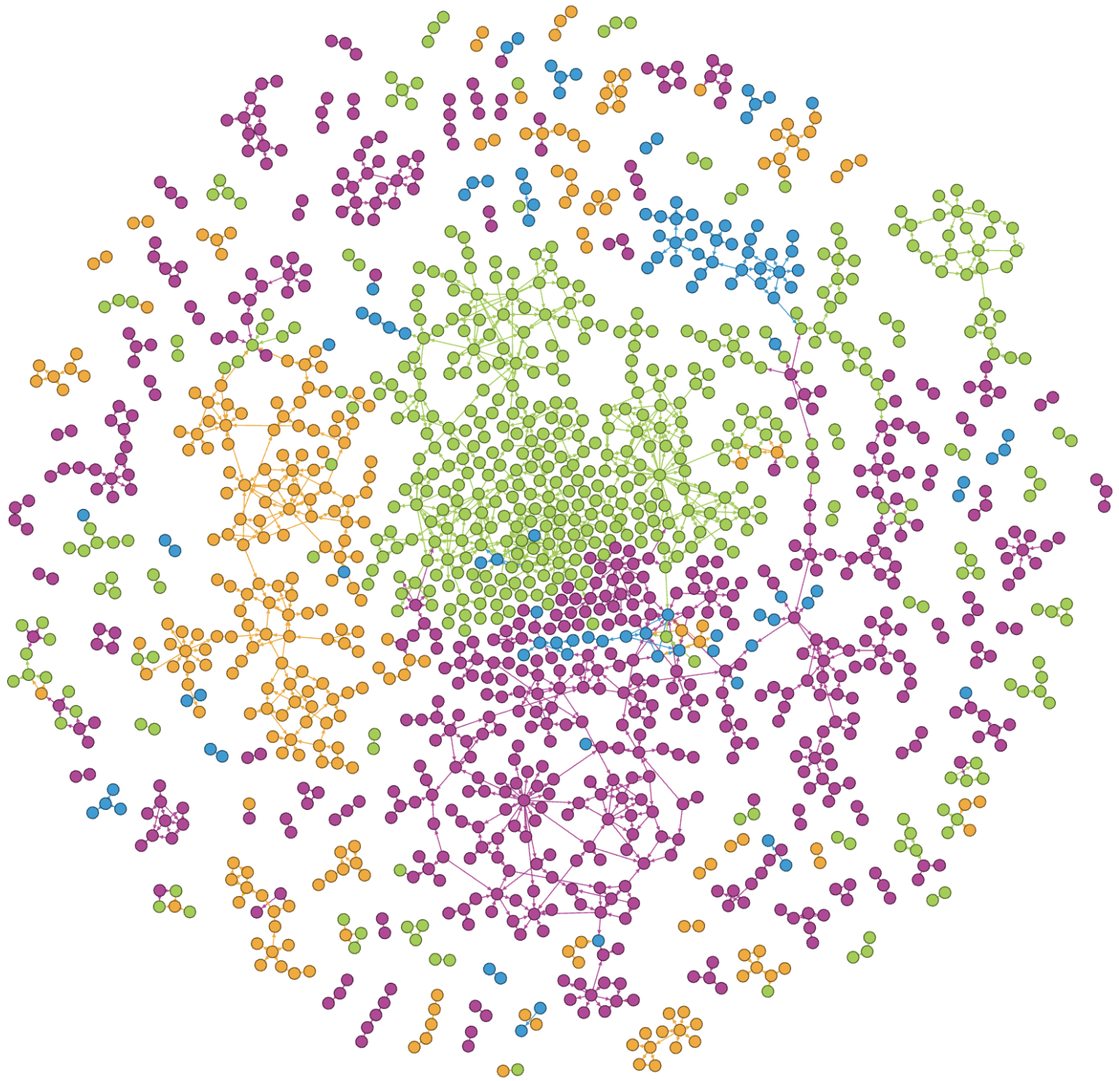


Abb. 4: Visualisierung der Cluster im BGB

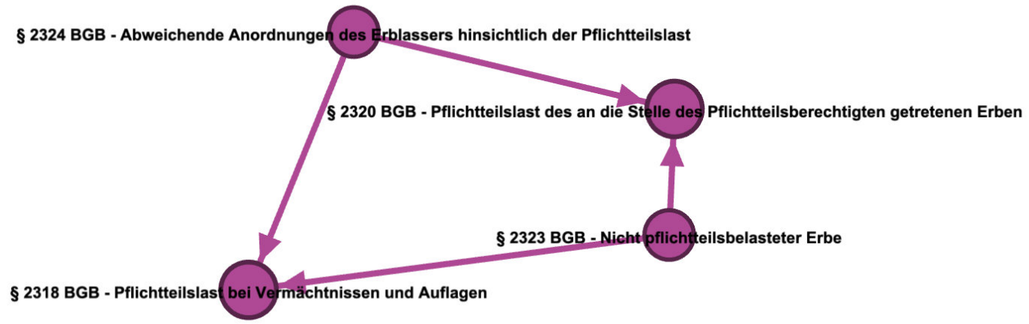


Abb. 5: Hier sieht man ein solches „Zitierviereck".

Ein weiteres Beispiel für Auffälligkeiten sind Unter-Netzwerke, die sich mehr oder weniger selbst zitieren, bzw. eine Art Viereck bilden. Auf den ersten Blick sieht dies wie ein Zirkelschluss aus. Betrachtet man allerdings die Richtung der Zitierung, erscheint es verständlicher. Auch im folgenden Beispiel sieht die Zitierung auf den ersten Blick verwirrend aus:

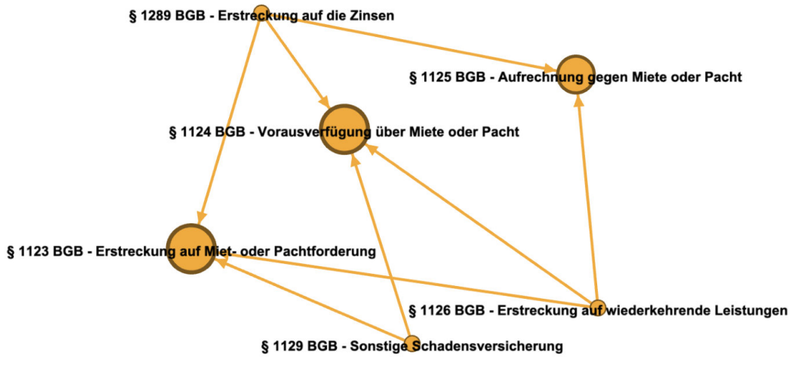


Abb. 6: Verschiedene Normen, die sich scheinbar selbst zitieren.

2. Gibt es bestimmte andere Gesetze, die besonders häufig zitiert werden?

In der folgenden Visualisierung sind nur die externen Verbindungen visualisiert, also alle Vorschriften, die eine Norm außerhalb des BGB zitieren. Die Gruppen, die hier zu sehen sind, sind Normen, die gemeinsam bestimmte Gesetze zitieren.

Abb. 7: Hervorhebung externer Gesetze in Rot

Der große rote Punkt Mitte rechts ist ein Gesetz, das besonders oft zitiert wird: das EGBGB. Damit hat sich die Hypothese bestätigt. Auch Zivilprozessordnung und Grundbuchordnung, die auf Platz 2 und 3 der meist-zitierten anderen Gesetze liegen, sind verständlich. Platz 4 für das Verschollenheitsgesetz[4] hat uns allerdings doch etwas überrascht.

Nachfolgende Darstellungen zeigen proportional die Häufigkeit der Zitierungen.

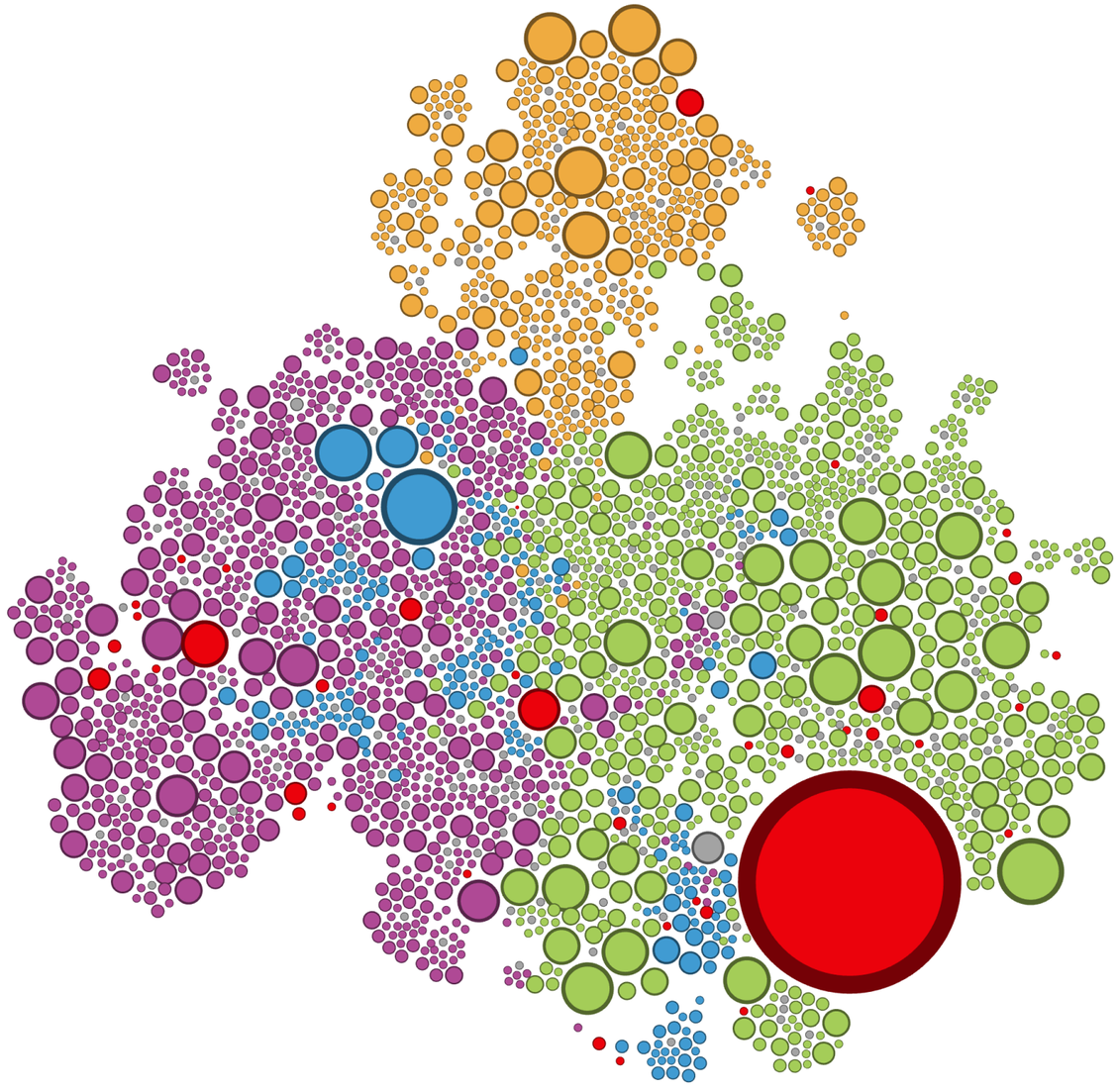


Abb. 8: Darstellung der Menge interner und externer Verweise (rot).

4 Das VerschG ist ein im Erbrecht häufiger relevantes Gesetz. Es regelt, wann eine Person als verschollen und damit rechtlich als tot gelten kann, obwohl man ihren Tod nie positiv feststellen konnte.

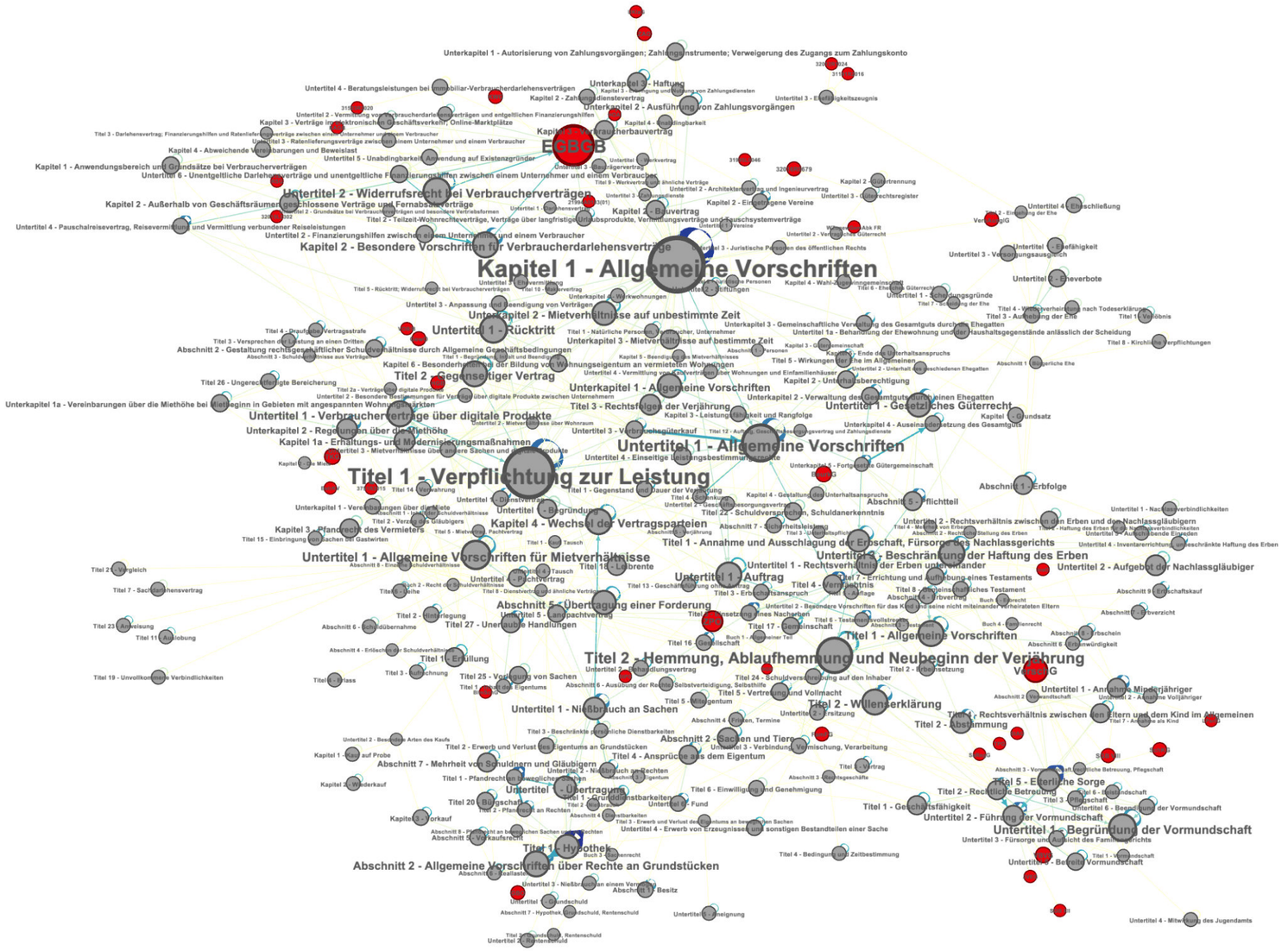


Abb. 9: Relative Darstellung der internen Verweise (graue Knoten) und externen Verweise (rote Knoten)

Diese Visualisierung betrifft die einzelnen strukturellen Knoten und visualisiert die Häufigkeit der Zitierung anderer Gesetze, wobei der Pfeil dicker wird, wenn bestimmte Gesetze von bestimmten Teilen häufiger zitiert werden (sog. Gewichtung):

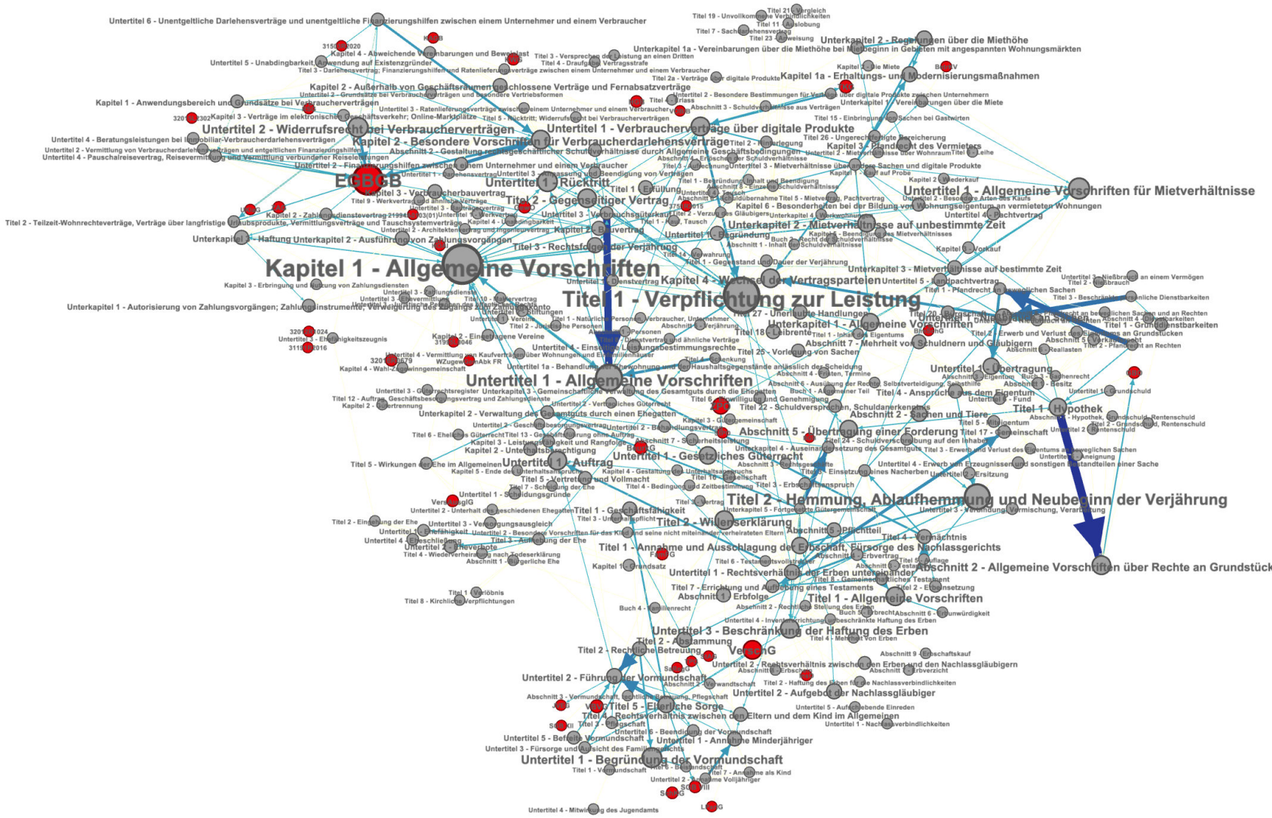


Abb. 10: Nutzung des Kartengewichts zur Darstellung mehrfacher Zitierungen einer Norm.

3. Gibt es bestimmte Bereiche des BGB, die besonders häufig zitiert werden?

In der folgenden Visualisierung wurden die eingehenden Zitierungen untersucht und je häufiger eine Norm aus einem Bereich des BGB zitiert wurde, desto größer wird der Knoten dargestellt.

Auch hier hat sich die Hypothese bewahrheitet, dass der Allgemeine Teil des BGB, insbesondere die Allgemeinen Vorschriften deutlich häufiger zitiert werden. Das „Vor-Die-Klammer-Ziehen" im BGB ist also auch in der Datenvisualisierung klar erkennbar.

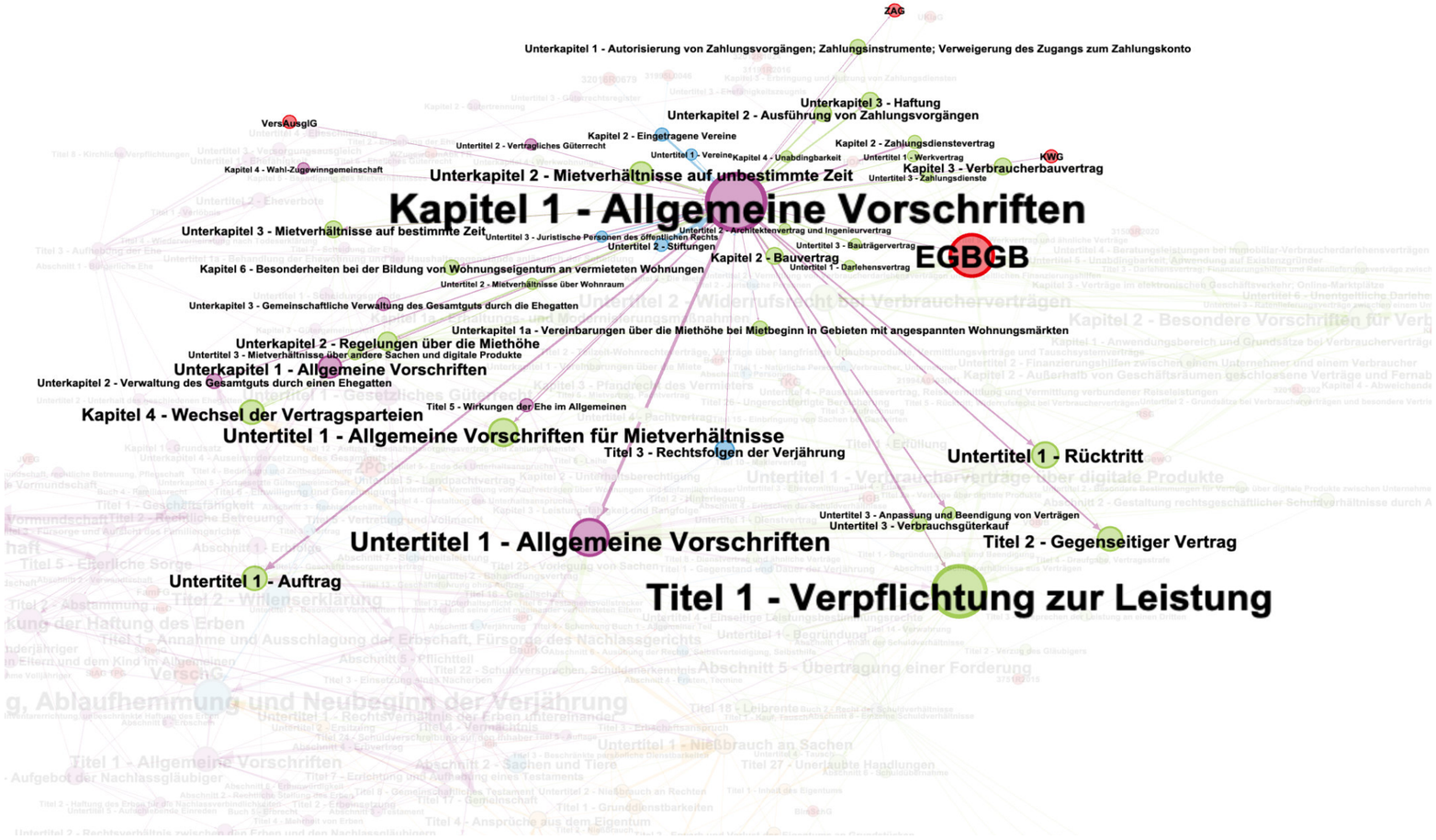


Abb. 11: Strukturelle Elemente und deren Zitierung; hier im BGB AT in Lila.

Im Vergleich hierzu der deutlich kleinere Knoten der §§ 203 ff. BGB:

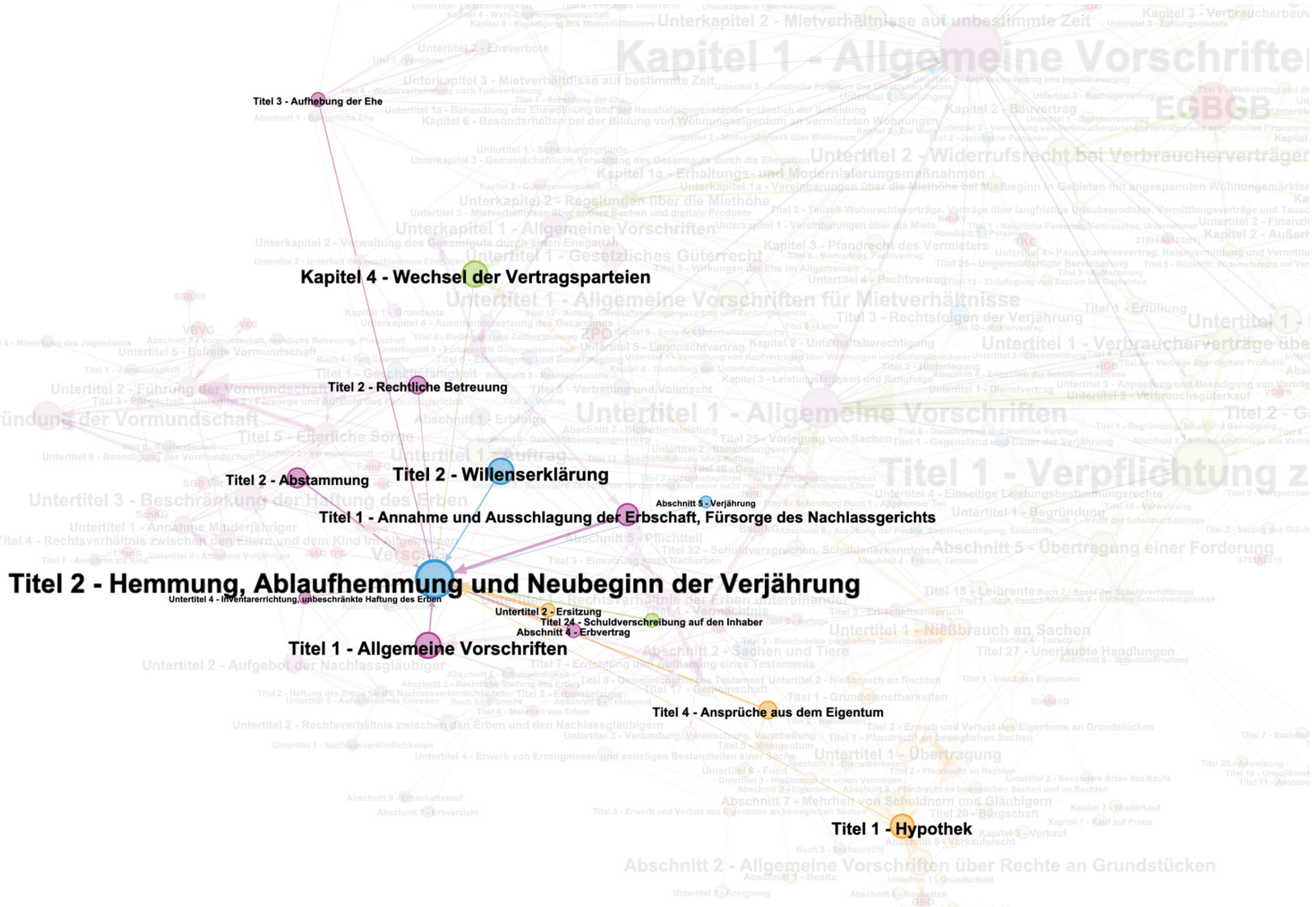


Abb. 12: Visualisierung der §§ 203 ff. BGB.

4. Gibt es bestimmte Normen des BGB, die besonders häufig zitiert werden?

Die mit am meisten zitierte Norm ist § 210 BGB, was man an den ganzen eingehenden Verbindungen sieht:

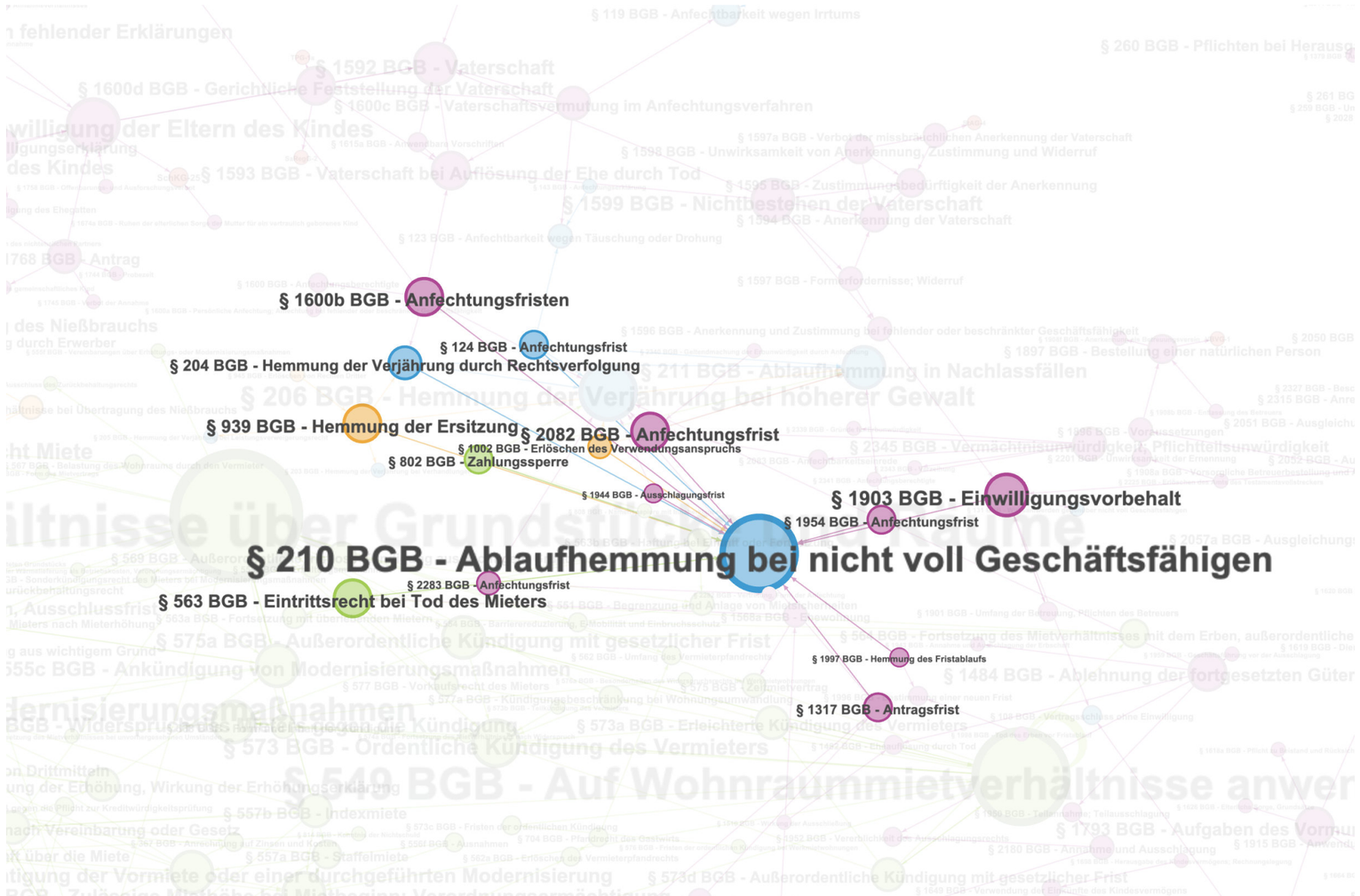


Abb. 13: Visualisierung der am häufigsten referenzierten Norm, § 210 BGB.

Umgekehrt ist wohl § 578 BGB eine der Normen, welche die meisten anderen Normen zitiert:

Abb. 14: § 578 BGB referenziert die meisten anderen Normen.

III. Spezifische Fragestellungen

1. Gibt es Normen, die als Zwischenschritt ganze Bücher des BGB verbinden?

Dieser Graph zeigt alle Verbindungsnormen, die mindestens zwei verschiedene Bücher des BGB verbinden. Die Bücher sind jeweils wieder in unterschiedlichen Farben dargestellt. Hier sind verschiedene Möglichkeiten denkbar, wie diese Verbindung von Büchern im BGB zustande kommen: Norm A (aus Buch 1) zitiert Norm B (aus Buch 2), diese wiederum zitiert Norm C (aus Buch 1 oder 3). Norm A (aus Buch 1) zitiert Norm B (aus Buch 2), die auch von Norm C (aus Buch 3) zitiert wird.

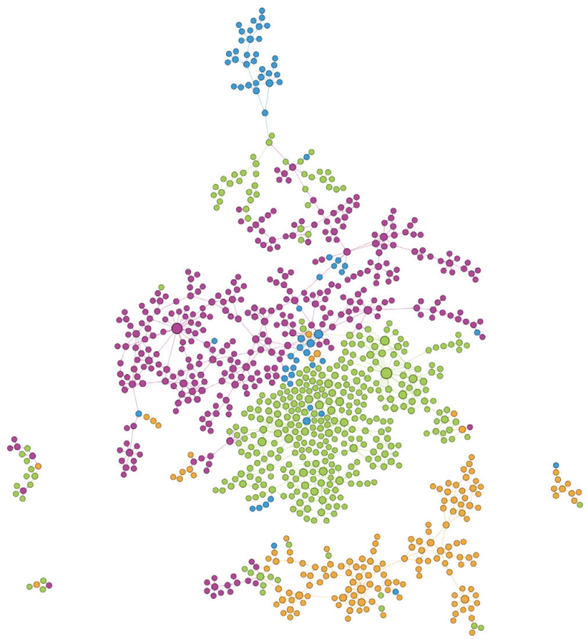


Abb. 15: Normen, die verschiedene Bücher miteinander verknüpfen

Abbildungen 15-17 zeigen hierbei Beispiele für Variante 1:

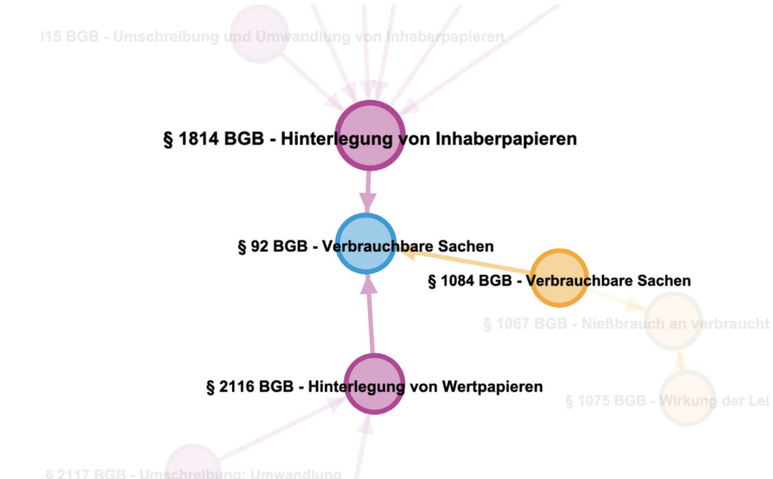


Abb. 16: Beispiel 1 für Variante 1.

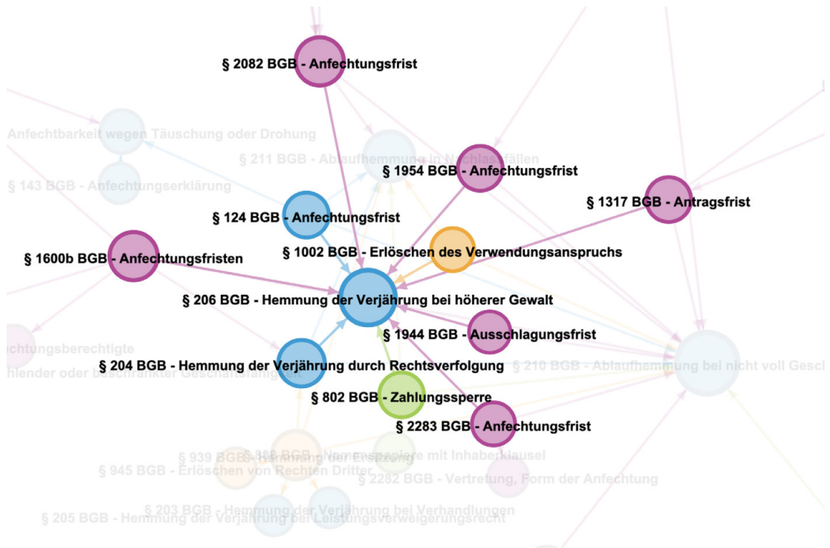


Abb. 17: Beispiel 2 für Variante 1.

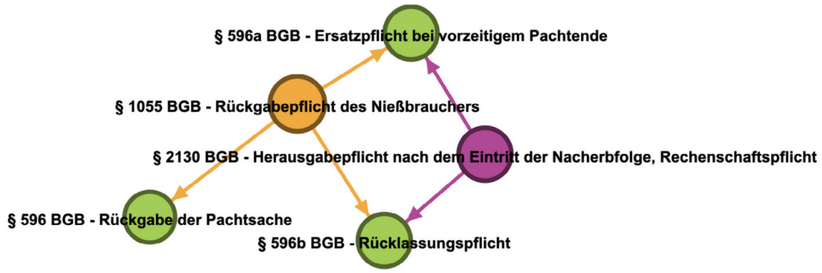


Abb. 18: Beispiel 3 für Variante 1.

Das folgende Bild zeigt ein Beispiel für Variante 2. So lässt sich ein Pfad von §§ 997, 994 BGB zu § 989 BGB erkennen.

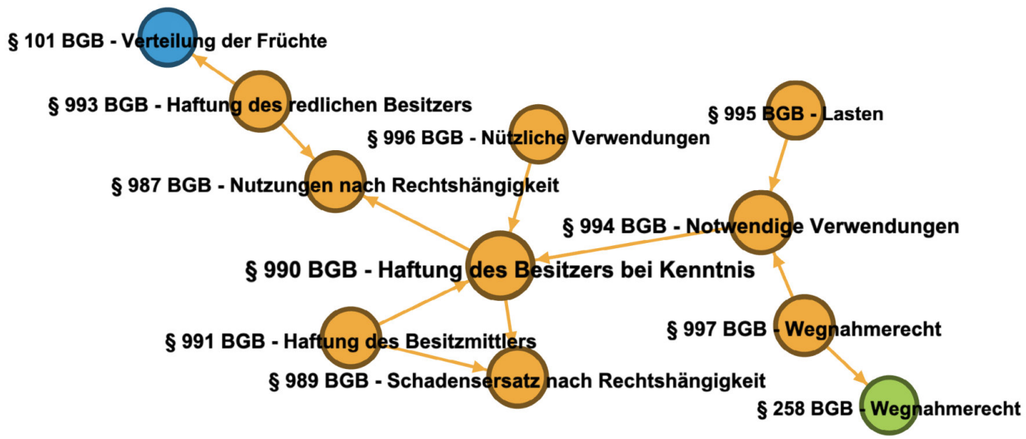


Abb. 19: Beispiel für Variante 2.

2. Gibt es Normen, die eine Vielzahl anderer Normen verbinden?

Das Beispiel des § 578 BGB haben wir bereits oben angesprochen. Diese Norm zitiert eine Vielzahl von anderen Normen. Hier noch einmal übersichtlich die Vielzahl solcher Normen, wobei § 578 BGB hier ganz zentral als Knoten (in grüner Darstellung in der Mitte des Netzwerkes) sichtbar ist:

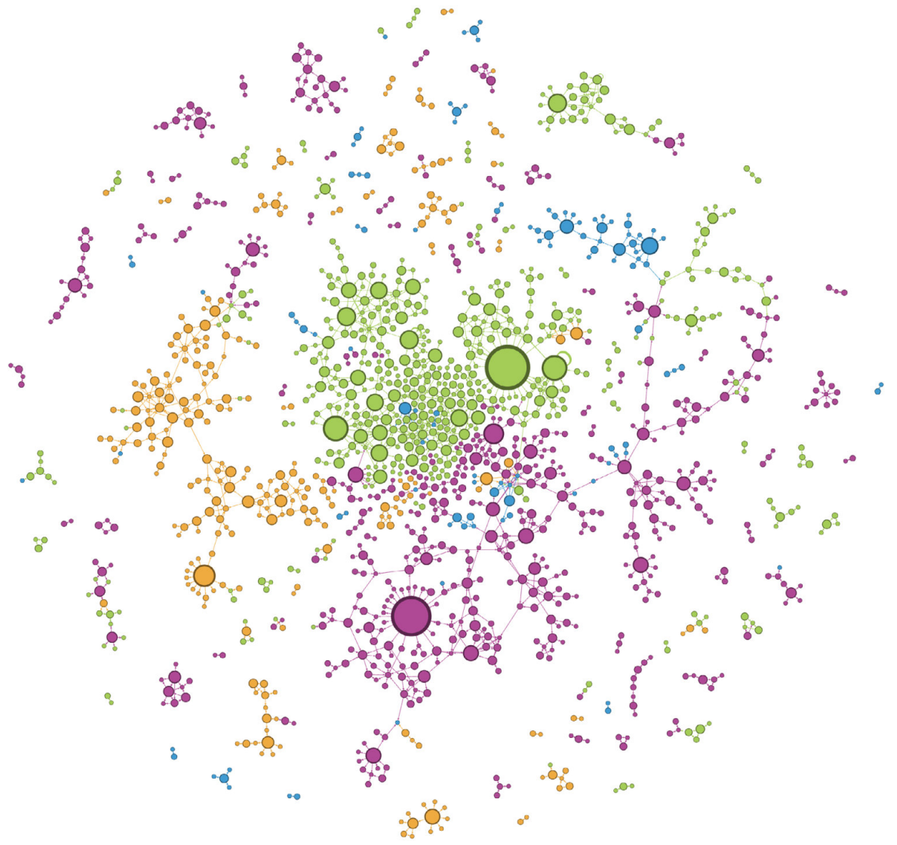


Abb. 20: Visualisierung derjenigen Normen, welche die meisten anderen Normen referenzieren.

3. Gibt es abgeschlossene Bereiche, die nur untereinander referenzieren?

Ja, es gibt mehrere solcher Bereiche. Beispielhaft seien die §§ 1570 ff. BGB genannt. Lediglich als eingehende Zitierung wird § 1570 BGB zusätzlich noch von § 1586a BGB zitiert.

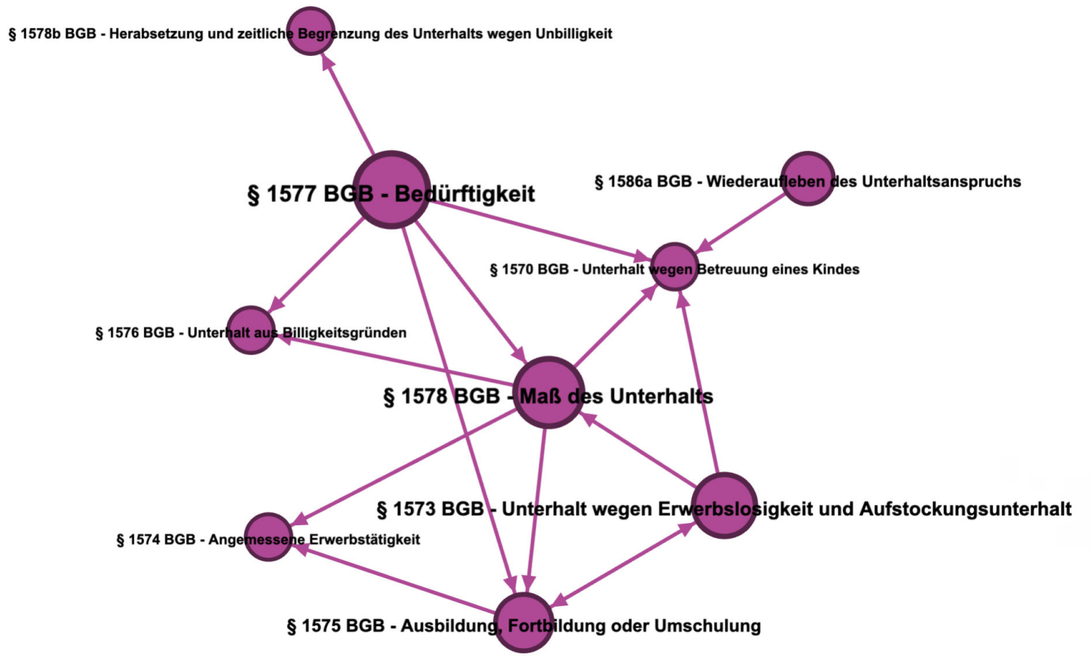


Abb. 21: Beispiel für einen abgeschlossenen Bereich, der sich nur selbst referenziert.

C. Ergebnis

Auch wenn dieser Beitrag lediglich einen kleinen Einstieg in die Datenvisualisierung anhand des BGB geben kann, so gehen wir doch von einem hohen Potenzial für zukünftige Entwicklungen aus.

Anwendungsfälle in der Praxis können nicht nur im Rahmen der Gesetzgebung sein, um etwa fehlerhafte Zitierungen, Zirkelschlüsse oder ähnlich problematische Veränderungen leicht erkennbar zu machen. Eine solche Darstellung kann auch Jurist:innen in der täglichen Arbeit unterstützen. Würde man alle möglichen Anspruchsgrundlagen für einen Fall visualisieren, könnte man hiermit Gemeinsamkeiten und Unterschiede leicht erkennbar machen. Aber auch in der juristischen Ausbildung können solche Visualisierungen helfen. Wie leicht wäre es, zu erklären, wie die Zusammenhänge im BGB nun wirklich sind, wenn man diese einfach visualisieren könnte, statt sie nur im Text markieren zu können.

Wir hoffen, mit diesen Beispielen Anregungen für die Verwendung von Datenvisualisierung auch für Jurist:innen gegeben zu haben. Vielleicht wird sie sich ja auch im juristischen Umfeld etablieren.

Zurück zum Inhaltsverzeichnis

Der Legal Hackathon 2022 Cologne:

Zwischen innovativem Zukunftsgeist, Massagen und Networking

Hendrik Scheja

Open Peer Review

Dieser Beitrag wurde lektoriert von: Julia Kešelj & Jan Broszeit

Hendrik ist geprüfter Mediator und studiert Jura an der Universität zu Köln mit dem Schwerpunkt Rechtsentwicklung in der Moderne bei Herrn Prof. Dr. Hans-Peter Haferkamp. Zuvor absolvierte er das Zusatzstudium der Technikwissenschaften an der Universität Bayreuth mit Weiterbildung zum Projektmanager (IHK). Im Legal Tech Lab Cologne hält er die Vorstandsposition für Finanzen inne.

Vom 16. - 18. September 2022 fand der Legal Hackathon nach einem virtuellen Eventjahr endlich wieder in voller Präsenz statt. Am Freitagabend öffnete ***Wolters Kluwer Deutschland*** (***WK***) hierfür allen Teilnehmern[1] seine Türen am Firmensitz ***WKEINS*** in Hürth.[2] Zugeschaltet per Videobotschaft sprach Bundesjustizminister ***Dr. Marco Buschmann*** – Schirmherr des Legal Hackathons – seine persönliche

1 Zum Zwecke der besseren Lesbarkeit wird bei den personenbezogenen Hauptwörtern nur die männliche Form verwendet. Diese Begriffe sollen für alle Geschlechter gelten.
2 Zur Pressemitteilung von Wolters Kluwer Deutschland GmbH über den Hackathon, hier abrufbar (Stand: 15.11.2022).

Begeisterung über die Veranstaltung aus. Er richtete sich in seiner Ansprache gezielt an die Teilnehmer und ihren innovativen Zukunftsgeist. Es sei von außerordentlichem Gewinn, wenn Gelegenheiten wie diese geschaffen und genutzt würden, um die Digitalisierung zur Lösung gesellschaftlicher Herausforderungen voranzutreiben.[3]

Der Bundesjustizminister Dr. Marco Buschmann eröffnet den Hackathon 2022 (Quelle: Oliver Hartmann)

Der Hackathon ist eine besondere und einmalige Gelegenheit für Viele, ihre Ideen zu Legal-Tech-Lösungen einem offenen Publikum vorzustellen. Dies ermöglicht über die Veranstaltungsreihe hinaus, Input aus verschiedenen Branchen und den damit verbundenen Denkrichtungen zu erhalten, um Lösungsideen weiterzuentwickeln. Nicht zuletzt deshalb ist es für jeden Hackathon eine Bereicherung, unterschiedliche Branchenberufe mit einzubinden. Weit gefehlt, wer bei einem Legal Hackathon lediglich Juristen und ITler erwartet.

> „Weit gefehlt, wer bei einem Legal Hackathon lediglich Juristen und ITler erwartet."

Längst gehören andere Berufsbilder als wichtiger Bestandteil dazu. Wissenslücken bei Theoretikern aus Wissenschaft und Forschung werden von ausgebildeten Praktikern mit ihrem erfahrungsreichen Fachwissen geschlossen.

Aus ganz Deutschland fanden sich zu diesem Anlass Denker und Praktiker zusammen, um die ihnen bekannten branchenspezifischen Probleme vorzustellen. Nicht selten schwebten schon erste unausgereifte Lösungsideen im Raum, bevor das Problem in voller Breite vorgestellt wurde. Um die spannendsten

Kreative Lösungsfindung (Quelle: Oliver Hartmann)

3 Näheres zum Digitalisierungsengagement des Bundes, hier abrufbar (Stand: 15.11.2022).

Ideen herum bildeten sich schnell die für das Wochenende bestehenden Teams. Ab jetzt hatten alle Teams bis Sonntag Zeit ihre Ideen zu verfolgen. Neben den Räumen mit Papier und Stift wurden den Teams Legal-Tech-Tools zur Ausgestaltung ihrer Ideen zur Verfügung gestellt. Das Beratungsangebot während des Hackathons wurde von Mitgliedern des ***Gateway Exzellenz Start-up Centers*** der ***Universität zu Köln*** abgerundet. ***Franziska Röhr***, Expertin für gewerbliche Schutzrechte, sowie ***Marc Gresch***, Eventmanager und Start-Up-Coach, standen den Teilnehmern während des Hackathons durchgehend für Fragen zur Seite. Doch wer glaubt, ein Hackathon bestehe ausschließlich aus schwerer intellektueller Arbeit, hat den Legal Hackathon 2022 Cologne schlicht verpasst: Mit großer Resonanz wurde mithilfe von Yoga Sessions sowie einem Masseur auf eine ausgezeichnete Work-Life-Balance Rücksicht genommen. Es sollte auch nicht unerwähnt bleiben, dass unter DJ-Klängen die Dachterrasse des ***WKEINS*** in Kombination mit einem Glas Wein die Kreativität erheblich anregte und die Zusammenarbeit innerhalb der Teams bis in die Nacht belebte. Mit welchem Ergebnis schloss der Hackathon nach all der gelebten Work-Life-Balance? Dieser Frage nahm sich die Jury (vgl. Abbildung 3) am Sonntag an. Im Rennen um die Platzierungen traten fünf Teams vor die Jury: ***CiteBrick, Adler***, ***ReadYourRights***, ***Protestomat*** und ***Positive Energy***.

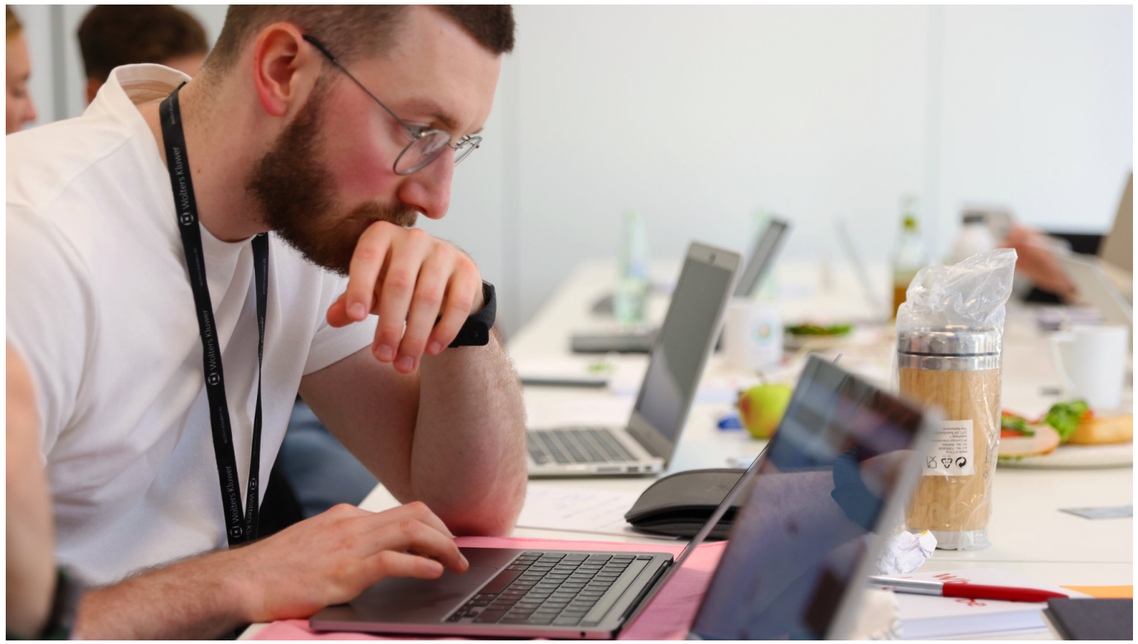
Die hochkarätige Jury, bestehend aus Praktikern und Wissenschaftlern, h.l.n.r: Dr. Tobias Kircher (RIMOWA GmbH), Prof. Dr. Karl-Nikolaus Peifer (Universität zu Köln) und Dr. Tim Odenthal (Ebner Stolz).

V.l.n.r.: Larissa Penner (Wolters Kluwer), Katharina Bisset (NetzBeweis GmbH und Nerds of Law OG) sowie Dr. Peter Schichl (Deutsche Telekom AG und Bundesverband der Unternehmensjuristen).

A. Projekt *CiteBrick*

CiteBrick nimmt sich jener selbstständigen Anwälte an, die in ihrer Mandatsarbeit häufig als Generalisten in jedem Rechtsgebiet tätig sind. Gerade am Anfang einer anwaltlichen Berufskarriere besitzen die Wenigsten eine fachanwaltliche Expertise. Dies kann dazu führen, dass rechtlich irrelevante Sachverhaltsrückfragen im

Mandantenkontakt erörtert werden, wohingegen relevante Knackpunkte übersehen werden. Dies kostet nicht nur Zeit, sondern vor allem Geld. Den Mehrwert liefert ***CiteBrick***, indem es den Dreischritt aus a) strukturierter Sachverhaltsermittlung, b) dem Recherchieren rechtlicher Schwerpunktprobleme und dem daraus resultierendem Anwaltsschreiben durch c) die Systematisierung von Textbausteinen bündelt. Wie? Mithilfe eines im Interviewstil geführten Prüfungsschemas. Dieses erfragt gezielt Sachverhaltsangaben. Basierend auf dem Sachverhalt recherchiert das Tool selbstständig Urteile sowie Rechtsauffassungen. Anschließend stellt es die besten sich daraus ergebenden Handlungsmöglichkeiten heraus. Das Mandantenbegehren wird anhand eines Entscheidungsbaums ermittelt, um die weiteren rechtlichen Schritte abzuwägen. Abschließend liefert ***CiteBrick*** das Anwaltsschreiben durch Textbausteine. ***CiteBrick*** strebt damit das All-Inclusive-Tool an oder kurzgesagt: die eierlegende Wollmilchsau für die Juristerei. Diese Ambition erkennt die Jury in gleicher Weise an und bezeichnet das Vorhaben als den *„**Mount Everest**“* des Juristen-Daseins. Und obwohl die energisch-ambitionierte Präsentation des Teams vor Überzeugung strahlte, staubte es keine Platzierung mehr an diesem Wochenende ab.



Quelle: Oliver Hartman

B. Projekt *Adler*

Das Team ***Adler*** beschäftigt sich mit der Unmenge an Gerichtsdaten. Ihr Problemaufriss: Es fehlt an Klarheit und Übersicht der Urteile. Wer kennt es nicht, wenn Landgerichte bei nahezu gleichgelagerten juristischen Problemen zu unterschiedlichen Ergebnissen kommen. Das ist nicht nur unbefriedigend, sondern erschwert zugleich die Rechtssicherheit und in der Konsequenz das Prozessrisiko. Eine spezifische Analyse der Urteile durch ein Auswertungstools könnte hierbei Abhilfe verschaffen. Beispielhaft wurden seitens des Teams während des Hackathons 56.000 Urteile des BGH analysiert. Das Zauberwort: qualitative Massenanalyse der Gerichtsurteile. Am Beispiel der Dieselgate-Prozesse kann so eine KI ermitteln, dass eine Korrelation zwischen den Keywords ‚Nutzungsentschädigung' in Abhängigkeit zum Keyword ‚Baujahr' und dem Keyword ‚Kilometerstand' besteht. Prozessrisiko und Gewinnaussichten können dadurch gezielter abgeschätzt werden. Die daraus gewonnenen Erfahrungswerte aus den Vorprozessen finden so in der anwaltlichen Beratung einen neuen Stellenwert. Mit dem damit errungenen vierten Platz zog die Podestplatzierung am Team ***Adler*** knapp vorbei.

C. Projekt *ReadYourRights*

ReadYourRights will nicht die Anwälte, sondern direkt den Mandanten ansprechen. Bereits ab der Zustellung von behördlichen Schriftstücken stehen viele Betroffene vor dem Problem, dass sie den Inhalt des Schreibens gar nicht verstehen. Sei es die tatsächliche Sprachbarriere oder durch kryptisches Behördendeutsch geschaffene Verständnisprobleme. *„**Was wollen die von mir?**“* ist eine nicht selten an Juristen gerichtete Frage. Doch nur die Wenigsten machen von einer anwaltlichen Vertretung vor Gericht Gebrauch. Im Jahr 2021 saßen allein 150.000 Angeklagte in Strafprozessen ohne anwaltliche Verteidigung auf der Anklagebank.

Nach der Strafprozessordnung wird regelmäßig dem Angeklagten erst ab einem zu erwartenden Strafmaß von über einem Jahr ein Pflichtverteidiger zur Seite gestellt. Diese Situation ist für ***ReadYourRights*** nicht nur unbefriedigend, sondern schmälert Betroffenenrechte vor Gericht in unangemessener Weise.

„Im Jahr 2021 saßen allein 150.000 Angeklagte in Strafprozessen ohne anwaltliche Verteidigung auf der Anklagebank.“

Eine erste Verständigungshilfe liefert ***ReadYourRights***, indem es durch Texterkennung des Dokuments eine Übersetzung in der jeweiligen Muttersprache oder eben in einfachem Deutsch liefert. Was muss, kann oder soll der Betroffene nun tun? Diese FirstAid-Informationen liefert das Tool und klärt über weitere Möglichkeiten in Anbetracht der Ausgangslage auf. Außerdem könne das Tool direkt Hilfestellung zur Ausübung von Betroffenenrechten liefern, indem es Vorlagen für Einsprüche liefere. Die Jury schätzte die ideell verfolgte Bestrebung, Betroffene in ihren Rechten zu stärken. Die Juroren würdigten daher kurzerhand das Tool ***ReadYourRights*** mit dem dritten Platz und bescherten ihnen damit ein Preisgeld von 500 € zur Fortführung ihrer Arbeit.[4]

4 Zur Homepage von *ReadYourRights*, hier abrufbar (Stand: 15.11.2022).

Quelle: Oliver Hartmann

D. Projekt *Protestomat*

Protestomat beschäftigt sich mit der Frage: ‚How to demonstrieren.' Wenn Bürger eine Demonstration besuchen, sind sie in aller Regel selbst Demonstranten. Denn diejenigen, die das Organisieren der Demonstration übernehmen, sind schließlich ‚die Anderen'. Doch selbst ‚die Anderen' sind am Ende nur ‚Ottonormalbürger' – von Hauptberuf ist da niemand Demonstrations-Organisator mit erfahrenem Crowd-Control-Gespür. Und dennoch steht jedermann dieses Grundrecht so selbstverständlich zur Verfügung, ohne zu wissen, wie es konform ausgeübt werden soll. Die wahren Probleme beginnen bei den Unklarheiten der Anmeldung einer Demonstration, der Zuordnung von Zuständigkeiten der Polizei und am Ende gewiss an der Hürde: Formulare über Formulare. Am liebsten Formulare ohne Erklärung.

Protestomat möchte mit dem Tool die Hemmschwelle des Demonstrierens senken, indem es bei den Schritten der Anmeldung unterstützt. Mithilfe eines barrierefreien und transparenten Tools soll die Ausübung der Grundrechte sowohl für Demonstranten als auch für Polizeibehörden klarer und störungsfreier vorbereitet und durchgeführt werden. Neben der Anmeldung können Auflagen und Verbote in direkter Kommunikation mit den Polizeibehörden gelöst werden. Dazu stehen Tipps und Empfehlungen aus vergangenen Demos unterstützend zur Seite. Sollte das primär zur Lösung angestrebte Gespräch mit der Polizei zur Aufklärung von Auflagen oder Verboten scheitern, werden weitere rechtliche Schritte vorgeschlagen. Das Projekt ist ein rein gemeinnütziges Tool, welches idealerweise über Crowdfunding finanziert werden könnte. Beispielsweise könne eine geplante Demonstration zum Thema A einen derart starken Rückhalt in der Bevölkerung haben, dass die Organisatoren während der Vorbereitung von Seiten der Demonstrierenden per Crowdfunding finanziert werden, um für mögliche prozessuale Auseinandersetzungen finanziell gewappnet zu sein. Dieses Vorhaben unterstützt nicht zuletzt die Jury und platziert ***Protestomat*** auf Platz Zwei. Das Team des ***Protestomat*** darf sich somit über das Preisgeld in Höhe von 1.000 € freuen.

Die Work-Life-Balance kam nicht zu kurz, etwa durch die Stärkung des Körpers und Geistes bei einer Yoga-Session. (Quelle: Oliver Hartmann)

E. Projekt *Positive Energy*

Last but not least: das Team ***Positive Energy***. Dessen Bestreben ist es, einen Powerboost für die Energiewende zu schaffen! In aller Deutlichkeit messen wir die voranschreitende Klimakatastrophe und den damit verbundenen ökologischen Schaden des Planeten. Nicht zuletzt deshalb sprechen ***Bundesregierung*** sowie ***Bundesnetzagentur*** steigende Umweltziele aus. Doch das Problem: Die tatsächliche Umsetzung hinkt drastisch hinter der Zielsetzung hinterher. Woran liegt das? Am Umsetzungswillen bei wartenden Hausbesitzern mit der noch genehmigungsbedürftigen Solaranlage auf dem Dach scheitert es selten.

Es sind rechtliche Hürden, welche die Umsetzung verlangsamen, erschweren und im Zweifelsfall am Ende zum Scheitern bringen. Größter und bedeutendster Player in dieser Energieentwicklung sind über 1.000 Stadtwerke in der Bundesrepublik Deutschland. Sie kommen der Umsetzung der Umweltziele aus der Politik nicht nach, weil Vertragsgeflechte zwischen mehreren Beteiligten den Ausbau von Solarkollektoren oder Energietrassen massiv behindern. Eine wesentliche Rolle spielt das streng regulierte Energierecht, durch das sich alle Stadtwerke einzeln durcharbeiten müssen, um zu einer Lösung im Sinne der Energiewende zu kommen. Die Abhilfe dafür schafft nun ***Positive Energy.*** Stadtwerke sollen dazu befähigt werden, sich selbst Energie-Projektziele zu stellen und alle erforderlichen Verträge mit einem Hybriden-Tool in juristischen Einklang zu bringen. Stadtwerke müssen dabei in der Lage sein, ihren individuellen Anforderungen aus Vertrags-, Bau- und Energierecht nachzukommen. Dieses juristische Geflecht gilt es zu entwirren und miteinander für alle Stadtwerke nach regionaler Besonderheit zur Verfügung zu stellen. In Ergänzung dazu kommen später zudem Bausteine wie der thermische Abgleich von Regionen und der Ausbau von Ladesäulen hinzu. Anwaltliches Wissen kommt von der Energiejuristin ***Kristina Hunger.*** Durch einen Zufall konnte auch die Zielgruppe schon vor Ort befragt werden, denn ein Mitarbeiter der ***Stadtwerke Aachen*** war glücklicherweise vor Ort.

F. And the winner is…

Das Projek***t Positive Energy*** weckte bei der Jury die meisten positiven Gefühle:

Den Bedarf einer schnelleren Umsetzung der Energiewende betonte die Jury und hob das Team ***Positive Energy*** mit besonders aktueller Dringlichkeit der Thematik

hervor. Es sei insbesondere auf die dringlichste Schwierigkeit und den zugleich einflussreichsten Stakeholder bedarfsorientiert zugegangen worden. Das Team ***Positive Energy*** wird somit zum Gewinnerteam gekürt. Im Interview gab das Team ***Positive Energy*** an, es werde die Arbeit Dank des dotierten Preisgelds von 2.500 € unter Federführung von ***Kristina Hunger*** (vgl. Abbildung 7) weiterverfolgen.[5]

Abschließend gilt es dem Eventmanagement einen besonderen Dank auszusprechen, namentlich an ***Astrid Ranz,*** für den gastfreundlichen Empfang aller Gäste im ***WKEINS*** sowie an ***Frederick Assmuth***, ***Oliver Hartmann***, ***Philipp Kühn*** und ***Steffen Martini***, die mit dem ***Legal Tech Lab Cologne*** einen Partner für die Ausgestaltung des Hackathons gefunden haben. Und nicht zuletzt an ***Julia Kešelj, LL.M.,*** Director of Partnerships and Events des ***Legal Tech Lab Cologne*** für die tatkräftige organisatorische Ausgestaltung. Der Hackathon hat den Teilnehmern nicht nur intellektuelle Freude bereitet, sondern ein nachhaltiges Netzwerk geschaffen, mit dem Visionen weiterverfolgt werden.

E. Hackathon 2023

Für alle Interessierten sei an dieser Stelle verraten, dass die Vorbereitungen für den kommenden Hackathon vom 08. - 10. September 2023 in Köln bereits im Gange sind. Die Anmeldung hierfür wird selbstverständlich auf der Website des ***Legal Tech Lab Cologne*** kommuniziert.[6]

Das Gewinnerteam Positive Energy, federführend die Energiejuristin Kristina Hunger (v.r.) (Quelle: Oliver Hartmann)

Zurück zum Inhaltsverzeichnis

5 Interview mit *Kristina Hunger* und *Anna Balmes* aus dem Team Positive Energy, hier abrufbar (Stand: 15.11.2022).
6 Zur Homepage des Legal Tech Lab Cologne e.V., hier abrufbar (Stand: 15.11.2022).

Impressum

Chefredaktion
Philipp Beckmann, Louis Goral-Wood, Julia Melles , Ramon Schmitt, Ferdinand Wegener

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

Layout & Design: Julia Melles, Helena Sommer, Michelle Duda

Illustration: Helena Sommer

Social Media: Alina Rosenkranz, Larissa Pilch,

IT: Alexander Adlmüller, Simon Damschen, Daniel Dischinger

E-Mail: ctrl@legaltechcologne.de

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.

LEGAL TECH LAB
COLOGNE

Cologne Technology
Review & Law