CTRL

1/25
ctrl-magazin.de

Grundwissen
Was man über Web Scraping wissen muss

Aufsatz
Das Recht auf Vergessenwerden im Internetzeitalter

Legal Tech
KI-Agenten - Die neue juristische Arbeitsweise?

Contemporary Technology Review & Law

Liebe Leserinnen und Leser,

Digitale Souveränität – ein Begriff, der derzeit so aktuell und vielschichtig diskutiert wird wie kaum ein anderer. Was bedeutet es, im digitalen Raum souverän zu handeln? Ein aktuelles Beispiel zeigt der Internationale Strafgerichtshof: Nachdem politische Spannungen dazu führten, dass ein US-Anbieter zeitweise das E-Mail-Konto eines Chefanklägers blockierte, wechselte das Gericht zu einer europäischen Open-Source-Lösung. Damit wird deutlich, wie zentral echte digitale Souveränität inzwischen geworden ist.

Mit dieser Ausgabe der CTRL greifen wir zentrale Aspekte rund um die Souveränität im digitalen Raum auf und beleuchten sie aus vielfältigen juristischen Blickwinkeln: Tim Rösch analysiert, wie das Vergaberecht als Katalysator, aber auch als Bremsklotz für die digitale Souveränität staatlicher Stellen wirkt und welche Weichenstellungen erforderlich sind, um die Abhängigkeit von einzelnen Technologielösungen zu minimieren. Ergänzend zeigt Luisa Mayr, warum das „Recht auf Vergessenwerden" im Zeitalter von Big Data integraler Bestandteil einer effektiven Selbstbestimmung bleiben muss und wie Europäischer Datenschutz im globalen Wettbewerb steht.

Immer wichtigerwird auch die Frage nach Datensicherheit: Jonas Neubert vermittelt in seinem Grundwissensbeitrag, wie Scraping-Technologien funktionieren, wo die rechtlichen Risiken liegen und warum Gerichte wie der BGH dem Datenmissbrauch mittlerweile entschiedener entgegentreten. Was bedeutet Souveränität für innovative Technologien wie (autonome) KI-Agenten? Christian Hartz skizziert, wie sich der Rechtsmarkt durch KI-basierte Agentensysteme wandelt und wo regulatorischer wie auch ethischer Rahmen dringend geschärft werden muss.

Im Gesundheitswesen ist die digitale Souveränität mehr als nur ein Schlagwort – hier kann sie über Leben entscheiden. Lea Heyder widmet sich daher kritisch den Haftungsfragen beim Einsatz von KI und Robotik in der Medizin und arbeitet die rechtlichen Grauzonen heraus.

Der internationale Blick darf nicht fehlen: Isabel Ecker betrachtet, ob und wie Cyberangriffe das völkerrechtliche Gewaltverbot herausfordern und warum eine einheitliche Staatenpraxis im Umgang mit hybriden Bedrohungen bislang auf sich warten lässt.

In allen Beiträgen wird deutlich: Souveränität ist im digitalen Raum kein statischer Zustand. Sie muss immer wieder neu ausgehandelt und juristisch wie politisch verteidigt werden. Die Diskussion über Open Source, Datenkontrolle, Marktregulierung und staatliche Handlungsspielräume bleibt dabei so lebendig wie notwendig.

Wir wünschen Euch allen ein angenehmes Weihnachtsfest und viel Spaß beim Lesen dieser neunten Ausgabe der CTRL!

Eure Chefredaktion

Larissa Schmitz
Chefredaktion

Ramon Schmitt
Chefredaktion

Ferdinand Wegener
Chefredaktion

Philipp Beckmann
Chefredaktion

Julia Melles
Chefredaktion

Michelle Duda
Chefredaktion

Julia Keselj
Chefredaktion

Isabel Ecker
Chefredaktion

Inhaltsverzeichnis

Grundwissen

5 Datenklau oder legitime Technik? Was man über Web Scraping wissen muss

Aufsätze

10 Zeugnisse der Vergangenheit Das Recht auf Vergessenwerden im Internetzeitalter

20 Künstliche Intelligenz und Robotik in der Medizin Revolution mit Verantwortung

32 Lassen Cyberangriffe das völkerrechtliche Gewaltverbot erodieren?

44 Spannungsfeld: Digitale Souveränität des Staats und das Vergaberecht

Legal Tech

55 KI-Agenten Die neue juristische Arbeitsweise?

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.

Zurück zum Inhaltsverzeichnis

Rückverlinkungen zum dynamischen Inhaltsverzeichnis

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

Die Köpfe
hinter der CTRL

Larissa Schmitz
Chefredaktion

Julia Melles
Chefredaktion

Ramon Schmitt
Chefredaktion

Ferdinand Wegener
Chefredaktion

Michelle Duda
Chefredaktion

Philipp Beckmann
Chefredaktion

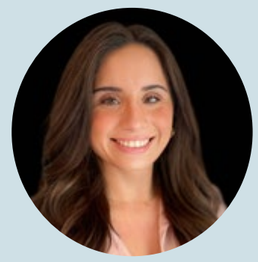
Julia Keselj
Chefredaktion

Isabel Ecker
Chefredaktion

Louis Goral-Wood
Mitbegründer

Hendrik Eppelmann
Lektoratsleitung

Daniel Dischinger
Lektoratsleitung



Maria Ucar
Social Media

Kim Carolin Salg
Social Media

Sophie Kondziela
Layout & Design

„Schon der bloße Kontrollverlust über unsere persönlichen Daten ist ein Schaden.“

Datenklau oder legitime Technik?
Was man über Web Scraping wissen muss

Jonas Neubert

Open Peer Review

Dieser Beitrag wurde lektoriert von: Lea Heyder und Daniel Dischinger

Jonas Neubert hat Rechtswissenschaften an der Friedrich-Schiller-Universität Jena studiert und ein Zertifikatsstudium im Energierecht als Energiejurist (Univ. Jena) abgeschlossen. Er engagiert sich ehrenamtlich im Bereich Legal Tech bei CTRL, LTLC und ethereum.org.

Neulich scrollte ich durch meinen LinkedIn-Feed, als eine Nachricht mich aufschrecken ließ: Wieder einmal waren Millionen von Nutzerdaten im Darknet aufgetaucht. Das brachte mich zum Nachdenken – wie oft geben wir eigentlich gedankenlos unsere persönlichen Informationen preis? Ein Urlaubsfoto hier, eine Telefonnummer dort. Was harmlos erscheint, kann durch Web Scraping, also dem automatisierten Abgreifen von Daten aus dem Internet, zu einem gewaltigen

Datenberg zusammengetragen werden. Besonders brisant wurde das Thema durch das später erläuterte, aufsehenerregende Urteil des Bundesgerichtshofs (BGH) im November 2024.

Aber lassen Sie uns einen Schritt zurückgehen. Web Scraping – für viele klingt das wie ein rätselhafter Fachbegriff aus der IT-Welt. Dabei begegnet uns diese Technologie täglich, ohne dass wir es merken. Stellen Sie sich einen digitalen Staubsauger vor, der durch das Internet surrt und dabei systematisch Informationen aufsaugt: Preise, Texte, Bilder, Profileinträge – alles landet in seiner Datenbank. Manchmal zum Nutzen der Verbraucher, manchmal mit deutlich fragwürdigen Absichten.

Ein Beispiel aus dem Alltag: Wer nicht stundenlang verschiedene Online-Shops nach dem günstigsten Preis für die begehrteste Heißluftfritteuse durchforsten möchte, nutzt ein Preisvergleichsportal. Diese Seiten verwenden Web Scraping, um binnen Sekunden Hunderte von Shops zu durchsuchen. Auch die viel diskutierte KI ChatGPT wurde mithilfe von Web Scraping trainiert – was allerdings nicht unumstritten ist. Die New York Times zog vor Gericht, weil OpenAI ihre Artikel ohne Erlaubnis „gescrapt“ hatte. Das Unternehmen verteidigte sich mit dem Argument des „fair use“ – eine Debatte, die die rechtlichen Grauzonen dieser Technologie deutlich macht.

Der wohl bekannteste Fall von missbrauchtem Web Scraping erschütterte die Social-Media-Welt, als Hacker die „Freunde finden“-Funktion von Meta (ehemals Facebook) ausnutzten. Wie bei einem digitalen Einbruch generierten sie zufällige Telefonnummern und konnten so massenhaft Nutzerprofile absaugen. Das Ergebnis? Über 533 Millionen persönliche Datensätze landeten im Darknet. Viele Betroffene erfuhren erst Monate später davon – ein digitaler Albtraum.

Hier kommt das wegweisende Urteil des BGH ins Spiel. Die Richter haben erkannt, was viele von uns intuitiv spüren: Schon der bloße Kontrollverlust über unsere persönlichen Daten ist ein Schaden – auch wenn (noch) kein konkreter Missbrauch stattgefunden hat. Das ist, als würde jemand Ihren Hausschlüssel kopieren. Selbst wenn nicht eingebrochen wurde, fühlen Sie sich zu Recht unsicher. Der BGH sieht Schadensersatzbeträge von 100 bis 250 Euro pro Person als angemessen an. Bei 533 Millionen Betroffenen ergibt das eine astronomische Summe von über 50 Milliarden Euro – selbst für einen Giganten wie Meta eine schmerzhafte Perspektive.

> „Schon der bloße Kontrollverlust über unsere persönlichen Daten ist ein Schaden“

Als Technikbegeisterter fasziniert mich besonders die technische Seite des Web Scrapings. Stellen Sie sich vor, Sie betreten eine riesige Bibliothek. Anstatt jeden einzelnen Band händisch durchzublättern, haben Sie einen hochentwickelten

Roboter, der das für Sie übernimmt. Genauso arbeitet Web Scraping. Lassen Sie mich Ihnen einen Blick hinter die Kulissen gewähren.

Im Kern ist jedes Scraping-Programm wie ein sehr schneller, automatisierter Webbrowser. Wenn Sie eine Website besuchen, sendet Ihr Browser eine HTTP-Anfrage – quasi einen digitalen Handschlag. Scraping-Tools wie Python's requests oder urllib machen genau das Gleiche, nur tausendfach schneller. Sie tarnen sich dabei mit sogenannten „User-Agent-Strings", einer Art digitalem Verkleidungsset, um wie ein normaler Browser zu erscheinen. Besonders spannend wird es bei der Datenverarbeitung. Wenn die Webseite einmal geladen ist, kommt die „Parse-Phase" – sozusagen das Aufdröseln des digitalen Garns. Tools wie BeautifulSoup oder lxml verwandeln den verschachtelten HTML-Code in einen übersichtlichen Strukturbaum, den DOM (Document Object Model). Stellen Sie sich vor, Sie hätten eine komplizierte Origami-Figur, die Sie vorsichtig entfalten, um zu verstehen, wie sie aufgebaut ist. Genauso arbeiten diese Parser.

Ein faszinierender Aspekt, den ich kürzlich bei einem Projekt kennenlernte, ist die Bildanalyse. Moderne Scraping-Tools sind wahre Alleskönner. Sie können nicht nur Text aus Webseiten lesen, sondern auch Text aus Bildern extrahieren. Dafür nutzen sie OCR (Optical Character Recognition) – die gleiche Technologie, die auch in Dokumentenscannern steckt. Ich erinnere mich an einen Fall, wo ein Scraper Preise aus Produktbildern eines Online-Shops las, weil der Betreiber versucht hatte, das Scraping durch Einbettung der Preise als Bilder zu verhindern. Ein cleveres Katz-und-Maus-Spiel!

Noch komplexer wird es bei dynamischen Webseiten. Viele moderne Websites laden ihre Inhalte erst nach, wenn Sie scrollen oder klicken. Für solche Fälle kommen „Headless Browser" zum Einsatz – Browser ohne Benutzeroberfläche, die JavaScript ausführen können. Selenium oder Puppeteer sind beliebte Tools dafür. Sie können sogar Mausklicks und Scrollbewegungen simulieren, als säße ein echter Mensch vor dem Bildschirm.

Die Webseitenbetreiber bleiben natürlich nicht untätig. Sie entwickeln immer ausgefeiltere Abwehrmechanismen. CAPTCHA-Systeme kennen Sie vermutlich – diese nervigen „Ich bin kein Roboter"-Tests. Aber es gibt noch viel mehr: Rate Limiting begrenzt die Anzahl der Anfragen von einer IP-Adresse, Honeypot-Links sind unsichtbare Fallen für Bots, und manche Seiten verschlüsseln ihre Daten auf komplizierte Weise.

Die Scraping-Community hat darauf kreative Antworten gefunden. Proxy-Rotation lässt Anfragen wie von verschiedenen Computern weltweit erscheinen. Browser-Fingerprinting simuliert authentisches Nutzerverhalten bis ins kleinste Detail. Einige Tools können sogar CAPTCHAs automatisch lösen – wobei die Legalität solcher Systeme oft fragwürdig ist. Als ich mit einem erfahrenen Web-Entwickler sprach, verglich er es mit einem digitalen Wettrüsten. Sobald eine Seite neue Schutzmechanismen einführt, finden Scraper Wege, sie zu umgehen. Deshalb ändern sich die CAPTCHA-Interfaces für uns Internetnutzer ständig und werden dementsprechend komplexer zu lösen. Eines der größten technischen Probleme beim Scraping ist die Skalierung. Stellen Sie sich vor, Sie möchten Millionen von Produktpreisen täglich aktuell halten. Das erfordert nicht nur enorme Rechenleistung, sondern auch eine ausgeklügelte Fehlerbehandlung. Was passiert, wenn eine Webseite nicht erreichbar ist? Wenn sich das Layout ändert? Wenn Ihre IP gesperrt wird? Professionelle Scraping-Systeme müssen all diese Fälle abfangen und intelligent darauf reagieren.

„Als ich mit einem erfahrenen Web-Entwickler sprach, verglich er es mit einem digitalen Wettrüsten“

Das BGH-Urteil wirft natürlich auch praktische Fragen auf. Wie soll man nachweisen, dass die eigenen Daten gescrapt wurden? Viele Menschen wissen gar nicht, dass ihre Informationen irgendwo im Darknet kursieren.

Immerhin: Das neue Leitentscheidungsverfahren ermöglicht es, tausende ähnlicher Fälle zu bündeln – ein wichtiger Schritt für effektiven Rechtsschutz in der digitalen Ära.

Was können wir konkret tun? „Ich habe doch nichts zu verbergen!“ – Diesen Satz höre ich oft. Aber unterschätzen Sie nicht die Macht der Datenkombination. Ein harmlos erscheinendes Hundefoto, verbunden mit Ihrem Arbeitsort und einem Like für eine Gesundheitsseite, kann verräterische Rückschlüsse zulassen. Plötzlich wissen Dritte, dass Sie viel auf Geschäftsreisen sind, allein wohnen und möglicherweise gesundheitliche Probleme haben – ein gefundenes Fressen für Versicherungen, potenzielle Arbeitgeber oder gar Betrüger. Seien Sie wachsam bei Apps, die Zugriff auf Ihre Kontakte wollen. Hinterfragen Sie Gewinnspielformulare kritisch. Überprüfen Sie Ihre Privatsphäre-Einstellungen regelmäßig. Und ja, auch starke Passwörter sind wichtiger denn je. Unternehmen müssen ihrer Verantwortung für Datensicherheit gerecht werden – notfalls durch empfindliche Strafen

.

Die Zukunft des Web Scrapings wird durch künstliche Intelligenz noch effizienter werden. Gleichzeitig entwickeln sich Gegenmittel, wie Tools, die persönliche Daten verschleiern oder gezielt Falschinformationen streuen, um Scraper in die Irre zu führen. Auch die Gesetzgeber werden aktiv. In den USA diskutierte man den „American Data Privacy and Protection Act“, der ähnlich wie die europäische DS-GVO Unternehmen stärker in die Pflicht nehmen sollte.

„Seien Sie wachsam bei Apps, die Zugriff auf Ihre Kontakte wollen“

Am Ende steht eine fundamentale Frage: Sind unsere Daten wirklich “Free Real Estate“, eine Ressource, die beliebig verwendet werden darf? Oder gleichen sie eher einem persönlichen Tagebuch, das niemand ohne ausdrückliche Erlaubnis anfassen sollte? Das BGH-Urteil sendet ein klares Signal in Richtung der zweiten Interpretation. Und das ist gut so – denn in einer zunehmend digitalen Welt brauchen wir klare Regeln zum Schutz unserer Privatsphäre.

Zurück zum Inhaltsverzeichnis

„Unternehmen, die zu Sammlern und Aggregatoren von Nutzerdaten geworden sind, haben heute mehr Macht und Einfluss als viele souveräne Staaten. “

Aufsatz

Zeugnisse der Vergangenheit
Das Recht auf Vergessenwerden im Internetzeitalter

Luisa Mayr

Open Peer Review

Dieser Beitrag wurde lektoriert von: Tim Rösch und Daniel Dischinger

Luisa Mayr studiert Rechtswissenschaft an der Universität Oxford und verbringt ihr Auslandsjahr an der Universität Bonn. Sie hat einen Artikel zur Schnittstelle von Haftungsregimen für KI-Technologien unter Sandbox-Regulierung veröffentlicht und interessiert sich besonders für die rechtsphilosophischen Diskurse, die den neuen rechtlichen Herausforderungen digitaler Technologien zugrunde liegen.

Der vorliegende Beitrag analysiert das rechtliche Spannungsfeld zwischen der Kontrolle der Nutzer über ihre persönlichen Daten und der Informationsfreiheit, die für das Funktionieren des demokratischen Diskurses notwendig ist. Es werden die philosophischen Grundlagen dieses Konflikts analysiert, bevor auf empirischer Ebene untersucht wird, wie sich dieses Spannungsverhältnis auf die Entwicklung des Datenschutzes ausgewirkt hat.

Wie kann man einen Ausgleich zwischen diesen Gegensätzen schaffen? Welches Maß an Kontrolle der Nutzer über ihre Daten ist gerechtfertigt? Das ist eine zentrale Frage angesichts der gegensätzlichen Richtungen, in die sich diese Spannungen entwickeln. Die Gerichte haben hier mit dem Recht auf Vergessen einen Ausgleich gefunden, der in diesem Artikel einer Bewertung unterzogen wird.

A. Philosophische Grundlagen

Mit der zunehmenden Bedeutung personenbezogener Daten hat sich die Frage eines angemessenen Datenschutzes zu einem vielschichtigen Rechtsproblem herauskristallisiert. Fehlende gesetzliche Beschränkungen würden Unternehmen erlauben, die Datenextraktion ohne persönliche Einwilligung zu maximieren und den Datenschutz zu ignorieren.[1] Es besteht demnach ein offensichtlicher Bedarf nach einem Recht zum Schutz der Privatsphäre, aber es herrscht noch kein Konsens über dessen Ausgestaltung.

I. Ursprung der Idee: Das Recht auf Selbstbestimmung über persönliche Daten

Shulga-Morskaya vertritt in ihrem Artikel die Ansicht, dass ein Recht auf informationelle Selbstbestimmung die sinnvollste Lösung darstellt.[2] Sie erläutert die rechtlichen Grundlagen, die auf ein Urteil des Bundesverfassungsgerichts aus dem Jahr 1983 zur Rechtmäßigkeit der Datenerhebung im Rahmen einer Volkszählung zurückgehen.[3] Das Gericht stellte fest, dass es kein spezifisches Recht auf Schutz vor derartigen Datenerhebungen gibt. Die Entwicklung eines neuen Grundrechts durch die Verfassungsrichter erfolgte daher unter der Prämisse einer weiten Auslegung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 GG ausdrücklich in Verbindung mit dem Recht auf Menschenwürde aus Art. 1 Abs. 1 GG.[4]

Das Recht auf Vergessenwerden ist aus diesem Grundsatz der informationellen Selbstbestimmung hervorgegangen, und es wird häufig als Alternative zu einem umfassenden Eigentumsrecht an personenbezogenen Daten dargestellt. **Cohen** führt zwei Argumente an, warum diese Rechtslage Nutzer:innen benachteiligen würde.[5] Erstens verweist er auf die bestehende Informationsasymmetrie: Nutzer:innen sind sich oft nicht bewusst, wie ihre Daten im Rahmen immer ausgeklügelter Methoden verwendet, weitergegeben und monetarisiert werden. Infolgedessen können sie die Risiken für ihre Privatsphäre oft nicht richtig einschätzen, um fundierte Entscheidungen zu treffen.

Zweitens betont **Cohen** die begrenzte Rationalität: Verbraucher:innen sind oft bereit, die Bedingungen von Datenverarbeiter:innen zu akzeptieren, aus Bequemlichkeit, ohne über die langfristigen Folgen nachzudenken. Studien aus der Verhaltensökonomie stützen diese Schlussfolgerung und zeigen, dass Verbraucher:innen kurzfristige Vorteile wie kostenlose Dienste über Datenschutzbedenken stellen. Cohen ist daher

1 Schwartz, Harv. LR 2004, 2056 (2056-2128).
2 Shulga-Morskaya, Protection of Personal Data Through Implementation of the Right to Informational Self-Determination, hier abrufbar (Stand: 06.12.2024).
3 BVerfGE 65, 1 – Volkszählung.
4 Fn. 4.
5 Cohen, STAN. L. REV. 2000, 1373 (1423-1428); Fn. 1 (2076-2083).

der Ansicht, dass ein solches Eigentumsrecht von persönlichen Daten zu einer Verschlechterung der Situation führen würde, da es die Verbraucher:innen überfordert. Es ist effizienter, wenn das Recht auf Vergessenwerden den Verbraucher:innen nur begrenzte Kontrollmöglichkeiten bietet.

II. Der Preis der Privatsphäre: Konflikt mit Informationsfreiheit

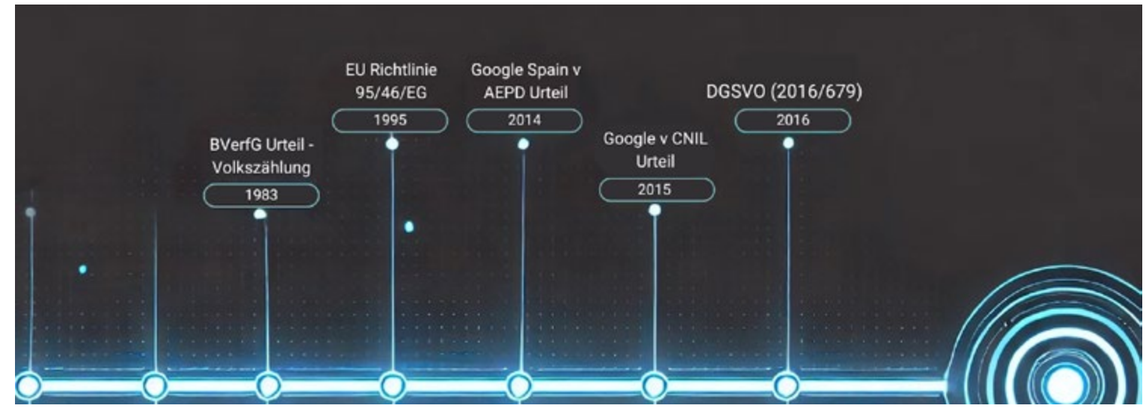
Wo Licht ist, ist auch Schatten. Die Möglichkeiten, seine Online-Präsenz zu verbessern, stehen im Spannungsverhältnis zur Informationsfreiheit, wenn sie über einen angemessenen Rahmen hinaus genutzt werden. Daten spielen nicht nur eine zentrale Rolle für die individuelle Identität, sondern erfüllen zugleich eine kollektive Funktion innerhalb der Gesellschaft.[6] Das Konzept des Informationsgemeinguts beinhaltet, dass die Privatsphäre nicht vom Wohlergehen der Gesellschaft losgelöst zu betrachten ist. Beispielsweise können demografische Daten oft Auslöser für politische Veränderungen sein, die zu mehr Gerechtigkeit und Chancengleichheit führen.

Zwischen 2015 und 2021 gab es Millionen an Auslistungsanträgen bei Suchmaschinen wie Bing und Google.[7] Sollte der Zugang zu diesen Informationen durch das Recht auf Vergessenwerden eingeschränkt werden? Wenn man die Entfernung persönlicher Suchanfragen vom Informationsgemeingut zulässt, muss man das Gleichgewicht zwischen persönlichem und öffentlichem Interesse abwägen. Die Regelung sollte nach Möglichkeit dieses Gleichgewicht gewährleisten.

B. Europas Verteidigung der Privatsphäre

In der Hoffnung, einen Ausgleich zu finden, haben sich Gesetzgeber und Gerichte immer wieder mit diesem Spannungsverhältnis auseinandergesetzt und so die Entwicklung der Datenschutzrechte geprägt.

6 van der Sloot, Law Innov. Technol. 2021, 223 (255).
7 Hier abrufbar (Stand: 12.01.2025).



I. Richtlinie 95/46/EG[8]

Während die Mitglieder des Europäischen Parlaments in den 1970er Jahren immer wieder strengere Datenschutzmaßnahmen forderten, begann die Kommission erst in den 1990er Jahren, die Datenschutzrichtlinie (Richtlinie 95/46/EG) auszuarbeiten. Dies war der erste bedeutende Schritt zur Schaffung eines effizienten Datenschutzes in der EU, wobei zwei zentrale Artikel besondere Aufmerksamkeit verdienen. Art. 12(b) garantiert die Berichtigung, Löschung oder Sperrung auf Antrag, soweit die Daten unvollständig oder fehlerhaft sind. Art. 14(a) sichert den Betroffenen das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, Widerspruch gegen die Verarbeitung ihrer Daten einzulegen, sofern das nationale Recht nichts anderes vorsieht. Wird dem Widerspruch stattgegeben, so darf die Verarbeitung der betreffenden Daten nicht fortgesetzt werden.

II. Entscheidungen des Europäischen Gerichtshofes

Auf Grundlage dieser Richtlinie wurde später vom Gerichtshof der Europäischen Union (EuGH) das Recht auf Vergessen entwickelt. Es wurde jedoch zuerst durch das sogenannte Google-Spain-Urteil bekannt. Der EuGH war mit der Schwierigkeit

8 Richtlinie 95/46/EG, 24.10.1995, ABl. L 281, 23.11.1995, hier abrufbar (Stand: 28.12.2024).

konfrontiert, neue Umstände basierend auf einer Verordnung von 1995 zu behandeln, die zu einer Zeit verfasst worden war, als das Internet gerade erst dabei war zu entstehen.

1. Google Spain SL gegen AEPD[9]

Im Mittelpunkt des Verfahrens stand ein Antrag von **Herrn González**, der die Entfernung seiner persönlichen Daten aus dem Index von **Google** sowie die Sperrung des künftigen Zugangs zu diesen Daten anstrebte. Es wurde insbesondere auf einen Artikel der Tageszeitung **La Vanguardia** aus dem Jahr 1998 verwiesen, in dem über eine Versteigerung seines Grundstücks aufgrund nicht geleisteter Beiträge zur Sozialversicherung berichtet wurde. **Herr González** forderte ein Ende der Berichterstattung, da die betreffende Angelegenheit seit Langem abgeschlossen war.

Der EuGH stellte im Mai 2014 in einer Grundsatzentscheidung klar, dass der materielle Anwendungsbereich der Richtlinie 95/46/EG[10] ein sogenanntes Recht auf Vergessenwerden (de-Listing) umfasst. Trotz seines begrenzten Geltungsbereiches zeigt der Gerichtshof eine positive Einstellung zum Schutz personenbezogener Daten. Zwei Aspekte dieses Urteils sind in diesem Zusammenhang hervorzuheben. Erstens wurde die Verantwortung der Suchmaschine für Online-Inhalte festgelegt. Zweitens musste das Gericht dieses Recht mit Art. 11 der Charta der Grundrechte der Europäischen Union in Einklang bringen.[11]

9 EuGH, C-131/12 - Google Spain SL und Google Inc. / Agencia Española de Protección de Datos und Mario Costeja González.
10 Fn. 9, S. 31–50.
11 Art. 11 Charta der Grundrechte der Europäischen Union, Titel II, ABl. C 364, 18.12.2000, S. 1–22.

a) Zuständigkeit der Suchmaschine für ihre Ergebnisse

Eine Grundfrage, die dem Gericht vorgelegt wurde, betraf die rechtliche Einordnung der Tätigkeiten einer Suchmaschine als „Datenverarbeitung"; nur dann erfüllt Google die Definition eines „für die Verarbeitung Verantwortlichen", gemäß Art. 2(d) der Richtlinie.[12]

> Art. 2(d) der Richtlinie 95/46 definiert der „für die Verarbeitung Verantwortliche" als „die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet."[1]
>
> 1 Fn. 9, Art. 2(d).

Die Verarbeitung personenbezogener Daten wurde in der Richtlinie umfangreich definiert. Es umfasst sowohl das Erheben, das Speichern, die Benutzung und die Weitergabe von Daten als auch das Sperren oder Vernichten jener Datensätze.[13] Google plädierte, dass seine Funktion nicht unter die Definition des Art. 2(d) fallen würde, da es weder über Kenntnisse der Daten verfüge noch Kontrolle über diese ausübe.

Dies fand im Gerichtsentscheid allerdings keine Berücksichtigung. Der EuGH entschied, dass der Betrieb einer Suchmaschine der Definition eines für Datenverarbeitung Verantwortlichen zuzuordnen ist, da Inhalte, die von Dritten ins Internet gestellt werden, von der Suchmaschine prozessiert, dann automatisch indexiert und Nutzer:innen in einem Ranking zur Verfügung gestellt werden. **Google** übt daher auch einen großen Einfluss auf die Sichtbarkeit dieser Daten und der Weblinks für die

12 Fn. 9, Art. 2(d).
13 Fn. 10, Rn. 21-28.

einzelnen Nutzer:innen aus. Zudem wird die Weitergabe der Daten durch das detaillierte Profil der Nutzer:innen der Suchmaschine bestimmt.[14] Das Urteil entsprach damit dem Ziel der Datenschutzrichtlinie.[15] Die Argumentation basiert auf den logischen Schlussfolgerungen der früheren Rechtsprechung, einschließlich des Urteils Satakunnan Markkinapörssi und Santamedia,[16] wobei festgestellt wurde, dass eine andere Auslegung hier den Zweck und Effekt der Richtlinie beeinträchtigen würde.

b) Ein Drahtseilakt der Grundrechte

Das Recht auf Vergessenwerden gilt jedoch nicht absolut und uneingeschränkt. Die Entfernung und Löschung von Links führen zur Erschwerung der Verbreitung von wichtigen Informationen, weshalb das Recht nur Anwendung in Situationen finden soll, in denen das Interesse einer Person am persönlichen Datenschutz das öffentliche Interesse überwiegt. So musste das Gericht die individuellen Rechte nach Art. 7 und 8 der Europäischen Charta der Grundrechte einerseits dem Recht der Öffentlichkeit zur Information nach Art. 11 andererseits gegenüberstellen.[17]

Um ein Gleichgewicht zwischen diesen Rechten herzustellen, stützte sich das Gericht auf den Grundsatz der Verhältnismäßigkeit. Mehrere Faktoren müssen hierbei berücksichtigt werden: Sind die Informationen richtig und relevant oder veraltet und irreführend? Ebenfalls wichtig ist der Antragsteller selbst: das öffentliche Interesse an den Informationen ist von höherem Gewicht, wenn es sich um eine Person des öffentlichen Lebens handelt. Ferner ist der Zeitfaktor zu berücksichtigen: Es wird vermutet, dass Informationen mit der Zeit an Relevanz verlieren und somit von geringerer öffentlicher Bedeutung sind.

Ein wichtiger Kritikpunkt ist hier jedoch, dass das Gericht diese Abwägung der Angemessenheit den Eigentümern der Suchmaschine überlässt. Eigentümer wie Google haben aber ein starkes kommerzielles Interesse an der Speicherung von Online-Informationen und stellen daher keine neutrale Partei dar. Dies gibt Anlass zur Sorge: Wenn das Gericht den Eigentümern der Suchmaschinen zu viel Kontrolle erlaubt, besteht die Gefahr, dass dieses Recht nicht ausreichend gewährleistet wird.

2. Google gegen CNIL und die territoriale Reichweite[18]

Eine weitere Entwicklung des Rechts auf Vergessenwerden erfolgte im Jahr 2015. Google wollte die Auslistungsanträge nur auf Suchergebnisse innerhalb der EU beschränken, anstatt die Entfernung auf weltweite Domains seiner Suchmaschine umzusetzen. Die französische Datenschutzbehörde Commission Nationale de l'Informatique et des Libertés (CNIL) verhängte eine Geldstrafe in Höhe von 100.000€ gegen Google und wandte sich an denEuGH mit der Forderung, den territorialen Geltungsbereich des Rechts auf Vergessenwerden festzulegen.

Der EuGH entschied diesen Streit in erster Linie im Rahmen der neuen EU-Datenschutz-Grundverordnung 2016/679 (DSGVO), die das Recht auf Vergessenwerden in Art. 17 Abs. 1 ausdrücklich festlegt.[19]

Art. 17 Abs. 1 DSGVO: „Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen." Abs. 3 sieht jedoch Ausnahmen vor zur „Ausübung des Rechts auf freie Meinungsäußerung und Information."

14 Fn. 10, Rn. 36-37.
15 Fn. 10, Rn. 34.
16 EuGH, C-73/07 - Tietosuojavaltuutettu / Satakunnan Markkinapörssi Oy and Satamedia Oy; Kranenborg, EDPL 2015, 1 (70).
17 Fn. 10, Rn. 81.

18 EuGH, C-507/17 - Google Inc. / Commission nationale de l'informatique et des libertés (CNIL).
19 EU-Verordnung (2016/679), 27.04.2016, ABl. L 119, 04.05.2016, S. 1–88.

Einerseits zielt die DSGVO darauf ab, ein hohes Schutzniveau für personenbezogene Daten in der gesamten Europäischen Union herzustellen.[20] Nur eine umfassende Entfernung aus sämtlichen Versionen einer Suchmaschine würde diesem Ziel vollständig entsprechen. Andererseits erschweren die grenzüberschreitenden Netzwerke des Internets, die Verlinkungen weltweit zugänglich zu machen, die praktische Umsetzung einer solchen Maßnahme.

In Anbetracht dieser globalen Vernetzung hat sich der Gerichtshof mit Zurückhaltung geäußert, um die grundlegenden Prinzipien des Völkerrechts, wie beispielsweise die „Völkerrechtliche Courtoisie" oder das „Interventionsverbot", nicht zu missachten.[21] Eine globale Anwendung des Rechts könnte die Verletzung der Souveränität von Drittstaaten gefährden, da zahlreiche Drittstaaten das Recht auf Vergessenwerden nicht anerkennen oder einen anderen Ansatz verfolgen. Auch wenn sie es anerkennen, werden verschiedene Drittstaaten das Spannungsverhältnis zwischen Privatsphäre und Informationsfreiheit unterschiedlich bewerten. Die weltweite Anwendung eines EU-Beschlusses hätte dann zur Folge, dass die Vorstellungen der EU von einem gerechten Ausgleich auch diesen Drittstaaten aufgezwungen würden.

Jedoch hat das Gericht die Verwendung von Geoblocking-Maßnahmen unterstützt, um zu verhindern, dass Nutzer:innen innerhalb der EU über Nicht-EU-Domänen auf die betreffenden Inhalte zugreifen können, wie z.B. google.com.[22]

C. Kritik und Analyse

Warum ist die Entwicklung dieses Rechts so wichtig? Der Anspruch auf die Löschung gewisser Daten ist nichts Neues.[23] In den meisten Rechtssystemen werden gewisse persönliche Daten nach einer bestimmten Frist gelöscht: Einträge im deutschen Strafregister aufgrund einer Geldstrafe oder von Gefängnisstrafen unter 3 Monaten werden nach 3 Jahren gelöscht, und Strafen über 3 Monate nach 5 Jahren. Damit wird anerkannt, dass kompromittierende Informationen aus der Vergangenheit nach einer gewissen Zeit an Relevanz verlieren.

Im Zeitalter der Technologie wird jedoch eine erhebliche Menge an Informationen zeitlich unbegrenzt allen zur Verfügung gestellt. Immer häufiger werden Personen mit alten Daten konfrontiert, die ihnen gewisse Möglichkeiten verwehren könnten.

I. Die Schattenseiten des Überwachungskapitalismus

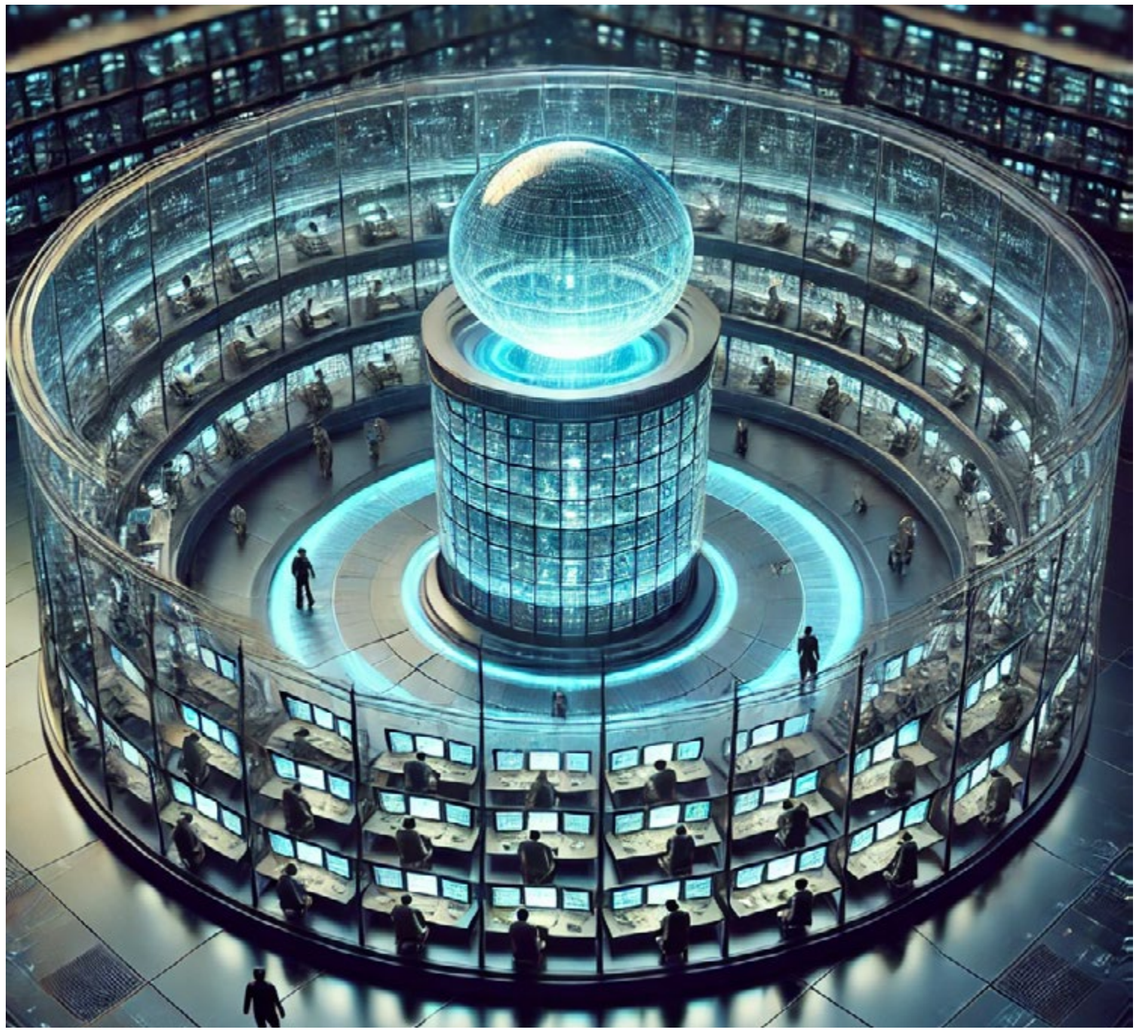
Das Phänomen der Massenerhebung von Daten wurde von der Harvard-Professorin **Shoshana Zuboff** als das neue Zeitalter des Überwachungskapitalismus bezeichnet.[24] Sie führt aus, dass jede Epoche des Kapitalismus einer dominanten Akkumulationslogik folgt; von der Massenproduktion zum Finanzkapitalismus im 20. Jahrhundert und zum datenbasierten Kapitalismus im 21. Jahrhundert.[25] Der Begriff „Informations-Zivilisation" beschreibt die Art und Weise, wie „Big Data" auf der Akkumulation von alltäglichen Erfahrungen Einzelner basiert. Diese werden aufgezeichnet und kommerzialisiert, um neue Wege der Monetarisierung zu finden.

Die Entwicklung dieses Systems des Überwachungskapitalismus erinnert an **Benthams** „Panoptikum"[26]: Nutzer:innen wissen oft nicht, wann und in welchem Umfang sie beobachtet werden und wie ihre Daten überwacht und weitergegeben werden.[27] **Zuboff** sieht dies jedoch nicht als eine zwangsläufige Folge des technologischen Fortschritts, sondern als ein gezieltes Instrument zur Gewinnmaximierung an. Die Entwicklung des Rechts auf Vergessenwerden entzieht diesen Unternehmen einen Teil der Kontrolle und gibt Nutzer:innen die Möglichkeit, sich von ihrer Vergangenheit zu distanzieren. In Deutschland und der EU wird diese Thematik auf politischer Ebene thematisiert: Vorschläge zur „Zerschlagung" von **Google** werden

20 Fn. 21, Art. 10, 11, 13, 17.
21 Fn. 19, Rn. 58-67.
22 Fn. 19, Rn. 70-72.
23 Sartor, Int. J. Law Inform. Technol. 2016, 24, 72 (98).

24 Zuboff, Journal of Information Technology 2015, 75 (75).
25 Fn. 21, (77).
26 Foucault, Discipline and Punish: The birth of the Prison, 1975 (205-207).
27 The Guardian, What does the panopticon mean in the age of digital surveillance?, hier abrufbar (Stand: 14.12.2024).

diskutiert[28] und Maßnahmen wie der Digital Services Act[29] wurden bereits im Jahr 2022 eingeführt.



28 Financial Times, Google break-up plan emerges from Brussels, hier abrufbar (Stand: 15.01.2025).
29 Verordnung (EU) 2022/2065 über einen Binnenmarkt für digitale Dienste (Digital Services Act), KOM (2022)2065 final.

II. Markttransparenz als Lichtblick

Dieses Bestreben nach Regulierung wird nicht von allen geteilt. **Varian** betont das transformative Potenzial von „Big Data", das zu einer Optimierung der wirtschaftlichen Abläufe beitragen kann30, und die neoliberale Marktvorstellung von einem intrinsisch undurchschaubaren Markt grundsätzlich hinterfragt.[31]

Er nennt vier innovative Anwendungen dieser Transparenz zur Untermauerung seiner Schlussfolgerung: i) Datenextraktion und -analyse, ii) neue Vertragsformen durch bessere Überwachung, iii) Personalisierung und Anpassung sowie iv) kontinuierliche Experimente.[32] Durch diese Fähigkeiten ergibt sich die Chance, bisher unerkanntes Verhalten zu beobachten. Beispielsweise könnte, im Fall der Nichtleistung der monatlichen Zahlungen eines Autokredits, der Autokreditgeber das Auto des Schuldners per Überwachungssystem deaktivieren und den Standort bestimmen. Dieser Übergang zur Echtzeitüberwachung verdeutlicht das Potenzial der gesteigerten Markttransparenz.

Unter Berücksichtigung beider oben dargestellten Ansichten hat der EuGH folgendes Gleichgewicht gefunden. Einerseits werden die potenziellen Vorteile der technologischen Innovation und Transparenz nicht durch strikte Pauschalregelungen eingeschränkt. Andererseits behalten die Nutzer ein gewisses Maß an Kontrolle über ihre gesammelten Informationen und die Ergebnisse, die in Suchmaschinen angezeigt werden. Damit ist es ihnen möglich, die Gestaltung ihres digitalen Erscheinungsbildes im Internet zu beeinflussen und ein gewisses Maß an Vertrauen in Unternehmen der „Big Data"- Branche zu behalten.

30 Varian, American Economic Review 2010, 100(2): 1–10.
31 Hayek, The Fatal Conceit: The errors of socialism, 1988 (14-15).
32 Varian, Business Economics 2014, 49(1): 27–31.

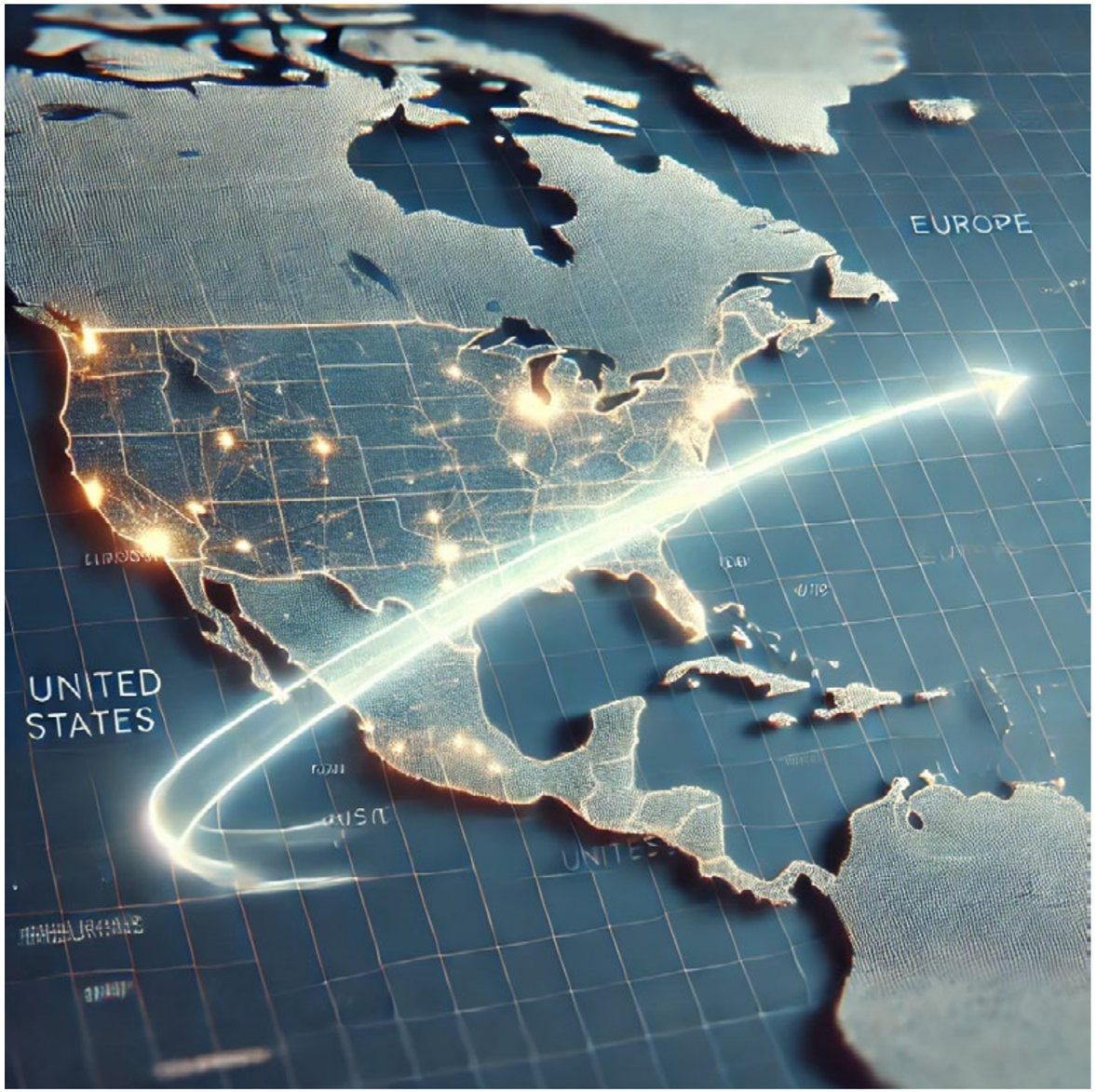
III. Die praktischen Herausforderungen im Datenschutz

Systembedingte Probleme und Herausforderungen bei der praktischen Umsetzung können jedoch dazu führen, dass das angestrebte Gleichgewicht von vornherein instabil ist. Wie **Shulga-Morskaya** betont, gehen die meisten Vorschriften von einer bilateralen Beziehung zwischen der betroffenen Person und der für die Verarbeitung verantwortlichen Person aus („data subject – controller"). Die Realität moderner Datenökosysteme ist jedoch eine andere: In der Praxis erfolgt die Datenverarbeitung in einem komplexen Netzwerk von betroffenen Personen und einer Vielzahl von Verantwortlichen („data subject – plethora of controllers").[33]

Als Beispiel führt sie den Einsatz von Werbetechnologien (Ad-Tech) auf Websites an. Diese funktionieren, indem sie persönliche Daten über Cookies und Zählpixel sammeln, die dann in Echtzeit-Auktionen verwendet werden. Ohne Wissen der Nutzer:innen konkurrieren Hunderte von Unternehmen um Werbeplätze auf der Website. Diese „unsichtbare Verarbeitung" schränkt Nutzer:innen in der Kontrolle ihrer eigenen Daten erheblich ein. Das Ad-Tech-System[34] stellt somit ein grundlegendes Machtungleichgewicht zwischen Nutzer:innen und Unternehmen dar.

D. Die Zukunft des Rechts auf Vergessenwerden

Die Weiterentwicklung dieses Rechts ist international von politischem Interesse, insbesondere während der zweiten Amtszeit von US-Präsident **Donald Trump**.[35] 2017 hatte er noch seine Bereitschaft zur Zusammenarbeit beim EU-U.S. Data Privacy Framework (DPF) gezeigt, da US-Unternehmen ohne dieses Abkommen auf den europäischen Märkten benachteiligt gewesen wären.[36] Was passiert aber, wenn die wirtschaftlichen Interessen nicht mehr mit dem Datenschutz übereinstimmen?



33 Fn. 3, (8-10).
34 Fn. 3, (9).
35 Financial Times, EU reassesses tech probes into Apple, Google and Meta, hier abrufbar (Stand 15.01.2025).
36 Lawfare Media, The Trump Administration Should Not Mess With the EU-U.S. Data Privacy Framework, hier abrufbar (Stand 21.01.2025).

Eine Antwort kann aus dem Umgang der USA mit der DSGVO abgeleitet werden. Diese wurde in offiziellen Stellungnahmen unter **Trump** als Instrument zur Begrenzung der Macht von US-Unternehmen angesehen.[37] Für US-Unternehmen bedeutet das Recht auf Vergessenwerden ebenso wie die DSGVO einen erheblichen Aufwand. Dies ist ein Ausdruck der ideologischen Kluft zwischen der Betonung des Schutzes der Privatsphäre in der EU und der Betonung freier Märkte, der Meinungsfreiheit und der geringen Regulierung in den USA. Wenn europäische Datenschutzstandards wie das Recht auf Vergessenwerden als eine Form der Zensur der Informationsfreiheit angesehen werden, besteht die Gefahr, dass **Trumps** Agenda die Deregulierung in der EU vorantreibt.

Bei seiner zweiten Amtseinführung waren die meisten Eigentümer großer US-Unternehmen anwesend, allen voran **Elon Musk** von **X**, der den Co-Vorsitz des Department of Government Efficiency (DOGE) übernimmt. Zum Schutz personenbezogener Daten, schränkte ein Gerichtsbeschluss den Zugang von DOGE zu Daten des US-Finanzministeriums ein.[38] Angesichts der engen Verbindung der neuen US-Regierung mit führenden Unternehmen im Silicon Valley ist es unwahrscheinlich, dass dem Schutz personenbezogener Daten gegenüber den wirtschaftlichen Interessen von US-Unternehmen Vorrang eingeräumt wird.

E. Fazit

Gerichte und Regulierungsbehörden werden mit drei konkurrierenden Interessen konfrontiert: Dem Bedürfnis von Privatunternehmen und Regierungen nach Daten und dem Recht auf sowie dem individuellen Interesse an Privatsphäre. Die Verflechtungen von Unternehmen und Regierungen nehmen kontinuierlich zu, anstatt dass diese als separate Machtfaktoren auftreten. Gemeinsam verfügen sie über eine weitaus größere Fähigkeit, ihre Macht zu missbrauchen. In den USA kann man derzeit verfolgen, wie das Gegengewicht und die Kontrollfunktionen der staatlichen Macht aufgrund enger Beziehungen zur Privatwirtschaft weniger wirksam werden. Dies erhöht die Relevanz von gesetzlichen Regelungen wie dem Recht auf Vergessenwerden, welche im „Zeitalter des Überwachungskapitalismus“ einen essenziellen Schutz der Nutzer gewährleisten.

Zurück zum Inhaltsverzeichnis

37 Politico, Why Trump's administration is going after the GDPR, hier abrufbar (Stand: 22.01.2025).
38 Financial Times, The courts stand between Musk and a Treasury takeover, hier abrufbar (Stand: 12.02.2025).

„Das Potenzial der Anwendung von KI und Robotik in der Medizin ist groß.“

Aufsatz

Künstliche Intelligenz und Robotik in der Medizin

Revolution mit Verantwortung

Lea Heyder

Open Peer Review

Dieser Beitrag wurde lektoriert von: Victoria Williams und Tim Stephan

Lea Heyder studiert seit dem Wintersemester 2018/19 Jura an der Universität zu Köln und hat den Schwerpunkt Internationales Strafrecht, Strafverfahren und praxisrelevante Gebiete des Strafrechts absolviert.

Sie kennen sie aus Filmen wie **iRobot (Will Smith), Matrix (Keanu Reeves),** aber auch **Star Wars.** Roboter und künstliche Intelligenzen sind seit Jahren Bestandteile von Kinoleinwänden. Wie sieht es jedoch aus, wenn diese tatsächlich am Menschen eingesetzt werden?[1] Wenn diese in der Chirurgie assistieren und medizini-

1 Beck/Faber/Gerndt, Rechtliche Aspekte des Einsatzes von KI und Robotik in Medizin und Pflege, Ethik Med 35, 2023, 247 (249).

sche Daten zur Erkennung von Krankheiten auswerten?[2] Und das schneller und präziser, als ein Mensch es in der gleichen Zeit je könnte.

Der Einsatz der Technologien bringt viele Möglichkeiten mit sich. Probleme entstehen insbesondere dann, wenn Fehler durch oder beim Einsatz des KI-Systems passieren.

Aber wer haftet in einem solchen Fall? Mit fortschreitender Entwicklung der Technologien und den technischen Hilfsmitteln in der Medizin können diese Fragen dadurch deutlich komplizierter werden und drängen sich immer mehr auf.[3]

A. Aufbau des Beitrags

Ziel dieses Beitrags ist es, sich mit zivilrechtlichen Haftungsfragen vor allem in Bezug auf den Einsatz in der Medizin, konkret im chirurgischen Bereich zu widmen und diese zu erörtern. Der Fokus liegt auf den Haftungsfragen im Zivilrecht. Zu diesem Zweck werden zunächst die Grundbegriffe der künstlichen Intelligenz und des Machine Learnings vorgestellt. Anschließend werden die zurzeit bestehenden und künftig einzusetzenden Operationsroboter vorgestellt und in ihrer Funktionsweise erläutert (B.I.). Aufbauend darauf werden die Einsatzgebiete in der Medizin erläutert (B.II.). Anschließend werden die Herausforderungen und Risiken thematisiert (C.) und die derzeit gegebenen rechtlichen Grundlagen dargestellt (D.I). Der Hauptaspekt liegt dann auf den haftungsrechtlichen Fragen (D.II.) und der möglichen Haftung von Ärzt:innen (D.II.1.) und Hersteller:innen (D.II.2.). Abschließend werden haftungsrechtliche Anpassungsvorschläge diskutiert (D.III.). Der Beitrag schließt mit einer Zukunftsperspektive (E.) und einem Fazit (F.).

2 Ruschemeier/Steinrötter, Der Einsatz von KI & Robotik in der Medizin, 2024, 9.
3 Beck/Faber/Gerndt, Rechtliche Aspekte des Einsatzes von KI und Robotik in Medizin und Pflege, Ethik Med 35, 2023, 247.

B. Von OP-Roboter bis KI-Diagnosen: Was steckt dahinter?

I. Definition und grundlegende Technologien

Zum besseren Verständnis des Aufsatzes werden zunächst die Grundbegriffe erläutert. Künstliche Intelligenz ist schwer in einer Definition zu beschreiben.[4] Allgemein umfasst sie das Übertragen menschlichen Denkens und kognitiver Fähigkeiten auf automatisierte Maschinen.[5] Sind diese Maschinen in der Lage, selbstständig neues Wissen zu verarbeiten und sich dadurch selbst fortzuentwickeln, nennt man das Machine Learning.[6] Die derzeitigen chirurgischen OP-Roboter sind der **Da Vinci** der Firma **Intuitive Surgical**[7] und **HUGO RAS** der Firma **Medtronic.**[8]

Der **Da Vinci** wird schon länger im Rahmen von Operationen eingesetzt und hilft bei komplizierten Eingriffen dadurch, dass er unwillkürliche Bewegungen der operierenden Personen ausgleicht.[9] Es gibt ihn in verschiedenen Versionen. In Benutzung sind der **Da Vinci Xi** als weltweit meistgenutztes roboter-assistiertes Multiport-Operationssystem, der **Da Vinci SP** im Rahmen der Single Port-Chirurgie und der **Da Vinci X,** als Einstiegsmöglichkeit in die roboterassistierte Chirurgie.[10] Multiport bedeutet, dass bei einem medizinischen Eingriff über verschiedene Zugänge gearbeitet wird. Single-Port-Operationen, dass bei minimalinvasiven chirurgischen Eingriffen über einen zentralen Zugang gearbeitet wird.[11]

Der **HUGO RAS** ist ein auf der technologischen Grundlage einer Arbeit des DLR (Deutsches Zentrum für Luft- und Raumfahrt) entwickelter OP-Roboter und wurde konkret aus dem Telechirurgiesystem **MiroSurge**[12] entwickelt.[13] Es ist ein roboti-

4 Eichelberger, in: Ruschemeier/Steinrötter, Der Einsatz von KI & Robotik in der Medizin, 2024, 97 (98).
5 Lihotzky, CTRL 1/21, 4 f.
6 Kupfermann, CTRL 1/21, 7 f.
7 Hier abrufbar (Stand: 23.02.25).
8 Hier abrufbar (Stand: 23.02.25).
9 Katzenmeier, Haftung für Schäden durch KI in der Medizin, MedR 2021, 859.
10 Hier abrufbar (Stand: 23.02.25).
11 Hier abrufbar (Stand: 23.02.25).
12 Hier abrufbar (Stand: 23.02.25).
13 Hier abrufbar (Stand: 23.02.25).

sches Operationsassistenzsystem und besteht aus zwei oder mehreren Roboterarmen.[14] Bei einem Eingriff werden diese flexibel und unabhängig voneinander von einer offenen Chirurgiekonsole aus gesteuert.[15] Im Unterschied zum **Da Vinci** sind beim **Hugo** die einzelnen Roboterarme individuell im Raum bewegbar.[16]

II. Anwendungsgebiete in der Medizin

Das Potenzial der Anwendung von KI und Robotik in der Medizin ist groß. Bereits im Alltag sind KI-gesteuerte Health-Apps in der Lage, Gesundheitszustände zu analysieren, sodass zumindest eine Ersteinschätzung des Gesundheitszustandes möglich ist. Im Detail kann überprüft werden, ob eine Auffälligkeit vorliegt, die einen Arztbesuch erforderlich macht oder auch einfach nur, um die körperliche Verfassung zu verbessern und zu überwachen.[17] Der Einsatz in der Medizin reicht von der Überwachung von Vitalfunktionen auf der Station und im OP bis hin zur Übernahme und Organisation von Verwaltungsaufgaben.[18]

Im Rahmen medizinischer Diagnostik ist es möglich, KI einzusetzen, um Computertomografie-Bilder auszuwerten sowie die Größe und ein mögliches Wachstum von Tumoren zu erkennen.[19] Dabei ist eine KI im Vergleich zum Menschen in der Lage, deutlich schneller und umfangreichere Datenmengen auszuwerten.[20] Dazu werden im Rahmen einer Mustererkennung Daten ausgewertet und mit vorhandenen Daten abgeglichen, um die Entscheidungsfindung zu unterstützen.[21] Im Bereich der Neurologie kann KI unter anderem eingesetzt werden, um frühzeitig Demenzerkrankungen zu ermitteln.[22]

14 Ebd.
15 Ebd.
16 Ebd.
17 Beck/Faber/Gerndt, Rechtliche Aspekte des Einsatzes von KI und Robotik in Medizin und Pflege, Ethik Med 35, 2023, 247 (250).
18 Ebd.
19 Katzenmeier, Haftung für Schäden durch KI in der Medizin, MedR 2021, 859.
20 Beck/Faber/Gerndt, Rechtliche Aspekte des Einsatzes von KI und Robotik in Medizin und Pflege, Ethik Med 35, 2023, 247 (250).
21 Hahn, in: Ruschemeier/Steinrötter, Der Einsatz von KI & Robotik in der Medizin, 2024, 20.
22 Katzenmeier, Haftung für Schäden durch KI in der Medizin, MedR 2021, 859.

In der Chirurgie ist es zudem möglich, KI und Robotik bei Operationen einzusetzen. Im Bereich der minimalinvasiven Eingriffe ist es beispielsweise möglich, durch den Einsatz chirurgischer Roboter, wie des **Da Vinci**[23] und **HUGO**[24], vereinfacht OP-Schritte durchzuführen.[25]

DALL·E 2025-02-06 20.37.25 - A futuristic medical robot analyzing patient data using advanced imaging techniques. The robot is surrounded by holographic screens displaying 3D medi.webp)

23 Hier abrufbar (Stand: 23.02.25).
24 Hier abrufbar (Stand: 23.02.25).
25 Beck/Faber/Gerndt, Rechtliche Aspekte des Einsatzes von KI und Robotik in Medizin und Pflege, Ethik Med 35, 2023, 247.

C. Wenn Technik versagt: Risiken und Herausforderungen

Der Einsatz von Robotik und KI geht in der Medizin mit einigen Risiken und Herausforderungen einher. Bei den derzeit gängigen medizinischen Behandlungen, die nicht auf dem Einsatz von KI-Systemen und Abläufen beruhen, besteht meist die Möglichkeit zu überprüfen, an welcher Stelle die Fehlerquelle angesiedelt ist.[26] Bei dem Einsatz von KI ist dies nicht immer ohne Weiteres möglich – ein Problem, das als Black-Box-Problematik bekannt ist.[27] Inhalt dieser Problematik ist , dass beim Einsatz von KI die Weise, wie diese zu dem Ergebnis der Arbeitsprozesse gelangt, nicht 1:1 nachvollziehbar ist.[28] Systeme der künstlichen Intelligenz generieren ihre Daten auf eine Art und Weise, dass die dort getroffenen Entscheidungen kaum vollständig nachvollziehbar sind.[29] Es besteht das erhöhte Risiko von Manipulationen.[30]

Daraus ergeben sich diverse Herausforderungen. Zum einen ist unklar, wie die Haftungsrisiken verteilt sind.[31] Es wäre eine naheliegende Option, die Personen zur Verantwortung zu ziehen, die als letzte Entscheidungen für die Behandlung an die KI übermittelt und diese Systeme bedient haben.[32] Dieses Vorgehen könnte jedoch dazu führen, dass Haftungsfragen ohne weitere Präzisierung der Fehlerquelle pauschal auf diese Person abgewälzt werden könnten.[33] Zum anderen stellt sich die Frage, wie bei Systemen, die täglich anhand neuer Informationen lernen und sich dadurch verbessern und fortentwickeln, ein einheitlicher überschaubarer Haftungsrahmen festsetzbar ist.[34]

Mit den Möglichkeiten der KI und Robotik gehen jedoch vor allem ethische, soziale und wirtschaftliche Aspekte einher, die zu einem Haftungsdilemma führen können.

26 Beck/Faber/Gerndt, Rechtliche Aspekte des Einsatzes von KI und Robotik in Medizin und Pflege, Ethik Med 35, 2023, 247.
27 Ebd.
28 Ebd.
29 Ebd.
30 Katzenmeier, Haftung für Schäden durch KI in der Medizin, MedR 2021, 859 (860).
31 Beck/Faber/Gerndt, Rechtliche Aspekte des Einsatzes von KI und Robotik in Medizin und Pflege, Ethik Med 35, 2023, 247.
32 Ebd.
33 Ebd.
34 Ebd.

Werden sie in der Medizin eingesetzt, handelt es sich beim Einsatz unter anderem um Behandlungen und Eingriffe am Menschen selbst.[35] Dies geht mit der Anforderung einher, die Vertraulichkeit und notwendige Sensibilität, die in einem Arzt-Patienten-Verhältnis erforderlich ist, möglichst zu wahren.[36] Ebenso darf die Autonomie der Patient:innen nicht eingeschränkt oder aberkannt werden.[37]

D. Rechtliche Rahmenbedingungen und Haftungsfragen

I. Aktuelle rechtliche Grundlagen

Derzeit gibt es keine speziellen gesetzlichen Regelungen, die die Haftung in Bezug auf den Einsatz von KI und Robotik in der Medizin festlegen.[38] Es gelten die allgemeinen haftungsrechtlichen Anforderungen an medizinische Behandlungen.[39] Findet eine Behandlung von Patient:innen durch Ärzt:innen statt, wird nach § 630a II BGB ein Behandlungsvertrag geschlossen.[40] Dieser sieht vor, dass die Behandlung nach den wissenschaftlichen und medizinisch bewährten Standards zu erfolgen hat.[41] Dabei haben die behandelnden Ärzt:innen Therapiefreiheit und damit die Möglichkeit, im Rahmen der Standardmethoden nach ihrem Ermessen die Behandlungsmethoden frei zu wählen.[42] Eine Verpflichtung zum Einsatz von KI-Systemen und Robotik bei Behandlungen besteht nicht.[43] Gemäß § 630a II Hs. 2 BGB ist es möglich, abweichende Vereinbarungen zu treffen.[44] Zu diesen Abweichungen wären Behandlungen unter Einsatz von KI-Systemen zu zählen, denn diese sind noch lange nicht

35 Beck/Faber/Gerndt, Rechtliche Aspekte des Einsatzes von KI und Robotik in Medizin und Pflege, Ethik Med 35, 2023, 247 (250).
36 Beck/Faber/Gerndt, Rechtliche Aspekte des Einsatzes von KI und Robotik in Medizin und Pflege, Ethik Med 35, 2023, 247 (251).
37 Ebd.
38 Katzenmeier, Haftung für Schäden durch KI in der Medizin, MedR 202, 859 (862).
39 BeckOGK/T.Voigt, BGB, Stand: 01.02.25, § 823 Rn. 1087.
40 MüKo/Wagner, BGB, 9. Aufl., § 630a Rn. 1.
41 Laufs/Katzenmeier/Lipp, ArztR, 8. Aufl., Rn. 34.
42 Eichelberger, in: Ruschemeier/Steinrötter, Der Einsatz von KI & Robotik in der Medizin, 2024, 97 (100).
43 BeckOGK/T.Voigt, BGB, Stand: 01.02.25, § 823 Rn. 1087.
44 BeckOK/Katzenmeier, BGB, 73. Edition, § 630a Rn. 189.

als medizinischer Standard einzuordnen.[45] Zusätzlich zu erwähnen ist, dass Roboter und KI-Systeme selbst regelmäßig als Medizinprodukte zu klassifizieren sind.[46] Darauf sind die Medizinprodukte-Verordnung[47] und das Medizinprodukte-Durchführungsgesetz[48] anzuwenden.

II. Haftungsfragen bei Robotik und KI

Treffen Ärzt:innen aufgrund einer durch KI durchgeführten Datenanalyse Behandlungsentscheidungen, ist es schwierig, direkt zu beantworten, wer die Haftung übernimmt.[49] Als Erstes kommt eine Haftung der behandelnden Ärzt:innen in Betracht. Zudem ist auch eine Haftung von Seiten der Hersteller:innen der eingesetzten Technologie nicht von Anfang an abzulehnen.[50] Hier ist zumindest ein großes Verständnis für die Arbeitsweise der Programme gegeben.[51] Denn als Hersteller:innen haben sie einen umfangreichen Einblick in die Funktionalität und Arbeitsweise der Systeme.[52]

1. Ärzt:innen

Orientiert man sich zunächst an vertraglichen Ansprüchen, ist festzuhalten, dass Ärzt:innen bei Behandlungsfehlern gemäß §§ 630a, 280 I BGB für ihre Pflichtverletzungen haften.[53] Zu dem Pflichtenprogramm von Ärzt:innen gehört es, die Behandlungen nach dem Erkenntnisstand der medizinischen Wissenschaft vorzunehmen.[54]

45 Beck/Faber/Gerndt, Rechtliche Aspekte des Einsatzes von KI und Robotik in Medizin und Pflege, Ethik Med 35, 2023, 247 (253).
46 Beck/Faber/Gerndt, Rechtliche Aspekte des Einsatzes von KI und Robotik in Medizin und Pflege, Ethik Med 35, 2023, 247 (258).
47 Hier abrufbar (Stand: 23.02.25).
48 Hier abrufbar (Stand: 23.02.25).
49 Beck/Faber/Gerndt, Rechtliche Aspekte des Einsatzes von KI und Robotik in Medizin und Pflege, Ethik Med 35, 2023, 247 (252).
50 Katzenmeier, Haftung für Schäden durch KI in der Medizin, MedR 2021, 859 (862).
51 Ebd.
52 Ebd.
53 BeckOK/Katzenmeier, BGB, 73. Edition, § 630a Rn. 196.
54 BeckOK/Katzenmeier, BGB, 73. Edition, § 630a Rn. 145.

Dies schließt einen Einsatz von KI und Robotik nicht aus.[55] Der Einsatz von KI und Robotik ist als neue medizinische Behandlungsweisen einzuordnen.[56] Wollen Ärzt:innen diese einsetzen, bedarf es einer umfassenden Aufklärung der Patient:innen gemäß § 630e I 3 BGB, einer Abwägung der Risiken und der Einwilligung der behandlungsbedürftigen Person.[57] Patient:innen sollten die Möglichkeit haben, genau zu überlegen, ob sie den Einsatz der neuen Methoden bei ihrer Behandlung wünschen.[58] Zu beachten ist, dass ein Fehler in der KI bzw. in der Arbeitsweise der Robotik noch kein Behandlungsfehler sein kann. Ein Fehler wird erst dann zu einer Pflichtverletzung der Ärzt:innen, wenn sie aufgrund der Ergebnisse und Arbeitsweisen fehlerhafte medizinische Leistungen erbringen.[59]

DALL·E 2025-02-06 20.34.53 - A highly detailed image of a Da Vinci surgical robot in an operating room. The robotic arms are performing a delicate surgery, controlled by a surgeon.webp

55 MüKo/Wagner, BGB, 9. Aufl., § 630e Rn. 38.
56 Eichelberger, in: Ruschemeier/Steinrötter, Der Einsatz von KI & Robotik in der Medizin, 2024, 97 (102).
57 Ebd.
58 Eichelberger, in: Ruschemeier/Steinrötter, Der Einsatz von KI & Robotik in der Medizin, 2024, 97 (102).
59 Eichelberger, in: Ruschemeier/Steinrötter, Der Einsatz von KI & Robotik in der Medizin, 2024, 97 (106).

a) § 278 S. 1 BGB

In Betracht kommt, ein autonomes System als digitalen Erfüllungsgehilfen gem. § 278 S. 1 BGB einzuordnen und den behandelnden Ärzt:innen die Fehler unter Anwendung dieser Norm zuzurechnen.[60] Die Einführung eines digitalen Erfüllungsgehilfen wurde bereits in Bezug auf Maschinen und Computerprogramme im 20. Jahrhundert diskutiert.[61] Nach § 278 S. 1 BGB wird das Verhalten eines Gehilfen zugerechnet.[62] Der Einsatz von KI-Systemen ist nicht als klassischer Anwendungsfall des § 278 BGB vorgesehen. Das schließt die Anwendung auf zuzurechnendes maschinelles und KI-gesteuertes Verhalten aber nicht von Anfang an aus.[63] Fraglich ist, ob KI und Robotik überhaupt Hilfspersonen i.S.d. § 278 S. 1 BGB sein können. Legt man den Wortlaut des § 278 BGB aus, ist festzustellen, dass nicht nur Menschen als Personen einzuordnen sind, sondern als normatives Tatbestandsmerkmal auch andere Wertungen möglich sind, was eine KI nicht gänzlich ausschließt.[64] Gegen die Einbeziehung spricht die systematische Auslegung. Das BGB sieht unter der Unterschrift „Personen" natürliche Personen (Titel 1) und juristische Personen (Titel 2) vor.[65] Dies lässt erkennen, dass man für eine „Person" zumindest eine Rechtsfähigkeit benötigt.[66] Diese weisen Robotik und KI nicht auf. Eine direkte Anwendung wäre damit abzulehnen.[67]

Denkt man über eine analoge Anwendung des § 278 S. 1 BGB nach, bedarf es einer planwidrigen Regelungslücke und einer vergleichbaren Interessenlage.[68] Der damalige Gesetzgeber wird sich kaum Gedanken zur Nutzung von KI und Robotik als menschliche Gehilfen und dahingehende Zurechnungsfragen gemacht haben, denn die damaligen Maschinen sind mit den heutigen nicht vergleichbar.[69] Gegen eine analoge Anwendung wurde vor allem angeführt, dass § 278 S. 1 BGB keine Verantwortungszurechnung für Sachen vorsehen kann, wenn die Handelnden diese lediglich wie Werkzeuge einsetzen.[70] Der Zweck und die Eigenschaften von KI und Robotik gehen damit so weit auseinander, dass eine analoge Anwendung nicht möglich erscheint.[71] Ob in Zukunft bei autonomen Entscheidungen durch KI die Anwendung zu überdenken ist, bleibt offen.[72] Dies würde zumindest einen Ansatzpunkt für die Haftungsfragen bei einem Einsatz von KI liefern.

b) § 823 I BGB

In Bezug auf eine deliktische Haftung von Ärzt:innen ist an § 823 I BGB zu denken. Im Rahmen der Haftung gem. § 823 I BGB sind die Verkehrspflichten der Ärzt:innen im Rahmen des Schutzes von Körper, Gesundheit und Selbstbestimmung der Patient:innen zu beachten.[73] Der Einsatz von KI und Robotik ist jedoch auch in der Deliktshaftung kein generell pflichtwidriges Verhalten.[74]

Kommt es zu einer Rechtsgutsverletzung im Rahmen des Einsatzes von KI-Systemen und Robotik, könnte bei den Haftungsfragen § 630h BGB entsprechend Anwendung finden.[75] In § 630h I BGB ist eine Fehlervermutung vorgesehen.[76] Es wäre denkbar, diese in dem Fall einer fehlerhaften KI heranzuziehen. Dann steht gemäß § 630h I BGB in Frage, ob ein voll beherrschbares Risiko für den Behandelnden vorlag.[77] Jedoch bedarf es für § 630h I BGB einer vollen Beherrschbarkeit des eingesetzten Systems.[78] Problematisch ist vor allem, dass die KI mithilfe von **Machine Learning** immer weitere Ansätze und Überlegungen tätigt, die nicht vor-

60 Katzenmeier, Haftung für Schäden durch KI in der Medizin, MedR 2021, 859 (861).
61 Lohmann/Preßler, RDi 2021, 538, Rn. 3.
62 Lohmann/Preßler, RDi 2021, 538, Rn. 8.
63 Ebd.
64 Lohmann/Preßler, RDi 2021, 538, Rn. 12.
65 Lohmann/Preßler, RDi 2021, 538, Rn. 13.
66 Ebd.
67 Lohmann/Preßler, RDi 2021, 538, Rn. 21.
68 Ebd.
69 Lohmann/Preßler, RDi 2021, 538, Rn. 24.

70 Lohmann/Preßler, RDi 2021, 538, Rn. 25.
71 Katzenmeier, Haftung für Schäden durch KI in der Medizin, MedR 2021, 859 (861).
72 Lohmann/Preßler, RDi 2021, 538, Rn. 27.
73 NK-BGB/Katzenmeier, BGB, 4. Aufl., § 823 Rn. 15.
74 Katzenmeier, Haftung für Schäden durch KI in der Medizin, MedR 202, 859 (861).
75 BeckOGK/T.Voigt, BGB, Stand: 01.02.25, § 823 Rn. 1089.
76 MüKo/Wagner, BGB, 9. Aufl. § 630h Rn. 1.
77 Hier abrufbar (Stand: 23.02.25).
78 Eichelberger, in: Ruschemeier/Steinrötter, Der Einsatz von KI & Robotik in der Medizin, 2024, 97 (112).

hersehbar sind.[79] Das führt zu der Problematik, dass die Prozesse der KI-Systeme für die Verwender:innen nicht einfach nachzuvollziehen sind.[80] Eine volle Beherrschbarkeit ist bei autonomen Systemen nicht gegeben.[81] Zu beachten ist, dass von den Ärzt:innen kein vollumfängliches Wissen in Bezug auf die Funktionsweise des KI-Systems verlangt werden kann.[82] Würde man die volle Beherrschbarkeit trotzdem annehmen, könnte das die Bereitschaft, die Systeme bei der Behandlung in Zukunft zu integrieren, hemmen.[83] Dadurch ist die Anwendbarkeit des § 630h BGB im Rahmen des Deliktsrechts eher abzulehnen.[84]

DALL·E 2025-02-06 20.34.44 -
A highly detailed image of a Da Vinci surgical robot in an operating room. The robotic arms are performing a delicate surgery, controlled by a surgeon.webp

79 Ebd.
80 BeckOGK/T.Voigt, BGB, Stand: 01.02.25, § 823 Rn. 1089.
81 Katzenmeier, Haftung für Schäden durch KI in der Medizin, MedR 2021, 859 (861).
82 Leupold/Wiebe/Glossner, IT-R, Teil 9.6.4 Rn. 84.
83 Eichelberger, in: Ruschemeier/Steinrötter, Der Einsatz von KI & Robotik in der Medizin, 2024, 97 (112).
84 Ebd.

c) § 831 I 1 BGB analog

Im Deliktsbereich gibt es noch den § 831 I 1 BGB, der eine Haftung für Verrichtungsgehilfen vorsieht. Auch hier ist eine analoge Anwendung des § 831 I 1 BGB nicht von vornherein abzulehnen.[85] Verrichtungsgehilfe ist, wer weisungsgebunden im Pflichtenprogramm einer anderen Person tätig wird.[86] Annehmen könnte man die Anwendung des § 831 I 1 BGB, da die KI-Systeme zur Arbeitserleichterung arbeitsteilig mit dem Menschen zusammenarbeiten und zur Unterstützung eingesetzt werden.[87]

Allerdings ist fraglich, ob ein KI-System mit einem menschlichen Verrichtungsgehilfen vergleichbar sein kann.[88] Eine KI könnte eventuell durch Machine Learning und programmierte Fähigkeiten tatsächlich selbstständig bei übernommenen Aufgaben entscheiden, was zu Haftungslücken führen kann.[89] Eine Pflichtverletzung würde vorliegen, wenn der Roboter oder die KI in Ausübung der Verrichtung der Aufgaben fehlerhaft agiert hätten.[90] § 831 I BGB sieht allerdings in § 831 I 2 BGB die Möglichkeit einer Exkulpation der Geschäftsherr:innen vor.[91] Danach können sich Geschäftsherr:innen entlasten, soweit sie ihren Pflichten nachgekommen sind.[92] Hier beginnt dann die altbekannte Problematik, dass die Prozesse der autonomen Systeme nicht hundertprozentig nachzuvollziehen sind.[93] Dies führt dazu, dass den Geschäftsherr:innen nicht vorzuwerfen sein kann, ihren Pflichten nicht nachgekommen zu sein, wenn sie das für sich Mögliche getan haben.[94] Werden die Systeme zweckwidrig von der steuernden Person eingesetzt, ist hingegen keine Exkulpation möglich.[95] Eine Anwendung von § 831 I 1 BGB auf Haftungsfragen zum Einsatz von KI und Robotik in der Medizin ist mit den Exkulpationsmöglichkeiten abzulehnen.

85 MüKo/Wagner, BGB, 9. Aufl., § 630e Rn. 30.
86 MüKo/Wagner, BGB, 9. Aufl., § 831 Rn.16.
87 Leupold/Wiebe/Glossner, IT-R, Teil 9.6.4 Rn. 86.
88 Ebd.
89 MüKo/Wagner, BGB, 9. Aufl., § 831 Rn. 30.
90 Ebd.
91 MüKo/Wagner, BGB, 9. Aufl., § 831 Rn. 46.
92 Ebd.
93 Katzenmeier, Haftung für Schäden durch KI in der Medizin, MedR 2021, 859 (862).
94 Ebd.
95 MüKo/Wagner, BGB, 9. Aufl., § 831 Rn. 30.

2. Hersteller:innen

a) ProdHaftG

In Betracht kommt weiter eine Haftung der Hersteller:innen der Systeme.[96] Gemäß § 1 I 1 ProdHaftG besteht die Möglichkeit der Hersteller:innen, bei Produktfehlern zu haften.[97] Ein Produkt ist gem. § 2 ProdHaftG jede bewegliche Sache, auch wenn sie einen Teil einer anderen beweglichen Sache oder einer unbeweglichen Sache bildet, sowie Elektrizität. Es stellt sich die Frage, ob KI und Robotik unter den Begriff fallen. Dies war lange unklar.[98] Allerdings erfasst die Neufassung der Produkthaftungs-RL mit Art. 4 Nr. 1 ausdrücklich Software und produktbezogene digitale Dienstleistungen.[99]

Gemäß § 3 ProdHaftG hat ein Produkt einen Fehler, wenn es nicht die Sicherheit bietet, die unter Berücksichtigung aller Umstände, insbesondere seiner Darbietung, des Gebrauchs, mit dem billigerweise gerechnet werden kann, des Zeitpunkts, in dem es in den Verkehr gebracht wurde, berechtigterweise erwartete werden kann. Es stellt sich die Frage, nach welchen Maßstäben Systeme, die von künstlicher Intelligenz gesteuert werden, zu bewerten sind, um festzustellen, wann Abweichungen von den Sicherheitsstandards gegeben sind. Denkbar wäre es, die Systeme mit den zurzeit durch Menschen gegebenen Sicherheitsstandards bei Wahrnehmung der Aufgaben zu vergleichen.[100] Wirklich ausreichen kann das nicht. Denn die KI-Systeme kommen zwar mit einem gewissen vorprogrammierten Algorithmus zum Einsatz. Allerdings besteht der Hauptaspekt ihrer Arbeit darin, dass sie durch neue Daten neue Zusammenhänge erlernen und sich somit stetig verbessern.[101] Dies erschwert es, wirklich feste vergleichbare Maßstäbe herauszuarbeiten, denn das Produkthaftungsgesetz stellt auf den Zeitpunkt des Inverkehrbringens ab.[102]

96 Katzenmeier, Haftung für Schäden durch KI in der Medizin, MedR 2021, 859 (862).
97 MüKo/Wagner, ProdHaftG, 9. Aufl., § 1 Rn. 1.
98 MüKo/Wagner, ProdHaftG, 9. Aufl., § 2 Rn. 21.
99 Hier abrufbar (Stand: 23.02.25).
100 Ebd.
101 Ebd.
102 Ebd.

Ein großer Problempunkt der hier diskutierten Haftung gem. § 1 I 1 ProdHaftG ist die Regelung des § 1 IV 1 ProdHaftG. Danach trägt die geschädigte Person für den Schaden und den ursächlichen Zusammenhang zwischen Fehler und Schaden die Beweislast. Dies kann bereits bei körperlich gegenständlichen Produkten zu Problemen führen. Die Fehler beim Einsatz der KI liegen meistens in dem Steuerungsalgorithmus oder einem falsch designten künstlichen neuronalen Netz.[103] Dann den Zusammenhang und falsch programmierten Part zu bestimmen, stellt eine große Schwierigkeit dar. Zusätzlich ist zu beachten, dass KI-Systeme häufig mit Daten unterschiedlich zugänglicher Datenbanken arbeiten und dabei an viele verschiedene Netzwerke anknüpfen.[104] Anhand dessen herauszufinden, zu welchem Zeitpunkt ein Fehler entstanden ist, ist aufwändig.[105] Geht man davon aus, dass Fehler erst dann passieren würden, wenn Daten anderer Netzwerke nach dem Inverkehrbringen des Systems genutzt werden, wird dies dazu führen, dass das Produkt bei Inverkehrbringen als fehlerfrei anzusehen ist und eine Haftung bereits gem. § 1 II Nr. 2 ProdHaftG ausgeschlossen ist.[106] Denn dann würde erst nach dem Inverkehrbringen der Fehler auftreten.[107]

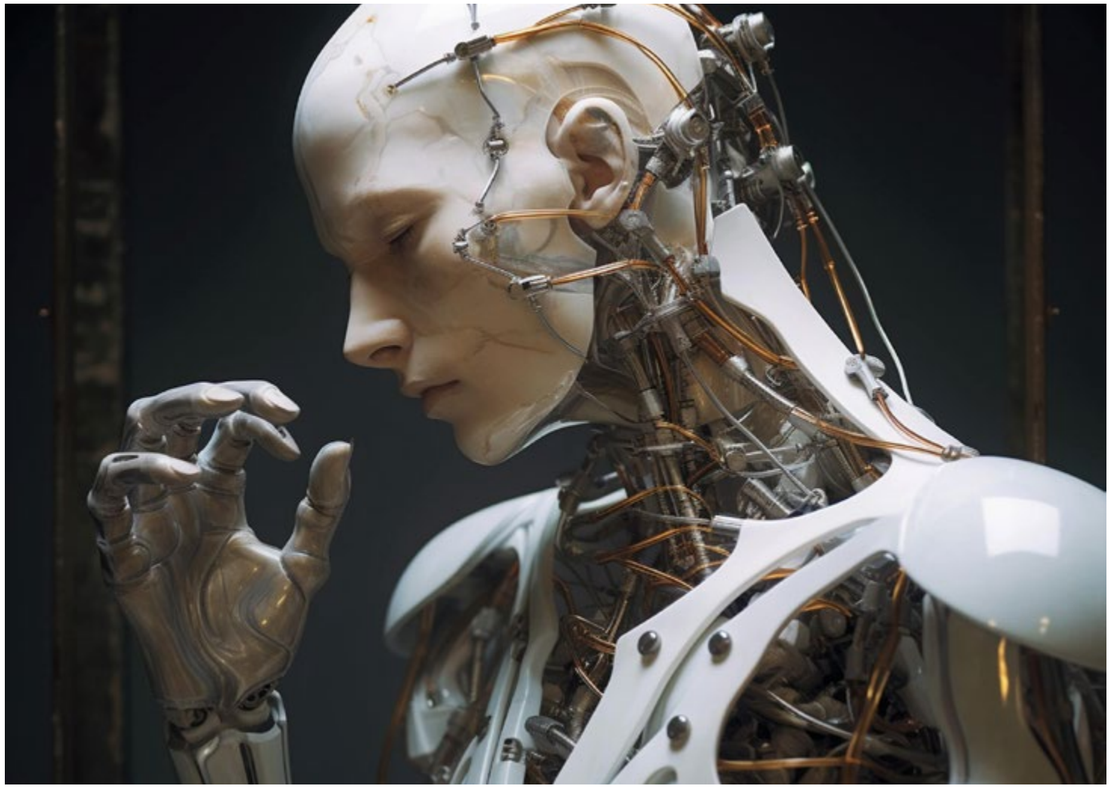
b) Produzentenhaftung

Für den Hersteller kommt noch die Produzentenhaftung gem. § 823 I BGB in Betracht. Diese sieht eine Haftung für fehlerhafte Produkte vor und sieht bei den Hersteller:innen die Verantwortung, wenn diese ihre Verkehrspflichten hinsichtlich der Produkte nicht beachtet haben.[108] Wie vorangegangen erwähnt, sind Roboter und KI-Systeme selbst regelmäßig als Medizinprodukte zu klassifizieren und stellen Produkte dar, die der Produzentenhaftung unterliegen.[109] Zudem sind die Medizin-

103 Katzenmeier, Haftung für Schäden durch KI in der Medizin, MedR 2021, 859 (863).
104 Ebd.
105 Ebd.
106 Ebd.
107 Ebd.
108 BeckOK/Förster, BGB, 73. Edition, § 823 Rn. 674.
109 Beck/Faber/Gerndt, Rechtliche Aspekte des Einsatzes von KI und Robotik in Medizin und Pflege, Ethik Med 35, 2023, 247 (258).

produkte-Verordnung[110] und das Medizinprodukte-Durchführungsgesetz[111] anzuwenden. Diese enthalten jedoch keine eigenen Haftungsregelungen, sodass § 823 I BGB Anwendung findet. Im Rahmen der Produzentenhaftung sind die Hersteller:innen verpflichtet, noch über den Zeitpunkt des Inverkehrbringens hinaus die Produkte zu beobachten und zu überwachen, um Gefahren zu verringern und auszuschließen.[112] Wendet man diese Regelung auf den Einsatz von autonomen Systemen an, sind die Hersteller:innen verpflichtet, auch die Auswertungsprozesse unter Hinzuziehen der genutzten Daten zu überwachen und die Machine Learning Vorgänge zu überprüfen.[113] Die Auswertungsstrategien und Entscheidungsprozesse der Systeme sind nicht ohne Weiteres für die Hersteller:innen vorhersehbar und erkennbar, sodass es schwer sein wird, ihnen die unvorhersehbaren Fehlentscheidungen wirklich vorzuwerfen.[114]

Festzuhalten ist, dass die Haftungsfragen beim Einsatz von autonomen Systemen unter anderem an den Fragen des Verschuldens scheitern.[115] Die diskutierten Normen bringen unbefriedigende Ergebnisse zum Vorschein. Zwar sind Ansprüche gegen Hersteller der Systeme nach dem ProdHaftG nicht gänzlich ausgeschlossen. Die Fehler zu beweisen und wirklich die Ursache der Fehler zu finden, wird jedoch große Schwierigkeiten darstellen.[116]



GRAFIK 4 https://pixnio.com/de/media/beige-robot-kunstliche-intelligenz-grafik-abbildung#

III. Notwendige Anpassungen des Rechtsrahmens

Die Hürden der Haftungszuweisung führen dazu, dass auch in Zukunft weiterhin rechtliche Anpassungen vorzunehmen sind. Durch die fehlende Möglichkeit, Verantwortungsbereiche abzugrenzen, ist eine Haftungszuweisung nur schwer möglich.[117] Es ist zu vermeiden, dass sich das medizinische Personal für die Entscheidung selbst nicht mehr verantwortlich fühlt und letztendlich blind Entscheidungen der KI anwendet.[118] Gegenstand der Diskussion ist die Frage, ob ein „Human in the Loop“ die richtige Lösung für die Haftungsproblematiken ist.[119] Die Idee dieser Figur ist es, einen Menschen als Letztentscheider:in zu benennen, der Verantwor-

110 Hier abrufbar (Stand: 23.02.25).
111 Hier abrufbar (Stand: 23.02.25).
112 BeckOK/Förster, BGB, 73. Edition, 823 Rn. 703.
113 Katzenmeier, Haftung für Schäden durch KI in der Medizin, MedR 2021, 859 (863).
114 Ebd.
115 Ebd.
116 Ebd.

117 Beck/Faber/Gerndt, Rechtliche Aspekte des Einsatzes von KI und Robotik in Medizin und Pflege, Ethik Med 35, 2023, 247 (254).
118 Ebd.
119 Ebd.

tung für die Entscheidungen der Systeme übernimmt.[120] Die Figur ist auf den Einsatz von KI in Bezug auf automatisierte Waffen zurückzuführen.[121] Die Hoffnung dahinter ist, dass sich die verantwortlichen Menschen dadurch weiter verantwortlich fühlen und im Schadensfall Ansprechpartner:innen gegeben sind.[122] Ganz ungefährlich wäre das nicht. Denn es besteht die Möglichkeit, dass die Personen dann für jegliche Problematiken zur Haftung gezogen werden und sozusagen den Kopf hinhalten müssen.[123] Eine derzeit diskutierte Modifizierung des „Human in the Loop" ist der Begriff „Meaningful Human Control" (MHC).[124] Inhalt dessen ist es, Menschen bei Maschinenentscheidungen nur dann zur Verantwortung zu ziehen, wenn dies angemessen erscheint.[125] Vorteil soll sein, dass die Ärzt:innen mit der KI zusammenarbeiten und die nach ihrem Ermessen besten Entscheidungen treffen, sodass sie selbst noch bestimmen können, wie oder welche Behandlung vorzunehmen ist und dadurch Verantwortung übernehmen.[126]

Von der Einführung der ebenfalls diskutierten Figur der „E-Person" rät die Datenethikkommission ausdrücklich ab.[127] Für die Einführung spricht, dass sie zwar die Möglichkeit eröffnet, eine Haftungsperson zu benennen. Allerdings kann dadurch nicht denjenigen, die den Einsatz und falschen Einsatz der Systeme zu verantworten haben, Verantwortung zugesprochen werden.[128] Zusätzlich ist eine Einführung einer Gefährdungshaftung im Gespräch.[129] Anknüpfen würde diese an eine digitale Gefahr, ähnlich der Tiergefahr in § 833 BGB.[130] Mit einer solchen Gefährdungshaftung bestünden große Unsicherheiten für die Hersteller:innen und die notwendigen Vorsorgemaßnahmen ihrerseits, um den Regelungen gerecht zu werden.[131] Problematisch an dieser Überlegung ist vor allem, dass es bei Haftungsfragen der KI meist nicht auf die allgemeinen Programmierungsfragen ankommen wird, sondern auf die dadurch getroffenen Entscheidungen.[132] Eine Gefährdungshaftung erscheint nicht zielführend.

Eine weitere Möglichkeit, um Haftungsrisiken abzudecken, wäre eine der Kfz-Haftpflichtversicherung ähnliche Haftpflichtversicherung für die Hersteller:innen und Anwender:innen von KI.[133] Dies könnte den Geschädigten einen direkten Anspruch gegen die Versicherung ermöglichen, ohne dass diese selbst erstmal versuchen müssten, sämtliche infrage kommende Haftungspersonen in Anspruch zu nehmen.[134] Das könnte einfacher zu integrieren sein, da bereits jetzt Haftungsfragen in der Medizin für die Patient:innen häufig zur Versicherung als erste Anlaufstelle für Haftungsfragen führen.[135]

E. Blick in die Zukunft: Wohin führt die medizinische Innovation?

Neben den Haftungsfragen sind beim Einsatz von KI-Systemen in der Medizin vor allem auch die datenschutzrechtlichen Aspekte zu beachten.[136] Dass sich die KI-Systeme im Einsatz stetig verbessern können, verlangt die Nutzung von Gesundheitsdaten.[137] Auch der Einsatz von Robotern benötigt Daten, um anhand dessen zu lernen und den Einsatz zu erproben.[138] Aktuell kommen als Trainingsgrundlage unter anderem das **Virtual Research Environment** (VRE)[139] und die **Health Data Cloud** (HDC)[140] zum Einsatz. Die Themen der Informationssicherheit und Schutz

120 Beck/Faber/Gerndt, Rechtliche Aspekte des Einsatzes von KI und Robotik in Medizin und Pflege, Ethik Med 35, 2023, 247 (255).
121 Ebd.
122 Ebd.
123 Beck/Faber/Gerndt, Rechtliche Aspekte des Einsatzes von KI und Robotik in Medizin und Pflege, Ethik Med 35, 2023, 247 (256).
124 Ebd.
125 Ebd.
126 Beck/Faber/Gerndt, Rechtliche Aspekte des Einsatzes von KI und Robotik in Medizin und Pflege, Ethik Med 35, 2023, 247 (257).
127 Gutachten der Datenethikkommission, hier abrufbar (Stand: 23.02.25).
128 Ebd.
129 Katzenmeier, Haftung für Schäden durch KI in der Medizin, MedR 2021, 859 (864).
130 Ebd.
131 Ebd.
132 Ebd.
133 Katzenmeier, Haftung für Schäden durch KI in der Medizin, MedR 2021, 859 (867).
134 Ebd.
135 Ebd.
136 Schirner/Ritter, in: Ruschemeier/Steinrötter, Der Einsatz von KI & Robotik in der Medizin, 2024, 53.
137 Ebd.
138 Ebd.
139 Hier abrufbar (Stand: 23.02.25).
140 Hier abrufbar (Stand: 23.02.25).

vor Compliance werden an Bedeutung gewinnen.[141] Es wäre zudem zu überlegen, ob es in Zukunft möglich sein wird, dass Ärzt:innen ganze Aufgaben an autonome Maschinen delegieren, ohne dass am Ende weitere Ärzt:innen tätig werden müssen.[142] Dann wäre zu fragen, ob die Ärzt:innen weniger Sorgfaltspflichten treffen könnten, wenn die KI und Robotik als „Kolleg:innen" im Rahmen einer horizontalen Arbeitsteilung zu sehen wären.[143] Denn im Rahmen dieser Arbeitsteilung können sich Ärzt:innen grundsätzlich darauf verlassen und darauf vertrauen, dass der andere Part die Handlungen sorgfältig und richtig ausübt.[144]

https://pixnio.com/de/media/robot-humanoid-kunstliche-intelligenz-wissenschaftliche-forschung-portrat#

141 Schirner/Ritter, in: Ruschemeier/Steinrötter, Der Einsatz von KI & Robotik in der Medizin, 2024, 60; Herbst, Der Einsatz von KI & Robotik in der Medizin, 2024, 77.
142 Eichelberger, in: Ruschemeier/Steinrötter, Der Einsatz von KI & Robotik in der Medizin, 2024, 97 (104).
143 Eichelberger, in: Ruschemeier/Steinrötter, Der Einsatz von KI & Robotik in der Medizin, 2024, 97 (110).
144 Ebd.

Sollte sich der Einsatz von KI und Robotik zur Standardmethode der Behandlungsmöglichkeiten entwickeln, würden im weiteren Verlauf auch die Anforderungen an die Aufklärung der Patient:innen herabsinken.[145] Eventuell könnte die voll umfassende Aufklärungspflicht auch bestehen bleiben, wenn eine gesellschaftliche allgemeine Skepsis gegenüber dem Einsatz in der Medizin gegeben sein sollte.[146] Fraglich wäre bei der Einordnung als Standardmethode dann weiter, ob der fehlende Einsatz von KI und Robotik bei der Behandlung als Behandlungsfehler qualifizierbar wäre.[147]

F. Fazit

Zusammenfassend ist festzuhalten, dass der Einsatz von KI und Robotik in der Medizin viele ungeklärte Haftungsfragen mit sich bringt. Vor allem die mögliche Verantwortungsdiffusion ist ein Problem. Auch soll der Einsatz der Maschinen nicht dazu führen, dass die behandelnden Personen sich hinter möglichen Fehlern der Maschinen verstecken und keine Verantwortung spüren. Allerdings ist der Einsatz von KI und Robotik in der Medizin wirklich vielversprechend. Allein die bisherigen Einsatzmöglichkeiten sind eine große Bereicherung. Wenn Menschen mithilfe von KI-gestützten Exoskeletten wieder mobiler werden,[148] wenn durch KI früher Tumore erkannt werden und vereinfachter und präziser Daten ausgewertet und interpretiert werden können, ist das ein bedeutender Fortschritt. Auch die Robotik ermöglicht eine einfachere Arbeitsweise bei minimalinvasiven Eingriffen. Es können Fehler ausgeglichen werden und auf Distanz operiert werden. Der Fortschritt geht sicherlich mit rechtlichen Hürden einher, die allerdings bei den gegebenen und zukünftigen Möglichkeiten der Verbesserung in der Medizin in Kauf genommen und gesetzlich ausdifferenziert werden sollten. Wichtig ist, dass der Einsatz mit einem gesunden Respekt und nicht blindem Vertrauen in die Technologien erfolgt.

145 Eichelberger, in: Ruschemeier/Steinrötter, Der Einsatz von KI & Robotik in der Medizin, 2024, 97 (102).
146 Ebd.
147 Eichelberger, in: Ruschemeier/Steinrötter, Der Einsatz von KI & Robotik in der Medizin, 2024, 97 (105).
148 S. hier (Stand: 23.02.25).

„Cyberangriffe haben sich in der modernen (hybriden) Kriegsführung zu einer der zentralen Strategien entwickelt.“

Aufsatz

Lassen Cyberangriffe das völkerrechtliche Gewaltverbot erodieren?

Isabel Ecker

Open Peer Review

Dieser Beitrag wurde lektoriert von: Ramon Schmitt und Julia Keselj

Isabel hat an der Universität zu Köln ihr erstes Examen abgelegt und anschließend, durch die Studienstiftung des deutschen Volkes, im Strafrecht promoviert. Im letzten Jahr hat sie als Stipendiatin des DAAD ihren Master an der University of Oxford absolviert, wobei sie sich auf das Völkerrecht sowie Law and Computer Science spezialisiert hat. Sie ist derzeit Rechtsreferendarin am Hanseatischen OLG und wird ihre Wahlstation I bei der Ständigen Vertretung Deutschlands bei den Vereinten Nationen in New York verbringen.

Cyberangriffe haben sich in der modernen (hybriden) Kriegsführung zu einer der zentralen Strategien entwickelt. In bewaffneten Auseinandersetzungen sind sie zu einem alltäglichen Instrument geworden, wie die zahlreichen Vorfälle im Krieg

zwischen Russland und der Ukraine belegen.[1] Zunehmend finden Cyberangriffe zwischen Staaten jedoch ebenso außerhalb bewaffneter Konflikte statt. Beispielhaft können gesteuerte Angriffe in Zeiten von Wahlen oder die Beeinflussung kritischer Infrastruktur durch die Infiltrierung mit Malware angeführt werden.[2] Dieser Aufsatz beschäftigt sich mit dieser Art von Angriffen, also Attacken außerhalb bewaffneter Konflikte (jus ad bellum). Untersucht wird, ob und unter welchen Voraussetzungen Cyberattacken gegen das Gewaltverbot des Art. 2 Abs. 4 der Charta der Vereinten Nationen (UN-Charta) verstoßen.[3] Die Analyse beginnt mit einer Darstellung des grundlegenden Inhalts des Gewaltverbots, wobei die Reichweite eines Verstoßes gegen das Gewaltverbot verdeutlicht werden soll. Anschließend wird hinterfragt, inwiefern das Gewaltverbot auf den Cyberspace anwendbar ist. Nachdem die generelle Anwendbarkeit festgestellt wurde, werden die Voraussetzungen untersucht, die Staaten an den Gewaltbegriff stellen. Es wird untersucht, inwiefern sich bezüglich der völkervertraglichen Norm eine nachträgliche Praxis und bezüglich der völkergewohnheitsrechtlichen Norm eine einheitliche Staatenpraxis entwickelt (hat). Eine Vielzahl an Staaten hat ihre Meinung zu der betreffenden Rechtsfrage über die vergangenen Jahre kundgetan.[4] Zuletzt hat die Afrikanische Union ihre Rechtsposition im Zusammenhang mit Cyberangriffen und dem Gewaltverbot veröffentlicht.[5] Allerdings zeigen sich nicht nur Unterschiede hinsichtlich der Voraussetzungen, die Staaten an die Erfüllung des Gewaltbegriffs stellen. Es muss darüber hinaus hinterfragt werden, inwieweit die bisher veröffentlichten staatlichen Positionen ausreichen, um eine weit überwiegende völkerrechtliche Praxis zu begründen. Es wird sich zeigen, dass der Streit um die Voraussetzungen des Gewaltbegriffs nicht auf Cyberattacken beschränkt ist, sondern in unmittelbarem Konnex zu der zugrundeliegenden Frage der generellen Gewaltdefinition im Rahmen des Art. 2 Abs. 4 UN-Charta bzw. des völkergewohnheitsrechtlichen Gewaltverbots steht. Die aktuellen Entwicklungen im Hinblick auf die Übertragung des „scale and effects"-Standards auf den Gewaltbegriff könnten zu einer präziseren Definition beitragen. Gleichzeitig gilt es jedoch, die Herausforderungen zu analysieren, die mit einer solchen Übertragung einhergehen.

A. Das Gewaltverbot und die Folgen eines Verstoßes - Rechtlicher Rahmen

Art. 2 Abs. 4 UN-Charta bildet den inhaltlichen Ausgangspunkt der Analyse:

> „All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

1 Z.B. *Thøgersen*, An Attack on Maersk Strikes Everywhere at Once': International law and the Political Economy of Digitalization, hier abrufbar (Stand: 22.02.25); *Mačák*, Nothing is certain but death and taxes (unless you get hacked): An international law perspective on Ukraine's cyber attack against Russia's Federal Tax Service, hier abrufbar (Stand: 22.02.25); *Buchan*, Ukranian 'IT Army': A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?, hier abrufbar (Stand: 22.02.25).
2 S. dazu *Schmitt*, Foreign Cyber Interference in Elections: An International Law Primer, Part I, hier abrufbar (Stand: 22.02.25); zum Phänomen der Cognitive Warfare *Wanyana*, Cognitive Warfare: Does it Constitute Prohibited Force?, hier abrufbar (Stand: 22.02.25).
3 Zu den Fragen des jus in bello, insb. der Regulierung von KI in Kriegszeiten s. *Wegener/Sochnyev/Venislavskyy*, CTRL 2/24, 80.
4 Eine Sammlung der veröffentlichen Rechtspositionen der Staaten findet sich hier (Stand: 27.02.25).
5 Hier abrufbar (Stand: 27.02.25).

Die Norm beschreibt ein umfassendes Gewaltverbot. Ihr Inhalt spiegelt die völkergewohnheitsrechtliche Norm des Gewaltverbots wider, die im Verlauf der Jahre den ius cogens Status im Sinne des Art. 53 der Wiener Vertragsrechtskonvention (WVK)[6] erreicht hat, also die gesamte Völkergemeinschaft bindet (erga omnes).[7]

Definition nach Art. 53 WVK: "For the purposes of the present Convention, a peremptory norm of general international law is a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character."

Eine zwingende Völkerrechtsnorm „erga omnes" bezeichnet eine Verpflichtung eines Staates gegenüber der ganzen Staatengemeinschaft zur Einhaltung der Norm.1 Hiervon zu unterscheiden ist eine Verpflichtung „erga omnes inter partes". Dieser Terminus beschreibt die Verpflichtung zur Befolgung der Normen, die nur zwischen bestimmten Staaten gelten, z.B. Staaten, die sich durch den Abschluss eines völkerrechtlichen Vertrages gebunden haben.2

1 IGH, Case concerning the Barcelona Traction, Light and Power Company, Belgium v. Spain (1970), Ziff. 33, hier abrufbar (Stand: 25.02.25).
2 *V. Arnauld*, Völkerrecht, 4. Auflage, 2019, S. 173.

6 Vienna Convention on the Law of Treaties, hier abrufbar (Stand: 27.02.25).
7 IGH, Case Concerning Military and Paramilitary Activities in and against Nicaragua Reports (1986), Ziff. 190; anzumerken ist, dass Uneinigkeit darüber besteht, welche Norm und welcher Inhalt des Gewaltverbots den ius cogens Kern bildet, wobei vorliegend die Auffassung zugrunde gelegt wird, dass allein die Gewaltverbotsnorm des Völkergewohnheitsrechts den ius cogens Status erlangen kann und nicht die völkervertragliche Norm der UN-Charta, s. dazu *Johnston*, Identifying the jus cogens norm in the jus ad bellum, 70 International and Comparative Law Quarterly 29 (2021).

Um die vollständige rechtliche Tragweite der Antwort auf die Frage, wann die Anwendung oder Androhung von Gewalt gegen Art. 2 Abs. 4 UN-Charta verstößt, zu erfassen, lohnt sich ein Blick auf die Rechtsfolgen, die ein Verstoß gegen das Gewaltverbot auslösen kann.[8] Neben der unmittelbaren politischen Bedeutung kann die Gewaltanwendung, wenn sie das Niveau eines bewaffneten Angriffs („armed attack") erreicht, das Selbstverteidigungsrecht des anderen Staates aus Art. 51 UN-Charta auslösen.

„Art. 51 UN-Charta: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."

8 Eine gute Übersicht bietet der Beitrag von *Akande*, The Use of Nerve Agents in Salisbury: Why does it Matter Whether it Amounts to a Use of Force in International Law?, hier abrufbar (Stand: 27.02.25), auch wenn dieser sich inhaltlich auf einen anderen Fall fokussiert.

Darüber hinaus kann die Gewalthandlung ihrerseits nicht mehr als Gegenmaßnahme („countermeasure") nach Art. 50 Abs. 1 der Artikel zur Staatenverantwortlichkeit (ILC-Artikel)[9] gerechtfertigt werden, vgl. Art 26 ILC-Artikel.[10]

Definition des Begriffs der Gegenmaßnahme („countermeasure"):
„Eine Gegenmaßnahme ist ein an sich völkerrechtswidriger gewaltfreier Akt, der ausnahmsweise gestattet ist, wenn er von dem „Opfer" eines vorangegangenen, noch andauernden völkerrechtlichen Delikts begangen wird, um dieses Delikt abzustellen."[1]

1 *V. Arnauld*, Völkerrecht, 4. Auflage, 2019, S. 256.

Aufgrund der bereits beschriebenen ius cogens Natur des Gewaltverbots, die eine erga omnes Verpflichtung auslöst, können außerdem Gegenmaßnahmen dritter Staaten („third party countermeasures") legitimiert sein.[11] Darüber hinaus werden weitere Maßnahmen nach den ILC-Artikeln legitimiert, wie nach Art. 41 Abs. 1 die interstaatliche Kooperations- und Koordinationsmöglichkeit und nach Abs. 2 das Hilfs- und Unterstützungsverbot gegenüber dem Aggressor-Staat. Zuletzt kann eine die Grenze des Art. 2 Abs. 4 UN-Charta überschreitende Gewaltanwendung die Frage bedingen, ob zwischen den zwei beteiligten Staaten ein internationaler bewaffneter Konflikt im Sinne des gemeinsamen Art. 2 der Genfer Konventionen entstanden ist, der eine Anwendung des humanitären Völkerrechts herbeiführen würde.[12] Insbesondere diese letzte Frage verdeutlicht die enormen rechtlichen Auswirkungen, die eine Gewaltanwendung nach sich ziehen kann.

9 International Law Commission, Draft Articles on the Responsibility of States for Internationally Wrongful Acts, hier abrufbar (Stand: 27.02.25).
10 *Akande*, The Use of Nerve Agents in Salisbury: Why does it Matter Whether it Amounts to a Use of Force in International Law?, hier abrufbar (Stand: 23.02.25).
11 *Akande*, The Use of Nerve Agents in Salisbury: Why does it Matter Whether it Amounts to a Use of Force in International Law?, hier abrufbar (Stand: 23.02.25).
12 *Akande*, The Use of Nerve Agents in Salisbury: Why does it Matter Whether it Amounts to a Use of Force in International Law?, hier abrufbar (Stand: 23.02.25).

Wann liegt nun Gewalt vor? Es besteht Einigkeit darüber, dass der Begriff der Gewalt seinem historischen Kern nach jedenfalls jegliche Art von bewaffneten und physischen Übergriffen („armed force") erfassen soll.[13] Ziel der Charta ist es, eine lückenlose und umfassende Gewaltprävention zu garantieren.[14] Für die Frage, ob Gewalt vorliegt, kommt es nicht darauf an, welche Art von Waffen verwendet wird.[15] Darüber hinaus soll nicht bewaffnete Gewalt erfasst werden, die aufgrund ihres Umfangs und ihrer Wirkung einem bewaffneten Angriff gleichsteht, also insbesondere physisch schwerwiegende Folgen nach sich zieht. Diese Schlussfolgerung lässt sich auf das Nicaragua Urteil des Internationalen Gerichtshofs (IGH) stützen.[16] Das Gericht stellte fest, dass es hinsichtlich der Einschätzung, ob die eingesetzte Gewalt ausreicht, um sie als bewaffneten Angriff im Sinne des Art. 51 UN-Charta zu qualifizieren, auf den Umfang und die Wirkung der Gewalt ankommt („scale and effects").[17] Diese Qualifizierung im Rahmen von Art. 51 der UN-Charta erlaubt den Schluss, dass auch nicht bewaffnete Attacken als Gewalt im Sinne von Art. 2 Abs. 4 der UN-Charta gelten können. Diese Schlussfolgerung ergibt sich aus der Tatsache, dass jeder bewaffnete Angriff im Sinne von Art. 51 UN-Charta zwangsläufig als Gewalt einzustufen ist.[18]

Die Schwelle der Gewalt soll jedoch bei nicht-physischen Zwangs- oder gewaltsamen Handlungen, die weder einen physischen Schaden noch Zerstörung verursachen, nicht überschritten sein.[19] Ebenso nicht erfasst werden politischer oder ökonomischer Zwang, da im Rahmen des Entwurfsprozesses eine Qualifizierung beider Mittel als Gewalt ausdrücklich abgelehnt wurde.[20] Verdeutlicht und bestätigt wurde dieses Verständnis der völkervertraglichen Norm durch die ausdrückliche Zurückweisung des Antrags Brasiliens auf der San Francisco Konferenz 1945, auch ökonomische Gewalt unter den Gewaltbegriff zu subsumieren.[21] Gewalt scheidet zudem bereits tatbestandlich aus, wenn eine der beiden normierten Ausnahmen greift, namentlich das Recht auf Selbstverteidigung nach Art. 51 UN-Charta oder eine Autorisierung des Gewalteinsatzes durch den UN-Sicherheitsrat nach Kapitel 7 der UN-Charta besteht.[22]

B. Cyberattacken als Gewalt

I. Anwendbarkeit des Völkerrechts auf Cyberattacken

Die anhaltende Debatte über den Einsatz von Cybermitteln durch einen Staat gegen einen anderen hat die grundsätzliche Diskussion über die Auslegung des Gewaltverbots neu entfacht.[23] Im Rahmen der folgenden Analyse des Gewaltverbots muss grundsätzlich zwischen der völkervertraglichen Norm sowie der parallel existierenden völkergewohnheitsrechtlichen Norm unterschieden werden. Während sich der Inhalt der vertraglichen Norm nach den Auslegungsregeln völkerrechtlicher Verträge nach Art. 31 Abs. 1 WVK richtet, muss für die völkergewohnheitsrechtliche Norm auf die anerkannten Voraussetzungen der Identifikation des Völkergewohnheitsrechts, namentlich auf die überwiegende Staatenpraxis (consuetudo) sowie die korrespondierende gemeinsame

13 *Corten*, The Law Against War, The Prohibition on the Use of Force in Contemporary International Law, 2023, S. 63.
14 *V. Arnauld*, Völkerrecht, 4. Auflage, 2019, S. 190.
15 IGH, Legality of the threat or use of nuclear weapons, Advisory Opinion, 1996, S. 22, hier abrufbar (Stand: 22.02.25).
16 IGH, Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua vs. United States), hier abrufbar (Stand: 27.02.25).
17 IGH, Nicaragua, Ziff. 195, hier abrufbar (Stand: 27.02.25).
18 Nicht jede Gewalt ist jedoch ein bewaffneter Angriff.
19 *Pobjie*, Prohibited Force, The meaning of "use of force" in international law, 2024, S. 116.
20 *Harris/Sivakumaran*, Cases and Materials on International Law, 9th Ed., Rn. 11-007.

21 UNIO 1945, 609, hier abrufbar (Stand: 23.02.25).
22 *V. Arnauld*, Völkerrecht, 4. Auflage, 2019, S. 256.
23 *Akande/Coco/Dias*, Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond, hier abrufbar (Stand: 22.02.25); *Usman/Mir/Ur-Rehman*, Beyond Conventional War: Cyber Attacks and the Interpretation of Article 2(4) of the UN Charter, hier abrufbar (Stand: 23.02.25).

Rechtsüberzeugung (opinio juris) zurückgegriffen werden.[24] vgl. Art. 38 Abs. 1 lit. b) IGH-Statut. Allerdings weisen die Entwicklungen beider Normen in Teilen Überschneidungen auf. Die erste Frage, die es zu klären gilt, ist, ob die allgemeinen Regelungen des Völkerrechts uneingeschränkt im Cyber-Kontext Anwendung finden.

Rechtsquellen des Völkerrechts, Art. 38 IGH-Statut:

1. Der Gerichtshof, dessen Aufgabe es ist, die ihm unterbreiteten Streitfälle nach Völkerrecht zu entscheiden, wendet an:

a) die internationalen Abkommen allgemeiner oder besonderer Natur, in denen von den im Streit befindlichen Staaten ausdrücklich anerkannte Normen aufgestellt sind;

b) das internationale Gewohnheitsrecht als Ausdruck einer allgemeinen, als Recht anerkannten Übung;

c) die von den zivilisierten Staaten anerkannten allgemeinen Rechtsgrundsätze;

d) unter Vorbehalt der Bestimmung des Artikels 59 die gerichtlichen Entscheidungen und die Lehren der anerkanntesten Autoren der verschiedenen Völker als Hilfsmittel zur Feststellung der Rechtsnormen.

[...]

24 International Law Commission (ILC), Draft Conclusions on identification of customary international law, with commentaries, 2018, S. 124, hier abrufbar.

1. Völkervertragliches Gewaltverbot

Hinsichtlich der völkervertraglichen Regelung des Art. 2 Abs. 4 UN-Charta muss die Reichweite der Norm durch Auslegung ermittelt werden. Nach Art. 31 Abs. 1 WVK muss ein völkerrechtlicher Vertrag „in Übereinstimmung mit der gewöhnlichen, seinen Bestimmungen in ihrem Zusammenhang zukommenden Bedeutung und im Lichte seines Zieles und Zweckes" ausgelegt werden. Bezugnehmend auf die vorherigen Ausführungen lässt sich feststellen, dass bei der Formulierung des Art. 2 Abs. 4 UN-Charta bewusst ein weitgehender und unbestimmter Rechtsbegriff gewählt wurde. „Gewalt" kann dem Wortsinn nach neue Entwicklungen wie Cyberangriffe erfassen. Die Charta verfolgt das Ziel, einen umfassenden und lückenlosen Schutz zu gewährleisten, der langfristig Bestand hat und durch seine präzise Formulierung auch zukünftige Gefahren antizipieren kann.[25] Eine kontextuelle Bezugnahme auf die Präambel verdeutlicht jedoch, dass die Verfasser:innen eine Verbindung zur Anwendung bewaffneter Gewalt herstellen wollten, was insbesondere durch die Formulierung „armed forces shall not be used" unmissverständlich zum Ausdruck kommt. Komplettiert wird der Auslegungskanon des Art. 31 Abs. 1 WVK durch eine Interpretation im Lichte des Ziels und Zwecks des Vertrags. Im Lichte der historischen Ereignisse soll durch die Charta der langfristige und nachhaltige internationale Frieden gesichert werden, der durch ein umfassendes Gewaltverbot garantiert wird.[26] Der Aspekt der Nachhaltigkeit unterstützt die Annahme einer bewusst weit gefassten Formulierung, die eine langfristige Anpassungsfähigkeit gewährleisten soll.

Unterstützt wird dieses Auslegungsergebnis durch die nach Art. 31 Abs. 3b) WVK ebenfalls mit einzubeziehende Staatenpraxis. Der ganz überwiegende Teil der Völkergemeinschaft hat die grundlegende Anwendbarkeit des allgemeinen Völkerrechts auf den Cyberspace bejaht.[27] Ein allgemeiner Konsens zeichnete sich bereits in den Jahren 2013 und 2015 durch die Berichte der UN Groups of

25 Vgl. IGH, Legality of the threat or use of nuclear weapons, Advisory Opinion, 1996, S. 22, hier abrufbar (Stand: 22.02.25).
26 Präambel der UN-Charta.
27 *Urs/Dias/Coco/Akande*, The International Law Protections against Cyber Operations, S. 34, hier abrufbar (Stand: 27.02.25).

Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security[28] ab, an denen auch Russland und China beteiligt waren.[29] Im Jahr 2020 wurde dieser Konsens durch die UN Open-Ended Working Group (OEWG), die allen Vertragsstaaten offenstand, weiter gefestigt.[30] Auch die Bundesregierung bekräftigte in ihrem Statement im März 2021 ausdrücklich ihre Überzeugung, dass das Völkerrecht, einschließlich der UN-Charta und des humanitären Völkerrechts (IHL), uneingeschränkt auf den Cyberspace anwendbar ist.[31]

Dennoch zeigen sich zwischen den staatlichen Positionen Abweichungen hinsichtlich der Anwendung völkerrechtlicher Normen. Beispielsweise signalisierte Russland, die automatische Anwendbarkeit des humanitären Völkerrechts in bewaffneten Konflikten nicht uneingeschränkt anerkennen zu wollen, indem es einen eigenständigen Entwurf für eine neue Konvention[32] in die OEWG einbrachte.[33] Ein weiteres Beispiel für eine Begrenzung der generellen Anwendbarkeit lieferte Großbritannien, als die Regierung 2018 erklärte, dass die Regel der Souveränität nicht auf den Cyberspace anwendbar sein soll.[34] Diese Statements verdeutlichen beispielhaft, dass einige Staaten zwischen der Anwendbarkeit verschiedener Regelungen des Völkerrechts differenzieren. Allerdings bezog sich bisher keine der Einschränkungen auf die generelle Geltung des Gewaltverbots aus Art. 2 Abs. 4 UN-Charta. Hinsichtlich dieser Norm dürfte daher Einigkeit zwischen den Vertragsparteien bestehen, dass das Gewaltverbot grundsätzlich durch Cyberangriffe verletzt werden kann.

28 Überblick, Ergebnisse und Reports hier abrufbar (Stand: 27.02.25).
29 UN GGE 2015 Report 2015, hier abrufbar (Stand: 27.02.25).
30 Überblick, Ergebnisse und Reports hier abrufbar (Stand: 27.02.25).
31 „[…] Germany reemphasizes its conviction that international law, including the UN Charter and international humanitarian law (IHL), applies without reservation in the context of cyberspace.", Position Paper On the Application of International Law in Cyberspace, S. 1, hier abrufbar (Stand: 27.02.25).
32 Proposal of the Russian Federation, Updated concept of the Convention of the United Nations on ensuring international information security, hier abrufbar (Stand: 27.02.25).
33 *Kajander*, Unnecessary Repetition: Russia's Latest Attempt at a New UN Convention on Cyberspace, hier abrufbar (Stand: 25.02.25).
34 Positionspapier Großbritannien (2018), hier abrufbar (Stand: 25.02.25).

2. Völkergewohnheitsrechtliches Gewaltverbot

Hinsichtlich der völkergewohnheitsrechtlichen Entwicklung lässt sich eine Parallele zu der zuvor dargelegten Staatenpraxis erkennen. Ein Großteil der Statements der Staaten betreffen sowohl das normierte als auch das völkergewohnheitsrechtliche Gewaltverbot. Eine überwiegende Rechtsüberzeugung im Sinne einer opinio juris dürfte sich daher gleichermaßen hinsichtlich der völkergewohnheitsrechtlichen Norm belegen lassen.[35] Hinsichtlich der korrespondierenden Staatenpraxis stellt sich das Problem, dass die Einhaltung der Norm keine aktive Handlung voraussetzt, sondern durch eine Nichtverletzung praktiziert wird. Solange kein Cyberangriff vorliegt, der eindeutig als Gewalt im völkerrechtlichen Sinne qualifiziert werden kann, kann sich die Staatenpraxis lediglich durch eine ausdrückliche Bestätigung der Anwendbarkeit entsprechender Normen manifestieren. Auch eine verbale Handlung kann zu einer Staatenpraxis führen.[36] Für den vorliegenden Analysegegenstand dürfte sich feststellen lassen, dass nach dem Willen der Staaten das völkervertragliche Gewaltverbot Cyberattacken erfassen soll. Die Anwendbarkeit sowohl der völkervertraglichen als auch der völkergewohnheitsrechtlichen Norm auf den Cyberraum dürfte daher nicht in Frage stehen.[37]

II. Die Tatbestandsvoraussetzungen im Cyberkontext

Vielmehr hat sich die Diskussion rund um die Anwendbarkeit verlagert. Deutliche Meinungsunterschiede zwischen den Staatenpositionen lassen sich hinsichtlich der Voraussetzungen finden, unter denen ein Cyberangriff die Schwelle der Gewalt überschreiten soll.

35 Vgl. die Staatenpositionen, hier abrufbar (Stand: 25.02.25).
36 ILC, Draft Conclusions on identification of customary international law, with commentaries, 2018, S. 133 f., hier abrufbar (Stand: 25.02.25).
37 *Urs/Dias/Coco/Akande*, The International Law Protections against Cyber Operations, S. 34, hier abrufbar (Stand: 25.02.25).

1. Auslegung der völkervertraglichen Norm

Ausgehend von der Formulierung des Art. 2 Abs. 4 UN-Charta und der obigen Auslegung des Gewaltbegriffs dürfte es jedenfalls ausreichend sein, wenn eine Cyberattacke einem kinetischen Gewalteinsatz gleichsteht.[38] Sie muss also in der Folge des Angriffs zu einer physischen Auswirkung, wie Lebensverlusten oder materieller Zerstörungen führen. Um zu bestimmen, wann das der Fall ist, rekurriert Schmitt im Tallinn Manual 2.0 in diesem Zusammenhang auf die Nicaragua-Entscheidung des IGH und zieht den „scale and effects"-Test zur Bestimmung des Gewaltbegriffs im Cyberkontext heran.[39] Das bedeutet, wenn die eingesetzte Cyber-Operation eine erhebliche Anzahl menschlicher Opfer oder die Zerstörung wichtiger Güter oder kritischer Infrastruktur verursache, wäre das Merkmal der Gewalt erfüllt.[40] Es müsse eine Vergleichbarkeit zwischen einer kinetischen Attacke im regulären Sinn und einer Cyberattacke bestehen.[41] Denkbar wäre zum Beispiel ein Angriff auf die Gesundheitsinfrastruktur, der zum Tod oder zu Verletzungen von Patienten führt.[42] Diese Position hat sich eine Vielzahl von Staaten zu eigen gemacht.[43] Auch sie beziehen sich größtenteils auf die Nicaragua-Rechtsprechung des IGH.

Deutlich umstrittener erscheint die Einordnung von Cyberattacken, die keine physischen Schäden im klassischen Sinn hinterlassen.[44] Ein praktisches Beispiel eines solchen Angriffs stellt die Stuxnet-Attacke der USA und Israels auf das iranische Nuklearprogramm dar, die zu einer schwerwiegenden Störung der Systeme führte.[45] Wird der Wortlaut des Art. 2 Abs. 4 UN-Charta isoliert im Sinne des Zwecks der Charta betrachtet, können derartige Angriffe erfasst werden. Allerdings widerspricht die erweiterte Auslegung dem bisher vorherrschenden historischen Verständnis der Norm. Maßgeblich für eine sich entwickelnde Neuausrichtung des Norminhalts kann jedoch über den Wortlaut und Zweck der Charta hinaus die nachträgliche Staatenpraxis sein, s. Art. 31 Abs. 3 WVK. Nach lit. a) wird in die völkervertragliche Auslegung der Norm „jede spätere Übereinkunft zwischen den Vertragsparteien über die Auslegung des Vertrags oder die Anwendung seiner Bestimmungen" mit einbezogen. Die Meinung müsste dafür nicht nur als einheitliche Praxis einzustufen sein, sondern darüber hinaus eine nachträgliche Einigung der Vertragsparteien darstellen. Eine derartige Einigkeit dürfte jedoch aufgrund inhaltlicher Abweichungen bisher nicht bestehen. Die Afrikanische Union, Costa Rica, und Norwegen haben in ihren Statements einen weitergehenden Anwendungsbereich für Cyberattacken herausgearbeitet.[46] Costa Rica und die Afrikanische Union halten Gewalt ebenso für gegeben, wenn

38 *Schmitt*, Tallinn Manual 2.0 on the international law applicable to cyber operations, S. 333.
39 *Schmitt*, Tallinn Manual 2.0 on the international law applicable to cyber operations, S. 330 f.
40 *Schmitt*, Tallinn Manual 2.0 on the international law applicable to cyber operations, S. 331.
41 Überwiegender Konsens der Staatenpositionen, hier abrufbar (Stand: 23.02.25).
42 *Urs/Dias/Coco/Akande*, The International Law Protections against Cyber Operations, S. 45 f., hier abrufbar (Stand: 25.02.25).
43 Positionspapiere der folgenden Staaten: Afrikanische Liga (2024), Europäischen Union (2024), Australien (2017), Österreich (2024), Canada (2022), Dänemark (2023), Estland (2021), Finnland (2020), Deutschland (2021), Irland (2023), Italien (2021), Niederlande (2019), Norwegen (2021), Rumänien (2021), Schweden (2022), alle hier abrufbar (Stand: 25.02.25).

44 *Usman/Mir/Ur-Rehman*, Beyond Conventional War: Cyber Attacks and the Interpretation of Article 2(4) of the UN Charter, S. 19, hier abrufbar (Stand: 23.02.25).
45 *Usman/Mir/Ur-Rehman*, Beyond Conventional War: Cyber Attacks and the Interpretation of Article 2(4) of the UN Charter, S. 19, hier abrufbar (Stand: 23.02.25).
46 Positionspapier der Afrikanischen Union (2024) S. 6 f., hier abrufbar (Stand 23.02.25); Positionspapier Costa Rica (2023), S. 11, hier abrufbar (Stand: 23.02.25); Positionspapier Norwegen (2021), hier abrufbar (Stand 23.02.25).

ein Cyberangriff zu einer dauerhaften Beeinträchtigung von Computersystemen der kritischen Infrastruktur führt, ohne dass es zu physischen Folgen kommt.[47] Norwegen geht davon aus, dass die erhebliche Störung staatlicher Systeme der kritischen Infrastruktur oder des Bankwesens (z.B. durch den Einsatz von Krypto-Viren) Gewalt verkörpern kann.[48] Die Niederlande halten einen noch größeren Anwendungsbereich für möglich, indem sie feststellen, dass zum jetzigen Zeitpunkt eine Gewaltanwendung nicht ausgeschlossen werden kann, wenn Cyberangriffe mit erheblichen finanziellen oder ökonomischen Folgen einhergehen.[49] Auch wenn ein Teil der Vertragsstaaten ihre Position veröffentlicht hat und auf die Übertragung des „scale and effects"-Test abstellt, so kann nicht von einer Einigung hinsichtlich der Voraussetzungen zwischen allen Vertragsstaaten gesprochen werden.

Es bleibt allerdings eine Berücksichtigung nach Art. 31 Abs. 3b) WVK. Hiernach ist „jede spätere Übung bei der Anwendung des Vertrags, aus der die Übereinstimmung der Vertragsparteien über seine Auslegung hervorgeht" einzubeziehen. Ständige Praxis, die einen solchen Konsens widerspiegelt, liegt vor, sobald ein Teil der Vertragsstaaten aktiv eine nachfolgende Praxis ausübt. Wie viele Vertragsparteien diese Praxis ausüben müssen, ist nicht genau festgelegt.[50] Auch Schweigen kann in Einzelfällen Akzeptanz der Praxis widerspiegeln, wenn die äußeren Umstände eine aktive Reaktion erzwingen. Im Fall von Cyberangriffen dürfte zu berücksichtigen sein, dass die UN Working Groups allen Vertragsparteien offenstehen. Das wiederum könnte dazu führen, dass eine Nichtbeteiligung kombiniert mit einem Schweigen tatsächlich zur Annahme von Akzeptanz führen könnte.[51] Ob jedoch hinsichtlich der Voraussetzungen bereits von einer einheitlichen und akzeptierten nachträglichen Praxis ausgegangen werden kann, erscheint fraglich. Erneut müssen die bereits beschriebenen inhaltlich abweichenden Positionen in den Blick genommen werden. Für die Annahme einer nachträglichen Praxis spricht jedenfalls, dass die überwiegenden Vertragsparteien übereinstimmend signalisiert haben, dass nicht jeder Cyberangriff automatisch den Gewaltbegriff erfüllen soll.

Bei genauer Betrachtung kann jedoch ein weiterer Punkt zu Problemen führen. In ihren Statements differenzieren einige Staaten nicht dezidiert zwischen der völkervertraglichen und der völkergewohnheitsrechtlichen Norm.[52] Einige beziehen sich nicht ausdrücklich auf Art. 2 Abs. 4 UN-Charta,[53] während wiederum andere Staaten ihre Argumentation ausschließlich unter Bezugnahme des Art. 2 Abs. 4 UN-Charta aufbauen.[54] Die teilweise auseinanderfallenden Formulierungen sorgen für eine noch unübersichtlichere Auffächerung der Statements, die die Annahme einer einheitlichen Praxis nach Art. 31 Abs. 3b) WVK hinsichtlich des völkervertraglichen Gewaltverbots nach Art. 2 Abs. 4 UN-Charta weiterhin erschwert.

47 Positionspapier Costa Rica (2023), S. 11, hier abrufbar (Stand: 23.02.25); Positionspapier der Afrikanischen Union (2024) S. 6 f., hier abrufbar (Stand 23.02.25).
48 Positionspapier Norwegen (2021), hier abrufbar (Stand 23.02.25).
49 Positionspapier Niederlande (2019), hier abrufbar (Stand 23.02.25).
50 *V. Arnauld*, Völkerrecht, 4. Auflage, 2019, S. 152.

51 Zu den Voraussetzungen nicht geäußert hat sich z.B. Pakistan (2023), Positionspapier hier abrufbar und China (2021), hier abrufbar (beides Stand: 23.02.25).
52 Positionspapiere von Australien (2020), Neuseeland (2020), Polen (2022), alle hier abrufbar (Stand: 23.02.25).
53 Positionspapier der Afrikanische Union (2024), hier abrufbar (Stand 23.02.25).
54 Positionspapiere von Canada (2022), Japan (2021), Großbritannien (2021), alle hier abrufbar (Stand: 23.02.25).

2. Völkergewohnheitsrecht

Die Bescheinigung einer praktischen Fortentwicklung des völkergewohnheitsrechtlichen Gewaltverbots erscheint meiner Ansicht nach noch komplexer und schwieriger zu begründen. Hinsichtlich verbaler Staatenpraxis und opinio juris bieten nur die Statements der Staaten einen Anhaltspunkt. Inhaltlich kann hier auf die bereits zur vertraglichen Norm dargestellten Staatenpositionen rekurriert werden. Für die Bejahung der Staatenpraxis bedarf es jedoch einer „weit überwiegenden Praxis" im Sinne einer „Quasi-Universalität"[55] nicht nur der Vertragsparteien, sondern der gesamten Völkergemeinschaft. Diese Praxis muss von gewisser Dauer, Einheitlichkeit und Verbreitung der Übung sein.[56] Im Hinblick auf diese äußerst umfassenden Kriterien dürfte eine Annahme von Völkergewohnheitsrecht hinsichtlich der Voraussetzungen, insbesondere der „scale and effects"-Kriterien zum jetzigen Zeitpunkt scheitern. Hinzukommen die bereits genannten Staaten, die bisher zu den genaueren Voraussetzungen des Gewaltbegriffs im Cyberspace geschwiegen haben.[57] Das Schweigen dürfte im Gegensatz zur völkervertraglichen Entwicklung in diesem Kontext nicht zwangsläufig als Zustimmung gewertet werden. Völkergewohnheitsrechtlich dürfte sich also noch keine weit überwiegende Überzeugung und Praxis gebildet haben.

3. Problem des "scale and effects"-Tests

Erkennbar ist jedenfalls die Tendenz der Staaten hin zu einer Übertragung des „scale and effects"-Tests auf die Frage, wann ein Cyberangriff im Sinne des Gewaltverbots vorliegen soll. Dieser Ansatz ist insofern überzeugend, als er versucht, den Anwendungsbereich des Gewaltbegriffs zu begrenzen.[58] Nicht jeder Cyberangriff soll unabhängig von seiner Natur oder seinen Folgen den Begriff der Gewalt erfüllen können. Andernfalls käme es zu einer Überdehnung des Anwendungsbereichs, der das Gewaltverbot nachhaltig entwerten würde.[59] In dieser Hinsicht erweisen sich die Merkmale als zur Abgrenzung geeignet.

Dennoch ist der Vorschlag nicht gänzlich frei von Problemen. Die Übertragung des Grundsatzes könnte zu einer Verwässerung der Grenzen zwischen dem Gewaltbegriff („force") und dem des bewaffneten Angriffs („armed attack") führen.[60] Während bisher überwiegende Einigkeit bestand, dass der Begriff „armed attack" nur besonders schwere Formen der Gewaltanwendung erfassen soll, während der Gewaltbegriff umfassender gelten soll,[61] könnte der neue Konsens den Gewaltbegriff verengen und dem des bewaffneten Angriffs gleichsetzen.[62] Das hätte zur Folge, dass bisher erfasste Formen der Gewalt, aus dem Anwendungsbereich des Gewaltverbots herausfallen und künftig jede Form der Gewalt automatisch das Recht der Selbstverteidigung auslösen würde, was das Stufenverhältnis zwischen Art. 2 Abs. 4 UN-Charta und Art. 51 UN-Charta auflösen würde.[63] Unabhängig von der Anknüpfung an den Cyberkontext, würde ein derartiges Verständnis gleichsam für sonstige Gewaltanwendungen gelten, sodass ein Großteil kleinerer und nicht so erheblicher Gewaltanwendungen nicht vom Gewaltverbot erfasst würde.[64] Diese Folge stünde im Widerspruch zur Intention, die sowohl dem völkervertraglichen als auch dem völkergewohnheitsrechtlichem Gewaltverbot zugrunde liegt, nämlich ein umfassendes Verbot von Gewalt zu begründen.[65] Die Verschmälerung des Gewaltbegriffs beträfe nicht ausschließlich den Cyberkontext, sondern stünde in unmittelbarem Zusammenhang zu der grundlegende dogmatische Frage, wie der Gewaltbegriff generell zu definieren ist.[66] In dieser Hinsicht muss eine vorsichtige und differenzierte Betrachtung erfolgen, um einer generelle über den Cyberkontext

55 *V. Arnauld*, Völkerrecht, 4. Auflage, 2019, S. 152.
56 *V. Arnauld*, Völkerrecht, 4. Auflage, 2019, S. 152.
57 Z.B. Positionspapier China, hier abrufbar (Stand: 23.02.25).
58 *Urs/Dias/Coco/Akande*, The International Law Protections against Cyber Operations, S. 72, hier abrufbar (Stand: 23.02.25).
59 *Urs/Dias/Coco/Akande*, The International Law Protections against Cyber Operations, S. 72, hier abrufbar (Stand: 23.02.25).
60 Vgl. Positionspapier USA, das die Begriffe sogar synonym verwendet, hier abrufbar (Stand: 23.02.25).
61 *V. Arnauld*, Völkerrecht, 4. Auflage, 2019, S. 190.
62 Vgl. Positionspapier Costa Rica, S. 11.
63 *Schmitt*, Tallinn Manual 2.0. on the international law applicable to cyber operations, S. 337.
64 Vgl. *Wanyana* in Bezug auf das Phänomen der cognitive warfare, Cognitive Warfare: Does it Constitute Prohibited Force?, hier abrufbar (Stand: 23.02.25)
65 Vgl. *V. Arnauld*, Völkerrecht, 4. Auflage, 2019, S. 190.
66 *Usman/Mir/Ur-Rehman*, Beyond Conventional War: Cyber Attacks and the Interpretation of Article 2(4) of the UN Charter,), S. 22., hier abrufbar (Stand: 23.02.25).

hinausgehende Aufweichung des Gewaltverbots vorzubeugen.[67] Es sollten daher weitere Kriterien zur Bestimmung des Begriffs des bewaffneten Angriffs, z.B. in Form eines „Gravity"-Kriteriums diskutiert werden.[68] Diese Herausforderung eröffnet zugleich die Möglichkeit, eine präzisere und nuancierte Definition des Gewaltbegriffs zu entwickeln.[69]

C. Fazit und Ausblick

Eines scheint bereits festzustehen: Das Gewaltverbot findet Anwendung auf den Bereich des Cyberspace. Nicht geklärt ist hingegen, unter welchen Voraussetzungen ein Cyberangriff die Schwelle des Gewaltverbots überschreiten soll. Während einige Staaten die Nähe und Vergleichbarkeit zu einem kinetischen Angriff betonen und infolgedessen für eine Übertragung des vom IGH in seiner Nicaragua-Entscheidung entwickelten „scale and effects"-Test plädieren, hat sich ein anderer Teil der Staatengemeinschaft nicht oder jedenfalls nicht gleichermaßen differenziert zu der Frage geäußert. Die Annahme einer überwiegenden Staatenpraxis zu den Anforderungen an den Gewaltbegriff im Cyberkontext, wenn keine unmittelbaren physischen Auswirkungen vorliegen, gestaltet sich daher komplex. Eine staatliche Übereinkunft in den UN-Gremien zeichnet sich mit Blick auf das Verhalten von Russland bisher nicht ab. Selbst wenn sich die Staatenpraxis zunehmend in Richtung einer Übertragung des „scale and effects"-Tests entwickeln sollte, wäre eine sorgfältige Abwägung der Grenzen zwischen dem Gewaltverbot und dem Selbstverteidigungsrecht unerlässlich. Die fortschreitende Entwicklung der Staatenpraxis in Bezug auf die Voraussetzungen des Gewaltbegriffs hat nicht nur Auswirkungen auf die rechtliche Einordnung von Cyberangriffen, sondern enthält tiefgreifende Implikationen für die fundamentalen Parameter des Gewaltverbots. Die Diskussion wirft die grundlegende Frage auf, ob überhaupt jemals ein gefestigter Konsens über die allgemeinen Voraussetzungen des Gewaltbegriffs bestanden hat. In diesem Bereich bleibt die völkerrechtliche Praxis im Wandel. Es liegt letztlich an den Staaten, die Kriterien für die Anwendung des Gewaltverbots im Cyberkontext – und darüber hinaus – zu präzisieren und zu definieren.

Zurück zum Inhaltsverzeichnis

67 *Usman/Mir/Ur-Rehman*, Beyond Conventional War: Cyber Attacks and the Interpretation of Article 2(4) of the UN Charter, S. 21, hier abrufbar (Stand: 23.02.25).
68 Vgl. *Urs/Dias/Coco/Akande*, The International Law Protections against Cyber Operations, S. 73 ff., hier abrufbar (Stand: 25.02.25).
69 *Usman/Mir/Ur-Rehman*, Beyond Conventional War: Cyber Attacks and the Interpretation of Article 2(4) of the UN Charter, S. 21, hier abrufbar (Stand: 23.02.25).

Aufsatz

Spannungsfeld: Digitale Souveränität des Staats und das Vergaberecht

Tim Rösch

Open Peer Review

Dieser Beitrag wurde lektoriert von: Hendrik Eppelmann und Kim Salg

Tim Rösch studierte Wirtschafts- und Steuerrecht im Master (LL.M) an der Ruhr-Universität Bochum, sein Interessenschwerpunkt liegt an der Schnittstelle von Recht, Digitalisierung und Finanzen. Er ist seit 2019 für verschiedene Bundesbehörden tätig und engagiert sich bei recode.law e.V. Der Aufsatz spiegelt ausschließlich die persönliche Auffassung des Autors wider.

Ein selbstbewusstes Ziel formulierten die ehemaligen Ampelkoalitionäre in ihrem Koalitionsvertrag 2021 – 2025: „Darüber hinaus sichern wir die digitale Souveränität, u. a. durch das Recht auf Interoperabilität und Portabilität sowie das Setzen auf offene Standards, Open Source und europäische Ökosysteme, etwa bei 5G oder KI."[1]

1 Der Aufsatz gibt ausschließlich die persönliche Auffassung des Autors wieder und steht nicht im Zusammenhang mit dessen dienstlicher Funktion. Zum Zwecke der besseren Lesbarkeit wird bei personenbezogenen Hauptwörtern nur die männliche Form verwendet. Diese Begriffe sollen für alle Geschlechter gelten.
SPD/BÜNDNIS 90 / DIE GRÜNEN/FDP, Koalitionsvertrag 2021 – 2025, 16, hier abrufbar (Stand: 09.02.2025).

Die Positionierung der digitalen Souveränität im Koalitionsvertrag verdeutlicht, dass deren Bedeutung längst im politischen Raum erkannt wurde. Gleichzeitig unterliegen Bedarfsträger und Vergabestellen (wie die am Einkaufsprozess Beteiligten im öffentlichen Dienst gemeinhin bezeichnet werden) bei der Auswahl von Produkten und Lieferanten dem strengen Regelungsregime des Vergaberechts und haben eine Vielzahl formeller und materieller Vorgaben zu erfüllen. Das Spannungsverhältnis zwischen dem strategischen Ziel der digitalen Souveränität einerseits und der rechtskonformen Beschaffung im öffentlichen Dienst andererseits aufzuzeigen, soll Gegenstand dieses Aufsatzes sein.

A. Digitale Souveränität im Überblick

Wer sich näher mit den digitalpolitischen Programmen auf Bundesebene befasst, stößt schnell auf den rechtlich unbestimmten Begriff der digitalen Souveränität.[2]

Regelmäßig wird auf die Definition des **Fraunhofer-Instituts für Offene Kommunikationssysteme (FOKUS)** zurückgegriffen. Demnach ist digitale Souveränität **„die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“**.[3] Eine souveräne Bundesverwaltung muss also auch im digitalen Raum stets über Handlungs- und Entscheidungsautonomie verfügen.

Digitale Souveränität beschreibt die Summe aller Fähigkeiten und Möglichkeiten der öffentlichen Verwaltung, ihre Rolle in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.

Digitale Souveränität ist hierbei als Oberbegriff zu verstehen – eine gute Übersicht über die verschiedenen Dimensionen gibt ein Bericht der KGSt[4] aus 2021: Insbesondere der teils synonym verwendete Begriff „technologische Souveränität“ und das in Bezug auf die wachsende Bedeutung von KI-Systemen zunehmend relevante Feld der „Datensouveränität“ können als Ausprägungen von digitaler Souveränität betrachtet werden.[5]

Als Bedrohung für die technologische Souveränität wird der **„Vendor-Lock-In“** beschrieben. Dieser Effekt bezeichnet (vereinfacht dargestellt) die Gefahr einer einseitigen Abhängigkeit vom Anbieter einer Software, Plattform oder Infrastruktur. Diese Abhängigkeit kann entweder durch die finanzielle Intensität eines gewünschten Anbieterwechsels, fehlende Migrationsmöglichkeiten und Schnittstellen zu einer anderen Lösung oder durch eine Monopolstellung des Anbieters ausgelöst werden.[6]

Die Nachteile liegen auf der Hand: Ist das Abhängigkeitsverhältnis erst einmal geschaffen, befindet sich die Institution in einer geschwächten Verhandlungsposition, muss Preis- und Leistungsanpassungen des Anbieters weitestgehend hinnehmen und ist bei der Erbringung von Dienstleistungen (im Falle des Staats: an die Bürger) von der Verfügbarkeit der Leistung eines Dritten abhängig. Zudem droht die Verknüpfung politischer Forderungen von Drittstaaten mit der Bereitstellung von

2 Bundesministerium des Innern und für Heimat (BMI), abrufbar hier, Bundesregierung, Digitalstrategie, 48 f., abrufbar hier (jeweils Stand 09.02.2025).
3 Goldacker, Digitale Souveränität (hrsg. Kompetenzzentrum Öffentliche IT, Fraunhofer- FOKUS), 3, abrufbar hier (Stand: 09.02.2025).

4 Kommunale Gemeinschaftsstelle für Verwaltungsmanagement.
5 Krellmann (hrsg. KGSt), Bericht Nr. 05/2021: Open Source in Kommunen, Ein Baustein für mehr Digitale Souveränität Teil 1, 12 f., abrufbar hier (Stand: 14.02.2025).
6 Detailliert hierzu: Krellmann (hrsg. KGSt), Bericht Nr. 05/2021: Open Source in Kommunen Teil 1, 13, abrufbar hier (Stand: 09.02.2025); PwC Strategy& (Germany) GmbH, Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern, 3 f., abrufbar hier: (Stand: 09.02.2025).

Technologien[7].

Gleichzeitig sieht sich die öffentliche Hand der Herausforderung gegenüber, dringend Fortschritte in der Digitalisierung erzielen zu müssen. Es dürfte breiter Konsens darüber bestehen, dass der Grad an Verwaltungsdigitalisierung in Deutschland noch deutliche Defizite aufweist – hat doch die Bundesregierung mit dem Onlinezugangsgesetz (OZG) und dem Update OZG 2.0 gleich zwei Gesetze auf den Weg gebracht, mit denen die Bereitstellung digitaler Verwaltungsleistungen forciert werden soll.[8] In Konsequenz kann ein Zielkonflikt entstehen: Einerseits sollen digitale Leistungen zügig bereitgestellt werden, andererseits droht bei der Beschaffung von marktgängigen und vermeintlich schnell einsetzbaren Technologien vorherrschender Konzerne ein Verlust an Souveränität.

„Ist das Abhängigkeitsverhältnis erst einmal geschaffen, befindet sich die Institution in einer geschwächten Verhandlungsposition."

Der Stärkung digitaler Souveränität kommt mithin auch in Bezug auf den allgemeinen Fortschritt in der Digitalisierung des öffentlichen Sektors eine hohe praktische Bedeutung zu. Die **Föderale IT-Kooperation (FITKO)** hat hierzu drei strategische Ziele erarbeitet: Das Vorhalten von Alternativoptionen, die Ertüchtigung der Verwaltung hin zu mehr Gestaltungkompetenz in der IT sowie die Stärkung der eigenen Position gegenüber Anbietern von IT-Lösungen.[9]

7 Vgl. Horstmann, Stellungnahme Anhörung „Open Source" im Ausschuss für Digitales, 3, abrufbar hier (Stand: 09.02.2025).
8 Vgl. Begründung der Bundesregierung zum Gesetzesentwurf, BT-Drs. 20/8093, 23.
9 FITKO, Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung, 6, abrufbar hier (Stand: 09.02.2025).

Flankiert werden diese Ziele von Handlungsempfehlungen, von denen für den Zweck dieses Aufsatzes insbesondere zwei herausgegriffen werden:

Einsatz von Open Source Software (OSS):

Der verstärkte OSS-Einsatz in der öffentlichen Verwaltung wird als zentrale Maßnahme zur Stärkung der digitalen Souveränität betrachtet. In Abgrenzung zu proprietärer Software überzeugt OSS insbesondere durch ein erhöhtes Maß an Innovationskraft, Adaptivität, Transparenz, Sicherheit und Unabhängigkeit.[10]

Stärkung des europäischen Markts

Um Abhängigkeiten der öffentlichen Verwaltung zu reduzieren, ist eine Diversifizierung der Anbieterseite erforderlich. Dies kann insbesondere durch mehr Kooperation auf europäischer Ebene und unter Einbeziehung des Innovationspotenzials von Start-Ups und KMU bei der Vergabe öffentlicher Aufträge erreicht werden.[11]

Wenn der Staat an den Markt zur Beschaffung einer Leistung herantritt, unterliegt er in der Regel dem Vergaberecht.[12] Digitale Souveränität stellt einen vergabefremden Aspekt dar, den das Vergaberecht als Kriterium zur Anbieter- oder Produktauswahl nicht explizit kennt. Hieraus ergeben sich einige Herausforderungen für die öffentliche Verwaltung, wenn sie Souveränitätserwägungen in ihre Einkaufsentscheidungen einfließen lassen möchte.

10 Bundesregierung, Digitalstrategie, 9, abrufbar hier (Stand 09.02.2025); PwC Strategy& (Germany) GmbH, Strategische Marktanalyse, 28, abrufbar hier: (Stand: 09.02.2025); Horstmann, Stellungnahme Anhörung „Open Source" im Ausschuss für Digitales, 3, abrufbar hier (Stand: 09.02.2025).
11 Vgl. bitkom, Aktionsplan Digitale Souveränität, Nr. 3, hier abrufbar (Stand: 09.02.2025); Bayerisches Staatsministeriums für Digitales, Pressemitteilung vom 26.09.2022, hier abrufbar (Stand 09.02.2025); FITKO, Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung, 10, abrufbar hier (Stand: 09.02.2025).
12 Dörr, in: Burgi/Dreher/Opitz, Beck'scher Vergaberechtskommentar, Bd. 1, 4. Auflage 2022, Einleitung, Rn. 2

B. Die Umsetzbarkeit digitaler Souveränität im Vergaberecht

I. Vergaberecht – ein Thema zur Selbstbeschäftigung der Verwaltung?

Nach § 97 Abs. 1 S. 1 des Gesetzes gegen Wettbewerbsbeschränkung (GWB) werden öffentliche Aufträge und Konzessionen im Wettbewerb und im Wege transparenter Verfahren vergeben. Öffentliche Auftraggeber sind hierbei u.a. die Gebietskörperschaften sowie deren Sondervermögen (§ 99 Abs. 1 Nr. 1 GWB).

Ein primäres Regelungsziel des Vergaberechts liegt im Schutz des Wettbewerbs.[13] Das Vergaberecht ist mithin keineswegs ein Selbstzweck, sondern dient aus staatlicher Sicht einem geordneten, wirtschaftlichen Einkauf sowie aus Unternehmenssicht der Schaffung von fairen Bedingungen im Wettbewerb um staatliche Aufträge.[14] Dass diese Aufträge wirtschaftliches Gewicht vorzuweisen haben, verdeutlichen die Zahlen aus dem aktuellen Monitoringbericht zum Vergaberecht: So belief sich das Gesamtvolumen öffentlicher Aufträge in Deutschland 2022 auf rund 132 Mrd. €.[15]

13 Dörr, in: Burgi/Dreher/Opitz, Beck'scher Vergaberechtskommentar, Bd. 1, 4. Auflage 2022, Einleitung, Rn. 11.
14 Vgl. Weiner, in: Gabriel/Krohn/Neun, Handbuch Vergaberecht, 4. Auflage 2024, § 1 Rn. 3.
15 Hier abrufbar (Stand 09.02.2025).

Der Dualismus des Vergaberechts in Deutschland

Bereits in der Vielzahl an Rechtsquellen (s. Abbildung 2) zeigt sich die Komplexität des Vergaberechts. Die anzuwendenden Vorschriften unterscheiden sich je nach Auftraggeber, Auftragsgegenstand sowie Nettoauftragswert: In Abhängigkeit der Erreichung bestimmter Schwellenwerte nach § 106 Abs. 2 GWB wird von ober- oder unterschwelligen Aufträgen gesprochen.

Das **Kartellvergaberecht** oberhalb der Schwellenwerte ist durch europäische Richtlinien geprägt und wird im nationalen Recht (v.a. GWB, VgV, VSVgV, KonzVgV, SektVO) umgesetzt. Unterhalb des Schwellenwerts kommt das sogenannte **Haushaltsvergaberecht** zu Anwendung – dieses ist rein national geprägt, findet sich für den Bund vor allem in der Unterschwellenvergabeordnung (UVgO) wieder und erlangt Geltung über die Bundeshaushaltsordnung.[16]

Ausgewählte aktuelle Schwellenwerte:

Bauaufträge	5.538.000 €
Liefer- und Dienstleistungsaufträge oberster und oberer Bundesbehörden sowie vergleichbarer Bundeseinrichtungen	143.000 €
Verteidigungs- oder sicherheitsspezifische Liefer- und Dienstleistungsaufträge	443.000,00 €

II. Open-Source first – zu Lasten der Produktneutralität?

Im Einsatz von OSS in der öffentlichen Verwaltung liegt ein Schlüssel zur Stärkung der digitalen Souveränität – die einschlägigen Fachkreise machen sich

16 § 55 BHO i.V.m. Ziffer 2 zu § 55 VV-BHO, § 1 Abs. 1 UVgO; vgl. Jentzsch, in: Leinemann/Otting/Kirch/Homann, VgV – UvgO, 1. Aufl. 2024, UVgO § 1 Rn. 4.

konsequenterweise für einen grundsätzlichen Vorrang von OSS in der IT-Beschaffung stark.[17] Auch die Bundesregierung scheint diese Auffassung zu teilen: Mit dem Gesetz zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung hat der Gesetzgeber den neuen § 16a in das E-Government-Gesetz (EGovG) aufgenommen, wonach Bundesbehörden bei neu anzuschaffender Software OSS grundsätzlich Vorrang einräumen sollen. Ausweislich der Gesetzesbegründung liegt das Regelungsziel in der Stärkung der digitalen Souveränität.[18]

Dieses Bekenntnis zu OSS ist zu begrüßen – es lässt allerdings Verbindlichkeit vermissen. Grund hierfür ist der primär deklaratorische Charakter: § 16a EGovG ist keine vergaberechtliche Norm. Dies hat zur Folge, dass hinsichtlich der Zulässigkeit eines OSS-Vorrangs in der Beschaffungspraxis noch einige Rechtsunsicherheit besteht. Begründet liegt dies unter anderem im Gebot der produktneutralen Ausschreibung: Im Vorlauf eines Vergabeverfahrens haben öffentliche Auftraggeber die Vergabeunterlagen zu erstellen. Ein zentrales Dokument stellt die Leistungsbeschreibung (LB) dar. Hierin hat der öffentliche Auftraggeber nach § 121 Abs. 1 S. 1 GWB den Auftragsgegenstand so eindeutig und erschöpfend wie möglich zu beschreiben. In Umsetzung des Wettbewerbsprinzips und des Gleichbehandlungsgrundsatzes hat die Formulierung der LB grundsätzlich produktneutral zu erfolgen (§ 31 Abs. 6 VgV). Hierdurch soll eine Vorfestlegung des öffentlichen Auftraggebers auf ein bestimmtes Produkt und eine dadurch bedingte Einschränkung des Markts verhindert werden.[19]

In der Festlegung auf OSS in der LB könnte folglich ein Verstoß gegen die Produktneutralität und in Konsequenz die Ungleichbehandlung von Marktteilnehmern begründet liegen, da hierdurch insbesondere proprietäre (also in ihrer Nutzung und Weitergabe durch den Hersteller beschränkte)) Lösungen kategorisch benachteiligt

17 ZenDiS (Zentrum digitale Souveränität), Positionspapier Digitale Souveränität im Vergaberecht, 9f., abrufbar hier (Stand: 10.02.2025); OSBA (Open Source Business Alliance), abrufbar hier (Stand: 10.02.2025).
18 BT-Drs. 20/10417, 32.
19 Endler, in: Osseforth, IT-Vergabe-HdB, 1. Aufl. 2022, § 7 Rn. 5-7.

werden. Als greifbares Beispiel kann Standard-Office-Software dienen: So ist LibreOffice als OSS hinsichtlich des Anwendungsszenarios und der Funktionalitäten weitestgehend mit marktbeherrschender, proprietärer Software vergleichbar. Durch die Festlegung auf OSS wäre eine erfolgreiche Teilnahme am Verfahren für den eigentlichen Marktführer nahezu aussichtslos, ohne das eigene Geschäfts- und Lizenzmodell grundlegend zu verändern.

Die Frage nach der Zulässigkeit eines OSS-Vorrangs im derzeit gültigen Vergaberecht untersucht **Wiebe** umfassend in einem lesenswerten Gutachten im Auftrag der **OSBA**. Sofern OSS im Ausgangspunkt ausschreibungspflichtig ist, kann im Ergebnis auch eine potenzielle Ungleichbehandlung durch sachliche Gründe gerechtfertigt sein, sodass OSS im Rahmen der Leistungsbeschreibung oder des Zuschlags priorisiert werden kann – es verbleiben allerdings Unsicherheiten.[20]

Daher fordern **OSBA** und **ZenDiS** richtigerweise den Gesetzgeber zum Handeln auf: Eine gesetzliche Verankerung des OSS-Vorrangs auf Basis von § 97 Abs. 2 oder Abs. 3 GWB erscheint zur Stärkung der digitalen Souveränität als legitimen Zweck zulässig.[21] Durch die Implementierung einer entsprechenden Regelung in der VgV und UVgO könnte die Rechtsunsicherheit für die Beschaffungsstellen beseitigt und somit ein flächendeckender OSS-Einsatz in der Bundesverwaltung begünstigt werden.[22]

20 Wiebe, Gutachten zur vorrangigen Beschaffung und Entwicklung von Open Source Software in der Bundesverwaltung, 40, abrufbar hier (Stand: 10.02.2025).
21 Wiebe, Gutachten zur vorrangigen Beschaffung und Entwicklung von Open Source Software in der Bundesverwaltung, 40, abrufbar hier (Stand: 10.02.2025).
22 ZenDiS, Positionspapier, 11, abrufbar hier (Stand: 10.02.2025); OSBA, abrufbar hier (Stand: 10.02.2025).

Eine große Chance zur Implementierung einer solchen Regelungen bietet die anstehende Reformierung des Vergaberechts: Im Dezember 2024 durch das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) auf den Weg gebracht, konnte das Vergaberechtstransformationsgesetz (VergRTransfG) nicht mehr in der auslaufenden Legislaturperiode umgesetzt werden. Eine künftige Bundesregierung sollte die Chance ergreifen und das mit § 16a EGovG kodifizierte OSS-Bekenntnis auch vergaberechtlich sattelfest ausgestalten. Die stärkere Berücksichtigung von Aspekten der digitalen Souveränität im VergRTransfG dürfte auch Anklang bei den Ländern finden, siehe hierzu Ziffer III 2.).

III. Stärkung des europäischen Markts

Unabhängig von der Priorisierung von OSS in der IT der öffentlichen Verwaltung, wird diese selbstverständlich auch in der Zukunft auf die Beschaffung am Markt angewiesen sein. Umso wichtiger erscheint es, die regulatorischen Rahmenbedingungen für einen innovationsfreundlichen, europäischen Binnenmarkt zu schaffen. Das Vergaberecht kann hierbei je nach Ausgestaltung als Bremsklotz oder Katalysator wirken.

1. Berücksichtigung von Start-Ups bei öffentlichen Ausschreibungen

Die Berücksichtigung von Mittelstandsinteressen stellt im Vergaberecht keine neue Überlegung dar: Mit dem in § 97 Abs. 4 GWB normierten Grundsatz der Losvergabe sollen diese Berücksichtigung finden, indem Aufträge grundsätzlich in Lose aufzuteilen und an mehrere Auftragnehmer zu vergeben sind.[23] Die nennenswerte Einbeziehung von Start-Ups scheint bislang allerdings kaum zu gelingen: Laut einer Studie des Leibniz-Zentrums für Europäische Wirtschaftsforschung (ZEW) haben seit ihrer Gründung gerade einmal 11% der deutschen Start-Ups an einer öffentlichen Ausschreibung teilgenommen, einen Auftrag erhielten lediglich 7%.[24]

23 Weiner in: Gabriel/Krohn/Neun, VergabeR-HdB, 4. Aufl. 2024, § 1 Rn. 66.
24 Abrufbar hier (Stand: 12.02.2025).

„Gerade für Start-Ups im Early- oder Growth-Stage können Eignungskriterien eine Hürde für die Teilnahme am Vergabeverfahren darstellen."

In der Ursachenforschung müssen auch die vergaberechtlichen Anforderungen kritisch betrachtet werden. So können öffentliche Aufträge nur an Unternehmen vergeben werden, die vom Auftraggeber festgelegte Eignungskriterien erfüllen, welche sich unter anderem auf die wirtschaftliche und finanzielle Leistungsfähigkeit beziehen dürfen, § 122 Abs. 2 S. 2 Nr. 2 GWB. Der öffentliche Auftraggeber kann insbesondere einen Mindestjahresumsatz oder Anforderungen an Bilanzkennzahlen als Eignungskriterium festlegen, wenn diese im Zusammenhang mit der Auftragsausführung stehen (§ 45 Abs. 1 VgV).[25]

Gerade für Start-Ups im Early- oder Growth-Stage können diese Eignungskriterien eine Hürde für die Teilnahme am Vergabeverfahren darstellen, da sie häufig über noch keine signifikanten Umsätze im mehrjährigen Betrachtungszeitraum[26] oder ausreichende Eigenkapitalausstattung verfügen. Insbesondere kann es für Start-Ups unmöglich sein, Nachweise zu historischen Finanzinformationen, beispielsweise Umsätzen der letzten fünf Jahren, vorzulegen – auch wenn die Voraussetzungen im Zeitpunkt der Teilnahme am Vergabeverfahren erfüllt sind.

Der Gesetzgeber hat dies erkannt und den Abbau von Hürden für junge Unternehmen als ausdrückliches Ziel im VergRTransfG-E aufgenommen. So sollen nach dem neuen § 42 Abs. 2 VgV (Art. 7 Nr. 16 lit. a) VergRTransfG-E) die besonderen Umstände von jungen Unternehmen bereits bei der Auswahl von Eignungskriterien Berücksichtigung finden. Der neu gefasste § 45 Abs. 5 VgV (Art. 7 Nr. 17 VergRTransfG-E) sieht vor, dass die Eigenschaft als junges Unternehmen einen berechtigten Grund darstellen kann, durch den der Nachweis der wirtschaftlichen Leistungsfähigkeit auch durch andere als die vom Auftraggeber geforderten Nachweise erbracht werden kann.

Die vorgesehenen Änderungen scheinen zwar grundsätzlich geeignet, die Hürden für junge Unternehmen zur Teilnahme an Vergabeverfahren zu senken – zu kritisieren ist jedoch, dass in Bezug auf § 45 Abs. 5 VgV lediglich Ermessensspielraum für die Vergabestellen eingeräumt wird und somit auch in Zukunft eine in der Praxis sehr unterschiedliche Handhabung zu erwarten ist. Bedauernswert ist zudem, dass dem Gesetzgeber bislang offenbar noch der Mut fehlt, innovative Ansätze zu verfolgen – denkbar wäre beispielsweise die Etablierung eines Public Venture Capitals im Unterschwellenbereich für unbürokratische, ergebnisoffene Innovationspartnerschaften zwischen Bundesbehörden und Start-Ups unter Anhebung der Direktauftragswertgrenzen[27].

2. Der Ausschluss von Bietern aus Drittstaaten – heiligt der Zweck die Mittel?

Dass es aus strategischen Erwägungen gewünscht sein kann, den Einfluss anderer Staaten auf eigene kritische Infrastrukturen zu begrenzen, veranschaulicht die Debatte um den Einsatz von Technik des Anbieters **Huawei** beim 5G-Ausbau in Deutschland.[28] Dieser wird maßgeblich von Unternehmen ausgeführt, welche keine öffentlichen Auftraggeber im Sinne des Vergaberechts sind. Bei der Untersagung der Nutzung von **Huawei**-Komponenten kam daher § 9b Abs. 4 BSI-Gesetz (BSIG)

25 Vgl. Freytag in: Osseforth, IT-Vergabe-HdB, 1. Aufl. 2022, § 10 Rn. 72-80.
26 BT-Drs. 20/14344, 92.

27 Vertiefend zu Direktauftragswertgrenzen BMWK, abrufbar hier (Stand 12.02.2025).
28 Vgl. Heiko Maas, Interview, ZEIT Nr. 51/2019 vom 04.12.2019, auszugsweise abrufbar hier (Stand: 13.02.2025); Pressemitteilung des BMI vom 11.07.2024, abrufbar hier (Stand: 13.02.2025).

zur Anwendung, wonach das Bundesministerium des Innern und für Heimat (BMI) den Einsatz einer kritischen Komponente gegenüber dem Betreiber der kritischen Infrastruktur bei Beeinträchtigung öffentlicher Sicherheitsinteressen untersagen kann.[29]

Dem Vergaberecht ist der Ausschluss eines Unternehmens allein aufgrund seiner Ansässigkeit grundsätzlich fremd – einem solchen Vorgehen steht der Gleichbehandlungsgrundsatz aus § 97 Abs. 2 GWB entgegen.[30] Eine Ungleichbehandlung wäre nur zulässig, wenn sie gesetzlich vorgesehen oder **„aus überwiegenden Gründen des Allgemeinwohls“**[31] geboten ist.

Eine derartige Ungleichbehandlung hat der Gesetzgeber erstmalig für Beschaffungen vorgesehen, die in den Anwendungsbereich des Bundeswehrbeschaffungsbeschleunigungsgesetzes (BwBBG) fallen. Nach § 7 Abs. 2 BwBBG dürfen Unternehmen von der Teilnahme an einem Vergabeverfahren ausgeschlossen werden, wenn der Bewerber oder Bieter in einem Staat außerhalb der EU ansässig ist und nicht die notwendige Gewähr für die Wahrung der Sicherheitsinteressen der Bundesrepublik Deutschland bietet. Der Anwendungsbereich des Gesetzes ist gem. § 2 S. 1 BwBBG auf Militärausrüstung sowie Bau- Instandhaltungsleistungen zur unmittelbaren Stärkung der Einsatzfähigkeit der Bundeswehr begrenzt und lässt sich nicht ohne Weiteres auf zivile Beschaffungen im IT-Umfeld anwenden.

Zweifelsfrei existieren in den Bundes- und Landesverwaltungen zahlreiche Anwendungsfälle, die ähnlich schutzbedürftig sind, ohne im engeren Sinne militärische Beschaffungen darzustellen. Dies verdeutlicht die aktuelle Stellungnahme des Bundesrats zum VergRTransfG-E: Dieser fordert die Aufnahme von Ergänzungsvorschlägen im Kontext der Beschaffung von Leistungen zur

29 Vgl. Meldung und FAQ des BMI, abrufbar hier (Stand: 13.02.2025).
30 Braun, in: Gabriel/Krohn/Neun, VergabeR-HdB, 4. Aufl. 2024, § 15 Rn. 13; VK Bund, Beschl. v. 12. 11. 2009 – VK 3-208/09, IBRRS 2009, 3926.
31 Weiner, in: Gabriel/Krohn/Neun, VergabeR-HdB, 4. Aufl. 2024, § 1 Rn. 52.

Härtung der Cyber- und Informationssicherheit entsprechend der Beschlusslage der Digitalministerkonferenz in das GWB und die VSVgV.[32] Nach den Beschlüssen der 2. Digitalministerkonferenz vom 18.01.2024 soll sich die Bundesregierung für Änderungen auf europäischer Ebene (Art. 346 AEUV, Richtlinie 2009/81/EG) einsetzen sowie national Änderungen im GWB vornehmen. Ziel ist die Schaffung von Ausnahmen für die Beschaffung von Cyber- und Informationssicherheitsleistungen oder alternativ die Integration in den Anwendungsbereich der Ausnahmen im Bereich Verteidigung und Sicherheit, um schnellere und rechtssichere Beschaffungen durchführen zu können.[33]

Es scheint nicht fernliegend, in diesem Kontext auch die Erweiterung bzw. Schaffung einer Vorschrift nach dem Vorbild des § 7 Abs. 2 BwBBG für Beschaffungen im Zusammenhang mit IT- und Cybersicherheitsleistungen zu prüfen. Durch eine Ausschlussmöglichkeit unzuverlässiger Anbieter aus Drittstaaten könnte ein Beitrag zur Stärkung der digitalen Souveränität in Deutschland und Europa geleistet werden, ohne den europäischen Binnenmarkt zu beeinträchtigen.

„Neben der rechtlichen Betrachtung darf die politische Dimension nicht vernachlässigt werden."

32 BT-Drs. 20/14518.
33 Beschluss zu TOP 9, abrufbar hier (Stand: 13.02.2025).

Eine unmittelbare Umsetzung der Vorschläge der Digitalministerkonferenz in nationales Recht lehnt die Bundesregierung aufgrund europarechtlicher Bedenken ab, will die Anpassung der EU-Vergaberichtlinien jedoch prüfen.[34] Es wäre wünschenswert, dass die künftige Bundesregierung die Vorschläge nach der Wahl aufnimmt und sich für eine Stärkung der digitalen Souveränität durch Anpassung des Vergaberechts auch auf europäischer Ebene einsetzt. Zumindest mit Frankreich dürfte man hier schnell einen Unterstützer finden – mit einer deutsch-französischen Kooperation in der digitalen Souveränität hat man hier bereits den richtigen Weg beschritten.[35]

Neben der rechtlichen Betrachtung darf allerdings auch die politische Dimension nicht vernachlässigt werden. So lassen die tarifären Maßnahmen der neuen Trump-Regierung in den USA eine harte Reaktion auf etwaige Beschränkungen des Zugangs zu europäischen Vergabeverfahren für US-Technologiekonzerne erwarten, China regierte bereits in der Vergangenheit verstimmt auf den 5G-Ausschluss von **Huawei**. Die Positionierung der künftigen Bundesregierung sowie der EU in der digitalen Souveränität wird mit Spannung zu verfolgen sein.

„Der Gesetzgeber ist angehalten, die Verwaltung durch die Schaffung verlässlicher Rechtsgrundlagen zur Umsetzung digitaler Souveränität zu befähigen."

34 BT-Drs. 20/14518, Gegenäußerung der Bundesregierung.
35 BMI, Pressemitteilung, abrufbar hier (Stand 13.02.2025).

D. Fazit

Digitale Souveränität ist keine rein akademische Diskussion, sondern als strategisches Ziel im politischen Raum klar formuliert. Mit dem Einsatz von OSS, der stärkeren Berücksichtigung von Start-Ups in öffentlichen Ausschreibungen sowie der Stärkung und Priorisierung des europäischen Markts können Lock-In-Effekte reduziert und perspektivisch vermieden werden. Die Bundesregierung unternimmt diesbezüglich bereits sichtbare Anstrengungen und in der Bundesverwaltung werden zweifelsfrei erste Erfolge erzielt. Dennoch liegt in der vergaberechtlichen Verankerung von digitaler Souveränität als legitimes Regelungsziel im nationalen Sicherheitsinteresse ein bislang nur zaghaft genutzter Hebel zur Stärkung der technologischen Resilienz und Unabhängigkeit der öffentlichen Verwaltung. Denn diese sollte letztlich nicht von der juristischen Kreativität und Risikobereitschaft einzelner Beschaffungsstellen abhängen – vielmehr ist der Gesetzgeber angehalten, die Verwaltung durch die Schaffung verlässlicher Rechtsgrundlagen zur Umsetzung digitaler Souveränität zu befähigen. Wissenschaft und Praxis haben zahlreiche gute und rechtlich fundierte Vorschläge erarbeitet – die neue Bundesregierung ist nun zur Handlung aufgerufen.

Zurück zum Inhaltsverzeichnis

AI
AI

KI-Agenten
Die neue juristische Arbeitsweise?

Christian Hartz

Open Peer Review

Dieser Beitrag wurde lektoriert von: Philipp Beckmann & Michelle Duda

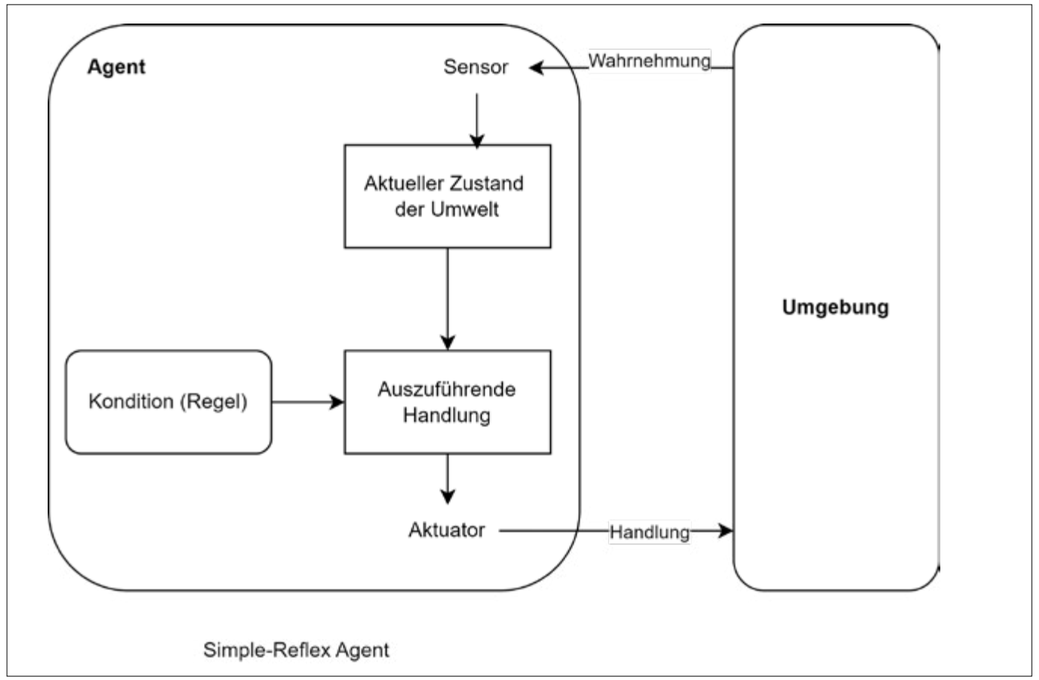
Christian Hartz ist Rechtsanwalt und Dozent im Bereich Strafrecht (Universität des Saarlandes) und Legal Tech (Universität zu Köln). Bei Wolters Kluwer, einem Anbieter von Fachinformationen, Software und Services im Bereich Recht, Wirtschaft und Steuern, ist er als Technology Implementation Manager und Legal Engineer im Team AI Strategy & Legal Engineering der Technologieorganisation Digital Experience Group */dxg tätig und unterstützt weltweit bei KI-Implementierungen. Global setzen bei Wolters Kluwer 4.500 Technologieexpert:innen gemeinsam mit den Zielgruppen- und Produktverantwortlichen neue Technologien wie beispielsweise die GPT-Zusammenfassungen auf Wolters Kluwer Online um.

(Autonome) KI-Agenten sind fortschrittliche Softwaresysteme, die komplexe Aufgaben eigenständig verarbeiten können. Sie nutzen häufig eine Kombination aus Tools und künstlicher Intelligenz (KI), lösen Aufgaben teilweise selbstständig und lernen kontinuierlich aus den generierten und eingegebenen Daten.

Nach **Russell/Norvig**[1] ist ein KI-Agent jedes System, welches durch Sensoren seine Umgebung wahrnehmen kann und mit dieser über einen Aktuator interagieren

1 Russel/Norvig, Artificial Intelligence, 4. Auflage 2021, S. 36.

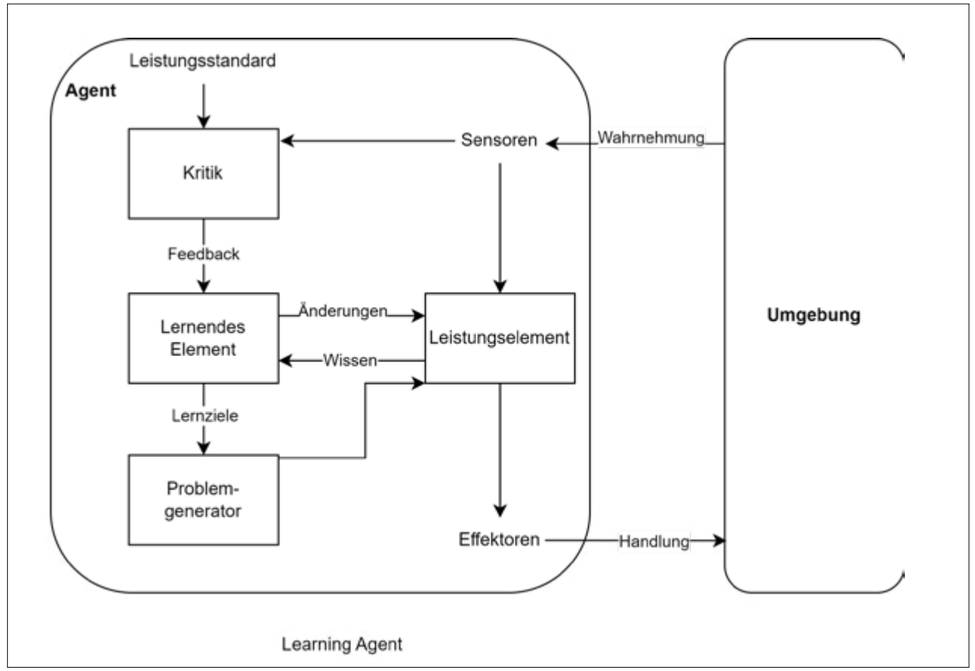
kann. Die einfachste Form eines Agenten ist der sogenannte Simple-Reflex-Agent, bei dem der Sensor die aktuelle Umgebung erfasst und basierend auf einer eingetretenen Bedingung eine Aktion ausführt.



Simple-Reflex Agent nach Russel/Norvig

Übertragen auf die Arbeit mit und an Texten könnte dies beispielsweise das Erkennen einer Fundstelle sein (zum Beispiel Hartz, CTRL 2/2022, 48), was hier dem Sensor entspricht, und das anschließende Normalisieren durch Mustererkennung (Autor: Hartz, Zeitschrift: CTRL, Jahr: 2022, Auflage: 2, Seite: 48), was als Bedingung bzw. Regel funktioniert. Diese Informationen würden dann möglicherweise als Metadaten in das Dokument zurückgeschrieben, was dem Aktuator entsprechen würde.

Komplexere Agenten können eigenständig lernen. Sie verfügen häufig über ein internes Feedback-System, das ihnen hilft, Ergebnisse zu reflektieren, aus ihnen zu lernen und ihre Fähigkeiten kontinuierlich zu verbessern, um ihre Nützlichkeit zu maximieren.



Learning Agent nach Russel/Norvig

Bei besonders komplexen Aufgaben arbeiten zahlreiche Sensoren und Effektoren zusammen, um eine Lösung zu finden. Beispielsweise nutzen autonom fahrende Fahrzeuge verschiedene Sensoren wie Abstandssensoren, Kameras und Geschwindigkeitssensoren, um die Umgebung präzise zu erfassen und anschließend über verschiedene Effektoren, etwa ein automatisches Bremssystem, entsprechende Aktionen auszuführen.

Ein Multi-Agenten-System ermöglicht es, mehrere Agenten entweder sequenziell (nacheinander) oder parallel arbeiten zu lassen. Durch eine gezielte Orchestrierung lassen sich Einzelaufgaben effizient zu einer übergreifenden Lösung zusammenfügen. Im juristischen Kontext kann das Erstellen eines juristischen Textes in verschiedene Aufgaben unterteilt werden, wie beispielsweise Recherche, Entwurf und Qualitätssicherung. Diese Teilaufgaben können von unterschiedlichen Agenten übernommen werden. Multi-Agenten-Systeme sind keine Zukunftstechnologie, sondern werden bereits heute in verschiedenen Anwendungen genutzt, oft im Hintergrund. So nutzt ChatGPT beispielsweise bei Deep-Research oder Suchfunktionen verschiedene Werkzeuge, wie eine Internetsuche oder die direkte Ausführung von Python-Code. Sprachmodelle spielen hierbei eine zentrale Rolle, insbesondere bei der Frage der Orchestrierung: Welches Tool soll wann eingesetzt werden?

A. Was sind Reasoning-Modelle und wie unterstützen sie KI-Agenten?

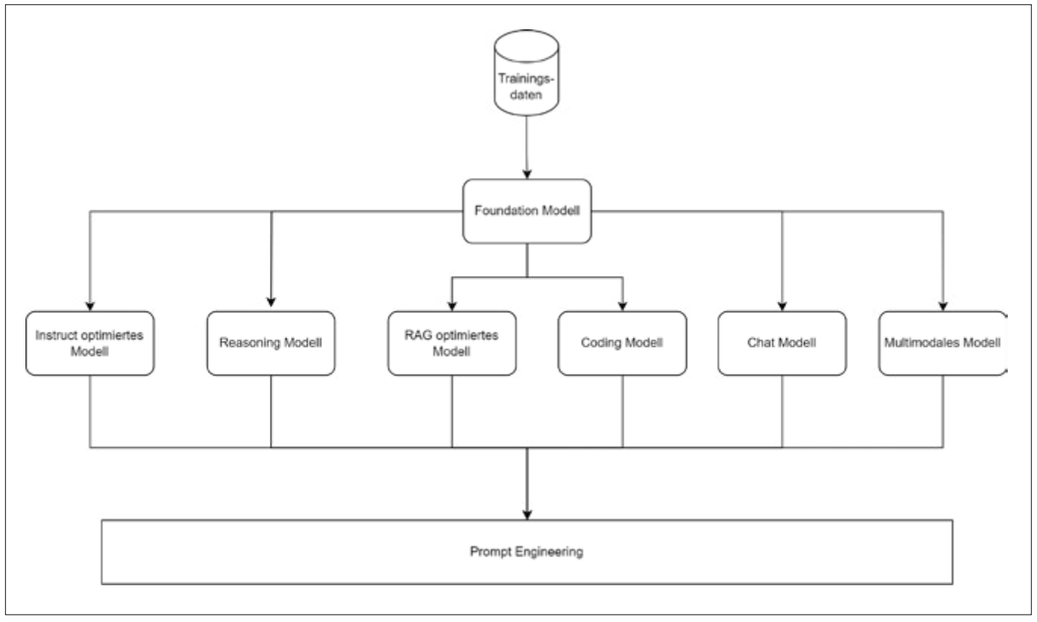
Seit dem Durchbruch von ChatGPT und dem Hype um Large-Language-Modelle (LLM) werden diese zunehmend für alltägliche Aufgaben eingesetzt. Sie spielen jedoch auch in Multi-Agenten-Systemen eine immer größere Rolle. Viele LLMs eignen sich nicht nur für die Ausführung einzelner Aufgaben, sondern können auch zur eigenständigen Planung genutzt werden, wodurch der Autonomiegrad der Agenten erheblich gesteigert wird.

Bei der Entwicklung eines Sprachmodells wird zunächst ein sogenanntes Foundation-Modell erstellt. Dieses Modell wird mit einer großen Menge an Texten trainiert und ist grundsätzlich in der Lage, Sprache zu verstehen. Würde man ein solches Modell jedoch direkt nutzen, entspräche das Ergebnis nicht den Erwartungen, die beispielsweise an ChatGPT gestellt werden. Daher werden diese Modelle in einem zweiten Schritt für spezifische Aufgaben optimiert, etwa für das Befolgen von Nutzeranweisungen (Instruktionen). Weitere Optimierungen können auf das Schreiben von Code, den Einsatz in Chatbots oder die Nutzung in RAG-Systemen abzielen.

Retrieval Augmented Generation (RAG) ist eine Technik, bei der das Sprachmodell nicht auf sein eigenes Wissen zurückgreift, sondern zuerst relevante Informationen sucht und diese dann zur Beantwortung der Frage nutzt.

Eine weitere Möglichkeit der Optimierung ist die Verbesserung des logischen Denkens und der Lösung komplexer Aufgaben, das sogenannte Reasoning. Reasoning-Modelle werden auf unterschiedliche Weise entwickelt. Grundsätzlich lassen sich zwei große Gruppen unterscheiden:

- (Instruct-)Modelle, die speziell instruiert oder gepromptet werden
- (Foundation-)Modelle, die gezielt für Reasoning optimiert werden



Vereinfachte Übersicht Sprachmodellvarianten

Oftmals werden auch hybride Ansätze verwendet, bei denen ein optimiertes Modell mit speziellem Prompting oder zusätzlichen Tools kombiniert wird.

Bekannte Reasoning-Modelle sind beispielsweise o1/o3 oder o3-mini von **OpenAI.** Auch andere Anbieter haben ähnliche Modelle entwickelt, darunter **DeepSeek** mit der R1-Modellfamilie, **Google** mit Gemini 2.0 Flash Thinking und **Moonshot AI** mit Kimi k1.5.

Sollte man also immer Reasoning-Modelle verwenden, weil sie genauere Ergebnisse liefern? Die kurze Antwort lautet: Nein. Der Einsatz macht lediglich in bestimmten Situationen Sinn. Gleichwohl können diese Modelle auch zusätzliche Herausforderungen mit sich bringen:

- Erhöhte Antwortzeit durch aufwendige Berechnungen
- Höhere Kosten im Vergleich zu Standardmodellen
- Spezifische Anforderungen an das Prompting
- Ausgabe zusätzlicher „think"-Tokens, die die Verarbeitung beeinflussen

I. Dauer der Antwort

Das „Nachdenken" eines Reasoning-Modells verlängert die Antwortzeit erheblich. Wenn zusätzlich externe Tools durch das Modell aufgerufen werden, kann die Bearbeitung mehrere Minuten dauern. Verglichen damit verarbeitet GPT-4o auch komplexe Prompts mit umfangreichen Rechtsprechungsdokumenten oft in weniger als 10 Sekunden. Aufgrund dieser Latenz sind Reasoning-Modelle für Anwendungen, die eine unmittelbare Interaktion erfordern – wie beispielsweise Chat-Funktionen –, weniger geeignet.

II. Kosten

Die Kosten für Reasoning-Modelle sind deutlich höher, da diese Modelle ihre eigenen Denkprozesse ebenfalls in Tokens ausdrücken. Auch wenn diese teilweise für Nutzende verborgen bleiben, entstehen dennoch Kosten für deren Erzeugung. Diese höheren Kosten werden durch entsprechend höhere Preise pro Token ausgeglichen.

Vergleicht man beispielsweise die Preise für **OpenAI** o1 und o3-mini mit denen von GPT-4o und GPT-4o-mini, ergeben sich folgende Unterschiede[2]:

Model-Name	Preis pro 1M Token Input	Preis pro 1M Token Output
OpenAI o1	15 $	60 $
OpenAI o3-mini	1,10 $	4,40 $
GPT-4o	2,50 $	10 $
GPT-4o-mini	0,15 $	0,60 $

Besonders bei wiederholenden Aufgaben kann es sinnvoll sein, das Reasoning-Modell für die initiale Planung oder zur Erstellung einer optimierten Prompt zu nutzen. Die eigentliche Ausführung kann dann auf kostengünstigere Modelle verlagert werden.

III. Prompt-Engineering für Reasoning-Modelle

Das Prompting von Reasoning-Modellen unterscheidet sich grundlegend von herkömmlichen Sprachmodellen. **Microsoft** empfiehlt in seinem Leitfaden zur Nutzung von o1 und o3-mini, direkt das Problem zu beschreiben, ohne Lösungswege vorzugeben.[3] Denn diese Modelle sind speziell für Reasoning-Vorgänge optimiert und entsprechend getestet.[4] Dies steht im Gegensatz zur üblichen Vorgehensweise

2 Quelle: OpenAI-Pricing-Website, (Stand 12.02.2025).
3 Mántaras im AI Azure Services Blog von Microsoft, hier einsehbar (Stand: 12.02.2025).
4 Vgl. etwa die Model-Card zu o3-mini, hier einsehbar (Stand: 12.02.2025).

beim Prompting normaler LLMs, bei denen strukturierte Hinweise oft hilfreich sind.

Zusätzlich lässt das o1-Modell keine System-Prompts zu, so dass sämtliche Informationen innerhalb des User-Prompts übermittelt werden müssen. Dies deutet darauf hin, dass **OpenAI** die Nutzereingaben interpretiert und systemseitig durch ergänzende Prompts erweitert. Eine zentrale Technik hierbei ist das sogenannte Chain-of-Thought Prompting[5], welches das Modell dazu anregt, systematisch über ein Problem nachzudenken. Inzwischen hat **OpenAI** die „Developer Message" eingeführt, die für Reasoning-Modelle als Äquivalent zur System Message fungiert.[6]

System-Prompt: Der System-Prompt oder System-Message enthält grundlegende Instruktionen für das Modell. Sie definiert den Rahmen der Interaktion, beispielsweise durch die häufig verwendete Vorgabe „You are a helpful AI Assistant"

User-Prompt: Der User-Prompt oder User-Message ist die direkte Eingabe der Nutzer:innen in der Oberfläche oder während einer Interaktion mit dem Sprachmodell, wie beispielsweise "Erstelle eine Zusammenfassung des folgenden Textes".

Developer-Prompt: Der Developer-Prompt oder Developer-Message ist eine speziell für Reasoning-Modelle eingeführte Variante der System-Prompt. Sie erlaubt Entwickler:innen spezifische Parameter für das Modell festzulegen und dessen Denkprozess gezielt zu steuern.

5 Wei u.a., Chain-of-Thought Prompting Elicits Reasoning in Large Language Models, hier einsehbar (Stand: 12.02.2025).
6 Siehe Microsoft, New features of o3-mini, hier einsehbar (Stand: 12.02.2025).

IV. Ausgabe der Reasoning-Modelle

Die Ausgabe von Reasoning-Modellen ähnelt grundsätzlich der Ausgabe herkömmlicher Algorithmen. Allerdings können diese Modelle zusätzlich ihre Gedankenschritte in Form von „think"-Tokens darstellen. Diese ermöglichen es, nachzuvollziehen, wie das Modell zu einem bestimmten Ergebnis gelangt ist. Die Darstellung dieser Token variiert je nach Modell: **DeepSeek** R1 bettet sie beispielsweise in XML-Tags ein und gibt sie vollständig aus. **OpenAI** hingegen hatte diese Gedankenschritte zunächst aus Wettbewerbsgründen nicht veröffentlicht, bietet nun jedoch eine zusammengefasste Version an.[7]

Unabhängig von diesen Unterschieden bleibt eines konstant: Sprachmodelle sind der zentrale Motor von KI-Agenten und ermöglichen deren leistungsfähige Automatisierung.

B. Large-Language-Modelle als Treibstoff der KI-Agenten

Workflowoptimierung und -automatisierung sind seit Langem essenzielle Werkzeuge zur Effizienzsteigerung in Arbeitsabläufen. Mit der Einführung von Sprachmodellen haben sich die Möglichkeiten in textlastigen Bereichen sowie in Anwendungen mit multimodalen Modellen erheblich erweitert. Anstatt umfangreiche Trainingsprozesse durchzuführen, können die meisten Modelle direkt „out-of-the-box" genutzt werden, um (Teil-)Aufgaben effizient zu bewältigen.

Dies gilt ebenso für KI-Agenten, die Workflows vollständig oder teilweise autonom durchlaufen können. Dank ihrer Fähigkeit, Informationen zu verarbeiten und Texte zu generieren, übernehmen sie eine zentrale Rolle im Automatisierungsprozess. Sie können Aufgaben initiieren, Ergebnisse überprüfen und durch gezielte Nachfragen iterativ optimieren.

7 Siehe hierzu mangels Erwähnung in den Release-Notes von o3-mini die Erwähnung in der Social Media-Präsenz von OpenAI auf der Plattform X, hier einsehbar (Stand: 12.02.2025).

Allerdings hängt die Qualität der Ergebnisse stark von den zugrunde liegenden Daten ab. Ein KI-Agent, der auf ungenaue oder fehlerhafte Daten zugreift, kann falsche oder irreführende Resultate liefern. Um Fehlerquellen wie Halluzinationen zu minimieren, benötigen Sprachmodelle nicht nur Zugang zu relevanten Informationen, sondern auch Daten mit hohen Qualitätsstandards. Dies ist insbesondere bei der Kombination interner und externer Datenquellen entscheidend, weshalb einheitliche Standards, wie sie in den **Common European Data Spaces** der **EU** angestrebt werden, von Vorteil sind.[8]

Da KI-Agenten große Mengen an Daten erzeugen und verarbeiten, müssen für jeden generierten Datensatz Metadaten konsistent hinterlegt werden und die Nutzbarkeit, Qualität, Fairness und der Datenschutz gewährleistet sein. Aufgrund der Komplexität und des Umfangs dieser Prozesse ist eine automatisierte Qualitätskontrolle unerlässlich. Ein Beispiel für ein solches System ist das **DataBri-X**-Projekt,[9] an dem auch **Wolters Kluwer** beteiligt ist, das sich mit der Entwicklung datengetriebener Qualitätsmechanismen befasst.

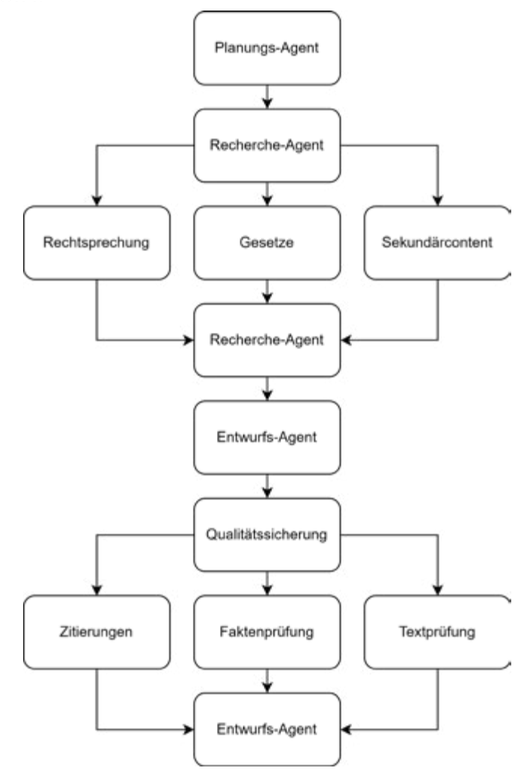
C. Anwendungsfälle für KI-Agenten im juristischen Umfeld

I. Entwerfen von juristischen Texten

Ein vielversprechender Anwendungsfall für den Einsatz von KI-Agenten ist das Entwerfen juristischer Texte. Hierbei geht es nicht nur um die reine Generierung eines Textes auf Basis eines Prompts, sondern auch um die gleichzeitige Analyse und Konsolidierung verschiedener relevanter Quellen. In einem solchen Szenario können spezialisierte Agenten von großem Nutzen sein – insbesondere, wenn sie in der Lage sind, eigenständig Unteragenten zu koordinieren und zu überwachen. Diese Agenten könnten folgendermaßen strukturiert sein:

- **Recherche-Agent**
  - » Rechtsprechung
  - » Gesetze
  - » Sekundärcontent
- **Entwurfs-Agent**
- **Qualitätssicherungs-Agent**
  - » Faktenprüfung
  - » Zitierungen
  - » Text

Der Ablauf eines solchen juristischen Multi-Agenten-Systems könnte folgendermaßen strukturiert sein:



8 Hier abrufbar (Stand: 12.02.2025).
9 Hier abrufbar (Stand: 12.02.2025).

Diese Darstellung fokussiert sich auf die einzelnen Aufgaben der Agenten und nicht darauf, welche spezifischen Tools jedem Agenten zur Verfügung stehen. Die genutzten Werkzeuge können von Agenten zu Agenten unterschiedlich sein. Beispielsweise könnte der Rechtsprechungs-Agent sowohl interne als auch externe Datenbanken durchsuchen, die relevanten Informationen aus diesen Quellen extrahieren, aufbereiten und zu einem kohärenten Gesamtergebnis zusammenführen.

Ein weiterer Vorteil dieses Systems ist die Möglichkeit, iterative Verbesserungen durchzuführen. Sollte der Qualitätssicherungs-Agent beispielsweise feststellen, dass wichtige Zitierungen fehlen, kann er den Recherche-Agenten erneut beauftragen, gezielt nach passenden Referenzen zu suchen. Dies verdeutlicht die Flexibilität des Systems: Während einige Prozesse, wie die Qualitätssicherung, parallel zur Recherche laufen können, erfordert der Übergang vom Entwurf zur finalen Qualitätsprüfung ein sequenzielles Vorgehen.

II. Überprüfung und Aufbereitung des Akteninhaltes

Ein zweiter relevanter Anwendungsfall ist die Überprüfung und strukturierte Aufbereitung von Akteninhalten. Je nach Umfang und Zeitpunkt der Datenübernahme kann dies eine komplexe Aufgabe sein, die sich nicht einfach durch einen einzelnen Prompt lösen lässt. Obwohl moderne Sprachmodelle über große Kontext-Fenster verfügen, stößt ihre Fähigkeit zur präzisen Informationssuche oft an Grenzen. Dies wird insbesondere im sogenannten „Needle-in-the-Haystack“-Problem deutlich: Wichtige Informationen, die sich tief in langen Dokumenten verbergen, werden nicht immer zuverlässig extrahiert.

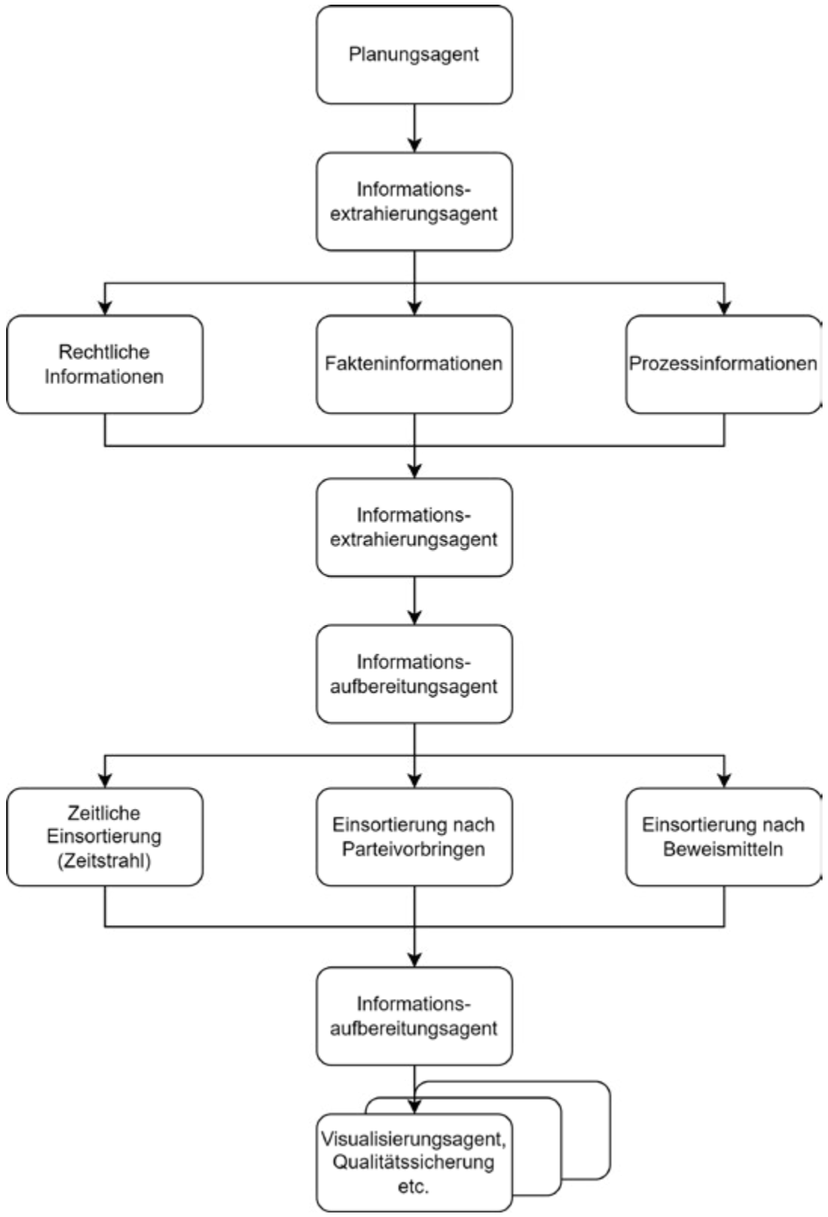
Unter optimalen Bedingungen sind LLMs mittlerweile durchaus in der Lage, solche Informationen zu identifizieren. In anspruchsvolleren Szenarien bestehen jedoch weiterhin Herausforderungen.[10]

Eine Möglichkeit zur Reduktion dieses Problems ist es, die einzelnen Dokumente zunächst getrennt aufzubereiten und dann die extrahierten Informationen als Ganzes zu verarbeiten.

Kontext-Fenster: Der Begriff Context-Window (auf Deutsch: Kontext-Fenster) bezeichnet die Anzahl der Token, die ein Sprachmodell gleichzeitig als Eingabe verarbeiten kann. Die Größe dieses Fensters variiert je nach Modell erheblich: Während ältere Modelle wie BERT mit einem kleinen Kontext-Fenster von nur 512 Token arbeiten, können moderne Modelle wie Gemini 1.5 Pro bis zu 2 Millionen Token gleichzeitig verarbeiten.

Token: Ein Token ist die kleinste Verarbeitungseinheit für ein Sprachmodell. Es kann ein ganzes Wort sein, aber auch nur ein Wortbestandteil. Zum Beispiel wird „Haus“ als ein Token gezählt, während „Hausbau“ in zwei Token – „Haus“ und „Bau“ – aufgeteilt wird. Generell kann man von einem ungefähren Verhältnis von 4:3 zwischen Token und Wörtern ausgehen, was bedeutet, dass 1000 Token etwa 750 Wörtern entsprechen.>

10 Siehe etwa Modaressi u.a., NoLiMa: Long-Context Evaluation Beyond Literal Matching, S. 5, hier einsehbar (Stand: 12.02.2025)..



Darstellung eines Akten-Agenten

Der zentrale Planungsassistent übernimmt neben der reinen Planung, welcher Agent verwendet wird, auch die Aufgabe, grundlegende Informationen bereitzustellen, die entweder aus einer direkten Nutzereingabe stammen oder aus bestehenden Datenquellen extrahiert werden. Dazu gehören essenzielle Angaben wie die vertretene Partei, das Ziel des Falls und andere relevante Rahmenbedingungen.

Der Extrahierungsagent arbeitet mit spezialisierten Sub-Agenten zusammen, die auf bestimmte Aufgaben fokussiert sind. Ein einfacher Ansatz wäre die Nutzung von Prompts, die alle relevanten Dokumente durchsuchen und relevante Informationen in Textform extrahieren. Eine erweiterte Methode besteht darin, diese Daten direkt als strukturierte Informationen zu speichern – etwa in RDF (Resource Description Framework), Property-Graphen wie **Neo4j** oder einem umfassenden Wissensgraphen.

Die extrahierten Informationen liegen zunächst in isolierter Form vor, da sie aus verschiedenen Dokumenten stammen. Im nächsten Schritt müssen sie daher systematisch gebündelt und aufbereitet werden, um eine ganzheitliche Analyse zu ermöglichen.

Darüber hinaus können weitere spezialisierte Agenten eingebunden werden. Dies umfasst unter anderem Qualitätssicherungs-Agenten, die die Genauigkeit der Informationen überprüfen, sowie Visualisierungs-Agenten, die die Daten in Form von Charts, Zeitstrahlen oder Tabellen aufbereiten. Diese beiden Beispiele verdeutlichen, wie durch die geschickte Kombination von Tools, Sprachmodellen und einer strukturierten Workflow-Integration KI-Agenten die juristische Arbeit effizienter gestalten können. Die Multimodalität, die eine Interaktion nicht nur über Text, sondern auch über Sprache und Bilder ermöglicht, eröffnet neue Möglichkeiten zur Automatisierung und Optimierung. In Kanzleien und Unternehmen kann dies dazu beitragen, die oft langwierige Digitalisierung von Akten mit einem sofort erkennbaren Mehrwert zu verbinden, wodurch die Akzeptanz für solche Technologien erheblich gesteigert

wird. Auch für die Justiz werden Multi-Agenten-Systeme vorgeschlagen.[11] Allerdings dürfen bei dieser technischen Betrachtung die essentiellen datenschutz- und berufsrechtlichen Anforderungen sowie regulatorische, ethische und gesellschaftliche Aspekte nicht außer Acht gelassen werden. Der Einsatz und die Entwicklung von KI-Agenten müssen sich in einem klaren rechtlichen und ethischen Rahmen bewegen, um Missbrauch und ungewollte Konsequenzen zu vermeiden. Diese wichtigen Fragestellungen sind integraler Bestandteil der weiteren Diskussion, werden in diesem Beitrag jedoch nicht behandelt.

D. (Aktuelle?) Grenzen der KI-Agenten

Obwohl KI-Agenten zahlreiche Einsatzmöglichkeiten bieten, haben sie auch ihre Grenzen. Einige dieser Limitationen könnten zukünftig überwunden werden, während andere alternative Ansätze erfordern.

I. Technische Herausforderungen

Insbesondere stoßen die zugrunde liegenden Sprachmodelle, die einen Großteil der Aufgaben übernehmen, an ihre Grenzen. Trotz der in den vergangenen Jahren deutlich gestiegenen Qualität der Antworten von LLM-Systemen sind diese nicht immer korrekt – wie Linklaters anmerkt: „They are still not always right and lack nuance".[12]

Ein möglicher Lösungsansatz zur Verringerung von Halluzinationen und Falschinformationen ist der Einsatz von Wissensgraphen. Insbesondere im medizinischen Bereich konnten Agenten mit Wissensgraphen gegenüber klassischen LLMs – selbst bei Einsatz von Chain-of-Thought-Prompting – Verbesserungen erzielen.[13]

11 Vgl. nur Jiang/Yang, Agents on the Bench: Large Language Model Based Multi Agent Framework for Trustworthy Digital Justice, hier einsehbar (Stand: 12.02.2025)..
12 Linklaters, The LinksAI English law benchmark – Version 2, February 2025, S. 3, hier einsehbar (Stand: 12.02.2025).
13 Vgl. dazu beispielsweise Su u.a., Knowledge Graph Based Agent for Complex Knowledge-Intensive QA in Medicine, S. 7, hier einsehbar (Zugriff: 12.02.2025).

Wissensgraphen (Knowledge Graphs) ermöglichen die Darstellung komplexer semantischer Zusammenhänge in einer für Maschinen lesbaren Form. Im Regelfall bestehen sie aus einer Vielzahl an Entitäten (beispielsweise ein Begriff wie Strafrecht und Diebstahl) und kombinieren diese mit deren Eigenschaften (beispielsweise Tatbestand) und der Beziehung zwischen ihnen (Diebstahl ist ein Tatbestand im Strafrecht). Ein Beispiel für die Verwendung eines Wissensgraphen ist **Wikidata**, welches auch einen Query Builder anbietet, um den Graphen einfach abzufragen.[1]

1 S. Wikidata Query Builder, hier einsehbar (Stand: 12.02.2025).

II. Qualitätssicherung und weitere Herausforderungen

Aufgrund der Halluzinationen, wie auch in einer **Stanford**-Studie aufgezeigt[14], verschiebt sich der Aufwand zunehmend vom reinen Verfassen hin zur Qualitätssicherung. Darüber hinaus bestehen weitere Probleme:

- Fehlende Transparenz und Erklärbarkeit der durch Black-Box-Algorithmen generierten Antworten und der zugrundeliegenden Prozesse
- Verzerrungen in den Daten, die sich in den Ergebnissen widerspiegeln
- Mangelnde Berücksichtigung der Individualität juristischer Fälle
- Fehlauswahl von Tools durch den Agenten

Die Problematik der Black-Box-Algorithmen ließe sich etwa dadurch adressieren, dass der Denkprozess, der Einsatz der verschiedenen Tools, deren Ein- und Ausgaben sowie – bei Bedarf – die verwendeten Quellen offengelegt werden.

14 Magesh u.a., Hallucination-Free? Assessing the Reliability of Leading AI Legal Research Tools, hier einsehbar (Stand: 12.02.2025).

Bias und Diskriminierung sind ernstzunehmende Herausforderungen im Umgang mit juristischen Informationen.[15] Juristische Daten können beispielsweise unterrepräsentierte Informationen (viele obergerichtliche vs. wenige untergerichtliche Entscheidungen) oder veraltete Daten enthalten, die ein verzerrtes Bild der aktuellen Normen vermitteln. Zudem führt die statistische Arbeitsweise der Sprachmodelle dazu, dass häufigere Lösungen überproportional oft als Antwort erscheinen. Um dies zu verhindern, folgt **Wolters Kluwer** bei der Entwicklung KI-gestützter Lösungen den selbst auferlegten strengen AI-Principles.[16]

Schließlich besteht die Gefahr, dass ein überwiegend autonom agierender Agent die falschen Werkzeuge auswählt und dadurch fehlerhafte Ergebnisse erzeugt. Um dies zu vermeiden, sollte der Autonomiegrad der KI-Agenten so gewählt werden, dass sie die gewünschten Resultate zuverlässig liefern.

E. Wie autonom sollten KI-Agenten sein?

Mit dem Fortschritt von Reasoning- und Sprachmodellen könnte der Grad der Autonomie von KI-Agenten weiter steigen. Insbesondere im juristischen Umfeld und angesichts des noch frühen Entwicklungsstadiums empfiehlt es sich jedoch, die Agenten engmaschig zu kontrollieren und spezifische Workflows zu definieren. Dies erleichtert die Überprüfung und stellt sicher, dass die (berufs-)rechtlichen Anforderungen an den KI-Einsatz erfüllt werden.

Um die Ergebnisqualität zu gewährleisten, gilt – ganz nach dem möglicherweise Galilei zugeschriebenen Motto[17] –: „Messen, was messbar ist“.

15 Ausführlich zu den Arten von Bias s. etwa: Sargeant/Magnusson, Bias in Legal Data for Generative AI, Generative AI and Law, 2024.
16 Wolters Kluwer, AI Principles, hier einsehbar (Stand: 12.02.2025).
17 Vgl. dazu Kleinert, Berichte zur Wissenschaftsgeschichte, Vol. 11, (1988), 253 f.

F. Fazit

KI-Agenten können als autonome und lernfähige Systeme einen zentralen Beitrag zur Optimierung komplexer Arbeitsabläufe und juristische Prozesse leisten – sei es durch die automatische Erfassung und Bearbeitung von Daten, die Koordination mehrerer spezialisierter Agenten oder den Einsatz von Reasoning-Modellen für präzisere Planung und Qualitätssicherung. Vielleicht schaffen sie es sogar, die von mehr als einem Drittel der Mitarbeitenden in Kanzleien und Rechtsabteilungen in der aktuellen Future Ready Lawyer Studie von **Wolters Kluwer** als Herausforderung eingestufte Integration in bestehende Systeme zu meistern.[18]

Trotz bestehender Herausforderungen wie technischer Limitationen, erhöhter Kosten und rechtlicher Fragestellungen, bietet die kontinuierliche Weiterentwicklung dieser Technologien enorme Chancen.

Mit einem verantwortungsvollen Einsatz können KI-Agenten nicht nur bestehende Prozesse effizienter gestalten, sondern auch den Weg für innovative, zukunftsweisende Anwendungen im juristischen Alltag ebnen.

Zurück zum Inhaltsverzeichnis

18 Wolters Kluwer, Future Ready Lawyer Studie 2024, S. 7, hier einsehbar (Stand: 12.02.2025)..

Impressum

Chefredaktion
Philipp Beckmann, Michelle Duda, Julia Keselj, Julia Melles,
Ramon Schmitt, Ferdinand Wegener, Larissa Schmitz, Isabel Ecker.

Front- und Backccover:

Herausgeber
CTRL Media UG (haftungsbeschränkt)
Meister-Gerhard-Straße 5
50674 Köln
Registergericht: Amtsgericht Köln unter HRB 116148

Geschäftsführer: Ferdinand Wegener

E-Mail: ctrlmagazin@gmail.com

Die in den Beiträgen vertretenen Ansichten sind Ausdruck der persönlichen Überzeugungen der jeweiligen Autorin oder des jeweiligen Autors. Sie geben weder die Auffassung der Redaktion noch der CTRL Media UG (haftungsbeschränkt) wieder.

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 ctrlmagazin@gmail.com oder über das Kontaktformular auf ctrl-magazin.de schicken.

Die Inhalte dieser Publikation unterliegen dem deutschen Urheberrecht. Die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung außerhalb der Grenzen des Urheberrechts bedürfen der schriftlichen Zustimmung der CTRL Media UG (haftungsbeschränkt). Downloads und Kopien dieser Publikation sind nur für den privaten, nicht kommerziellen Gebrauch gestattet. Soweit die Inhalte dieser Publikation nicht von dem jeweiligen Autor erstellt wurden, werden die Urheberrechte Dritter beachtet. Insbesondere werden Inhalte Dritter als solche gekennzeichnet. Sollten Sie trotzdem auf eine Urheberrechtsverletzung aufmerksam werden, bitten wir um einen entsprechenden Hinweis. Bei Bekanntwerden von Rechtsverletzungen werden wir derartige Inhalte umgehend entfernen.

ctrl-magazin.de

Contemporary Technology
Review & Law