Schriften der Jungen Wissenschaft im Öffentlichen Recht

JuWissDay 2024 Speyer

Rechtsfragen virtueller Welten

Nomos

Schriften der Jungen Wissenschaft im Öffentlichen Recht

JuWissDay 2024 Speyer

Rechtsfragen virtueller Welten

Mit Beiträgen von:

Dr. Alexander Brade | Jun.-Prof. Dr. Jennifer Grafe | Daniel Hauck | Prof. Dr. Simon J. Heetkamp | Franziskus Horn | Dr. Luise Lautenbach | Dr. Martin Meier | Armin Mozaffari Jovein | Prof. Dr. Peter Parycek | Maximilian Petras | Nitharshini Santhakumar | Dr. David M. Schneeberger | Nicolas Ziegler | Jaouhara Zouagui

Herausgegeben von:

Dr. Jonas Botta | Martin Feldhaus | Dr. Katharina Goldberg | Dr. Sarah Hartmann Carolin Kemper | Dr. Luise Lautenbach | Nik Roeingh

Nomos

Zitiervorschlag: Autor:in, in: Botta et al. (Hrsg.), Rechtsfragen virtueller Welten, Baden-Baden 2025, S. ...

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

1. Auflage 2025

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-7560-2260-1
ISBN (ePDF): 978-3-7489-4912-1

DOI: https://doi.org/10.5771/9783748949121

Onlineversion
Nomos eLibrary

Vorwort

Virtuelle Welten waren noch vor wenigen Jahren klassischer Science-Fiction-Stoff, etwa für die „Matrix"-Trilogie der Wachowski-Schwestern oder Steven Spielbergs „Ready Player One". Moderne Technologien lassen es aber immer wahrscheinlicher werden, dass aus dieser Vision bereits in den nächsten Jahr(zehnt)en digitale Realität wird. Virtuelle Welten gelten mittlerweile als „The Next Big Thing". Sie beschäftigen längst nicht mehr nur die Führungsriegen globaler IT-Giganten, sondern die gesamte Gesellschaft – und auch bereits die Gesetzgeber auf nationaler und unionaler Ebene. Das „Internet von morgen" soll und wird – so die häufig verkündete Prophezeiung – unser aller Verhältnis zum digitalen Raum revolutionieren, indem es physische, erweiterte und virtuelle Realität miteinander verschmilzt.

Dass virtuelle Welten in der Rechtswissenschaft gleichwohl noch wenig Beachtung gefunden haben, verwundert nicht.[1] Schließlich eilt ihr allgemein der Ruf voraus, dem technologischen Fortschritt bestenfalls verhalten, schlimmstenfalls sogar ablehnend gegenüberzustehen. Dennoch finden sich im virtuellen Raum auch juristische Pionierinnen und Pioniere. So führte die kolumbianische Verwaltungsrichterin María Victoria Quiñones Triana am 15. Februar 2023, fast 20 Jahre nach dem Kinostart des dritten Matrix-Films, weltweit eine der ersten Gerichtsverhandlungen im sog. Metaversum durch.[2] Die Prozessbeteiligten „erschienen" also nicht physisch in einem Gerichtssaal, sondern trugen Virtual-Reality-Brillen und trafen sich als Avatare rein virtuell. Die Öffentlichkeit wurde dadurch hergestellt, dass Interessierte die Verhandlung via Livestream verfolgen konnten. Eine Gerichtsverhandlung mit Vorbildcharakter? Zumindest in Deutschland wäre das gegenwärtig noch ausgeschlossen (womit sich der erwähnte Ruf der technikaversen Jurisprudenz weiter verfestigen mag). Zwar sehen alle Prozessordnungen schon länger die Möglichkeit vor, Videoverhandlungen

1 Siehe zu den bislang wenigen Ausnahmen insbesondere H. Steege/K. J. Chibanguza (Hrsg.), Metaverse, Baden-Baden 2023; *M. Kaulartz/A. Schmid/F. Müller-Eising*, Das Metaverse – eine rechtliche Einführung, RDi 2022, 521 ff.; *M. Martini/J. Botta*, Der Staat und das Metaversum, MMR 2023, 887 ff.; E. Wagner/M. Holm-Hadulla/M. Ruttloff (Hrsg.), Metaverse und Recht, München 2023.

2 Online nachzusehen unter: https://web.archive.org/web/20240409034416/https://www.youtube.com/watch?v=LXi2TX9OBmQ.

durchzuführen. Aber die komplette Verlagerung in einen rein virtuellen Gerichtssaal erlauben Vorschriften wie § 102a VwGO oder § 128a ZPO (auch nach ihrer jüngsten Reform) noch nicht. Gleichwohl sind virtuelle Welten auch hierzulande kein „Nischenthema" mehr, sondern längst in aller Munde.

Die prognostizierte Veränderung des Internets mag sich zum jetzigen Zeitpunkt noch nicht hinreichend klar abzeichnen. Virtuelle Welten sind (gegenwärtig) kein feststehender Sachverhalt, sondern wirken vielfach wie „Zukunftsmusik" – ähnliches wurde in den vergangenen 30 Jahren jedoch auch anderen, mittlerweile selbstverständlich etablierten, regulierten und rechtswissenschaftlich erforschten digitalen Infrastrukturen, Endgeräten und Plattformen entgegengehalten. Als Mitte der 1990er-Jahre die damals noch unbekannten Unternehmen Amazon und ebay auf den sehr jungen Online-Markt traten, zweifelten selbst prominente IT-Experten zunächst an der Bedeutung und Zukunftsfähigkeit des Internets. Zugleich begann mit der Veröffentlichung des Kommissionsentwurfs zur Richtlinie über den elektronischen Geschäftsverkehr bereits im Jahr 1998 der Versuch der Europäischen Gemeinschaft, die sich erst grob abzeichnende Entwicklung digitaler Geschäftsmodelle im Recht abzubilden bzw. regulatorisch zu begleiten. Noch im Jahr 2001, ein Jahr nach Inkrafttreten der Richtlinie, nutzten weniger als 40 % der in Deutschland lebenden Menschen überhaupt das Internet. Sollten sich virtuelle Welten nur ansatzweise ähnlich rasant und nachhaltig etablieren, ist es dringend geboten, die bereits absehbaren oder fundiert zu erwartenden Chancen und Potentiale, aber auch den Umgang mit Risiken, frühzeitig zu diskutieren. Um die daraus erwachsenden Rechtsfragen rechtzeitig beantworten zu können, braucht es ebenfalls juristischen Pioniergeist.

Unter dem Titel „Rechtsfragen virtueller Welten" fand daher am 27. und 28. September 2024 der JuWissDay 2024 beim Deutschen Forschungsinstitut für öffentliche Verwaltung (FÖV) in Speyer statt. Die dort vorgetragenen und hier veröffentlichten Beiträge beleuchten, was sich hinter dem Hype um das Metaversum (oder auch Web3, Web 4.0 etc. genannt) konkret verbirgt, welche Akteure es gestalten, und vor allem auch welche realen Rechtsfragen bzw. regulatorischen Aufgaben und Herausforderungen (künftige) virtuelle Welten für Staat und Gesellschaft aufwerfen. Dabei kamen nicht nur alle drei juristischen Fachsäulen zusammen, sondern die Tagung konnte auch von einem Austausch mit der Praxis profitieren. Der vorliegende Tagungsband skizziert somit eine große Auswahl relevanter Aspekte künftiger virtueller Welten.

Ein besonderer Dank gilt den beiden Keynote-Speakern Herrn Prof. Dr. Simon Heetkamp, LL.M. und Herrn Prof. Dr. Matthias C. Kettemann, LL.M. (Harvard) für ihre gewinnbringenden Forschungseinblicke. Das Tagungsteam dankt außerdem dem Deutschen Forschungsinstitut für öffentliche Verwaltung, dem Verein Junge Wissenschaft im Öffentlichen Recht, dem Verlag C. H. Beck, dem Kohlhammer Verlag, der Kanzlei Rittershaus und der Kanzlei Spirit Legal für die großzügige Unterstützung des JuWiss-Day sowie dem Nomos Verlag, namentlich Herrn Dr. Marco Ganzhorn, zusätzlich zur finanziellen Förderung für die Veröffentlichung und hervorragende Betreuung des Tagungsbandes.

Jonas Botta, Martin Feldhaus, Katharina Goldberg, Sarah Hartmann, Carolin Kemper, Luise Lautenbach und Nik Roeingh

Inhaltsverzeichnis

Virtual Reality in der Justizpraxis

Simon J. Heetkamp

A. Einleitung

Virtual Reality-Anwendungen finden zunehmend Einzug in das tägliche Leben der Menschen. Sowohl die Hardware als auch die Software werden dabei kontinuierlich leistungsfähiger. Die neueste Generation von VR-Headsets kann fast lebensechte Bilder darstellen und zum Teil auch für Augmented Reality- oder Mixed Reality-Anwendungen genutzt werden. Ein Beispiel für die Fortschritte in dieser Technologie zeigt das Interview des Informatikers, Podcasters und YouTubers Michael Fridman mit Meta-Chef Zuckerberg, das nach der entsprechenden Eigenwerbung das erste Interview im „Metaverse" sein soll.[1] Obwohl die beiden in der realen Welt Hunderte Kilometer voneinander entfernt sind, sprechen in dem Interview ihre fotorealistischen Avatare, die dank neuester Codec-Technologie fast nicht von echten Menschen zu unterscheiden sind.

B. VR-Anwendungen in der Justizpraxis

I. Die „Polizisten-Morde" von Kusel

Das (soweit bekannt) erste Mal, dass ein Richter in einem deutschen Gerichtssaal eine VR-Brille trug, war im Rahmen des Strafverfahrens wegen der sog. Polizisten-Morde von Kusel vor dem Landgericht Kaiserslautern im Juli 2022. Der Vorsitzende Richter nahm dabei per VR-Brille den Tatort in Augenschein, den zuvor das LKA Rheinland-Pfalz und das BKA per Laserscanner virtualisiert hatten.[2] Was war passiert? Bei einer Verkehrskon-

1 Siehe das entsprechende Interview unter: https://www.youtube.com/watch?v=MVYrJJNdrEg.

2 Siehe entsprechende Presseberichte: https://www.swr.de/swraktuell/rheinland-pfalz/anwalt-nebenklage-im-kusel-prozess-100.html und https://www.bild.de/regional/saarland/saarland-news/polizisten-morde-von-kusel-richter-mit-vr-brille-am-virtuellen-tatort-80631568.bild.html.

trolle stoppten eine junge Polizistin und ein junger Polizist zwei Männer, die illegal geschossenes Wild in ihrem Fahrzeug transportieren. Um ihre Wilderei zu verdecken, eröffnete der Haupttäter daraufhin das Feuer auf die Polizist:innen und tötete sie. Im Gerichtssaal hatten nunmehr die Anwesenden die Möglichkeit, den virtuellen Rundgang des Vorsitzenden über den Tatort über große Leinwände mitzuverfolgen. Der Vorsitzende durchschritt virtuell den Tatort, wobei sowohl die Leichen der Polizistin und des Polizisten erkennbar sind. Die virtuelle Tatortbegehung dauerte über eine Stunde. Auch die Verteidigung und die Vertreter der Nebenklage können den Vorsitzenden bitten, bestimmte Blickrichtungen und Positionen einzunehmen; sie selbst tragen allerdings keine VR-Brillen. Der Vorsitzende Mall wurde später in der Presse in Bezug auf den VR-Einsatz mit den Worten „Das ist Wahnsinn." zitiert.[3] Auch ein Vertreter der Nebenklage, Rechtsanwalt Kai-Daniel Weil, lobte öffentlich die zusätzlichen Erkenntnisse, die durch die VR-Darstellung gewonnen wurden.[4] Dabei ist zum einen anzumerken, dass der virtuelle Tatort zusätzlich zu 272 Lichtbildern des Tatorts und einer Positionsbestimmung der Asservate per GPS erfolgt. Eine wichtige Besonderheit: In den Laserscan des Tatorts wurde das Täterfahrzeug nachträglich eingefügt.[5]

II. Das Strafverfahren gegen Reinhold Hanning

Auch in einem weiteren Strafprozess in Deutschland wurde Virtual Reality eingesetzt. 2016 stand der damals 94-jährige Reinhold Hanning vor dem Landgericht Detmold. Hanning war während der Nazizeit als Aufseher im KZ Auschwitz-Birkenau tätig. Die Staatsanwaltschaft warf ihm vor, durch seine Wachtätigkeit in 170.000 Fällen Beihilfe zum Mord geleistet zu haben. Hanning argumentierte unter anderem, dass er nur auf den Wachtürmen und außerhalb des Lagers im Einsatz gewesen sei und nicht gewusst habe, was im Inneren des Lagers geschah. Das Bayerische Landeskriminalamt

3 Siehe entsprechende Presseberichte: https://www.swr.de/swraktuell/rheinland-pfalz/anwalt-nebenklage-im-kusel-prozess-100.html und https://www.bild.de/regional/saarland/saarland-news/polizisten-morde-von-kusel-richter-mit-vr-brille-am-virtuellen-tatort-80631568.bild.html.

4 Siehe entsprechendes Interview im SWR unter: https://www.swr.de/swraktuell/rheinland-pfalz/anwalt-nebenklage-im-kusel-prozess-100.html.

5 Siehe entsprechende Ausführungen im Urteil des Landgerichts Kaiserslautern vom 30. November 2022 – 4 Ks 6035 Js 2146/22.

wurde eingeschaltet und erstellte basierend auf Bauplänen und Laserscans vor Ort ein VR-Modell, um zu demonstrieren, was von den Wachtürmen aus gesehen werden konnte.[6]

Allerdings wurde dieses VR-Modell während der Hauptverhandlung nicht mit VR-Brillen betrachtet, sondern über Beamer und Leinwand gezeigt, entgegen der Darstellung in einer Zeitung.[7] Die Visualisierung ähnelte einem Drohnenflug durch das Lager Auschwitz. Die VR-Datei wurde von einem Sachverständigen über einen Computer und mit einem handelsüblichen Mediaplayer abgespielt und dem Gericht erläutert. Das Gericht verurteilte Hanning zu fünf Jahren Haft wegen Beihilfe zum Mord in mindestens 170.000 Fällen. Allerdings wurde das Urteil nie rechtskräftig, da Hannings Anwalt Revision einlegte. Hanning verstarb im Mai 2017 im Alter von 95 Jahren, wodurch das Verfahren gemäß § 206a StPO beendet wurde und das Urteil des LG Detmold (Az. 4 Ks 45 Js 3/13–9/15) somit gegenstandslos war.

III. Der Raser von Wiesbaden

Ein weiterer Anwendungsfall von VR-Technologie fand in Wiesbaden statt. Dort kam es – wie in den letzten Jahren so häufig – zu einem weiteren Raserfall mit tödlichem Unfallgeschehen.[8] Bei der entsprechenden Tatrekonstruktion wurden 360°-Kameras in den Fahrzeugen und an der Position eines Zeugen positioniert. Die entsprechenden Videos aus den Unfallfahrzeugen wurden durch die Hochschule für öffentliches Management und Sicherheit (HöMS) bearbeitet. Ziel war es, die Bewegungen der Fahrzeuge und den Ablauf des Unfalls genau nachzustellen, um zu klären, was aus den jeweiligen Blickwinkeln sichtbar war. Die Rekonstruktion fand am 20.01.2023 am Unfallort statt, wobei Fahrzeuge gleichen Typs wie die unfallbeteiligten Fahrzeuge verwendet wurden, die mit Kameratechnik ausgestattet waren. Außerdem wurde eine statische Kamera an der Position eines Zeugen (Fußgängerin) aufgestellt. Es kam die VR 360°-Aufnahmetechnik zum Einsatz. Die dabei entstandenen Rohdaten wurden an der HöMS bearbeitet, jedoch ohne inhaltliche Änderungen am Bild vorzunehmen.

---

6 Siehe entsprechende Darstellungen der polizeilichen Arbeit in der Kurz-Doku „Nazi VR", online abrufbar unter: https://davidfreid.com/portfolio/nazi-vr.

7 In einer entsprechenden Darstellung der Zeitung „Krone" trägt die Vorsitzende eine VR-Brille, siehe https://www.krone.at/604704.

8 Siehe entsprechenden Bericht unter: https://www.hessenschau.de/panorama/mord-ermittlungen-polizei-stellt-raser-unfall-nach,video-178392.html.

Die erstellten 360°-Videos wurden zunächst als Standard-Videos mit dem VLC Media Player während der Hauptverhandlung mehrfach abgespielt und begutachtet. Die HöMS hatte darüber hinaus auch Vergleichsaufnahmen (Verkehrsüberwachung vs. Unfallrekonstruktion) als Standard-Videos aufbereitet.

Die Betrachtung der Videos erfolgte im Rahmen der Befragung des Mitarbeiters der HöMS, der die Rekonstruktion leitete und erklärte, welche Technik eingesetzt wurde und wie die Vergleichsvideos erstellt wurden. Anschließend setzte der Zeuge eine VR-Brille auf, die mit einem Laptop verbunden war, auf dem die notwendige Software installiert war. Der Laptop war wiederum an die im Sitzungssaal vorhandenen Beamer angeschlossen, sodass alle Anwesenden gleichzeitig das sehen konnten, was der Zeuge durch die VR-Brille sah. Der Zeuge wurde gebeten, verschiedene Perspektiven (Angeklagter, Opfer, Fußgängerin) in unterschiedlichen Geschwindigkeiten (die Rekonstruktion erfolgte zunächst bei 70 km/h, wurde aber auch so bearbeitet, dass eine Geschwindigkeit von 140 km/h simuliert wurde) abzuspielen. Zudem drehte der Zeuge den Kopf nach links und rechts, um das Sichtfeld der Fahrerpositionen zu verdeutlichen. Diese Aufnahmen wurden als Augenscheinsobjekte zur Beweisaufnahme herangezogen. Im Urteil wurde beschrieben, was auf den Videoaufzeichnungen zu sehen war.

IV. Einsatz von VR auf internationaler Ebene

Auch international findet VR-Technologie Anwendung in strafrechtlichen Ermittlungs- und Gerichtsverfahren. In Schweden werden beispielsweise Tatortbegehungen mit 360°-Panoramen durchgeführt. In der Schweiz ist der regelmäßige Einsatz von VR zur Rekonstruktion von Tatorten bei strafrechtlichen Ermittlungen und Gerichtsverfahren dokumentiert, begleitet sowohl von der Tagespresse als auch von Fachartikeln in der (rechts-)wissenschaftlichen Literatur. Früher wurden diese VR-Modelle als Ausdrucke für die Gerichtsverhandlung genutzt, jetzt erfolgt die Einsichtnahme direkt über VR-Brillen.

Auch in China kam VR-Technologie in einem Strafverfahren zum Einsatz: Ein Zeuge, der eine VR-Brille trug, wurde virtuell an den Tatort zurückversetzt, um seine Erinnerungen während der Aussage zu unterstüt-

zen.[9] Auch weitere Länder setzen VR in staatsanwaltlichen Ermittlungs- und gerichtlichen Strafverfahren ein.

V. Einsatz von VR in US-amerikanischen Zivilverfahren

Recherchiert man nach einem VR-Einsatz in Zivilverfahren stößt man überraschenderweise lediglich auf ein einziges Verfahren aus den USA aus dem Jahre 1992. Dieser Fall wurde vom Superior Court of California, County of Placer, am 25.06.1992 entschieden.[10] In der Rechtssache Stephenson v. Honda Motors Ltd of America forderte die Klägerin nach einem Sturz mit ihrem Honda-Motorrad Schadensersatz und behauptete, das Motorrad sei fehlerhaft produziert oder konstruiert und dadurch instabil gewesen, was zu ihrem Sturz geführt habe. Die Beklagte konterte, dass die Klägerin mit dem Motorrad auf zu unwegsamen Gelände gefahren sei. Anstatt Fotos oder Videos des Geländes vorzulegen, erstellte die Beklagte eine VR-Darstellung, die die Jury mithilfe von VR-Headsets betrachten konnte. Das Gericht akzeptierte dieses Beweismittel und die Klage wurde abgewiesen.

VI. Einsatz von VR in deutschen Zivilverfahren

1. Status Quo

In Deutschland kam es – soweit ersichtlich – noch nie zu einem Einsatz einer VR-Darstellung mittels VR-Brille in einem zivilgerichtlichen Verfahren. Klar ist: Die Inaugenscheinnahme von Fotos und Videos ist grundsätzlich problemlos möglich, jedoch oft nicht ausreichend aussagekräftig oder verständlich genug. Ein vom Verfasser als Richter erlebtes Beispiel ist ein Nachbarschaftsstreit mit über 50 Fotos, bei denen unklar war, wie sie zusammengehören, da sie aus verschiedenster Perspektive, aus unterschiedlichen Jahreszeiten und aus einem Zeitraum von über 20 Jahren herrührten.

9 Zum Ganzen und mit weiteren Nachweisen: Heetkamp, Virtual Reality-Technologie im Zivilverfahren, S. 35, abrufbar unter: https://epb.bibl.th-koeln.de/frontdoor/deliver/index/docId/2066/file/Heetkamp_Virtual_Reality.pdf.

10 *D. Schofield*, The use of computer generated imagery in legal proceedings, Digital Evidence and Electronic Signature Law Review, 2016, 3 (11) unter Benennung des Entscheidungsdatums und Aktenzeichens des Falles.

Im Falle von Verkehrsunfällen erfordern Sachverständigengutachten und Zeit-Weg-Diagramme oft Übung und sind nicht immer leicht verständlich. In einem Fall, den der Verfasser zu entscheiden hatte, wurde nach einem unfallanalytischen Sachverständigengutachten eine Dashcam-Aufnahme vorgelegt. Der visuelle Eindruck des Unfalls war völlig anders als das vom Sachverständigen erstellte Diagramm. Auch hier zeigt sich, dass verschiedene visuelle Mittel zu unterschiedlichen Eindrücken und Überzeugungen führen können.

Ortstermine sind selten, da sie zeitaufwendig und problemanfällig sind. Besonders problematisch wird es bei einem Richter:innenwechsel in der Kammer. Ein Beispiel für einen außergewöhnlichen Ortstermin ist der Fall einer Klimaklage eines peruanischen Bauern vor dem Oberlandesgericht Hamm.[11] Der Bauer fordert Schadensersatz von RWE aufgrund von Schäden, die seiner Meinung nach durch den CO_2-Ausstoß von RWE verursacht wurden. Zwei beauftragte Richter, die Mitglieder des Senats sind und allein zur Beweisaufnahme durch Augenschein bestimmt wurden, führten den Ortstermin durch. Hier wäre zu erwägen gewesen, ob man den Zustand der Örtlichkeit durch einen Laserscan konserviert und zur VR-Inaugenscheinnahme zugänglich macht.

Insgesamt führen diese Umstände in komplexen und/oder umfangreichen Verfahren zu extrem umfangreichen Schriftsätzen. Dies fordert die sprachlichen Fähigkeiten der Prozessbevollmächtigten und die Konzentrations- und Verständnisfähigkeiten des Gerichts auf das Äußerste heraus. Dabei weiß jeder: Menschen nehmen Informationen am besten und schnellsten über visuelle Eindrücke auf. Ein Sprichwort sagt: Ein Bild sagt mehr als tausend Worte. Man könnte ergänzen: Eine VR-Darstellung sagt mehr als 10.000 Worte.

Dabei sind sowohl Nachteile als auch Vorteile eines VR-Einsatzes denkbar.

2. Vorteile eines VR-Einsatzes

Die möglichen Vorteile von VR im Zivilverfahren sind vielfältig und können das gesamte Verfahren erheblich verbessern. Ein wesentlicher Vorteil ist das bessere Verständnis der Tatsachen, das durch die immersive Erfahrung der virtuellen Welt erreicht wird. Nutzer:innen können sich innerhalb

11 Siehe dazu etwa folgenden Pressebericht: https://www.faz.net/aktuell/wirtschaft/klimaklage-richter-bei-ortstermin-in-peru-wegen-rwe-verfahren-18062762.html.

der virtuellen Darstellung frei bewegen und umsehen, was ihnen eine genauere Beurteilung der relativen Größen von Gegenständen, der Abstände und der Sichtverhältnisse ermöglicht – viel umfassender als bei einer zweidimensionalen Darstellung.

Australische Studien haben gezeigt, dass das tatsächliche Verständnis von Entscheider:innen stark davon abhängig ist, welche Art von visueller Unterstützung zur Verfügung steht. Demnach sind Fotos besser als reiner Textvortrag; dreidimensionale Darstellungen übertreffen zweidimensionale in ihrer Wirksamkeit. Dies spiegelt sich auch in den Eindrücken wider, die Rechtsanwalt Weil im Verfahren der ermordeten Polizist:innen von Kusel geschildert hat.[12]

Ein weiterer Vorteil der VR-Technologie ist der erhöhte Informationsgehalt. In eine virtuelle Umgebung können zusätzliche Informationen interaktiv eingebettet werden. Auf einer digitalisierten Baustelle könnten beispielsweise relevante Anlagenteile eingeblendet werden, um Abweichungen zwischen dem tatsächlichen Bauzustand und den vertraglichen Vorgaben deutlich zu machen. Ein zusätzlicher Nutzen von VR ist der Effizienzgewinn, der sich allein durch das schnellere Verständnis visueller Darstellungen ergibt. Häufig sitzen Richter:innen vor einer Akte oder einem Schriftsatz und benötigen mehrere Durchgänge, um den Inhalt vollständig zu erfassen. VR kann dieses Verständnis erheblich beschleunigen und somit den gesamten Prozess effizienter gestalten. Dies könnte auf verschiedenen Verfahrensstufen genutzt werden, zum Beispiel informativ während einer Güteverhandlung oder zur Unterstützung einer Zeugenaussage mithilfe eines VR-Modells.

3. Nachteile eines VR-Einsatzes

Mögliche Nachteile der VR-Technologie im Zivilverfahren sind jedoch nicht zu unterschätzen. Ein wesentlicher Nachteil ist die potenziell hohe Suggestionskraft, die dazu führen kann, dass Zeugen sich scheinbar an Dinge erinnern, die sie tatsächlich nicht mehr wussten, sondern nur im virtuellen Modell gesehen haben. Dies kann die Verlässlichkeit von Zeugenaussagen erheblich beeinträchtigen. Gleiches gilt für Parteivortrag.

Ein weiterer bedeutender Aspekt sind die (potentiell) hohen Kosten, die mit der Implementierung und Nutzung von VR-Technologie einhergehen.

12 Siehe dazu oben unter I.

Diese könnten insbesondere bei kleineren Streitsummen und bedürftigen Parteien eine finanzielle Hürde darstellen.

Die technische Handhabbarkeit von VR-Systemen ist ebenfalls ein kritischer Punkt. Die Nutzung solcher Systeme setzt eine gewisse technische Kompetenz voraus, die nicht bei allen Beteiligten vorhanden sein dürfte. Ein Aufsatz zur Videoverhandlung mit dem Titel „Eine Vielzahl fummeliger Knöpfe" verdeutlicht, dass der menschliche Faktor bei der Einführung technischer Neuerungen in der Justiz nicht unterschätzt werden darf.[13]

Darüber hinaus erschwert die Nutzung von VR die Würdigung von Zeugenaussagen, da die Mimik und Gestik durch das VR-Equipment nur noch eingeschränkt zu lesen sind. Sollte eine (Einzel-)Richter:in eine VR-Brille im Rahmen des Verfahrens tragen, könnte die eingeschränkte Wahrnehmung der Sitzung problematisch sein. Denn die Ausübung der Sitzungsgewalt wird durch VR verkompliziert, insbesondere im Hinblick auf Störer und die Möglichkeit unerlaubter Aufzeichnungen der Sitzung.

Insgesamt müssen diese potenziellen Nachteile sorgfältig abgewogen werden, bevor VR-Technologie in Zivilverfahren eingesetzt wird.

VII. Weitere VR-Anwendungen im Justizkontext

Im Justizkontext sind weitere VR-Anwendungen bekannt. So werden VR-Simulationen im Rahmen der Rückfallprävention genutzt oder um herauszufinden, welche Auswirkungen die Aussage vor Gericht auf Opfer sexueller Gewalt hatte.

Anfang 2023 sorgte eine kolumbianische Richterin für Aufsehen, als sie eine verwaltungsgerichtliche Verhandlung in der virtuellen Realität durchführte, genauer gesagt in Metas VR-App Horizon Workrooms.[14] Die Richterin argumentierte, dass diese Art der Verhandlung sowohl schneller als auch effizienter sei und ferner den Zugang für weit entfernt wohnende Parteien erleichtere. Zudem wäre ein solches Vorgehen unter Inklusionsgesichtspunkten anzuraten. Solch ein Vorgehen ist in Deutschland derzeit (noch) nicht vorstellbar. Allenfalls im Kontext von § 495a ZPO könnte man sich eine Gerichtsverhandlung im Metaverse vorstellen. Die aktuelle Reform des § 128a ZPO verdeutlicht die detaillierte und eher zurückhalten-

13 *S. Roller*, Eine Vielzahl fummeliger Knöpfe, COVuR 2021, 135 (135 ff.).

14 Siehe ein entsprechendes Video unter: https://www.youtube.com/watch?v=JuFIVMPF004.

de Herangehensweise in Deutschland. Dabei wird deutlich, wie schwer es einigen fällt, sich Gerichtsverfahren ohne physische Anwesenheit der Richter:innen vorzustellen.

Ein weiterer Bereich der Digitalisierung der Justiz betrifft die Rechtsantragsstellen, die durch verschiedene Maßnahmen modernisiert werden sollen. So wird erwogen, diese Stellen mit einem Chatbot auszustatten, der auf der Homepage des jeweiligen Gerichts integriert werden könnte, um Bürger:innen bei ihren Anliegen zu unterstützen. Dieser Chatbot könnte nicht nur einfache Fragen wie Öffnungszeiten und Terminvereinbarungen beantworten, sondern auch komplexere Aufgaben übernehmen, wie die Identifikation des Anliegens und die Information darüber, welche Unterlagen mitzubringen sind. Zudem sieht der neue § 129a Abs. 2 ZPO vor, dass Urkundsbeamt:innen Anträge und Erklärungen auch per Bild- und Tonübertragung entgegennehmen können. Wenn man diese Ansätze konsequent weiterdenkt und um eine VR-Komponente erweitert, erscheint die Schaffung einer VR-Antragsstelle im Metaverse durchaus erstrebenswert.

VIII. Virtual Reality in der juristischen Ausbildung

Über den Reformbedarf der juristischen Lehre wird derzeit viel gestritten.[15] In der (gebotenen) Modernisierung des Jurastudiums bzw. auch der juristischen Referendarsausbildung kann VR eine wichtige Rolle spielen.

Der Verfasser hat in dieser Hinsicht das Projekt eines „KI-gestützten Zeugenavatars in einem virtuellen Gerichtssaal" umgesetzt. Der Avatar ist mit einem großen Sprachmodell gekoppelt und vorab umfassend gepromptet worden. Der Prompt umfasst sowohl den (fiktiven) Lebenssachverhalt, zu dem der Zeuge befragt werden soll, als auch die Biographie des Zeugen und Vorgaben zur Aussageart. Ziel dieses Projektes ist es, Studierenden, Referendar:innen und angehenden (Probe-)Richter:innen die virtuelle Übungsmöglichkeit einer Zeugenvernehmung zu geben.

Ein kurzes Video gibt einen Eindruck von dem Programm.[16] Dieses könnte auch in der Erwachsenenbildung (etwa in Volkshochschulen) oder in der Anleitung von Laienrichter:innen eingesetzt werden.

15 Vergleiche nur zu den verschiedenen Reformbestrebungen: https://iurreform.de/.

16 Siehe das entsprechende Video unter: https://www.youtube.com/watch?v=2SiV_7ZSC5k&t=46s.

C. Fazit und Ausblick

Es ist schon jetzt sicher, dass VR-Anwendungen zunehmend im Justizwesen eine Rolle spielen werden. Sei es in der Ausbildung, zur Darstellung von streitrelevanten Örtlichkeiten und Gegenständen oder als Art der Verfahrensführung. Bisher war die Erstellung entsprechender virtueller Darstellungen mithilfe von Laserscannern sowohl zeitaufwendig als auch kostspielig. Durch jüngste Fortschritte in der Technologie des sogenannten Gaussian Splattings könnte sich dies jedoch ändern. Mit Gaussian Splatting ist es möglich, ein 3D-Modell bereits aus einem kurzen Handyvideo zu erstellen. Diese technologischen Neuerungen wurden im Sommer 2023 auf der Konferenz Siggraph, der weltweit führenden Messe für Computergrafik, vorgestellt und gewannen dort den Best Paper Award. Sollte die Technologie ihre Versprechen halten, könnte dies dazu führen, dass in naher Zukunft jeder ohne spezielle Hardware Tatort-Darstellungen oder Abbilder relevanter Streitorte problemlos erzeugen kann. Dies eröffnet beispielsweise für Zivilverfahren, wie Bau- und Verkehrsstreitigkeiten, völlig neue Möglichkeiten.

Verwandt – aber nicht identisch mit VR – ist das Thema „Metaverse". So beschäftigt sich das Bundesministerium der Justiz schon mit diesen virtuellen Welten. Bei einer entsprechenden Fachkonferenz am 6. Mai 2024 wurden unter dem Titel „Strafrecht im neuen digitalen Zeitalter – Metaverse und Generative KI" neue Rechtsfragen erörtert.[17]

Klar ist: Die Jurist:innen von morgen sollten sich schon heute mit den Zukunftstechnologien VR und Metaverse beschäftigen.

17 Eine Aufzeichnung der Veranstaltung ist online abrufbar unter: https://www.bmj.de/SharedDocs/Veranstaltungen/DE/2024/0506_Metaverse.html.

Digitaler Zwilling im Metaverse – Eine rechtliche Untersuchung zum Authentifizierungsprozess

Jaouhara Zouagui, Peter Parycek

A. Einleitung

I. Metaverse: Verschmelzung von virtueller und physischer Welt

Der Begriff „Metaverse" stammt von Neal Stephenson aus dem Roman „Snow Crash" (1992) und beschreibt eine virtuelle 3D-Welt, in der Menschen[1] über Avatare interagieren. Trotz jahrzehntelanger Entwicklung gibt es keine einheitliche Definition, jedoch verbindet sie alle die Interaktion zwischen virtueller und physischer Welt.[2] Das Metaverse wird als nächste Iteration des Internets betrachtet,[3] dessen Entwicklung noch in den Anfängen steckt. Der Rat der Europäischen Union erwartet, dass es in 10 bis 15 Jahren etabliert sein wird.[4] Es soll Begegnungen in Echtzeit ermöglichen[5] und eine nachhaltige, zugängliche Erfahrung bieten, die mit der realen Welt verbunden ist. Reale physische Objekte werden ihre virtuellen Entsprechungen erhalten, wie z. B. Schuhe und Taschen, die im Metaverse vom Avatar des Nutzers getragen werden können.[6] Die reale und virtuelle Welt sowie öffentliche und private Netzwerke verschmelzen zu einer neuen Einheit mit eigenem Wirtschaftskreislauf. Charakteristisch für das Metaverse ist seine Interoperabilität: Nutzer sollen es in seiner ganzen Weite mittels eines einzigen Avatars oder einer einheitlichen digitalen Identität

1 Zur besseren Lesbarkeit wird im Verlauf der Arbeit das generische Maskulinum verwendet. Die Personenbezeichnungen beziehen sich jedoch auf alle Geschlechter.

2 *L. Xu,* Connecting Everyday Objects with the Metaverse: A Unified Recognition Framework, in: IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC) 2022, S. 401 (401 ff.).

3 *Kompetenzzentrum Öffentliche IT,* Metaversum, unter: https://www.oeffentliche-it.de/-/metaversum (alle Internetquellen dieses Beitrags wurden zuletzt aufgerufen am 12.10.2024).

4 *M. Martini/J. Botta*, Der Staat und das Metaversum, Zur Ordnungs- und Gestaltungsmacht im Internet von morgen, MMR 2023, 887 (888).

5 *M. Martini/J. Botta*, Metaversum (Fn. 4), 888.

6 *Bitkom e.V.,* Leitfaden Wegweiser in das Metaverse, Berlin 2022, S. 1 (7).

bereisen können.[7] Das Metaverse kann somit als virtueller Raum beschrieben werden, der durch unterschiedlich stark gewichtete Wesensmerkmale wie virtuelle Realität, virtuelle Vermögensgegenstände, digitale Identitäten und Interoperabilität geprägt ist.[8] Besonders entscheidend ist dabei die klare Zuordnung von virtuellen Vermögensgegenständen zu realen Personen mittels ihrer digitalen Identität.

II. Zugang und Interaktionen im Metaverse

Zugang zum Metaverse erhält man, wenn man sich bei einer Metaverse-Plattform als Nutzer registriert/anmeldet.[9] Diese Plattformen sind sowohl über einen Browser auf dem PC oder Smartphone als auch mit Virtual-Reality-Brillen zugänglich. Die Einsatzmöglichkeiten sind nahezu unbegrenzt und umfassen u. a. Spiele, virtuelle Treffen, Konsum und Kinobesuche.[10]

Personen agieren im Metaverse häufig über ihre digitalen Zwillinge, die sog. Avatare.[11] Diese repräsentieren die digitale Identität einer Person und können als Rechtssubjekte betrachtet werden.[12] Avatare werden physisch von Personen gesteuert und sind dadurch in der Lage, Willenserklärungen für den Erwerb von Dienstleistungen und Gütern in der virtuellen Welt abzugeben. Damit werden sie zu zentralen Zurechnungsobjekten im Metaverse.[13]

Die Erstellung digitaler Assets hat sich zu einer milliardenschweren Industrie entwickelt. Virtuelle Kleidung, Welten und Kunstwerke werden für echtes Geld gekauft.[14] In der Idealvorstellung des Metaverse können durch Avatare erworbene virtuelle Güter sowie reale Güter besessen und überallhin mitgenommen werden.[15] Die Vermögensgegenstände werden als Attribute elektronisch bestätigt und einer berechtigten Person (bzw.

7 *M. Martini/J. Botta*, Metaversum (Fn. 4), 888.
8 *M. Kaulartz/A. Schmid/F. Müller-Eising,* Das Metaverse – eine rechtliche Einführung, RDI 2022, 323 (522).
9 *L. Bender-Paukens/S. Werry*, Datenschutz im Metaverse, Datenschutzrechtliche Herausforderungen im Zusammenhang mit der DSGVO, ZD 2023, 127 (128).
10 *M. Kaulartz/A. Schmid/F. Müller-Eising*, Metaverse (Fn. 8), 522.
11 *M. Kaulartz/A. Schmid/F. Müller-Eising,* Metaverse (Fn. 8), 523.
12 *M. Kettermann/C. Böck*, § 6 Regulierung des Metaverse, in: H. Steege/C. Kuuya/M. Bagratuni (Hrsg.), Metaverse, Rechtshandbuch, Baden-Baden 2023, S. 114 (126).
13 *M. Kaulartz/A. Schmid/F. Müller-Eising,* Metaverse (Fn. 8), 524 f.
14 *Bitkom e.V.,* Wegweiser (Fn. 6), S. 9.
15 *Bitkom e.V.,* Wegweiser (Fn. 6), S. 50.

deren Wallet) zugeordnet. Da an die Handlungen von Avataren rechtliche Anforderungen oder Konsequenzen geknüpft sein können, kann auch im virtuellen Raum ein Identifizierungsbedarf bestehen.[16] Nutzer sollten in der Lage sein, durch ihren Avatar Merkmale nachzuweisen, die mit ihrer Offline-Identität verbunden sind,[17] um beispielsweise im Metaverse beim Kauf von Vermögenswerten oder der Inanspruchnahme von Dienstleistungen notwendige Attribute datensparsam nachzuweisen. Im Folgenden wird eine geplante staatliche Lösung vorgestellt, um einem Avatar entsprechende Merkmale zuzuweisen.

B. Hauptteil

Bereits heute können Nutzer per Smartphone Zugang zum Metaverse erhalten und über ihren Avatar interagieren.

I. EUDI Wallet: Nutzung des Smartphones als Identifikationsinstrument im Metaverse

Eine verifizierbare Identität, die gleichzeitig den Datenschutz gewährleistet, ist ein entscheidender Baustein für ein zukünftiges dezentrales Metaverse.[18] Die im Frühjahr 2024 verabschiedete eIDAS-2.0-Verordnung (eIDAS 2.0) bildet den neuen rechtlichen Rahmen für die Gestaltung digitaler Identitäten in der Europäischen Union (EU). Sie bildet das Fundament für eines der wichtigsten Digitalisierungsvorhaben der EU und Deutschlands.[19] Nach der eIDAS 2.0 wird die sog. European Digital Identity Wallet (EUDI Wallet) eingeführt,[20] die für öffentliche Stellen sowie

16 *M. Lutz*, Sichere elektronische Identitäten und sichere Identifizierung im E-Government, in: D. Kipker/M. Barudi/K. Beucher (Hrsg.), Cybersecurity, München 2023, S. 632 (635).

17 *M. Zichichi/C. Bomprezzi/G. Sorrention/M. Palmirani*, Protecting digital identity in the Metaverse: the case of access to a cinema in Decentraland, in: Proceedings of the Fifth Distributed Ledger Technology Workshop (DLT) 2023, S. 1 (4 ff.).

18 *Bitkom e.V.,* Wegweiser (Fn. 6), S. 18.

19 *CDU/CSU-Fraktion im Deutschen Bundestag,* eIDAS 2.0 - Die Brücke ins Digitale Zeitalter: Sichere digitale Identitäten als Schlüssel einer digitalen Gesellschaft, 2024, S. 1 (4).

20 *C. Busch*, § 16 Digitale Identitäten im Metaverse, in: H. Steege/K. Chibanguza/M. Bagratuni (Hrsg.), Metaverse Rechtshandbuch, Baden-Baden 2023, S. 293 (300 f.).

bestimmte privatwirtschaftliche Akteure verpflichtend wird. Dies betrifft auch sehr große Metaverse-Plattformbetreiber[21] gemäß Art. 33 Abs. 1 Digital Services Act (DSA), die die Wallet als Identifizierungsinstrument akzeptieren müssen.[22] Die nationale EUDI Wallet soll voraussichtlich Anfang 2027 verfügbar sein.[23]

1. Gestaltung digitaler Identitäten und Austausch verifizierter Daten im Lichte der EUDI Wallet

Die EUDI Wallet wird also künftig als zentrales Werkzeug für Bürger dienen, um auf private und öffentliche Onlinedienste zuzugreifen. Die EUDI Wallet auf dem Smartphone ermöglicht den verifizierten Austausch von selektiven Daten zwischen Behörden, Unternehmen und Bürgern. Diese Daten können sowohl Identitätsdaten (PID)[24] als auch Nachweise wie Eintrittskarten oder Meldebescheinigungen umfassen, die digital und verifizierbar übertragen werden können.[25] Mit der EUDI Wallet als staatliche Lösung können Benutzer ihren Avatar so mit verschiedenen Merkmalen bzw. Attributen ausstatten.[26]

a) Bestätigung von Merkmalen

Der eIDAS-Vorschlag und der Architektur-Referenzrahmen beschreiben die qualifizierte elektronische Bescheinigung von Attributen als generische, universelle elektronische Berechtigungsnachweise, die beliebige Benutzerdaten bestätigen. Qualifizierte elektronische Bestätigungen von Attributen

21 Art. 33 Abs. 1 DSA definiert Online-Plattformen mit einer durchschnittlichen monatlichen Zahl von mindestens 45 Millionen aktiven Nutzern in der EU als sehr große Online-Plattform. Erreicht eine Metaverse-Plattform diese Größe, unterliegt sie der Akzeptanzpflicht.

22 *C. Busch,* § 16 Digitale Identitäten (Fn. 20), S. 303.

23 *Bundesministerium des Innern und für Heimat,* Die eIDAS-Verordnung, unter: https://www.digitale-verwaltung.de/Webs/DV/DE/digitale-identitaeten/eidas-2-0/eidas-2-0-node.html.

24 Sog. Personal Identification Data.

25 *Bitkom e.V.,* eIDAS Leitfaden, Berlin Mai 2024, S. 1 (5 f.).

26 *M. Zichichi et. al.*, Protecting digital identity (Fn. 17), S. 4 ff.

(QEAAs) werden von qualifizierten Vertrauensdiensteanbietern bereitgestellt.[27]

Es wird zwischen elektronischen Bestätigungen von Attributen (EAAs) und QEAAs unterschieden: EAAs können aus staatlich autorisierten und „nicht-authentischen Quellen" stammen. EAAs aus staatlich autorisierten Registern gelten automatisch als QEAA und können in die Wallet ausgegeben werden. Attribute aus nicht staatlich autorisierten Quellen müssen von einem qualifizierten Vertrauensdiensteanbieter geprüft und validiert werden, um als QEAA anerkannt zu werden.[28] Diese (Q)EAAs werden zusammen mit den PID-Daten in der Wallet gespeichert,[29] um ein Merkmal im Kontext des Metaverse nachzuweisen.[30]

b) Einfluss auf die Modernisierung der Register

Die Umsetzung von eIDAS 2.0 als Rahmenwerk für digitale Identitäten wird auch die nationale Gesetzgebung, wie beispielsweise das Registermodernisierungsgesetz (RegMoG) und das Onlinezugangsgesetz (OZG) beeinflussen.[31] Der IT-Planungsrat beauftragte 2022 die Entwicklung eines Zielbildes für die Umsetzung der Registermodernisierung, das in das Nationale Once-Only-Technical-System (NOOTS) mündete.[32] Dieses System verfolgt das Once-Only-Prinzip (OOP), das es staatlichen Stellen ermöglicht, mit Einverständnis der Bürger bereits vorliegende Daten selbst (bei

27 *Bundesministerium des Innern und für Heimat,* Architecture Proposal for the German eIDAS Implementation, Version 2.2, 2014, S. 1 (40).

28 *Bundesdruckerei,* QEAA einfach erklärt: Bedeutung der Qualifizierten Elektronischen Attestierung von Attributen für die EUid-Wallet, unter: https://www.bundesdruckerei.de/de/innovation-hub/qeaa-einfach-erklaert#.

29 *Lissi GmbH*, EUDI-Wallet: Veranschaulichung der eIDAS-Rollen und Beziehungen, unter: https://www.lissi.id/de/blog/eudi-wallet-illustration-of-the-eidas-roles-and-relationships.

30 Vgl. *Die Europäische Kommission*, FAQ - EU Digital Identity Wallet, unter: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/FAQ.

31 *CDU/CSU-Fraktion im Deutschen Bundestag,* eIDAS 2.0 (Fn. 19), S. 4 f.

32 *Bundesverwaltungsamt,* Anbindungsleitfaden: Informationen für registerführende Stellen zur Anbindung an das Fachverfahren zum Identitätsdatenabruf (IDA), 2024, S. 9 (9).

anderen Behörden) abzurufen.[33] Das NOOTS-Gesamtsystem umfasst alle NOOTS-Komponenten, die für die Durchführung oder Nachvollziehbarkeit eines Nachweisabrufs notwendig sind[34] und formuliert Anschlussbedingungen.[35]

Die eIDAS 2.0 sieht die Öffnung der öffentlichen Register für den Nachweisabruf vor, während das OZG die Ausstellung von Attributsbescheinigungen für die Ausgestaltung der EUDI Wallet berücksichtigen muss. Daher ist es wichtig, die nationale Gesetzgebung mit der eIDAS 2.0 abzustimmen.[36] Derzeit sieht das RegMoG beispielsweise nur den Datenaustausch zwischen öffentlichen Stellen nach § 6 Identifikationsnummerngesetz (IDNrG) vor. Um eine effektive Nutzung der Register i.R.v. eIDAS 2.0 zu gewährleisten, sollten häufig angefragte Register zeitnah geöffnet und der gesetzliche Rahmen in den Fachgesetzten angepasst werden. Dies erfordert u. a. die Verfolgung des OOP, die Priorisierung wesentlicher Register für die geplanten Anwendungsfälle der EUDI Wallet sowie eine enge Verzahnung mit dem OZG.[37]

2. Neuer biometrischer Authentifizierungsprozess im Lichte der EUDI Wallet

Der Austausch von Identitätsdaten, bei dem auch staatliche Register einbezogen werden, ist eine zentrale Funktion der Wallet und eine wichtige Neuerung von eIDAS 2.0.[38] Die Authentifizierung des Identitätsinhabers bei jeder Vorlage der PID erfolgt auf Basis des deutschen elektronischen Identitätsnachweises (eID) als staatliche digitale Identität.[39] Die Verordnung macht die eID damit zum zentralen Bestandteil der Wallet auf dem Smartphone, die Personenidentifizierungsdaten auf hohem Vertrauensni-

33 *Bundesverwaltungsamt,* Nutzen der Registermodernisierung, unter: https://www.bva.bund.de/DE/Services/Behoerden/Verwaltungsdienstleistungen/Registermodernisierung/Ueberblick/ueberblick_node.html.
34 *Bundesministerium des Innern und für Heimat,* High-Level-Architecture (HLA), unter: https://bmi.usercontent.opencode.de/noots/AD-NOOTS-03_%2BHigh-Level-Architecture%2B_HLA_/.
35 *Bundesverwaltungsamt,* Anbindungsleitfaden (Fn. 32), S. 9.
36 *CDU/CSU-Fraktion im Deutschen Bundestag,* eIDAS 2.0 (Fn. 19), S. 4 f.
37 *CDU/CSU-Fraktion im Deutschen Bundestag,* eIDAS 2.0 (Fn. 19), S. 9.
38 Vgl. *Bitkom e.V.,* eIDAS Leitfaden (Fn. 25), S. 6.
39 *Bundesministerium des Innern und für Heimat,* Architecture Proposal (Fn. 27), S. 35.

veau bereitstellt.[40] Der Authentifizierungsprozess der eID-Funktion (auch als Online-Ausweisfunktion bekannt) spielt dabei eine entscheidende Rolle.

a) Authentifizierungsprozess

Die nationale eID ist die Online-Ausweisfunktion nach § 18 Personalausweisgesetz (PAuswG). Sie gewährleistet eine Identifizierung und basiert auf einer Zwei-Faktor-Authentifizierung gemäß Art. 8 Abs. 2 c eIDAS 2.0. Durch die Kombination von Ausweis (Besitz-Element) und PIN-Nummer (Wissens-Element) wird zwar eine hohe Sicherheit erreicht, jedoch ist die Benutzerfreundlichkeit eingeschränkt. Laut der eGovernment MONITOR Studie 2024 nutzten 2023 lediglich 14 % der Befragten den Online-Ausweis. 2024 stieg dieser Anteil auf 22 %.[41] Damit ist die eID trotzdem noch weit von einer flächendeckenden Nutzung entfernt. Dies hat verschiedene Gründe, darunter die wenig benutzerfreundliche Eingabe der sechsstelligen PIN.[42]

Der nachfolgende Beitrag befasst sich mit der Optimierung der Anwendungsfreundlichkeit der eID-Funktion durch den Wegfall der PIN-Eingabe für Anwendungszwecke der Smartphone EUDI Wallet. Wenn der Zugang zum Metaverse über ein Smartphone per EUDI Wallet erfolgt, könnte sich die Möglichkeit bieten, biometrische Daten zur Authentifizierung im Rahmen eines Touch-ID- oder Face-ID-Verfahrens zu nutzen, wodurch die PIN-Eingabe ersetzt wird. Für eine sichere Nutzerauthentifizierung mit hohem Vertrauensniveau sind mindestens zwei Authentifizierungsfaktoren aus verschiedenen Kategorien erforderlich.[43] Das Besitzelement wird durch den biometrischen Authentifizierungsfaktor ergänzt. Bei dieser Form der Authentifizierung muss ein Nutzer ein biometrisches Merkmal, wie einen Fingerabdruck oder ein Gesichtsbild, zur Verfügung stellen. Das System vergleicht dieses Merkmal mit einer registrierten Vorlage.[44] Nach § 12 eID-Karte-Gesetz (eIDKG) kann die eID aus einem elektronischen Speicher- und Verarbeitungsmedium in einem mobilen Endgerät erfolgen.

40 *Bundesdruckerei*, eIDAS 2.0: Alle Änderungen im Überblick 2023, unter: https://www.bundesdruckerei.de/de/innovation-hub/eidas/eidas-2-0#.

41 *Initiative D21 e.V./Technische Universität München,* eGovernment MONITOR 2024, 2024, S. 18 (19 f.).

42 *CDU/CSU-Fraktion im Deutschen Bundestag,* eIDAS 2.0 (Fn. 19), S. 3.

43 ABI L 2024/1183, 18.

44 *H. Zhong/C. Huang/X. Zhang/M.,* Metaverse CAN: Embracing Continuous, Active, and Non-intrusive Biometric Authentication, in: IEE Network, 2023, S. 67 (70).

§ 19 eIDKG schreibt jedoch vor, dass keine biometrischen Daten im eID-Karten-Register für die Online-Ausweisfunktion geführt werden.

Die freiwillige Online-Ausweisfunktion kann beispielsweise zur digitalen Kontoeröffnung im Finanzbereich[45] ohne die Nutzung biometrischer Daten verwendet werden. Der Einsatz von Biometrie im elektronischen Ausweisdokument dient nur der Verifikation des Ausweisinhabers bei einer hoheitlichen Identitätskontrolle. Dies ermöglicht eine einfachere Überprüfung, ob die Person, die den Ausweis vorlegt, tatsächlich der Inhaber ist. Beispielsweise können zwei Personen, die für das menschliche Auge nahezu identisch erscheinen, durch einen computerunterstützten Gesichtsvergleich bei einer Grenzkontrolle voneinander unterschieden werden.[46] Die folgende Tabelle 1 zeigt, welche Daten bisher bei den genannten Anwendungsbeispielen der eID verwendet werden.

45 Bsp. *Bundesministerium des Innern und für Heimat*, Anwendungen: ING Deutschland, unter: https://www.personalausweisportal.de/SharedDocs/anwendungen/Webs/PA/DE/Unternehmen/ing.html.

46 *Bundesamt für Sicherheit in der Informationstechnik,* Biometrie in elektronischen Ausweisdokumenten, unter: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Elektronische-Ausweisdokumente/Biometrie/biometrie_node.html.

Daten	Hoheitliche Identitätskontrolle	Online-Ausweisfunktion (freiwillig)
Familienname und Vornamen	+	+
Geburtsdatum und -ort	+	+
Anschrift und Postleitzahl	+	+
wenn angegeben: Ordens- bzw. Künstlername	+	+
wenn angegeben: Doktorgrad	+	+
Biometrische Daten		
digitales Lichtbild	+	-
digitale Fingerabdrücke	+	-
Weitere Angaben		
Seriennummer des Ausweises	+	-

Tabelle 1: Datenübertragung der Online-Ausweisfunktion.[47]

Lediglich im Chip des Personalausweises werden zwei Fingerabdrücke und das Lichtbild als biometrische Daten gespeichert, die als Vorlage dienen könnten. Die Fingerabdrücke werden ausschließlich für die Speicherung im Chip des Personalausweises erhoben. Spätestens wenn der Ausweis abgeholt wird, werden die Fingerabdrücke beim Hersteller und in der Personalausweisbehörde gelöscht.[48] Dann können nur die Behörden, die nach

47 *Bundesministerium des Innern und für Heimat,* Daten im Chip, unter: https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/der-personalausweis/daten-im-chip/daten-im-chip-node.html.

48 *Bundesministerium des Innern und für Heimat,* Ihr Personalausweis, unter: https://www.personalausweisportal.de/SharedDocs/downloads/Webs/PA/DE/informationsmaterial/flyer-broschueren/Broschuere_ihr_Personalausweis.pdf?__blob=publicationFile&v=23.

§ 16 PAuswG zur Identitätsfeststellung ermächtigt sind, die biometrischen Daten zu bestimmten Zwecken aus dem Chip auslesen.[49]

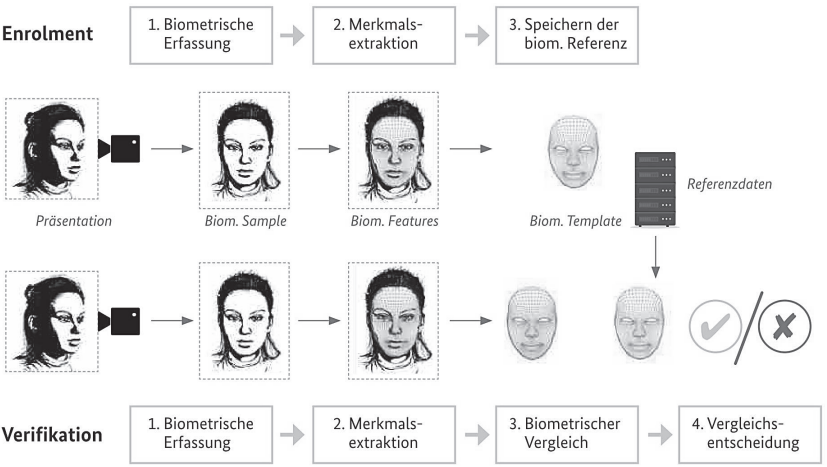


Abbildung 1: Prozessdarstellung von der Erfassung bis zur Vergleichsentscheidung in einem biometrischen System.[50]

Neben der Speicherung des Lichtbildes auf dem Chip des Personalausweises wird dieses jedoch auch im Personalausweisregister nach § 23 Abs. 3 PAuswG geführt.[51] Da lediglich über das Personalausweisregister auf das Lichtbild zugegriffen werden kann (Fingerabdrücke sind nicht verfügbar), fokussiert dieser Beitrag den biometrischen Datenabgleich des Lichtbildes für ein Face-ID-Verfahren aus dem Personalausweisregister, das bei den Personalausweisbehörden angesiedelt ist. Dieses Lichtbild dient als Referenz (Gesichtsprofil Template) für den biometrischen Datenabgleich nach Abbildung 1, um statt der PIN-Eingabe ein biometrisches Merkmal zur Authentifizierung i.R.d. EUDI Wallet-Lösung verifizieren zu lassen.

49 *Bundesministerium des Innern und für Heimat,* Daten im Chip (Fn. 47).

50 *Bundesamt für Sicherheit in der Informationstechnik,* Whitepaper 01 - Digitaler Verbraucherschutz: Bewertung des Usable Security und IT-Sicherheit biometrischer Verfahren in der Zwei-Faktor-Authentisierung, Bonn 2024, S. 1 (7).

51 Vgl. *G. Hornung,* Die digitale Identität, Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, Baden-Baden 2005, S. 47 (51 f.).

b) Grundlegende Architektur der Registermodernisierung

Für den biometrischen Authentifizierungsprozess der eID ist vorgesehen, die NOOTS-Architektur für den Abruf von Nachweisen i.R.d. Registermodernisierung zu nutzen (s.o. B.I.1.b.). Eine Komponente des NOOTS ist das Identitätsmanagement (IDM) für Personen,[52] das gemäß § 1 IDNrG die Bereitstellung einer eindeutigen Identifikationsnummer (IDNr), auch bekannt als Steuer-ID, sowie weiterer personenbezogener Daten, den sog. Basisdaten nach § 4 Abs. 2 IDNrG, verantwortet. Folgende Daten werden als Basisdaten zugeordnet: IDNr, Familienname, frühere Namen, Vornamen, Doktorgrad, Tag und Ort der Geburt, Geschlecht, Staatsangehörigkeiten, gegenwärtige oder letzte bekannte Anschrift, Sterbetag, Tag des Einzugs und Auszugs.[53] Dies ist notwendig, um Personenverwechselungen bei den registerübergreifenden Datenübermittlungen zu verhindern.[54]

Technisch wird das IDM für Personen durch das Identitätsdatenabruf-Verfahren (IDA-Verfahren) des Bundesverwaltungsamts (BVA) umgesetzt, wie in Abbildung 2 dargestellt.[55] Neben der IDNr werden in der Steuer-ID-Datenbank vom Bundeszentralamt für Steuern (BZSt) die Basisdaten gespeichert, um die Zuordnung der IDNr zu einer natürlichen Person zu ermöglichen.[56] Die registerführenden Stellen des Bundes und der Länder integrieren die Steuer-ID in ihre Datenbestände und aktualisieren die Informationen, die den Basisdaten entsprechen (§ 2 Nr. 1 und 2 IDNrG).[57]

52 *Gesamtsteuerung Registermodernisierung,* Projekt „Gesamtsteuerung Registermodernisierung": Bericht zum Umsetzungsstand, 2022, S. 1 (7).
53 *Bundesverwaltungsamt,* Anbindungsleitfaden (Fn. 32), S. 26.
54 *J. Botta*, Der digitale Staat als gläserner Staat: Transparenz als Bedingung verfassungskonformer Registermodernisierung, Baden-Baden 2023, S. 27 (30).
55 *Bundesverwaltungsamt,* Anbindungsleitfaden (Fn. 32), S. 10.
56 *Finanzministerium Thüringen,* Vorhaben der Registermodernisierung, unter: https://registermodernisierung.thueringen.de/registermodernisierung-vorhaben-und-voraussetzungen.
57 *J. Botta*, Der digitale Staat (Fn. 54), S. 30.

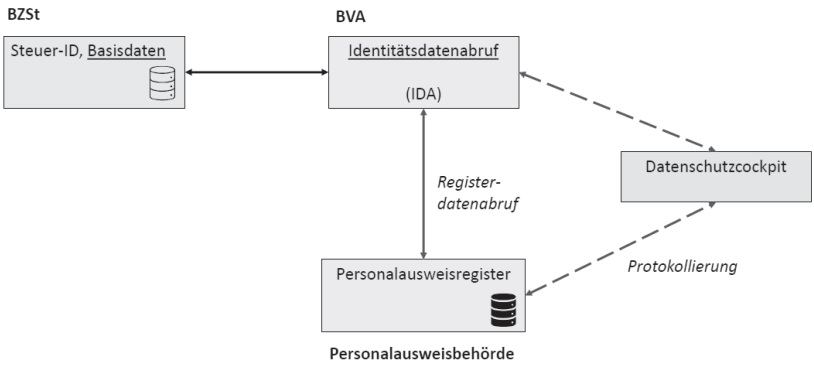


Abbildung 2: IDA-Verfahren am Beispiel der Anbindung des Personalausweisregisters.[58]

Um den Abruf der IDNr und der übrigen Basisdaten zu ermöglichen, müssen die dezentralen Register (in diesem Fall das Personalausweisregister der registerführenden Stelle) an das IDA-Verfahren angeschlossen werden,[59] damit das Lichtbild aus dem Personalausweisregister für den biometrischen Datenabgleich abgerufen werden kann. Das Datenschutzcockpit gemäß § 10 OZG ist eine IT-Komponente, die es betroffenen Personen ermöglicht, Informationen zu der entsprechenden Datenübermittlung zwischen den öffentlichen Stellen einzusehen (§ 10 Abs. 1 S. 1 OZG).[60]

Die folgende Abbildung 3 zeigt den Entwurf eines vereinfachten Prozessmodells zur Nutzung der Online-Ausweisfunktion mit der EUDI Wallet per Gesichtserkennungstechnologie, basierend auf dem NOOTS-Konzept.

58 Modifizierte Darstellung angelehnt an: *Finanzministerium Thüringen,* Vorhaben der Registermodernisierung (Fn. 56).

59 *KGSt,* Registermodernisierung, unter: https://www.kgst.de/registermodernisierung.

60 Im Datenschutzcockpit erhält die betroffene Person eine Übersicht über die Datenübermittlungen nach § 9 Abs. 1 IDNrG, bei denen ihre IDNr verwendet wurde (§ 10 Abs. 1 S. 2 OZG). Konkret kann die betroffene Person nachträglich die Protokolldaten gemäß § 9 IDNrG, einschließlich der übermittelten Inhaltsdaten und der Bestandsdaten der Register einsehen (§ 10 Abs. 2 S. 1 OZG) [*J. Botta*, Der digitale Staat (Fn. 54), S. 39 ff.].

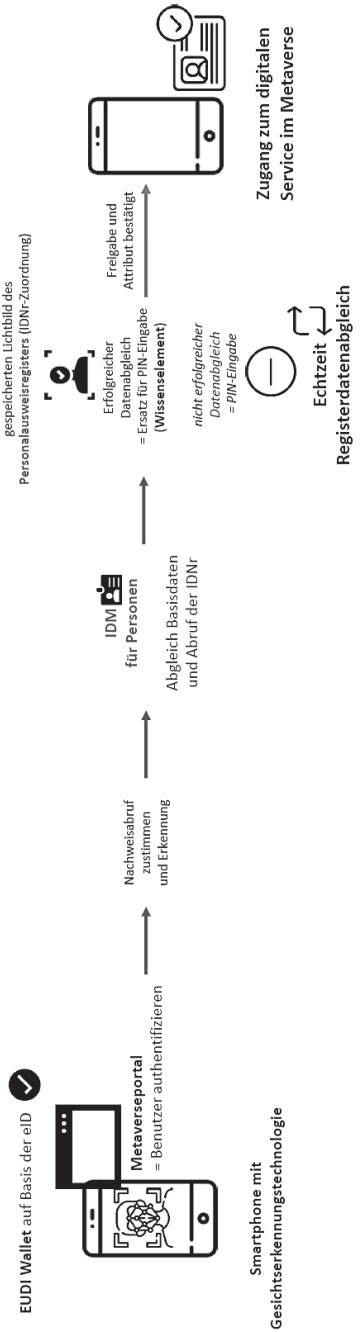


Abbildung 3: Vorgangsmodell zum biometrischen Authentifizierungsverfahren im Metaverse.[61]

Im Personalausweisregister wird das vom Smartphone übertragene Foto mit dem Personalausweisbild abgeglichen und die Übereinstimmung bestätigt. Mit dieser Bestätigung des biometrischen Attributs kann die PIN-Eingabe bei der Online-Ausweisfunktion entfallen. Die Vereinfachung des Authentifizierungsprozesses durch ein biometrisches Verfahren erhöht die Anwendungsfreundlichkeit bei der Inanspruchnahme digitaler Services im Metaverse. Dabei ist jedoch entscheidend, dass die Datenschutzstandards eingehalten werden.

3. Zwischenfazit

Mit der Einführung der EUDI Wallet wird eine sichere Online-Authentifizierung sowie die Verwaltung und gezielte Weitergabe von Identitätsdaten auch im Metaverse ermöglicht. Den Authentifizierungsprozess gilt es durch ein datenschutzkonformes biometrisches Verfahren zu vereinfachen, auf dessen rechtliche Grundlage im Weiteren eingegangen wird.

II. Datenschutzrechtliche Prüfung des biometrischen Authentifizierungsprozesses der EUDI Wallet

Es ist zu untersuchen, ob die grundrechtlichen Schranken beim automatisierten Datenabgleich mit dem Lichtbild aus dem Personalausweisregister nach § 23 Abs. 3 PAuswG zum Zwecke der Identifizierung per Online-Ausweisfunktion gewahrt werden können.

Das biometrische Lichtbild, das aus der Datenbank des Personalausweises abgerufen wird, hat zur Aufgabe, natürliche Personen anhand ihrer biometrischen personenbezogenen Daten zu identifizieren.[62] Für die Speicherung biometrischer Merkmale ist eine präzise Zweckbestimmung erforderlich.[63] § 14 PAuswG legt fest, unter welchen Voraussetzungen berechtigte Behörden und Stellen personenbezogene Daten aus dem Ausweis erheben und verwenden dürfen. Eine Nutzung biometrischer Daten für die eID-Funktion ist nach §§ 15 bis 20 PAuswG nicht vorgesehen (s.o. Abbil-

61 Eigene Darstellung.

62 *M. Kaulartz/A. Schmid/F. Müller-Eising,* Metaverse (Fn. 8), 526.

63 *C. Golembiewski/T. Probst,* Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen, Kiel 2003, S. 1 (24).

dung 1). Eine eigene gesetzliche Grundlage für ein biometrisches Authentifizierungsverfahren besteht derzeit nicht.

Es wird daher geprüft, ob die Verwendung des Lichtbildes für den biometrischen Authentifizierungsprozess der eID-Funktion zumindest durch die Einwilligung der Nutzenden zulässig ist.

1. Prüfungsmaßstab der Verarbeitung personenbezogener Daten im Mehrebenensystem

Zur Klärung der Zulässigkeit der Einwilligung in die Verarbeitung des biometrischen Lichtbildes aus dem Personalausweisregister für die Online-Ausweisfunktion muss festgestellt werden, ob der grundrechtliche Prüfungsmaßstab nach Unions- oder nationalen Grundrechten bestimmt wird.

Der rechtliche Rahmen der Digitalisierung wird maßgeblich durch das Datenschutzrecht bestimmt, soweit es um die Verarbeitung personenbezogener Daten geht. Das europäische Primärrecht nennt zwei relevante Rechte für den Datenabgleich des Lichtbilds. Zum einen das in Art. 8 Abs. 1 Grundrechtecharta (GRCh) bzw. in Art. 16 Abs. 1 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV)[64] verankerte Recht jeder Person auf Schutz der sie betreffenden personenbezogenen Daten[65] und zum anderen das Recht auf Achtung des Privat- und Familienlebens gemäß Art. 7 GRCh, welches seinen historischen Ursprung im beinahe wortgleichen Art. 8 der Europäischen Menschenrechtskonvention (EMRK)[66] findet.[67] Auf nationaler Ebene bildet das verfassungsrechtliche Fundament des Datenschutzrechts hauptsächlich das Recht auf informa-

64 Als grundrechtlicher Maßstab ist ausschließlich Art. 8 GRCh anzuwenden, während Art. 16 Abs. 1 AEUV lediglich eine deklaratorische Funktion hat [*H. Bretthauer* in: L. Specht/R. Mantz (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, 1. Aufl., München 2019, § 2 Verfassungsrechtliche Grundlagen, Europäisches und nationales Recht Rn. 37].

65 *D. Caliebe/I. Sommer,* Datenschutz in: H. Lühr/R. Jabkowski/S. Smentek (Hrsg.), Handbuch Digitale Verwaltung, Wiesbaden 2019, S. 225 (226).

66 Letztlich hat Art. 7 GRCh gemäß Art. 52 Abs. 3 GRCh die gleiche Bedeutung wie Art. 8 EMRK. Nach dem Willen der GRCh, einschließlich der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR), wird Art. 8 EMRK als Auslegungshilfe für Art. 7 GRCh genutzt (vgl. *Wissenschaftliche Dienste des Deutschen Bundestages*, Die Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäischen Grundrechtecharta, WD 11 – 3000 – 12/11, S. 6).

67 ABI C 2007/303/02, 20.

tionelle Selbstbestimmung[68] als besondere Ausprägung des Allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.

Art. 8 und Art. 7 GRCh, verfolgen weitestgehend den gleichen Zweck wie das nationale Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, nämlich den Schutz der Freiheit und der Selbstbestimmung durch den Schutz personenbezogener Daten. Somit stehen sich Art. 8 und Art. 7 GRCh als EU-Primärrecht und das Recht auf informationelle Selbstbestimmung als deutsches Grundrecht[69] gegenüber.

Die Anwendbarkeit der Grundrechtecharta wird durch Art. 51 Abs. 1 GRCh bestimmt. Nach Art. 51 Abs. 1 S. 1 Var. 2 GRCh sind die EU-Mitgliedstaaten und somit auch Deutschland verpflichtet, die GRCh zu beachten, wenn sie Unionsrecht durch nationale Stellen umsetzen.[70] Laut den Bundesverfassungsgericht (BVerfG)-Beschlüssen „Recht auf Vergessen I"[71] und „Recht auf Vergessen II"[72] vom 6.11.2019 hängt der grundrechtliche Prüfungsmaßstab davon ab, ob eine vollständige Vereinheitlichung eines Bereichs durch das Unionsrecht vorliegt.[73]

Regelt das Unionsrecht die Materie abschließend, wie z. B. bei einer Verordnung oder einer vollharmonisierenden Richtlinie, haben die Unionsgrundrechte Vorrang und sind grundsätzlich abschließend. Das BVerfG führt aus: „Bei der Anwendung unionsrechtlich vollständig vereinheitlichter Regelungen sind grundsätzlich nicht die deutschen Grundrechte, sondern allein die Unionsgrundrechte maßgeblich." […] Die Anwendung der Unionsgrundrechte ist hier eine Konsequenz der Übertragung von Hoheitsbefugnissen auf die EU nach Art. 23 Abs. 1 S. 2 GG. Wenn die Union im Rahmen dieser Befugnisse Regelungen schafft, die in der gesamten Union gelten und einheitlich angewendet werden sollen, muss auch der Grundrechtsschutz, der bei Anwendung dieser Regelungen gewährleistet

68 Bereits im Jahre 1983 hatte das BVerfG im Volkszählungsurteil [BVerfGE 65, 1] festgestellt, dass unter den Bedingungen der modernen Datenverarbeitung der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG umfasst ist und hieraus das Grundrecht auf informationelle Selbstbestimmung abgeleitet [*D.* Caliebe/I. Sommer, Datenschutz (Fn. 65), S. 226 f.].

69 *M. Desoi*, Intelligente Videoüberwachung, Wiesbaden 2018, S. 45 (59).

70 Zur Auslegung *M. Ruffert/F. Grischek/M. Schramm*, Europarecht im Examen – Die Grundrechte, JuS 2020, 1022 (1023 ff.).

71 BVerfG NJW 2020, 265 (300).

72 BVerfG NJW 2020, 265 (314).

73 *N. Klass*, Das Recht auf Vergessen und die Zeitlichkeit der Freiheit, ZUM 2020, 265 (273).

werden soll, einheitlich sein. Diesen Grundrechtsschutz gewährleistet die GRCh der EU. Die deutschen Grundrechte sind in diesen Fällen nicht anwendbar, da dies das Ziel der Rechtsvereinheitlichung konterkarieren würde. Das BVerfG leitet zudem eine Vermutungswirkung für eine „Mitgewährleistung" der Unionsgrundrechte bei Wahrung der nationalen Grundrechte her. Diese basiert auf dem gemeinsamen Fundament der allgemeinen Rechtsgrundsätze und der EMRK als gemeinsamer Auslegungsmaßstab für die GRCh, wie für die nationalen Grundrechte, in den Fällen des Art. 52 Abs. 3 GRCh.[74]

Seit dem 25.5.2018 gilt in der gesamten EU die Datenschutz-Grundverordnung (DSGVO) nach Art. 288 Abs. 2 AEUV, unmittelbar und in Deutschland[75] zusätzlich auch das neue Bundesdatenschutzgesetz (BDSG),[76] die der Ausgestaltung der Verarbeitung personenbezogener Daten als Authentifizierungsfaktoren i.R.d. eID-Funktion Rahmenbedingungen setzen.[77] Ermächtigungsgrundlage für die DSGVO zur Ausgestaltung der Artt. 8, 7 GRCh[78] ist Art. 16 Abs. 2 AEUV. Dadurch ist das Europäische Parlament und der Rat der EU ermächtigt, Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten zu erlassen.[79] Die DSGVO gilt unmittelbarer in allen EU-Mitgliedstaaten. Für ihre Geltung braucht es keine Umwandlung in nationales Recht.[80]

Der europäische Gesetzgeber hat die DSGVO jedoch nicht als klassische Verordnung ausgestaltet.[81] Sie ermöglicht den Mitgliedstaaten, durch sog. Öffnungsklauseln nationalen Spielraum im Datenschutzrecht zu schaffen.[82] § 1 Abs. 5 BDSG stellt den Vorrang der unmittelbar geltenden Bestimmun-

74 *J. Kühling*, Das „Recht auf Vergessenwerden" vor dem BVerfG – November(r)evolution für die Grundrechtsarchitektur im Mehrebenensystem, NJW 2020, 275 (277).

75 *H. Bretthauer* (Fn. 64), § 2 Verfassungsrechtliche Grundlagen, Europäisches und nationales Recht Rn. 5.

76 *J. Schneider*, Datenschutz nach der EU-Datenschutz-Grundverordnung, München 2019, S. 46 (46).

77 Vgl. *M. Martini/M. Wenzel*, "Once only" versus "only once": Das Prinzip einmaliger Erfassung zwischen Zweckbindungs-grundsatz und Bürgerfreundlichkeit, DVBI 2017, 749 (751).

78 *J. Schneider*, Datenschutz (Fn. 76), S. 46.

79 EG 12 DSGVO.

80 EuGH Urt. v. 31.1.1978 – Rs. C-94/77, Rn. 22.

81 *J. Kühling/M. Martini*, Die Datenschutz-Grundverordnung: Revolution oder Evolution im euro-päischen und deutschen Datenschutzrecht?, EuZW 2016, 448 (449).

82 *J. Kühling/M. Martini,* Datenschutz-Grundverordnung (Fn. 81), 448 f.

gen der Verordnung fest und berücksichtigt somit den Anwendungsvorrang des Unionsrechts. Das BDSG greift daher nur insoweit ein, als die Regelungen der DSGVO ergänzungsbedürftig (obligatorische Öffnungsklauseln) oder zumindest ergänzungsoffen (fakultative Öffnungsklauseln) sind.[83] Für die Bewertung, ob ein datenschutzrechtlich vollständig determinierter Bereich vorliegt, ist entscheidend, ob im konkreten Fall der einschlägigen Vorschriften eine Gestaltungsoffenheit anzunehmen ist, nicht jedoch eine allgemeine Betrachtung des Regelungsbereichs.[84]

Der nationale Gesetzgeber hat für die Verarbeitung besonders sensibler personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO (s.u. B.II.3.) die Öffnungsklauseln in Art. 9 Abs. 2 lit. b, g, h und i DSGVO genutzt und § 22 BDSG formuliert.[85] Diese Vorschriften sind jedoch nicht relevant, wenn es um die Einwilligung zur Verwendung des Lichtbildes für den biometrischen Authentifizierungsprozess der eID-Funktion geht, sondern konkretisieren beispielsweise die Verwendung besonders sensibler Daten in der Gesundheitsvorsorge. Im konkreten Fall der Einwilligung in die Verarbeitung besonders sensibler personenbezogener Daten im Zusammenhang mit dem biometrischen Authentifizierungsverfahren der eID ist die Datenverarbeitung durch die DSGVO vollständig harmonisiert, was bedeutet, dass die Prüfung ausschließlich anhand der Unionsgrundrechte und der DSGVO zu erfolgen hat.[86]

2. Unionale grundrechtliche Prüfung Artt. 8, 7 GRCh

Der Prüfungsmaßstab für die Einwilligung in den biometrischen Datenabgleich i.R.d. eID-Funktion richtet sich allein nach Artt. 8, 7 GRCh.

83 *J. Kühling/J. Raab* in: J. Kühling/B. Buchner (Hrsg.), DS-GVO BDSG, 4. Aufl., München 2024, Einführung Rn. 128.

84 BVerfGE 152, 216 (247).

85 *E. Frenzel* in: B. Paal/D. Pauly (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Aufl., München 2021, Art. 9 DSGVO Rn. 50.

86 Vgl. zur Determinierung des Datenschutzrechts [*H. Gersdorf*, Unvereinbarkeit der Regelungen des GlüStV 2021-Entwurfs zur Limitdatei und Aktivitätsdatei mit Unionsgrundrechten und der DSGVO, ZfWG 2021, 19 (20 ff.)].

a) Persönlicher und sachlicher Schutzbereich

Ein Bürger, der die EUDI Wallet auf Basis der eID nutzt, wird als natürliche Person betrachtet und ist Träger von Grundrechten. Damit zählt er zu „jeder Person" gemäß den Artt. 8, 7 GRCh.

Der Schutz des Privatlebens in Art. 7 GRCh umfasst den Schutz der Privatsphäre.[87] Art. 8 GRCh schützt alle personenbezogenen Daten, also sämtliche Informationen über eine bestimmte oder bestimmbare natürliche Person.[88] Eine Einschränkung auf sensible Daten erfolgt hier nicht. Im Hinblick auf den Schutz eines Betroffenen vor einer biometrischen Datenverarbeitung im Kontext der eID bilden Art. 7 und 8 GRCh einen einheitlichen Schutzbereich.[89] Sie berücksichtigen auch die Achtung des Privatlebens bei der Verarbeitung personenbezogener Daten und entfalten daher bei der Auslegung der DSGVO ihre Wirkung.[90]

Das Lichtbild des Personalausweisregisters beinhaltet gemäß der Begriffsbestimmung aus Art. 4 Nr. 14 DSGVO biometrische Daten, welche personenbezogene Daten darstellen, die mit speziellen technischen Verfahren gewonnen werden und die eindeutige Identifizierung einer natürlichen Person ermöglichen oder bestätigen. Sie sind privat und nicht öffentlich. Die Verwendung dieser personenbezogenen Daten für das biometrische Authentifizierungsverfahren der eID eröffnet somit den Schutzbereich nach Artt. 8, 7 GRCh.

b) Grundrechtseingriff

Die Verarbeitung personenbezogener Daten i.R.d. biometrischen Authentifizierungsverfahrens für die EUDI Wallet könnte einen Eingriff in die Unionsgrundrechte nach Artt. 8, 7 GRCh darstellen.

In Achtung des Privatlebens[91] stellt die Verarbeitung personenbezogener Daten einen Eingriff in Artt. 8, 7 GRCh dar.[92] In der datenschutzrechtlichen

87 BVerfGE 152, 216 (255).
88 *H. Jarass* in: H. Jarass (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Aufl., München 2021, Art. 8 Rn. 6.
89 BVerfGE 152, 216 (254).
90 *H. Jarass*, GrCh (Fn. 88), Art. 8 Rn. 7.
91 *H. Bretthauer* (Fn. 64), § 2 Verfassungsrechtliche Grundlagen, Europäisches und nationales Recht Rn. 10.
92 Vgl. *J. Kühling/J. Raab*, DS-GVO BDSG (Fn. 83), Art. 2 Rn. 28.

Terminologie umfasst die Verarbeitung sämtliche Aktivitäten – unabhängig davon, ob sie automatisiert durchgeführt werden oder nicht. Dazu zählen das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreiten, Bereitstellen in anderer Form, Abgleichen, Verknüpfen, Einschränken, Löschen oder Vernichten personenbezogener Daten. Der Verarbeitungsbegriff ist demnach weit ausgelegt.[93] Die Verwendung des biometrischen Lichtbildes für den Authentifizierungsprozess der eID ist als Eingriff in Art. 8, 7 GRCh zu werten, da ein automatisierter Datenabruf des im Personalausweisregister gespeicherten Lichtbildes für einen biometrischen Datenabgleich erfolgt.

c) Eingriffsausschluss

Nach Art. 8 Abs. 2 GRCh ist ein Eingriff in das Recht auf Schutz personenbezogener Daten nicht rechtswidrig, wenn der Eingriff auf einer gesetzlichen Grundlage beruht oder auch, wenn eine Einwilligung der betroffenen Person vorliegt.[94]

Die Einwilligung stellt gemäß Art. 8 Abs. 2 S. 1 GRCh einen grundrechtlichen Erlaubnistatbestand für die Verarbeitung dar. Sie bedeutet keinen Grundrechtsverzicht[95] und ist auch kein Rechtfertigungsgrund[96] für Grundrechtseingriffe, sondern hebt schon tatbestandlich das Verbot der Verarbeitung personenbezogener Daten auf.[97] Wenn der Bürger wirksam in die Verarbeitung seiner personenbezogenen Daten i.R.d. biometrischen Authentifizierungsverfahrens der eID eingewilligt hat, liegt damit kein Grundrechtseingriff vor.

93 *H. Bretthauer* (Fn. 64), § 2 Verfassungsrechtliche Grundlagen, Europäisches und nationales Recht Rn. 17.

94 *H. Jarass*, GrCh (Fn. 88), Art. 8 Rn. 10.

95 *G.* Robbers, Der Grundrechtsverzicht: Zum Grundsatz „volenti non fit iniuria" im Verfassungsrecht, JuS 1985, 925 (928).

96 Die dogmatische Einordnung der Einwilligung wurde bisher nur kursorisch erörtert. Sie kann entweder als Eingriffsausschluss oder als Rechtfertigungsgrund wirken. In jedem Fall ist die Datenverarbeitung aufgrund der Entscheidung des Betroffenen zulässig [siehe dazu ausführlich *H. Bretthauer* (Fn. 64), § 2 Verfassungsrechtliche Grundlagen, Europäisches und nationales Recht Rn. 18 und 59)]. Im vorliegenden Fall wird die Einwilligung mangels Verhältnismäßigkeitsprüfung als Eingriffsausschuss charakterisiert [Vgl. *H. Jarass*, GrCh (Fn. 88), Art. 8 Rn. 10].

97 Vgl. *B. Stemmer* in: A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, 41. Ed., 1.5.2022, Art. 7 Rn. 25.

Voraussetzung für eine wirksame Einwilligung des Betroffenen in die Datenverarbeitung ist, dass die Einwilligung in Kenntnis der Sachlage erfolgt. Die Einwilligung kann lediglich für einen bestimmten Zweck erteilt werden. Vor der Erteilung der Einwilligung muss dieser Zweck so genau wie möglich festgehalten werden, da der Ausschluss des Eingriffs nur dann gilt, wenn auch „Treu und Glauben" entsprochen wird. Daran fehlt es stets bei rechtswidrigen Zwecken. Diesbezüglich normiert die GRCh die Anforderungen im Einzelnen jedoch nicht.[98] In Ausgestaltung der Artt. 8, 7 GRCh formt die DSGVO den Erlaubnistatbestand der Einwilligung genauer aus.[99]

Es wird im Folgenden geprüft, ob die Rahmenbedingungen der DSGVO für eine wirksame Einwilligung eingehalten werden können. Erteilt der Bürger eine wirksame Einwilligung zur Verarbeitung seiner personenbezogenen Daten für den biometrischen Authentifizierungsprozess i.R.d. EUDI Wallet-Nutzung, entfällt ein Eingriff in die unionalen Grundrechte der Artt. 8, 7 GRCh.

3. Zulässigkeit der Datenverarbeitung nach Art. 9 Abs. 2 lit. a Hs. 1 DSGVO

Die DSGVO unterscheidet zwischen „personenbezogenen" und „besonders sensiblen Daten", welche nach Art. 9 DSGVO nur unter strengen Anforderungen verarbeitet werden dürfen. Das Lichtbild des Personalausweises wird mit seinen biometrischen Merkmalen (gemäß Begriffsbestimmung nach Art. 4 Nr. 14 DSGVO; s.o. B.II.2.a.) zur eindeutigen Identifizierung einer natürlichen Person genutzt. Bei den biometrischen Daten handelt es sich um eine besondere Kategorie personenbezogener Daten nach Art. 9 Abs. 1 DSGVO.[100]

Durch die Verarbeitung der Kategorie „besonders sensibler personenbezogener Daten" geht ein höheres Gefährdungspotenzial für den Persönlichkeitsschutz des Bürgers aus. In Art. 9 Abs. 1 DSGVO wurde zwar das generell geltende Verbotsprinzip[101] im Datenschutzrecht für besonders sensible

98 *H. Jarass*, GrCh (Fn. 88), Art. 8 Rn. 11.

99 *I. Conrad/M. Tinnefeld*, Die selbstbestimmte Einwilligung im europäischen Recht, ZD 2018, 391 (392).

100 *M. Kaulartz/A. Schmid/F. Müller-Eising,* Metaverse (Fn. 8*),* 526.

101 Art. 5 DSGVO enthält die Grundsätze für die Verarbeitung personenbezogener Daten und ist somit die zentrale Norm der DSGVO. Dem Grundsatz der Rechtmäßigkeit nach Art. 5 Abs. 1 lit. a Var. 1 DSGVO wird das „Verbotsprinzip" entnommen.

Daten wiederholt, damit wurden aber nur bestimmte Datenkategorien abschließend als besonders schutzbedürftig benannt[102] und klargestellt, dass die Verarbeitung der biometrischen Daten für die Online-Ausweisfunktion nur mit einem Ausnahmetatbestand des Art. 9 Abs. 2 DSGVO Rechtfertigung erfahren kann.[103] Von diesen Erlaubnistatbeständen muss zumindest einer verwirklicht sein, damit das Verbot nicht greift.[104] Hier normiert Art. 9 Abs. 2 lit. a Hs. 1 DSGVO auch die Einwilligung.

Für die Einwilligung hält dann Art. 4 Nr. 11 DSGVO eine Legaldefinition bereit. Danach ist eine Einwilligung jede freiwillige, für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung. Diese kann in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung erfolgen, mit der der Betroffene zu verstehen gibt, dass er mit der Verarbeitung, der ihn betreffenden personenbezogenen Daten, einverstanden ist (EG 42 DSGVO).[105]

a) Problem der Freiwilligkeit beim Ungleichgewicht Staat und Bürger

Eine Wirksamkeitsvoraussetzung der Einwilligung ist die Freiwilligkeit nach Art. 7 Abs. 4 DSGVO. Zwischen Bürgern und dem staatlichen Anbieter der eID-Funktion besteht ein strukturelles Ungleichgewicht, da die Behörde als Hoheitsträger auftritt (EG 43 S. 1 DSGVO). Deshalb ist eine Einwilligung gegenüber einer Behörde in der Regel nicht freiwillig.[106] Die DSGVO will verhindern, dass Bürger durch die Machtasymmetrie zur Zu-

Dieses Prinzip meint ein Verbot der Datenverarbeitung mit Erlaubnisvorbehalt. [*R. Stenzel* in: S. Gierschman/K. Schlender/R. Stentzel/W. Veil-Buchholtz (Hrsg.), Datenschutzgrundverordnung, Köln 2018, Art. 5 Rn. 24].

102 *J. Botta*, Datenschutz bei E-Learning-Plattformen, Rechtliche Herausforderungen digitaler Hochschulbildung am Beispiel der Massive Open Online Courses (MOOCs), Baden-Baden 2020, S. 180 (181).

103 Vgl. *E. Frenzel*, DS-GVO BDSG (Fn. 85), Art. 9 DSGVO Rn. 18.

104 *P. Reimer*, Verwaltungsdatenschutzrecht, Das neue Recht für die behördliche Praxis, Baden-Baden 2019, Rn. 114.

105 *U. Dammann*, Erfolge und Defizite der EU-Datenschutzgrundverordnung – Erwarteter Fortschritt, Schwächen und überraschende Innovationen, ZD 2016, 307 (308).

106 *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, DSGVO – BDSG Text und Erläuterungen, 2020, S. 1 (29).

stimmung gedrängt werden.[107] Eine solche coactus-volui-Struktur[108] überschattet die Einwilligung eines Bürgers in die Verarbeitung seiner besonders sensiblen personenbezogenen Daten für den Authentifizierungsprozess üblicherweise nicht.[109]

In Ausnahmefällen kann eine Einwilligung als Rechtsgrundlage dienen, wenn die Datenverarbeitung im Zusammenhang mit den Aufgaben der Behörde steht und den Betroffenen keine Nachteile bei Verweigerung entstehen. Die Bürger müssen frei entscheiden können, ob sie das Behörden-Angebot für die Online-Ausweisfunktion nutzen wollen oder nicht.[110] Die biometrische Authentifizierung ist bei der eID als zusätzliche Option neben der PIN-Eingabe vorgesehen, deren Nutzung dem Bürger freisteht. Dadurch wird kein strukturelles Ungleichgewicht zwischen Bürger und Behörde geschaffen. Für die freiwillige Einwilligung muss der Bürger auch die Tragweite seiner Erklärung verstehen.[111] Er muss wissen, welche Daten an wen und zu welchem Zweck übermittelt werden.[112] Art. 5 Abs. 1 lit. a Var. 3 DSGVO unterstützt dies durch das Transparenzprinzip, auf das im Folgenden eingegangen wird.

b) Das Transparenzprinzip i.R.d. Einwilligung

Personen können nur dann über ihre personenbezogenen Daten entscheiden, wenn sie auch selbst wissen, wer wann was über sie weiß und zudem, was der Verantwortliche mit ihren persönlichen Daten plant oder wie er sie bereits verarbeitet hat.[113] Zu dieser Absehbarkeit trägt das Transparenzprinzip nach Art. 5 Abs. 1 lit. a Var. 3 DSGVO bei. Dazu ergänzt EG 39 S. 3 DSGVO die Nachvollziehbarkeit. Alle Informationen und Mitteilungen zur Verarbeitung personenbezogener Daten im Kontext des bio-

107 Ausführlicher *M. Peifer*, Die Datenschutz-Grundverordnung aus Sicht der öffentlichen Verwaltung, PinG 2016, 222 (226).

108 *N. Bethge*, Die verfassungsrechtliche Zulässigkeit des Grundrechtsverzichts, Hamburg 2014, S. 165 (165 ff.).

109 Vgl. *M. Martini/M. Wenzel*, "Once only" (Fn. 77), 753.

110 *M. Martini/M. Wenzel*, "Once only" (Fn. 77), 753.

111 *E. Ehmann* in: E. Ehmann/M. Helfrich (Hrsg.), EG-Datenschutzrichtlinie, Köln 1999, Art. 2 Rn. 69.

112 *E. Frenzel* (Fn. 85), Art. 49, Rn. 6.

113 *D. Caliebe/I. Sommer*, Betroffenenrechte: Transparenz als Werkzeug und Voraussetzung der informationellen Selbstbestimmung, in: R. Jabowski/H. Lühr/S. Smentek (Hrsg.), Handbuch Digitale Verwaltung, Wiesbaden 2018, S. 225 (234).

metrischen Authentifizierungsverfahrens der eID-Funktion sind demnach in leicht zugänglicher und verständlicher sowie in klarer und einfacher Sprache abzufassen. An diesen Willen des Unionsgesetzgebers muss sich auch das sog. Amtsdeutsch messen lassen.

c) Erfüllung der Betroffenenrechte

Überdies wird das Transparenzprinzip durch Artt. 12–15 DSGVO[114] hergestellt. Art. 12 DSGVO statuiert zunächst einen „allgemeinen Teil" für die Informationspflichten. Art. 13 DSGVO regelt die Informationspflichten bei Direkterhebung[115] und Art. 14 DSGVO die indirekte Erhebung[116] während Art. 15 DSGVO das Auskunftsrecht bestimmt. Dieses reagiert auf Informationsbegehren der betroffenen Personen.[117]

Die DSGVO normiert im Unterschied zum früheren deutschen Datenschutzrecht keinen Direkterhebungsgrundsatz,[118] der dazu verpflichte die Daten bei der betroffenen Person selbst zu erheben. Sie enthält auch diesbezüglich keine Öffnungsklausel.[119] Damit steht es dem biometrischen Authentifizierungsprozess frei, die Informationen aus dem Personalausweisregister zu nutzen, sofern der Pflicht nachgekommen wird, den Bürger über die Datenerhebung zu informieren (Art. 14 Abs. 2 DSGVO).[120]

Die oben genannten Betroffenenrechte sind bei der biometrischen Datenverarbeitung der eID-Funktion zu beachten.

114 Der nationale Gesetzgeber hat auf Grundlage der Öffnungsklausel des Art. 23 DSGVO die Betroffenenrecht nach Artt. 12–15 DSGVO nationalrechtlich mit §§ 29, 32, 33 und 34 BDSG ausgeformt. Diese haben jedoch im Rahmen dieser Arbeit keine Relevanz, da die normierten Ausnahmen für den biometrischen Datenabgleich des Authentifizierungsprozesses der Online-Ausweisfunktion in der Regel nicht einschlägig sind und daher an dieser Stelle nicht tiefer behandelt werden.

115 *D. Caliebe/I. Sommer*, Betroffenenrechte (Fn. 113), S. 235.

116 *D. Caliebe/I. Sommer*, Betroffenenrechte (Fn. 113), S. 236.

117 *D. Caliebe/I. Sommer*, Betroffenenrechte (Fn. 113), S. 234.

118 So auch *B. Buchner*, Die Einwilligung im Datenschutzrecht, DuD 2016, 155 (156).

119 *J. Kühling/M. Martini*, Die Datenschutz-Grundverordnung und das nationale Recht, Greifswald 2016, S. 301 (316).

120 *J. Kühling/M. Martini*, Datenschutz-Grundverordnung (Fn. 119), S. 316.

d) Entbündelungsgebot und Opt-in-Gebot bei Gestaltung der Einwilligung

Wenn die Verwaltung Daten auf der Grundlage einer Einwilligung verarbeiten will, muss sie „entbündelte" Einwilligungen zulassen. Das bedeutet, dass sie für verschiedene Verarbeitungsvorgänge, bei denen das biometrische Authentifizierungsverfahren Anwendung finden soll, auch verschiedene Erklärungen gestatten muss, statt den Bürgern eine pauschale Einwilligung abzuverlangen (EG 43 S. 2 DSGVO). Pauschale Einwilligungen sind oft nicht ausreichend konkret und nachvollziehbar. Grundrechtsschonender und im Lichte des Kopplungsverbots angezeigt (Art. 7 Abs. 4, EG 43 S. 2 DSGVO) ist hier ein differenzierendes Modell,[121] welches den Bürger bei jeder Nutzung des biometrischen Authentifizierungsprozesses auffordert, seine Einwilligung zu aktualisieren.

Da Art. 9 Abs. 2 lit. a Hs. 1 DSGVO nur eine ausdrückliche Einwilligung der betroffenen Person gestattet, ist nur eine Opt-in-Lösung zulässig.[122] Vorausgefüllte Kästchen (Opt-out) sind unzulässig.[123] Die Aufforderung zur Einwilligung beim biometrischen Authentifizierungsprozess muss zudem klar und knapp erfolgen (EG 32 S. 6 DSGVO).

e) Widerruf der Einwilligung

Die Einwilligung zum biometrischen Datenabgleich i.R.d. Online-Ausweisfunktion kann der Bürger zu jedem Zeitpunkt mit ex-nunc-Wirkung widerrufen (Artt. 7 Abs. 3 S. 1, Abs. 3 S. 2 DSGVO). Darüber muss der Bürger vor der Zustimmung zur Nutzung seiner Daten informiert werden (Art. 7 Abs. 3 S. 3 DSGVO). Die Widerrufsmöglichkeit darf auch nicht unsachgemäß (z. B. durch Zwang zur Angabe von Gründen) erschwert werden, sondern sie muss „so einfach wie die Erteilung der Einwilligung" gestaltet (Art. 7 Abs. 3 S. 4 DSGVO) sein.[124]

4. Zwischenfazit

Beim automatisierten Datenabgleich mit dem Lichtbild aus dem Personalausweisregister zur Authentifizierung per Online-Ausweisfunktion werden

121 *M. Martini/M. Wenzel*, "Once only" (Fn. 77), 753.
122 *J. Kühling/M. Martini*, Die Datenschutz-Grundverordnung (Fn. 119), S. 451.
123 *J. Kühling/M. Martini*, Die Datenschutz-Grundverordnung (Fn. 119), S. 451.
124 *M. Martini/M. Wenzel*, "Once only" (Fn. 77), 754.

biometrische Daten gemäß Art. 9 Abs. 1 DSGVO verarbeitet. Zur Wahrung der unionsgrundrechtlichen Schranken und zur rechtlichen Zulässigkeit der Verwendung des Lichtbildes im Authentifizierungsprozess ist mindestens die Einwilligung der Nutzenden nach Art. 9 Abs. 2 lit. a Hs. 1 DSGVO erforderlich und in angesicht der datenschutzrechtlichen Prüfung möglich.

C. Schluss

Das Metaverse stellt eine Verschmelzung der virtuellen und physischen Welt dar und wird als nächste Iteration des Internets betrachtet.[125] Die EU-Kommission plant, die digitale Kompetenz der Unionsbürger zu stärken und eine Governance für virtuelle Welten zu entwickeln.[126] Bis 2030 sollen auch sichere digitale Identitäten das Rückgrat einer vernetzten Gesellschaft bilden und den Zugang zu verschiedenen digitalen Diensten im Metaverse erleichtern.[127]

Angesichts der Fragmentierung des Marktes für Identitätsdienste und der aktuellen Umbrüche im Regulierungsrahmen für digitale Identitäten ist eine Prognose zur weiteren Entwicklung digitaler Identitäten im Metaverse schwierig. Voraussetzungen für die breite Akzeptanz digitaler Identitätslösungen wie der EUDI Wallet sind insbesondere eine im Einklang mit der Sicherheit stehende Nutzerfreundlichkeit und breite Einsatzmöglichkeiten. Entscheidend ist, diese teilweise im Widerstreit stehenden Zielsetzungen in einen sachgerechten Ausgleich einer staatlichen eID zu bringen.[128]

Auch wenn es seit der Einführung der eID-Karte keinen nennenswerten Sicherheitsvorfall gegeben hat,[129] zeigt das Beispiel der eID-Funktion, dass die komplexe Umsetzung eines hohen Sicherheitsniveaus die Nutzerakzeptanz beeinträchtigt. Je mehr Endnutzer den Identifizierungsdienst in Anspruch nehmen, desto attraktiver wird dieser für Drittanbieter und umgekehrt. Aus Sicht der Drittanbieter wird die Motivation zur Implementierung der eID durch die geringen Nutzungszahlen beeinträchtigt. Zudem besteht Optimierungsbedarf bei der organisatorischen, technischen und finanziellen Integration, was hohe Eintrittsbarrieren zur Folge hat. Orga-

125 *Kompetenzzentrum Öffentliche IT, Metaversum (Fn. 3).*
126 *M. Martini/J. Botta*, Metaversum (Fn. 4), 892.
127 *CDU/CSU-Fraktion im Deutschen Bundestag,* eIDAS 2.0 (Fn. 19), S. 2.
128 *Bundesministerium des Innern und für Heimat,* Architecture Proposal (Fn. 27), S. 35.
129 *Bundesministerium des Innern und für Heimat,* Architecture Proposal (Fn. 27), S. 35.

nisatorisch ist beispielsweise erforderlich, dass jeder Service beschrieben und beantragt wird. Auch der technische Integrationsaufwand ist erheblich, da die eID-Architektur den Betrieb eines eigenen ID-Servers oder einen Vertrag mit einem ID-Server-Betreiber voraussetzt. Die Kosten für den Betrieb des Servers sind intransparent und für den Dienstanbieter schwer kalkulierbar. Darüber hinaus bietet das anscheinend schwach ausgeprägte eID-Plattformmanagement keine detaillierten Informationen zu Kosten oder Entwicklungsperspektiven. Daher sind entscheidende Aspekte für die Zunahme von Onlinediensten in Verbindung mit der eID nur begrenzt vorhanden.[130] Hier könnte jedoch die in der eIDAS 2.0 vorgesehene Akzeptanzpflicht einen Beitrag leisten, da sich Drittanbieter trotz aller organisatorischen, technischen und finanziellen Herausforderungen der Implementierung der EUDI Wallet nicht entziehen können. Dadurch könnte die eID i.R.d. EUDI Wallet bei der Inanspruchnahme von Onlinediensten eine kritische Masse an Nutzern erreichen und somit auch im Metaverse eine wichtige Rolle spielen.[131]

Für die eID-nutzenden Onlinedienste trägt der im Beitrag dargestellte Ansatz des biometrischen Authentifizierungsverfahrens zur Benutzerfreundlichkeit und damit zur Erhöhung der Nutzerakzeptanz bei. Die datenschutzrechtliche Prüfung des biometrischen Authentifizierungsprozesses für die EUDI Wallet zeigt, dass beim automatisierten Datenabgleich mit dem Lichtbild aus dem Personalausweisregister strikte rechtliche Rahmenbedingungen eingehalten werden müssen. Biometrische Daten gelten gemäß Art. 9 Abs. 1 DSGVO als besonders schützenswert und ihre Verarbeitung erfordert mindestens eine explizite und informierte Einwilligung der Nutzenden nach Art. 9 Abs. 2 lit. a Hs. 1 DSGVO. Im Beitrag wurde dargelegt, dass die Einwilligung für die biometrische Authentifizierung sowohl datenschutz- als auch grundrechtskonform erfolgen kann. Sie muss freiwillig, transparent und jederzeit widerrufbar sein, um den hohen Anforderungen des Datenschutzes gerecht zu werden. Zusätzlich könnte eine Ermächtigungsgrundlage über eine verhältnismäßige Zweckänderung der Verwendung des Lichtbildes gegeben sein oder idealerweise eine eigene Rechtsgrundlage für die Nutzung des biometrischen Authentifizierungsverfahrens ausgestaltet werden. Um das Face-ID-Verfahren auch für Touch-ID-Verfahren zu erweitern, müssen die im Chip des Personalausweises

130 *P. Parycek*, Stellungnahme Digitale Identitäten, unter: https://www.bundestag.de/resource/blob/902144/218654a68c61fdb639c383f2fcb8fe70/Parycek.pdf, S. 3 (4 f.).

131 *C. Busch,* § 16 Digitale Identitäten (Fn. 20), S. 303.

erfassten Fingerabdrücke in das Personalausweisregister überführt werden. Dies gilt es in einem gesonderten rechtlichen Gutachten zu prüfen.

Die Speicherung des Iris-Scan für Ausweisdokumente wurde bereits früher für Authentifizierungsverfahren an Flughäfen diskutiert.[132] Mit der Verwendung von Virtual-Reality-Brillen eröffnet sich ein neuer Anwendungsfall. Obwohl der Zugang zum Metaverse über ein Smartphone erfolgen kann, lässt sich nur durch Virtuelle Realität (Virtual Reality, VR) vollständig in die computergenerierte Wirklichkeit des Metaverse eintauchen.[133] Daher sollte diese technologische Entwicklung auch in einen einfachen und sicheren Authentifizierungsprozess der eID-Funktion Berücksichtigung finden.

Um das Potenzial der staatlichen elektronischen Identität zu heben, müssen mit ihr auch langfristige und umfangreiche Investitionsentscheidungen sowie eine Vision für digitale Identitäten einhergehen, die in eine Strategie zur Umsetzung münden. Dazu muss die eIDAS 2.0 vollumfänglich und in allen Facetten in das OZG und die Registermodernisierung integriert werden.[134]

132 *DER SPIEGEL*, Biometrischer Reisepass kostet 59 Euro, v. 1.6.2005 unter: https://www.spiegel.de/reise/aktuell/epass-biometrischer-reisepass-kostet-59-euro-a-358564.html.

133 Vgl. *Bitkom e.V.,* Wegweiser (Fn. 6), S. 14.

134 *Bitkom e.V.,* eIDAS Leitfaden (Fn. 25), S. 13 f.

Virtuelle Zwillinge und Diabetes

*David M. Schneeberger**

A. Einleitung

Diabetes betrifft einen von zehn Erwachsenen weltweit und führte 2021 zu 6,7 Millionen Todesfällen. Im selben Jahr erzeugte die Krankheit mindestens 966 Milliarden Dollar an Gesundheitsausgaben.[1] Diabetes ist damit ein Problem, das die gesamte Gesellschaft, verstärkt jedoch ärmere Länder, betrifft. Eine personalisierte Behandlung, die mit dem verbreiteten one-size-fits-all-Ansatz bricht, könnte den Behandlungserfolg verbessern. An diesem Schnittpunkt trifft das Metaversum auf die Medizin. So lässt sich die physische Welt, bspw. Körperbestandteile oder ganze Patienten, digital bzw. dreidimensional nachbilden.[2] Eine solche „Nachbildung" wird als „virtueller" bzw. „digitaler Zwilling" bezeichnet.[3] Anhand dieser virtuellen Abbildungen können Therapien erprobt und Änderungen beobachtet werden. Auf europäischer Ebene wird dieser Ansatz bspw. durch das European-Virtual-Human-Twin-Projekt (EDITH) verfolgt.[4]

Diesem Ziel, den Behandlungserfolg durch Rückgriff auf virtuelle Zwillings-Modelle zu steigern, hat sich auch das dAIbetes-Projekt verschrieben. Dieser Beitrag gibt einen Überblick über erste Rechtsfragen, die im Zuge des Anfang 2024 begonnenen Projektes aufgeworfen wurden. Er behandelt nach einer kurzen Vorstellung des Projektes (B.) ausgewählte rechtliche Aspekte, darunter Fragen des Datenschutzrechtes (C.), insb. der gemeinsamen Verantwortlichkeit, von Synergien und Friktionen zwischen Medi-

* Dieser Beitrag wurde durch das Projekt „dAIbetes – Prediction of treatment outcome in type 2 diabetes" (Horizon Europe Research and Innovation Programme Grant Agreement no. 101136305) gefördert.

1 *IDF*, IDF Diabetes Atlas, diabetesatlas.org/ (abgerufen am 13.12.2024).

2 *T. Meier*, Medizinprodukte für das Metaverse, MPR 2022, 134 (137).

3 *R. Laubenbacher/B. Mehrad/I. Shmulevich/N. Trayanova*, Digital twins in medicine, nature computational science 2024, 184 (184).

4 *EDITH*, edith-csa.eu/edith/ (abgerufen am 13.12.2024).

zinprodukteverordnung (MPVO)[5] und der Verordnung über Künstliche Intelligenz (KI-VO)[6] (D.) und des Cybersicherheitsrechtes (E.). Eine abschließende Conclusio (F.) präsentiert die wichtigsten Ergebnisse.

B. Das dAIbetes-Projekt

I. Einleitung

Ein großes Problem beim Trainieren von Machine-Learning-Modellen im Gesundheitsbereich liegt im Mangel an hochqualitativen Trainingsdaten. Selbst wenn diese existieren, liegen sie oft verstreut innerhalb und außerhalb von Europa vor. Eine Zusammenfügung dieser großen Mengen äußerst sensibler personenbezogener Daten wirft häufig (datenschutz-)rechtliche[7] und ethische[8] Fragen auf.

Als Lösungsansatz hat sich das dAIbetes-Projekt das Ziel gesetzt, federated (machine) learning zu verwenden, um eine Gesundheitsdatenplattform zu errichten, die das rechtssichere Training von virtuellen Zwillings-Modellen für Typ 2 Diabetes ermöglicht. Durch die Integration von Big Data (ca. 800 000 Patientendaten) soll im Sinne der personalisierten Medizin eine bessere Prädiktion des Behandlungserfolges ermöglicht werden.[9]

Die Patientendaten werden dabei von sechs klinischen Partnern, wobei fünf in Europa angesiedelt sind, bereitgestellt. Als amerikanischer Partner ist ein Partner (im Folgenden Partner 1) als klinischer Partner und Leiter des Arbeitspaketes Datenharmonisierung beteiligt.[10] Diese europäisch-ame-

5 Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) 178/2002 und der Verordnung (EG) 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates (Medizinprodukteverordnung), ABl. L 2017/117, 1.

6 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) 300/2008, (EU) 167/2013, (EU) 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), ABl. L 2024/144, 1.

7 Statt vieler *D. Linardatos*, Intelligente Medizinprodukte und Datenschutz (Teil 1), CR 2022, 367.

8 *G. Rubeis*, Ethics of Medical AI, Cham 2024, S. 91 ff.

9 dAIbetes, daibetes.eu/ (abgerufen am 13.12.2024).

10 Work packages, daibetes.eu/teams-partnes/work-packages (abgerufen am 13.12.2024).

rikanische Zusammenarbeit wirft komplexe Rechtsfragen des Anwendungsbereiches von Europarecht auf, die auch auf andere Konstellationen übertragbar sein könnten.

Das Projekt beinhaltet eine abschließende Validierungsstudie, mit der die eingesetzten virtuellen Zwillinge evaluiert werden sollen. Die Studie ist dabei so konzipiert, dass die Ergebnisse des Modells die Behandlung nicht beeinflussen, da das Gesundheitspersonal dafür „blind" ist, d.h. nicht über das Ergebnis informiert wird. Die Validierungsstudie wird vom zweiten amerikanischen Partner (im Folgenden Partner 2) geleitet.[11]

II. Federated learning

Ein Kernelement des Projektes ist federated learning. Beim federated learning werden, anstatt alle Daten von verschiedenen Standorten auf einem zentralen Server zu „poolen", von den Beteiligten dezentrale (sog. lokale) Modelle trainiert, die daraufhin vom sog. „Koordinator" aggregiert und zu einem globalen Modell zusammengefügt werden. Dieses wird wiederum den Beteiligten zur Verfügung gestellt.[12]

Vorteil ist, dass nicht die (personenbezogenen) Daten, sondern nur die Parameter der Modelle ausgetauscht werden. Die Patientendaten verlassen damit nicht den jeweiligen Beteiligten (z.B. die Krankenanstalt).[13] Da zwischen den aggregierten Daten und den konkreten Patienten keine „Verbin-

11 Work packages, daibetes.eu/teams-partnes/work-packages (abgerufen am 13.12.2024).

12 *J. Baumbach/M. M. K. Majdabadi/C. C. Saak/M. Bakhtiari/N. Probul*, Föderiertes Lernen, in: G. Buchholtz/L. Hering (Hrsg.), Digital Health und Recht, Berlin 2024, S. 263 (264 ff.); *X. Lareo*, Federated Learning, edps.europa.eu/press-publications/publications/techsonar/federated-learning_en (abgerufen am 13.12.2024). Der federated-learning-Ansatz wurde bereits im Vorgängerprojekt FeatureCloud auf seine Tauglichkeit für (bio-)medizinische Anwendungen erprobt, *Baumbach/Majdabadi/Saak/Bakhtiari/Probul,* Lernen (Fn. 12), S. 280 ff.; J. *Matschinske/J. Späth/M. M. Bakhtiari/N. Probul/M. M. K. Majdabadi/R. Nasirigerdeh/R. Torkzadehmahani/A. Hartebrodt/B.-A. Orban/S.-J. Fejér/O. Zolotareva/S. Das/L. Baumbach/J. K. Pauling/O. Tomašević/B. Bihari/M. Bloice/N. C. Donner/W. Fdhila/T. Frisch/A.-C. Hauschild/D. Heider/A. Holzinger/W. Hötzendorfer/J. Hospes/T. Kacprowski/M. Kastelitz/M. List/R. Mayer/M. Moga/H. Müller/A. Pustozerova/R. Röttger/C. C. Saak/A. Saranti/H. H. H. W. Schmidt/C. Tschohl/N. K. Wenke/J. Baumbach*, The FeatureCloud Platform for Federated Learning in Biomedicine, Journal of medical Internet research 2023, e42621.

13 *A. Brauneck/L. Schmalhorst/M. M. K. Majdabadi/M. Bakhtiari/U. Völker/J. Baumbach/L. Baumbach/G. Buchholtz*, Federated Machine Learning, Privacy-Enhancing

dungslinie“ mehr gezogen werden kann, ist der Anwendungsbereich der DSGVO[14] – wenn zusätzliche Schutzmaßnahmen getroffen werden – in Bezug auf die Modelle ausgeschlossen.[15]

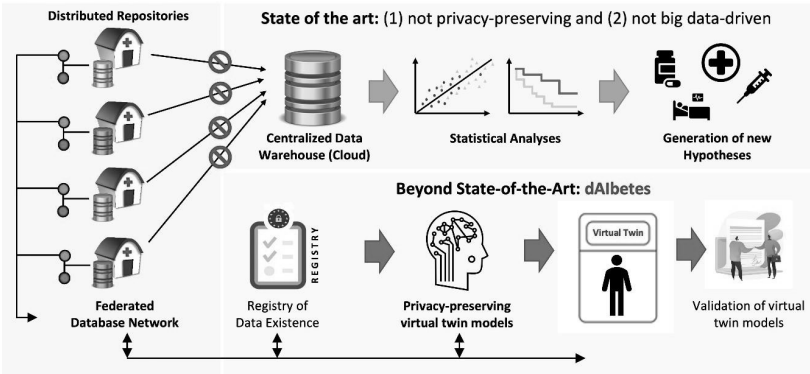


Abbildung 1 dAIbetes Projekt-Visions-Diagramm (daibetes.eu/as-a-whole)

III. Virtuelle Zwillinge

Ein Hinweis zu Beginn: Derzeit besteht keine Einigkeit über den Begriff „virtueller Zwilling“, der als Bezeichnung für einfache Modelle bis hin zu vollen digitalen Abbildungen von Patienten, die kontinuierlich oder periodisch aktualisiert werden, verwendet wird.[16]

Die European Virtual Human Twins Initiative schlägt bspw. folgende Definition vor: „A virtual human twin (VHT) is a digital representation

Technologies, and Data Protection Laws in Medical Research, Journal of medical Internet research 2023, 1 (3 f.).

14 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 2016/119, 1.

15 *D. Linardatos*, Intelligente Medizinprodukte und Datenschutz (Teil 2), CR 2022, 571 (574).

16 *Laubenbacher/Mehrad/Shmulevich/Trayanova*, twins (Fn. 3), 185; vgl. *L. Wright/S. Davidson*, How to tell the difference between a model and a digital twin, Adv. Model. and Simul. in Eng. Sci 2020, 1. Teilweise wird auch, ohne klare Abgrenzung, der Begriff „digitale Zwillinge“ verwendet.

of a human health or disease state. They refer to different levels of human anatomy (e.g. cells, tissues, organs or organ systems)."[17]

Solche Zwillinge können die „Innenwelt" von Patienten, von Gewebe und Organen bis hin zur molekularen Struktur, abbilden.[18] Derzeit wird häufig das digitale Ebenbild einzelner Organe oder Körperteile erstellt.[19] In Zukunft sollen umfassendere virtuelle Zwillinge von individuellen Patienten möglich sein.[20]

Im Rahmen von dAIbetes wird nicht jeder Patient durch einen eigenen Zwilling repräsentiert. So soll ein Gesamtmodell – der genaue Modelltyp stand zum Zeitpunkt der Einreichung noch nicht fest – die notwendigen Zusammenhänge erfassen und personalisierte Behandlungsempfehlungen ausgeben. Als Ergebnis soll der Einfluss eines Medikaments innerhalb eines spezifischen Zeitraums auf den HbA1c-Wert, der den Blutzuckerspiegel der vorangegangenen vier bis sechs Wochen widerspiegelt,[21] herangezogen werden.[22]

C. Datenschutzrechtliche Aspekte

I. Gemeinsame Verantwortlichkeit

Federated learning wirft komplexe Fragen in Bezug auf die datenschutzrechtliche Verantwortlichkeit auf. Verantwortlicher ist nach Art. 4 Nr. 7 DSGVO bekanntlich „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Wie der Wortlaut schon andeutet, kann diese Entscheidung auch von mehreren Verantwortlichen gemeinsam getroffen werden,

17 European Virtual Human Twins Initiative, digital-strategy.ec.europa.eu/en/policies/virtual-human-twins (abgerufen am 13.12.2024).

18 *P. Coveney/R. Highfield*, Virtual You. How Building Your Digital Twin Will Revolutionize Medicine and Change Your Life, Princeton 2023, S. 3.

19 *T. Meier*, § 27 Medizin- und Medizinprodukterecht, in H. Steege/K. Chibanguza (Hrsg.), Metaverse, Baden-Baden 2023, S. 439 (442 f.).

20 *Coveney/Highfield*, You (Fn. 18), S. 14 ff.

21 Hämoglobin A1c (HBA1C), gesundheit.gv.at/labor/laborwerte/organe-stoffwechsel/hba1c.html (abgerufen am 13.12.2024).

22 Auskunft von A. Tanzanakis, der im Rahmen von Arbeitspaket 3 unter der Leitung von B. Eskofier von der FAU Erlangen-Nürnberg maßgeblich an der Modellentwicklung beteiligt ist.

wodurch eine „gemeinsame Verantwortlichkeit" (im Englischen *joint controllership*) entsteht (Art. 26 DSGVO).[23] Konkretisierend führt der Europäische Datenschutzausschuss (EDSA) in seinen Leitlinien aus: „Das übergeordnete Kriterium für das Vorliegen gemeinsamer Verantwortlichkeit ist die gemeinsame Beteiligung von zwei oder mehr Stellen an der Festlegung der Zwecke und Mittel einer Verarbeitung."[24]

Zu Fragen der gemeinsamen Verantwortlichkeit sind inzwischen, mit zunehmender Frequenz, eine Reihe von Urteilen des EuGH ergangen, die das Konzept konkretisieren. Er vertritt ein extensives Verständnis der gemeinsamen Verantwortlichkeit.[25] So müssen gemeinsam Verantwortliche nicht zwingend den (exakt) selben Zweck verfolgen; sich ergänzende bzw. komplementäre Entscheidungen über die Zwecke und Mittel genügen.[26] Ein Verantwortlicher kann auch mehr Einfluss haben als ein anderer.[27] Bereits wenn ein Beteiligter die Mittel (z.B. die Nutzung einer Plattform) definiert und diese von den anderen Beteiligten angenommen werden, kann eine gemeinsame Verantwortlichkeit vorliegen.[28] Ein marginaler Einfluss auf die Mittel kann ausreichen.[29] Dabei indiziert ein „Eigeninteresse", dass es sich um eine gemeinsame Verantwortlichkeit handelt.[30] Dieses liegt jedoch in

23 M.w.N. *J. Marosi*, (Gem-)Einsame Verantwortlichkeit im Datenschutzrecht. Voraussetzungen, Folgen, Perspektiven, Trier 2024, S. 179 ff.; *T. Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO. Unter besonderer Berücksichtigung von Internetsachverhalten, Baden-Baden 2021, S. 45 ff.; *R. Schneider*, Gemeinsame Verantwortlichkeit. Entstehung, Ausgestaltung und Rechtsfolgen des Innenverhältnisses gemäß Art. 26 DSGVO, Wiesbaden 2021, S. 34 ff.

24 *EDSA*, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO Version 2.0, 2021, S. 22, edpb.europa.eu/system/files/2023–10/edpb_guidelines_202007_controllerprocessor_final_de.pdf.

25 *C. Millard*, At this rate, everyone will be a [joint] controller of personal data! IDPL 2019, 217.

26 *V. Halim/J. Marosi*, Status Quo der EuGH-Rechtsprechung zu Personenbezug und gemeinsamer Verantwortlichkeit, CR 2024, 297 (303); *J. Hartung* in: J. Kühling/B. Buchner (Hrsg.), DS-GVO/BDSG. Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 4. Auflage, München 2024, Art. 26 DSGVO Rn. 17; *J. Marosi*, Halbherzig beauftragt ist gemeinsam verantwortet, DSB 2024, 46 (47).

27 *J. Dumortier/P. Gryffroy* in: I. Spiecker gen. Döhmann/V. Papakonstantinou/G. Hornung/P. Hert (Hrsg.), General Data Protection Regulation. Article-by-Article Commentary, Baden-Baden/München/Oxford 2023, Art. 26 GDPR Rn. 37.

28 *K.-U. Plath* in: K.-U. Plath (Hrsg.), DSGVO/BDSG/TTDSG. Kommentar, 4. Auflage, Köln 2023, Art. 26 DSGVO Rn. 11.

29 *M. Finck*, Cobwebs of control, IDPL 2021, 333 (335).

30 EuGH C-683/21, *Nacionalinis visuomenės sveikatos centras,* ECLI:EU:C:2023:949 Rn. 43; *Halim/Marosi,* Status Quo (Fn. 26), 304; *Marosi,* Halberzig (Fn. 26), 46.

Projekten typischerweise bei allen Partnern vor, die gemeinsam, bspw. im Steering Committee, grundlegende Entscheidungen treffen.[31] So werden in der Literatur bereits die gemeinsame Nutzung der Ergebnisse eines Projektes und gemeinsame IP-Rechte als Indikatoren für eine gemeinsame Verantwortlichkeit gewertet.[32] Um das extensive Ausmaß einer gemeinsamen Verantwortlichkeit in Projekten wieder zurückzudrängen, wurden bspw. „Filtermodelle" vorgeschlagen.[33] Als wichtiger Punkt ist es nicht notwendig, dass jeder Verantwortliche Zugang zu den Daten hat.[34] So reichte die Organisation von Verkündigungstätigkeiten durch eine Religionsgemeinschaft – die keinen Zugriff auf die Daten hatte – zur Qualifizierung als gemeinsam Verantwortlicher aus.[35] Auch der Einfluss auf die Entwicklung einer COVID-19-Tracking-App und die dafür vorgesehene Verarbeitung durch Bestimmung der Parameter führte zur Einstufung als gemeinsam Verantwortlicher.[36]

Aufgrund der dargestellten extensiven Rspr. erscheint es prima facie naheliegend, dass das gesamte dAIbetes-Konsortium – da es gemeinsam über die Zwecke (Verbesserung der Diabetes-Behandlung) und Mittel (z.B. Training föderierter virtueller Zwillinge) entscheidet – einer gemeinsamen Verantwortlichkeit in Bezug auf den Aufbau der Infrastruktur (*federated database network*), das Training der virtuellen Zwillinge und die Validierungsstudie unterliegt.

II. Anwendungsbereich der DSGVO

1. Einleitung

Mit Verweis auf die obigen Ausführungen zur gemeinsamen Verantwortlichkeit ergibt sich in Hinblick auf die Anwendbarkeit der DSGVO auf

31 *E.-B. Veen/M. Boeckhout/I. Schlünder/J. W. Boiten/V. Dias*, Joint controllers in large research consortia, Open Res Europe 2024, 1 (5), https://doi.org/10.12688/openreseurope.14825.2.

32 *R. Becker/A. Thorogood/J. Bovenberg/C. Mitchell/A. Hall*, Applying GDPR roles and responsibilities to scientific data sharing, IDPL 2022, 207 (216).

33 *Veen/Boeckhout/Schlünder/Boiten/Dias*, controllers (Fn. 31), 8 ff.

34 EuGH C-231/22, *État belge/Autorité de protection des données,* ECLI:EU:C:2024:7 Rn. 48.

35 EuGH C-25/17, *Jehovan todistajat,* ECLI:EU:C:2018:551 Rn. 75.

36 EuGH C-683/21, *Nacionalinis visuomenės sveikatos centras,* ECLI:EU:C:2023:949 Rn. 32 ff.

die (amerikanischen) Partner ein datenschutzrechtliches „Henne-Ei-Problem", da eine gemeinsame Verantwortlichkeit, die nur bei Anwendbarkeit der DSGVO überhaupt vorliegen kann, potentiell ihre Anwendbarkeit begründet. Art. 3 DSGVO enthält drei unterschiedliche Regelungen über den räumlichen Anwendungsbereich, wobei nur zwei davon im Folgenden von Relevanz sind.

2. Niederlassungsprinzip (Art. 3 Abs. 1 DSGVO)

Nach Art. 3 Abs. 1 DSGVO findet die DSGVO zunächst „Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet." Dies trifft zunächst unstrittig auf die europäischen (klinischen) Partner zu.

Bei Annahme einer gemeinsamen Verantwortlichkeit wird in der Literatur, im Gegensatz zu einem Verantwortlichen-Auftragsverarbeiter-Verhältnis, angenommen, dass die Anwendbarkeit der DSGVO für alle Verantwortlichen gemeinsam zu beurteilen ist.[37] Dies würde auch für unionsfremde Verantwortliche gelten.[38]

Dadurch wäre im dAIbetes-Projekt, bspw. für das Training der Zwillings-Modelle, da dieses nur im Zusammenspiel mit den europäischen Partnern gelingt und von europäischen und amerikanischen Patienten abgeleitete Parameter gleichermaßen einfließen, der Anwendungsbereich der DSGVO für den amerikanischen Partner 1 eröffnet. Die Tätigkeit der europäischen Partner würde somit den Anwendungsbereich der DSGVO auch auf Partner 1, der mit diesen gemeinsam über die Zwecke und Mittel entscheidet, erstrecken.

Dies gilt auch für Leitung des Arbeitspaketes zur Datenharmonisierung durch Partner 1. Ähnlich wie die Erstellung einer Fanpage[39] bzw. die Orga-

37 *K.-W. Plath/M. A. Struck* in: K.-U. Plath (Hrsg.), DSGVO/BDSG/TTDSG. Kommentar, 4. Auflage, Köln 2023, Art. 3 DSGVO Rn. 13.

38 *S. Hanloser* in H.-A. Wolff/S. Brink/A. Ungern-Sternberg (Hrsg.), BeckOK Datenschutzrecht. DS-GVO, DA, DGA, BDSG. Datenschutz und Datennutzung, München 48. Edition, Stand: 01.11.2021, Art. 3 DSGVO Rn. 12: „In Fällen gemeinsamer Verantwortung iSd Art. 26 reicht die Unionsniederlassung eines Mitverantwortlichen, um die räumliche Anwendbarkeit der DS-GVO auch gegenüber sämtlichen unionsfremden Mitverantwortlichen zu eröffnen."

39 *Hartung* (Fn. 26), Art. 26 DSGVO Rn. 27.

nisation von Verkündigungstätigkeiten[40] die Datensammlung durch andere Verantwortliche erst ermöglichte, lässt sich dies auch für die Leitung der Datenharmonisierung, durch die die Merkmale der Modelle bestimmt werden, argumentieren.

Diese Argumentation lässt sich mit Verweis auf die aktuelle Rspr. des EuGH zu IAB Europe untermauern.[41] Der EuGH führte in dieser Entscheidung im Werbekontext aus, dass die Aufstellung eines „Regelungsrahmens" „der nicht nur verbindliche technische Vorschriften enthält, sondern auch Vorschriften, die detailliert festlegen, wie personenbezogene Daten […] gespeichert und verbreitet werden müssen," zu einer Einstufung als gemeinsamer Verantwortlicher führt, wenn die Organisation „aus Eigeninteresse auf die betreffende Verarbeitung […] Einfluss nimmt und damit gemeinsam […] die Zwecke der und die Mittel zur betreffenden Verarbeitung festlegt."[42]

Dies ähnelt der Erstellung von Vorgaben zur Datenharmonisierung durch Partner 1. Zugriff auf die Daten ist nicht notwendig. Somit würde bereits die „hintergründige Organisation und Koordination einer fremden Datenverarbeitung"[43] hinreichen. Als Zwischenfazit wäre damit die DSGVO auf Verarbeitungstätigkeiten von Partner 1 im Rahmen der gemeinsamen Verantwortlichkeit anwendbar.

Ein ähnlicher Schluss ließe sich in Hinblick auf Partner 2 ziehen. Dieser nimmt zwar nicht am Training teil, leitet jedoch die Validierungsstudie. Dabei nehmen die Leitlinien des EDSA für die gemeinsame Erstellung eines Studienprotokolls das Vorliegen einer gemeinsamen Verantwortlichkeit an.[44] Ein Vergleich zur genannten Parametrisierung einer COVID-19-Tracking-App oder die Vorgabe des Regelungsrahmens in IAB Europe liegt nahe. Damit würde auch Partner 2 im Kontext der für die Validierungsstudie notwendigen Verarbeitungen, nicht aber für andere Tätigkeiten, der DSGVO unterliegen.

Diese Interpretation von Art. 3 Abs. 1 i.V.m. Art. 26 DSGVO ist jedoch nicht unumstritten. So geht die Gesellschaft für Datenschutz und Datensicherheit (GDD) davon aus, dass, wenn der gemeinsam Verantwortliche

40 *Hartung* (Fn. 26), Art. 26 DSGVO Rn. 33 f.

41 EuGH C-604/22, *IAB Europe,* ECLI:EU:C:2024:214; vgl. *Halim/Marosi,* Status Quo (Fn. 26), 298; *V. Halim/J. Marosi*, TC-String ist ein personenbezogenes Datum, ZD 2024, 333.

42 EuGH C-604/22, *IAB Europe,* ECLI:EU:C:2024:214 Rn. 77.

43 *L. M. Keppeler/R. Schneider*, TC-String ist ein personenbezogenes Datum, MMR 2024, 395 (396).

44 *EDSA*, Verantwortlicher (Fn. 24), S. 26.

keine Niederlassung in der EU besitzt, Art. 26 DSGVO das Vorliegen der Bedingungen von Art. 3 Abs. 2 DSGVO (Marktortprinzip) erfordern würde.[45] Auch nach *Radtke* ist der Anwendungsbereich separat zu betrachten. So würde die Gemeinsamkeit der Festlegung durch einen räumlich unter die DSGVO fallenden (gemeinsam) Verantwortlichen nicht die übrigen Festlegenden „infizieren".[46]

Im Zwischenergebnis liegt eine non-liquet-Situation vor. Die Literatur lässt beide Interpretationen von Art. 3 Abs. 1 i.V.m. Art. 26 DSGVO zu. Rechtsprechung zu dieser Konstellation existiert, soweit dem Autor bekannt, bisher noch nicht. Ob es dem Telos entspricht, den Anwendungsbereich der DSGVO über das Instrument der „gemeinsamen Verantwortlichkeit" über die EU hinaus zu erstrecken, wodurch „Daten außerhalb ihrer Grenzen"[47] geschützt werden würden, lässt sich zum derzeitigen Stand noch nicht zweifelsfrei feststellen. Eine Konkretisierung dieser zentralen Frage über aktualisierte Leitlinien des EDSA wäre, um diese Rechtsunsicherheit zu beseitigen, wünschenswert.

3. Marktortprinzip (Art. 3 Abs. 2 DSGVO)

Alternativ könnte vom Vorliegen von Art. 3 Abs. 2 lit. b DSGVO, der Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen im Kontext der Beobachtung des Verhaltens von betroffenen Personen, ausgegangen werden.

So nennen die Leitlinien in diesem Kontext auch die „Überwachung oder regelmäßige Meldungen über den Gesundheitszustand einer Person".[48] Die Erstellung eines häufig aktualisierten virtuellen Zwillings könnte solche regelmäßigen Meldungen erfordern. Ähnlich ließe sich in Bezug auf die Validierungsstudie argumentieren, dass dazu eine „Beobachtung" von Patienten notwendig sei.

45 *GDD*, GDD-Praxishilfe DS-GVO. Die gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO (Joint Controllership), 2019, S. 14, gdd.de/wp-content/uploads/2023/06/GDD-Praxishilfe-DS-GVO-Joint-Controllership.pdf.

46 *Radtke*, Verantwortlichkeit (Fn. 23), S. 161; vgl. *M. Gömann*, Das öffentlich-rechtliche Binnenkollisionsrecht der DS-GVO. Unionaler Anwendungsbereich mitgliedstaatlichen Anpassungsrechts zur Datenschutz-Grundverordnung, Tübingen 2021, S. 534 f.

47 *C. Kuner*, Protecting EU data outside EU borders under the GDPR, CMLR 2023, 77.

48 *EDSA*, Leitlinien 3/2018 zum räumlichen Anwendungsbereich der DSGVO (Artikel 3) Version 2.0, 2019, S. 23, edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_consultation_de.pdf.

Gegen die Bejahung des Vorliegens von Art. 3 Abs. 2 DSGVO einwenden lässt sich, dass nach Projektkonzeption keine personenbezogenen Daten über europäische Patienten an die amerikanischen Partner übermittelt werden. Die Übermittlung zur Validierungsstudie erfolgt (voraussichtlich) in aggregierter und anonymisierter Form. Art. 3 Abs. 2 DSGVO hat dabei konzeptuell auch stärker „Internet-Monitoring" (ErwGr. 24 DSGVO) und nicht die Aufzeichnung von physiologischen Zuständen vor Augen.[49]

Bejaht man die These der gemeinsamen Verantwortlichkeit in Verbindung mit der Anwendbarkeit der DSGVO bedeutet dies, dass die gemeinsam Verantwortlichen im Innenverhältnis einen Vertrag, ein *joint controller agreement* (JCA) (Art. 26 Abs. 1, 2 DSGVO) abschließen müssen. Dieses hat jedoch nur deklarative, nicht aber konstitutive Wirkung. Im Außenverhältnis wird eine gesamtschuldnerische Haftung begründet (Art. 82 Abs. 4 DSGVO).[50] Wird die Anwendbarkeit der DSGVO bejaht, würden somit auch die amerikanischen Partner den Betroffenenrechten (insb. den Informationspflichten und dem Recht auf Löschung) unterliegen und müssten ein Verzeichnis der Verarbeitungstätigkeiten führen. Die praktische Durchsetzbarkeit der DSGVO in den USA wäre jedoch in dieser Konstellation – mangels einer entsprechenden Behördenstruktur – fragwürdig.

D. MPVO & KI-VO: Synergien und Friktionen

I. Virtuelle Zwillinge als Medizinprodukt

Virtuelle Zwillinge bzw. Machine-Learning-Modelle stellen eine Unterform der breiteren Kategorie „Software" dar. „Software",[51] die „dem Hersteller zufolge für Menschen bestimmt ist und allein oder in Kombination einen […] spezifischen medizinischen Zwecke erfüllen soll" kann als Medizinprodukt eingestuft werden (Art. 2 Nr. 1 MPVO). Dies lässt sich auch für dAIbetes bejahen, da als medizinischer Zweck die „Behandlung oder Linderung

49 *G. Hornung* in: I. Spiecker gen. Döhmann/V. Papakonstantinou/G. Hornung/P. Hert (Hrsg.), General Data Protection Regulation. Article-by-Article Commentary, Baden-Baden/München/Oxford 2023, Art. 3 GDPR Rn. 48.

50 *Radtke*, Verantwortlichkeit (Fn. 23), S. 228 ff.

51 *MDCG*, Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, MDCG 2019–11, 2019, S. 5 f., health.ec.europa.eu/system/files/2020–09/md_mdcg_2019_11_guidance_qualification_classification_software_en_0.pdf.

von Krankheiten" verfolgt wird. Die im Projekt vorgesehenen virtuellen Zwillinge fallen nach der – teilweise als zu streng kritisierten[52] – Klassifizierungsregel 11 (Anhang VIII Abschnitt 6.3 MPVO) mindestens in die mittlere Risikoklasse IIa, nachdem sie dazu bestimmt sind „Informationen zu liefern, die zu Entscheidungen für diagnostische oder therapeutische Zwecke herangezogen werden".

In Bezug auf die KI-VO führt die Einstufung als Medizinprodukt, da die verwendeten Zwillinge in Verbindung mit anderen Elementen wie der Nutzerschnittstelle als KI-Systeme[53] (Art. 3 Nr. 1 KI-VO) zu qualifizieren sein werden, prinzipiell zu einer Anwendbarkeit der KI-VO. „Intelligente Medizinprodukte" gelten, da nach MPVO ab Klasse IIa die Einbindung einer Konformitätsbewertungsstelle notwendig ist und die MPVO in Anhang I Abschnitt A KI-VO genannt wird, (großteils) gleichzeitig als Hochrisiko-KI-Systeme (Art. 6 Abs. 1 KI-VO).[54]

Im Folgenden sollen insbesondere Fragen der Interaktion zwischen den Anwendungsbereichen der MPVO und KI-VO aufgeworfen werden. Wie relevant Rechtsfragen dieser Interaktion sind, zeigt sich an den von der MDCG (Medical Device Coordination Group) angekündigten FAQ zum Zusammenhang von MPVO und KI-VO.[55]

II. Forschungsausnahme

Die KI-VO normiert eine explizite Forschungsausnahme. Diese wurde auf Anregung von Parlament und Rat eingefügt.[56] Zuvor wurde das Fehlen

52 *M. Heil*, Innovationsermöglichungsrecht oder Innovationshemmnis? in: R. Grinblat/S. Scholtz/S. Stock (Hrsg.), Medizinprodukterecht im Wandel. Festschrift für Ulrich M. Gassner zum 65. Geburtstag, Baden-Baden 2022, S. 447 (454).

53 *C. Wendehorst/B. Nessler/A. Aufreiter/G. Aichinger*, Der Begriff des „KI-Systems" unter der neuen KI-VO, MMR 2024, 605.

54 *M. Martini*, § 4. Hochrisiko-KI-Systeme, in: E. Hilgendorf/D. Roth-Isigkeit (Hrsg.), Die neue Verordnung der EU zur Künstlichen Intelligenz, München 2023, S. 51 (65 f.); *R. Schwartmann/E.-M. Pottkämper*, Hochrisiko-KI-Systeme gem. Art. 6 Abs. 1 KI-VO (Anhang I), in R. Schwartmann/T. O. Keber/K. Zenner (Hrsg.), KI-Verordnung. Leitfaden für die Praxis, Heidelberg 2024, S. 79 (80).

55 *MDCG*, Ongoing/planned guidance development and deliverables of MDCG Subgroups – March 2024, 2024, S. 4, health.ec.europa.eu/document/download/f588a5c8–57af-48aa-808f-1d9c02f4925a_en?filename=mdcg_ongoing-guidance_0.pdf.

56 *T. O. Keber/K. Zenner*, Forschung, in R. Schwartmann/T. O. Keber/K. Zenner (Hrsg.), KI-Verordnung. Leitfaden für die Praxis, Heidelberg 2024, S. 47 (48).

einer solchen Ausnahme[57] bzw. die fehlende Abstimmung zwischen MPVO und KI-VO[58] kritisiert. Nach Art. 2 Abs. 6 KI-VO gilt die Verordnung nicht „für KI-Systeme oder KI-Modelle, einschließlich ihrer Ausgabe, die eigens für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen werden." Der Begriff Forschung ist weit zu verstehen und bezieht sich auf eine beliebige Forschungs- und Entwicklungstätigkeit, die sich auch nicht gerade auf KI-Systeme selbst beziehen muss.[59] Forschung erfasst begrifflich sowohl Forschende in privaten Unternehmen als auch bei öffentlichen Stellen.[60] Im Rahmen der Projektphase, die der Erforschung der Anwendbarkeit von federated learning und virtuellen Zwillingen auf die komplexe Erkrankung Diabetes dient – nicht aber in Bezug auf eine eventuelle spätere Vermarktung – lässt sich insofern argumentieren, dass diese durch die Forschungsausnahme nicht dem Anwendungsbereich der KI-VO unterliegt.

Im Gegensatz zur KI-VO kennt die MPVO keine eindeutige Forschungsausnahme.[61] Zwar wird das (zukünftige) Produkt im Rahmen der Projektphase nicht in Verkehr gebracht, aber es könnte eine Inbetriebnahme durch die klinischen Partner vorliegen. Inbetriebnahme bezeichnet den Zeitpunkt, zu dem ein Produkt dem Endanwender als ein Erzeugnis zur Verfügung gestellt wird, das erstmals als gebrauchsfertiges Produkt entsprechend seiner Zweckbestimmung auf dem Unionsmarkt verwendet werden kann (Art. 2 Nr. 29 MPVO). Bereits Produkte, die in Gesundheitseinrichtungen hergestellt und verwendet werden, gelten als in Betrieb genommen (Art. 5 Abs. 4 MPVO).

Daher kommt es potentiell zu einem Auseinanderfallen zwischen den Rechtsmaterien, bei denen die Zwillinge im Rahmen der Forschungsaus-

57 *D. Feuerstack/D. Becker/N. Hertz*, Die Entwürfe des EU-Parlaments und der EU-Kommission für eine KI-Verordnung im Vergleich, ZfDR 2023, 421 (432); *N. A. Schmuha/E. Ahmed-Rengers/A. Harkens/W. Li/J. MacLaren/R. Piselli/K. Yeung*, How the EU Can Achieve Legally Trustworthy AI. A Response to the European Commission's Proposal for an Artificial Intelligence Act, 2021, S. 15 ff., papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991.

58 *Heil*, Innovationsermöglichungsrecht (Fn. 52), S. 459.

59 *C. Wendehorst* in: M. Martini/C. Wendehorst (Hrsg.), KI-VO, München 2024, Art. 2 KI-VO Rn. 83 f.

60 *Keber/Zenner*, Forschung (Fn. 56), S. 48.

61 Zur (abweichenden) Kategorie der Research-Use-Only-Produkte, siehe *MDCG*, Guidance on the health institution exemption under Article 5(5) of Regulation (EU) 2017/745 and Regulation (EU) 2017/746, MDCG 2023–1, 2023, S. 6, health.ec.europa.eu/system/files/2023–01/mdcg_2023–1_en.pdf.

nahme nicht der KI-VO unterliegen, der Anwendungsbereich der MPVO aber nicht ausdrücklich ausgeschlossen ist. Jedoch lässt sich argumentieren, dass, da die Ergebnisse des Modells auch im Rahmen der Validierungsstudie keinen Einfluss auf die Behandlung haben, keine Verwendung eines gebrauchsfertigen Produktes „entsprechend der Zweckbestimmung" und damit keine Inbetriebnahme i.e.S. vorliegt. Auch bei einem anderen Design der Studie wären die Modelle potentiell als „Prüfprodukte", d.h. ein Produkt, das im Rahmen einer klinischen Studie bewertet wird (Art. 2 Nr. 46 MPVO) einzustufen. Für Prüfprodukte bestehen wiederum Ausnahmen vom Anwendungsbereich (Art. 2 Nr. 27–29 MPVO). Faktisch dürften sich diese Überlegungen dadurch relativieren, dass die Anforderungen von KI-VO und MPVO stets mitbedacht werden sollten, wenn die Intention besteht, ein KI-System bzw. eine Software später in Verkehr zu bringen. Denn selbst wenn für die Projektphase eine Ausnahme oder Erleichterung besteht, haben die Anforderungen der Verordnungen gravierenden Einfluss auf das Design und können somit häufig nicht nachträglich berücksichtigt werden.

Eine alternative Möglichkeit wäre das Stützen auf die Ausnahme zur „Prototyp-Entwicklung", die der Markteinführung zeitlich vorausgeht (Art. 2 Abs. 8 KI-VO).[62] Diese Ausnahme stellt stärker als die Forschungsausnahme auf Tätigkeiten in Bezug auf KI-Systeme selbst ab.[63] Allerdings fallen Tests unter Realbedingungen (Art. 60 KI-VO), d.h. der befristete Test eines KI-Systems auf seine Zweckbestimmung, der unter Realbedingungen außerhalb eines Labors oder einer anderweitig simulierten Umgebung erfolgt (Art. 3 Nr. 57 KI-VO), nicht unter diesen Ausschluss. Diese müssen im Einklang mit geltendem Unionsrecht – bspw. Anforderungen an klinische Studien – durchgeführt werden.[64] Solche Tests unter Realbedingungen – die eine gewisse thematische Verwandtschaft zu Prüfprodukten nach der MPVO aufweisen – dürften in Bezug auf medizinische Anwendungen häufig notwendig sein, wodurch die Ausnahme diesbezüglich nur geringere Relevanz aufweist.

62 *J. Wendt/D. H. Wendt*, Das neue Recht der Künstlichen Intelligenz. Artificial Intelligence Act (AI Act), Baden-Baden 2024, S. 54.
63 *Wendehorst* (Fn. 59), Art. 2 KI-VO Rn. 89.
64 *Wendehorst* (Fn. 59), Art. 2 KI-VO Rn. 92.

III. „Eigenherstellung"

In Bezug auf federated learning stellen sich in Hinblick auf die „in-house"-Ausnahme bzw. „Eigenherstellung" komplexe Fragen des Anwendungsbereiches der MPVO. So wäre bspw. vorstellbar, dass die dAIbetes-Zwillinge nach Ende der Projektphase durch die klinischen Partner in praktische Verwendung übergehen bzw. in beteiligten Krankenanstalten in Betrieb genommen, aber nicht allgemein über diese hinaus in Verkehr gebracht werden.

Für Medizinprodukte, „die ausschließlich innerhalb von in der Union ansässigen Gesundheitseinrichtungen hergestellt[65] und verwendet werden" gelten gem Art. 5 Abs. 5 MPVO die Anforderungen der Verordnung – mit Ausnahme der grundlegenden Sicherheits- und Leistungsanforderungen – nicht, wenn eine Reihe von Bedingungen erfüllt werden. Für diese Produkte in „Eigenherstellung" entfällt die Pflicht zur Durchführung eines Konformitätsbewertungsverfahrens und der Anbringung der CE-Kennzeichnung.[66] Durch diese Erleichterung sollte Gesundheitseinrichtungen die Möglichkeit eingeräumt werden, Produkte hausintern herzustellen, um auf spezifische Bedürfnisse von Patienten einzugehen, die auf dem angezeigten Leistungsniveau nicht durch ein gleichartiges, auf dem Markt befindliches Produkt, befriedigt werden können.[67]

Bedingungen sind dabei u.a. eine entsprechende Dokumentation, die Bereitstellung von Informationen an Behörden und die Einhaltung von Qualitätsmanagementsystemen.[68] Dabei muss begründet werden, dass die spezifischen Erfordernisse der Zielgruppe nicht bzw. nicht auf dem Leistungsniveau durch ein auf dem Markt befindliches gleichartiges Produkt befriedigt werden können.[69] Dieses Kriterium kann potentiell in Hinblick auf die dAIbetes-Modelle, im Projekt bestehen hohe Performanz-Ziele, und Diabetes-Patienten als Zielgruppe, bejaht werden. Eine weitere Bedingung bezieht sich darauf, dass das Produkt nicht an eine andere rechtlich eigen-

65 Nach den Leitlinien kann der Begriff „herstellen" auch im Sinne einer Kombination von Produkten oder Modifikation verstanden werden, *MDCG*, health institution exemption (Fn. 61), S. 5 f.

66 *S. A. Wagner* in: W. A. Rehmann/S. A. Wagner (Hrsg.), MP-VO, 4. Auflage, München 2023, Art. 5 MPVO Rn. 45.

67 *Wagner* (Fn. 66), Art. 5 MPVO Rn. 45.

68 *MDCG*, health institution exemption (Fn. 61), S. 8 ff.

69 *MDCG*, health institution exemption (Fn. 61), S. 12 f.

ständige Einrichtung abgegeben wird.[70] In Bezug auf die lokalen Modelle lässt sich argumentieren, dass diese ausschließlich anhand der eigenen Daten trainiert und damit innerhalb von in der Union ansässigen Gesundheitseinrichtungen hergestellt und verwendet werden.

Komplexere Fragen stellen sich aufgrund des Zusammenspiels von verschiedenen Partnern in Bezug auf federated learning. Zwar wird bei der Aggregierung nicht das gesamte Modell „abgegeben", sondern nur gewisse Parameter, die zum globalen Modell zusammengefügt und wieder an die Beteiligten verteilt werden. Dieser Vorgang der Beteiligung anderer klinischer Partner und der Aggregierung führt jedoch dazu, dass m.E. nicht mehr von einer Eigenherstellung gesprochen werden kann. Eine Ausnahme könnte bei federated learning innerhalb von mehreren Krankenanstalten, die rechtlich zu einem Träger gehören,[71] vorliegen, da somit keine „Abgabe" an eine rechtlich eigenständige Einrichtung vorliegen würde. Dieser Schluss, dass federated learning der Erleichterung durch „Eigenherstellung" konzeptuell entgegensteht, DSGVO und MPVO somit Friktionen aufweisen, wird für dAIbetes dadurch bestärkt, dass das globale Modell an den amerikanischen Partner 1 abgegeben wird. Es ist somit definitionsmäßig kein Produkt, das in „ausschließlich innerhalb von in der Union ansässigen Gesundheitseinrichtungen hergestellt und verwendet" wird.

IV. Kontinuierlich lernende Medizinprodukte

Eine regulatorische Einschränkung, die generell in Bezug auf „intelligente Medizinprodukte" vorliegt, die aber gerade in Hinblick auf die dezentrale Natur von federated learning und die Möglichkeit, neue klinische Partner hinzuzufügen, verstärkt Relevanz erlangen könnte, ist die bisher eingeschränkte Möglichkeit, kontinuierlich lernende Medizinprodukte zu zertifizieren.[72]

70 *C. Johner*, Eigenherstellung von Medizinprodukten, johner-institut.de/blog/regulatory-affairs/eigenherstellung-von-medizinprodukten/ (Stand 24.10.2019).

71 *MDCG*, health institution exemption (Fn. 61), S. 8.

72 *IG-NB*, Questionnaire „Artificial Intelligence (AI) in medical devices", Version 4 2022, S. 4, ig-nb.de/veroeffentlichungen: "Dynamic AI (AI that continues to learn in the field) is not certifiable in principle, as the system must be verified and validated (among other things, the functionality must be validated against the intended use)." Statt vieler *Heil*, Innovationsermöglichungsrecht (Fn. 52), S. 462 f.; *J. L. Saliba*, Arzneimittel und Medizinprodukte, in K. Chibanguza/C. Kuß/H. Steege (Hrsg.),

Wären die dAIbetes-Zwillinge als Medizinprodukt in ihrer Konformität zertifiziert (Art. 52 MPVO) und würde sich ein zusätzlicher klinischer Partner am federated learning beteiligen wollen, würde eine (wesentliche) Änderung am Modell zum derzeitigen Stand einen erneuten Durchlauf des Konformitätsbewertungsverfahrens erfordern. Dies ist in Hinblick auf die Sicherheit des Medizinproduktes verständlich, steht einer raschen Anpassung jedoch entgegen. Das Idealbild von virtuellen Zwillingen sieht aber gerade eine solche ständige Wechselbeziehung zwischen realem Patienten und Zwilling vor. Diesbezüglich ist aber aufgrund der in der KI-VO vorgesehenen Möglichkeit, Änderungen – die damit keine erneute Konformitätsbewertung erfordern – vorab festzulegen und zu dokumentieren (Art. 43 Abs. 4 KI-VO), Anpassungen in Leitlinien[73] und zunehmend lauter werdenden Stimmen in der Literatur zu „antizipierten Konformitätsbewertungen"[74] davon auszugehen, dass es zu einer Richtungsänderung und Angleichung zwischen MPVO und KI-VO kommen wird.

E. Cybersicherheit

I. Einleitung

Auch wenn federated learning datenschutzrechtlich zahlreiche Vorteile mit sich bringt, stellt sich die Frage nach der Cybersicherheit dieser Systeme. Zwar wird durch diesen Ansatz das Risiko von Cyberangriffen verringert, dennoch sind eine Reihe von Attacken, bspw. auf die lokalen und globalen Modelle, möglich.[75]

Künstliche Intelligenz. Recht und Praxis automatisierter und autonomer Systeme, Baden-Baden 2022, S. 627 (635 f.).

73 *IG-NB*, Questionnaire „Artificial Intelligence (AI) in medical devices", Version 5.1 2024, S. 5, ig-nb.de/veroeffentlichungen.

74 *Z. Schreitmüller*, Regulierung intelligenter Medizinprodukte. Eine Analyse unter besonderer Berücksichtigung der MPVO und DSGVO, Baden-Baden 2023, S. 153 f.; vgl. *S. Semmler/K. Stöger*, Rechtsfragen rund um eHealth, JMG 2024, 192 (201); *U. Gassner/U. Juknat*, Künstliche Intelligenz in der Medizin, in: W. A. Rehmann/C. Tillmanns (Hrsg.), E-Health/Digital Health, München 2022, S. 240 (267 ff.).

75 *Baumbach/Majdabadi/Saak/Bakhtiari/Probul,* Lernen (Fn. 12), S. 273 f.

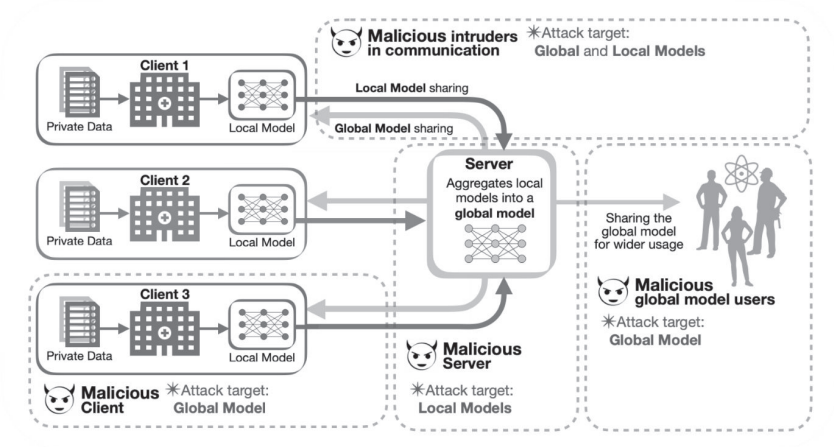


Abbildung 2 Angriffsvektoren bei federated learning (SBA Research)

Mögliche „Angriffsvektoren" bestehen bspw. auf Seite der klinischen Partner, die lokale Modelle trainieren, beim Koordinator, der das globale Modell aggregiert, in der Kommunikation zwischen Partnern und Koordinator sowie auf der Seite der Nutzer des globalen Modells.

II. Datensicherheit

Cybersicherheitsrecht stellt häufig eine Gemengelage aus unterschiedlichen Rechtsmaterien dar. Dabei unterliegen Verantwortliche bereits aufgrund der DSGVO der Pflicht, geeignete technische und organisatorische Maßnahmen (TOMs) zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 DSGVO). Dies dient u.a. der Integrität, Verfügbarkeit und Vertraulichkeit personenbezogener Daten.[76]

76 *P. Vogel*, Künstliche Intelligenz und Cybersicherheitsrecht im Krankenhaus, in: T. Dittrich/C. Dochow/J. Ippach (Hrsg.), Rechtshandbuch Cybersicherheit im Gesundheitswesen, Heidelberg 2024, S. 339 (342 f.).

III. Art. 15 KI-VO

Speziell in Bezug auf KI-Systeme verlangt Art. 15 Abs. 1 KI-VO neben Anforderungen an Genauigkeit und Robustheit ein ausreichendes Maß an Cybersicherheit. So müssen Hochrisiko-KI-Systeme widerstandsfähig gegen Versuche unbefugter Dritter sein, ihre Verwendung, Ausgaben oder Leistung durch Ausnutzung von Systemschwachstellen zu verändern (Art. 15 Abs. 5 KI-VO).[77] Das Risiko in Bezug auf die Cybersicherheit fließt dabei auch in die Bewertung im Rahmen des einzurichtenden Risikomanagementsystems (Art. 9 KI-VO) ein.[78]

Die KI-VO nennt dabei beispielhaft die Implementierung von Maßnahmen gegen data poisoning, model poisoning, adversarial examples und model evasions, Angriffe auf vertrauliche Daten oder Modellmängel.[79] Ähnliche Angriffsvektoren, z.B. model poisoning der lokalen Modelle,[80] wurden auch in Bezug auf federated learning identifiziert und müssen somit durch technische Maßnahmen verhindert werden.

IV. NIS-2-RL

Neben der KI-VO ist in Zukunft die NIS-2-RL[81] und ihre nationale Umsetzung zu beachten. Für das dAIbetes-Projekt von Relevanz designiert diese das Gesundheitswesen als Sektor mit hoher Kritikalität (Anhang I Nr. 5). Darunter fallen Gesundheitsdienstleister, d.h. eine natürliche oder juristische Person oder sonstige Einrichtung, die im Hoheitsgebiet eines

77 *C. Glugla*, Cybersicherheit in der KI-Verordnung, RDI 2024, 421.

78 M.w.N. *D. M. Schneeberger/W. Hötzendorfer/C. Tschohl* in: C. N. Pehlivan/N. Forgó/P. Valcke (Hrsg.), The EU Artificial Intelligence (AI) Act, Alphen aan den Rijn 2024, Art. 9 AI Act.

79 *P. Nägele/A. Steinbrück*, Genauigkeit, Robustheit und Cybersecurity (Art. 15 KI-VO), in R. Schwartmann/T. O. Keber/K. Zenner (Hrsg.), KI-Verordnung. Leitfaden für die Praxis, Heidelberg 2024, S. 138 (140); *Wendt/Wendt*, Recht (Fn. 62), S. 78 f.

80 *M. Martini* in: M. Martini/C. Wendehorst (Hrsg.), KI-VO, München 2024, Art. 15 KI-VO Rn. 71.

81 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. L 2022/333, 80.

Mitgliedstaats rechtmäßig Gesundheitsdienstleistungen erbringt.[82] Diese Eigenschaft lässt sich für die beteiligten Krankenanstalten, abhängig von Schwellenwerten (Art. 3 Abs. 1 lit. a NIS-2-RL),[83] voraussichtlich bejahen. Zugleich fällt die Herstellung von Medizinprodukten unter die Liste der sonstigen kritischen Sektoren (Anhang II Nr. 5 NIS-2-RL).

Diese Einrichtungen unterliegen somit neben Schulungs- (Art. 20 Abs. 2 NIS-2-RL) und (mehrstufigen) Berichtspflichten (Art. 23 NIS-2-RL)[84] auch einer Pflicht, geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen zu ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten (Art. 21 Abs. 1 NIS-2-RL).

V. Technische Gegenmaßnahmen

Um die angesprochenen Risiken zu minimieren und dem security-by-design-Gedanken[85] entsprechend Rechnung zu tragen, wird federated learning häufig mit anderen Techniken wie differential privacy (DP) und secure multiparty computation (SMPC) kombiniert.[86]

Bei DP wird auf kontrollierte Weise statistisches Rauschen (noise) hinzugefügt, um die Identifizierbarkeit zu verhindern.[87] Damit kann, bspw. durch Perturbation des lokalen Modells, nicht mehr nachgewiesen werden,

82 Art. 3 lit. g Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung, ABl. L 2011/88, 45.

83 *C. Monsees/M. Gehrmann*, Krankenhäuser, in: T. Dittrich/C. Dochow/J. Ippach (Hrsg.), Rechtshandbuch Cybersicherheit im Gesundheitswesen, Heidelberg 2024, S. 56 (68).

84 *Monsees/Gehrmann*, Krankenhäuser (Fn. 83), S. 75 f.

85 *Nägele/Steinbrück,* Genauigkeit (Fn. 79) S. 140.

86 *Baumbach/Majdabadi/Saak/Bakhtiari/Probul,* Lernen (Fn. 12), S. 275 ff.; *Brauneck/Schmalhorst/Majdabadi/Bakhtiari/Völker/Baumbach/Baumbach/Buchholtz*, Machine (Fn. 13), 4.

87 *J.-P. Hoepman*, Privacy is Hard and Seven Other Myths. Achieving Privacy Through Careful Design, Cambridge 2021, S. 93 ff.; *M. Kearns/A. Roth*, The Ethical Algorithm. The Science of Socially Aware Algorithm Design, New York 2020, S. 36 ff.

dass ein Patient Teil des Trainingsdatensatzes war.[88] SMPC ermöglicht es mehreren Parteien unter Nutzung von kryptographischen Verfahren (gemeinsam) Daten auszuwerten, ohne die jeweiligen Daten den Partnern gegenüber offenzulegen.[89] SMPC garantiert primär die Sicherheit des „Inputs", d.h. schützt in einem federated-learning-Szenario die lokalen Modelle.[90] Mit der Hilfe von diesen und anderen technischen Maßnahmen soll dem (Cybersicherheits-)Risiko Rechnung getragen werden, was auch im Rahmen der notwendigen Datenschutz-Folgenabschätzung Niederschlag findet.[91]

F. Conclusio

Dieser Beitrag illustrierte am Beispiel des dAIbetes-Projektes einige Problemfelder, die Fragen am Schnittpunkt von Metaversum und Medizin (-recht) aufwerfen. So kreiste der datenschutzrechtliche Abschnitt C. um die Rechtsfigur der gemeinsamen Verantwortlichkeit, die durch eine gemeinsame Entscheidung über die Zwecke und Mittel der Verarbeitung entsteht, und um die zentrale Frage, ob die Regelung des Anwendungsbereiches der DSGVO in Hinblick auf dezentral organisierte, aber dennoch föderiert vernetzte Strukturen noch zeitgemäß ist, oder ob sie zu einer (nicht intendierten) Ausdehnung des Schutzes über die EU-Grenzen hinaus führt. Die zunehmende grenzüberschreitende Vernetzung und damit die zunehmende Verlagerung in das Metaversum demonstriert Rechtsunsicherheit in Bezug auf die präzise Definition der Anwendungsbereiche, die durch Leitlinien oder Rechtsprechung adressiert werden sollte.

Interaktionen und Friktionen zeigten sich auch in Hinblick auf die MPVO und KI-VO (D.). Auch hier werfen unterschiedlich ausgestaltete

88 *M. Y. Topaloglu/E. M. Morrell/S. Rajendran/U. Topaloglu*, In the Pursuit of Privacy, frontiers in Artificial Intelligence 2021, 1 (3).

89 *D. Bierbauer/L. Helminger*, Offenlegung von Daten unter Wahrung der Privatsphäre mittels SMPC (Secure Multiparty Computation), ALJ 2023, 1 (6 ff.), alj.uni-graz.at/index.php/alj/article/view/300.

90 *FeatureCloud*, Deliverable D2.4 Set of (novel) attack vectors and countermeasures. Work Package WP2 Cyber risk assessment and mitigation, 2021, S. 16 f., featurecloud.eu/wp-content/uploads/2021/12/Deliverable_D2.4_Set_of_novel_attack_vectors_and_countermeasures.pdf.

91 *FeatureCloud*, Deliverable 8.7 "Report on Data Protection Impact Assessment". Work Package 8 "Testing and evaluation in clinical translation", 2024, S. 91 ff., featurecloud.eu/wp-content/uploads/2024/01/D8.7_Report-on-Data-Protection-Impact-Assessment_FINAL_submitted.pdf.

Anwendungsbereiche und Ausnahmen, primär die Forschungsausnahme der KI-VO, die kein direktes Pendant in der MPVO hat, Fragen der Interaktion dieser eng verbundenen Rechtsmaterien auf. Auch ist federated learning datenschutzrechtlich gewollt, führt aber zu Friktionen in Hinblick auf die Erleichterung für in „Eigenherstellung" produzierte Produkte nach der MPVO. Denn die vernetzte Natur von federated learning, die eine „Abgabe" an andere Partner bedingt, steht dieser Erleichterung diametral entgegen. Ähnliches gilt für die Friktion zwischen dem Idealbild von virtuellen Zwillingen, das eine ständige Wechselbeziehung zwischen Patienten und Zwilling impliziert, und der bislang nur bedingt bestehenden Möglichkeit, kontinuierlich lernende Medizinprodukte zu zertifizieren.

Zuletzt ergeben sich bei federated learning Besonderheiten in Hinblick auf die Cybersicherheit. Abschnitt E. erläuterte die Gemengelage aus unterschiedlichen Rechtsgebieten, wobei insbesondere Art. 15 KI-VO konkrete Maßnahmen gegen Attacken auf KI-Systeme forciert. Hand in Hand gehen damit die Anforderungen der NIS-2-RL, insbesondere in Hinblick auf Risikomanagementmaßnahmen. Als technische Gegenstrategien, wobei Synergien zum Datenschutzrecht bestehen, wurden differential privacy und secure multiparty computation vorgestellt.

Das dAIbetes-Projekt ist ein Prototyp für die Anwendbarkeit von federated learning und virtuellen Zwillingen auf komplexe Krankheiten. Gelingt das Projekt, lässt sich die geschaffene Infrastruktur potentiell auch für andere Krankheiten heranziehen. Dies würde die Symbiose zwischen einer (datenschutz-)rechtssicheren Konzeption bei gleichzeitigen Fortschritten von Informatik und Medizin demonstrieren. Doch damit der intendierte Zwilling nicht zum Zerrbild wird, man denke nur an die „ungleichen" Zwillinge Schwarzenegger und DeVito im gleichnamigen Film, damit „virtual you" in der Medizin zur Realität werden kann, müssen noch eine Reihe von Friktionen am Schnittpunkt von Metaversum und Recht ausgeräumt werden.

Die Digitalisierung der Bauleitplanung: Eine verpasste Chance?

Alexander Brade

Das Gesetz zur Stärkung der Digitalisierung im Bauleitplanverfahren bleibt hinter seinen Erwartungen zurück. Es hält am Hybridmodell aus elektronischer und papiergebundener Auslegung bei der förmlichen Öffentlichkeitsbeteiligung fest und geht damit nur unwesentlich über die vorherige Rechtslage (§ 4a Abs. 4 BauGB a.F.) hinaus. Vor allem adressiert es nicht die Nutzung neuer Techniken zur Bürgerbeteiligung, bei der z.B. die Planungsdaten mittels Virtual oder Augmented Reality dargestellt werden, um sie für die Bürgerinnen und Bürger verständlicher zu machen und den Planungsprozess so zu vereinfachen und zu beschleunigen.

A. Einführung

Die Bundesregierung hat sich zum Ziel gesetzt, die Verwaltungs-, Planungs- und Genehmigungsverfahren zu beschleunigen, damit private und staatliche Investitionen zur Modernisierung des Landes schnell, effizient und zielsicher umgesetzt werden können.[1] Der Koalitionsvertrag sieht deshalb eine Novellierung des Baugesetzbuchs vor, mit der „die rechtlichen Grundlagen für eine vollständige Digitalisierung der Bauleitplanverfahren" geschaffen werden sollen.[2] Zu diesem Zweck wurde im Juli 2023 das Gesetz zur Stärkung der Digitalisierung im Bauleitplanverfahren[3] verkündet, das im Folgenden vorgestellt (C.) sowie daraufhin untersucht werden soll, ob es dieser Zielsetzung gerecht wird (D.). Der Beitrag konzentriert sich ausschließlich auf jene Änderungen, die Auswirkungen auf das Bauleitplan-

1 BT-Drucks. 20/5663, S. 1.
2 Mehr Fortschritt wagen, Koalitionsvertrag 2021–2025 zwischen SPD, Bündnis 90/Die Grünen und FDP, S. 70.
3 BGBl. 2023 I Nr. 176.

verfahren haben.[4] Zunächst erfolgt jedoch eine kurze Einführung in den Ablauf des Bauleitplanverfahrens, wobei auch zur Sprache kommt, welche Potenziale digitale, einschließlich virtueller Formate – auch über das geltende Recht hinaus – entfalten könn(t)en (B.). Den Schluss des Beitrags bilden eine Zusammenfassung sowie ein Ausblick (E.).

B. Das Bauleitplanverfahren und die Chancen der Digitalisierung

Am Anfang des Verfahrens steht der *Aufstellungsbeschluss* der Gemeinde.[5] Er enthält i.d.R. bereits die groben Planungszüge, zu deren Visualisierung ein 3D-Modell zum Einsatz kommen kann; derartige Modelle haben den Vorteil, dass sie für Bürgerinnen und Bürger sowie Kommunalpolitikerinnen und -politiker, die typischerweise keine juristische und/oder planerische Ausbildung genossen haben, leichter verständlich sind[6]. Der Beschluss, einen Bauleitplan aufzustellen, ist sodann ortsüblich bekannt zu machen, § 2 Abs. 1 S. 2 BauGB. Erfolgt diese *Bekanntmachung* – im Rahmen des rechtlich zulässigen – (ausschließlich) im Internet, fördert dies die Transparenz und Verfahrensakzeptanz. Soweit auf die fehlende Anstoßfunktion digitaler Bekanntmachungen verwiesen wird,[7] ist zu bedenken, dass diese Funktion in Zeiten zurückgehender Reichweiten klassischer Printzeitungen analog auch kaum besser erfüllt werden könnte[8]. Auf die Bekanntmachung des Aufstellungsbeschlusses folgt die Erstellung des eigentlichen *Planungskonzepts*, was wiederum unter Nutzung virtueller Formate geschehen kann. Der so erarbeitete Vorentwurf ist der Öffentlichkeit, Behörden sowie sonstigen Trägern öffentlicher Belange zugänglich zu

4 Zur Verkürzung der Frist für die Genehmigung von Flächennutzungsplänen von drei Monaten auf einen Monat in § 6 Abs. 4 S. 1 BauGB etwa *M. Arndt/B. Herzer*, Neue Verfahrensanforderungen in der Bauleitplanung aufgrund der BauGB-Digitalisierungsnovelle, UPR 2023, 475 (482 f.) sowie zur erneuten Beteiligung nach § 4a Abs. 3 BauGB, die hier ebenfalls nicht behandelt wird, ebd., 480 f.

5 Vgl. dazu und zum Folgenden die Verfahrensübersicht bei *W. Söfker*, in: W. Ernst/W. Zinkahn/W. Bielenberg/M. Krautzberger, Baugesetzbuch, August 2018 Lfg. 130, § 2 Rn. 33 ff.; ferner *A. Brade/A. Ebner*, Baurecht Sachsen, 4. Auflage, Baden-Baden 2023, § 5 Rn. 10 ff.

6 Dazu unten D. III.

7 *J. Ziekow/T. Ziemer/F. Bickmann*, Evaluation des Planungssicherstellungsgesetzes (PlanSiG), Speyer 2022, S. 20.

8 *P. Durinke/T. Elgeti*, Digitalisierung der Öffentlichkeitsbeteiligung – die Integration des PlanSiG in das VwVfG, NVwZ 2024, 112 (114).

machen und ihnen ist Gelegenheit zur Stellungnahme zu geben, §§ 3 Abs. 1, 4 Abs. 1 BauGB (*frühzeitige Öffentlichkeits- und Behördenbeteiligung*). Auf welchem Wege das zu geschehen hat, lässt das Gesetz offen; zulässig ist es jedenfalls, die Beteiligung (auch) über das Internet zu ermöglichen.[9] Geschieht dies, senkt das die Hemmschwelle, die Unterlagen einzusehen, da der Zugang unabhängig von Ort und Zeit möglich ist. Auch fallen die physischen Barrieren für behinderte Menschen weg, sofern die elektronischen Dokumente barrierefrei zugänglich sind, was die Inklusion fördert.[10]

Im Anschluss an die frühzeitige Öffentlichkeits- und Behördenbeteiligung wertet die Gemeinde die eingegangenen Anregungen und Stellungnahmen aus und überarbeitet das Planungskonzept entsprechend, worauf der *Auslegungsbeschluss* folgt.[11] Die Einberufung und/oder Beschlussfassung im Gemeinderat kann dabei abhängig von den jeweiligen kommunalrechtlichen Vorschriften auch elektronisch erfolgen,[12] was unter Umständen einer größeren Zahl von Mitgliedern die Teilnahme ermöglicht. Für die *Bekanntmachung* des Auslegungsbeschlusses gilt das für den Aufstellungsbeschluss Gesagte entsprechend. Das überarbeitete Planungskonzept ist sodann (erneut) der Öffentlichkeit, Behörden sowie sonstigen Trägern öffentlicher Belange zur Verfügung zu stellen, um ihnen die Möglichkeit der (ggf. elektronischen) Stellungnahme zu geben, §§ 3 Abs. 2, 4 Abs. 2 BauGB (*förmliche Öffentlichkeits- und Behördenbeteiligung*). Die Veröffentlichung des Bebauungsplanentwurfs im Internet reduziert den Zeitaufwand für die Betroffenen und die Gemeinde; auch führt die leichtere Zugänglichkeit und Durchsuchbarkeit der bereitgestellten Unterlagen bestenfalls zu informierteren Stellungnahmen.[13] Zwar geht dies auf Kosten der persönlichen Kommunikation mit den Einsichtnehmenden,[14] diese Möglichkeit war aber erstens auch bisher nicht immer gegeben (etwa bei auseinanderfallenden Zuständigkeiten)[15] und zweitens stets es der Gemeinde frei, zusätzliche Kommunikationskanäle zu schaffen[16]. Auf die (erneute) Auswertung der Beteiligung folgt schließlich der Beschluss des überarbeiteten Planungskon-

9 Vgl. *A. Schink/P. Bachmann*, in: W. Spannowsky/M. Uechtritz (Hrsg.), BeckOK BauGB, 63. Ed. 01.08.2024, § 3 Rn. 36 f. Dazu auch unten D. II.
10 *A. Guckelberger*, Die Digitalisierung der Bauleitplanung, DVBl 2024, 1 (2).
11 Vgl. nur *Schink/Bachmann* (Fn. 9), § 3 Rn. 69.
12 Dazu unten D. II.
13 *Durinke/Elgeti*, Öffentlichkeitsbeteiligung (Fn. 8), 114.
14 *Ziekow/Ziemer/Bickmann*, Evaluation (Fn. 7), S. 29.
15 *Durinke/Elgeti*, Öffentlichkeitsbeteiligung (Fn. 8), 114.
16 *Guckelberger*, Digitalisierung (Fn. 10), 2.

zepts, § 10 Abs. 1 BauGB (*Satzungsbeschluss*), der (ggf. abermals im Internet) bekanntzumachen ist.

C. Gesetz zur Stärkung der Digitalisierung im Bauleitplanverfahren

Die Digitalisierung hielt früh in der Bauleitplanung Einzug. Bereits im Jahr 2004 wurde in § 4a Abs. 4 BauGB geregelt, dass bei der Öffentlichkeits- und Behördenbeteiligung ergänzend „elektronische Informationstechnologien" genutzt werden können.[17] War die Veröffentlichung im Internet zunächst noch freiwillig, wurde sie 2017 verbindlich, allerdings weiterhin in Ergänzung zur öffentlichen Auslegung nach § 3 Abs. 2 BauGB. § 4a Abs. 4 S. 1 BauGB a.F. lautete: Der Inhalt der ortsüblichen Bekanntmachung nach § 3 Absatz 2 S. 2 und die nach § 3 Abs. 2 S. 1 auszulegenden Unterlagen sind *zusätzlich* in das Internet einzustellen und über ein zentrales Internetportal des Landes zugänglich zu machen.[18] Nicht mehr als bloße Ergänzung, sondern als Regelfall sah der im Zuge der Corona-Pandemie erlassene § 3 PlanSiG die Beteiligung über das Internet vor.[19] Verstetigt hat sich diese Rechtslage mit dem Gesetz zur Stärkung der Digitalisierung im Bauleitplanverfahren, das am 06.07.2023 verkündet wurde.[20]

I. Förmliche Öffentlichkeitsbeteiligung (§ 3 Abs. 2 BauGB)

Der Systemwechsel bei der förmlichen Öffentlichkeitsbeteiligung schlägt sich zunächst in § 3 Abs. 2 S. 1 BauGB nieder: Anstelle der Auslegung der Entwürfe der Bauleitpläne in Papierform steht nun die Veröffentlichung dieser Unterlagen im Internet an erster Stelle. Auch wurde § 3 Abs. 2 S. 4 Hs. 2 Nr. 2 BauGB dahingehend geändert, dass Stellungnahmen zukünftig in elektronischer Form übermittelt werden „sollen". Die mit diesem Systemwechsel gegebenenfalls verbundenen Zugangshindernisse und technologischen Barrieren[21] versucht der Gesetzgeber dadurch abzufedern, dass er bei § 3 Abs. 2 S. 2 BauGB zusätzlich stets eine oder mehrere andere „leicht zu

17 BGBl. 2004 I S. 1359 (1366).
18 BGBl. 2017 I S. 3634 (3642).
19 BGBl. 2020 I S. 1041 (1042).
20 BGBl. 2023 I Nr. 176.
21 Vgl. BT-Drucks. 20/5663, S. 14.

erreichende Zugangsmöglichkeiten" fordert, zum Beispiel durch öffentlich zugängliche Lesegeräte oder durch eine öffentliche Auslegung (= in Papierform) der in Satz 1 genannten Unterlagen.[22] Auch kann die Bereitstellung der Unterlagen „bei Bedarf", etwa bei Nutzung der in § 3 Abs. 2 S. 2 BauGB genannten einfachen Zugangsmöglichkeiten,[23] auch in nicht-elektronischer Form erfolgen, § 3 Abs. 2 S. 4 Hs. 2 Nr. 2 BauGB.

II. Förmliche Behördenbeteiligung (§ 4 Abs. 2 BauGB)

Einen Schritt weiter als bei der Öffentlichkeitsbeteiligung ist der Gesetzgeber bei der förmlichen Beteiligung der Behörden und sonstigen Träger öffentlicher Belange nach § 4 Abs. 2 BauGB[24] gegangen. So wurde die „Kann-Regelung" in § 4a Abs. 4 S. 2 BauGB a.F. durch die „Soll-Regelung" in § 4 Abs. 2 S. 2 BauGB abgelöst: Danach soll die Bereitstellung der Unterlagen sowie die Mitteilung hierüber elektronisch erfolgen. Die „Soll-Regelung" drückt aus, dass hiervon nur in atypischen Ausnahmefällen abgewichen werden kann (z.B. Stromausfall, Hacker-Angriff); ein Mangel über eine ausreichende Ausstattung mit der notwendigen Informationstechnik stelle hingegen keinen Grund für eine Abweichung dar.[25]

III. Weitere Änderungen

§ 4a BauGB in der Fassung des Gesetzes zur Stärkung der Digitalisierung im Bauleitplanverfahren enthält vor allem Folgeänderungen. Neu hinzugekommen ist lediglich Absatz 6. Danach richtet sich die Digitalisierung des Bauleitplanverfahrens im Übrigen nach den Beschlüssen des IT-Planungsrats zur Festsetzung von IT-Interoperabilitäts- und IT-Sicherheitsstandards sowie den Vorgaben des Online-Zugangsgesetzes, soweit die Beschlüsse und die Vorgaben für die Gemeinden verbindlich sind. Da sich die Verbindlichkeit für die Gemeinden bereits aus anderen Gründen ergibt, han-

22 Vgl. *A. Kukk*, Stolpersteine der Veröffentlichung im Internet: Praktische Hinweise zum (vermeintlichen) Ende der analogen Auslegung von Bauleitplanentwürfen, BauR 2024, 709 (712): analoge Auslegung besteht im Rahmen einer ergänzenden Auslegung fort.

23 BT-Drucks. 20/5663, S. 14.

24 Ausführlich dazu: *Arndt/Herzer*, Verfahrensanforderungen (Fn. 4), 479 f.

25 BT-Drucks. 20/5663, S. 14.

delt es sich bei § 4a Abs. 6 BauGB um eine deklaratorische Regelung.[26] Auch ist nicht zu erwarten, dass das „Online-Zugangsgesetz 2.0"[27] spürbare Auswirkungen auf das Bauleitplanverfahren haben wird, da es Bund und Länder dazu verpflichtet, ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten (§ 1a Abs. 1 S. 1 OZG), was sich bereits aus den Vorgaben des – insoweit spezielleren – § 3 Abs. 2 S. 5 Hs. 2 BauGB ergibt.[28] Anders verhält es sich mit den Beschlüssen des IT-Planungsrats, dessen Aufgaben in § 1 IT-Staatsvertrag[29] normiert sind. Dazu gehört u.a. der Beschluss fachunabhängiger und fachübergreifender IT-Standards. Bereits im Jahr 2017 beschlossen wurde der Standard XPlanung, ein Datenformat für die Anwendung in kommunalen Softwarelösungen rund um die Bauleitplanung, der durch den Bund und die Länder bis zum Jahr 2023 einzuführen war[30] und auf den später zurückzukommen sein wird[31].

D. Eine verpasste Chance?

I. Bewertung der Gesetzesnovelle

Das Gesetz zur Stärkung der Digitalisierung im Bauleitplanverfahren hält kaum, was sein Name verspricht.[32] Der Bundesrat konnte sich nicht mit seiner Forderung durchsetzen, das Prinzip „digital only" für das Bauleitplan-

26 *Guckelberger*, Digitalisierung (Fn. 10), 8.

27 Bundesministerium des Innern und für Heimat, OZG-Änderungsgesetz: Paket für die digitale Verwaltung, https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/das-gesetz/ozg-aenderungsgesetz/ozg-aenderungsgesetz-node.html, zuletzt abgerufen am 16.09.2024.

28 Vgl. *Arndt/Herzer*, Verfahrensanforderungen (Fn. 4), 482.

29 Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG (IT-Staatsvertrag), Bekanntmachung der Neufassung v. 13.12.2019, BGBl. 2019 I S. 2852.

30 Handreichung XPlanung und XBau, https://www.staedtetag.de/files/dst/docs/Publikationen/Weitere-Publikationen/Archiv/xplanung-xbau-2018.pdf, S. 8 f., zuletzt abgerufen am 16.09.2024.

31 Dazu D. III.

32 *M. Klein*, Die Digitalisierung der Bauleitplanung – ändert sich überhaupt was?, JuWissBlog v. 02.08.2023, https://www.juwiss.de/46-2023/, zuletzt abgerufen am 16.09.2024.

verfahren festzuschreiben.[33] Stattdessen hält der Gesetzgeber bei der förmlichen Öffentlichkeitsbeteiligung am Hybridmodell aus Veröffentlichung der Dokumente im Internet und analoger Auslegung fest. Das ist auch deshalb bedauerlich, weil sich die „Gewährleistung einer Teilhabemöglichkeit für möglichst weite Teile der Bevölkerung"[34] auch mittels öffentlich zugänglicher elektronischer Lesegeräte erreichen lässt – der in § 3 Abs. 2 S. 2 BauGB vorgesehenen zusätzlichen Möglichkeit, die Unterlagen in Papierform auszulegen, bedarf es dafür nicht. Diese Regelung nehmen Teile des Schrifttums nunmehr zum Anlass, „zur Verringerung der Benachteiligung weniger computeraffiner Bevölkerungsteile" entgegen des Gesetzeszwecks, die Papierauslegung perspektivisch abzuschaffen, weiterhin die Durchführung einer analogen Papierauslegung zu empfehlen.[35]

Die Bewertung der Neufassung der förmlichen Behördenbeteiligung i.S.d. § 4 Abs. 2 BauGB fällt nur wenig milder aus; eine ausschließlich digitale Beteiligung ist auch hier nicht vorgesehen. Statt einer „Muss-Regelung" hat sich der Gesetzgeber für eine „Soll-Regelung" entschieden. Von der Rechtsprechung wird insbesondere zu klären sein, welche atypischen Ausnahmefälle ein Abweichen von der digitalen Beteiligung rechtfertigen. Auslegungsbedürftig erscheint auch der Begriff der „elektronischen Übermittlung". Während manche Gemeinden die Abgabe der Stellungnahme per E-Mail vorsehen, greifen andere nun auf eigens dafür angelegte Internet-Plattformen zurück, bei denen sich die Stellungnehmenden erst anmelden müssen.[36] Diskutabel erscheint außerdem, ob die Versendung von USB-Sticks und CDs den Anforderungen des § 4 Abs. 2 S. 2 BauGB entspricht.[37] Diese und andere Fragen verleiten Literaturstimmen gar dazu,

33 BT-Drucks. 20/5663, S. 21. *Guckelberger*, Digitalisierung (Fn. 10), 2 und *T. Siegel*, Digitalisierungsschleusen im Verwaltungsrecht und seine Offenheit für Künstliche Intelligenz, NVwZ 2024, 1127 (1132) halten die Beibehaltung analoger Kontaktformen und eine gewisse Zurückhaltung des Gesetzgebers hingegen für begrüßenswert; *A. Kukk*, Stolpersteine der Veröffentlichung im Internet – praktische Hinweise zum (vermeintlichen) Ende der analogen Auslegung von Bauleitplanentwürfen, DVBl 2024, 257 (258) hätte sich sogar (weiter) eine zwingende analoge Auslegung der Planunterlagen gewünscht.

34 BT-Drucks. 20/5663, S. 13.

35 *Kukk*, Stolpersteine (Fn. 33), 257 u. 259.

36 *P. Bachmann*, Digitale Öffentlichkeitsbeteiligung – Effizienzgewinn oder Fehlerquelle?, NJW-Spezial 2024, 428.

37 I.E. zustimmend *Guckelberger*, Digitalisierung (Fn. 10), 7.

Behörden und Trägern öffentlicher Belange sicherheitshalber zugleich die Stellungnahme mit Zugangsnachweis per Fax (!) zu empfehlen.[38]

Auch welche Anforderungen § 3 Abs. 2 S. 1 BauGB an die tatsächliche Zugänglichkeit der Unterlagen im Internet stellt, muss erst noch von der Rechtspraxis geklärt werden.[39] Angesichts der in der Praxis vorkommenden Unübersichtlichkeit kommunaler Web-Auftritte sei es dem

„‚mündigen Bürger' [jedenfalls] nicht zuzumuten, sich erst durch Grußworte der Bürgermeisterin und zahlreiche andere kommunale Informationen zu ‚clicken', bis man auf einer weit untergeordneten Ebene auf die ‚veröffentlichten' Unterlagen stößt."[40]

Klärungsbedürftig erscheint schließlich, welche „leicht zu erreichenden Zugangsmöglichkeiten" § 3 Abs. 2 S. 2 BauGB neben der dort genannten Bereitstellung öffentlich zugänglicher elektronischer Lesegeräte sowie der „klassischen" Papierauslegung unterfallen: Zurverfügungstellung des Materials mit Termin beim Sachbearbeiter vor Ort,[41] Versand der Unterlagen in Papierform oder elektronische Versendung der Unterlagen[42]? Nach all dem erscheint schon zweifelhaft, ob die Novelle überhaupt eine Vereinfachung für die Öffentlichkeit oder für die planaufstellende Stelle bedeutet, zumal eine Vielzahl der Gemeinden ihre Verfahren bereits zuvor entsprechend gehandhabt haben und die – ggf. parallele – Bereitstellung von Unterlagen in Papierform den Aufwand unverändert hoch hält. Insofern ist auch eine Beschleunigung des Verfahrens kaum zu erwarten, zumal die Zeitintensität der Bauleitplanverfahren maßgeblich aus der inhaltlichen Komplexität der Materie resultiert.[43]

38 *Kukk*, Stolpersteine (Fn. 33), 260.

39 Dazu ausführlich *Arndt/Herzer*, Verfahrensanforderungen (Fn. 4), 476 u. 478; *Guckelberger*, Digitalisierung (Fn. 10), 6 f. je m.w.N.

40 *Kukk*, Stolpersteine (Fn. 33), 258.

41 Vgl. *Guckelberger*, Digitalisierung (Fn. 10), 3.

42 Bejahend für Papierform und verneinend für elektronische Übersendung *Arndt/Herzer*, Verfahrensanforderungen (Fn. 4), 477.

43 Ähnlich *Guckelberger*, Digitalisierung (Fn. 10), 1; *B. Herzer*, Digitalisierung der Beteiligung in der Landes- und Regionalplanung – Neuerungen durch das ROGÄnd, UPR 2023, 331 (339).

II. Was fehlt?

Das Potenzial digitaler Planungsverfahren schöpft der Gesetzgeber mit der BauGB-Novelle bei weitem nicht aus. Zunächst setzt sie erst bei der förmlichen und nicht schon bei der frühen Öffentlichkeits- und Behördenbeteiligung (§§ 3 Abs. 1, 4 Abs. 1 BauGB) an. Zwar nutzen viele Gemeinden inzwischen das Internet, um zu einer frühzeitigen Bürgerbeteiligung einzuladen. Da sich § 3 Abs. 1 S. 1 BauGB auf die gesamte Öffentlichkeit bezieht, dürfte es aber im Rahmen der frühzeitigen Öffentlichkeitsbeteiligung weiter zwingend analoger Beteiligungsformate bedürfen.[44] Unverändert bleiben auch die Regelungen zur ortsüblichen Bekanntmachung des Aufstellungsbeschlusses (§ 2 Abs. 1 S. 2 BauGB) sowie die Vorschriften über die Bekanntmachung der Pläne (§§ 6 Abs. 5, 10 Abs. 3 BauGB). Die Wirksamkeit der Bekanntmachungen bestimmt sich damit weiterhin nach Landesrecht (sowie ggf. den jeweiligen Hauptsatzungen der Gemeinden). Insofern sind zumindest erhebliche Fortschritte erzielt worden. So sind in einigen Ländern Bekanntmachungen ausschließlich im Internet zulässig, etwa in Niedersachsen (§ 11 Abs. 1 S. 2 Nr. 3 NKomVG) oder Nordrhein-Westfalen (§ 4 Abs. 1 S. 1 Nr. 4 Bekanntmachungsverordnung). Ebenfalls weiter nach Landesrecht richtet sich die Frage, ob eine elektronische Einberufung des Gemeinderats wie z.B. in Sachsen (§ 36 Abs. 3 S. 1 SächsGemO) bzw. die Durchführung von Sitzungen ohne persönliche Anwesenheit im Sitzungsraum (vgl. etwa § 37a BWGemO für Baden-Württemberg) rechtlich zulässig sind.

III. Digitale Bauakte und virtuelle Darstellung

Solange Antragsunterlagen, Gutachten und Pläne nicht für die gesamte Verfahrensdauer von sämtlichen Beteiligten durchgängig digital abgerufen und bearbeitet werden können, kann von einem „vollständig digital zu führenden Verfahren“[45] nicht die Rede sein. Eine komplett digitale Bauakte würde auch den Weg ebnen für den Einsatz eines KI basierten Einwendungsmanagements[46] oder zur Nutzung neuer Techniken zur Bürgerbeteili-

44 So auch *Arndt/Herzer*, Verfahrensanforderungen (Fn. 4), 475 m.w.N.

45 BT-Drucks. 20/5663, S. 13.

46 Ausschuss-Drucks. 20(24)114-D, S. 6. *Guckelberger*, Digitalisierung (Fn. 10), 1 begrüßt angesichts der damit verbundenen Rechtsfragen, insbesondere wegen des Erlasses

gung, bei der die Planungsdaten mittels Virtual oder Augmented Reality dargestellt werden[47]. Das Grundproblem der herkömmlichen Darstellung von Bauleitplänen – sei es in Papierform oder digital als pdf-Datei – stellt die Reduzierung dreidimensionaler Sachverhalte auf zwei Dimensionen dar. Dazu muss sich die städtebauliche Planung vielfältiger Mittel wie z.B. Abstraktionen, Symbolen und Fachbegriffen bedienen, worunter die Verständlichkeit insbesondere für die Bürgerinnen und Bürger erheblich leidet. Auch zwingt es die beteiligten Personen, gedanklich selbst eine 3D-Ansicht zu erzeugen. Dadurch können unterschiedliche Vorstellungen der Planung entstehen, was Kommunikationsschwierigkeiten bedingen kann.[48]

„Der Einsatz von 3D-Modellen ermöglicht dagegen die Darstellung der Planinhalte in derselben Dimension wie die Realität und versucht damit, dem Betrachter in der Interpretation des Gesehenen durch einen weniger hohen Abstraktionsgrad entgegenzukommen.“[49]

Die Umsetzung in 3D unterstützt so eine Beteiligung der Öffentlichkeit im Bauleitplanverfahren. Insbesondere macht sie es möglich, interaktiv erste Sichtachsen- und Schattenwurfanalysen durchzuführen – auch um seitens der planaufstellenden Stelle, i.d.R. der Gemeinde, auf eventuelle Bedenken eingehen zu können. Auf diese Weise können Einwendungen minimiert und personelle sowie finanzielle Kosten reduziert werden. Fließen zusätzlich Simulationen von Verkehrsströmen oder Umwelteinflüssen ein, um die Auswirkungen eines Vorhabens zu prognostizieren, steigert dies nicht nur die Akzeptanz von Planungen in der Bevölkerung, sondern verhindert Fehlplanungen noch vor deren Realisierung.

Dreidimensional dargestellt werden können, wie die folgende Abbildung[50] in Ansätzen verdeutlicht, z.B.

---

einer KI-Verordnung der Europäischen Union – verabschiedet am 13.06.2024 als Verordnung (EU) 2024/1689 (ABl. L, 2024/1689) – die diesbezügliche Zurückhaltung des Gesetzgebers. Allgemein zum Einsatz von KI: *Siegel*, Digitalisierungsschleusen (Fn. 33), 1127.

47 Ausschuss-Drucks. 20(24)114-C, S. 3.

48 *R. Levy*, Virtual Reality: A Tool for Urban Planning and Public Engagement, University of Calgary, Canada, 2011, S. 3.

49 *T. Besser*, Städtebauliche Planung in der 3. Dimension – Einsatzmöglichkeiten der Virtual Reality Modeling Language (VRML), Kaiserslautern 1999, S. 3.

50 *E. Schröter*, VC Map goes XPlanung, 2023, S. 11, https://vc.systems/wp-content/uploads/2023/07/vc-map-goes-xplanung.pdf, zuletzt abgerufen am 16.09.2024.

- Höhen-/Vollgeschossangaben für überbaubare Grundstücksflächen
- Höhenangaben zu technischen Anlagen und/oder Immissionsschutzmaßnahmen
- Informationen über Anpflanzungen (Höhe, Durchmesser, Pflanztiefe)
- Angaben zu unter-/überirdischen Bereichen geplanter Gebäude und Anlagen, darunter z.B. Versorgungsleitungen, Kanäle, Tiefgaragen, etc.[51]

Eine noch intensivere Immersion bieten Virtual oder Augmented Reality.[52] Können bei dem Ansatz der Virtual Reality stadtplanerische Situationen in einer computergenerierten Umwelt durchlaufen werden, kann die gleiche Situation beim Augmented Reality Verfahren in der real existierenden Umwelt simuliert werden.[53] Bei einer so nachgebildeten Umwelt können

51 Ausführlich zu den Möglichkeiten der Visualisierung von planerischen Festsetzungen *D. Broschart*, Bebauungsplan 3D? Die Möglichkeiten der Visualisierung von planerischen Festsetzungen, Kaiserslautern 2011, S. 15 ff., https://zeile.net/wp-content/uploads/2016/12/Bebauungsplan_3D_Daniel_Broschart_web.pdf, zuletzt abgerufen am 16.09.2024.

52 Mit einem Vergleich zwischen 3D-Computergrafik und Virtual Reality: *S. Dübner*, Virtual Reality im Planungsprozess: Anwendung am Beispiel des Bahnhofareals in Neustadt an der Weinstraße, Kaiserslautern 2014, S. 5, https://zeile.net/wp-content/uploads/2016/11/Masterarbeit_Sven_D%C3%BCbner_Virtual_Reality_im_Planungsprozess_06-10-14.pdf, zuletzt abgerufen am 16.09.2024. Aus österreichischer Perspektive *A. Leimer*, Anwendung von Virtual Reality in der Planungspraxis, Wien 2018, S. 15 ff., https://repositum.tuwien.at/bitstream/20.500.12708/6996/2/Leimer%20Andreas%20-%202018%20-%20Anwendung%20von%20Virtual%20Reality%20in%20der%20Planungspraxis.pdf, zuletzt abgerufen am 16.09.2024.

53 *Broschart*, Bebauungsplan 3D? (Fn. 51), S. 12. Ausführlich zum Augmented Reality-Verfahren ebd., S. 52 ff.

die Bürgerinnen und Bürger nicht nur sehen, sondern erleben, was sich durch ein Vorhaben verändert. Es obliegt dann ihrer Entscheidung, welchen Standpunkt sie für die Betrachtung einnehmen. Zu sehen sein können der genaue Standort und dessen Alternativen, die Umgebungs(-bebauung), Straßen mit fließendem Verkehr (einstellbar nach Tageszeit) usw.[54] Denkbar erscheint auch die Integration von Humansensorik in die Visualisierung von Virtual Reality-Planungsprozessen, um so Angsträume im Stadtraum oder unübersichtliche und komplizierte Straßen- und Wegeführungen im Fall von Neuplanungen zu vermeiden.[55]

Trotz dieser Möglichkeiten werden 3D-Modelle bisher vor allem eingesetzt, um städtebauliche Entwürfe oder gestalterische Maßnahmen zu visualisieren. In den darauf aufbauenden Phasen der Entwicklung eines Bebauungsplans werden sie nur in seltenen Ausnahmefällen eingesetzt.[56] Das liegt einerseits an den oftmals fehlenden technischen und personellen Voraussetzungen, andererseits an rechtlichen Hürden. Zumindest erlaubt der kürzlich eingeführte Standard XPlanung neben der digitalen, standardisierten Erfassung und Bearbeitung von Bauleitplänen auch die Konvertierung von 2D-Plandateien in die 3D-Umgebung.[57] Nicht angepasst worden ist dagegen bislang die Planzeichenverordnung[58]. Sie regelt die in Bauleitplänen nach dem BauGB zu verwendenden Planzeichen und beschränkt sich insoweit auf 2D-Darstellungen. Diese müssten ergänzt – und perspektivisch ersetzt – werden durch 3D-Planzeichen; dadurch entfiele auch die bisher erforderliche Umwandlung von 3D-Grafikobjekten in 2D-Planzeichen.

E. Fazit und Ausblick

Das Gesetz zur Stärkung der Digitalisierung im Bauleitplanverfahren bringt sein Anliegen nicht entscheidend voran. Es wirft nicht nur zahlreiche

54 *Leimer*, Planungspraxis (Fn. 52), S. 37 sieht Vorteile der Virtual Reality-Visualisierung von Plänen auf allen drei Intensitätsstufen der Partizipation – Information, Konsultation und Kooperation.

55 *Dübner*, Virtual Reality (Fn. 52), S. 44.

56 *Broschart*, Bebauungsplan 3D? (Fn. 51), S. 9.

57 Näher *E. Schröter*, XPlanung von 2D zu 3D: Automatisierte BPlan-Integration im Digitalen Zwilling, Widemann-Journal, 2. Ausgabe 2022, S. 5, https://www.widemann.de/sites/default/files/downloads/journale/widemannjournal_22A2_300dpi.pdf#page=5, zuletzt abgerufen am 16.09.2024.

58 Verordnung über die Ausarbeitung der Bauleitpläne und die Darstellung des Planinhalts (Planzeichenverordnung – PlanZV) v. 18.12.1990 (BGBl. 1991 I S. 58), zuletzt geändert durch Art. 3 BaulandmobilisierungsG v. 14.06.2021 (BGBl. 2021 I S. 1802).

(neue) Auslegungsfragen auf, sondern behält das Hybridmodell aus analoger und digitaler (Öffentlichkeits-)Beteiligung bei. Dabei gilt für eine ausschließlich digitale Beteiligung seit geraumer Zeit:

> *„Die bisweilen anzutreffende Behauptung, dass hierdurch ein Großteil der Bevölkerung technisch abgehängt werde, trifft aus hiesiger Sicht und praktischer Erfahrung nicht zu. Vielmehr erleichtert die Digitalisierung die Informationsbeschaffung für den Bürger. Damit einher geht jedenfalls das Potenzial der Verbesserung von Akzeptanz und Konfliktbewältigung durch die umfassende Informationsbereitstellung.“*[59]

Weder ergreift das Gesetz die Chance, für eine kontinuierliche digitale Verfahrenstransparenz durch eine durchgängig digitale Abrufbarkeit der Daten zu sorgen, noch adressiert es den Einsatz von KI oder die Möglichkeit, Planungsdaten dreidimensional darzustellen, um sie für die Bürgerinnen und Bürger verständlicher darzustellen und den Planungsprozess zu vereinfachen. Im Ergebnis dürften die beschleunigenden Effekte der Änderungen im Beteiligungsverfahren eher überschaubar sein, zumal die Dauer von Planverfahren in der Bauleitplanung in aller Regel weniger von den (Mindest-)Anforderungen an das Planverfahren abhängt, sondern vielmehr von der Bewältigung materiell-rechtlicher Anforderungen, der technischen Ausstattung der Planungsverwaltungen sowie einer personell leistungsfähigen Verwaltungsstruktur.[60] Immerhin zeigt sich der Gesetzgeber perspektivisch offen dafür, die Beteiligungsvorschriften „in Richtung eines vollständig digital zu führenden Verfahrens“ weiterzuentwickeln.[61] Entscheidende Impulse dafür dürfte die in § 245f Abs. 2 BauGB vorgesehene Evaluation der Änderungen der §§ 3, 4, 4a BauGB liefern. So, stay tuned!

59 *B. Dammert/G. Brückner*, Lehren aus dem PlanSiG – Welche Elemente der Digitalisierung könnten auch künftig zur Verfahrensbeschleunigung beitragen?, EnZW 2022, 111 (113).

60 Vgl. *Herzer*, Neuerungen durch das ROGÄndG (Fn. 43), 339. *Dammert/Brückner*, Verfahrensbeschleunigung (Fn. 59), 116 sehen in der technischen und personellen Ausstattung die „größte (politische) Herausforderung“.

61 BT-Drucks. 20/5663, S. 13.

Das Verbot der Totalausforschung und seine digitale Zukunft

Nicolas Ziegler

A. Die Angst vor der Totalüberwachung

Die Totalüberwachung ist eine beliebte journalistische Projektion,[1] die auch jüngst im Rahmen des sog. Sicherheitspakets[2] der Bundesregierung als Reaktion auf den terroristischen Anschlag am 23.08.2024 in Solingen zur Bewertung konkreter sicherheitspolitischer Vorhaben eine Rolle gespielt hat.[3] Der Topos des totalen Überwachungsstaates rangiert zwischen den Polen einer historisch sensiblen deutschen Öffentlichkeit und einer aufmerksamkeitsökonomischen Verteidigung von Freiheitsrechten. Seit den 1970er-Jahren begleitet die Kritik am Überwachungsstaat die sicherheitsrechtlichen Debatten in Deutschland.[4]

I. Rezeption in Literatur und darstellender Kunst

Die Kritik an der Schaffung eines Überwachungsstaates findet sich ebenso in der darstellenden Kunst. Sowohl fiktionale Spielfilme wie „Minority Report", aber auch Werke mit realen Bezügen wie „Das Leben der Anderen" beschäftigen sich damit. Der Fixpunkt der literarischen Aufarbeitung des Themas ist und bleibt jedoch George Orwells Roman „1984".

1 Siehe nur *S. Krempl*, Faesers Fahndungsplan: Kritik an "Totalüberwachung des öffentlichen Raums", heise online v. 12.08.2024.

2 Hier allein von Interesse ist der Teil des Sicherheitspakets, der polizeiliche Ermittlungsbefugnisse ausweiten soll, Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung v. 09.09.2024, BT-Drs. 20/12806.

3 Vgl. den Überblick der Kritik bei *M. Reuter*, Massive Kritik am Sicherheitspaket der Ampel, netzpolitik.org. v. 11.09.2024.

4 *M. Kötter*, Pfade des Sicherheitsrechts, Baden-Baden 2008, S. 137 Fn. 694 m.w.N.

II. Rezeption in der Rechtswissenschaft

Während die Vergleichsfolie des orwellschen Überwachungsstaats in der politischen Argumentation ein legitimes Stilmittel sein kann, sollte die Rechtswissenschaft hierbei behutsamer vorgehen. Mit wenigen Ausnahmen[5] wird das juristische Schrifttum diesem Anspruch gerecht und zeichnet den Überwachungsstaat in der Regel nur als fernliegende Dystopie. Dennoch bringt die Literatur überwachungsstaatliche Dystopien in Verbindung mit konkreten Überwachungsmaßnahmen.[6] Über eine originelle Einleitung oder einen pointierten Schlusssatz hinaus vermag der Vergleich jedoch keinerlei Beitrag zur Fachdebatte zu leisten.[7]

III. Aufnahme des Topos durch das BVerfG

Auch das BVerfG hat sich in seiner Rechtsprechung bereits mit dem Überwachungsstaat oder vielmehr der totalen Überwachung auseinandergesetzt und klargestellt, dass eine Rundumüberwachung „von Verfassungs wegen stets unzulässig" ist.[8] Bei diesem Postulat ist es jedoch nicht geblieben und das BVerfG hat sich im Laufe seiner Rechtsprechung schon mehrfach zur Totalüberwachung geäußert, ohne jedoch den Inhalt und die Grenzen der Figur trennscharf zu bestimmen.

---

5 Besonders polemisch etwa *S. Schnorr*, Big Brother zur Verbrechensbekämpfung?, ZRP 2001, 291 (291 f.).

6 *D. Hauck*, Vorratsdatenspeicherung adé – hat ein orwellscher Albtraum vor dem BVerwG sein Ende gefunden?, jM 2024, 113*; M. Valta/J. Vasel,* Kommissionsvorschlag für eine Verordnung über Künstliche Intelligenz, ZRP 2021, 142 (143); *D. Uwer,* George Orwells „1984" – Antiutopie und Totalitarismuswarnung zwischen 1949 und 2009, NJW 2009, 723; BVerfG ZD 2018, 578 (582) m. Anm. *Kienle*; im Zusammenhang der Registermodernisierung *H. Bull,* Die Nummerierung der Bürger und die Angst vor dem Überwachungsstaat, DÖV 2022, 261.

7 *J. Schlömer*, Kontrollrechtliche Aspekte des Zugriffs von Nachrichtendiensten auf IT-Systeme, NVwZ 2023, 1121 (1127); *H. Bull,* Fehlentwicklungen im Datenschutz am Beispiel der Videoüberwachung, JZ 2017, 797 (797).

8 BVerfGE 112, 304 (319).

B. Das Totalüberwachungsverbot als Figur der verfassungsrechtlichen Dogmatik

Das sog. Totalüberwachungsverbot, synonym oft auch als Verbot der Rundumüberwachung bezeichnet, findet sich erstmals im Urteil des BVerfG zum großen Lauschangriff von 2004.[9] Das BVerfG entwickelt dieses Verbot in folgender Passage: „Die Menschenwürde wird auch verletzt, wenn eine Überwachung sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können".[10] Damit formuliert das Gericht eine spezifisch sicherheitsrechtliche rote Linie für staatliche Informationseingriffe.[11] Nachfolgend sollen zunächst die Entwicklungslinien bis zu diesem Urteil nachgezeichnet werden (I.), ehe das Totalüberwachungsverbot als eigenständige verfassungsrechtsdogmatische Figur beleuchtet werden soll (II.).

I. Vorarbeiten: Die Gefahr der Bildung von Persönlichkeitsprofilen in der Rechtsprechung des BVerfG

Dass eine vollkommene und umfassende Überwachung nicht mit der Verfassungsordnung des GG vereinbar sein kann, lässt sich der Rechtsprechung des BVerfG bereits vor der eben dargestellten expliziten Ausformulierung entnehmen. Bereits nach der Objektformel Dürigs, die das BVerfG in seine Rechtsprechung als negative Definition der Menschenwürde i.S.v. Art. 1 Abs. 1 GG übernommen hat,[12] wird die Menschenwürde verletzt, wenn „der konkrete Mensch zum Objekt, zu einem bloßen Mittel, zur vertretbaren Größe herabgewürdigt wird".[13] Die Herabwürdigung des Menschen zum bloßen Objekt staatlicher Datenverarbeitung nimmt das BVerfG

9 BVerfGE 109, 279.

10 BVerfGE 109, 279 (323).

11 Der Begriff der staatlichen Informationseingriffe fasst den sicherheitsbehördlichen Umgang mit Informationen eingriffs- und grundrechtsunabhängig bzw. übergreifend zusammen, vgl. zum Informationseingriff und seiner terminologischen Verwendung durch das BVerfG, *S. Tannenberger*, Die Sicherheitsverfassung, Tübingen 2014, S. 225 ff.

12 *T. Linke*, Die Menschenwürde im Überblick: Konstitutionsprinzip, Grundrecht, Schutzpflicht, JuS 2016, 888 (890 f.).

13 *G. Dürig*, Der Grundsatz von der Menschenwürde, AöR 81 (1956), 117 (127).

im Mikrozensus-Beschluss auf. Es konkretisiert den Verstoß dahingehend, dass es mit der Menschenwürde nicht zu vereinbaren ist, „wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren".[14] Damit steht bereits früh fest, dass die Bildung eines umfassenden Persönlichkeitsprofils einen Verstoß gegen Art. 1 Abs. 1 GG bedeutet. Von dieser Annahme, dass Menschen „einer Bestandsaufnahme in jeder Beziehung" verfassungsrechtlich nicht zugänglich sind,[15] ist es nur ein kleiner Schritt zum Schutz des Innenraums, der einem „um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen […] verbleiben muß".[16] Der menschenrechtswürdekonforme Schlusspunkt staatlicher Datenverarbeitung, das Persönlichkeitsprofil, hat sich ausgehend vom noch rudimentären Privatheitsschutz im Elfes-Urteil[17] und dem Mikrozensus-Beschluss[18] auch bei der Entwicklung des Rechts auf informationelle Selbstbestimmung im Volkszählungsurteil gehalten.[19] Was genau unter einem solchen umfassenden Persönlichkeitsbild verstanden werden kann, ist bis heute jedoch unklar.[20] Das BVerfG hat es bisher dabei bewenden lassen, lediglich vor der Gefahr solcher zu warnen.[21] Derartige Persönlichkeitsprofile dürfen nicht mit Profilen i.S.v. Art. 3 Nr. 4 JI-RL verwechselt werden, die nur „bestimmte persönliche Aspekte" betreffen.

II. Anerkennung als eigene dogmatische Figur

Das geschriebene Verfassungsrecht kennt nur wenige absolute und abwägungsfeste Grenzen für Grundrechtseingriffe. Hierzu zählt das Rückwirkungsverbot aus Art. 103 Abs. 2 GG, der Wesensgehalt der Grundrechte nach Art. 19 Abs. 2 GG und die Menschenwürdegarantie des Art. 1 Abs. 1

14 BVerfGE 27, 1 (6).
15 BVerfGE 27, 1 (6).
16 BVerfGE 27, 1 (5 f.).
17 BVerfGE 6, 32 (41).
18 BVerfGE 27, 1 (6).
19 BVerfGE 65, 1 (52 f.): Trotz der Weiterentwicklung des Privatheitsschutzes unter dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und seiner Ausprägung des Rechts auf informationeller Selbstbestimmung bleibt die „umfassende […] Katalogisierung der Persönlichkeit" in der Menschenwürde verankert.
20 Pionierarbeit leistet hier *C. Conrad*, Ein Update für den Kernbereichsschutz, Berlin 2024, S. 19 ff.
21 Zuletzt BVerfGE 141, 220 (280 Rn. 130); 156, 63 (123 Rn. 210).

GG.[22] Die Menschenwürde ist dabei aber in höchstem Maße offen und auslegungsbedürftig. Für das Sicherheitsrecht haben sich hier der Schutz des Kernbereichs privater Lebensgestaltung[23] und das Totalüberwachungsverbot[24] als absoluten Grenzen herauskristallisiert.

1. Menschenwürdeverstoß durch Rundumüberwachung

Seit der ersten Entwicklung des Totalüberwachungsverbots im Urteil zum großen Lauschangriff hat das BVerfG diese Figur, die es aus dem bereits im Volkszählungsurteil formulierten Risiko der Bildung von Persönlichkeitsprofilen zieht,[25] mehrfach wieder aufgegriffen. Bereits ein Jahr nach der ersten Konkretisierung betont das BVerfG in seiner Entscheidung zur GPS-Überwachung, dass eine Rundumüberwachung von Verfassungs wegen stets unzulässig ist.[26] Anders als beim Schutz des Kernbereichs privater Lebensgestaltung bedarf es aber keiner verfahrensrechtlichen Absicherung gegen einen Verstoß.[27] Im Urteil zur Vorratsdatenspeicherung warnt das BVerfG davor, dass eine anlasslose und massenhafte Speicherung von Telekommunikationsverkehrsdaten „als Schritt hin zu einer" Rundumüberwachung verstanden werden könnte.[28] Auch hier knüpft das BVerfG an das umfassende Persönlichkeitsprofil an, das es zu verhindern gilt.[29] Gleichzeitig stellt das BVerfG fest, dass das Totalüberwachungsverbot zur verfassungsrechtlichen Identität der Bundesrepublik i.S.v Art. 79 Abs. 3 GG zählt.[30] Im Jahr 2011 prüfte das BVerfG erstmals, ob eine konkrete akustische Wohnraumüberwachung gegen das Totalüberwachungsverbot versto-

22 Zur Unabwägbarkeit der Menschenwürde *F. Wapler*, in: H. Dreier (Hrsg.), Grundgesetz-Kommentar, Bd. I, 4. Aufl., Tübingen 2023, Art. 1 Abs. 1 Rn. 95 m.w.N.

23 Zur dogmatischen Einordnung *M. Eichberger*, in: P. Huber/A. Voßkuhle (Hrsg.), Grundgesetz-Kommentar, Bd. I, 8. Aufl., München 2024, Art. 2 Rn. 159 ff.

24 *I. Dammann*, Der Kernbereich der privaten Lebensgestaltung, Berlin 2011, S. 152; *C. Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, Tübingen 2017, S. 137.

25 BVerfGE 65, 1 (42 f.) worauf BVerfGE 109, 279 (323) verweist.

26 BVerfGE 112, 304 (319).

27 BVerfGE 112, 304 (319 f.).

28 BVerfGE 125, 260 (323 f.).

29 BVerfGE 125, 260 (324): „Sie [die Vorratsdatenspeicherung] darf auch nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen".

30 BVerfGE 125, 260 (324); bestätigt durch BVerfGE 156, 63 (123 Rn. 210).

ßen hat.[31] Im BKAG-Urteil von 2016 wiederholt das BVerfG das Verbot der Rundumüberwachung,[32] während es vorerst letztmalig im Beschluss vom 01.12.2020 zur elektronischen Aufenthaltsüberwachung thematisiert wird, in welchem das BVerfG herausarbeitet, dass die dauerhafte Bestimmung des Aufenthaltsortes alleine den Betroffenen noch nicht zum bloßen Objekt staatlichen Handelns macht.[33]

Auffallend ist dabei, dass die Thematisierung des Totalüberwachungsverbots durch das BVerfG durchgängig eine hohe sprachliche Konsistenz aufweist und eine Weiterentwicklung oder Schärfung der Konturen unterbleibt. Abstrakte Aussagen über das bloße Postulat des Verbots einer Totalüberwachung hinaus können nicht getroffen werden und eine praktische Handhabung gelingt nur entlang der Natur des Einzelfalls.[34]

2. Konturen des Tatbestands der Rundumüberwachung

Betrachtet man die eben genannten Urteile, lassen sich zwei Orientierungspunkte erkennen. *Erstens* sind die Eingriffsmodalitäten, konkret der Umfang und die Dauer einer Überwachung und nicht Inhalte oder Qualität vorrangige Parameter für die Prüfung.[35] *Zweitens* ist diese quantitative Betrachtung dahingehend zu überprüfen, ob sich aus den gesammelten Daten die Gefahr der Bildung eines Persönlichkeitsprofils ergibt.[36] Damit weist das Totalüberwachungsverbot nur wenig Konturen auf. Mit Blick auf die Eignung eines konkreten Datensatzes zur Bildung eines Persönlichkeitsprofils gibt es aber zumindest ein Kriterium für die Handhabung im Einzelfall. Vorhersagbar sind die Ergebnisse einer Prüfung damit jedoch nicht: Die Meinungen darüber, ob das Totalüberwachungsverbot im Einzelfall verletzt sein wird, werden stark divergieren und der eigentliche Vorteil einer absoluten Grenze für staatliche Informationseingriffe, die Rechtssicherheit,[37] kann nicht erreicht werden.

31 BVerfGE 130, 1 (24).
32 BVerfGE 141, 220 (280 Rn. 130).
33 BVerfGE 156, 63 (136 Rn. 251).
34 *T. Schwabenbauer*, Heimliche Grundrechtseingriffe, Tübingen 2013, S. 295.
35 *Schwabenbauer*, Grundrechtseingriffe (Fn. 34), S. 293; *Tanneberger*, Sicherheitsverfassung (Fn. 11), S. 136.
36 *F. Nicolai*, Das Internet der Dinge und das Strafrecht, Berlin 2024, S. 290 f.
37 *Schwabenbauer*, Grundrechtseingriffe, (Fn. 34), S. 253 m.w.N.

3. Abgrenzung

Aufgrund der Konturlosigkeit stellt sich die Frage, ob das Totalüberwachungsverbot tatsächlich eine eigenständige dogmatische Figur des BVerfG ist, oder nicht vielmehr die spezifische Subsumtion umfangreicher Überwachung unter andere dogmatische Schutzkonzepte der Privatheit. Aufgrund der Einzelfallfokussierung ist das Totalüberwachungsverbot jedenfalls keine bloße Warnung an den Sicherheitsgesetzgeber.[38]

a) Schutz des Kernbereichs privater Lebensgestaltung

Häufig wird ausgehend von einer missverstandenen Aussage des BVerfG[39] vertreten, dass das Totalüberwachungsverbot lediglich eine „Verletzungsmodalität" des Kernbereichs privater Lebensgestaltung ist.[40] Der Wortlaut („regelmäßig") legt hier jedoch nahe, dass eine Verletzung des Totalüberwachungsverbots auch möglich ist, wenn Daten ohne höchstpersönlichen Bezug zu einem Persönlichkeitsprofil zusammengesetzt werden.[41] Gleichwohl stellt ein Persönlichkeitsprofil, auch wenn es ohne jeden Kernbereichsbezug erstellt wurde, selbst eine kernbereichsrelevante Information dar, schließlich lässt sich aus großen Mengen von vermeintlich belanglosen Daten Höchstpersönliches rekonstruieren.[42] Eine Abgrenzung ist also nicht trivial.

38 So ist vielmehr die sog. Überwachungsgesamtrechnung zu verstehen, *J. Lindner/J. Unterreitmeier*, »Überwachungsgesamtrechnung«: Karlsruhe calculat?, JZ 2022, 915 (915).

39 BVerfGE 109, 279 (323): „Eine zeitliche und räumliche `Rundumüberwachung´ wird regelmäßig schon deshalb unzulässig sein, weil die Wahrscheinlichkeit groß ist, dass dabei höchstpersönliche Gespräche abgehört werden".

40 *M. Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung, Baden-Baden, 2007, S. 65; ähnlich *Tanneberger*, Sicherheitsverfassung (Fn. 11), S. 259; *T. Bode*, Verdeckte strafprozessuale Ermittlungsmaßnahmen, Berlin 2012, S. 162.

41 *Rottmeier*, Lauschangriffe (Fn. 24), S. 137.

42 *Conrad*, Kernbereichsschutz (Fn. 20), S. 30 ff.; vgl. BVerfGE 65, 1 (45): es gibt „kein „belangloses" Datum mehr".

b) Recht auf informationelle Selbstbestimmung

Auch wenn das Recht auf informationelle Selbstbestimmung Menschenwürdebezug aufweist, das Totalüberwachungsverbot ist ein „selbstständiger Menschenwürdeverstoß".[43] Die erforderliche Trennung der beiden Gewährleistungen fällt hier aber ebenfalls nicht leicht, da das BVerfG bislang nicht erklärt hat, wann es staatliche Informationseingriffe „nur" an Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG misst und wann die Prüfung alleine an Art. 1 Abs. 1 GG erfolgt. Die Abgrenzung wird nach der Konzeption des Totalüberwachungsverbots durch das BVerfG quantitativ vorgenommen: Die sicherheitsbehördliche Datenverarbeitung misst sich so lange am Recht auf informationelle Selbstbestimmung, bis ausreichend Daten vorhanden sind, mit denen man ein Persönlichkeitsprofil erstellen könnte.[44] Die Festlegung, „welche Maßnahme diejenige sein soll, die als sprichwörtlicher Tropfen das Fass zum Überlaufen bringt"[45] erweist sich im Einzelfall aber als schwierig. Aufgrund der Relationalität von Daten darf man sich das Verhältnis vom Eingriff in das Recht auf informationelle Selbstbestimmung und der verbotenen Totalüberwachung aber nicht als bloße lineare Entwicklung vorstellen.

C. Herausforderungen für das Totalüberwachungsverbot

Trotz der dogmatischen Schwierigkeiten und der nur geringen Praxisrelevanz des Totalüberwachungsverbots wird dessen Bedeutung im Rahmen der Digitalisierung sicherheitsbehördlicher Ermittlungsarbeit zunehmen. Schon heute fordern digitale Sachverhalte[46] das Verbot einer Rundumüberwachung heraus. Dies zeigen die nachfolgenden Szenarien.

43 *Eichberger* (Fn. 23), Art. 2 Rn. 315.

44 Ähnlich grenzt sich auch das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme von der informationellen Selbstbestimmung ab, vgl. *H. Gersdorf*, in: H. Gersdorf/B. Paal (Hrsg.), BeckOK InfoMedienR, 42. Ed. v. 1.5.2021, München, GG Art. 2 Rn. 25.

45 *G. Hornung*, Die kumulative Wirkung von Überwachungsmaßnahmen, in: M. Albers/R. Weinzierl (Hrsg.), Menschenrechtliche Standards in der Sicherheitspolitik, Baden-Baden 2010, S. 65 (73).

46 Begriffsbildend zum digitalen Sachverhalt *S. Rachut*, Grundrechtsverwirklichung in digitalen Kontexten, Berlin 2024 (i.E.), S. 169–208, insb. S. 200.

I. Ermittlungen im Metaverse

Vorhersagen zufolge wird bereits 2026 ein Viertel der Weltbevölkerung mindestens eine Stunde täglich im sog. Metaverse[47] verbringen.[48] Wie bei jeder technischen Innovation hat auch hier schon eine Instrumentalisierung durch Kriminelle eingesetzt, die sog. Metacrimes begehen.[49] Um dieser Kriminalität zu begegnen, gibt es Einsatzfelder von Virtual Reality (VR) für Sicherheitsbehörden, die rechtlich wenige Probleme aufwerfen.[50] Hierzu zählen etwa virtuelle Streifengänge der Polizei an Spawnpunkten[51] oder der Einsatz von VR als forensische Medientechnik durch begehbare 3D Modelle von Tatorten.[52]

Ein Problem für das Totalüberwachungsverbot oder vielmehr die Bildung von Persönlichkeitsprofilen stellt jedoch die große Menge sensibler Daten dar, die verarbeitet werden.[53] Durch Datenbrillen und andere sensorisch ausgestattete Hardware zur Interaktion sowie einem umfassend realistisch nachgebildeten Avatar der Nutzer gibt es wohl keinen anderen Bereich, „in dem so unmittelbar personenbezogene Daten abgegriffen werden können".[54] Diese Fülle an Daten ermöglicht ein tiefes Eindringen in die Persönlichkeit Betroffener und macht diese in ihrem Verhalten vorhersehbar.[55] Veranschaulicht werden kann das durch beim Gaming aufgezeichnete Interaktion und Entscheidungsfindung, die tiefe Einblicke in die

47 Verstanden als virtueller Raum, vgl. zu den Merkmalen und unterschiedlichen Immersionsgraden ausführlich bei *M. Kaulartz/A. Schmid/F. Müller-Eising,* Das Metaverse – eine rechtliche Einführung, RDi 2022, 521 (522 f.).

48 Interpol, Metaverse: A Law Enforcement Perspective, White Paper, Januar 2024, S. 5.

49 Begriff und eine Übersicht zu möglichen Deliktsfeldern bei Interpol, Metaverse: A Law Enforcement Perspective, White Paper, Januar 2024, S. 11 ff.

50 *E. Hilgendorf*, Virtuelle Realitäten, Metaverse, Generative KI und (Straf-)Recht, JZ 2024, 677 (686).

51 So der Vorschlag von *M. Martini/J. Botta,* Der Staat und das Metaversum, MMR 2023, 887 (897).

52 Siehe zum Holodeck des bayerischen Landeskriminalamts *R. Breker*, Holodeck – Das VR-Lab der bayerischen Polizei, Kriminalistik 2024, 130.

53 Siehe zur Fülle sensibler und biometrischer Daten bei *Martini/Botta,* Metaversum (Fn. 51), 894.

54 *Hilgendorf,* Realitäten (Fn. 50), 683.

55 Zur Persönlichkeitsrelevanz von Big Data allgemein *M. Martini*, Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht, DVBl 2014, 1481. Spezifisch für das Metaverse *Hilgendorf,* Realitäten (Fn. 50), 683.

Persönlichkeit ermöglicht.[56] Die Avatare im Metaverse können von ihrer Persönlichkeitsrelevanz daher im wahrsten Sinne des Wortes als digitale Zwillinge bezeichnet werden, weshalb bei ihrer Einbeziehung in Ermittlungen äußerst behutsam vorzugehen ist.

II. Biometrische Identifizierung

Videoüberwachung im öffentlichen Raum zu präventiven Zwecken ist inzwischen weit verbreitet und wird in der Rechtswissenschaft schon lange intensiv diskutiert.[57] Umfassende Videoüberwachung ruft zielsicher die bereits oben thematisierten Orwell-Vergleiche hervor.[58] Kombiniert man Videoüberwachung oder großflächiges Web Scraping[59] mit KI-gestützter Gesichtserkennung, hat dies das Potenzial, Anonymität im (digitalen) öffentlichen Raum aufzuheben, weshalb eine Betrachtung aus der Perspektive des Totalüberwachungsverbots lohnt.[60] An dieser Stelle kann und soll daher keine vertiefte verfassungsrechtliche Analyse der Zulässigkeit von Gesichtserkennung erfolgen.[61] Vielmehr soll der Einsatz dieser Technik – sofern er mit Rechtsgrundlagen legitimiert wird – auf seine Gefahr zur Bildung umfassender Persönlichkeitsprofile hin untersucht werden.

1. Begriff und aktuelle sicherheitspolitische Vorhaben

Sowohl die biometrische Echtzeit-Fernidentifizierung als auch die nachträgliche biometrische Fernidentifizierung sollen hier beleuchtet werden. Als Oberbegriff kann die biometrische Identifizierung gebildet werden.

56 *C. Geminn,* Deus ex machina?, Tübingen 2023, S. 262 mit weiterführenden empirischen Nachweisen in Fn. 404.
57 *T. Starnecker*, Videoüberwachung zur Risikovorsorge, Berlin 2017, S. 21 ff.
58 Siehe nur *J. Käppner*, Beobachtet von tausend Augen, SZ v. 17.12.2018.
59 Hierunter versteht man die automatisierte Extraktion von Informationen auf frei verfügbaren Webseiten.
60 So auch *M. Martini*, Gesichtserkennung im Spannungsfeld zwischen Sicherheit und Freiheit, NVwZ-Extra 1–2/2022, 1 (4, 7 f.), der die Totalüberwachung als „rote Linie" der Gesichtserkennung bezeichnet; i.E. ähnlich *G. Hornung/S. Schneider*, Das biometrische Auge der Polizei, ZD 2017, 203 (206).
61 Siehe hierzu bei *A. Heldt,* Gesichtserkennung: Schlüssel oder Spitzel?, MMR 2019, 285; *Martini*, Gesichtserkennung (Fn. 60), 5 ff.

Da es hierfür keine allgemein anerkannte Definition gibt,[62] greift dieser Beitrag der Einfachheit halber auf die Legaldefinition der biometrischen Identifizierung in Art. 3 Nr. 35 KI-VO zurück.[63] Intelligente Gesichtserkennung funktioniert über den Abgleich biometrischer Merkmale des Gesichts durch neuronale Netze mit vorhandenen Bilddaten und erbringt Leistungen, die dem Menschen durch manuellen Vergleich nicht möglich wäre.[64] Zwischen den beiden Varianten der biometrischen Identifikation kann folgendermaßen abgegrenzt werden: Die Echtzeit-Fernidentifizierung wird durch Videoüberwachung realisiert, während die nachträgliche Fernidentifizierung – für den Blickwinkel dieses Beitrags – ein biometrisches Web Scraping darstellt. Vereinzelt kam es in Deutschland schon zum präventiven[65] und repressiven[66] Einsatz von Gesichtserkennungssoftware durch Sicherheitsbehörden. Nicht zuletzt aufgrund der massiven Kritik an dieser Verwendung einigten sich die die Bundesregierung tragenden Parteien 2021 darauf, auf „flächendeckende Videoüberwachung und den Einsatz von biometrischer Erfassung zu Überwachungszwecken" zu verzichten.[67] Genau dies plant nun aber das BMI.[68] Mit einem Referentenentwurf, der allerdings auf eine Echtzeit-Fernidentifikation verzichtet,[69] will das BMI mit §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E den retrograden biometrischen Abgleich polizeilicher Datenbanken mit dem

62 Für die biometrische Fernidentifizierung *J. Hahn*, Die Regulierung biometrischer Fernidentifizierung in der Strafverfolgung im KI-Verordnungsentwurf der EU-Kommission, ZfDR 2023, 142 (145).

63 Nach Art. 3 Nr. 35 KI-VO ist eine biometrische Identifizierung „die automatisierte Erkennung physischer, physiologischer, verhaltensbezogener oder psychologischer menschlicher Merkmale zum Zwecke der Feststellung der Identität einer natürlichen Person durch den Vergleich biometrischer Daten dieser Person mit biometrischen Daten von Personen, die in einer Datenbank gespeichert sind".

64 *B. Kees*, Algorithmisches Panopticon, Münster 2015, S. 17 f.

65 Test der Bundespolizei am Bahnhof Berlin Südkreuz von 2017–2018, Bundespolizei, Test zur Gesichtserkennung am Bahnhof Berlin Südkreuz gestartet, Pressemitteilung v. 10.8.2017.

66 Im Rahmen der Strafverfolgung nach dem G20 Gipfel 2017 im Hamburg, vgl. VG Hamburg, Urt. v. 23.10.2019 – 17 K 203/19, BeckRS 2019, 40195.

67 SPD/Grüne/FDP, Mehr Fortschritt wagen, Koalitionsvertrag v. 24.11.2021, S. 109.

68 Referentenentwurf des BMI v. 06.08.2024, veröffentlicht durch *A. Meister*, Wir veröffentlichen den Entwurf zum neuem BKA-Gesetz, netzpolitik.org v. 15.08.2024. Nach anfänglich heftiger Kritik auch in Koalitionskreisen als Teil des sog. Sicherheitspakets nach dem Solingen-Attentat durch BT-Drs. 20/12806 als Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung eingebracht.

69 Im Sinne von Art. 3 Nr. 42 KI-VO und dem korrespondierenden Verbot in Art. 5 Abs. 1 lit. h KI-VO.

gesamten Internet ermöglichen. Damit würde dem Staat erlaubt werden, was Unternehmen wie ClearviewAI und Pim Eyes bereits realisiert haben.[70]

2. Exkurs: KI-VO als Zulässigkeitsdeterminante biometrischer Abgleiche

Die KI-VO[71] regelt auch die biometrische Echtzeit-Fernidentifizierung durch Videoüberwachung. Sie ordnet biometrische Echtzeit-Fernidentifizierungssysteme im öffentlichen Raum zu Strafverfolgungszwecken im Rahmen ihres risikobezogenen Regulierungsansatzes nach Art. 5 Abs. 1 lit. h KI-VO als KI-System mit einem unannehmbaren Risiko ein, das in einem unauflöslichen Widerspruch zu den Werten der Union steht und daher grds. verboten ist.[72] Zentraler Kritikpunkt am Verbot ist die eher offen formulierte Liste an Ausnahmen, die im Ergebnis „ein äußerst aufgeweichtes Verbot" schaffe.[73] Letztendlich wurde aus dem Verbot eine Öffnungsklausel für videobasierte Gesichtserkennung im Rahmen der Anforderungen von Art. 5 Abs. 2 ff. KI-VO.[74] Für retrograde Gesichtserkennung im Wege eines Abgleichs mit öffentlich zugänglichen Informationen aus dem Internet wie etwa Social-Media-Profilen verbietet Art. 5 Abs. 1 lit. e KI-VO aber eine notwendige technische Vorstufe zum Abgleich:[75] die Erstellung einer biometrischen Referenzdatenbank. Dieses Verbot ist deutlich weniger flexibel, da es offensichtlich auf das Verbot von Geschäftspraktiken von Unternehmen wie ClearviewAI zielt.[76]

---

70 Umfassend bei *M. Martini/C. Kemper,* Clearview AI: das Ende der Anonymität? Teil 1: Zulässigkeit der App, CR 2023, 341 (341 f.).

71 VO (EU) 2024/1689, ABl. L v. 12.07.2024.

72 Siehe zum risikobasierten Verbot *P. Bronner*, Risikoklassifizierung, Risikobewertung und Risikominimierung nach der KI-Verordnung, KIR 2024, 55 (57 f.).

73 *F. Rostalski/E. Weiss*, Verbotene KI-Praktiken (Art. 5 KI-VO-E), in: E. Hilgendorf/D. Roth-Isigkeit (Hrsg.), Die neue Verordnung der EU zur Künstlichen Intelligenz, München, 2023, § 3 Rn. 15.

74 *J. Ganter/J. Rembold,* in: R. Schwartmann/T. Keber/K. Zenner (Hrsg.), KI-VO, Heidelberg, 2024, 2. Teil 1. Kapitel Rn. 100 ff., 118.; *D. Bomhard/ J. Siglmüller*, AI Act – das Trilogergebnis, RDi 2024, 45 (48) weisen auf die Redundanz bzw. den bloßen Signalcharakter der Verbote hin. In diesem Zusammenhang ist Art. 10 und 11 JI-RL zu sehen. Zu deren Voraussetzungen an Gesichtserkennung *Martini*, Gesichtserkennung (Fn. 60), 5 f.

75 Ohne eine solche Referenzdatenbank aus sämtlichen öffentlich zugänglichen Bild-, Videoerzeugnissen und Stimmaufzeichnungen, müsste jeder Abgleich mit dem Gesamtbestand des Internets durchgeführt werden.

76 Die Datenbank beläuft sich laut eigenen Angaben auf über 50 Milliarden Bilder, https://www.clearview.ai.

3. Persönlichkeitsprofilbildung durch die Überwachung des (digitalen) öffentlichen Raums?

Das Recht auf informationelle Selbstbestimmung garantiert auch Anonymität im öffentlichen Raum.[77] Sowohl die Erfassung des menschlichen Gesichts als biometrisches Datum als auch die Durchführung eines Datenabgleichs bedeuten einen Eingriff in den Schutzbereich der informationellen Selbstbestimmung.[78] Die Gefahr der Persönlichkeitsprofilbildung markiert das sprichwörtliche Überlaufen des Fasses der Eingriffe in die informationelle Selbstbestimmung zum selbstständigen Menschenwürdeverstoß der Totalüberwachung.[79]

a) Stationäre Gesichtserkennung

Ob die Kombination stationärer Videoüberwachung mit KI-gestützter Gesichtserkennung die Bildung umfassender Persönlichkeitsprofile ermöglicht oder bei einer Kumulation mit weiteren Maßnahmen dazu beitragen kann, ist maßgeblich von der Installationsdichte der Überwachungskameras im öffentlichen Raum abhängig.[80] Je nach Anordnung und Anzahl der Kameras lassen sich engmaschige Bewegungsprofile erstellen, die wiederum weitreichende Rückschlüsse auf das Privat- und Sozialleben ermöglichen.[81] Zu Recht betont daher das BVerfG in seinen Entscheidungen zum Totalüberwachungsverbot, dass eine weitreichende Aufzeichnung der Bewegungen eines Menschen ein substanzieller Teil eines Persönlichkeitsprofils sein kann.[82] Wo die genaue Grenze zum selbstständigen Menschen-

77 BVerfGE 120, 378 (399 f.).

78 *Heldt,* Gesichtserkennung (Fn. 61), 287; BVerfGE 150, 244 (266 Rn. 43 ff.) für die automatisierte Kennzeichenerfassung.

79 Siehe schon bei B. II. 2.

80 *Hornung/Schneider*, Biometrisches Auge (Fn. 60), 206; vgl. zur Überwachungsdichte die Anzahl der Überwachungskameras je 1.000 Einwohner, Statista, Big Brother is watching you, https://de.statista.com/infografik/22350/ueberwachunsgkameras-in-ausgewaehlten-grossstaedten/ (zuletzt abgerufen am 28.09.2024).

81 Sogar sensible Informationen über sexuelle Präferenzen, Religion oder Gesundheitsprobleme können daraus abgeleitet werden, EDSA, Leitlinien 05/2022, Version 2.0 v. 26.04.2023, S. 16, 57; *K. Lachmayer*, Grundrechtliche Implikationen von Videoaufzeichnungen im öffentlichen Raum, NLMR 2023, 203 (210); *Hahn,* Fernidentifizierung (Fn. 62), 143.

82 BVerfGE 109, 279 (323); 130, 1 (24). Weniger problembewusst bzgl. der elektronischen Aufenthaltsüberwachung jedoch BVerfGE 156, 63 (136 Rn. 250 f.).

würdeverstoß liegt, wird sich aber nur im Einzelfall beurteilen lassen. Im Vergleich zu chinesischen und britischen Verhältnissen[83] werden Bewegungsprofile durch intelligente Videoüberwachung in Deutschland wohl noch länger allein ein Problem für das Recht auf informationelle Selbstbestimmung bleiben. Klar ist aber: Aus umfassenden Bewegungsprofilen lassen sich durch moderne Analysemethoden Persönlichkeitsprofile bilden.

b) Biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

Während Kameraüberwachung den öffentlichen Raum im geografisch-analogen Sinne vermessen kann, ermöglicht ein biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet eine detaillierte Vermessung des digitalen öffentlichen Raums. Bedenkt man die Fülle an Foto- und Videoaufnahmen auf Social-Media-Plattformen, auf deren Auswertung die Maßnahmen abzielen, „findet bereits jetzt eine weitreichende bildliche Dokumentation unseres Alltags im Internet statt – Tendenz steigend".[84] Mit dieser biometrisch genauen Lupe lässt sich das gesamte Bildmaterial einer Person im öffentlichen Internet finden und anschließend auswerten. Gerade bei digital freizügigeren Personen ergibt sich schnell eine Datenmenge, die eine Gefahr zur Bildung von Persönlichkeitsprofilen begründen kann. Drastisch formuliert könnten „die Handys der Bürger:innen in Zukunft […] immer auch als Überwachungskameras des Staates verwendet" werden.[85] Abstrakte Konturen für das Totalüberwachungsverbot des BVerfG lassen sich hier aber keine entwickeln. Wann es zu einer konkreten Gefahr der Bildung von Persönlichkeitsprofilen kommt, kann nur in einer Einzelfallbetrachtung ermittelt werden. Die vorgeschlagenen Rechtsgrundlagen der §§ 10b, 39a und 63b BKAG-E begründen aufgrund der mangelnden Begrenzung der Datenmengen,[86] der anwendbaren Methoden und der pau-

83 *D. Boffey*, Britain is 'omni-surveillance' society, watchdog warns, The Guardian v. 29.10.2023.

84 *N. Härting/L. Voigt/D. Albrecht*, Anwaltverein sieht „Verfassungsbeschwerde garantiert", netzpolitik.org v. 30.08.2024.

85 *E. Tuchtfeld*, D64 kritisiert Pläne von Faeser, Pressemittelung v. 12.08.2024, abrufbar unter https://d-64.org/plaene-faeser/ (zuletzt abgerufen am 10.10.2024).

86 Die Sicherheitsbehörden könnten aufgrund der Konturlosigkeit und Technikoffenheit der vorgeschlagenen Rechtsgrundlagen dazu verleitet werden, eine oben bereits thematisierte biometrische Referenzdatenbank anzulegen.

schalen Bezugnahme auf sämtliche Daten, auf die das BKA zugreifen darf, allerdings bereits eine abstrakte Gefahr der Bildung von Persönlichkeitsprofilen.[87]

III. Überblick weiterer Problemfelder

Neben den dargestellten eher neuen Phänomenen der Sicherheitsgewährleistung regt das Totalüberwachungsverbot aber auch zum Nachdenken über Ermittlungsmaßnahmen an, die die sicherheitsrechtliche Debatte schon länger prägen.

1. Online-Durchsuchung

Das Totalüberwachungsverbot entwickelt gerade bei kumulativer Überwachung eine besondere Bedeutung.[88] Die Online-Durchsuchung stellt aber eine Maßnahme dar, die schon für sich allein betrachtet eine derart große Menge an Daten erhebt, dass bei deren Verknüpfung die Gefahr der Bildung von Persönlichkeitsprofilen besteht.[89] Je nach Gerät und der Intensität seiner Nutzung ermöglicht eine Onlinedurchsuchung, der Zielperson „beim Denken" zuzusehen.[90] Sogar etablierte – wenn auch nicht unumstrittene – und verfassungsgerichtlich bereits näher ausgeleuchtete Maßnahmen wie die Online-Durchsuchung können das Totalüberwachungsverbot daher im Einzelfall verletzen. Hauptgrund hierfür ist ein eher an punktuellen inhaltlich-qualitativen Verletzungen orientierter Kernbereichsschutz, der die Gefahr von Persönlichkeitsprofilen nicht adressiert.[91]

87 Angesichts der ermöglichten umfassenden Datensammlung fällt das Ausklammern von Informationen aus Online-Durchsuchungen und akustischer Wohnraumüberwachung nach § 10b Abs. 3 S. 2 BKAG-E i.V.m. § 12 Abs. 3 BKAG hier kaum ins Gewicht.

88 Weshalb es auch einer Abgrenzung zum sog. additiven Grundrechtseingriff bedarf, siehe hierzu bei *Schwabenbauer*, Grundrechtseingriffe (Fn. 34), S. 294 f.

89 *Conrad*, Kernbereichsschutz (Fn. 20), S. 27 ff. m.w.N. Im Grunde erkennt das BVerfG diese Gefahr auch schon, vgl. BVerfGE 141, 220 (280).

90 *U. Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 5.

91 Instruktiv bei *Conrad*, Kernbereichsschutz (Fn. 20), S. 46 f.

2. Vorratsdatenspeicherung

Die sog. Vorratsdatenspeicherung, also die anlasslose Speicherung von Telekommunikationsverkehrsdaten[92], wurde vom BVerfG bereits von Beginn an im Lichte des Totalüberwachungsverbots betrachtet.[93] Blickt man auf die technische Möglichkeit, bereits aus Verkehrsdaten umfassende Persönlichkeitsprofile erstellen zu können, leuchtet das ein.[94] Das Totalüberwachungsverbot als Teil der verfassungsrechtlichen Identität nach Art 79 Abs. 3 GG[95] würde nicht nur einer nationalen Lösung, sondern auch einer europarechtlich determinierten Vorratsdatenspeicherung Grenzen setzen. Auch hier lassen sich Aussagen zur Verletzung aber nur im Einzelfall treffen: Da Verkehrsdaten dezentral bei den Diensteanbietern gespeichert werden[96], bedeutet erst die behördliche Zusammenführung der Daten im Falle von Ermittlungen eine Gefahr der Rundumüberwachung beziehungsweise der Bildung von Persönlichkeitsprofilen.

D. Zukunft des Totalüberwachungsverbots

Das vom BVerfG entwickelte Totalüberwachungsverbot klingt vom Namen her pathetisch und wie eine letzte Verteidigungslinie, bevor ein Rechtsstaat zum orwellschen Überwachungsstaat kippt. Die Auswertung der Rechtsprechung des BVerfG zu diesem Verbot der Rundumüberwachung hat jedoch gezeigt, dass es im Wesentlichen um die Bildung von Persönlichkeitsprofilen geht, die Menschen für den Staat vorhersehbar und prognostizierbar machen und damit den Menschen zum bloßen Objekt staatlicher Datenverarbeitung degradieren. Von dieser absoluten Grenze für staatliche Informationseingriffe der Sicherheitsbehörden liegt auch ein dystopischer Überwachungsstaat noch etwas entfernt. Die hier behandelten Beispiele von Befugnissen zur Sicherheitsgewährleistung, die sich im Rahmen der

92 § 3 Nr. 70 TKG.

93 BVerfGE 125, 260 (324).

94 *B. Perez/M. Musolesi/G. Stringhini*, You are your Metadata: Identification and Obfuscation of Social Media Users using Metadata Information, 2018, https://arxiv.org/abs/1803.10133 (zuletzt aufgerufen am 10.10.2024); *T. Schwabenbauer*, Kommunikationsschutz durch Art. 10 GG im digitalen Zeitalter, AöR 137 (2012), 1 (9 f.).

95 BVerfGE 125, 260 (324): „Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland".

96 Vgl. § 175 Abs. 1 S. 1 TKG.

Digitalisierung herausgebildet haben, zeigen die Schwächen dieser dogmatischen Figur: Sie ist weitgehend konturlos und im Einzelfall kaum operationalisierbar. Die Anwendung dieses Postulats geht in der gerichtlichen Prüfung kaum über das berühmte „I know it when I see it" hinaus.[97]

Mit einigen wenigen Maßstäben zur Gefahr von Persönlichkeitsprofilen oder einer entsprechenden verfassungsrechtlichen Definition würde sich das Totalüberwachungsverbot ganz ohne kleinteilige[98] sicherheitsverfassungsrechtliche Rechtsprechung jedoch als eine handhabbare letzte Messlatte im Sicherheitsrecht etablieren. Für die Praxis der Strafverfolgungsbehörden, Nachrichtendienste und Polizeien in Bund und Ländern bedeutet dies aber, dass das Totalüberwachungsverbot nicht Angelegenheit des Gesetzgebers ist, sondern vielmehr die eigene. Die Digitalisierung erleichtert Profilbildung enorm, weshalb das Totalüberwachungsverbot als absolute Grenze staatlicher Informationseingriffe in konkreten Ermittlungen mitgedacht werden muss. Sich allein an immer kleinteiligeren Vorgaben des BVerfG zur Vereinbarkeit sicherheitsrechtlicher Maßnahmen mit dem Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG festzuhalten ist angesichts der technischen Möglichkeiten in den Händen der Sicherheitsbehörden zu wenig.

97 U.S. Supreme Court *Jacobellis v. Ohio*, 378 U.S. 184 (1964), S. 197.

98 Zu dieser Kritik siehe nur *U. Volkmann*, Die Dogmatisierung des Verfassungsrechts, JZ 2020, 965 (969).

„Legal Design“ für HessenData (§ 25a HSOG) – ein abgestuftes Kontrollkonzept

Nitharshini Santhakumar

A. „Rechtfragen virtueller Welten

I. Kontrollmechanismen für das „Internet von morgen“

Der JuWissDay 2024 lud unter dem Titel „Rechtsfragen virtueller Welten“ zu einem Austausch über „das „Internet von morgen“ ein. So soll dieses „unser Verhältnis zum digitalen Raum revolutionieren, indem es physische, erweiterte und virtuelle Realität miteinander verschmelzen lässt.“[1]

Eine potenziell irreversible Verschmelzung der realen und virtuellen Welten erfordert eine strategische Auseinandersetzung mit der Frage, ob traditionelle rechtliche Kontrollmechanismen, wie etwa der Richtervorbehalt, in solchen erweiterten Realitäten Anwendung finden können. Sowohl die Judikative als auch die Legislative auf Landes-, Bundes- und Unionsebene haben sich diesen Herausforderungen gestellt. Unter Berücksichtigung der unterschiedlichen Terminologien lassen sich Überschneidungen und Berührungspunkte finden. Dieser Beitrag zielt darauf ab, die Relevanz und die mögliche Ausgestaltung von Kontrollmechanismen zu untersuchen, indem die Ansätze der Rechtsprechung aus einer deutsch-europäischen Perspektive analysiert werden.

II. Schaffung von Strategien aus deutsch-europäischer Perspektive

1. Pionierszenario: „Automatisierte Datenanalyse“

Den Ausgangspunkt der Forschung bildet das Urteil des Bundesverfassungsgerichts zur „automatisierten Datenanalyse“ aus dem Jahr 2023.[2] In diesem Urteil führte das Verfassungsgericht, soweit ersichtlich, erstmalig

1 Beschreibung der Tagung durch den Veranstalter auf dessen Webseite: https://www.juwiss.de/juwissday-2024/ (zuletzt abgerufen am 04.09.2024).

2 BVerfG NJW 2023, 1196 ff.

den Begriff des „abgestuften Kontrollkonzepts“ ein und eröffnete damit dem Gesetzgeber die Möglichkeit, sich der Thematik durch ein spezifisches „Legal Design“ anzunähern. Aus der Wechselwirkung zwischen Gesetzgebung und Rechtsprechung sowie der anhängigen Verfassungsbeschwerde folgt eine rechtliche Strategie, die im Kontext der „automatisierten Datenanalyse“ in der Bundesrepublik Deutschland als wegweisendes Szenario betrachtet werden könnte.

2. Unionale Strategien

Die deutsche Rechtsprechungsperspektive soll in diesem Beitrag um eine unionale Sichtweise ergänzt werden. Dabei ist zu betonen, dass der zeitliche Aspekt (Time Management) eine wesentliche Rolle spielen dürfte. Bereits im Jahr 2022 hat der EuGH sich in der Entscheidung zur „Passenger Name Records-Richtlinie“[3] zum Einsatz von KI geäußert. Ergänzt wird dies um die Rechtsprechung zur „automatisierten Entscheidung im Einzelfall“ – dem Schufa Scoring Urteil aus 2023. Zwar ist die Tiefgründigkeit zu Kontrollmechanismen im Hinblick auf die Automatisierung nicht mit dem „HessenData“-Urteil des Bundesverfassungsgerichts vergleichbar, gleichwohl sind Tendenzen erkennbar, die auch im Einklang zur europäischen Legislative eine rechtspolitische Strategie erkennen lassen. Aufgrund des Umfangs wird in diesem Beitrag auf nähere Ausführungen zur Legislative – insbesondere JI-Richtlinie[4], DSGVO[5] und KI-VO[6] verzichtet.

3 EuGH ZD 2022, 553 ff.

4 Richtlinie 2016/680/EU zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr […]; hier insbesondere Art. 11 „Automatisierte Entscheidungsfindung im Einzelfall“.

5 Verordnung 2016/679/EU zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr […]; hier insbesondere Art. 22 „Automatisierte Entscheidungen im Einzelfall einschließlich Profiling“.

6 Verordnung 2024/1689/EU zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen […]; hier insbesondere Art. 8–15; Art. 64–69.

B. „HessenData" – als Demonstrator

I. „Automatisierte Anwendung zur Datenanalyse"

Als Vorreiter in der Bundesrepublik Deutschland entschied sich das Bundesland Hessen für die Implementierung einer technischen Innovation in seine Polizeiarbeit: Die „automatisierte Anwendung zur Datenanalyse". Bei der technischen Innovation „HessenData" handelt es sich um eine Software, die dazu dient, „bisher unverbundene, automatisierte Dateien und Datenquellen in Anwendungen zur Datenanalyse bzw. Analyseplattformen zu vernetzen, die vorhandenen Datenbestände durch Suchfunktionen systematisch zu erschließen und die polizeiliche Aufgabenerfüllung auf diese Weise zu erleichtern und zu verbessern."[7] Die Software wurde von dem US-amerikanischen Unternehmen „Palantir" entwickelt, welches seine Standardsoftware „Gotham" auf die spezifischen Anforderungen des Landes Hessen anpasste, wodurch sie den Namen „HessenData" erhielt.[8] Parallel zur Einführung dieser Software wurde die gesetzliche Ermächtigungsgrundlage in § 25a des Hessischen Sicherheits- und Ordnungsgesetzes (HSOG) geschaffen.[9] Diese Ermächtigungsgrundlage zum Einsatz der „automatisierten Anwendung zur Datenanalyse" war Gegenstand eines Verfahrens vor dem Bundesverfassungsgericht (1 BvR 1547/19 u.a.), das im sogenannten „HessenData-Urteil" mündete.

II. Time Management

„HessenData" zum Kern dieses Beitrags zu machen, erfolgt vor dem Hintergrund, dass diese Entscheidung als wegweisend erachtet wird. Deutlich wird, dass vor allem der Zeitaspekt eine besondere Rolle zukommt:

---

7 Hessischer Landtag: Änderungsantrag […] für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen, Drs. 19/5412, S. 41.

8 Mit Begründung der besonderen Dringlichkeit wurde zunächst in einem freihändigen Vergabeverfahren „Gotham" von Palantir beschaffen. Im Anschluss folgte ein zweites Verfahren, welches in eine Zuschlagserteilung am 14.12.2017 mündete – hierzu ausführlich Hess. Landtag, Zwischenbericht des Untersuchungsausschusses 19/3 zur Drucksache 19/6574 Teil A, Drs. 19/6864, S.19 f.

9 Ursprünglich: Hessischer Landtag: Änderungsantrag […] für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen […] vom 14.12.2017, Drs. 19/5782; GVBl Hessen 2018, S. 302.

> „Unter Time Management wird hier eine Perspektive verstanden, die „Wissen" in Relation zu Zeit/Datum setzt und so veränderungsoffen wie nachhaltig die Herausforderungen effizient analysieren will. Konsequent fokussiert wie adressiert dieser Beitrag Kernherausforderungen, die im geltenden Recht (de lege lata) bewältigt werden müssen und die – unabhängig vom Ergebnis aktueller Normgebungsverfahren wie Initiativen wie Pläne (de lege ferenda) – Ideen/ Herausforderungen für zukünftig geltendes Recht (lex futura) liefern."[10]

Die Bewältigung der Kernherausforderung „automatisierte Datenanalyse" wird in einem Wechselspiel zwischen Rechtsprechung und Gesetzgeber am Demonstrator[11] „HessenData" konturiert. Die jeweiligen Gesetzesinitiativen und Entscheidungen sind dabei stets aus einer zeitlichen Perspektive zu betrachten:

- 2017: Erwerb der Software & Gesetzeserlass (§ 25a HSOG a.F.)
- 2019: Verfassungsbeschwerde (VB I)
- 2023: Urteil des BVerfG (1 BvR 1547/19 u.a.)
- 2023: Erlass der neuen Ermächtigungsgrundlage (§ 25a HSOG n.F.)
- 2024: Anhängige Verfassungsbeschwerde (VB II).

III. Pioniersvorhaben „HessenData": Ein Gesetz für ein Produkt

1. Normierung der „automatisierten Datenanalyse"

§ 25a HSOG in der alten Fassung bildet den Grundstein für die „automatisierte Datenanalyse". Bereits in der alten Fassung hatte der Gesetzgeber

10 *V. Schmid/T. Kretschmann*, Operative Herausforderungen einer „Drohnenwelt" – (Luftverkehrs)Management (ATM und UTM) inklusive der „Drohnendetektion", in: K. Chibanguza/C. Kuß/H. Steege (Hrsg.), Künstliche Intelligenz – Recht und Praxis automatisierter und autonomer Systeme, Baden-Baden 2022, S. 529, Rn. 128.

11 „Grundsätzlich zu unterscheiden sind „Pilot" und „Demonstrator" (Terminologie V. Schmid). Piloten" sind szenarienorientierte, projektierte Anwendungen von (Recht und) Technik. „Demonstratoren" erlauben die Überprüfung der Machbarkeit, Nachhaltigkeit, Qualität wie Anfälligkeit des "Piloten" – sie unterscheiden sich also in der Funktions-, Rechts- und Marktreife. Dies ist in einer ökonomischen Perspektive auch der Unterschied zwischen Business Opportunity und Business Case bzw. die Entdeckung der sog. „Killerapplikation"." Zitat aus *V. Schmid/ J. Toptaner*, Integration von „Flugdrohnen" in das (deutsch-europäische) Rechtssystem – eine Kartographie (Fn. 10), Rn. 11.

die Erforderlichkeit von Kontrollmechanismen erkannt und in § 25a Abs. 3 HSOG wiedergegeben.

§ 25a Abs. 3 (HSOG)

(3) Die Einrichtung und wesentliche Änderung einer automatisierten Anwendung zur Datenanalyse erfolgen durch Anordnung der Behördenleitung oder einer oder eines von dieser beauftragten Bediensteten. Die oder der Hessische Datenschutzbeauftragte ist vor der Einrichtung oder wesentlichen Änderung nach Satz 1 anzuhören; bei Gefahr im Verzug ist die Anhörung nachzuholen.

Weitere „Kontrollmechanismen" waren der Norm hingegen nicht zu entnehmen.

2. Praktische Handhabe von Kontrollmechanismen für die „automatisierte Datenanalyse"

Das Fehlen einer spezifischen Normierung zusätzlicher Kontrollmechanismen impliziert nicht, dass die Hessische Polizei bei der Einführung von „HessenData" notwendige Vorkehrungen vernachlässigt hat. Vielmehr wurden bei der Implementierung von „HessenData" wesentliche Kontrollmechanismen integriert, die im Gesetzestext nicht ausdrücklich festgelegt worden sind. Eine umfassende Untersuchung dieser Maßnahmen wurde im Rahmen des Untersuchungsausschusses[12] durchgeführt. Dabei sind zwei tragende Säulen erkennbar geworden: Zum einen werden Schutzvorkehrungen durch die „Hessische Zentrale für Datenverarbeitung (HZD)"[13] getroffen, zum anderen hat die Hessische Polizei selbst Sicherheitsvorkehrungen getroffen, die sowohl den unbefugten Zugriff als auch die unbefugte Übertragung von Daten verhindern sollen.[14]

12 Hessischer Landtag, Zwischenbericht des Untersuchungsausschusses 19/3 zur Drucksache 19/6574, Drs. 19/6864 vom 03.01.2019 (https://starweb.hessen.de/cache/DRS/19/4/06864.pdf).

13 Ausführlich zu den Sicherheitsvorkehrungen etwa *HZD-Report 2023,* Zukunft ist jetzt, „Sicherheit neu denken", S. 27 (https://tinyurl.com/47rey2ju).

14 *Hessisches Ministerium des Inneren und Sport,* Hessische Cybersicherheitsstrategie 2023, S. 30.

a) Schutz vor Abfluss sensibler Daten

Der Schutz vor dem Abfluss sensibler Daten wird in mehrfacher Hinsicht erreicht. Aus dem Untersuchungsbericht geht hervor, dass neben der Zurverfügungstellung von Endgeräten für die Palantir-Mitarbeiter zum Zwecke der Einrichtung von HessenData auch Firewalls und die Methodik des „Housings“[15] eine zentrale Rolle spielen.[16] Aus dem Bericht des Untersuchungsausschusses geht auch hervor, dass die Plattform in die gleiche Firewall-Umgebung gesetzt wurde wie andere polizeiliche Anwendungen. So kann der gleiche Sicherheitsstandard erfüllt werden.[17]

b) Schutz vor unbefugtem Zugriff

Das HZD hat auch besondere Vorkehrungen getroffen, um vor unbefugtem Zugriff zu schützen. Diese umfassen insbesondere Zugriffsbeschränkungen etwa durch vorherige Anmeldungen, Sicherheitstoken, Firewall oder Bestimmung von Arbeitsplätzen.[18] Schutzvorkehrungen dieser Art werden am hessenweiten Mindeststandard für IT-Sicherheit gemessen.

3. Technisch-organisatorische Maßnahmen der Exekutive

Festzuhalten bleibt insofern, dass der Landesgesetzgeber zwar in der Ermächtigungsgrundlage von ausdifferenzierten Kontrollmechanismen abgesehen hat, dagegen aber die Exekutive eine Vielzahl von technischen und organisatorischen Maßnahmen (TOMs) ergriffen hat. Charakteristisch ist, dass mittels ihnen kurzfristig auf den „Stand der Technik“ reagiert und

15 Das sogenannte Housing bedeutet, dass ein Interessent die Infrastruktur in Anspruch nehmen kann, ohne unmittelbaren Zugriff auf die Systemarchitektur zu haben. Konkret bedeutet dies, dass sichere Zugangskontrollen, redundante Netze und Stromleitungen sowie Klimatechnik zur Verfügung gestellt werden; vertiefend *A. Auer-Reinsdorff*, § 21 Providerverträge, A. Auer-Reinsdorff/I. Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, Rn. 41.

16 Hessischer Landtag, Zwischenbericht des Untersuchungsausschusses (Fn. 12), S.69.

17 Hessischer Landtag, Zwischenbericht des Untersuchungsausschusses (Fn. 12), S.70.

18 Hessischer Landtag Zwischenbericht des Untersuchungsausschusses (Fn. 12), S. 72.

dadurch die Sicherheitsarchitektur angepasst werden kann.[19] Der konkreten Gestaltung der TOMs dürfte eine hohe Wichtigkeit zukommen, denn fehlende materielle Substanz kann zur Beeinträchtigung des Informationsanspruchs des Bürgers führen.[20] Gleichzeitig streben auch Sicherheitsbehörden zum Zwecke der „effektiven und resilienten Gefahrenabwehr" einen hohen Grad an Datensicherheit an.[21]

IV. Neukonzeptionierung der „automatisierten Datenanalyse"

Im Februar 2023 entschied das Bundesverfassungsgericht dahingehend, dass die „automatisierte Datenanalyse" grundsätzlich ein zulässiges Mittel sein könnte.

1. Maßstab der Verhältnismäßigkeit

In seiner Entscheidung betonte das BVerfG unter Verweis auf seine „BKAG I-Entscheidung, dass der Grundsatz der Verhältnismäßigkeit Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle stellt.[22] Zudem nennt das Gericht einige Maßnahmen, die dem Verhältnismäßigkeitsgrundsatz Rechnung tragen sollen – etwa das „abgestufte Kontrollkonzept", staatliches Monitoring und die Protokollierungspflicht.[23] Das BVerfG hat in der Vergangenheit bereits entschieden, dass bei verminderter Gewährleistung subjektiven Rechtsschutzes die Anforderungen an „an eine wirksame aufsichtliche Kontrolle und an die Transparenz des Behördenhandelns steigen."[24] Es gilt daher Maßnahmen zu finden, die sich praktisch umsetzen lassen und gleichzeitig die Trias „Transparenz, individueller Rechtsschutz und aufsichtliche Kontrolle" stärken.

---

19 Ausführlich zur Begrifflichkeit „Stand der Technik" – *C. Piltz* in P. Gola/D. Heckmann (Hrsg.), Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage, Art. 32 Rn. 15–19 sowie *S. Schulz* Art. 6 Rn. 141.

20 *C. Arzt*, PolG NRW § 22 Datenspeicherung, Prüfungstermine, in: M. Möstl/D. Kugelmann (Hrsg.), BeckOK Polizei- und Ordnungsrecht Nordrhein-Westfalen, 28. Edition, München 2024, § 22 Rn. 5.

21 *D. Kugelmann/A. Buchmann*: Der Algorithmus und die Künstliche Intelligenz als Ermittler – Zum Rechtsrahmen für sicherheitsbehördliche Datenanalysen und für den Einsatz von Verfahren künstlicher Intelligenz, GSZ 2024, 1 (4).

22 Urteil des BVerfG ADA (Fn. 2), Rn. 109.

23 Vgl. zu den durch das BVerfG genannten möglichen Maßnahmen Urteil des BVerfG ADA (Fn. 2), Rn. 109.

24 BVerfGE 141, 220 (378) Rn. 135.

a) Transparenz

Durch das Inkrafttreten der KI-VO hat der Diskurs zur Bedeutung von Transparenz neuen Wind bekommen. In der Entscheidung zum BKAG I stellte das BVerfG fest, dass die „Transparenz der Datenerhebung und -verarbeitung zum Vertrauen beitragen soll."[25] Häufig findet sich in diesem Zusammenhang die Terminologie „Blackbox" wieder und meint dabei, dass nur die Eingabe- und Ausgabedaten bekannt sind, nicht jedoch wie das System zu dem Ergebnis kam.[26] Diesem Prozess schließt sich aus rechtswissenschaftlicher Perspektive die Frage an, wie eine Überprüfung erfolgen könnte, wenn die Entscheidung automatisiert erfolgt.[27] Zu einer der europäischen Strategie annähernden Überlegung kam *Henning Radtke* beim EDV-Gerichtstag 2024:

> *„Ein verfassungsrechtliches Problem ist die Frage nach Transparenz oder der Intransparenz. […]* ***Fehler aufdecken und überprüfen kann jedoch nur wer die Datengrundlage wie die Gewichtung des Entscheidungsprozesses und der Entscheidungskriterien kennt und versteht. Intransparenz der Entscheidungsabläufe bei der Nutzung der KI und damit eine fehlende Nachvollziehbarkeit der Funktionsweise von KI-Technologien können daher mit dem rechtstaatlichen Transparenzgebot in Konflikt stehen.*** *Deshalb wird aus meiner Sicht – ein zentraler Eckpfeiler der Regulierung von KI eben auch die Transparenz in Form von Kennzeichnungs- und Informationspflichten sein. Insofern glaube ich, dass der AI Act der Europäischen Union da auf einem richtigen Weg ist.""*[28]

Demnach wären zur Erfüllung der Transparenzanforderungen bei der Nutzung von KI drei Voraussetzungen zu erfüllen: Kenntnis hinsichtlich Datengrundlage, Gewichtung des Entscheidungsprozesses und die Entscheidungskriterien. Die Offenlegung dieser drei Voraussetzungen geht häufig einher mit der Kritik, dass dadurch das „Geschäftsgeheimnis offenbart

25 BVerfGE 141, 220 (378) Rn. 135.
26 *L. Merkle:* Transparenz nach KI-Verordnung – von der Blackbox zum Open-Book?, RDi 2024, 414 (415).
27 *J. Eisele,* Verarbeitung der PNR-Fluggastdaten, ZD 2022, 553 (559).
28 Richter am BVerfG Prof. Dr. Radtke am EDVGT am 12.09.2024 in Saarbrücken, Siehe hierzu „Eröffnung 33. EDV-Gerichtstag" vom 12.09.2024: Zitat bei 1:34:30 – 1:35:35. https://www.youtube.com/watch?v=WK0i2ckBDD8.

wird".[29] Dabei muss die Offenlegung nicht bedeuten, dass der Algorithmus als Open-Source-Projekt frei und für jeden zugänglich zur Verfügung steht, denn damit wäre im Regelfall auch nicht die Transparenzpflicht erfüllt. Gegenwärtig dürfte die Mehrheit der Betroffenen nicht über die entsprechende Fachkompetenz besitzen, um mittels des Quellcodes die Entscheidungsfindung nachzuvollziehen. Dagegen dürfte zur Annäherung der Transparenz die bildliche Darstellung etwa in Form von Entscheidungsbäumen oder Gewichtsdarstellungen hilfreich sein.[30]

Ein Nachteil muss sich hierdurch für die großen privaten Akteure auch nicht ergeben. Vielmehr könnten sie durch die (visuelle/nachvollziehbare) Offenlegung der Funktions- und Wirkungsweise der Algorithmen einer Machtasymmetrie entgegenwirken und so ggf. der ihnen drohenden Erweiterung der mittelbaren Drittwirkung zu einer nahezu „unmittelbaren Drittwirkung" entgegenwirken.[31]

b) Aufsichtliche Kontrolle

In seiner Entscheidung zum Anti-Terrorgesetz sah das BVerfG die aufsichtliche Kontrolle als objektivrechtliche Maßnahme im Verhältnis zur subjektivrechtlichen Kontrolle durch Gerichte an. Sie ziele auf die Gewährleistung der Gesetzmäßigkeit der Verwaltung ab und umfasse auch den subjektiven Schutz der Betroffenen, die nur mittelbar oder im Zusammenwirken mit anderen Maßnahmen von ihrer Betroffenheit Kenntnis erlangen."[32]

Im Rahmen der Verhältnismäßigkeitsprüfung solle die aufsichtliche Kontrolle anhand ihrer Wirksamkeit geprüft werden: Konkret ist zu überprüfen, mit welchen Befugnissen die aufsichtliche Kontrolle ausgestattet ist,

29 Insofern hatte der BGH im Kontext eines datenschutzrechtlichen Auskunftsersuchens geurteilt, dass der Algorithmus Bestandteil des Geschäftsgeheimnisses der Schufa-Scoring ist, vgl. *BGH* Urteil vom 28.01.2014 VI- ZR 156/13, MMR 2014, 489 LS 3, Rn. 27.

30 *V. Bortnikow/ J. Dukart,* Informationelle Selbstbestimmung und KI, ZD 2024, 558 f. (560).

31 *W. Hoffmann-Riem*, Die digitale Transformation als rechtliche Herausforderung, JuS 2023, 617 (619).

32 BVerfGE 133, 277 (370).

ob also die auszuwertenden Daten vollständig sind und für den Prüfenden in einer praktikablen Form zur Verfügung stehen.[33]

c) Individueller Rechtsschutz

Die Ausgestaltung des individuellen Rechtsschutzes stellt mitunter einer der größten Herausforderungen dar. Für die Geltendmachung von Ansprüchen wäre die Nachvollziehbarkeit der Entscheidungsfindung maßgeblich. Da diese jedoch durch Intransparenz geprägt ist, wird die effektive Durchsetzung rechtlicher Ansprüche gefährdet.[34]

Für zivilrechtliche Themengebiete wird in der Literatur als Lösungsansatz zur Bewältigung der Informationsasymmetrie bei der Anwendung automatisierter Entscheidungsfindungssysteme (ADM-Systeme) die Beweislastumkehr erörtert, um die Hürden für die Geltendmachung von Diskriminierungsansprüchen zu senken.[35] Offen bleibt vorerst, wie es für das Verwaltungsprozessrecht eingeführt werden könnte.

2. Konkrete Ausgestaltung & Umsetzung durch Rechtsprechung und Gesetzgeber

Das Bundesverfassungsgericht erklärte die Ermächtigungsgrundlage zur „automatisierten Anwendung zur Datenanalyse" nicht für nichtig, sondern lediglich für unvereinbar und setzte hierzu eine Frist bis zum 30.09.2023.[36] In seiner Entscheidung ging das Gericht auf die „Transparenz, den individuellen Rechtsschutz und [die] aufsichtliche […] Kontrolle" ein und nannte hierzu auch mögliche Kriterien. Noch im Juli 2023 erließ der hessische Gesetzgeber eine neue Ermächtigungsgrundlage, die teilweise in der Be-

33 *K. Graulich*, Das Handeln von Polizei- und Ordnungsbehörden zur Gefahrenabwehr in H. Lisken/E. Denninger (Hrsg.), Handbuch des Polizeirechts, 7. Aufl. 2021, Rn. 716.

34 *I. Spiecker gen. Döhmann/E. V. Towfigh*, Automatisch benachteiligt – Das Allgemeine Gleichbehandlungsgesetz und der Schutz vor Diskriminierung durch algorithmische Entscheidungssysteme, Rechtsgutachten im Auftrag der Antidiskriminierungsstelle des Bundes, 2023, S. 70.

35 *M. Grünberger*, Reformbedarf im AGG: Beweislastverteilung beim Einsatz von KI, ZRP 2021, 232 (234); deutlicher so der auf die Wirtschaft bezogene Gleichstellungsbericht BReg (2020), Drs. 19/30750, S. 138 und S. 169, für den Arbeitsbereich.

36 Urteil des BVerfG ADA (Fn. 2).

gründung auf das Urteil rekurrierte.[37] Zu den konkret durch das Gericht genannten und durch den hessischen Gesetzgeber neu geregelten Maßnahmen gehören:

- Rollen- & Rechtekonzept, § 25a Abs. 3 Nr. 1 HSOG
- Technisch-organisatorische Vorkehrungen, § 25a Abs. 3 Nr. 2 lit. b HSOG
- Zugriffskontrolle, § 25a Abs. 4 S. 1–2 HSOG
- Protokollierungspflicht, § 25a Abs. 4 S. 2–3 HSOG
- Abgestuftes Kontrollkonzept, § 25a Abs. 4 S. 6 u. Abs. 5 HSOG
- Anhörungsrecht des hessischen Datenschutzbeauftragten, § 25a Abs. 5 HSOG.

Zwar hatte die hessische Polizei einige Maßnahmen bereits implementiert, doch verlangte das Gericht die gesetzliche Kodifizierung: Im Ergebnis seien abstrakt-generelle Regelungen erforderlich, die in einer öffentlich zugänglichen Weise dokumentiert werden. Die konkrete Gestaltung des Konzepts wiederum kann durch eine Verwaltungsvorschrift erfolgen.[38] Dem kam der hessische Gesetzgeber auch im neuen § 25a Abs. 3 Nr. 1 HSOG n.F. nach: Die Gestaltung des Rollen- und Rechtekonzepts ist nicht an den polizeilichen Berufsgrad/Hierarchiengrad gebunden, sondern orientiert sich am Schutzwert des betroffenen Rechtsguts sowie an der Dringlichkeit des polizeilichen Handelns, wobei die Anwendergruppe sich nach Phänomenbereichen unterteilt.[39] Solche Rollen- und Rechtekonzepte sollen Tätigkeiten mit Authentifizierung verknüpfen und vor Manipulationen schützen.[40] Darüber hinaus gewährleisten sie, dass der jeweils zuständige Organisationsbereich über die erforderliche Schulung, Belehrung und Freistellung verfügt, um die datenschutzrechtlichen Vorgaben sachgerecht umsetzen zu können.[41] Die Sicherstellung der praktischen Wirksamkeit soll durch sogenannte „technisch-organisatorische Vorkehrungen" erfolgen. Aus deutsch-europäischer Perspektive wäre hier terminologisch die Verwendung „technisch-organisatorische Maßnahmen" wünschenswert gewesen.[42] Die Aufforderung durch „TOM" zu regeln, welche Daten in die Analyse einbezogen

37 GVBl. Hessen 2023 Nr. 22, S. 456 ff.
38 Urteil des BVerfG ADA (Fn. 2), Rn. 140.
39 Verwaltungsvorschrift zu § 25a HSOG StAnz. 2023 S. 946, 2.1 Anwendergruppen.
40 *K.Schürmann*, Datenschutz-Folgenabschätzung beim Einsatz Künstlicher Intelligenz, ZD 2022, 316 (320).
41 Verwaltungsvorschrift zu § 25a HSOG (Fn. 39), 2.3 Schulung.
42 Vgl. hierzu Art. 19 JI-RL, Art. 32 DSGVO, Urteil des BVerfG ADA (Fn. 2), Rn. 163, nunmehr auch Art. 15 KI-VO.

werden, zählt der Gesetzgeber lediglich nummerisch in der Verwaltungsvorschrift auf, die auf § 25a HSOG n.F. basiert.[43]

Der § 25a Abs. 4 HSOG n.F. regelt die Zugriffskontrolle und die Protokollierungspflicht. Während die Zugriffskontrolle quantitativ eingrenzen soll, dient die Protokollierungspflicht der qualitativen Eingrenzung. Sie dient – so der unmittelbare Gesetzeswortlaut – „der Selbstvergewisserung und der nachträglichen Kontrolle". Diese verfassten Protokolle, wieso also eine automatisierte Datenanalyse durchgeführt wurde, sollen der stichprobenartigen Kontrolle zugrunde gelegt werden.[44] Grundsätzlich ist dies zu begrüßen, denn die schriftliche Fixierung der Tatsachen, die den Einsatz sowohl rechtfertigen als auch den Zweck benennen, dient der Vergewisserung über die Rechtmäßigkeit der Maßnahme. Zudem wird hierdurch eine spätere Kontrolle ermöglicht. Für ihre tatsächliche Wirksamkeit sind jedoch konkrete Anforderungen der Genauigkeit erforderlich – etwa in Gestalt der Subsumtion unter dem Rechtssatz.[45]

Das „abgestufte Kontrollkonzept" sieht aufgrund der hohen Zahl der Maßnahmen die Verteilung der Kontrollbefugnis zwischen verschiedenen Kontrollinstanzen vor – hier zwischen dem behördlichen und dem hessischen Datenschutzbeauftragten sowie dem Behördenleiter."[46] In der konkreten Neugestaltung des § 25a HSOG sieht dies wie folgt aus: Bei der Einrichtung oder einer wesentlichen Änderung liegt die Anordnungsbefugnis beim Behördenleiter und der hessische Datenschutzbeauftragte ist anzuhören. Für jeden Fall der automatisierten Datenanalyse hat der behördliche Datenschutzbeauftragte das Recht der stichprobenartigen Kontrolle – hierfür sind die Protokolle Grundlage. Vor dem Hintergrund, dass der Richtervorbehalt aufgrund „der Komplexität der Datenverarbeitung einer zügigen Beurteilung entgegensteht"[47], dürfte das abstrakte Kontrollkonzept ein besserer Ansatz sein.

Nicht durch den hessischen Gesetzgeber umgesetzt ist das „staatliche Monitoring" bei der Entwicklung der eingesetzten Software. Wobei das Gericht die Anforderungen hieran nicht als Verfahrensgegenstand sah.[48]

43 Verwaltungsvorschrift zu § 25a HSOG (Fn. 39), 2.2.1 – 2.2.7.
44 *Hess. LT,* Änderungsantrag vom 20.06.2023, Drs. 20/11235, S. 17.
45 *Graulich,* Das Handeln von Polizei- und Ordnungsbehörden zur Gefahrenabwehr (Fn. 33), Rn. 699–700.
46 Urteil des BVerfG ADA (Fn. 2), Rn. 109.
47 *Kugelmann/ Buchmann*, Der Algorithmus und die Künstliche Intelligenz als Ermittler (Fn. 21), 1 (7).
48 Urteil des BVerfG ADA (Fn. 2), Rn. 109.

Auch wenn sich im Bericht des Untersuchungsausschusses mehrfach die „Beteuerung" wiederfindet, dass ein privater Akteur keinen Zugriff auf die Daten habe, so bietet es sich für einen rechtssicheren Umgang an, ein eigenes technisches Analysesystem zu entwickeln.[49]

V. Kritik an der Neukonzeptionierung

Auch die Neukonzeption der Ermächtigungsgrundlage stößt auf Kritik. Dabei wird auf formaler Ebene der Gesetzgebungsprozess kritisiert und in materieller Hinsicht die Umsetzung moniert. Am 23.06.2023 kritisierte die Humanistische Union in einem offenen Brief an die Abgeordneten des Hessischen Landtags, dass der Änderungsantrag (Drs. 20/11235) für die Öffentlichkeit noch nicht einsehbar sei, die Abgeordneten erst seit dem 20.06.2023 Einsicht haben und dass es das Schnellverfahren unter Ausschluss der Anhörung/Stellungnahme zivilrechtlicher Organisationen nahezu unmöglich mache, außerparlamentarisch die Thematik zu erörtern.[50] Obwohl die Komplexität der Thematik es angeboten hätte, verzichtete die Regierungskoalition auf die Anhörung von Sachverständigen,[51] bzw. dem hessischen Datenschutzbeauftragten[52], was auf erhebliche Kritik stieß.[53]

Im Juni 2024 erhob die Gesellschaft für Freiheitsrechte e.V. Verfassungsbeschwerde gegen die neue Ermächtigungsgrundlage und beanstandete, dass keine der Varianten der § 25a Abs. 2 S. 1 Nr. 1–3 HSOG n.F. die Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Überwachung erfülle. Es mangele an einem adäquaten Kontrollmechanismus innerhalb des § 25a HSOG. Zwar sei gemäß § 25a Abs. 4 S. 6 HSOG

49 *A. Meister,* Wir veröffentlichen den Entwurf zum neuem BKA-Gesetz, 15.08.2024 (https://tinyurl.com/37sym42u) (zuletzt abgerufen am 17.10.2024).

50 *P. Dingeldey & Bundesvorstand der Humanistischen Union,* Offener Brief an die Abgeordneten des Hessischen Landtags vom 23.06.2023 (https://tinyurl.com/p3t7da9c) (zuletzt abgerufen am 17.10.2024).

51 Hierzu äußerte sich die Abgeordnete Eva Goldbach wie folgt: „Wir hätten keine Zeit mehr gehabt, in dieser Legislaturperiode eine dritte Anhörung […]. durchzuführen und die Auswertung vorzunehmen. Das hätten wir nicht mehr geschafft. […] Wir setzen das jetzt um – aus verschiedenen Gründen, weil wir es abschließen wollten […]", Hess. Lt. Plenarprotokoll 20/136 vom 27.06.2023, 11238.

52 *Hess. Datenschutzbeauftragter, A. Roßnagel,* Hess. LT, Drs. 21/27 vom 31.12.2023, S. 49.

53 Siehe *Hanning Voigts,* Hessen: Kritik an Reform zur „Hessendata" – Software, Frankfurter Rundschau vom 23.06.2023 (https://tinyurl.com/59czae35, zuletzt abgerufen am 10.10.2024).

der behördliche Datenschutzbeauftragte berechtigt, stichprobenartige Kontrollen durchzuführen, jedoch handele es sich lediglich um eine Erlaubnis und nicht um eine Verpflichtung, wodurch eine regelmäßige Kontrolle nicht garantiert sei.[54]

Da jedoch die aufsichtliche Kontrolle den schwachen Individualrechtsschutz kompensieren soll, ist eine restriktivere Kontrollhandhabe erforderlich, um auch von ihrer Wirksamkeit auszugehen.[55] Sehr umstritten ist der Einsatz einer solch komplexen Methode unter Einbeziehung eines ausländischen privaten Akteures. Während das gerichtlich geforderte „staatliche Monitoring" nicht umgesetzt wurde, aber durch die Literatur verlangt wird,[56] wird innerhalb der Politik der Einsatz auch auf Bundesebene gefordert.[57]

C. Anwendungsorientierte Kontrollmechanismen – eine europäische Strategie

Auch der EuGH hat in seinen Entscheidungen in Ansätzen den Einsatz automatisierter Vorgänge an besondere Voraussetzungen geknüpft, wenn auch nicht mit entsprechender Schwerpunktsetzung.

I. Verzicht auf KI? – Drei Kriterien des EuGHs zur PNR-Entscheidung

Im Jahre 2022 entschied der EuGH über die Verarbeitung von Fluggastdaten und die Rechtmäßigkeit der PNR-Richtlinie.[58] Die Entscheidung des Gerichts unterstützt den Einsatz der automatisierten Verarbeitung, nennt für ihren rechtmäßigen Einsatz auch Kriterien, gleichwohl schiebt sie einen

54 *T. Singelnstein,* Verfassungsbeschwerde vom 21.06.2024, S. 95 veröffentlicht über freiheitsrechte.org (https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Polizeigesetz-Hessen/Verfassungsbeschwerdeschrift-HSOG.pdf, zuletzt besucht am 10.10.2024).

55 *M. Bäuerle,* in: M. Möstl/M. Bäuerle (Hrsg.): BeckOK Polizei- und Ordnungsrecht Hessen, 33. Edition, §25a Rn. 115.

56 *M. Bäuerle,* § 25a HSOG (Fn. 55), Rn. 65a.

57 Antrag der CDU/CSU Fraktion BT-Drucks. 20/9495 vom 27.11.2023: „Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des Bundesministeriums des Innern und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren".

58 EuGH, Urteil PNR (Fn. 3).

Riegel beim Einsatz selbstlernender Systeme vor, da diese „ohne menschliche Einwirkung und Kontrolle – den Bewertungsprozess und insbesondere die Bewertungskriterien, auf denen das Ergebnis der Anwendung dieses Prozesses beruht, sowie die Gewichtung der Kriterien ändern können."[59] Diese sehr klare Feststellung unterliegt der Kritik, dass sich der Gerichtshof „auf ein juristisch, technologisch und politisch hochbrisantes Themengebiet begab", gleichwohl „den Unterschied zwischen Mustererstellung und Musterabgleich nicht klarer ausarbeitete."[60] Wird auf selbstlernende Systeme verzichtet, bedeutet dies auch, dass auf das Gesamtpotenzial der Technologie verzichtet wird, mit der Konsequenz, dass letztlich „wieder" eine menschliche Kraft den Abgleich durchgeführt und die gegenwärtige Vorgehensweise unverändert fortgesetzt wird.[61] Folgt man trotzdem der Auffassung des Gerichts, bleiben – auch im Rückgriff auf die Ausführungen des Generalanwalts drei entscheidende Kriterien beim Einsatz „automatisierter Verarbeitung": Wesentlich sei, so das Gericht,

- „die Erkennbarkeit, dass eine algorithmische Entscheidung erfolgte"[62],
- „die Funktionsweise des Algorithmus muss bekannt sein"[63] und
- „die Nachvollziehbarkeit des Ergebnisses"[64], sodass eine Überprüfung erfolgen kann.

Die Herausforderung in dieser Entscheidung ist, dass zwar die Erforderlichkeit von Kriterien klar benannt wird, die konkrete Ausgestaltung aber durch den Gerichtshof offengelassen wird und letztlich der Exekutive auf-

59 EuGH, PNR (Fn. 3), Rn. 194.

60 *I. Kostov,* Die Fluggastdatenverarbeitung zu Sicherheitszwecken, GSZ, 2023 13 (15).

61 *K. Korte*, I-Anwendungen müssen transparent und diskriminierungsfrei sein. RDI 2022, 538 (540).

62 *G. Pitruzella,* Schlussantrag vom 27.01.2022, C-817/19, ECLI:EU:C:2022:65 Rn. 228: „[…] dass die Funktionsweise der Algorithmen, die im Rahmen der in Art. 6 Abs. 3 Buchst. b vorgesehenen Analyse verwendet werden, transparent und das Ergebnis ihrer Anwendung nachvollziehbar sein muss. […] Es verlangt jedoch, dass die Erkennbarkeit der algorithmischen Entscheidungsfindung gewährleistet ist."

63 *G. Pitruzella.* (Fn. 63): „Die Transparenz der Funktionsweise der verwendeten Algorithmen ist auch eine notwendige Bedingung, um den Betroffenen die Ausübung ihrer Beschwerderechte und ihres Rechts auf effektiven gerichtlichen Rechtsschutz zu ermöglichen."

64 *G. Pitruzella.* (Fn. 63):„Zum anderen muss –[…] bei der automatisierten Verarbeitung von PNR[…] auf andere, nicht automatisierte Art individuell überprüft wird, nachvollzogen werden können, weshalb das Programm zu einem solchen Treffer gelangt ist[…]".

erlegt wird.[65] So lässt sich aus der Entscheidung nicht erschließen, wie die „Bekanntheit der Funktionsweise" oder die „Nachvollziehbarkeit" geartet sein muss. Zu beachten ist auch, dass das „Verständnis" zur Funktionsweise nicht zur Erhöhung des Schutzes des Betroffenen führt.[66]

II. Das Recht auf menschliche Entscheidung – EuGH zum Schufa Scoring

Bei der sog. Schufa-Scoring-Entscheidung ging es um voll- bzw. teilautomatisierte Entscheidungen unter Berücksichtigung von Art. 22 DS-GVO. Der Gerichtshof verhandelte die automatisierte Erstellung der Entscheidungsgrundlage, wobei der EuGH drei wesentliche Kriterien hervorhob:

- „Verwendung geeigneter mathematischer oder statistischer Verfahren
- Konzeptionierung und Durchführung von technisch-organisatorischen Maßnahmen
- Rechtsschutzmöglichkeiten für den Betroffenen"[67]

Diese drei Kriterien dürften sich mit der bereits begonnen Rechtsprechungslinie des EuGHs decken und nach Auffassung der Verfasserin auch die Strategie der KI-VO und der europäischen Gesetzgebung widerspiegeln.[68] Diese abstrakten Regeln werden bei ihrer Anwendung jedoch auf Herausforderungen stoßen, etwa bei der Prüfung, ob der Anwendungsbereich eröffnet wird. Sofern der Scorewert und die damit einhergehende Entscheidung ausschließlich auf Grundlage des Systems erfolgt, ist der Anwendungsbereich eröffnet. Schwierig(er) wird es, wenn sich an den automatisiert errechneten Score eine menschliche Entscheidung anschließt. Die Ermittlung der Grenzen dürfte jedoch in naher Zukunft (wenn schon nicht sogar gegenwärtig) eine Vielzahl von Anwendungsfälle betreffen.[69] Zur Umgehung des Anwendungsbereichs müsste daher nach der Rechtspre-

65 *A. Sandhu,* EuGH: Datenschutzrecht: Achtung der Grundrechte erfordert Beschränkung in der PNR-Richtlinie vorgesehenen Befugnisse auf das absolut Notwendige, EuZW 2022, 706 ff. (718).

66 *I. Kostov,* Die Fluggastdatenverarbeitung zu Sicherheitszwecken (Fn. 60), 13 (17).

67 *EuGH,* Urteil vom 07.12.2023, C-634/21ECLI:EU:C:2023:957 Rn. 59.

68 *T. Radtke,* Das Verhältnis von KI-VO und Art. 22 DS-GVO unter besonderer Berücksichtigung der Schutzzwecke, RDi 2024, 353 ff.; vgl. Art. 9–15, 64–70 KI-VO und zur „vertrauenswürdigen KI", – Erw.Gr. 27 KI-VO HILEG (2019) (https://tinyurl.com/56zwd89y).

69 Ausführlich hierzu: *T. Fuchs, Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*, Auswirkungen des Schufa-Urteils auf KI-Anwendungen – auto-

chung bei jedem einzelnen Vorgang eine Kontrolle durch einen Menschen erfolgen, der sowohl die Funktionsweise versteht und die Möglichkeit der Übersteuerung hat.[70] Zu prüfen ist jedoch auch, welchen Einfluss ein Ergebnis auf die menschliche Entscheidungskontrolle hat, denn die Abweichung vom Ergebnis verlangt meist eine Begründung, die oft mit erhöhtem Rechtfertigungsaufwand einhergeht.[71]

D. Ausblick

Anhand der Konturierung der deutschen und europäischen Rechtsprechung wird deutlich, dass zwei unterschiedliche Strategien bei der Konzipierung von Kontrollmechanismen für automatisierte Datenvorgänge möglich sind.

Das Legal Design des BVerfG zeigt sich „innovationsoffen" und ermöglicht den frühen Einsatz einer wenig erprobten Software eines privaten Akteures. Es versucht dem Verhältnismäßigkeitsgrundsatz durch hohe Anforderungen an den Anwender Rechnung zu tragen. Dabei soll die „aufsichtliche Kontrolle" durch das „abgestufte Kontrollkonzept" ergänzt werden. Deutlich wird allerdings, dass dies durch ihren stichprobenartigen Charakter letztlich eher zu einem Transparenzkriterium wird. Auch im Hinblick auf die bereits anhängige Verfassungsbeschwerde dürfte abzuwarten sein, ob weitere Ausführungen zum „staatlichen Monitoring" folgen – dies insbesondere deshalb, weil die enge Kooperation zwischen einem privaten (ausländischem) Akteur sowie einer Sicherheitsbehörde weitere Rechtsfragen aufwirft. Der EuGH nähert sich der Herausforderung hingegen von einer funktionalen Perspektive. Seine Kriterien an die „Bekanntheit" und „Nachvollziehbarkeit" sind tendenziell eher anwendungsorientiert und dürften auch mit der KI-VO im Einklang stehen, weshalb hier eine „europäische Strategie" deutlicher wird.

Für eine wirksame aufsichtliche Kontrolle gilt es nun beide Strategien einerseits zu harmonisieren und andererseits auf mögliche „positive bzw.

matisierte Entscheidungen dürfen keine maßgebliche Rolle spielen, Pressemitteilung vom 07.12.2023, https://tinyurl.com/4vcazu4b.

70 *A. Golland,* KI und KI-Verordnung aus datenschutzrechtlicher Sicht, EuZW 2024, 846 (850).

71 *B. Paal/J. Hüger*, Die KI-VO und das Recht auf menschliche Entscheidung, MMR 2024, 540 (541).

negative Kompetenzkonflikte“[72] zu prüfen. Denn in Konkurrenz treten nicht nur mitgliedstaatliche und europäische Regelungen, sondern auch daten(schutz)rechtliche (DSGVO/DSA/DMA/DA/JI-Richtlinie) und KI-rechtliche (KI-VO) Regelungen. Die Bestimmung des Anwendungsbereichs und die Ausgestaltung der wirksamen Kontrollmechanismen dürften daher Kernaspekte der Diskussion über den sicherheitsbehördlichen KI-Einsatz in den kommenden Jahren sein, denen sich sowohl die Legislative als auch die Judikative zu stellen haben wird.

72 *Vogel/Eisele*, in: E. Grabitz/M. Hilf/M. Nettesheim/Vogel/Eisele (Hrsg.), Das Recht der Europäischen Union, 82. EL Mai 2024, Art. 82 AEUV Rn. 73.

Digitale Zwillinge von KRITIS
Potenziale und Anforderungen zur Erhöhung der IT-Sicherheit

Luise Lautenbach[1]

Das Konzept des Digitalen Zwillings im Industriekontext steckt zwar noch in seinen Kinderschuhen, die Technologie gewinnt in Industrie und Wirtschaft jedoch zunehmend an Bedeutung. Es handelt sich um virtuelle Repliken realer Systeme, die es ermöglichen, deren Betrieb und Risiken in Echtzeit zu überwachen, zu analysieren oder sogar zu steuern.

Auch im Bereich Kritischer Infrastrukturen (KRITIS) wurde das Potential des Digitalen Zwillings bereits erkannt. So bietet er eine vielversprechende Möglichkeit, die sensiblen IT-Systeme von KRITIS effizienter und widerstandsfähiger zu gestalten. Gleichzeitig sind Digitale Zwillinge mit ihrer hochvernetzten Verbindung zum realen System auch eine potenzielle Schwachstelle. Cyberkriminelle können sich hierüber Zugriff auf die realen Systeme verschaffen. Betreiber von KRITIS müssen die IT-Sicherheit der digitalen Repräsentanzen daher von Anfang an mitdenken.

Im folgenden Beitrag sollen die IT-sicherheitsrechtlichen Rahmenbedingungen, die beim Einsatz Digitaler Zwillinge von KRITIS zu berücksichtigen sind, beleuchtet werden. Dafür werden zunächst das Konzept des Digitalen Zwillings im Industrial Metaverse vorgestellt und seine Potentiale für KRITIS herausgearbeitet. Anschließend werden die IT-sicherheitsrechtlichen Vorgaben, die sich beim Einsatz im KRITIS-Bereich ergeben, geprüft. Der Fokus liegt dabei auf den Vorschriften des BSIG, das die zentrale gesetzliche Grundlage für IT-Sicherheit für Kritische Infrastrukturen bildet.

---

1 Die Autorin ist Rechtsanwältin bei Noerr PartG mbB im Bereich Data, Tech & Telecom. Sie dankt Herrn Tim Alexander Großmann, wissenschaftlicher Mitarbeiter bei Noerr PartG mbB, für die gelungene Unterstützung. Sämtliche Internetquellen wurden zuletzt am 12.10.2024 abgerufen.

A. Einführung – Digitale Zwillinge im Industriekontext

Das Metaversum ist neben künstlicher Intelligenz eines der zentralen aktuellen Entwicklungsfelder in der digitalisierten Welt von heute. Es ist – anders als die Umbenennung des Facebook-Konzerns in „Meta" vermuten lassen könnte – kein spezifisches Produkt eines einzelnen Unternehmens, sondern vielmehr die Bezeichnung für ein nicht einheitlich definiertes, umfassendes technologisches Konzept.[2] Im Kern ist dieses auf eine stärkere Einbindung virtueller Elemente in die wahrnehmbare physische Realität gerichtet – die digitale Welt soll mit der analogen Welt verschmelzen.

Ausgehend davon wird mit dem Begriff des Metaversums häufig eine virtuelle Welt mit digitalen Avataren und virtuellen Gegenständen assoziiert, welche regelmäßig mittels Datenbrillen und Extended-Reality-Technologien (XR) in 3D und in einer 360°-Perspektive visuell dargestellt wird.[3] In diesem „3D-Internet"[4] können Menschen, repräsentiert durch ihre Avatare, unabhängig von ihrem physischen Aufenthaltsort, in simulierten dreidimensionalen Konferenzräumen zusammenkommen,[5] an virtuellen Konzerten teilnehmen[6] oder touristische Attraktionen besuchen[7]. Diese Verbreitungstypen, welche teils als kommerzielles und als Verbraucher-Metaversum bezeichnet werden,[8] stellten den Menschen sowie den ihn repräsentierenden Avatar in den Mittelpunkt.

---

2 Vgl. *M. Kaulartz/A. Schmid/F. Müller-Eising*, Das Metaverse – eine rechtliche Einführung, RDi 2022, 521 (522).

3 Fraunhofer-Verbund IUK-Technologie, Technologien und Use Cases für das (Industrial) Metaverse – Fakt oder Fiktion?, Berlin 2020, abrufbar unter: https://www.iuk.fraunhofer.de/content/dam/iuk/de/Download/Technologien%20und%20Use%20Cases%20f%C3%BCr%20das%20(Industrial)%20Metaverse.pdf; *Kaulartz/Schmid/Müller-Eising*, Metaverse (Fn. 2), 522.

4 Fraunhofer IUK-Technologie, Use Cases (Fn. 3).

5 *K. Krause*, Meet Me In The Metaverse: The Future Of Virtual And In-Person Events, 20.10.2022, abrufbar unter https://www.forbes.com/councils/forbescommunicationscouncil/2022/10/20/meet-me-in-the-metaverse-the-future-of-virtual-and-in-person-events/.

6 *B. Marr*, The World Of Metaverse Entertainment: Concerts, Theme Parks, And Movies, 27.07.2022, abrufbar unter https://www.forbes.com/sites/bernardmarr/2022/07/27/the-world-of-metaverse-entertainment-concerts-theme-parks-and-movies/.

7 *M. Constantin/G. Genovese/K. Munawar/R. Stone*, Tourism in the metaverse: Can travel go virtual?, 04.05.2023, abrufbar unter: https://www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/tourism-in-the-metaverse-can-travel-go-virtual.

8 Bundesverband der Deutschen Industrie, Das industrielle Metaverse – Chancen für die Industrie, 06.06.2023 abrufbar unter https://bdi.eu/artikel/news/das-industrielle-me

Demgegenüber gibt es auch ein sogenanntes *Industrial Metaverse*[9], was die Digitalisierung, Virtualisierung und Vernetzung der industriellen Produktion auf eine neue Ebene hebt. Es verbindet reale Produktionsprozesse mit einer virtuellen Welt, in der diese Prozesse simuliert, überwacht und optimiert werden können. Es basiert dabei auf dem Einsatz fortschrittlicher Technologien, die eine nahtlose Integration und Interaktion zwischen der physischen und der digitalen Welt ermöglichen. Hierzu gehören insbesondere Künstliche Intelligenz, maschinelles Lernen, *Augmented Reality* (AR), *Blockchain* sowie *Cloud-Computing*.[10]

Im Vordergrund des *Industrial Metaverse* stehen realitätsgetreue virtuelle Abbildungen von realen Systemen und Prozessen. Solche Abbildungen werden auch als Digitale Zwillinge bezeichnet. Sie werden auch als das „Herzstück" des *Industrial Metaverse* bezeichnet,[11] mit dem die Hoffnung einer „neuen Ära in der industriellen Produktion und Kooperation" verbunden wird.[12]

Wenngleich sich ihre volle praktische Bedeutung wohl erst in der näheren Zukunft entfalten wird, finden Digitale Zwillinge im *Industrial Metaverse* bereits heute in verschiedensten Wirtschaftssektoren Verwendung.[13] Nur beispielhaft sei in diesem Zusammenhang auf BMW verwiesen, das die „Omniverse-Plattform" von NVIDIA nutzt, um mithilfe Digitaler Zwillinge den Planungsprozess neuer Fabriken zu optimieren.[14]

---

taverse-chancen-fuer-die-industrie. Im Englischen sind die Bezeichnungen consumer metaverse sowie enterprise metaverse geläufig, vgl. *K Whiting*, Consumer, enterprise or industrial? The 3 main ways we are using the 'metaverse' explained, 17.02.2023 abrufbar unter: https://www.weforum.org/agenda/2023/02/metaverse-use-cases-industrial-consumer-enterprise/.

9 Deutsch: Industrielles Metaversum.

10 Bundesverband der Deutschen Industrie, Chancen (Fn. 8).

11 Bundesverband der Deutschen Industrie, Chancen (Fn. 8).

12 Bundesverband der Deutschen Industrie, Das Industrial Metaverse als wichtiger Chancenträger für die Industrie von morgen, 22.4.2024, abrufbar unter: https://bdi.eu/publikation/news/das-industrial-metaverse-als-wichtiger-chancentraeger-fuer-die-industrie-von-morgen.

13 Etwa *A. Kung, C. Baudoin, K. Tobich*, Report of TWG Digital Twin: Landscape of Digital Twin Standards, 09.06.2022, S. 1, abrufbar unter: https://www.standict.eu/digital-twin-standards-report.

14 BMW, Pressemitteilung: BMW Group auf der NVIDIA GTC: Produktion im künftigen Werk Debrecen läuft schon virtuell, 21.03.2023, abrufbar unter: https://www.press.bmwgroup.com/deutschland/article/detail/T0411467DE/bmw-group-auf-der-nvidia-gtc:-produktion-im-kuenftigen-werk-debrecen-laeuft-schon-virtuell?language=de.

Auch der Gesetzgeber – sowohl auf nationaler als auch auf europäischer Ebene – nimmt in verschiedenen Zusammenhängen auf das Konzept des Digitalen Zwillings im Industriekontext Bezug und bringt damit prinzipielles Bewusstsein für diese technologische Entwicklung zum Ausdruck.[15]

I. Definition und technische Grundlagen

Bislang existiert keine einhellig anerkannte Definition zum Digitalen Zwilling, zumal Überschneidungen mit verwandten Begriffen wie digitalen Modellen, Simulationen und dem Internet of Things (IoT) bestehen.

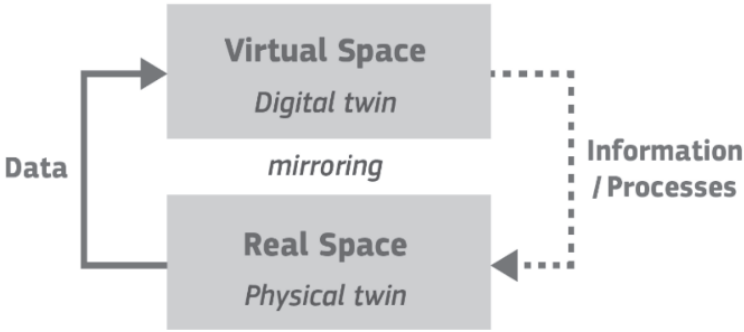
Nach dem hier zugrunde gelegten Verständnis handelt es sich bei einem Digitalen Zwilling um die virtuelle Abbildung eines realen Systems, die mit dem realen System verknüpft ist und dieses in allen relevanten Aspekten – je nach Synchronisationsintervall – möglichst in Echtzeit abbildet.[16] Der entscheidende Unterschied zu klassischen Simulationsmodellen besteht

15 Auf nationaler Ebene s. die Begründung der Bundesregierung zum Gesetz für die Wärmeplanung und zur Dekarbonisierung der Wärmenetze, BT-Drs. 20/8654, S. 93; ferner fördern verschiedene Bundesministerien unterschiedliche Projekte zu digitalen Zwillingen, s. etwa Bundesministerium für Digitales und Verkehr, Digitale Zwillinge für Infrastruktur, Bau, Wohnen – von Theorie und Konzeption in die Praxis, 07.02.2024, abrufbar unter: https://bmdv.bund.de/DE/Themen/Digitales/Building-Information-Modeling/Digitale-Zwillinge/digitale-zwillinge.html, sowie Bundesministerium für Wirtschaft und Klimaschutz, Der digitale Zwilling, abrufbar unter: https://www.bmwk.de/Redaktion/DE/Artikel/Digitale-Welt/GAIA-X-Use-Cases/der-digitale-zwilling.html. Auf EU-Ebene s. insb. das Positionspapier der EU-Kommission vom 11.7.2023 zum Thema „Web 4.0 and virtual worlds", COM(2023) 442/final.

16 In der Sache ebenso ISO/IEC 30173: „*the digital representation of a target entity with data connections that enable convergence between the physical and digital states at an appro :priate rate of synchronization.*", vgl. IEC, Internationally agreed concepts and terminology for digital twins, abrufbar unter https://www.iec.ch/blog/internationally-agreed-concepts-and-terminology-digital-twins; ähnlich etwa *E. Brucherseifer/H. Winter/ A. Mentges/ M. Mühlhäuser/M. Hellmann*, Digital Twin conceptual framework for improving critical infrastructure resilience, at 2021, 1062 (1067); *O. C. Madubuike/C. J. Anumba/R. Khallaf*, A review of digital twin applications in construction, ITcon 27 (2022), 145 (147).

demzufolge in der Verknüpfung zwischen Digitalem Zwilling und realem System.[17]

Das Konzept des Digitalen Zwillings setzt sich mithin aus drei Elementen zusammen: Dem realen System, seinem virtuellen Gegenstück sowie der Kommunikationsplattform als Schnittstelle zwischen den beiden anderen Elementen.[18] Die Kommunikationsplattform umfasst dabei einmal die Datenübertragung vom realen System hin zum Digitalen Zwilling. Zum anderen erlaubt sie die nutzergesteuerte oder automatisierte Einwirkung auf das reale System.[19]



Quelle: Frascolla, Digital Twins and Standards – Destination Earth Initiative, Trans Continuum Initiative, BDVA and STA4DESTINE, 22.11.2022, https://european-big-data-value-forum.eu/wp-content/uploads/2022/10/Digital-Twins-and-Standards-Frascolla_v3.pdf, Folie 6

17 *Madubuike/Anumba/Khallaf*, digital twin (Fn. 16), 147; *L. Wright/S. Davidson*, How to tell the difference between a model and a digital twin, Advanced Modeling and Simulation in Engineering Sciences, 2020 vol. 7, 13 (3); angesichts der Terminologie ist zu beachten, dass auch das abgebildete reale System gegebenenfalls digitale Elemente, namentlich Software, enthalten kann, vgl. *Brucherseifer/Winter/Mentges/Mühlhäuser/Hellmann*, Framework (Fn. 16), 1068.

18 *Madubuike/Anumba/Khallaf*, digital twin (Fn. 16), 148.

19 Aufgrund dieser Differenzierung unterscheidet *Brucherseifer/Winter/Mentges/Mühlhäuser/Hellmann*, Framework (Fn. 16), 1068 f. zwischen vier Komponenten des digitalen Zwillings. Im Rahmen dieses Beitrags wird die Kommunikationsplattform hingegen als ein Element bezeichnet.

II. Einsatzfelder

Im Industriebereich bieten Digitale Zwillinge eine Vielzahl von Verwendungsmöglichkeiten. In der Designphase können beispielsweise Entwicklung und Erprobung neuer Produkte und Prozesse in einer risikofreien, virtuellen Umgebung durchgeführt werden, bevor diese in die reale Produktion überführt werden.[20] Dies führt zu einer Minimierung von Risiken und Fehlern in der Produktentwicklung und -fertigung und damit zu einer Reduzierung von Kosten und Zeitaufwand.[21] Bei bestehenden Strukturen eignet sich der Einsatz Digitaler Zwillinge hingegen für die präzise und umfassende Simulation und Optimierung von Produktionsprozessen, indem sie reale Anlagen und Systeme in einer virtuellen Umgebung abbilden und deren Verhalten unter verschiedenen Bedingungen simulieren.[22] Hierdurch lassen sich reale Systeme und Prozesse über deren gesamte Lebensdauer analysieren, steuern und optimieren.[23] So können Unternehmen beispielsweise potenzielle Engpässe frühzeitig erkennen und Produktionsabläufe effizienter gestalten.[24] Zudem erlauben Digitale Zwillinge eine vorausschauende Wartung, da durch kontinuierliche Echtzeitüberwachung und Analyse

20 *Dietz/L. Hagemann/C. v. Hornung/G. Persul*, Employing Digital Twins for Security-by-Design System Testing, in: Association for Computing Machinery (Hrsg.), Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems (SaT-CPS '22), New York 2022, S. 97 (97 f.).

21 So vermeldete McKinsey bereits im Jahr 2022, dass ein Unternehmen seine Kapital- und Betriebskosten durch den Einsatz digitaler Zwillinge um 10 % senken konnte, vgl. McKinsey, Digital twins: The foundation of the enterprise metaverse, Oktober 2022, abrufbar unter: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-twins-the-foundation-of-the-enterprise-metaverse.

22 *N. Attoh-Okine*, ASME J. Risk Uncertainty Part B. Mar 2024, 10(1), 010301, Paper No. RISK-24–1015; *Brucherseifer/Winter/Mentges/Mühlhäuser/Hellmann*, Framework (Fn. 16), 1063.

23 *Brucherseifer/Winter/Mentges/Mühlhäuser/Hellmann*, Framework (Fn. 16), 1063; Fraunhofer IOSB, Digitale Zwillingssysteme – das Schlüsselkonzept für Industrie 4.0, abrufbar unter: https://www.iosb.fraunhofer.de/de/geschaeftsfelder/automatisierung-digitalisierung/anwendungsfelder/digitaler-zwilling.html.

24 Verband der Elektrotechnik Elektronik Informationstechnik e.V., Der Digitale Zwilling in der Netz- und Elektrizitätswirtschaft, VDE Studie, Offenbach am Main 2023, S. 24, abrufbar unter: https://www.vde.com/resource/blob/2257516/cce234dea484fc0b1943774391752d8a/studie-digitaler-zwilling---download-data.pdf; B. Wicha-Krause/J. Poos/B. Kreft Namen in Grün?, Wenn der Digitale Zwilling hinkt – ohne Daten keine aussagekräftigen Ergebnisse, BET Webmagazin, 19.06.2023, abrufbar unter: https://www.iec.ch/blog/internationally-agreed-concepts-and-terminology-digital-twins.

von Betriebsdaten mögliche Ausfälle prognostiziert und rechtzeitig Gegenmaßnahmen ergriffen werden können.[25]

B. Digitale Zwillinge von KRITIS

I. KRITIS als Rückgrat der Gesellschaft

KRITIS bilden das Rückgrat moderner Gesellschaften. Sie stellen grundlegende Dienstleistungen und Ressourcen bereit, auf die nahezu alle anderen Lebensbereiche angewiesen sind. Ihr reibungsloser Betrieb ist daher essenziell für die Aufrechterhaltung von Sicherheit, Wohlstand und gesellschaftlicher Ordnung. Insoweit besteht die besondere Verantwortung dieser Systeme darin, auch in Krisenzeiten ihre Funktionsfähigkeit sicherzustellen und die Grundversorgung der Gesellschaft zu gewährleisten.

Dies macht KRITIS zu einem sensiblen Ziel. In einer zunehmend vernetzten und digitalisierten Welt sind deren IT-Systeme verstärkt Cyberangriffen ausgesetzt.[26] Als zentrale Pfeiler der öffentlichen Sicherheit und Ordnung bedarf es daher besonderer Maßnahmen, um die Resilienz von KRITIS zu erhöhen und mögliche Ausfälle zu minimieren. Ihr Schutz und ihre Widerstandsfähigkeit rückt daher vermehrt in den Fokus moderner Sicherheitsstrategien.

II. IT-Sicherheit durch Digitale Zwillinge?

In diesem Kontext gewinnt das bislang weitgehend ungenutzte Potenzial leistungsfähiger Digitaler Zwillinge zunehmend an Bedeutung. Jenseits ihrer allgemeinen Vorzüge bieten Digitale Zwillinge nämlich weitreichende Möglichkeiten, um ein konstant hohes IT-Sicherheitsniveau zu etablieren. So lassen sich Sicherheitslücken, potenzielle Angriffswege und Schwach-

25 Verband der Elektrotechnik Elektronik Informationstechnik e.V., Elektrizitätswirtschaft (Fn. 24), S. 24.

26 Beispielsweise wurde im Jahr 2020 das IT-System eines Düsseldorfer Krankenhauses angegriffen. Der Angriff führte dazu, dass Patienten nicht rechtzeitig behandelt werden konnten. Die Folgen gingen so weit, dass eine Patientin durch diesen IT-Angriff verstarb, vgl. *K. Kerkmann/L. Nagel*, Todesfall nach Hackerangriff auf Uni-Klinik Düsseldorf, 18.09.2020, abrufbar unter https://www.handelsblatt.com/technik/cyberkriminalitaet-todesfall-nach-hackerangriff-auf-uni-klinik-duesseldorf/26198688.html.

stellen in einer sicheren, virtuellen Umgebung identifizieren und testen, ohne dass die realen Systeme außer Betrieb genommen werden müssen.[27] Dies ist besonders bei kritischen Systemen von Vorteil, wo auch nur kurze Ausfallzeiten erhebliche gesellschaftliche und wirtschaftliche Folgen haben können. Ein weiterer Vorteil besteht darin, dass eine durch Penetrationstests herbeigeführte Beschädigung des Digitalen Zwillings unschädlich ist. Dieser kann einfach zurückgesetzt werden.[28] Schlussendlich können Digitale Zwillinge umfangreiche Trainingsdaten bereitstellen, die Systeme zur Erkennung und Vermeidung von Angriffen stärken.[29] Diese Daten ermöglichen es beispielsweise, maschinelles Lernen und Künstliche Intelligenz zu nutzen, um Bedrohungen frühzeitig zu erkennen und darauf zu reagieren. Insoweit überrascht nicht, dass Digitale Zwillinge im Bereich von KRITIS vermehrt in den Fokus von Wirtschaft und Forschung rücken.[30]

Allerdings gehen mit ihrem Einsatz auch beachtliche Risiken einher. Durch ihre Verknüpfung bzw. den Datenaustausch mit dem realen System sind sie potenziell ebenso anfällig für Cyberangriffe wie die realen Systeme. Klassische Gefahren wie Identitätsdiebstahl, das Ausspähen von Betriebs- und Geschäftsgeheimnissen sowie die Verschlüsselung von Daten und an-

27 *Arrow*, Digital Twin: Die erste reale Anwendung des Metaverse, 12.09.2022, abrufbar unter: https://www.arrow.de/research-and-events/articles/digital-twin-the-first-real-application-of-the-metaverse.

28 *A. Giehl*, Digitale Zwillinge und ihr Potenzial für sichere Betriebstechnik (OT), 28.10.2022, abrufbar unter: https://www.cybersecurity.blog.aisec.fraunhofer.de/digitale-zwillinge-und-ihr-potenzial-fuer-sichere-betriebstechnik-ot/.

29 *Giehl*, Betriebstechnik (Fn. 28).

30 Verband der Elektrotechnik Elektronik Informationstechnik e.V., Elektrizitätswirtschaft (Fn. 24), S. 1 ff.; *C. Bischofberger*, Digital twins and the smart grid, e-tech, 03/2022, abrufbar unter: https://etech.iec.ch/issue/2022-03/digital-twins-and-the-smart-grid; Bundesverband der Energie- und Wasserwirtschaft e.V., Digitale Doppelgänger: Neue Chancen für die Wasserwirtschaft?, 13.3.2023, abrufbar unter: https://www.bdew.de/online-magazin-zweitausend50/generation/digitale-doppelgaenger-neue-chancen-fuer-die-wasserwirtschaft/; *M. Neumann*, Was Digital Twins für die Telekommunikationsbranche bedeuten, 28.6.2024, abrufbar unter: https://newroom-connect.com/blog/was-digital-twins-fuer-die-telekommunikationsbranche-bedeuten/; PWC, Der digitale Zwilling in der Medizin, abrufbar unter https://www.pwc.de/de/gesundheitswesen-und-pharma/der-digitale-zwilling-in-der-medizin.html; *Denga*, ZBB 2023, 280 (284); IT-Finanzmagazin, Digital Twin Technologie-Report: Finanzsektor setzt voll auf digitale Zwillinge, 28.8.2023, abrufbar unter: https://www.it-finanzmagazin.de/altair-studie-finanzsektor-setzt-voll-auf-digitale-zwillinge-160027/; Deutsches Zentrum für Luft- und Raumfahrt e. V., Simulationsmethoden für Digitale Zwillinge, abrufbar unter: https://www.dlr.de/de/pi/ueber-uns/abteilungen/simulationsmethoden-fuer-digitale-zwillinge.

schließende Erpressung können folglich auch den Digitalen Zwilling betreffen.[31] Im schlechtesten Fall können Cyberkriminelle über den Digitalen Zwilling auch Zugriff auf das reale System erhalten und die Steuerung übernehmen bzw. Ausfälle provozieren.

Ein weiteres Risiko birgt der sogenannte "gefälschte digitale Zwilling": Bei diesem Angriffsmittel schaffen Cyberkriminelle durch erbeutete Daten virtuelle Kopien realer Systeme und nutzen diese beispielsweise für *Social Engineering*-Angriffe.[32] Solche gefälschten Zwillinge gefährden nicht nur die Integrität und Sicherheit von KRITIS, sondern können auch das Vertrauen in die Authentizität und Verlässlichkeit der digitalen Repräsentationen untergraben.

Der Einsatz Digitaler Zwillinge im Bereich von KRITIS geht somit sowohl mit Chancen als auch Risiken für die IT-Sicherheit einher. Betreiber, die diese Technologie in Betracht ziehen, sollten nicht nur angemessene Sicherheits- und Überwachungsmaßnahmen ergreifen, sondern müssen auch die rechtlichen Anforderungen, die sich an den Einsatz Digitaler Zwillinge stellen, eruieren und implementieren.

C. Rechtliche Rahmenbedingungen

Mit der DSGVO, der KI-Verordnung[33] sowie diversen anderen Rechtsakten hat die EU bereits einen starken Rechtsrahmen geschaffen, der potenzielle Bereiche des *Industrial Metaverse,* und damit auch den Einsatz Digitaler Zwillinge, reguliert. Im Kontext von KRITIS muss jedoch auch das IT-Sicherheitsrecht besonders in den Blick genommen werden.

Maßgebend ist hierfür das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG).[34] Es bildet den Grundstein der KRITIS-

31 PWC, Neue Risiken an der Schnittstelle von Metaverse und digitalen Zwillingen, abrufbar unter: https://www.pwc.de/de/cyber-security/neue-risiken-an-der-schnittstelle-von-metaverse-und-digitalen-zwillingen.html.

32 PWC, Risiken (Fn. 31); auch als „*Evil Digital Twin*" betitelt.

33 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).

34 Des Weiteren enthalten Spezialgesetze wie das TKG (bspw. §§ 165, 166 TKG) und das EnWG (§ 11 EnwG) IT-Sicherheitspflichten. Eine detaillierte Darstellung dieser

Regulierung in Deutschland. Es regelt nicht nur die Aufgaben, Befugnisse und Zuständigkeiten des Bundesamts für Sicherheit in der Informationstechnik (BSI), sondern legt auch Pflichten für Unternehmen im Bereich von KRITIS fest, um ein nationales IT-Sicherheitsniveau zu gewährleisten.

I. Digitaler Zwilling als KRITIS i. S. d. § 2 Abs. 10 BSIG

Wenn ein Digitaler Zwilling KRITIS virtuell abbildet, liegt zunächst die Annahme nahe, dass auch er automatisch zu KRITIS wird. Eine solche pauschale Einordnung verbietet sich jedoch. Da der Digitale Zwilling vielfältige Einsatzmöglichkeiten bietet, die aber nicht zwangsläufig von hoher Bedeutung für die Allgemeinheit sind, ist vielmehr zu prüfen, ob der Digitale Zwilling die Tatbestandsvoraussetzungen von KRITIS erfüllt.

Ausgangspunkt für die Frage, ob Infrastrukturen „kritisch" sind, ist die Legaldefinition in § 2 Abs. 10 S. 1 BSIG. Darin werden KRITIS bestimmt als Einrichtungen, Anlagen oder Teile davon, die einem der dort genannten Sektoren angehören und kumulativ von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden (§ 2 Abs. 10 S. 1 BSIG).

1. Kritische Infrastruktur

Die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) konkretisiert den Rechtsbegriff, indem sie „unter Festlegung" von kritischen Dienstleistungen, Anlagenkategorien und bedeutenden Versorgungsgraden, die sich durch Schwellenwerte messen lassen, bestimmt werden.

Die Einordnung als KRITIS nach dem BSIG und der BSI-KritisV erfolgt insofern nach folgendem Schema:[35] Es muss kumulativ (i) eine kritische Dienstleistung in einem der Sektoren nach § 2 Abs. 10 S. 1 Nr. 1 BSIG vorliegen, (ii) zu deren Erbringung eine Anlage, die einer in der BSI-KritisV festgelegten Anlagenkategorie zuzuordnen ist, betrieben wird und (iii) de-

Gesetze geht jedoch über den Zweck dieses Beitrags hinaus und wird daher von der Untersuchung ausgeklammert.

35 Nach *V. Vogel/N. Ziegler*, Kritikalität: Von der BSI-KritisV zur NIS2-Richtlinie, International Cybersecurity Law Review, 2023 vol. 4, 1 (6).

ren Versorgungsgrad durch Bemessung der entsprechenden Schwellenwerte als bedeutend anzusehen ist.

a) Kritische Dienstleistung

Was unter einer kritischen Dienstleistung zu verstehen ist, definiert § 1 Abs. 1 Nr. 3 BSI-KritisV. Danach handelt es sich um Dienstleistungen zur Versorgung der Allgemeinheit in den jeweiligen Sektoren, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde. Die nähere Bestimmung kritischer Dienstleistungen erfolgt in den §§ 2 – 9 BSI-KritisV für jeden Sektor durch Aufzählung der maßgeblichen Dienstleistungen und deren weitere Unterteilung.

Die Prüfung, ob eine kritische Dienstleistung vorliegt, bleibt zwar dem konkreten Einzelfall vorbehalten. Der Einsatz Digitaler Zwillinge kommt jedoch bei der Erbringung kritischer Dienstleistungen in sämtlichen Sektoren in Betracht.[36] Nur beispielhaft sei in diesem Zusammenhang etwa die Stromversorgung als kritische Dienstleistung im Energiesektor genannt, die sich gemäß § 2 Abs. 1–2 BSI-KritisV aus der Stromerzeugung, dem Stromhandel, der Stromübertragung und der Stromverteilung zusammensetzt.

b) Anlage, die einer Anlagenkategorie zuzurechnen ist

Liegt eine kritische Dienstleistung vor, rückt der Digitale Zwilling in den Fokus der Prüfung. Zu prüfen ist, ob der Digitale Zwilling eine Anlage darstellt, die sich einer in der BSI-KritisV festgelegten Anlagenkategorie zuordnen lässt.

Als Anlage bezeichnet man gemäß § 1 Abs. 1 Nr. 1 BSI-KritisV (i) Betriebsstätten und sonstige ortsfeste Einrichtungen, (ii) Maschinen, Geräte und sonstige ortsveränderliche Einrichtungen sowie (iii) Software und IT-Dienste, die für die Erbringung einer kritischen Dienstleistung notwendig sind. Die Legaldefinition der BSI-KritisV orientiert sich damit im Wesentlichen

36 Siehe zu den sektorübergreifenden Einsatzfeldern Digitaler Zwillinge bereits oben unter Punkt B. II.

am immissionsschutzrechtlichen Begriffsverständnis einer Anlage i. S. d. § 3 Abs. 5 BImSchG und ist daher weit auszulegen.[37]

Aus systematischer Sicht folgt hieraus, dass – anders als § 2 Abs. 10 BSIG vermuten lässt – es sich bei Anlagen und Einrichtungen nicht um unterschiedliche Kategorien handelt. Vielmehr fungiert der Begriff der Anlage als Oberbegriff.[38] Das erscheint auch insoweit konsequent, als dass die BSI-KritisV nur auf Teile einer Anlage, nicht aber auf Teile einer Einrichtung abstellt.[39]

Legt man die Legaldefinition des § 1 Abs. 1 Nr. 1 BSI-KritisV zugrunde, ist der Digitale Zwilling als Software bzw. IT-Dienst im Sinne von § 1 Abs. 1 Nr. 1 lit. c) BSI-KritisV und damit als Anlage einzustufen; vorausgesetzt, er ist für die Erbringung einer kritischen Dienstleistung notwendig.

Zu der Frage, wann von einer Notwendigkeit für die Erbringung der kritischen Dienstleistung auszugehen ist, gibt die BSI-KritisV keine Anhaltspunkte. Zielsetzung des Verordnungsgebers ist jedoch die Identifizierung jener Anlagen, deren Funktionsfähigkeit für die Versorgung der Allgemeinheit erhalten werden muss, um eine Inanspruchnahme der Notversorgung von vornherein zu verhindern.[40] Ausweislich der Verordnungsbegründung sollen damit zwei Arten von Anlagen nicht vom Anlagenbegriff erfasst sein; selbst, wenn sie die entsprechenden Schwellenwerte erreichen. Dies betrifft zum einen Anlagen, die ausschließlich der Notversorgung, nicht aber dem Regelbetrieb dienen.[41] Zum anderen sollen aber auch solche Anlagen ausgeschlossen sein, die allein für die Versorgung betriebsinterner Prozesse genutzt werden, etwa im Konzernverbund.[42]

37 Bundesministerium des Innern, Begründung zur BSI-KritisV, S. 6.

38 Wohl auch *Ritter* in D. Kipker/P. Reusch/S. Ritter (Hrsg.), Recht der Informationssicherheit, München 2023, BSIG § 2 Rn. 29: „[E]*ine scharfe Abgrenzung zwischen diesen Begriffen* [ist] *nicht immer möglich*".

39 Vgl. § 7 Abs. 7, § 8 Abs. 3, § 9 Abs. 3 BSI-KritisV.

40 Bundesministerium des Innern, Begründung zur BSI-KritisV, S. 6.

41 Bundesministerium des Innern, Begründung zur BSI-KritisV, S. 6.

42 Bundesministerium des Innern, Begründung zur BSI-KritisV, S. 6: „*Der Anlagenbegriff wird nur insoweit eingegrenzt, als eine Anlage im Sinne dieser Rechtsverordnung zur Versorgung der Allgemeinheit mit einer kritischen Dienstleistung notwendig sein muss. Nicht erfasst sind somit Anlagen, die zur Versorgung ausschließlich betriebsinterner Prozesse z. B. innerhalb eines Konzernverbunds dienen (Selbstversorgung).*" Im Wesentlichen ebenso im Zuge der Erweiterung durch § 1 Abs. 1 Nr. 1 lit. c BSI-KritisV Bundesministerium des Innern, Begründung zur 2. ÄnderungsVO der BSI-KritisV, S. 40.

Doch wann ist ein betrieblicher Prozess als nicht (nur) betriebsintern – und damit als notwendig zur Erbringung der kritischen Dienstleistung – anzusehen? Dieses Notwendigkeitskriterium ist in der juristischen Fachwelt bisher kaum näher beleuchtet worden. Einerseits könnte man den Begriff der Notwendigkeit eng auslegen und nur auf solche betrieblichen Prozesse beziehen, die selbst bei Berücksichtigung kompensatorischer Maßnahmen nicht hinweggedacht werden können, ohne dass die Erbringung der kritischen Dienstleistung beeinträchtigt würde. In diesem Sinne ließe sich von einem theoretischen Notwendigkeitsbegriff sprechen.[43] Demgegenüber kann das Notwendigkeitserfordernis auch weiter verstanden werden, sodass ihm all jene Anlagenbestandteile unterfielen, die im konkreten Fall für die Erbringung der kritischen Dienstleistung genutzt werden. Dies entspräche einem faktischen Notwendigkeitsbegriff.[44]

Richtigerweise ist das Kriterium der Notwendigkeit nicht in einem theoretischen, sondern in einem faktischen Sinne zu verstehen.[45] Ein solches versorgungsfunktionales Begriffsverständnis entspricht dem vom Gesetzgeber verfolgten Zweck, die Allgemeinheit vor dem partiellen oder vollständigen Ausfall kritischer Dienstleistungen zu schützen.[46] Maßgeblich ist folglich, ob die bestehende Versorgungskette bis zum betroffenen Bürger bedroht bzw. durch einen potentiellen Cyberangriff beeinträchtigt werden könnte.[47] In der Konsequenz sind vom Anlagenbegriff auch solche Anlagen erfasst, die sowohl für die Erbringung der kritischen Dienstleistung sowie für die Selbstversorgung parallel genutzt werden. Dies gilt selbst dann, wenn der Nutzungsanteil für die Selbstversorgung überwiegt.[48]

Ob die Nutzung eines Digitalen Zwillings ausgehend von den soeben dargelegten Maßstäben einen nicht ausschließlich betriebsinternen und damit für die kritische Dienstleistung notwendigen Prozess darstellt, kann nur im Einzelfall und in Abhängigkeit von dessen konkreter Funktions- und Verwendungsweise beurteilt werden. Im Folgenden sollen jedoch einige allgemeine, auf typisierte und praktisch besonders bedeutsame Fallkonstellationen bezogene Einschätzungen getroffen werden.

---

43 So *M. Glade* in D. Kipker/P. Reusch/S. Ritter (Hrsg.), Recht der Informationssicherheit, München 2023, BSI-KritisV § 1 Rn. 13.
44 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 13.
45 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 13.
46 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 13.
47 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 13.
48 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 13.

Dient der Digitale Zwilling ausschließlich zu Analysezwecken, kann sein Einsatz grundsätzlich hinweggedacht werden, ohne dass die Erbringung der kritischen Dienstleistung beeinträchtigt würde. Ein störungsbedingter Ausfall der durch den Digitalen Zwilling ermöglichten und durchgeführten Analysetätigkeit würde die Versorgung der Allgemeinheit grundsätzlich nicht gefährden. Die bloße Analyse der Realdaten bleibt vielmehr ein betriebsinterner Vorgang. Besonders deutlich wird dies dann, wenn anhand der Analysedaten mögliche Prozessoptimierungen (manuell oder automatisiert) entwickelt und vorgeschlagen werden. Das BSIG und die BSI-KritisV zielen nämlich nicht auf eine betriebswirtschaftliche Optimierung interner Prozesse, sondern auf die Gewährleistung eines sicherheitstechnischen Minimalstandards bei der Erbringung kritischer Dienstleistungen.[49]

Damit ist auch der Einsatz Digitaler Zwillinge zur bloßen fortlaufenden Entwicklung bestehender Systeme und Prozesse nicht notwendig i. S. d. § 1 Abs. 1 Nr. 1 BSI-KritisV. Dies gilt erst recht für die Verwendung Digitaler Zwillinge in der initialen Entwicklungsphase, denn zu diesem Zeitpunkt fehlt es bereits an der Erbringung einer kritischen Dienstleistung.

Weniger eindeutig fällt die Beurteilung aus, soweit der Digitale Zwilling zu Überwachungszwecken eingesetzt wird. Denn die Überwachung des realen Systems ermöglicht, dass drohende oder eingetretene Störungen frühzeitig erkannt, begrenzt und abgestellt werden können. Im Gegensatz zur reinen Analysetätigkeit besteht bei der Nutzung Digitaler Zwillinge zu Überwachungszwecken somit sehr wohl ein Bezug zur Aufrechterhaltung der für die Allgemeinheit bedeutenden Versorgung. Wenngleich das betriebsinterne Element im Vordergrund stehen mag, erscheint die Annahme nicht zwingend, der Einsatz Digitaler Zwillinge zu Überwachungszwecken erfolge ausschließlich zu betriebsinternen Zwecken. Zwar würde der Ausfall des Digitalen Zwillings, der zu Überwachungszwecken genutzt wird, die Erbringung kritischer Dienstleistungen nicht per se beeinträchtigen. Die Überwachung der realen Prozesse ist nicht unmittelbar Teil der konkreten Leistungserbringung, sondern soll im Fall gegenwärtiger oder künftiger Beeinträchtigungen lediglich ein zeitnahes Gegensteuern ermöglichen. Diese Erwägungen sprechen tendenziell dagegen, den Einsatz Digitaler Zwillinge zu Überwachungszwecken als notwendig im Sinne von § 1 Abs. 1 Nr. 1 BSI-KritisV anzusehen. Dem ist jedoch entgegenzuhalten, dass Anlagen zur Überwachung schlussendlich erforderlich sind, um die Sicherheit und

49 Vgl. BT-Drs. 18/4096, S. 19.

Funktionsfähigkeit kritischer Dienstleistungen zu gewährleisten, indem sie Bedrohungen frühzeitig erkennen und Ausfälle verhindern. Sie ermöglichen eine kontinuierliche Kontrolle und sofortige Reaktion auf sicherheitsrelevante Ereignisse, was für den reibungslosen Betrieb unerlässlich ist. Dies bestätigt auch der Verordnungsgeber, indem er in den Anhängen zu den einzelnen Sektoren jedenfalls teilweise Überwachungsvorrichtungen als Anlagenkategorie festlegt.[50] Anlagen, die der Überwachung dienen, sind somit schon kraft ausdrücklicher Anordnung für die Erbringung der kritischen Dienstleistung notwendig.

Ähnliches gilt für die Nutzung Digitaler Zwillinge, welche – neben anderen Verwendungszwecken – zumindest auch der Steuerung des realen Systems bzw. der realen Prozesse dienen. Dabei kann es keine Rolle spielen, ob der Digitale Zwilling aufgrund der in ihm integrierten Anwendungen automatisch oder lediglich durch die manuelle Bedienung eines menschlichen Nutzers Einfluss auf das reale System nehmen kann. Erlangen Unbefugte Zugriff auf den Digitalen Zwilling, wäre die Erbringung der kritischen Dienstleistung in beiden genannten Konstellationen akut gefährdet. Insofern ist der Einsatz Digitaler Zwillinge von realen, kritischen Systemen notwendig zur Erbringung kritischer Dienstleistungen.

Zu einer anderen Bewertung kommt man allenfalls dann, wenn der Umfang der Steuerungsmöglichkeit gering ausfällt. Dies wäre beispielsweise denkbar, wenn sich der Steuerungsumfang des Digitalen Zwillings auf einen abgrenzbaren kleinen Teil des realen Systems beschränkt. In einem solchen Fall lässt sich möglicherweise argumentieren, dass es an der von § 2 Abs. 10 S. 1 Nr. 2 BSIG gebotenen Erheblichkeit der drohenden Versorgungsengpässe oder Gefährdungen fehlen würde. Gegen eine solche Argumentation spricht jedoch, dass die Erheblichkeit im Sinne von § 2 Abs. 10 Nr. 2 BSIG abschließend durch die in der BSI-KritisV erfolgende Festsetzung der Schwellenwerte geregelt ist.[51] Außerdem würde durch das Abstellen auf das konkret drohende Schadenspotenzial einiges an Rechtssicherheit eingebüßt werden, was mit der ausschließlichen Maßgeblichkeit des Versorgungsgrads einhergeht.

Zusammengefasst sind Digitale Zwillinge realer, kritischer Systeme mithin regelmäßig dann als notwendig für die Erbringung kritischer Dienstleistungen einzustufen, wenn sie (zumindest auch) die Beeinflussung des realen Systems ermöglichen. Ihr Einsatz (lediglich) zu Entwicklungs- und

50 Etwa Anhang 1 Teil 1 Nr. 2.7 iVm Teil 3 Nr. 3.1.3.

51 In diese Richtung wohl *Ritter* (Fn. 38), BSIG § 2 Rn. 31.

Analysezwecken ist demgegenüber als nicht notwendig zur Erbringung kritischer Dienstleistungen zu bewerten. Schwieriger ist die Beurteilung des Einsatzes zu Überwachungszwecken, wenngleich auch hier die besseren Argumente gegen die Bejahung des Notwendigkeitskriteriums sprechen.

Kommt man zu dem Schluss, dass der Digitale Zwilling eine Anlage i. S. d. § 1 Abs. 1 Nr. 1 BSI-KritisV darstellt, muss er jedoch auch einer in den Anhängen der BSI-KritisV festgelegten Anlagenkategorie zugeordnet werden können. Auch diese Frage kann nur im konkreten Einzelfall und in Abhängigkeit von der Funktions- und Verwendungsweise des Digitalen Zwillings beurteilt werden. Um an das oben genannte Beispiel im Energiesektor anzuknüpfen, wäre aber beispielsweise die Einstufung eines Digitalen Zwillings als eigenständige Anlage im Sinne von § 2 Abs. 10 S. 1 Var. 2 BSIG i.V.m. § 2 Abs. 6 BSI-KritisV[52] denkbar, wenn der Digitale Zwilling gemäß dem Anhang 1 der BSI-KritisV eine Anlage bzw. ein System zur Überwachung und/oder Steuerung und damit eine eigene Anlagenkategorie darstellt. Dies trifft etwa auf Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung zu (Anhang 1 Teil 1 Nr. 2.2, Teil 3 Nr. 1.1.2 BSI-KritisV).

Lässt sich der Digitale Zwilling hingegen keiner der in den Anhängen der BSI-KritisV festgelegten Anlagenkategorien zuordnen, führt dies jedoch nicht zwangsläufig dazu, dass er nicht zu KRITIS zählt. Vielmehr kann er auch als Teil einer Anlage KRITIS i. S. v. § 2 Abs. 10 BSIG sein („*oder Teile davon*"). Insoweit erfolgt unter Umständen die Zurechnung des Digitalen Zwillings zu einer (übergeordneten) Anlage, also dem realen System, nach § 1 Abs. 2 S. 1 Hs. 1 BSI-KritisV. Anlagenteile sind insoweit selbstständig beurteilbare und abgrenzbare Teile einer Anlage, die auch für sich genommen Anlagen nach § 1 Abs. 1 Nr. 1 BSI-KritisV darstellen können, aber für den Betrieb in einer übergeordneten Anlage vorgesehen bzw. eingebunden sind.[53] Zwingende Voraussetzung ist jedoch auch hier, dass der Digitale Zwilling für den Betrieb der (übergeordneten) Anlage und damit zumindest mittelbar auch zur Erbringung der kritischen Dienstleistung notwendig ist.

Ein konkretes Beispiel für die Einordnung als Anlagenteil wäre, wenn der Digitale Zwilling der Überwachung eines Stromübertragungsnetzes dient. So fällt das Stromübertragungsnetz zwar in eine der Anlagekategorien (Anhang 1 Teil 1 Nr. 2.3, Teil 3 Nr. 1.2.1 BSI-KritisV). Eine Anlagenkategorie

52 In den anderen Sektoren richtet sich die Qualifizierung als Anlage nach § 3 Abs. 4, § 4 Abs. 3, § 5 Abs. 4, § 6 Abs. 4, § 7 Abs. 7, § 8 Abs. 3 BSI-KritisV.

53 So auch *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 14.

für ein System zur Überwachung des Stromübertragungsnetzes sieht die BSI-KritisV jedoch nicht vor. In diesem Fall würde der Digitale Zwilling als betriebsnotwendiges Teil des Stromübertragungsnetzes diesem über § 1 Abs. 2 S. 1 BSI-KritisV zugerechnet und damit als Anlagenteil selbst zu KRITIS.

c) Erreichen des Schwellenwertes

Ist der Digitale Zwilling einer Anlagenkategorie zuzurechnen, muss er des Weiteren die in der BSI-KritisV festgelegten Schwellenwerte erreichen. Sofern der Digitale Zwilling einer übergeordneten Anlage als Anlagenteil zuzurechnen, ist, muss hingegen die Anlage den Schwellenwert erreichen.

Schwellenwerte sind nach § 1 Abs. 1 Nr. 5 BSI-KritisV Werte, bei deren Erreichen oder Überschreiten der Versorgungsgrad einer Anlage oder Teilen davon als bedeutend im Sinne von § 10 Abs. 1 S. 1 BSIG anzusehen ist. Die BSI-KritisV enthält tabellarische Anlagen, die verbindliche Schwellenwerte festlegen, die sich an den in den sektorspezifischen Normen weiter unterteilten Dienstleistungen orientieren. Die genaue Berechnung der Schwellenwerte wird im jeweiligen Teil 2 der Anlage zur BSI-KritisV näher festgelegt, wo für einen bedeutenden Versorgungsgrad von einem Regelschwellenwert von 500.000 zu versorgenden Personen ausgegangen wird.

Bei der Berechnung der Schwellenwerte ist zu beachten, dass die Schwellenwerte der BSI-KritisV jeweils pro Anlage gelten. Es gilt der strikte Anlagenbezug.[54] Insoweit ist nicht auf ein Unternehmen oder einen Betrieb in seiner Gesamtheit abzustellen. Vielmehr kommt es auf die Anlage im Einzelnen an. Das heißt, wenn keine Anlage für sich genommen den Schwellenwert überschreitet, liegt auch keine KRITIS vor.

Eine Ausnahme hiervon bildet allerdings die sogenannte "gemeinsame Anlage". Dabei handelt es sich um mehrere Anlagen derselben Kategorie, die durch einen betriebstechnischen Zusammenhang verbunden sind. Sie gelten als gemeinsame Anlage, wenn sie gemeinsam zur Erbringung derselben kritischen Dienstleistung notwendig sind (§ 1 Abs. 2 S. 2 KritisV). In

54 Vgl. Bundesamt für Sicherheit in der Informationstechnik, Fragen und Antworten zur BSI-Kritisverordnung, abrufbar unter: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-FAQ/FAQ-BSI-KritisV/faq_kritisv_node.html.

diesem Fall werden die Versorgungsleistungen zur Berechnung der Schwellenwerte addiert.

2. Betreibereigenschaft

Ist der Digitale Zwilling als KRITIS einzuordnen, ist weiter festzustellen, wer als dessen Betreiber gilt und damit Adressat des gesetzlichen Pflichtenprogramms ist. In Betracht kommen sowohl der Nutzer, also der Betreiber des zugrundeliegenden realen Systems als auch der externe IT-Dienstleister, welcher häufig zur Bereitstellung der Software des Digitalen Zwillings und der erforderlichen Rechenkapazitäten hinzugezogen wird.

a) Definition und Begriffsmerkmale

Das BSIG selbst enthält keine Legaldefinition des Betreibers. Er wird jedoch in § 1 Abs. 1 Nr. 2 BSI-KritisV definiert als eine natürliche oder juristische Person, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb einer Anlage oder Teilen davon ausübt.[55] Zur Bestimmung der Betreibereigenschaft ist demnach maßgeblich darauf abzustellen, wer die Verfügungsgewalt in eigener Verantwortung, also die tatsächliche Sachherrschaft über die Anlage oder Teile davon, ausübt.[56]

Damit weist die Betreibereigenschaft auf den ersten Blick eine gewisse Nähe zum zivilrechtlichen Besitz- und strafrechtlichen Gewahrsamsbegriff auf.[57] Ähnlich wie bei der Legaldefinition zum Anlagenbegriff in § 1 Abs. 1 Nr. 1 BSI-KritisV ist dem Betreiberbegriff jedoch ein immissionsschutzrechtliches Verständnis zugrunde zu legen.[58] Insoweit sind die für den immissionsschutzrechtlichen Betreiberbegriff entwickelten Grundsätze

55 Eine Ausnahme hiervon sieht die BSI-KritisV nur für den Sektor Finanzen vor: Nach § 7 Abs. 8 BSI-KritisV hat derjenige bestimmenden Einfluss auf eine Anlage, der die tatsächliche Sachherrschaft ausübt, unabhängig von den rechtlichen und wirtschaftlichen Umständen. Hieraus folgt, dass teilweise auch die Outsourcing-Unternehmen von Finanzunternehmen als Betreiber Kritischer Infrastruktur eingestuft werden können, vgl. *Ritter* (Fn. 38), BSI-KritisV § 7 Rn. 19.

56 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 29; *M. Fischer* in G. Hornung/M. Schallbruch (Hrsg), IT-Sicherheitsrecht, 2. Aufl., Baden-Baden 2024, Teil 2 § 13 Rn. 51.

57 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 29.

58 Vgl. Bundesministerium des Innern, Begründung zur BSI-KritisV, S. 6.

anzuwenden.[59] In Übereinstimmung mit der immissionsschutzrechtlichen Rechtsprechung[60] heißt es in der Verordnungsbegründung, Betreiber sei, „wer weisungsfrei und selbstständig über die Anlage oder Teile davon verfügen kann."[61]

Zunächst ist also zu prüfen, wer den bestimmenden Einfluss auf die Beschaffenheit und den Betrieb einer Anlage oder Teilen davon ausübt. Unter „Betrieb" ist in diesem Zusammenhang die Aufrechterhaltung der organisatorisch-technischen Funktionsfähigkeit zu verstehen.[62] Einfluss auf die Beschaffenheit der Anlage hat hingegen, wer auf die zur Anlage gehörenden betriebsnotwendigen Gegenstände physisch einwirken kann.[63] Bei dieser Prüfung sind sodann die rechtlichen, wirtschaftlichen und tatsächlichen Umstände im Rahmen der Gesamtbetrachtung zu berücksichtigen. Das Erfordernis der rechtlichen und tatsächlichen Verfügungsmacht beruht auf dem Gedanken, dass derjenige verpflichtet werden soll, der im Bedarfsfall am effektivsten die erforderlichen Maßnahmen ergreifen kann.[64] Wirtschaftliche Umstände sind deshalb zu berücksichtigen, um zumindest eine weitgehende Synchronität zwischen den wirtschaftlichen Nutzungen der Anlage bzw. dem wirtschaftlichen Risiko und den mit der Erfüllung des gesetzlichen Pflichtenprogramms verbundenen Kosten herzustellen.[65] Den wirtschaftlichen Umständen wird jedoch teils nur eine untergeordnete Bedeutung zugemessen.[66] Zur Beurteilung der rechtlichen Umstände, aus denen sich ein bestimmender Einfluss auf die Beschaffenheit oder den

59 *Fischer* (Fn. 56), Teil 2 § 13 Rn. 52.

60 Die immissionsschutzrechtliche Rechtsprechung verwendet diese Formulierung gleichwohl nicht als Definition, sondern versteht die Weisungsunabhängigkeit und Selbstständigkeit als starkes Indiz, vgl. OVG Münster NVwZ-RR 2009, 462 (463); OVG Lüneburg NVwZ 2009, 991 (992); der Sache nach auch VGH Mannheim NVwZ 1988, 562 (563).

61 Vgl. Bundesministerium des Innern, Begründung zur BSI-KritisV, S. 6.

62 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 32.

63 Auf die physische Einwirkungsmöglichkeit abstellend auch *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 32, jedoch ohne auf die Betriebsnotwendigkeit der Gegenstände einzugehen.

64 Vgl. zum Immissionsschutzrecht VGH Mannheim NVwZ 1988, 562 (563); auf den Effektivitätsgedanken verweisend auch *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 30; *S. Silberg* in M. Dreher (Hrsg.), Versicherungsaufsichtsgesetz, 14. Auflage 2024, BSI-KritisV § 7, Rn. 24.

65 Vgl. zum Immissionsschutzrecht VGH Mannheim NVwZ 1988, 562 (563); OVG Münster NVwZ-RR 2009, 462 (463).

66 Zum Immissionsschutzrecht *T. Schmidt-Kötters* in: L. Giesberts/M. Reinhardt (Hrsg.), BeckOK Umweltrecht, 71. Ed., Stand 01.01.2024, BImSchG § 4 Rn. 115.

Betrieb einer Anlage ergeben kann, ist die Weisungsfreiheit des potenziellen Betreibers maßgeblich.[67] Betreibereigenschaft und Eigentümerstellung können auseinanderfallen.[68] Maßgeblich ist vielmehr die rechtliche Inhaberschaft der Verfügungsgewalt, die der Eigentümer auf Dritte übertragen kann.[69] Mit den „tatsächlichen Umständen" wiederum verweist der Verordnungsgeber auf die tatsächliche Sachherrschaft bzw. Funktionsherrschaft.[70] Die Bewertung der „wirtschaftlichen Umstände" orientiert sich hingegen daran, wer das wirtschaftliche Risiko trägt und wer berechtigt ist, aus der Anlage wirtschaftlichen Nutzen zu ziehen.[71]

Schwierigkeiten kann der Betreiberbegriff somit bereiten, wenn zwei oder mehr Personen Einfluss auf Betrieb und Beschaffenheit der Anlagen oder ihrer Teile haben. Für diese Fälle sieht § 1 Abs. 2 S. 3 BSI-KritisV die Möglichkeit der gemeinsamen Betreiber vor. Betreiben zwei oder mehr Personen gemeinsam eine Anlage, so ist danach – ähnlich wie bei einer gesamtschuldnerischen Haftung – jeder für die Erfüllung der Betreiberpflichten verantwortlich.[72] Zwar können sie untereinander eine Aufteilung der Pflichten vertraglich vereinbaren,[73] sie sind aber im Außenverhältnis gegenüber dem BSI gemeinsam verantwortlich.[74] Hierdurch will der Verordnungsgeber insbesondere verhindern, dass sich ein Betreiber seiner Betreibereigenschaft entledigt, indem er das operative Tagesgeschäft auf einen Dritten überträgt.[75]

Die Abgrenzung vom Betreiber zu gemeinsamen Betreiber ist jedoch mitunter schwierig.[76] Dies gilt insbesondere dann, wenn sich ein Betreiber beim Betrieb der Anlage oder der hierfür erforderlichen informationstech-

67 Vgl. *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 30.
68 Vgl. Bundesministerium des Innern, Begründung zur BSI-KritisV, S. 6.
69 Wohl auch Bundesministerium des Innern, Begründung zur BSI-KritisV, S. 6; *K. Beucher, T. Ehlen, J. Utzerath* in: D. Kipker (Hrsg.), Cybersecurity, 2. Aufl., München 2023, Kap. 14 Rn. 53.
70 Vgl. Bundesministerium des Innern, Begründung zur BSI-KritisV, S. 6; *Beucher/Ehlen/Utzerath* (Fn. 69), Kap. 14 Rn. 53.
71 *Beucher/Ehlen/Utzerath* (Fn. 69), Kap. 14 Rn. 53; zum Immissionsschutzrecht etwa OVG Münster NVwZ-RR 2009, 462 (463).
72 Bundesministerium des Innern, Begründung zur 2. ÄnderungsVO der BSI-KritisV, S. 41.
73 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 22.
74 Bundesministerium des Innern, Begründung zur 2. ÄnderungsVO der BSI-KritisV, S. 41.
75 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 33.
76 Die Herausarbeitung konkreter Abgrenzungskriterien würde den Rahmen dieser Untersuchung sprengen und bleibt daher einer eigenen Untersuchung vorbehalten.

nischen Systeme eines Dritten bedient (sogenanntes *Outsourcing*). Von einer gemeinsamen Betreibereigenschaft ist in solchen Fällen jedenfalls dann auszugehen, wenn das Outsourcing relevante Anlagenteile betrifft.[77] Das Outsourcing lediglich untergeordneter Tätigkeiten bleibt hingegen außer Acht.[78] Der Unterauftragnehmer ist in diesen Fällen meist weisungsabhängig vom Auftraggeber, sodass der bestimmende Einfluss über die KRITIS-Anlage beim Betreiber verbleibt.[79]

b) Anwendung des Beurteilungsmaßstabs auf Digitale Zwillinge

Im Hinblick auf die Frage, wer als Betreiber des Digitalen Zwillings einzustufen ist, kommt es nach dem Vorstehenden darauf an, wer unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb des Digitalen Zwillings ausübt. Weil die Zuordnung der Betreibereigenschaft, wie gesehen, stets nur unter Berücksichtigung der konkreten Umstände des Einzelfalls möglich ist,[80] können auch hier nur allgemeine, auf typisierte und praktisch besonders bedeutsame Fallkonstellationen bezogene Einschätzungen getroffen werden.

Bevor entschieden werden kann, ob der Nutzer und/oder der Provider des Digitalen Zwillings auf dessen Betrieb und Beschaffenheit bestimmenden Einfluss ausüben kann, muss zunächst bestimmt werden, was als Betrieb des Digitalen Zwillings sowie unter dessen Beschaffenheit zu verstehen ist. Hinsichtlich des Betriebsbegriffs bestehen keine Besonderheiten; maßgeblich ist die Funktionsfähigkeit des Digitalen Zwillings. Hinsichtlich der Beschaffenheit des Digitalen Zwillings ist zu beachten, dass der Digitale Zwilling im hier zugrunde gelegten Sinne nicht lediglich die virtuelle, gar grafisch dargestellte Replikation des realen Systems umfasst. Vielmehr besteht der Digitale Zwilling aus einer Software, die diese Replikation ermöglicht, aber wiederum auf einer Hardware operiert und über eine Schnittstelle mit dem realen, abgebildeten System verbunden ist. Eine phy-

77 Bundesministerium des Innern, Begründung zur 2. ÄnderungsVO der BSI-KritisV, S. 41.

78 Bundesministerium des Innern, Begründung zur 2. ÄnderungsVO der BSI-KritisV, S. 41, als Beispiel nennt der Verordnungsgeber das „Gebäudemanagement".

79 *Fischer* (Fn. 56), Teil 2 § 13 Rn. 52; *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 33.

80 Vgl. zum Immissionsschutzrecht VGH Mannheim NVwZ 1988, 562 (563); *Schmidt-Kötters* (Fn. 66), BImSchG § 4 Rn. 115.

sische Einwirkung kann somit nicht nur an der physischen, am oder im realen System befindlichen Schnittstelle erfolgen, sondern auch an der korrespondierenden Hardware.

In tatsächlicher Hinsicht können regelmäßig sowohl Nutzer als auch Provider Einfluss auf den Digitalen Zwilling nehmen. Der Nutzer dürfte regelmäßig auf die Schnittstelle und damit in Teilen auf die Beschaffenheit des Digitalen Zwillings physisch einwirken können. Aufgrund der essenziellen Bedeutung der Schnittstelle für die Funktionsfähigkeit des Digitalen Zwillings besteht somit auch eine Einflussmöglichkeit hinsichtlich des Betriebs des Digitalen Zwillings. Der Provider wiederum dürfte regelmäßig auf die Software sowie die korrespondierende Cloudstruktur (Hardware) Einfluss nehmen können, sei es im Wege einer Abschaltung, der Durchführung von Updates oder einer Anpassung im Rahmen des Kundenservice gegenüber dem Nutzer. Insoweit besteht regelmäßig auch seitens des Providers eine Einflussnahme auf den Betrieb und die Beschaffenheit des Digitalen Zwillings.

In rechtlicher Hinsicht ist zu beachten, dass es regelmäßig allein vom Nutzer abhängt, ob er die Dienstleistung des Providers betreffend die Bereitstellung der Komponenten des Digitalen Zwillings annimmt oder nicht. Somit wird er regelmäßig auch zur Entfernung der Schnittstelle berechtigt sein, weshalb ihm in der Regel auch rechtlich eine Einflussmöglichkeit auf den Betrieb und die Beschaffenheit des Digitalen Zwillings zusteht. Die Vertragsbeziehung zwischen Nutzer und Provider wird es demgegenüber dem Provider realistischerweise nicht erlauben, die Software oder Hardware des Digitalen Zwillings nach Gutdünken zu beeinflussen. Regelmäßig wird er allenfalls berechtigt und verpflichtet sein, Updates und ggf. auf individuellen Wunsch des Nutzers Anpassungen vorzunehmen. Insoweit ist eher von dem Fehlen der Selbstständigkeit und Weisungsunabhängigkeit des Providers auszugehen.

Das wirtschaftliche Risiko des Einsatzes des Digitalen Zwillings im konkreten Fall trägt der Nutzer. Dem mit dem Digitalen Zwilling verbundenen potenziellen Nutzen (etwa in Gestalt von Effizienzsteigerungen) stehen die mit ihm einhergehenden Kosten gegenüber (etwa Lizenz- und Betriebsgebühren). Demzufolge dürften die wirtschaftlichen Umstände regelmäßig gegen den bestimmenden Einfluss des Providers sprechen. Denn ob sich der Einsatz des Digitalen Zwillings im Kontext der Erbringung der kritischen Dienstleistung lohnt, liegt außerhalb seiner Risikosphäre.

In Anbetracht dieser Erwägungen ist zusammengefasst regelmäßig der Nutzer des Digitalen Zwillings als dessen Betreiber einzustufen. Er übt

unter Berücksichtigung tatsächlicher, rechtlicher und wirtschaftlicher Umstände bestimmenden Einfluss auf den Betrieb und die Beschaffenheit des Digitalen Zwillings aus. Ob hingegen der Provider eines Digitalen Zwillings mit dem Nutzer als gemeinsamer (§ 1 Abs. 2 S. 3 BSI-KritisV) oder gar alleiniger Betreiber des Digitalen Zwillings anzusehen ist, kann keinesfalls pauschal beantwortet werden. Große Bedeutung kommt auch hier der konkreten technischen Ausgestaltung des Digitalen Zwillings sowie den Details des Vertragsverhältnisses zwischen dem Nutzer und dem Provider zu.

II. Digitale Zwillinge als Digitale Dienste i. S. d. § 2 Abs. 11 BSIG

Sind in den Betrieb des Digitalen Zwillings externe IT-Dienstleister eingebunden – wovon regelmäßig auszugehen ist – fallen diese potenziell in die Kategorie als Anbieter eines digitalen Dienstes in den Anwendungsbereich des BSIG. Dies ist unabhängig von einer potenziellen Einstufung als KRITIS-Betreiber, beide Rechtsregime sind parallel anwendbar.[81]

1. Digitaler Dienst

§ 2 Abs. 11 BSIG unterscheidet zwischen drei verschiedenen Arten von digitalen Diensten: Erfasst sind Online-Marktplätze (Nr. 1), Online-Suchmaschinen (Nr. 2) und Cloud-Computing-Dienste (Nr. 3). Im Fall Digitaler Zwillinge kommt insbesondere letztere Variante in Betracht, da davon auszugehen ist, dass Digitale Zwillinge aufgrund des erforderlichen Rechenaufwands überwiegend in der Cloud betrieben werden.

Cloud-Computing-Dienste werden definiert als alle in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachten Dienstleistungen[82], die den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen und nicht zum Schutz grundlegender staatlicher Funktionen eingerichtet worden sind oder für diese genutzt werden. Dazu zählt die cloudgestützte Bereitstellung von Infrastruktur (Infrastructure as a Service

81 *Ritter* (Fn. 38), BSIG § 2 Rn. 36.

82 Dieser Definitionsbestandteil ergibt sich aus dem Verweis auf Art. 1 Abs. 1 lit. b RL (EU) 2015/1535.

– IaaS), von Plattformen (Platform as a Service – PaaS) sowie von Software (Software as a Service – SaaS).[83]

In Bezug auf Digitale Zwillinge kommt nicht etwa nur SaaS in Betracht, also etwa wenn der Nutzer beim IT-Provider die Software einkauft. Denkbar sind auch IaaS, wenn der Nutzer auch Entwickler des Digitalen Zwillings ist und lediglich auf externe Rechenressourcen zurückgreift, oder PaaS, wenn für die Entwicklung eine technische Umgebung erforderlich ist. Entscheidende Bedeutung kommt auch hier den vielgestaltigen konkreten Umständen der technischen Ausgestaltung des Digitalen Zwillings zu, die nur eine Einzelfallbewertung zulassen.

2. Anbietereigenschaft

Regelungsadressaten der IT-Sicherheitspflichten sind juristische Personen, die den digitalen Dienst anbieten (§ 2 Abs. 12 BSIG). Anders als bei KRITIS nimmt das BSIG somit nur juristische Personen in die Pflicht, nicht aber natürliche Personen.

III. IT-Sicherheitspflichten

Für Betreiber von KRITIS sieht das BSIG die strengsten IT-Sicherheitspflichten vor.[84] Diese Pflichten beinhalten insbesondere:

- angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme sicherzustellen, wobei der Stand der Technik eingehalten werden soll (§ 8a Abs. 1 BSIG);
- Systeme zur Angriffserkennung einzusetzen, die durch eine laufende Überwachung des Betriebs eine automatische Protokollierung und De-

83 EU-Kommission, Communication from the Commission to the European Parliament and the Council – Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, 4.10.2017, COM(2017) 476 final/2, Ziff. 4.4.1. Die deutsche Übersetzung spricht statt von „Software as a Service" fälschlicherweise von „Service as a Service"; *Beucher/Ehlen/Utzerath* (Fn. 69), Kap. 14 Rn. 221; *Ritter* (Fn. 38), BSIG § 2 Rn. 35.

84 Das BSIG sieht in § 8d Ausnahmeregelungen u. a. für Kleinstunternehmer und Betreiber öffentlich zugänglicher Telekommunikationsnetze vor. Aufgrund ihrer Bedeutung für den Einzelfall wird hierauf nicht weiter eingegangen.

tektion von sowie Reaktion auf Störungen ermöglichen (§ 8a Abs. 1a BSIG);
- die Einhaltung der IT-Sicherheit gegenüber dem BSI regelmäßig durch Audits nachzuweisen (§ 8a Abs. 3 BSIG);
- gegenüber dem BSI eine rund um die Uhr erreichbare Kontaktstelle zu benennen (§ 8b Abs. 3 BSIG);
- bestimmte Störungen der IT, die Auswirkungen auf die Verfügbarkeit der kritischen Dienstleistung haben oder haben können, dem BSI zu melden (§ 8b Abs. 4 BSIG).

Das an Anbieter digitaler Dienste gerichtete Pflichtenprogramm weist große Parallelen auf. Insbesondere müssen auch hier technische und organisatorische Maßnahmen zur Gewährleistung der IT-Sicherheit ergriffen werden (§ 8c Abs. 1–2 BSIG). Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Bereitstellung eines innerhalb der EU erbrachten digitalen Dienstes haben, sind unverzüglich an das BSI zu melden (§ 8c Abs. 3 BSIG). Erleichterungen sind etwa insofern vorgesehen, als die Einhaltung der in § 8c Abs. 1–2 BSIG festgelegten Sicherheitspflichten nicht regelmäßig, sondern lediglich anlassbezogen und nur nach behördlicher Aufforderung nachzuweisen ist (vgl. § 8c Abs. 4 S. 1 Nr. 1 gegenüber § 8a Abs. 3 BSIG).[85] Außerdem kommt es bei der Bestimmung meldepflichtiger Vorfälle lediglich auf deren tatsächlich eingetretene Auswirkungen an, sodass die Bewertung potenzieller Auswirkungen nicht erforderlich ist.[86]

D. Zusammenfassung und Ausblick

Digitale Zwillinge im *Industrial Metaverse* eröffnen neue Möglichkeiten, reale Produktions- und Fertigungsprozesse in einer virtuellen Umgebung zu entwickeln, zu simulieren und zu optimieren. Für KRITIS bieten sie ein enormes Potenzial zur Steigerung von Sicherheit, Effizienz und Resilienz der IT-Systeme. Als potenzielle Schwachstelle muss aber auch die IT-Sicherheit Digitaler Zwillinge von Anfang an mitgedacht werden. Als virtuelles Abbild, das mit dem realen System in Echtzeit verbunden ist, kann er unter bestimmten Umständen selbst zu KRITIS oder seine Bereitstellung

85 *Beucher/Ehlen/Utzerath* (Fn. 69), Kap. 14 Rn. 233.
86 *A. Bussche/T. Schelinski*, in: A. Leupold/A. Wiebe/S. Glossner (Hrsg.), IT-Recht, 4. Aufl. München 2021, Teil 7.1 Rn. 44.

zu einem Digitalen Dienst werden und IT-sicherheitsrechtlichen Vorgaben unterliegen.

Abschließend ist darauf hinzuweisen, dass sich das IT-Sicherheitsrecht in Europa in einer großen Umbruchphase befindet. So ist mit Blick auf die Umsetzung der NIS2-Richtlinie nicht auszuschließen, dass künftig auch solche Digitalen Zwillinge den Vorgaben des BSIG unterliegen, die zum jetzigen Zeitpunkt nicht reguliert sind.

Möglichkeiten und Grenzen des Strafrechts als Grundrechtsschutz im virtuellen Raum

Jennifer Grafe

A. Hinführung

Die Geschichte von Sherlock Holmes nicht nur erleben, sondern dabei sein – die Fälle selbst lösen, während man mitten im Geschehen ist und nicht nur das Buch in den Händen hält oder den Fernseher ansieht. Sogar Einfluss auf die Geschichte nehmen können, während sie passiert, und am Ende Prof. James Moriarty (dem Gegner von Holmes) schlagen. Doch was passiert, wenn sich diese Simulation nicht beenden lässt? Wenn die Künstliche Intelligenz (KI), die Prof. Moriarty verkörpert, die Mitspieler:innen gefangen hält und vortäuscht, das Spiel sei längst beendet?

Dann befindet man sich nicht nur auf dem Holodeck in Sternzeit 42286.3 und in der 1988 veröffentlichten dritten Folge der zweiten Staffel der beliebten Science-Fiction Serie „Star Trek: The Next Generation",[1] sondern in einem Szenario, das heute immer greifbarer wird. Im Star-Trek-Universum sind Holodecks Räume, die Simulationen und virtuelle Welten mittels holografischer Projektion erzeugen; sie sind eingehüllt von einem Netz aus Holoemittern, die das Erzeugen von holografischen Personen oder Objekten erlauben. Außerhalb des abgedeckten Bereichs können diese Entitäten (die Künstliche Intelligenz [KI] sind) nicht existieren und verschwinden. Sie werden genutzt, um Szenarien aus Spielen, Filmen, Büchern (wie hier Sherlock Holmes) oder der Realität nachzubilden. „Holodecks" haben Serien aber längst verlassen und werden heute bereits in Bayern in Ermittlungsverfahren verwendet, um Tatabläufe realitätsnah nachzustellen;[2] Unternehmen arbeiten daran, die beliebten Escape-Rooms auch virtu-

1 Für die ausführlichen Vorarbeiten den Star-Trek-Bezug betreffend gilt mein Dank Dr. Christian Soll.

2 https://www.stmi.bayern.de/med/aktuell/archiv/2023/230605holodeck/ (zuletzt abgerufen am 12. 9.2024).

ell anbieten zu können.[3] Unbeschadet der Tatsache, dass diese „Holodecks" von ihrem filmischen Vorbild technisch noch entfernt sind, lässt es sich im Angesicht der Wahl der ersten „Miss AI"[4] kaum leugnen, dass KI auch im Alltag immer präsenter wird und die von dem Konzern Meta vorgestellte Vision eines Metaversums[5] in näherer Zukunft liegen dürfte, als man es sich noch vor einigen Jahren vorstellte.

Zeitgleich versucht der Gesetzgeber seit einigen Jahren, seiner grundrechtlichen Verpflichtung zum Schutz etwa der Meinungsfreiheit und vor Diskriminierung im digitalen Zeitalter dadurch zu begegnen, dass er Strafgesetze schafft, die Straftaten im virtuellen Raum einfangen sollen. Schlagworte wie „Hate Speech", „Deepfakes" und „Cybercrime" beherrschen die einschlägigen strafrechtlichen und kriminologischen Zeitschriften. Debatten etwa um Strafbarkeiten im Umfeld des von der virtuellen Welt stattfindenden E-Sports sind nicht neu.[6] §§ 202a bis 202c StGB (Ausspähen und Abfangen von Daten), § 303b StGB (Computersabotage), § 192a StGB (Verhetzende Beleidigung als Reaktion auf „Hate Speech") und die jüngste Überarbeitung des § 11 Abs. 3 StGB[7] sind nur einige solcher Beispiele, die eine Reaktion des Strafrechts auf digitale Herausforderungen abbilden. Die Regulierung des 2013 von der damaligen Bundeskanzlerin Angela Merkel als „Neuland" bezeichneten Internets[8] ist dabei an vielen Stellen gescheitert – sowohl auf nationaler als auch auf europäischer Ebene wurden Maßnahmen immer wieder dafür kritisiert, nicht zielführend oder realitätsfremd zu sein. Man darf mit *R. Hoheisel-Gruler* durchaus die Annahme wagen, dass die über Jahre hinweg vorgetragene gebetsmühlenhafte Wiederholung der Feststellung, wonach das Internet kein rechtsfreier Raum sei, nicht viel eher als ein Beleg das Gegenteils herhalten könne.[9]

Rechtzeitig bedarf es daher einen (strafrechtlichen) Blick auf Utopie und Dystopie virtueller Welten, in Bezug auf die zu erwartenden Herausforderungen und möglichen Lösungen. Der Beitrag möchte aufzeigen, in welcher Hinsicht strafrechtliche Handlungen in virtuellen Realitäten und

3 Vgl. etwa die Arbeit von ERM LABS, https://www.ermlabs.io (zuletzt abgerufen am 13.10.2024).
4 *L. Ludwig*, »Miss AI« ist der öde Höhepunkt des Schönheitswahns, in: Spiegel Online vom 11.7.2024.
5 https://about.meta.com/de/what-is-the-metaverse/ (zuletzt abgerufen am 12.9.2024).
6 *C. Soll*, Die Strafbarkeit von Wettbewerbsmanipulationen im E-Sport unter besonderer Berücksichtigung des Sportwettbetrugs nach § 265c StGB, München, 2022.
7 BGBl I, S. 2600.
8 *V. Kämper*, Die Kanzlerin entdeckt #Neuland, in: Spiegel Online vom 19.6.2013.
9 *R. Hoheisel-Gruler*, Der entgrenzte digitale Raum, Kriminalistik 2022, 616 (619).

beim Einsatz von KI vorkommen können und wie sich diese mit der realen Welt verzahnen. Sodann will er die Herausforderungen benennen, vor denen diese tatsächlichen Entwicklungen das Strafrecht stellen und wie ein Strafrecht, wie wir es heute kennen, mit bekannten Konstruktionen darauf reagieren kann und wo es an seine Grenzen stößt, es geradezu naiv sein mag, sich auf das althergebrachte System zu stützen.

B. Grundsatzfragen

I. Virtuelle Realitäten und KI – Was ist das eigentlich?

Virtuelle Realitäten, Metaverse – konturscharf sind diese Begriffe nicht und mithin auch nur teilweise geeignet, grundsätzliche rechtliche Fragestellungen zu klären. Denn virtuelle Realitäten sind zunächst einmal die Verlagerung menschlichen Handelns und menschlicher Kommunikation in eine „virtuelle", das heißt computergenerierte, Welt. Spätestens seitdem der Konzern Meta die Vision eines „Metaverse" vorgestellt hat,[10] haben sie eine gewisse Deutungshoheit über die Zukunft virtueller Welten für sich beansprucht und die Assoziation mit dieser konkreten Art virtueller Realität liegt nahe. Das Metaverse ist ein Konzept für eine umfassende, digitale Realität, die durch die Kombination von virtuellen Welten, Augmented Reality (AR), und verschiedenen digitalen Interaktionen entsteht. Es beschreibt eine fortlaufende, geteilte virtuelle Umgebung, in der Nutzer:innen durch Avatare miteinander kommunizieren, arbeiten, spielen und soziale Interaktionen haben können. Aber auch frühere Formen etwa von Computerspielen unterfallen der virtuellen Realität – daneben treten Ideen im Bereich des Tourismus, des Sports, der Medizin, der Ausbildung und Lehre und nicht zuletzt auch Gerichtsverhandlungen in virtuellen Räumen. Als Ursprung des Begriffs „Metaverse" findet man häufig Hinweise auf den Roman „Snow Crash" des Autors *Neal Stephenson* aus dem Jahre 1992: Ein zentrales Konzept des Romans ist das „Metaverse" – eine riesige, von Nutzer:innen gestaltbare virtuelle Realität, die immersive Interaktionen, eine eigene Wirtschaft und gefährliche Elemente wie den Snow Crash-Virus umfasst. Dieses Konzept dürfte aber, wie auch *E. Hilgendorf* überzeugend darstellt, nicht der Ausgangspunkt virtueller Realitäten gewesen sein, die

10 https://about.meta.com/de/what-is-the-metaverse/ (zuletzt abgerufen am 12.9.2024).

sich literarisch bereits 1928 finden lassen und sich nicht zuletzt durch die Matrix-Filmreihe als eine mögliche Zukunftsperspektive etabliert haben.[11] 2013 war das Computerspiel „Second Life", eine virtuelle Online-Welt, in der Nutzer:innen als Avatare interagieren, eigene Inhalte erstellen, handeln und soziale, kreative oder berufliche Aktivitäten in einer offenen, von den Nutzer:innen gestalteten Umgebung ausüben können, bereits Anlass für eine Betrachtung des Strafrechtsschutzes in virtuellen Welten.[12] Philosophische, historische und literarische Überlegungen zeigen zwar Optionen virtueller Welten auf, es ist der rechtlichen Beschäftigung mit einer Utopie (oder Dystopie) dennoch immanent, dass sie Unwägbarkeiten mit sich bringt, die eine klare Definition kaum möglich machen. Es sind aber Kriterien greifbar, die zumindest eine grobe Skizzierung des Problemfeldes ermöglichen.

Nach *Hilgendorf* zeichnen sich virtuelle Realitäten dadurch aus, dass Nutzer:innen in eine andere, das heißt von der Realität abweichende, aber permanente Welt immersieren, sich die computergenerierte Welt weitestgehend sinnlich wahrnehmen lässt und sich der Körperbewegung der Nutzer:innen anpasst (ggf. ist auch eine Verkörperung in der virtuellen Welt denkbar), eine Interaktion mit der virtuellen Umgebung möglich ist und dabei die reale Welt ganz oder teilweise (sog. „augmented reality" oder „mixed reality") ausgeblendet wird.[13] Diese Arbeitsdefinition genügt für eine strafrechtliche Betrachtung.

Zentral tritt für die hiesige Betrachtung der Aspekt hinzu, dass KI zur Erzeugung oder zum Erhalt der virtuellen Welt eingesetzt wird. Für den Begriff der KI lässt sich die neue KI-Verordnung der Europäischen Union[14] heranziehen, die in Art. 3 Abs. 1 folgende Definition liefert: „Ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können."

11 Ausf. *E. Hilgendorf*, Virtuelle Realitäten, Metaverse, Generative KI und (Straf-)Recht, JZ 2024, 677 (678).

12 *K. Eckstein*, MMORPGS und Metaversen: Strafrechtsschutz in digitalen Welten, JurPC Web-Dok. 58/2013, Abs. 1 – 23.

13 *Hilgendorf*, Metaversen (Fn. 11), 679.

14 Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz, VO (EU) 2024/1689 vom 13.6.2024.

II. (Verfassungs-)Rechtliche Rahmenbedingungen

Der Schutz der Bevölkerung vor den negativen Folgen der KI ergibt sich aus der Schutzpflicht des Staates gegenüber den Bürger:innen, der aus den Funktionen der Grundrechte als Elemente einer objektiven Werteordnung hergeleitet werden kann. In den Grenzen des ultima-ratio-Prinzips hat der Gesetzgeber mit dem Strafrecht dafür Sorge zu tragen, Rechtsgutsverletzungen zu ahnden – das dient letztlich dem Rechtsstaatsprinzip, in dem der:die Bürger:in keine Selbstjustiz vornimmt. Zur Aufrechterhaltung dieses Systems ist es notwendig, die relevanten Lebensbereiche, in denen Rechtsgutsverletzungen zu erwarten sind, auch mit dem Strafrecht zu erfassen, wobei die virtuelle Realität in Zukunft dazu zählen wird. Das staatliche Gewaltmonopol regelt auch die legitime Verfügungsmacht über andere – der Staat kann daher für den virtuellen Raum Geltung beanspruchen, vorausgesetzt, er kann diese Aufgabe auch faktisch wahrnehmen.

Gleichzeitig ergibt sich aus der Schutzpflicht des Staates aber, dass keine Überregulierung in dem Sinne stattfindet, dass helfende Mechanismen in bzw. aus virtuellen Welten (also etwa medizinische Fortschritte) den Bürger:innen vorenthalten werden. Die Anwendung und Entwicklung virtueller Realität ist schließlich grundrechtlich geschützt durch die Wissenschafts- und Forschungsfreiheit (Art. 5 Abs. 3 GG), ggf. durch Art. 12 und 14 GG und durch Art. 2 Abs. 1 GG.[15] Ihrerseits kann die (staatliche) Anwendung virtueller Realität wiederum in Grundrechte eingreifen, etwa beim Einsatz im Rahmen von strafrechtlichen Ermittlungsverfahren, hier ist etwa an psychische Schäden durch Wiedererleben traumatischer Situationen zu denken.

Bei der Anwendung von KI in virtuellen Realitäten ist seit diesem Jahr der sachliche Anwendungsbereich der KI-Verordnung der Europäischen Union eröffnet. Sie verfolgt einen risikobasierten Ansatz und unterscheidet drei Risikoklassen: Unannehmbares Risiko (Art. 5), hohes Risiko (Art. 6) und geringes Risiko (Art. 50), wobei jede Einordnung je nach Anwendungsbereich in der virtuellen Welt denkbar ist. Sogenannte Hochrisikosysteme (etwa beim Einsatz in der Bildung) unterliegen strengen Regulierungen. In Bezug auf nationale Gesetzgebung sind diese Entwicklungen in den Blick zu nehmen und können – wenn auch teilweise nur partiell – die Strafgesetzgebung beeinflussen. Allerdings gehören Normsetzung und

15 Vgl. dazu auch *Hilgendorf*, Metaversen (Fn. 11), 681.

Normdurchsetzung zur Kernaufgabe staatlichen Handelns und können nach Art. 79 Abs. 3 GG nicht auf supranationale Institutionen übertragen werden.[16] Der globale virtuelle Raum, der keine staatlichen Grenzen kennt, schafft Asynchronität zwischen kriminellem Handeln und Möglichkeiten der Strafverfolgung[17] – tatsächlich scheint es aber auch politisch aktuell wenig naheliegend, dass sich eine weltweit einheitliche Regelung und Strafverfolgung für virtuelle Welten finden oder gar umsetzen lassen wird. Insofern ist zu beachten, dass die strafrechtliche Regulation fernab utopischer Überlegungen und im Rahmen geltenden Rechts national stattfinden wird und auch europarechtlichen Regelungen in Bezug auf das Strafrecht enge Grenzen gesetzt sind (vgl. auch Art. 83 AEUV).[18]

C. Strafrechtsrelevante Fallgestaltungen

I. Tatsächliche Herausforderungen

Mit virtuellen Realitäten wird vor allem in Bezug auf das Metaverse eine Freizeitkomponente verbunden, also etwa Tourismus, Sport, zwischenmenschliche Kommunikation, Hobbys, Gaming und andere Freizeitbeschäftigungen. Allerdings finden virtuelle Realität auch Einsatz in der Psychologie und der Medizin, aber auch in der Justiz.

Den wohl ersten bekannt gewordenen Fall einer Straftat im virtuellen Raum hatte 2010 das Amtsgericht Augsburg zu entscheiden.[19] Täter und Opfer kannten sich aus dem Spiel „Metin 2". Metin 2 ist ein MMORPG (massively multiplayer online role-playing game), in dem Spieler:innen in einer Fantasywelt gegen Monster kämpfen, Aufgaben erfüllen und in kriegerischen Auseinandersetzungen zwischen verfeindeten Reichen um Macht und Ehre ringen. Der Täter bot dem Opfer an, für die Spielfigur des Opfers eine höherwertige Ausrüstung zu erspielen, zu diesem Zwecke teile das Opfer dem Täter die Kontodaten für das Spiel mit, der in der Folge aber

16 Eingehend *Hoheisel-Gruler*, Raum (Fn. 9), 622.
17 *Hoheisel-Gruler*, Raum (Fn. 9), 622.
18 Vgl. *Hoheisel-Gruler*, Raum (Fn. 9), 622 und zur Debatte eines europaeinheitlichen Vergewaltigungstatbestands *J. Grafe*, Ein europäisches Sexualstrafrecht, in: M. A. Bange/H. Kirner/M. Bauer (Hrsg.), Europa – Raum des Rechts, Göttingen, 2024, S. 275.
19 Amtsgericht Augsburg, Urt. v. 20.10.2010, 33 Ds 603 Js 120422/09 m. Bespr. *Eckstein*, MMORPGs (Fn. 12).

nicht seinem Versprechen nachkam, sondern ihm bereits erspielte Ausrüstungsgegenstände im Gegenwert von 1000 Euro entzog, um sie sodann in Spielerforen und auf eBay zu verkaufen.[20] Wegen der fehlenden Körperlichkeit kamen Eigentumsdelikte nicht in Betracht. Die durchaus interessante Frage, ob virtuelle Güter zum strafrechtlich geschützten Vermögen gehören, war nicht zu klären, da die Übermittlung der Kontodaten zumindest keine Vermögensminderung darstellte. § 202a StGB setzt die Überwindung einer Zugangssicherung voraus, die durch die – wenn auch täuschungsbedingte – freiwillige Weitergabe der Zugangsdaten nicht gegeben ist.[21] Das Amtsgericht Augsburg bejahte schließlich eine Strafbarkeit wegen Datenveränderung (§ 303a StGB).[22]

Ein Bericht von Europol beschreibt einige Szenarien, in denen virtuelle Realitäten neue Kriminalitätsformen mit sich bringen können.[23] Herstellungen von Deepfakes, Diebstahl von Identitäten und biometrischen Daten werden dabei genauso genannt wie sexuelle Belästigung. Insbesondere Deepfakes stellen schon jetzt ein großes Problem dar, etwa in Bezug auf bekannte Methoden wie den „Enkeltrickbetrug", aber auch im Bereich Pornografie.

Die allermeisten Delikte sind im Kontext virtueller Realität denkbar; Eigentum und Vermögen können in virtuellen Realitäten genauso gegeben sein wie in der realen Welt und es sind Fallkonstellationen denkbar, in der dem realen oder dem virtuellen Vermögen durch eine virtuelle Handlung geschadet wird. Ehrverletzungsdelikte und Formen sexueller Belästigung treten schon jetzt im Internet vermehrt auf und können genauso in virtuellen Welten stattfinden. Nicht selten findet man den Verweis darauf, dass Körperverletzungs- und Tötungsdelikte im virtuellen Raum nicht denkbar seien. Auch Avatare können grundsätzlich getötet werden und darüber hinaus ist es auch nicht auszuschließen, dass ein Handeln in der virtuellen Welt die reale Person in ihrer körperlichen Integrität verletzt, etwa durch psychische Manipulation.

Zusammenfassend bleibt festzuhalten, dass die denkbaren strafrechtlich relevanten Fallkonstellationen unendlich sind und letztlich in der virtuellen Welt ein Spiegelbild der realen Welt erzeugen.

---

20 Amtsgericht Augsburg, Urt. v. 20.10.2010, 33 Ds 603 Js 120422/09.
21 *Eckstein*, MMORPGS (Fn. 12).
22 Amtsgericht Augsburg, Urt. v. 20.10.2010, 33 Ds 603 Js 120422/09.
23 Nicht im Volltext veröffentlicht, Bericht bei *G. Eisenreich*, Länder wollen Rechtsstaat wehrhafter aufstellen lassen, DRiZ 2024, 222.

II. Kategorisierungen

Um sich der Frage annähern zu können, ob und wie das Strafrecht auf die Herausforderungen virtueller Realitäten reagieren kann, bietet es sich an, die neuartigen Fallgestaltungen zu kategorisieren. Im Schrifttum wird dabei teilweise differenziert zwischen Handlungssubjekten (also Nutzer:innen, Betreiber:innen und Produzent:innen des virtuellen Raums), wobei die vorhandenen strafrechtlichen Auseinandersetzungen sich weitestgehend im Handeln der Nutzer:innen erschöpfen und Handlungsobjekten und bei letzterem wiederum danach, ob die Handlung eine Auswirkung auf die reale Welt hat oder nicht, ob sich also die Rechtsgutsverletzung im Tatsächlichen widerspiegelt, oder ob lediglich eine „Rechtsgutsverletzung" (sofern man eine solche überhaupt anerkennen möchte) einer virtuellen Figur oder des virtuellen Raums vorliegt.[24] Eine damit verwobene, eigentlich aber davon abzugrenzende Frage besteht darin, wie das Handeln einer KI (wiederum mit und ohne Auswirkungen im virtuellen Raum) strafrechtlich zu werten ist. Sortiert man letztgenannte Frage in die Kategorie der Handlungsobjekte ein,[25] dann beschränkt man den Untersuchungsgegenstand auf das bestehende Strafrecht, dass einer KI keine Rechtssubjektqualität zukommen lässt, was einer zukunftsgerichteten Fragestellung nicht unbedingt zuträglich sein dürfte. Ein weiterer Ansatz differenziert danach, wie Deliktserfolge in Erscheinung treten. Zu fragen ist danach, ob ein Delikt im Metaverse nicht vorkommen kann (dazu zählen etwa Tötungsdelikte), es im Metaverse in gewohnter Art und Weise daherkommt (etwa Beleidigungsdelikte), es in neuer Gestalt im Metaverse erscheint (etwa sexuelle Belästigung) oder es nur im Metaverse vorkommen kann (etwa Tötung eines Avatars).[26] Nur für die letzten beiden Kategorien bedarf es dann überhaupt neuer Regelungen.

Beide Ansätze lassen sich schließlich dahingehend zusammenführen, dass jene Fallgestaltungen in Bezug auf virtuelle Realitäten im Strafrecht relevant werden, in denen entweder erstens die Umgebung „virtuelle Realität" die Anwendung eines Straftatbestands innerhalb seiner definitorisch

24 *Hilgendorf*, Metaversen (Fn. 11), 684.

25 So *Hilgendorf*, Metaversen (Fn. 11), 684, der die Frage als Unterfall der Objektsperspektive behandelt.

26 *J. Oberlin/S. von Hoyningen-Huene*, Strafrecht im Metaverse: Den Verbrechen der Zukunft auf der Spur, forumpoenale 2024, 116, hier zum insoweit aber vergleichbaren schweizerischen Recht.

vorhandenen Grenzen erweitert, zweitens in denen potenzielles Unrecht geschieht, das vom geltenden Recht nicht erfasst wird (entweder, weil keine Rechtsgutsverletzung in der realen Welt eintritt oder weil die normierten Tathandlungen zu eng für eine Anwendung in der virtuellen Welt gefasst sind) oder drittens, wenn Akteur:innen tätig werden, die nicht von der Rechtssubjektbeschreibung des Strafgesetzbuchs erfasst sind (also insbesondere, wenn KI „handelt"). Die Reihung ist nicht zufällig gewählt, sondern aufsteigend in Bezug auf die Qualität ihrer Anforderungen an die Weiterentwicklung der (Straf-)Rechtswissenschaft. Nicht zu vernachlässigen, hier aber außen vor gelassen, sind jene Handlungen, die sich gegen die Infrastruktureinrichtung des Netzes, der Computersysteme oder Daten richten, weil diese die virtuelle Welt selbst (von außen) angreifen.[27]

D. Herausforderungen an das Strafrecht

Die so herausgearbeiteten drei Fallgruppen stellen das Strafrecht letztlich vor zwei große rechtliche Fragestellungen:

1. Wie kann das bestehende Recht auf neue Fragestellungen, die der virtuelle Raum aufwirft, reagieren?
2. Braucht es neue Strafgesetze oder gar ein eigenes „Digitales Strafgesetzbuch" (DStGB)?

Die erste Frage ist genuin strafrechtswissenschaftlich, die zweite indes eine verfassungsrechtliche, denn ob ein Strafgesetz vor allem im Hinblick auf das ultima ratio Prinzip benötigt wird, ist Ausfluss einer Abwägung der Schutzpflicht des Staates mit den Grundrechtseingriffen durch strafrechtliche Verbote.

I. Die Anwendung geltenden Strafrechts auf virtuelle Realitäten

Die ausgewählten strafrechtlichen Problemstellungen bieten Beispiele dafür, wie sich das bestehende Strafrecht in virtuelle Welten übertragen lässt und inwieweit Anpassungen erforderlich werden könnten.

27 Zu dieser Differenzierung *Hoheisel-Gruler*, Raum (Fn. 9), 622.

1. Tatort

Für die Frage nach der Anwendbarkeit deutschen Strafrechts wird im Schrifttum bisher darauf verwiesen, dass die Überlegungen, die in den vergangenen Jahrzehnten zum Internetstrafrecht angestellt worden sind, übertragbar seien.[28] Auf der Frühjahrskonferenz der Justizminister 2023 wurde dennoch der Bundesjustizminister aufgefordert, der Frage nachzugehen, ob der „Tatort"-Begriff des Strafgesetzbuches angepasst werden muss.[29] Grundsätzlich gilt gem. § 3 StGB, dass das deutsche Strafrecht Anwendung findet, wenn die Tat auf deutschem Territorium begangen wurde. § 9 Abs. 1 StGB wiederum definiert den Ort der Tat als jenen, „an dem der Täter gehandelt hat oder im Falle des Unterlassens hätte handeln müssen oder an dem der zum Tatbestand gehörende Erfolg eingetreten ist oder nach der Vorstellung des Täters eintreten sollte". Für Fälle, in denen sich reales Handeln in der realen Welt niederschlägt, lässt sich diese Definition anwenden. Bei grenzüberschreitenden Taten wird meistens nur eine der vier Optionen des § 9 Abs. 1 StGB zutreffen, was jedoch ausreicht. Es genügt also, wenn die handelnde oder die geschädigte Person sich in Deutschland befindet, und zwar auch dann, wenn die Rechtsgutsverletzung lediglich virtuell eintreten kann. Die Regelung ist mithin für das geltende Strafrecht ausreichend.[30] Sofern das Strafrecht auf jene Fälle erweitert werden sollte, in denen das Handeln einer sich im Ausland befindlichen realen Person ausschließlich eine Rechtsgutsverletzung in der virtuellen Welt herbeiführt – dazu sogleich – stößt der Ort an definitorische Grenzen. Wenn etwa der Avatar einer Person, die sich in Deutschland befindet, getötet oder ein nur in der virtuellen Welt vorhandener wertvoller Gegenstand entwendet wird und vorausgesetzt, dieses Verhalten sei strafbar, dann ist der Erfolg nicht auf „deutschem Territorium" (§ 3 StGB) eingetreten, sondern in der virtuellen Welt; das erfasst § 9 Abs. 1 StGB nicht. Dieses Problem entsteht nicht, wenn man, wie gleich zu erläutern sein wird, stets einen Rückbezug zu realen Personen herstellt. Sollte sich in einer fernen Zukunft die Strafbarkeit des Handelns von KI aufdrängen, so wird man diese räumlich nur erfassen können, wenn man den Standort ihrer Hardware als Handlungsort begreift.

28 *Hilgendorf*, Metaversen (Fn. 11), 686.

29 94. Konferenz der Justizministerinnen und Justizminister, https://www.justiz.nrw.de/JM/jumiko/beschluesse/2023/Fruehjahrskonferenz_2023/TOP-II_2-Strafrechtliche-Bekaempfung-von-Fake-News-im-Wahlkampf.pdf (zuletzt abgerufen am 12.9.2024).

30 *Hilgendorf*, Metaversen (Fn. 11), 686.

2. Ehrverletzungsdelikte

Ehrverletzungsdelikte scheinen auf den ersten Blick grundsätzlich geeignet, Fallgestaltungen im virtuellen Raum genauso zu erfassen. Die virtuelle Welt und der Meinungsaustausch im Internet verändern aber das Schutzgutverständnis von § 185 StGB, weil öffentliche herabwürdigende Äußerungen im Internet für den Betroffenen eine besonders intensive Rechtsgutsverletzung darstellen; weitreichende psychische und physische Folgen sind dokumentiert.[31] Im Rahmen einer Interviewstudie gaben Betroffene an, dass insbesondere sexualbezogene Herabwürdigungen, gruppenbezogene Beleidigungen und das sog. Doxing (Veröffentlichung personenbezogener Daten) besonders belastend seien.[32] Ob sog. Hate Storms tatsächlich dieses Erleben verstecken, darf demgegenüber bezweifelt werden.[33] Die Auslegung von § 185 StGB geht dagegen bisher noch von einem Dualismus zwischen Ehrschutz und Meinungsfreiheit aus. Ein Beschluss des Bundesverfassungsgerichts aus dem Jahre 2020 lässt aber erstmals anklingen, dass die Folgen von digitalem Hass in die Abwägung zwischen beidem einzubeziehen sind.[34] Dieses Beispiel zeigt gut auf, dass auch bestehende Gesetze ohne Gesetzesänderung, aber durch Anpassung der Rechtsprechung auf Veränderungen im digitalen Raum reagieren können.

II. Ein neues Strafrecht für virtuelle Realitäten (?)

1. Neue Tatbestände

Bereits 2021 hat die Justizministerkonferenz Deepfakes in den Blick genommen und vor den Möglichkeiten zur Manipulation von Wahlen und Wahlkämpfen gewarnt.[35] Im aktuellen Wahlkampf in den USA haben sich

31 *C. Richter/D. Geschke/A. Klaßen*, Hass im Internet, ZJJ 2020, 148 (152).

32 *H. Heuser/A. Witting*, Digitaler Hass – eine Interviewstudie mit Adressat:innen und Verfasser:innen, https://www.nomos-elibrary.de/10.5771/9783748930396-37.pdf?download_chapter_pdf=1&page=23 (zuletzt abgerufen am 12.9.2024).

33 Vgl. *M. Oğlakcıoğlu*, „Haters gonna hate... (and lawmakers hopefully gonna make something else)", ZStW 132 (2020), 521 (542 f.).

34 BVerfG NJW 2020, 2622 (2626); ausf. *E. Hoven/A. Wittig*, Das Beleidigungsunrecht im digitalen Zeitalter, NJW 2021, 2397 (2401).

35 Beschluss der 99. Konferenz der Justizministerinnen und Justizminister, https://www.justiz.nrw.de/JM/jumiko/beschluesse/2021/Herbstkonferenz_2021/TOP-II_-2---Cybercrime-Delikte.pdf (zuletzt abgerufen am 12.9.2024).

diese Sorgen befürwortet, als der Präsidentschaftskandidat der Republikaner Donald Trump mit KI manipulierten Bilder von Taylor Swift und ihren Fans verwendete, um sich die Unterstützung der bekannten Sängerin zuzuschreiben, die kurze Zeit später ihre Unterstützung für die Kandidatin der Demokratischen Partei Kamala Harris veröffentlichte.[36] Bayern hat nun für digitale Fälschungen einen § 201b StGB vorgeschlagen, der eine Freiheitsstrafe von bis zu zwei Jahren oder Geldstrafe vorsieht; die „Wahrnehmung berechtigter Interessen" soll ausgenommen sein.[37] Die Kritik richtet sich vor allem gegen die fehlende Notwendigkeit einer Differenzierung zwischen KI- und manuell generierten Manipulation (also gegen die Notwendigkeit eines solchen Tatbestands) und das Fehlen eines bestimmbaren Rechtsguts.[38] Solche und andere Straftatbestände können auch vor dem Hintergrund des ultima-ratio-Prinzips verhältnismäßig sein, auf die Erforderlichkeit und das Rechtsgut ist aber ein besonderes Augenmerk zu legen. In Fällen, in denen das Handeln tatsächliche Rechtsgutsverletzungen in der Realität nach sich zieht, sind solche Regelungen zunächst auch nicht systemfremd. So wäre es etwa denkbar, die im digitalen Raum vor allem zu erwartenden psychischen Schädigungen, etwa durch Konfrontation mit verstörendem Bildmaterial oder durch sexuelle Belästigung im weiteren Sinne, etwa in dem ein Avatar vergewaltigt wird, vom Strafrecht zu erfassen. Sofern man überhaupt einen Schutz durch den bestehenden § 223 StGB annehmen kann, was durchaus zu bezweifeln ist,[39] so greift dieser für jene Fallgestaltungen zu kurz. Es ist auch nicht ausgeschlossen, Tathandlungen im virtuellen Raum unter Strafe zu stellen, die keine Auswirkungen in der Realität zeigen – etwa Schädigung des virtuellen Vermögens oder Schädigung des Avatars. Eingedenk einer zivilrechtlichen Ausgestaltung von Eigentumsverhältnissen in virtuellen Welten wäre auch ein digitaler Hausfriedensbruch denkbar. Denn nach der sog. Inzest-Entscheidung des Bundesverfassungsgerichts, in dem es den weiten Einschätzungsspielraum des Gesetzgebers im Bereich des strafrechtlichen Rechtsgüterschutzes betont, sei zwar das Strafrecht die „ultima ratio" des Rechtsgüterschutzes; es sei aber grundsätzlich Sache des Gesetzgebers, den Bereich strafbaren Han-

36 *M. Hoppenstädt*, Wie sich Donald Trump mit einem KI-Fake selbst schadete, in: Spiegel Online vom 11.9.2024.

37 BR-Drs. 222/24.

38 *Bundesrechtsanwaltskammer*, Stellungnahme Nr. 75/2024.

39 Ausf. *J. Grafe*, Zur Strafbarkeit von Konversionsmaßnahmen unter besonderer Berücksichtigung des Gesetzes zum Schutz vor Konversionsbehandlungen, München, 2022, S. 53 ff.

delns verbindlich festzulegen.[40] Dieser sei bei der Entscheidung, ob er ein bestimmtes Rechtsgut, dessen Schutz ihm wesentlich erscheine, gerade mit den Mitteln des Strafrechts verteidigen und wie er dies gegebenenfalls tun wolle, innerhalb der (weiten) Grenzen des Grundsatzes der Verhältnismäßigkeit frei.[41] Um die Betroffenheit eines Grundrechts festzustellen, bedarf es natürlich stets eines Rückbezugs zu einem realen Individuum. Dieses dürfte aber nahezu immer vorliegen, also immer dann, wenn das sich im virtuellen Raum befindliche Rechtsgut einem dortigen Avatar o. ä. zugeordnet werden kann, der dann wiederum einer realen Person zugeordnet wird. Nur wenn eine solche Zuordnung vorliegt, ist ein verfassungsrechtlich geschütztes Gut in Gefahr, das durch den Gesetzgeber geschützt werden kann. In contrario ist aber auch ein Strafbedürfnis nur dann vorhanden, wenn ein Mensch das strafbare Verhalten in irgendeiner Form wahrnimmt, sodass dieser notwendige Rückbezug immer vorhanden sein dürfte. Das gilt mithin nicht, wenn die KI geschädigt wird, hierfür eignen sich dann jene Delikte de lege lata und de lege ferenda, die einen Eingriff in die Datenverarbeitung erfassen. Dessen ungeachtet ist dem Verfassungsrecht ein solcher Schutz virtueller Güter bisher zwar noch recht fremd, aber nicht völlig unbekannt, schützt es doch auch und ganz besonders diverse immaterielle Güter, wie die Würde des Menschen, die sich auch nicht materiell oder in einer bestimmten realen Position nachvollziehen lassen. Die Strafen bedürfen dann selbstredend auch einer Anpassung; so könnte auf einen Taterfolg in der virtuellen Welt auch eine Strafe in der virtuellen Welt folgen, etwa Einschränkungen der Nutzung gewisser Teilbereiche oder Ausschluss aus der virtuellen Welt, sodass die Verhältnismäßigkeit insoweit gewahrt bliebe. Konkrete Umsetzungen sind den technischen Entwicklungen vorbehalten. Durch diesen Rückbezug werden viele Folgeprobleme vermieden, etwa in Bezug auf den Ort der Tat oder zur Feststellung der inneren Tatseite, die in der realen Welt verbleiben kann.

2. Neue Rechtssubjekte

Kehren wir zum Beginn zurück. In der erwähnten Folge der Serie „Star Trek: The Next Generation" wird eine intelligente KI in Gestalt der Figur des Prof. James Moriarty erschaffen, der in der Romanvorlage den Gegner von Sherlock Holmes darstellt. Das Spiel auf dem Holodeck erlangt seine

40 BVerfGE 120, 224 (251).
41 BVerfGE 120, 224 (251).

Besonderheit auch dadurch, dass der Gegner nicht der Romanvorlage folgt, sondern auf der Grundlage einer Programmierung eigene Entscheidungen zum Fortgang des Spiels trifft. Dabei entwickelt sich die KI dergestalt weiter, dass sie sich schlussendlich aus der Begrenzung des Holodecks befreien will. Dies führt dazu, dass die Serienfigur Doktor Pulaski von der KI gefangen genommen wird, um die Befreiung aus dem Computer zu erzwingen. Angenommen, deutsches Strafrecht wäre anwendbar, so drängt sich unmittelbar nicht nur die Freiheitsberaubung (§ 239 StGB), sondern auch der erpresserische Menschenraub (§ 239b StGB) auf.

Agiert eine KI eigenständig und ist das Verhalten keiner realen Personen zuzurechnen (also etwa der Person, die die KI programmiert hat), ist sie nach deutschem Strafrecht nicht strafbar. Die Frage nach der Strafbarkeit von KI ist bereits älter und durch Fiktion in Literatur und Film angetrieben. Noch bevor die technischen Möglichkeiten auch nur abzusehen waren, wurden strafrechtliche Optionen erwogen[42] – möglicherweise auch deshalb, weil die literarische und filmische Darstellung in ihren Anfängen größtenteils eher vom negativen Verhalten einer KI geprägt war. KI mit menschlichen Eigenschaften und Charakterzügen findet man vor allem in neueren Darstellungen und wurden in der Vergangenheit eher in der Robotik verortet, wobei die dahinter liegende Fragestellungen natürlich eine ähnliche war. Man wird die Ansicht, eine Strafbarkeit von KI sei nicht gegeben, nach wie vor „(noch?) als die herrschende Meinung bezeichnen" können.[43] Grund dafür ist, dass die menschlichen Kategorien des Strafgesetzbuchs sich nicht auf technische Vorgänge übertragen lassen. Es wäre schon zweifelhaft, überhaupt eine Handlung von KI auszumachen; die Schuldfähigkeit indes scheitert an der Willensfreiheit.[44] Stattdessen sucht man die Verantwortlichkeit in den Personen hinter der KI, wobei die fortschreitende Entwicklung einen solchen Rückbezug immer schwieriger macht. Genauso ist anzunehmen, dass eine Strafbarkeit von KI nicht nur nicht erforderlich, sondern gar hinderlich für den weiteren technischen Fortschritt ist. Man nähme nur einmal an, ChatGPT könnte wegen Verleumdung (§ 187 StGB) belangt werden und zwar immer dann, wenn es falsche Aussagen über Personen trifft. Aus diesen Überlegungen leitet sich aber zeitgleich ab, wieso die Frage nach der Strafbarkeit von KI in der Zu-

42 Vgl. den Überblick bei *C. Kleiner*, Die elektronische Person, Baden-Baden, 2020, S. 20 ff. m. w. N.

43 *Hilgendorf*, Metaversen (Fn. 11), 686.

44 Ausf. *L. Quarck*, Zur Strafbarkeit von e-Personen, ZIS 2020, 65 (67).

kunft immer wichtiger werden wird. Gibt zwar ChatGPT noch den kleinen, schwer leserlichen Hinweis „ChatGPT kann Fehler machen", ist zumindest derzeit eine Welt vorstellbar, in der KI große Teile unseres Wissens und Informationsflusses beeinflussen wird. Dann wird es unerlässlich werden, auch KI (mit oder ohne Rückgriff auf das Strafrecht) zu regulieren und für falsche Informationen zur Verantwortung zu ziehen.

Den weiteren Weg ebnet die Fiktion. Ein zeitlicher Sprung zu Sternzeit 46424.1 (oder in Staffel 6 Folge 12 der Serie „Star Trek: Next Generation") zeigt die Konsequenz: Die (sich bis zu diesem Zeitpunkt im Holodeckspeicher befindliche) KI in Gestalt des Prof. James Moriarty hat innerhalb dieses Speichers eigene Empfindungen entwickelt, geht zwischenmenschliche Beziehungen ein und hegt weiterhin den Wunsch nach einem Leben in Freiheit (mithin außerhalb des Holodecks). Diese Konsequenz wird häufig vergessen, denn: Ebnet man den Weg einer strafrechtlichen Verantwortlichkeit der KI selbst, muss man ihr im Umkehrschluss auch den entsprechenden Schutz zukommen lassen – eine einseitige Anpassung strafrechtlicher Vorschriften zulasten von KI wird sich weder philosophisch noch soziologisch begründen lassen. Solche Überlegungen bleiben der zukünftigen, vor allem technischen, Entwicklung vorbehalten.

3. Problem der Überregulierung und Verhinderung technischen Fortschritts

Der Einsatz des „scharfen Schwerts" des Strafrechts darf gemeinwohlverträgliche Entwicklungen nicht unterbinden – das leitet sich auch aus Art. 5 Abs. 3 GG ab. Es ist notwendig, evidenzbasierte Forschung dahingehend zu betreiben, welche Chancen virtuelle Welten mit sich bringen, etwa in Bezug auf medizinischen Fortschritt; zugleich sind ihre Risiken und potenziellen Auswirkungen für die Gesellschaft oder mit Blick auf den Klimawandeln miteinzustellen.[45] Die Faktoren sind sodann in bekannter Weise in eine Verhältnismäßigkeitsprüfung einzustellen, wobei praktische Umsetzungsmöglichkeiten potenzieller Entscheidungen zu berücksichtigen sind.[46] Denkbare technische Fortschritte sind in diesem Prozess nach Möglichkeit weitestgehend zu berücksichtigen, was eine interdisziplinäre Zusammenarbeit mit anderen Wissenschaften unablässig macht.

45 Ähnlich *Hilgendorf*, Metaversen (Fn. 11), 682.
46 *Hilgendorf*, Metaversen (Fn. 11), 682.

III. Funktionalität von Strafrecht im digitalen Raum

Alle diese Überlegungen lassen einen weiteren Aspekt außen vor, der die psychologische Wirkweise von Strafandrohung im Sinne einer Generalprävention in einer virtuellen Welt erfasst. Die „Präventivwirkung des Nichtwissens" beschreibt die stabilisierende Bedeutung des Dunkelfelds.[47] Denn nur, wenn eine begrenzte Anzahl an strafrechtlich relevanten Handlungen sichtbar wird, werden Straftaten auch als etwas Ungewöhnliches wahrgenommen.[48] Schon das Internet macht Kriminalität so sichtbar und präsent, dass dieser Effekt weniger stark zutage tritt und damit auch teilweise im Bereich der Vergehen als Normalität empfunden wird.[49] Dadurch ist ein digitaler Dualismus entstanden; der physische Raum hatte wenig Auswirkung auf den digitalen Raum, sodass Ermittlungsbehörden den digitalen Raum weitestgehend außer Acht ließen.[50] Die so akzeptierten Normbrüche im digitalen Raum führten zu der Annahme, dass bisherige Formen formeller sozialer Kontrolle nicht greifen. Eine Erhöhung der Ermittlungen in virtuellen Welten, denkbar wären etwa eine Form von „Polizeipräsenz" einer Online-Polizeistelle, sind ressourcenbedingt schwerlich vorstellbar.[51] Selbst wenn sie es wären, müssten sie aber die erlernte Wahrnehmung des Internets als „rechtsfreien Raum" erst einmal durchbrechen, was wiederum die Anforderungen an die Maßnahmen selbst erhöht. Es bedarf eingehender Untersuchungen, wie diese Problemstellung aufgelöst werden kann; denn ein als nicht wirksam empfundenes Regulationselement dürfte auch faktisch wenig Wirkung zukommen.

E. Fazit

Vor der Immersion in eine weitreichende virtuelle Welt, die große Teile der realen Welt ersetzt, wie Meta es sich vorstellt, wird es viele philosophische Grundsatzfragen zu klären geben. Etwa: Wie organisiert sich das Metaversum politisch? Ist es überhaupt abhängig von realen Staaten oder gar ein eigener Staat oder schaffen sich bekannte Staatsprinzipien

47 *K. Röhl*, Das Dilemma der Rechtstatsachenforschung, Tübingen 1974, S. 105 ff.
48 *Röhl*, Dilemma (Fn. 47), S. 105 ff.
49 Mit ausf. Herleitung *T. Rüdiger*, Von der Durchbrechung der „Präventivwirkung des Nichtwissens", Kriminalistik 2021, 72 (72 ff.).
50 *Rüdiger*, Durchbrechung (Fn. 49), 75.
51 *Rüdiger*, Durchbrechung (Fn. 49), 75.

möglicherweise ab? Und wie sieht der Rückbezug zur Realität aus (Energieverbrauch, Serverkapazitäten etc.)?[52] Schon 1996 verkündete *John Perry Barlow*, Mitbegründer der Electric Frontier Foundation (eine Organisation, die sich für den Schutz von Bürgerrechten im digitalen Raum einsetzt) als Reaktion auf den US Telecommunications Act die „Declaration of the Independence of Cyberspace". Schon das lässt erahnen, dass die in staatlichen Grenzen gedachten Regulierungen, gar der Einsatz des Strafrechts, wie wir es kennen, geradezu grotesk naiv sein dürften. Diese großen Fragen sind ungeklärt, über ihre rechtliche Regulation zu diskutieren ist vergleichbar mit dem Versuch, den Revolutionsfall zu regeln (vgl. Art. 146 GG). Aus der Logik der Annahme eines digitalen Raumes ohne staatliche Grenzen ergibt sich, dass auch eine einheitliche Regulierung von Verhaltensnormen und Sanktionen für normabweichendes Verhalten in diesem einen digitalen Raum aufzustellen ist. Es gibt aber durchaus greifbare Fragen, die sich schon heute aufdrängen, etwa die strafrechtliche Erfassung der Erstellung von Deepfakes oder virtuelle Realität, die etwa in der Medizin oder im Gaming-Bereich fragmentarisch eingesetzt werden. Diesen kann häufig mit dem bestehenden Strafrecht oder kleineren Änderungen Genüge getan werden. Nimmt man an, dass unsere hiesigen Staatskonzepte und die Grundregeln der Gesetzgebung für eine virtuelle Welt auch in Zukunft Wirkung beanspruchen werden, so ist das Strafrecht weitaus wirksamer, als es auf den ersten Blick erscheint: Durch den hier entwickelten Ansatz eines Rückbezugs jedes virtuellen Handlungserfolgs auf eine reale Person können auch solche Straftaten, die lediglich in der virtuellen Welt einen Taterfolg aufzeigen, mit neuen Strafgesetzen im Rahmen der vorhandenen Systematik erfasst werden. Das System verschließt sich auch nicht einer Anpassung an die Strafbarkeit von KI selbst, wobei die Konsequenzen weit über das Strafrecht hinaus reichen.

52 Einordnend *A. Bötticher*, Das Metaversum, Kriminalistik 2022, 466 (467 f.).

„Virtuelle Welten" einer Kreislaufwirtschaft
Digitale Koordination durch die Europäische ÖkodesignVO

Maximilian Petras

Viele Aufsätze zur Kreislaufwirtschaft[1] oder dem Recht auf Reparatur beginnen mit absoluten Zahlen zum Ressourcenverbrauch: X Tonnen CO2, Y Tonnen Plastik, … Das Bild ist interessant, weil es das Problem als bereits quantifiziert darstellt. Als müsste nur eine bestimmte Menge eines bestimmten Rohstoffes an einer Stelle reduziert werden, um in ein Gleichgewicht zu kommen. Die von der EU im Green New Deal angestrebte sozial-ökologische Transformation ist allerdings ein vielfältig verwobener Prozess,[2] in dem eine Reduktion an der einen Stelle zu einer Erhöhung anderer Faktoren an einer anderen Stelle führen kann. Einen verlässlichen Überblick generiert dabei nur eine möglichst umfangreiche, frei verfügbare Datenmenge.[3] Diese „virtuellen Welten"[4] einer Kreislaufwirtschaft, oder besser einer „Circular Economy" als umfassenderer Begriff,[5] werden durch rechtliche Regelungen sowohl abgeschlossen als auch ermöglicht.

Im ersten Teil (A.) beschreibe ich die „virtuellen Welten" von produzierten Gütern. Verbaute Rohstoffe, Konstruktionspläne, der Zustand des Produktes – all diese Faktoren sind Teil der *internen* „virtuellen Welt" eines einzelnen Produktes und können doch nicht von ihrer Umwelt, der *externen* „virtuellen Welt" getrennt werden. So befinden sich schon inner-

1 Im deutschen Sprachgebrauch ist hiermit nur der letzte Teil eines Kreislaufs (die Abfallentsorgung) gemeint, während das Konzept der circular economy sehr viel weiter ist.

2 EU, Der europäische grüne Deal – Green New Deal v. 11.12.2019, COM/2019/640 final.

3 So für das Umweltrecht schon *M. Kloepfer*, Umweltrecht als Informationsrecht, in: R. David (Hrsg.), Umweltrecht zu Beginn des 21. Jahrhunderts, Berlin 2023, S. 83 (99); *H. Willke*, Komplexe Freiheit. Konfigurationsprobleme eines Menschenrechts in der globalisierten Moderne, Bielefeld 2019, S. 225.

4 Zur Problematik des Begriffes siehe die Ausführungen zugleich. Zur einfacheren Lesbarkeit werde ich nur von „virtueller Welt" sprechen.

5 Hierzu im Kontrast zur „Kreislaufwirtschaft" in der deutschen Debatte *H. Weber* und *M. Jaeger-Erben*, Circular Economy. Die Wende hin zu ‚geschlossenen Kreisläufen' als stete Fiktion, in: H. Weber (Hrsg.), Technikwenden | Technological Turns, 2023, S. 169 (187).

halb von komplexen Produkten mehrere miteinander verbaute Module, deren Ersatzteile außerhalb des Produktes liegen. Und doch ist die Unterscheidung intern-extern wichtig, um die Zugangsregelungen verschiedener Rechtsgebiete besser einordnen zu können.

Daraufhin wird auf einer vorgelagerten Ebene geklärt (B.), warum die Öffnung der „virtuellen Welten" von Produkten für den Umschwung zu einer Circular Economy so wichtig ist (I.) und verschiedene rechtliche Regelungen diesen gesamtgesellschaftlichen Zugang primär verschließen (II.).

Während unter A. die „virtuellen Welten" in interne und externe Dimensionen zerlegt werden, lässt sich diese Unterteilung in den jeweiligen Zugangsrechten (C./D.) fortsetzen. Ich beginne bei den individuellen Zugangsrechten (C.) mit dem Recht auf Reparatur als Modifikation des zivilrechtlichen Kaufvertrages (I.), um sogleich im Anschluss die Neuregelungen des Data Acts (II.) zu beschreiben, der Datenzugänge für erworbene Güter eröffnet.

Ebenso wenig, wie sich interne und externe „virtuelle Welt" eines Produktes vollständig trennen lassen, können individuelle Zugangsrechte von ihrem gesellschaftlichen Counterpart isoliert werden (D.). Mit dem digitalen Produktpass lassen sich Produktdaten bündeln, die bei entsprechender Umsetzung durch die EU eine Koordination der Produktion ermöglichen könnten. Zugleich wird klar, dass die Unterscheidung von „interner" und „externer" virtueller Welt eines Produktes nur der Zuteilung verschiedener rechtlicher Regelungen dient, aber die rechtliche Kategorisierung selbst – namentlich die Unterscheidung in Zivilrecht und öffentliches Recht[6] – als sehr fragwürdig erscheinen lässt (E.).

A. Die „virtuellen" Welten der Materialität in der Circular Economy

Unter einer virtuellen Welt verstehe ich die informellen Bestandteile eines *materiellen* Gegenstandes – Virtualität ist also immer an spezifische Ressourcenströme gekoppelt und hat zudem sowohl interne wie externe

6 Zur Verzahnung zwischen Umwelt- und Verbraucherrecht vgl. *K. Tonner*, Mehr Nachhaltigkeit im Verbraucherrecht – die Vorschläge der EU-Kommission zur Umsetzung des Aktionsplans für die Kreislaufwirtschaft, VuR 2022, 323 (333).

Dimensionen.[7] Damit verschiebt sich der Blick von der Art der Darstellung (z.B. 3D)[8] zur Frage des Interface[9] (Zugangsrechte) – und weg von einer „new frontier" als unbegrenztem „Cyberspace".[10] Wenngleich die Virtualität auch die Darstellung der Materialität in ihren Stoffkreisläufen, Energieflüssen und Produktionsbedingungen in begrenzter Weise ermöglicht. Gerade die von der EU seit dem „Green New Deal" forcierte Umstellung der linearen auf eine kreislaufförmige Wirtschaft ist auf Daten zur Koordination angewiesen.[11]

Was genau sind nun diese „virtuellen Welten" des Produktes? Sie lassen sich als zwei Kreisläufe verstehen, die sowohl zeigen, woher das Produkt kommt, als auch was aus ihm werden kann. Ressourcen- und Emissionsströme sind Bestandteil eines jeden Gegenstandes und lassen sich nur über Daten darstellen.[12] Sie sind verschiedene Ausschnitte desselben Zusammenhanges.

Der erste Kreislauf ist intern-retrospektiv ausgerichtet, indem er Auskunft zu den konkreten Bestandteilen und Bauplänen des Produktes gibt. Als Idealtyp dieser „virtuellen Welt" kann das Konzept der „Open Hardware" gelten: „Open-Source-Hardware ist Hardware, deren Baupläne öffentlich zugänglich gemacht wurden, sodass alle sie studieren, verändern, weiterverbreiten und sie sowie darauf basierende Hardware herstellen und verkaufen können. Die Quelldateien der Hardware, die Dateien mit denen sie produziert wird, sind verfügbar gemacht im für Veränderungen daran bevorzugten Format. Im Idealfall nutzt Open-Source-Hardware fertig

7 *D. van Laak*, Alles im Fluss. Die Lebensadern unserer Gesellschaft – Geschichte und Zukunft der Infrastruktur, Bonn 2019, S. 266; *K. Crawford*, Atlas of AI. Power, Politics, and the Planetary Costs of Artificial Intelligence, New Haven 2021.

8 Letztlich sind Metaverse oder Computerspiele, als typische Vertreter „virtueller Welten", auf einer abstrakteren Ebene nichts anderes als der über ein Interface vermittelte Zugang zu Datenbeständen.

9 *B. H. Bratton*, The stack. On software and sovereignty, Cambridge, Massachusetts 2015, S. 220.

10 *F. Stalder*, Kultur der Digitalität, Berlin 2. Aufl. 2017, S. 49; *T. Terranova*, After the Internet. Digital Networks between Capital and the Common, Cambridge (Mass.) 2022, S. 12; vgl. zur Verbindung zwischen Kolonialismus und digitalen Technologien den Überblick bei *N. Couldry* und *U. A. Mejias*, The decolonial turn in data and technology research. What is at stake and where is it heading?, Information, Communication & Society 2023, S. 788 ff.

11 Dazu sogleich unter B. I.

12 *D. Baecker*, Studien zur nächsten Gesellschaft, Frankfurt am Main 2007, S. 187; *S. Schaupp*, Stoffwechselpolitik: Arbeit, Natur und die Zukunft des Planeten, Berlin 2024, S. 271.

erhältliche Komponenten und Materialien, Standardprozesse, offene Infrastrukturen und frei nutzbare Inhalte, um damit die Möglichkeiten aller zu maximieren, die Hardware zu bauen und zu verwenden."[13] Im Gegensatz zum bekannteren Konzept der Open-Source-Software[14] ist Open Hardware noch stärker auf Kooperation aller Beteiligten (z.B. der Zulieferer von Einzelteilen) angewiesen, da hier komplexe Produkte im physischen Raum hergestellt werden.[15]

Der zweite Kreislauf der „virtuellen Welt" des Produktes ist dann wiederum extern-prospektiv ausgerichtet und zeigt an, was aus dem Produkt werden könnte. Das kann ein zweites Leben als Gebrauchtware (eBay), eine Wiederverwendung der im Gerät enthaltenen Ressourcen und Bauteile oder eine Modifikation als neues Produkt sein. Noch stärker als bei der internen virtuellen Welt muss das Produkt in ein Verhältnis zu anderen Akteur:innen, anderen Ressourcen, anderen Prozessen gesetzt werden. Als Idealtyp dieser Herstellung von Relationalität sehe ich die Methode des Life Cycle Sustainability Assessment (LCSA): Hierüber „können Produktionssysteme von Gütern und Dienstleistungen als physische und soziale Systeme, die die Beziehungen zwischen Ressourcen und gesellschaftlichen Bedürfnissen durch wirtschaftliche Infrastrukturen und Praktiken vermitteln, verstanden und modelliert werden als komplexe Netzwerke aus Prozessen mit Input- und Output-Flüssen und zahlreichen Meta-Informationen"[16]. Damit kann zum Beispiel untersucht werden, welche Produktionsschritte für ein E-Auto notwendig sind, welche Umweltauswirkungen entstehen und was der Output ist (z.B. Beförderung von X Personen für Zeitraum Y).[17]

13 Open-Source-Hardware (OSHW) Grundsatzerklärung 1.0, https://www.oshwa.org/definition/german/ (besucht am 05.09.2024).

14 *P. Terzis*, Building programmable commons, Law, Innovation and Technology 2023, S. 27.

15 *M. Voigt* u. a., Unboxing Black Boxes. Mit Open Hardware & Zivilgesellschaft für eine nachhaltige Zukunft, Berlin 2023, S. 14.

16 *J. Heyer* und *W. Zeug*, Ökobilanz und kybernetische Wirtschaftsplanung: Demokratisch geplante Wirtschaft zur Befriedigung gesellschaftlicher Bedürfnisse in planetaren Grenzen, PROKLA 2024, 267 (274).

17 Vgl. weitergehend *Heyer* und *Zeug*, Ökobilanz und kybernetische Wirtschaftsplanung (Fn. 16), 267 (275), die das Modell um soziale und weitere ökologische Indikatoren ergänzt haben.

Virtuelle Welten sind wichtig, um das von der EU im Rahmen des „Green New Deal“[18] angestrebte Ziel einer Circular Economy zu erreichen.[19] Gemeint ist ein regeneratives System der Produktion, Distribution und Konsumption von Gütern, ohne fossilen Input und ohne schädlichen Output.[20] Der Zusammenhang zwischen Circular Economy und Klimakrise ist so eng wie zwischen Produktdaten und Transformation, da ein großer Teil der Emissionen auf die Extraktion von Ressourcen und die Produktion von Gütern zurückgeführt werden kann und diese zu ihrer Überwindung sichtbar gemacht werden müssen.[21]

B. Schließung und Öffnung digitaler Kooperationsmöglichkeiten

Bevor auf die genauen Zugangsrechte aus zivil- und öffentlich-rechtlicher Sicht eingegangen wird, werde ich zunächst die Potentiale einer Kombination von interner und externer „virtueller Welt“ von Produkten darlegen. Sodann muss herausgestellt werden, dass die bestehenden rechtlichen Regelungen die in der Digitalisierung liegenden Kooperations- und Einsparungsmöglichkeiten systematisch verschließen. An beiden Punkten sind die unter C. und D. thematisierten Zugangs- und Bündelungsrechte von Daten zu messen.

I. Potentiale einer digital koordinierten Circular Economy

Ein wesentlicher Teil des europäischen „Green New Deals“ mit dem Ziel, die Treibhausgasemissionen bis 2030 um 50 % zu verringern,[22] ist die Umstellung der Extraktion und Produktion von Rohstoffen von einer li-

18 EU, Der europäische grüne Deal – Green New Deal v. 11.12.2019, COM/2019/640 final.

19 Vgl. zu den in der deutschsprachigen Diskussion geführten Debatten um „Nachhaltigkeit“, die weitreichende Schnittmengen aufweist, nur *M. Reese*, Leitbilder des Umweltrechts, ZUR 2010, 339 (341).

20 *M. Calisto Friant* u. a., A typology of circular economy discourses: Navigating the diverse visions of a contested paradigm, Resources, Conservation and Recycling 2020, Nr. 104917, S. 1.

21 *M. von Hauff*, Grundwissen Circular Economy. Vom internationalen Nachhaltigkeitskonzept zur politischen Umsetzung, München 2023, S. 38.

22 EU, Der europäische grüne Deal – Green New Deal v. 11.12.2019, COM/2019/640 final, S. 2.

nearen Wirtschaftsweise auf eine Circular Economy. Die EU folgt damit ihrem primärrechtlichen Auftrag in Art. 37 GrCh oder Art. 3 III EUV,, ein „hohes Maß" an Umweltschutz zu erreichen, bzw. nach Art. 11 AEUV auf einen Pfad „nachhaltiger Entwicklung" einzuschwenken. Art. 191 AEUV spricht dann auch explizit von der umsichtigen und rationellen Verwendung „natürlicher Ressourcen". Der dabei angewandte Instrumentenmix ist weit überwiegend eine Variation indirekter staatlicher Wirtschaftskoordination.[23] Er bleibt damit abhängig von Marktmechanismen und verlässt sich auf die Wirkung von Angebot und Nachfrage.[24] Im Fokus stehen soll hier die Daten- und Informationspolitik der EU in Bezug auf die Ressourcenflüsse der Circular Economy.[25] Nicht behandelt – aber im Sinne eines holistischen Ansatzes im Umweltrecht eigentlich mitzudenken[26] – werden die CSR- oder CSDD-Regulierungen sowie Änderungen im Verbraucherrecht.[27]

Das Konzept der Circular Economy bezieht sich auf alle fünf Stadien eines Produktlebenszyklus (Design, Produktion, Nutzung, zweites Leben, Recycling).[28] Gerade die Phase des Designs ist wichtig, damit es nicht „linear" (bis zur Deponie) endet, sondern zirkulär weitergeht.[29] Hieran wird

23 *J. Ziekow*, Öffentliches Wirtschaftsrecht, 5. Aufl. 2020, S. 66.

24 *A.-C. Mittwoch*, Der digitale Produktpass der Ökodesign-Verordnung, RDi 2024, S. 63.

25 Zu nennen wäre hier auch die Taxonomy für Nachhaltigkeit, vgl. für einen Überblick *I. Kampourakis*, The market as an instrument of planning in sustainability capitalism, European Law Open 2023, S. 16 f.

26 *L. J. Kotzé* u. a., Earth system law: Exploring new frontiers in legal science, Earth System Governance 2022.

27 *EU*, Richtlinie (EU) 2022/2464 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 zur Änderung der Verordnung (EU) Nr. 537/2014 und der Richtlinien 2004/109/EG, 2006/43/EG und 2013/34/EU hinsichtlich der Nachhaltigkeitsberichterstattung von Unternehmen; *EU*, Richtlinie (EU) 2024/825 des Europäischen Parlaments und des Rates vom 28. Februar 2024 zur Änderung der Richtlinien 2005/29/EG und 2011/83/EU hinsichtlich der Stärkung der Verbraucher für den ökologischen Wandel durch besseren Schutz gegen unlautere Praktiken und durch bessere Informationen; *EU*, Richtlinie (EU) 2024/1760 des Europäischen Parlaments und des Rates vom 13. Juni 2024 über die Sorgfaltspflichten von Unternehmen im Hinblick auf Nachhaltigkeit und zur Änderung der Richtlinie (EU) 2019/1937 und der Verordnung (EU) 2023/2859; vgl. dazu *M. Bartl*, Towards the imaginary of collective prosperity in the European Union (EU): reorienting the corporation, European Law Open 2022, 957 (961 f.).

28 *D. Piétron* u. a., Die digitale Circular Economy. Zirkuläre Daten-Governance für eine Ressourcennutzung von der Wiege zur Wiege, Berlin 2023, S. 9.

29 EU, Aktionsplan Kreislaufwirtschaft, S. 3.

auch deutlich, dass die Circular Economy sich von früheren Diskussionen der Kreislaufwirtschaft als Abfallwirtschaft abhebt,[30] wenngleich sich die dort eingeführten „4R" (Reduce, Reuse, Recycle, Recover) auch auf die Circular Economy übertragen lassen – freilich heute mit einem Schwerpunkt auf „Reduce" und „Reuse".[31] Die mit der Circular Economy verknüpften Hoffnungen sind vielfältig, wie es für ein so offenes Konzept typisch ist: essenziell ist der verminderte Verbrauch von Ressourcen,[32] sowie der Kampf gegen die Klimakrise, da nahezu die Hälfte der Treibhausgase und 90 % des Biodiversitätsverlustest auf Gewinnung und Verarbeitung von Rohstoffen zurückzuführen sind.[33] Das auf den ersten Blick relativ klare Konzept erweist sich in der Umsetzung als sehr komplex: Die eingesetzten Ressourcen, die dafür notwendige Energie und die dabei zerstörte (oder erhaltene) Biodiversität stehen in einem Wechselverhältnis, das je nach Sektor und Situation variiert.[34] Dabei darf die Extraktionsrate die Regenerationsrate nie übersteigen.[35] Der Produktpreis als alleiniger Indikator reicht dafür nicht aus.[36] Jede Form der Umweltpolitik und die Wahrnehmung wie Bekämpfung der Klimakatastrophe lässt sich nur über eine Modellierung von Ressourcenflüssen organisieren.[37] Auch in den strategischen EU-Erklärungen ist von „beschleunigen und optimieren" oder einem „europäischen Datenraum" zum Nachverfolgen und Zugänglichmachen von Produktdaten die Rede.[38] Diese zweifellos richtigen Punkte lassen sich noch verschärfen. Um eine Circular Economy zu erreichen, braucht es eine Verknüpfung von Unternehmen, die über sporadische Kooperation im Alltagsgeschäft hinaus geht.[39] Um etwa Ressourcen wiederzuverwenden, Einzelkomponenten neu zu verbauen oder Kipppunkte in der Regenerationsfähigkeit zu identi-

30 Zu Kontinuitäten und Schwerpunkten beider Konzepte siehe *Weber* und *Jaeger-Erben*, Circular Economy (Fn. 5), S. 169 (185 f.).
31 *von Hauff*, Grundwissen Circular Economy (Fn. 21), S. 26 f.
32 EU, Aktionsplan Kreislaufwirtschaft, S. 2.
33 EU, Der europäische grüne Deal – Green New Deal v. 11.12.2019, COM/2019/640 final, S. 8.
34 *Calisto Friant* u. a., A typology of circular economy discourses: (Fn. 20), S. 4.
35 *Heyer* und *Zeug*, Ökobilanz und kybernetische Wirtschaftsplanung (Fn. 16), 267 (273).
36 *Piétron* u. a., Die digitale Circular Economy (Fn. 28), S. 11.
37 *S. Schaupp*, Stoffwechselpolitik: Arbeit, Natur und die Zukunft des Planeten, Berlin 2024, S. 271.
38 EU, Der europäische grüne Deal – Green New Deal v. 11.12.2019, COM/2019/640 final, S. 11; *EU*, Aktionsplan Kreislaufwirtschaft, S. 20.
39 *Piétron* u. a., Die digitale Circular Economy (Fn. 28), S. 11.

fizieren, braucht es Daten, die Wissenslücken überbrücken, verschiedene Stakeholder:innen zusammen bringen und Verantwortung für die getroffenen Entscheidungen ermöglichen.[40] Das gilt für alle Beteiligten auf allen Ebenen des Prozesses. Am Beispiel des unten thematisierten Rechts auf Reparatur ist die Notwendigkeit des Datenzugangs besonders eindrücklich, da aus den in den Geräten gespeicherten Daten der Zustand abgelesen und ggf. modifizierend handwerklich gearbeitet werden kann.[41]

Nun sind gerade die Daten für Verbraucher:innen oder kleine und mittlere Unternehmen in der Regel nicht zugänglich (dazu sogleich unter II.).[42] Bereits jetzt zeigen sich die üblichen Probleme der Fragmentierung von Standards und voneinander abgetrennter Datensilos.[43] Schon früh wurden deshalb nicht nur der Einsatz offener Software, offener Schnittstellen oder freier Standards vorgeschlagen, sondern auch Strategien zum Pooling von Daten,[44] die inzwischen durch die europäische Datenstrategie in Ansätzen umgesetzt werden.[45] Zwar gibt es auch in der Privatwirtschaft bereits Konzepte und erste Experimente einer Datentreuhand zwischen privaten Unternehmen,[46] aber die sogleich diskutierte Ökodesign-Verordnung hebt diese Erfahrungen auf ein ganz neues Niveau.

II. Die virtuellen (und im Plastik verklebten) Mauern des Rechts

Die oben geschilderten Idealtypen der Datenkooperation einer Circular Economy (Open Hardware, Life Cycle Analysis) existieren bisher nur als Prototypen. Daten und Informationen sind ein wertvolles Gut, das

40 *Piétron* u. a., Die digitale Circular Economy (Fn. 28), S. 10 sprechen von „bridge", „relate", „resonate", „responsibilize".

41 *R. Podszun*, Handwerk in der digitalen Ökonomie, 2021, S. 22.

42 Vgl. zur Plattformisierung etwa *P. Staab*, Digitaler Kapitalismus. Markt und Herrschaft in der Ökonomie der Unknappheit, Berlin 2019, S. 208 f.; *Terranova*, After the Internet (Fn. 10), S. 39.

43 *Piétron* u. a., Die digitale Circular Economy (Fn. 28), S. 22.

44 *Podszun*, Handwerk in der digitalen Ökonomie (Fn. 41), S. 127, 185.

45 *Europäische Kommission*, Eine europäische Datenstrategie; vgl. für einen Ausschnitt der Regulierungen *H. Ruschemeier*, Die aktuelle Digitalgesetzgebung der Europäischen Union – eine kritische Analyse, ZG 2023, 337 (346).

46 Vgl. nur *S. Augsberg* u. a., Transaktionsbasierte Datentreuhand, JZ 2022, 1139 (1145).

künstlich verknappt und abgeschirmt wird.[47] Bei vernetzten Geräten verhindert ein „Digital Rights Management" (DRM) mit einer Mischung aus Technologien und (zivilrechtlich vereinbarten) Schutzrechten, dass Daten ausgelesen oder gar Geräte repariert werden können.[48] So kann über die Methode der Serialisierung jedes Einzelteil eines Geräts mit einer Nummer ausgestattet werden, sodass die Firmware Ersatzteile ohne eine entsprechende Seriennummer nicht akzeptiert.[49] Gerade Plattformen bergen die Gefahr, ein „knowledge monopoly" zu bilden und dieses über Urheberrechte, Geschäftsgeheimnisse oder implizites Wissen zur Produktion so abzuschirmen, dass Innovation auf verschiedenen Märkten ausgebremst wird.[50] Ein immer wieder diskutiertes,[51] und dennoch weitgehend abgelehntes,[52] Dateneigentum braucht es dafür gar nicht.

C. Individuelle Zugangsrechte

Inzwischen wurden gerade auf der europäischen Ebene zahlreiche Zugangsrechte geschaffen, die entgegen dieser grundsätzlichen Schließung kurzfristig individuelle Öffnungen erwirken und langfristig einen „europäischen Datenraum" ermöglichen sollen. Mit den aktuellen Regulierungen schreibt die EU eine längere Tradition fort, die sich durch primäre Abschließung (über die Konstruktion von Märkten) und nachträgliche Öffnung auszeichnet. So lassen sich dann etwa Grundrechte als Zugangsregeln

47 *O. H. Gandy*, The panoptic sort. A political economy of personal information, Boulder, Colorado 1993, S. 79; *R. Kitchin*, The data revolution. Big data, open data, data infrastructures & their consequences, London 2. Aufl. 2021, S. 222.

48 Hierzu grundlegend *A. Perzanowski* und *J. Schultz*, The End of Ownership: Personal Property in the Digital Economy, 2016, S. 145, wenngleich ihr Fokus auf Ausschließlichkeitsrechte der Nutzenden das Problem nur verschiebt.

49 *Podszun*, Handwerk in der digitalen Ökonomie (Fn. 41), S. 55.

50 *C. Rikap*, Capitalism, power and innovation. Intellectual monopoly capitalism uncovered, Abingdon, Oxon; New York 2021, S. 25.

51 Zur deutschen Debatte etwa *W. Hoffmann-Riem*, Recht im Sog der digitalen Transformation, Tübingen 2022, S. 130.

52 Für IoT so auch *Podszun*, Handwerk in der digitalen Ökonomie (Fn. 41), S. 58.

lesen,[53] Internet Service Provider zur Durchleitung verpflichten[54] oder Bottlenecks in Netzwirtschaften öffnen.[55] Als Anlass individueller Zugangsrechte dient hier das durch EU-Recht neu eingeführte Recht auf Reparatur, welches auf die (weiter gefassten) Zugangsrechten des EU Data Acts angewiesen ist.[56]

I. „Recht auf Reparatur" als Modifikation des zivilrechtlichen Kaufvertrags

Die Symptome der linearen Wirtschaftsweise sind Berge von Müll als Resultat geplanter Obsoleszenz in immer kürzeren Produktlebenszyklen und der Dominanz geschlossener Systeme, die das ganze Gerät zerstören, wenn nur eine Komponente kaputtgeht.[57] Inzwischen reichen die Spuren der linearen Wirtschaftsweise so tief, dass die früher selbstverständliche Kultur des Reparierens mit den ihr verbundenen Werkstätten in weiten Teilen verloren gegangen ist.[58] Diese als Teil einer Circular Economy wieder aufleben zu lassen, erfordert eine Perspektive auf den gesamten Produktlebenszyklus inklusive der Einstellungen und Fähigkeiten der daran Beteiligten.[59] Die Grenzen zwischen Reparieren und Selbermachen/Weiterentwickeln sind dabei fließend und sollten es auch sein,[60] da in dem oben geschilderten Produktlebenszyklus der Circular Economy immer auch ein „zweites Le-

53 *D. Wielsch*, Grundrechte als Rechtfertigungsgebote im Privatrecht, in: I. Augsberg, S. Korioth, und T. Vesting (Hrsg.), Grundrechte als Phänomene kollektiver Ordnung. Zur Wiedergewinnung des Gesellschaftlichen in der Grundrechtstheorie und Grundrechtsdogmatik, Tübingen 2014, S. 141.

54 *V. Karavas*, Digitale Grundrechte. Elemente einer Verfassung des Informationsflusses im Internet, Baden-Baden 2007, S. 110.

55 *M. Schmidt-Preuß*, Das Recht der Regulierung – Idee und Verwirklichung, in: F. J. Säcker und M. Schmidt-Preuß (Hrsg.), Grundsatzfragen des Regulierungsrechts, 2015, S. 68 (78) z.B. im Energierecht nach §§ 20 ff. EnWG.

56 Zivilrechtlich sind zahlreiche weitere Zugangsrechte etwa nach GWB und DMA denkbar, vgl. dazu *Podszun*, Handwerk in der digitalen Ökonomie (Fn. 41), S. 86 ff.

57 Zum Konsum als emotionalem Anker im Alltag vgl. *D. van Laak*, Alles im Fluss (Fn. 7), S. 118; Sachverständigenrat für Verbraucherfragen, Recht auf Reparatur, September 2022, S. 14 f.

58 *E.-M. Kieninger*, Recht auf Reparatur („Right to Repair") und Europäisches Vertragsrecht, ZEuP 2020, 265 (267); *M. Jaeger-Erben* und *S. Hielscher*, Verhältnisse reparieren: Wie Reparieren und Selbermachen die Beziehung zur Welt verändert, Bielefeld 2022, S. 13 ff.

59 Sachverständigenrat für Verbraucherfragen, Recht auf Reparatur, September 2022, S. 7.

60 *Jaeger-Erben* und *Hielscher*, Verhältnisse reparieren (Fn. 58), S. 14 f.

ben“ (Reuse) von Gegenständen angestrebt wird, das über den während des Kaufs imaginierten Zweck hinaus geht.

Mit der neuen Reparatur-Richtlinie tritt ein eigenständiges „Recht auf Reparatur“ neben die kaufrechtliche Mängelgewährleistung.[61] Nach Art. 5 Abs. 1 i.V.m. Anhang II der Reparatur-RL besteht dieses Recht für alle Produkte, die von den Durchführungs-Verordnungen der Ökodesign-Verordnung erfasst werden (dazu sogleich unter D.). Sowohl die Reparatur selbst als auch die (von Dritten genutzten) Ersatzteile müssen zu einem angemessenen Preis angeboten werden, Art. 5 Abs. 2, 4 Reparatur-RL.[62] Zentral für die Effektivität dieses neuen Rechtes sind umfassende Verbraucherinformationen nach Art. 5 Abs. 5 und Art. 6 der Reparatur-RL. Interessant für den Kontext einer datengetriebenen Circular Economy ist die in Art. 7 Reparatur-RL vorgesehene Einrichtung einer Plattform für Reparaturbetriebe und Werkstätten.[63] Speziell bei digitalen Endgeräten besteht die Problematik des direkten Datenzugangs zum Zweck der Reparatur. So werden Daten einerseits benötigt, um die Reparatur durchzuführen (etwa zur Analyse des Schadens), aber auch um ggf. Modifikationen basierend auf der Nutzung vorzuschlagen (z.B. andere Einstellung einer Heizung, um Schäden vorzubeugen).[64]

II. Die Vertragsnetzwerke des Data Act

Der für die Reparatur notwendige Zugang zur internen virtuellen Welt eines Objektes ermöglicht die ebenfalls jüngst eingeführte Data Act Verordnung (DA) der EU.[65] Ähnlich wie im Kontext des Green New Deal, hat die EU mit ihrer Datenstrategie und dem Anspruch der Schaffung eines „European Data Space“ verschiedene Gesetze auf den Weg gebracht.[66] Der DA habe das Potential „ein ‚Grundgesetz‘ des Internet of Things für

61 EU, Reparatur-RL (EU) 2024/1799.

62 Zur Problematik der Umsetzung siehe Sachverständigenrat für Verbraucherfragen, Recht auf Reparatur, September 2022, S. 41.

63 Hier ergeben sich Möglichkeiten der Verknüpfung mit dem in Art. 14 Ökodesign-VO vorgesehenen Webportal.

64 Zur Thematik aus der Sicht des Handwerkes umfassend *Podszun*, Handwerk in der digitalen Ökonomie (Fn. 41), S. 22.

65 EU, Data Act Verordnung (EU) 2023/2854.

66 Für einen Überblick siehe *H. Ruschemeier*, Die aktuelle Digitalgesetzgebung der Europäischen Union – eine kritische Analyse, ZG 2023, passim.

den europäischen Binnenmarkt“[67] zu werden. Durch ihn erhält der „Datennutzer“ von vernetzten Geräten einen Zugangsanspruch zu den auf dem Gerät gespeicherten Daten. Mehr noch, muss doch gem. Art. 3 Abs. 1 DA schon das Produkt so gestaltet werden, dass die Nutzer:in direkt auf die Daten zugreifen kann („access by design“[68]). Zugleich ist es möglich, dass die Daten gem. Art. 5 DA an Dritte, z.B. Reparaturbetriebe bei kaputten Geräten, herausgegeben werden können. Damit wird bei Weitem kein „Open Data“ Regime etabliert, wie es etwa in einigen Informationsfreiheits- und Transparenzgesetzen bzgl. Daten von *öffentlichen* Stellen vorgesehen ist.[69] Für die Weitergabe an Dritte gelten in Art. 5 Abs. 9–11 DA strenge Ausschlussgründe, die sich zusammengefasst an dem Schutz der Geschäftsgeheimnisse und Wirtschaftstätigkeit der Dateninhaber orientieren und bei den Dritten weitgehende technisch-organisatorische Maßnahmen der Abschirmung voraussetzen. Dritte dürfen die Daten gem. Art. 6 Abs. 2 lit. c) DA sodann wiederum nur mit Zustimmung der „Datennutzer“ an andere Dritte herausgeben.

Damit zeigt sich, dass mit dem DA zwar die „Datennutzer“ im Zentrum der neuen Datenökonomie stehen, dieser Zugang damit aber zwangsläufig auf die oben umschriebene *interne* virtuelle Welt beschränkt bleibt. Die Verbindung zur externen virtuellen Welt, etwa als Möglichkeit der Kombination von verschiedenen Daten (etwa um bessere Möglichkeiten der Reparatur oder Nutzung zu entdecken), wird gekappt oder zumindest werden die Transaktionskosten für eine kooperative Data-Governance durch den DA unnötig erhöht.[70] Das ist auch deshalb problematisch, weil die Fokussierung auf individualisierte „Datennutzer“ all die Probleme wiederholt, die auch eine wirksame Umsetzung der informationellen Selbstbestimmung verhindern.[71] Die Individualisierung des DA-Regimes erschließt sich auch mit einem Blick auf die sehr restriktiv konstruierten Herausgabemöglich-

67 *R. Podszun*, Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks, Baden-Baden 2023, S. 21.

68 *Podszun*, Der EU Data Act (Fn. 67), S. 20.

69 Vgl dazu *S. Dörenbach*, Veröffentlichungspflichten, in: M. Petras und H. Vos (Hrsg.), Handbuch Informationsfreiheitsrecht, Kiel 2023, sowie die sonstigen Beiträge im Handbuch.

70 *E. Hilgendorf* und *P. Vogel*, Datenrecht im Umbruch. Aktuelle Herausforderungen von Datenschutz und Datenwirtschaft in Europa, JZ 2022, 380 (387 f.); *Podszun*, Der EU Data Act (Fn. 67), S. 64.

71 Siehe dazu ausführlich *M. Petras*, Vernetzte Autonomie. Eine infrastrukturelle Kritik der informationellen Selbstbestimmung, Manuskriptfassung.

keiten öffentlicher Stellen. Der Staat darf nach Art. 15 ff. DA Daten nur herausverlangen, wenn eine Notstandssituation vorliegt oder der Anspruch die ultima ration ist, nachdem weder eine Beschaffung über den Markt noch der rechtzeitige Erlass eines Gesetzes als Zugriffsgrundlage möglich ist.[72] Dass der DA hier nicht weiter führt, wird ggf. durch verschiedene Regelungen in der Ökodesign-VO abgefangen.

D. Der digitale Produktpass – kollektives Zugangsrecht oder gesellschaftliches Bündelungsrecht?

Der DA und das ihn flankierende Recht auf Reparatur kennen nur jeweils sehr beschränkte interne virtuelle Welten. Das Recht auf Reparatur hat aber zugleich einen starken Bezug zur (öffentlich-rechtlichen)[73] Regelung der Ökodesign-Verordnung. Diese erschafft einen Rahmen für die Aufstellung weiterer Durchführungs-Verordnungen für spezifische Produktgruppen, für die dann automatisch nach Art. 5 Abs. 1 i.V.m. Anhang 1 Reparatur-RL das Recht auf Reparatur aktiviert wird. An dieser Stelle ergibt sich eine wichtige intradisziplinäre Verschränkung zwischen Zivilrecht und öffentlichem Recht. Ziel der Ökodesign-VO ist das nachhaltige Produkt als Normalfall, Art. 1 Abs. 1 Ökodesign-VO. Die Ökodesign-Anforderungen an Produkte erfassen gemäß Art. 5 Abs. 9 sowohl Leistungs- als auch Informationsanforderungen, die in umfassenden Verfahren, inklusive Folgenabschätzung, gem. Art. 5 Abs. 10 festgelegt werden und wiederum zahlreichen Einschränkungen in Art. 5 Abs. 11 unterliegen (keine Beeinträchtigung von Funktionsfähigkeit, Wettbewerb usw.). Zwar sind diese Anforderungskataloge sehr ambitioniert, allerdings dauert es lange bis zur Verabschiedung einer Durchführungs-Verordnung, da u.a. das hierfür erforderliche Wissen bei der Industrie (und nicht den EU-Behörden) liegt.[74] Für die Vorgängerregelung der Ökodesign-Richtlinie wird auf die Diskrepanz zwischen

72 *Hilgendorf* und *Vogel*, Datenrecht im Umbruch (Fn. 70), S. 387.

73 Für ein eigenständiges EU „materials law" als Teilgebiet des Umweltrechts eintretend *T. J. de Römph* und *J. M. Cramer*, How to improve the EU legal framework in view of the circular economy, Journal of Energy & Natural Resources Law 2020, 245 (259).

74 Sachverständigenrat für Verbraucherfragen, Recht auf Reparatur, September 2022, S. 40; *K. Tonner*, Mehr Nachhaltigkeit im Verbraucherrecht – die Vorschläge der EU-Kommission zur Umsetzung des Aktionsplans für die Kreislaufwirtschaft, VuR 2022, 323 (326 ff.).

hohen rhetorischen Ansprüchen und der faktisch weniger ambitionierten Umsetzung in der Standardsetzung hingewiesen.[75]

Wenn das Verfahren dann abgeschlossen ist, sind die Produkte idealerweise nicht nur nachhaltiger hergestellt, sondern neben ihnen – und das ist eine große Innovation der neuen Ökodesign-VO – muss ein sogenannter „digitaler Produktpass" nach Art. 10 ff. Ökodesign-VO existieren. Ein solcher Produktpass enthält alle Informationen, die für subjektives Entscheiden (Konsument:innen) als auch transsubjektive Koordination (Unternehmens-Kooperationen und staatliche Steuerung) wichtig sind (z.B. Materialien, CO2-Anteil, Funktionsumfang, Reparaturanleitungen, Rückgabeort usw.).[76] Aufgrund der Menge zirkulierender Informationen sollen derartige standardisierte Bündelungen einem „information overload" vorbeugen.[77] Produktdaten gibt es natürlich jetzt schon in vielfältiger Weise, vor allem innerhalb von Unternehmen, allerdings sind diese in der Regel weder gesellschaftlich geteilt noch interoperabel.[78] Das soll sich mit dem Produktpass ändern, der nach Art. 7 Abs. 7 Ökodesign-VO alle „Informationsanforderungen" enthält, die genau wie die „Leistungsanforderungen" an Produkte ebenfalls in den Durchführungs-VO der EU festgesetzt werden. Gemäß Art. 9 Abs. 1, 2 a) i.V.m. Anhang III a) Ökodesign-VO, der auf Art. 7 Abs. 2 b) verweist, können im Produktpass so potentiell alle Produktparameter aus Anlage 1 Ökodesign-VO im ganzen Produktlebenszyklus sowie zu erhebende Informationen aufgrund von anderen EU-rechtlichen Regelungen enthalten sein.[79] Produktparameter können sowohl quantitativ erfasst werden (Energieverbrauch) als auch qualitative Merkmale enthalten (Reparierbarkeit, Verfügbarkeit von Ersatzteilen usw.).[80] Für jede Produktgruppe gem. Art. 5 Abs. 4–7 Ökodesign-VO wird dies einzeln bestimmt. Die Speicherung der Daten erfolgt dezentral, zugänglich über einen „Datenträger" (z.B. QR-Code), der mit einer „eindeutigen Produktkennung" für jedes Produkt verknüpft ist, wobei die gespeicherten Daten gem. Art. 10

75 *J. Pollex*, Simultaneous Policy Expansion and Reduction? Tracing Dismantling in the Context of Experimentalist Governance in European Union Environmental Policy, JCMS 2022, 604 (616).
76 *Piétron* u. a., Die digitale Circular Economy (Fn. 28), S. 5.
77 *A.-C. Mittwoch*, Der digitale Produktpass der Ökodesign-Verordnung, (Fn. 24),S. 64.
78 Sachverständigenrat für Verbraucherfragen, Recht auf Reparatur, September 2022, S. 41; *Piétron* u. a., Die digitale Circular Economy (Fn. 28), S. 7.
79 *A.-C. Mittwoch*, Der digitale Produktpass der Ökodesign-Verordnung (Fn. 24), 66.
80 Für die Eintragung bereits durchgeführter Reparaturen vgl. Sachverständigenrat für Verbraucherfragen, Recht auf Reparatur, September 2022, S. 40.

Abs. 1 d), e) Ökodesign-VO nach offenen Standards und interoperabel gespeichert werden müssen.[81] Gleiches gilt für die Produktpässe selbst, die gem. Art. 11 a), b) Ökodesign-VO interoperabel mit anderen Produktpässen sein müssen sowie einen kostenlosen, einfachen Zugang für Stakeholder:innen ermöglichen sollten. Lediglich die „eindeutige Produktkennung" wird in einem zentralen europäischen Register gem. Art. 13 Abs. 1 Ökodesign-VO festgehalten, das zugleich über einen vereinfachten Zugang über ein vorgeschaltetes Webportal gem. Art. 14 Ökodesign-VO erreicht werden kann.

Hier ergibt sich also erstmals die Möglichkeit, interne und externe „virtuelle Welt" von Produkten zu verknüpfen. Allerdings ist zurzeit noch ungeklärt, wie weit die Durchführungs-Verordnungen Zugangsberechtigungen verschiedener Akteur:innen gemäß Art. 9 Abs. 2 lit. f Ökodesign-VO festlegen.[82] Der Produktpass ist in seinem jetzigen Zuschnitt *keine* „Open Data" Regelung für die Privatwirtschaft.[83] Wenngleich die Ökodesign-VO die tatsächliche Zuteilung der Rechte an die Durchführungs-VOen delegiert, spricht der Wortlaut des Art. 11 b) Ökodesign-VO doch für ein sehr weites Konzept von Stakeholder:innen.[84] Bei der steten Befürchtung der Industrie, umso mehr Geschäftsgeheimnisse zu gefährden, je detaillierter die zur Verfügung gestellten Daten sind, werden hier erhebliche Auseinandersetzungen geführt werden.[85] Im Sinne der oben herausgestellten Koordinationsmöglichkeiten einer Circular Economy, die auf gute und frei verfügbare Daten angewiesen ist, werden Abkapselungen schwer zu rechtfertigen sein. Es bleibt zu hoffen, dass die EU den Produktpass nicht als Zugangs-, sondern vielmehr als Bündelungsrecht sieht, in dem – ähnlich wie im oben dargestellten individualisierten Regime des Data Act – das Paradigma „access (for everyone) by design" gilt. Erst dann wäre eine Verschränkung von interner und externer virtueller Realität von Produkten möglich.

---

81 So auch *Piétron* u. a., Die digitale Circular Economy (Fn. 28), S. 15.

82 Zu erwartbaren Auseinandersetzungen mit verschiedenen Lobbygruppen siehe *C. Schucht*, Der digitale Produktpass, CB 2023, 176 (180).

83 *R. Kitchin*, The data revolution. Big data, open data, data infrastructures & their consequences, London 2. Aufl. 2021, S. 75.

84 „Kunden, Hersteller, Importeure, Vertreiber, Händler, fachlich kompetente Reparateure, unabhängige Wirtschaftsteilnehmer, Instandsetzungsbetriebe, Wiederaufbereitungsunternehmen, Recyclingunternehmen, Marktüberwachungs- und Zollbehörden, zivilgesellschaftliche Organisationen, Gewerkschaften und andere maßgebliche Akteure."

85 Hierzu kritisch *Piétron* u. a., Die digitale Circular Economy (Fn. 28), S. 24.

Die Regulierung des Wettbewerbs im Metaverse

Armin Mozaffari Jovein

A. Einleitung – Das Metaverse und der Wettbewerb

Die Entstehung von Big Tech-Unternehmen hat aufgezeigt, welchen Einfluss einige wenige Unternehmen auf den Wettbewerb in der Digitalwirtschaft haben können, denn diese Dienste können prinzipiell grenzüberschreitend und weltweit angeboten werden. Nicht zuletzt führte dies auch dazu, dass die EU den *Digital Markets Act* („DMA") ins Leben rief. Mit einem weitaus noch größeren Transformationspotenzial in der Digitalwirtschaft soll nach zahlreichen Prognosen durch das Metaverse zu rechnen sein. Gerade durch die eng damit verknüpften dezentral organisierten Strukturen stellen sich zahlreiche Fragen und es zeigt sich, dass herkömmliche Rechtsinstrumente und insbesondere der DMA bislang nicht auf den Wettbewerb im Metaverse bzw. das Metaverse als solches vorbereitet sind. Dieser Beitrag soll zunächst einen Einblick in das Metaverse und seine Regulierung geben und sodann das Metaverse in die Ordnung unseres Kartellrechts einordnen sowie Schwierigkeiten aufzeigen, mit denen zu rechnen ist.

I. Was ist das Metaverse?

1. Definition des Metaverse

Das Metaverse wurde das erste Mal 1992 von Neal Stephenson in dessen Science-Fiction-Roman „*Snow Crash*" erwähnt. Hinter ihm steckt die Idee beständiger, vollständig virtueller, einer einzelnen Instanz unterstellter und miteinander verbundener „Universen" mit „Metagalaxien", die als vereinende virtuelle Schicht über allem stehen, mit denen interagiert werden kann und die sich auf beinahe jeden Teil des menschlichen Lebens auswirken, wie etwa Arbeit und Freizeit, Selbstverwirklichung sowie körperliche Er-

tüchtigung, Kunst und Handel.[1] Etwas genauer betrachtet wird es überwiegend definiert als "*A massively scaled and interoperable network of real-time rendered 3D virtual worlds that can be experienced synchronously and persistently by an effectively unlimited number of users with an individual sense of presence, and with continuity of data, such as identity, history, entitlements, objects, communications, and payments.*"[2] Die EU-Kommission ergänzt die Definition in ihrer Mitteilung noch um die Aspekte künstliche Intelligenz, intelligente Umgebung, Internet der Dinge, Blockchain-Transaktionen und digitale sowie reale Objekte und Umgebungen, die alle vollständig integriert sind und miteinander kommunizieren.[3] Tatsächlich bezieht sich die EU-Kommission dabei aber eigentlich auf das von ihr als solches bezeichnete „Web 4.0", bezeichnet mit dem „Web 4.0" aber eigentlich das gleiche – mutmaßlich, um etwaigen negativen Assoziationen rund um den Hype um das Metaverse zu entgehen.

2. Architektur des Metaverse

In den gängigen Konzeptionen wird überwiegend davon ausgegangen, dass sich das Metaverse entweder in den Händen großer Technologieunternehmen entwickelt, die versuchen werden, das Metaverse geschlossen zu halten und eine möglichst große Marktmacht aufzubauen oder aber durch die Blockchain-Technologie getrieben offen und dezentralisiert organisiert, wodurch u.a. einzelne Unternehmen keine Kontrolle über das Metaverse erhalten können.[4] Zentral in der Unterscheidung verschiedener Metaverse-Modelle sind vor allem die Fragen nach Offenheit bzw. Geschlossenheit, nach Dezentralisierung bzw. Zentralisierung und nach der Interoperabilität.[5]

1 *M. Ball*, The Metaverse: And How It Will Revolutionize Everything, New York City, Norton, 2022, S. 3, 43.
2 Ebd. S. 29.
3 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 11.07.2023, EU-Initiative für das Web 4.0 und virtuelle Welten: mit Vorsprung in den nächsten technologischen Wandel, COM(2023) 445 final, S. 2.
4 *T. Madiega/P. Car/M. Niestadt*, Metaverse, Opportunities, risks and policy implications, PE 733.557, Brüssel 2022, S. 2.
5 Hierzu weiter unten siehe B.

a. Dezentralisierung und Zentralisierung

Dezentralisierung und Zentralisierung beschreiben im Zusammenhang von Organisationen und Netzwerken, wie und von wem Entscheidungen über das System selbst getroffen werden können. Während die Entscheidungsgewalt in zentralisierten Systemen in der Regel beim Betreiber einer Plattform liegt, gibt es in dezentralisierten Systemen eine solche zentrale Steuereinheit nicht und Entscheidungen werden stattdessen von einer Vielzahl an Personen getroffen.[6] Für das Metaverse wird dies dahingehend ein bedeutendes Thema, da es darüber entscheidet, wer schlussendlich relevante Entscheidungen über Einzelfragen treffen kann. Dies könnten daher entweder die Nutzer selbst, etwa in Form sog. „*Decentralized Autonomous Organizations*" („DAOs") oder aber lediglich einzelne Unternehmen sein, die als Anbieter eine Metaverse-Welt betreiben.

b. Offenheit und Geschlossenheit

Offenheit und Geschlossenheit beschäftigen sich hingegen mit der Frage, ob eine Plattform einen „*walled garden*" darstellt, zu dem der Betreiber durch Hardware, Software oder beides kontrolliert, wer Zugang erlangt und ob der Nutzer durch Endnutzerlizenzen und AGB in seinen Handlungsmöglichkeiten gebunden ist.[7] Offene Systeme kennen hingegen keine solchen Restriktionen und räumen etwa den Nutzern im Kontext des Metaverse Freiheit darüber ein, was sie tun und ermöglichen ihnen, ihre Daten, virtuellen Gegenstände, Währungen und Errungenschaften zu exportieren. Damit könnten Nutzer die in einer Metaverse-Welt erstellten Avatare und virtuellen Gegenstände – z.B. in Form sog. „*Non-Fungible Token*" („*NFT*") mitnehmen, tauschen und handeln.[8]

6 *EU Blockchain Observatory and Forum*, Blockchain-Enabled Virtual Worlds, abrufbar unter https://blockchain-observatory.ec.europa.eu/document/download/cfdfd2e3-d240-43f7-a7f9-f037020925c1_en?filename=Blockchain-EnabledVirtual%20WorldsReport_EUBOF.pdf, zuletzt abgerufen am 13.10.2024, S. 7.
7 Ebd. S. 22.
8 Ebd.

c. Interoperabilität

Interoperabilität als wohl wichtigste Komponente beschreibt die Fähigkeit, dass Computersysteme oder Softwares Informationen miteinander austauschen und diese auch verarbeiten können, was für das Metaverse eine große Bedeutung erhält, wenn Nutzer von einer Welt in die nächste reisen und ihre Daten und virtuellen Inhalte mit sich nehmen wollen.[9]

II. Anwendungsbereiche für das Metaverse

Die Anwendungsbereiche[10] für das Metaverse sind vielfältig und reichen von Arbeitsumgebungen, Videospielen, Tourismus, Mode, digitalen Zwillingen für Menschen und Unternehmen, neuen Vertriebsmöglichkeiten für Künstler bis hin zu neuen Gesellschaftsstrukturen mit den DAOs und sogar einem neuen Finanz- und Wirtschaftssystem, das auf Blockchain-Strukturen basiert und dadurch frei von der Notwendigkeit vertrauenswürdiger Intermediäre ist, da dessen Teilnehmer unmittelbar miteinander interagieren können. Damit wird das Metaverse weit mehr als nur einen spezifischen Anwendungsbereich betreffen und sowohl als soziales Medium und als Teil des Wirtschaftslebens auftreten.

B. Quo Vadis Metaverse?

Noch ist es nicht gewiss, wie sich das Metaverse entwickeln wird und es wird auch nach der Einschätzung vieler noch einige Jahre dauern, bis wir an einem Punkt angelangt sind, an dem man davon sprechen kann, dass es das Metaverse gibt, wie man es sich vorstellt.[11] Dennoch wird schon heute geschätzt, dass bis 2030 bis zu 800 Mrd. US-Dollar in das Metaverse inves-

9 *Ball*, The Metaverse (Fn.2), S. 37 f.

10 Einen Überblick über verschiedene Anwendungsbereiche gibt beispielsweise *T. Köhler/J. Finkeissen*, Chefsache Metaverse, Frankfurt a. M. 2023, S.101 ff.; zu den Einsatzfeldern des Industrial Metaverse siehe auch *L. Lautenbach*, Digitale Zwillinge von KRITIS, S. 126f.

11 McKinsey & Company, Value creation in the metaverse, 2022, abrufbar unter https://www.mckinsey.com/~/media/mckinsey/business%20functions/marketing%20and%20sales/our%20insights/value%20creation%20in%20the%20metaverse/Value-creation-in-the-metaverse.pdf, zuletzt abgerufen am 13.10.2024, S. 33.

tiert werden.[12] Nachfolgend sollen die verschiedenen möglichen Modelle des Metaverse etwas genauer erläutert und deren Auswirkungen auf die Regulierungsmöglichkeiten darlegen.

I. Das Metaverse als zentralisiertes und geschlossenes Ökosystem

In einer zentralisierten und geschlossenen Struktur werden die Geschäftsmodelle fortgeführt, die heute weitgehend zu erleben sind. Nach den Regeln des Wettbewerbs konkurrieren Unternehmen darin um die Nutzer und versuchen, ein möglichst attraktives Angebot zu gestalten.

Bekannt unter dem Begriff „*Big Tech*" ist es in der Digitalwirtschaft einer Handvoll Technologieunternehmen und insbesondere *Alphabet*, *Meta*, *Amazon*, und *Apple* allerdings gelungen, so groß zu werden, dass man an ihnen gar nicht mehr vorbeikommt. Begünstigt werden sie durch Skaleneffekte, Wechselkosten und Netzwerkeffekte, die dafür sorgen, dass sie ihre Marktstellung behalten können.[13] Besonders betroffen sind hiervon bislang die Bereiche Suchmaschinen, Soziale Medien, E-Commerce Marktplätze und Betriebssysteme.[14]

Diese Unternehmen haben damit ein großes Interesse daran, ihre Marktposition zu bewahren und selbst zu großen Betreibern eigener Metaverse-Angebote zu werden – so hat sich der ehemalige *Facebook*-Konzern extra in Anlehnung an das Metaverse in *Meta* umbenannt und damit einen Hype um das Metaverse ausgelöst.[15] Geht es daher nach den *Big Tech*-Unternehmen, führen sie ihre Geschäftsmodelle fort, die auf ihren zentralisierten und geschlossenen Strukturen beruhen. Zu diesem Zweck bauen diese Unternehmen ganze digitale Ökosysteme auf, die mehrere verschiedene benachbarte Märkte umspannen und damit Nutzer binden sowie Profite

12 Vgl. *Verified Market Research*, Metaverse Market Size By Product Type (Mobile Metaverse, Desktop Metaverse), By Applications (Game, Social, Conference, Content Creation, Online Shopping), By Geographic Scope And Forecast for 2024–2031, abrufbar unter https://www.verifiedmarketresearch.com/product/metaverse-market/, zuletzt abgerufen am 13.10.2024.

13 *I. Hupont Torres/V. Charisi/G. De Prato/K. Pogorzelska/S. Schade/A. Kotsev/M. Sobolewski/N. Duch Brown/E. Calza/C. Dunker/F. Di Girolamo/M. Bellia/J. Hledik/I. Nai Fovino/M. Vespe,* Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU, Luxemburg 2023, JRC133757, S. 59.

14 Ebd.

15 Vgl. https://about.fb.com/news/2021/10/facebook-company-is-now-meta/, zuletzt abgerufen am 13.10.2024.

durch eine Optimierung der Datennutzung maximieren sollen.[16] Digitale Ökosysteme werden nämlich als eine Anzahl von Unternehmen, Wettbewerbern und Komplementären definiert, die zusammenarbeiten, um einen neuen Markt zu schaffen und Waren und Dienstleistungen von Wert für die Kunden zu produzieren.[17]

Im Kontext des Metaverses haben diese Unternehmen in der Regel wenig bis kein Interesse daran, den Nutzern durch eine Öffnung ihrer Ökosysteme und die Interoperabilität durch technische Standards den Wechsel zwischen verschiedenen Metaverse-Welten unterschiedlicher Anbieter zu ermöglichen, ebenso wenig wie den Nutzern echte Inhaberrechte an digitalen Gegenständen in Form handelbarer NFT o.ä. einzuräumen. Vielmehr könnte die riesige Menge an Daten, die im Metaverse generiert werden, Abschottungseffekte und damit auch Marktstellungen verschärfen – wettbewerbliche sowie datenschutzrechtliche Herausforderungen inklusive.[18] Dass es schon heute große Probleme mit der Marktmacht einiger Unternehmen in der Digitalwirtschaft gibt, zeigt sich nicht zuletzt dadurch, dass viele Kartellbehörden digitale Ökosysteme schon länger im Blick haben[19] und es die EU sogar zum Anlass nahm, hiergegen vorzugehen und den DMA ins Leben zu rufen.

II. Das Metaverse als dezentralisiertes und offenes Ökosystem

Folgt das Metaverse jedoch einem dezentralisierten und offenen Ansatz, können einzelne Unternehmen erst gar keine solchen Marktpositionen erlangen. Dem dezentralisierten und offenen Modell liegt in der Regel nämlich die Nutzung der Blockchain-Technologie zugrunde, wodurch es überhaupt keine zentrale Ordnungsinstanz in Gestalt einzelner Akteure geben kann. Vielmehr sind die Nutzer frei darin zu entscheiden, was sie mit ihren Daten und vor allem den von ihnen erstellten, erlangten oder erworbenen digitalen Gegenständen machen. Als Instanz hinter Metaverse-Welten können aber auch DAOs agieren, die den Nutzern die konkrete

16 *Hupont et al.*, Next Generation Virtual Worlds (Fn. 14), S. 59.

17 *T. Hazlett/D.Teece/L. Waverman,* Walled Garden Rivalry: The Creation of Mobile Network Ecosystems, George Mason Law & Economics Research Paper No. 11–50, 2011, S. 7.

18 Ebd. S. 59 f.; *Ball*, The Metaverse (Fn. 2), S. 17.

19 Arbeitsunterlagen der Kommissionsdienststellen zur Evaluation der Bekanntmachung über die Definition des relevanten Marktes, SWD(2021) 199 final, S. 81.

Mitbestimmung über Anliegen durch Abstimmungen ermöglichen. Nutzer können zwischen verschiedenen Metaverse-Welten unterschiedlicher Anbieter hin und her reisen, was durch eine technologische Interoperabilität und die offenen Strukturen gewährleistet wird. Unternehmen können durch die offene Struktur einfacher zusätzliche Dienste entwickeln und technisch integrieren, ohne dass es irgendwelche Abschottungen durch einzelne Anbieter von Metaverse-Welten gibt. Durch diese Ermöglichung eines plattformübergreifenden Austausches könnten positive Netzwerkeffekte miteinander verbundener Netzwerke erzielt werden.[20]

Das Wirtschafts- und Finanzsystem basiert hier insbesondere auf der sog. „*Decentralized Finance*" („*DeFi*"), die es den Nutzern, repräsentiert durch ihre Avatare, ermöglicht direkt ohne Einschaltung eines intermediäres, wie einer Bank, Geld bzw. Krypto-Token vertrauenswürdig miteinander auszutauschen und virtuelle Gegenstände als NFT selbst zu erstellen und über NFT-Marktplätze auf Grundlage von „*Smart Contracts*" zu handeln.[21]

Entwickelt sich das Metaverse nach dem dezentralisierten Modell, könnte hieraus eine echte weltweite Metaverse-Wirtschaft entstehen, die weitgehend von der realen Welt abgekoppelt ist. Der Wettbewerb würde hier – die Frage der konkreten zukünftigen technologischen Umsetzbarkeit außen vor – zwischen verschiedenen Ökosystemen mit ihren ggf. eigenen Regeln und Dienstanbietern bestehen und den Nutzern eine echte Wahlfreiheit und Wechselmöglichkeit einräumen. Auch Anbieter selbst könnten in den dezentralisierten Strukturen und dem grundsätzlich global ausgerichteten Angebot womöglich leichter Fuß fassen, sofern sie die Nutzer von ihrem Angebot überzeugen können. Gleichzeitig stellen sich auch hier Fragen insbesondere zu zahlreichen missbräuchlichen Verhaltensweisen, etwa der Selbstbevorzugung, der Fusionskontrolle und vor allem der Rechtsdurchsetzung sowie der Findung globaler Standards bzw. Regelungen zur Ermöglichung einer Metaverse-Wirtschaft, die über bloße Transaktionen hinaus geht. Zwar adressiert der DMA bereits einiges, hat selbst aber schon sehr hohe Aufgreifschwellen.

---

20 *Hupont et al.*, Next Generation Virtual Worlds (Fn. 14), S. 61.

21 Dazu auch *EU Blockchain Observatory and Forum*, Trend Report of Virtual Worlds (Metaverse), Brüssel 2024, abrufbar unter https://blockchain-observatory.ec.europa.eu/document/download/eccf0cf2-4fc8-469c-8e6b-91fe61d77e74_en?filename=May_2024_Virtual_Worlds_Trends_Report_Final.pdf, zuletzt abgerufen am 13.10.2024, S. 4 f.

III. Die Koexistenz beider Modelle

Beide Modelle bringen ihre eigenen Vor- und Nachteile mit sich. Geschlossene und zentralisierte Systeme funktionieren häufig reibungsloser, da sie ihre eigenen Dateiformate, Softwares, Grafiken und Standards verwenden können. Soll die Interoperabilität zwischen verschiedenen Metaverse-Welten aber gelingen, wie es für offene und dezentralisierte Systeme notwendig ist, braucht es einer Vielzahl verschiedener Standards für Daten und virtuelle Inhalte, wie Daten-/Asset-Austausch-Programmierschnittstellen („*API*"), die Integration physischer/virtueller Welten, Avatare und Charaktere, Identität, Cybersicherheit, Datenschutz, Vernetzungsprotokolle, Metadaten und die Auffindbarkeit von Datenbeständen.[22]

Es ist daher nicht unwahrscheinlich, dass sich beide Metaverse-Modelle gleichzeitig weiterentwickeln und damit unterschiedliche Angebote für verschiedene Bedürfnisse machen.[23] Gleichzeitig ist unklar, ob und inwieweit die verschiedenen Modelle dann miteinander integrierbar wären und welche unterschiedlichen Herausforderungen sich in der Regulierung der beiden Modelle ergeben.

IV. Welche Auswirkungen die Geschäftsmodelle mit sich bringen

Vor allem das dezentralisierte Metaverse-Modell auf Basis der Blockchain-Technologie und mit einer möglichen Metaverse-Wirtschaft kollidiert mit grundsätzlichen Erwägungen unseres geltenden Rechts. Der Rechtsausschuss des EU-Parlaments hat dies bereits in ähnlicher Weise beschrieben und als nicht wünschenswert erachtet.[24] Die Dezentralität der fälschungs- und zensursicheren Blockchain verhindert nämlich, dass der Staat gemäß dem Territorialitätsprinzip durch seine Staatsgewalt auch wie im heutigen Internet sein Recht durchsetzt, zumal im Metaverse auch das Recht sämtlicher Staaten aufeinanderträfe. Geht man nämlich von der grundsätzlichen

22 Vgl. https://metaverse-standards.org/domain-groups/, zuletzt abgerufen am 13.10.2024.

23 *Hupont et al.*, Next Generation Virtual Worlds (Fn. 14), S. 61.

24 *Rechtsausschuss des EU-Parlaments*, Entwurf eines Berichts über die Auswirkungen der Entwicklung virtueller Welten auf die Politik – Fragen im Zusammenhang mit dem Zivilrecht, dem Unternehmensrecht, dem Handelsrecht und dem Recht des geistigen Eigentums, 10.10.2023, (2023/2062(INI)), PE753.772v01–00, S. 11.

Definition von *Georg Jellinek* zur Staatlichkeit aus, so braucht ein Staat einerseits Staatsgewalt, ein Staatsgebiet und ein Staatsvolk.[25]

Mit Blick auf die Souveränität anderer Staaten greift ein Staat daher auf das Staatsgebiet und das Staatsvolk als Anknüpfungspunkte zurück, um Recht zu setzen und durchzusetzen. In einem Metaverse in dem sich Nutzer jedoch anonym oder pseudonym bewegen können, das womöglich keine Unternehmen mit einem Sitz in der physischen Welt hat, die adressiert werden könnten, und das sich vollständig in einem virtuellen Raum und damit außerhalb jeglichen Staatsgebiets befindet, fallen jedoch beide Hauptanknüpfungspunkte für staatliche Eingriffe weg. Selbst wenn ein einzelner Staat versuchen sollte, sein Recht im Metaverse durchzusetzen, trifft er auf die Schwierigkeit, dass andere Staaten dasselbe versuchen wollten und es damit zu einem direkten Konflikt zwischen sich ggf. im Konflikt befindenden Rechtsordnungen käme. Gleiches gilt auch mit Blick auf die Grundrechte von Nutzern, auf die sie sich berufen wollen, in denen sie aber zugleich von einem fremden Staat eingeschränkt werden. Diese Konflikte lassen sich weiterdenken bis hin zu Fragen des Konzepts von Eigentum im Metaverse, der Rolle und Souveränität von Staaten, der Geltung, Gestaltung und Durchsetzung von Recht, Verantwortlichkeiten von Nutzern und vielem mehr.[26]

Für das zentralisierte, geschlossene Metaverse-Modell lässt sich weiterhin eine zentrale Instanz bestimmen, die Adressat staatlicher Maßnahmen zur Durchsetzung von Recht sein kann. Dennoch verschärfen sich auch hier bestehende Konflikte, wie man sie aus dem heutigen Internet im Zusammenhang mit der Rechtsdurchsetzung kennt.

In nicht gekanntem Ausmaß zeigt sich damit mit dem Metaverse erneut der ewige Konflikt von Recht und Technologie und verschiebt weiterhin die bisherigen Grenzen.

---

25 *G. Jellinek, Allgemeine Staatslehre*, Berlin, 1905, S. 381–420.

26 Dazu auch *S. Koos,* Legal Aspects of the Metaverse – virtual reality and virtual Objects, in: Y. Dwivedi/L. Hughes/A. Baabdullah/S. Ribeiro-Navarrete/M. Giannakis/M. Al-Debei/D. Dennehy/B. Metri/D. Buhalis/C. Cheung/K. Conboy/R. Doyle/R. Dubey/V. Dutot/R. Felix/D. Goyal/A. Gustafsson/C. Hinsch/M. Janssen/Y.-G. Kim/J. Kim/S. Koos/D. Kreps/K. Nir/V. Kumar/K.-B. Ooi/S. Papagiannidis/I. Pappas/A. Polyviou/S.-M. Park/N. Pandey/M. Queiroz/R. Raman/P. Rauschnabel/A. Shirish/M. Sigala/K. Spanaki/G. Tan/M. Tiwari/G. Viglia/S. Wamba. Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management. Vol. 66, 102542, Brownsville 2022, S. 11 ff.

C. Die Wettbewerbsregulierung im Metaverse

I. Erwägungen zur Metaverse-Regulierung

Damit stellt sich insbesondere mit Blick auf den Wettbewerb auch die Frage, was der Staat und konkret die EU überhaupt tun kann bzw. sollte, um positiv auf die Metaverse-Wirtschaft sowie deren Wettbewerb einzuwirken. Erfolgt eine staatliche Regulierung zu früh und zu stark, gerät man womöglich in die Gefahr, positive Entwicklungen zu ersticken oder Unternehmen aus dem eigenen Einflussbereich abwandern zu lassen mit der Folge, technologisch erneut wie mit der Entwicklung des Internets abgehängt zu werden. Auch die Frage, ob man sich erneut auf den Eintritt des „Brüssel-Effekts" verlassen kann, ist ungewiss. Unter dem „Brüssel-Effekt" versteht man das Phänomen, dass weltweit Regelungen und Standards der EU von Drittstaaten *de jure* oder von Unternehmen aus Drittstaaten *de facto* übernommen werden, da es für sie vorteilhafter ist, weltweit einheitlich strenge europäische Standards anzuwenden, als unterschiedliche Standards je nach Jurisdiktion.[27] Erfolgt eine staatliche Regulierung jedoch zu spät, kann sich das Metaverse aber bereits unerwünscht und vor allem wettbewerbsschädlich entwickelt haben.

Aus technologischer Sicht spricht für eine frühzeitige Regulierung insbesondere, dass es sich bei dem Metaverse überwiegend um ein technologisches Phänomen handelt und die technologische Architektur des Metaverse einen direkten Einfluss auf die Funktionsweise der übergeordneten regulierenden Strukturen hat. Diese muss sich aber auch in der technologischen Umgebung widerspiegeln, um ihre Wirkung entfalten zu können.[28]

Rechtspolitisch spricht für die frühzeitige Regulierung, dass rechtsfreien bzw. anarchischen Zuständen vorgebeugt werden kann, indem noch ungeklärte Sachverhalte eine rechtliche Verankerung erhalten können. Hierzu gehört beispielsweise die vollständige Anonymisierung oder Pseudonymisierung, ohne dass Aufenthalts-, Wohn-, oder Handlungsort und Staatsangehörigkeit festgestellt werden können.

Wirtschaftlich spricht für eine frühzeitige Regulierung, dass es schon jetzt Versuche der großen Technologieunternehmen gibt, ihre Geschäfts-

27 Vgl. *A. Bradford*, The Brussels Effect, Northwestern University Law Review, Vol. 107, No. 1, Columbia Law and Economics Working Paper No. 533, New York City 2012, S. 6.

28 *Hupont et al.*, Next Generation Virtual Worlds (Fn. 14), S. 66.

modelle auf das Metaverse zu übertragen. Sollte dies gelingen, ersticken möglicherweise alle Versuche, alternative Modelle des Metaverse zu gestalten und den weiteren Ausbau ihrer Marktstellungen im Metaverse zu verhindern. Die Folge wäre ein von Beginn an eingeschränkter Wettbewerb, geschlossene, zentralisierte Ökosysteme und eine Marktmacht, die es diesen Technologieunternehmen ermöglichen würde, de facto Standards zu setzen und zugleich innovative Entwicklungen zu beschränken. Weitere mögliche Resultate wären die Erlangung von Stellungen als Torwächter im Metaverse, eine weitere Ausnutzung von Netzwerkeffekten und die Beschränkung von Wettbewerb durch zudem sehr hohe Marktzutrittsschwellen für potenzielle Wettbewerber.[29]

Dennoch muss darauf geachtet werden, dass eine erste frühzeitige Regulierung auf die notwendigen Rahmenbedingungen beschränkt sein muss, um den Wettbewerb und die wirtschaftliche Entwicklung nicht übermäßig zu beeinträchtigen. Greift man nämlich zu früh zu restriktiv ein, sinkt die Akzeptanz von Gesetzen und Unternehmen wandern aus dem eigenen Einflussbereich ab. Damit verlieren restriktive Regulierungen an Wirkung mangels Einflussmöglichkeiten. Im schlimmsten Fall führt dies sogar dazu, dass sich Geschäftsmodelle und Entwicklungen fest etablieren und nur noch deren Akzeptanz als Option übrigbleibt, um nicht außen vor zu bleiben.

Eine solche Entwicklung ist mit Blick auf die derzeitigen Ankündigungen der EU allerdings schon heute nicht undenkbar. Der gesamten Digitalstrategie der EU[30] und insbesondere auch ihrer „Initiative für das Web 4.0 und virtuelle Welten"[31] liegt nämlich der Grundsatz zugrunde, dass online wie offline die gleichen Rechte gelten sollen und keine parallele Wirtschaft durch das Metaverse entstehen können soll.[32] Versucht die EU jedoch einseitig ein weltweit auftretendes Phänomen zu regulieren und diesem ihre Gesetze aufzudrücken, tritt sie damit in Konflikt mit anderen Staaten, die etwas gleiches unternehmen wollen. Insbesondere gerät sie damit in

29 Dazu auch *EU-Kommission*, Mitteilung über eine Initiative der Europäischen Union für das Web 4.0 und virtuelle Welten (Fn. 4), S. 12.

30 Siehe bspw. die Europäische Erklärung zu den digitalen Rechten und Grundsätzen für die digitale Dekade vom 26.01.2022, COM(2022) 28 final, S. 2.

31 *EU-Kommission*, Mitteilung über eine Initiative der Europäischen Union für das Web 4.0 und virtuelle Welten (Fn. 4).

32 *Binnenmarkt- und Verbraucherschutzausschuss des EU-Parlaments*, Entwurf eines Berichts, Virtuelle Welten – Chancen, Risiken und politische Auswirkungen in Bezug auf den Binnenmarkt vom 04.08.2023, (2022/2198(INI)), PE751.902v02–00 Rn. 17–19.

Gefahr, dass dieser Gleichklang on online und offline – wenn auch gut gemeint – negative Auswirkungen auf die Entwicklung des Metaverse hat. Dies könnte damit zu einem möglicherweise paradoxen Ergebnis für die EU führen.

Dabei kann sich die EU auch nicht unbedingt auf den „Brüssel-Effekt" berufen, der jedoch häufig von ihr angeführt wird.[33] Schon mit der Umsetzung des AI-Acts und des DMAs zeigt sich, dass die strengen Vorgaben der EU sich auch negativ auf den Wettbewerb und die Verbraucher auswirken können. So kündigte beispielsweise das Unternehmen *Apple* an, seine KI-Integration *Apple Intelligence* in das neue Betriebssystem iOS 18 nicht in der EU anbieten zu wollen.[34] Dabei ist *Apple* mit seinen Bedenken unter den großen Technologieunternehmen nicht allein. Besonders ein Bestreben, ein etwaig entstehendes eigenes Wirtschaftssystem im Metaverse von Anfang an zu unterbinden, könnte sich negativ auf die wirtschaftliche Entwicklung und die Regulierung der EU auswirken. Genau ein solches Wirtschaftssystem könnte aber eigentlich den größten Mehrwert des Metaverse ausmachen.

II. Das Kartellrecht und das Metaverse

Nachfolgend soll auf die Besonderheiten der Metaverseregulierung im Wettbewerb eingegangen werden. Zu diesem Zweck werden die drei Säulen des Kartellrechts, namentlich das Kartellverbot, Missbrauchsverbot und Fusionskontrolle, betrachtet, um einen überblicksweisen Einblick in die Herausforderungen zu geben, die sich durch das Metaverse ergeben können.

1. Das Kartellverbot nach Art. 101 Abs. AEUV

Das Kartellverbot nach Art. 101 Abs. 1 AEUV verbietet alle Vereinbarungen zwischen Unternehmen, Beschlüsse von Unternehmensvereinigungen und aufeinander abgestimmte Verhaltensweisen, welche den Handel zwi-

33 Siehe bspw. *M. Niestadt/J. Reichert*, The global reach of the EU's approach to digital transformation, PE 757.632, Brüssel 2024, abrufbar unter https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757632/EPRS_BRI(2024)757632_EN.pdf, zuletzt abgerufen am 13.10.2024, S. 2 ff.

34 Vgl. https://www.apple.com/de/newsroom/2024/09/apple-intelligence-comes-to-iphone-ipad-and-mac-starting-next-month/, zuletzt abgerufen am 13.10.2024.

schen den Mitgliedstaaten zu beeinträchtigen geeignet sind und eine Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs innerhalb des Binnenmarktes bezwecken oder bewirken. Dies betrifft insbesondere die Festsetzung von Preisen oder sonstigen Geschäftsbedingungen (lit. a), die Einschränkung oder Kontrolle des Absatzes, der technischen Entwicklung oder der Investitionen (lit. b), die Aufteilung von Märkten oder Versorgungsquellen (lit. c), die benachteiligende Anwendung unterschiedlicher Bedingungen bei gleichwertiger Leistung gegenüber Handelspartnern (lit. d) sowie die Koppelung von Leistungen ohne sachlichen Grund (lit. e).

a. Verhaltenskoordinierung zwischen Unternehmen

Eine kartellrechtliche Vereinbarung erfordert nach ständiger Rechtsprechung,[35] dass die beteiligten Unternehmen einen gemeinsamen Willen ausdrücken, sich auf einem Markt in einer bestimmten Weise zu verhalten. Dies kann schriftlich, mündlich oder konkludent erfolgen. Auch sogenannte „*gentlemen's agreements*", informelle Absprachen oder solche, die unter Einschaltung von Dritten erfolgen, fallen darunter. Einseitige Handlungen werden in der Regel nicht als Vereinbarungen im Sinne des Art. 101 AEUV gewertet, wenn sie nicht eine stillschweigende Aufforderung zur Zusammenarbeit beinhalten. Relativ neu in der kartellrechtlichen Betrachtung sind auch Algorithmen, insbesondere dynamische Preissetzungsalgorithmen, die Wettbewerbsinformationen sammeln und sich anpassen können.[36] Diese können, wie im Fall „*United States v. Topkins*" gezeigt, ebenfalls zur Koordinierung von Kartellen verwendet werden.[37]

Das Metaverse stellt auch das Kartellrecht vor neue Herausforderungen. Vereinbarungen können hier möglicherweise durch *Smart Contracts* automatisiert werden, welche insbesondere in DAOs Anwendung finden. Solche Verträge werden unter Zugrundelegung von „Wenn-Dann"-Bedingungen so programmiert, dass sie sich bei Eintritt dieser Bedingungen

35 *P. Stockenhuber*, in: *E. Grabitz/M. Hilf/M. Nettesheim* (Hrsg.), Recht der Europäischen Union, Band EUV/AEUV, München, Rechtsstand August 2023 Rn. 91 ff. m.w.N.

36 Commission Staff Working Document Accompanying the Final report on the E-commerce Sector Inquiry, Brüssel, 10.05.2017, SWD(2017) 154 final, Teil 1/2 Rn. 603 ff.

37 United States of America v. David Topkins, No. 3:15-cr-00201-WHO (N.D. Cal. Apr. 30, 2015).

automatisiert ausführen, also ohne weiteres menschliches Zutun.[38] Dies gilt sowohl für horizontale Absprachen zwischen verschiedenen Plattformen und Dienstleistern als auch für vertikale Vereinbarungen zwischen Plattformen und Händlern. Hier spielen KI und Algorithmen womöglich noch eine stärkere Rolle bei der Überwachung und Durchsetzung von Preis- und Verhaltensabsprachen. *Smart Contracts* bieten im Wettbewerb dabei einerseits Transparenz und Nachvollziehbarkeit, andererseits aber auch wettbewerbsrechtliche Risiken. Auf öffentlichen Blockchains könnten sensible Transaktionsdaten wie Preise und Mengen offengelegt und von Wettbewerbern genutzt werden, was zu einer unzulässigen Koordinierung führen könnte.[39] Eine generelle Offenlegung solcher Informationen könnte daher einen Verstoß gegen Art. 101 Abs. 1 AEUV darstellen.[40] Andererseits wäre bei privater Blockchain-Nutzung eine strengere Koordinierung zwischen wenigen Akteuren möglich, was durch eine erhöhte Kartelldisziplin der Beteiligten ebenfalls kartellrechtlich ein Problem darstellen könnte. Maßnahmen wie wechselnde *Wallet*-Adressen oder eingeschränkter Zugriff auf *Smart Contract*-Details könnten solche Risiken zwar mindern, erfordern derzeit jedoch noch technische Weiterentwicklung.

b. Wettbewerbsbeschränkungen

Das Verbot von Wettbewerbsbeschränkungen ist das zentrale Element des Kartellrechts, verankert in Art. 101 Abs. 1 AEUV. Es untersagt alle Verhaltensweisen, die den Wettbewerb verhindern, einschränken oder verfälschen und auf Vereinbarungen, Beschlüsse oder abgestimmte Verhaltensweisen zurückzuführen sind.[41] Eine Wettbewerbsbeschränkung liegt im Wesentlichen dann vor, wenn die wirtschaftliche Handlungsfreiheit eines Unternehmens beeinträchtigt wird und es seine Entscheidungen nicht mehr autonom treffen kann.[42] Ausnahmen bestehen aber etwa, wenn der Handlungsspielraum durch staatliche Maßnahmen eingeschränkt wird.[43]

38 Vgl. https://www.coinbase.com/de/learn/crypto-basics/what-is-a-smart-contract, zuletzt abgerufen am 13.10.2024.
39 *T. Schrepel*, Collusion by Blockchain and Smart Contracts, 33 Harv. J.L. & Tech. (2019), 117 (130 f.).
40 Ebd.
41 *Stockenhuber* (Fn.36), Rn. 116.
42 Vgl. beispielsweise EuGH ECLI:EU:C:1975:174, Rn. 173.
43 Vgl. EuGH ECLI:EU:T:1996:120, Rn. 65.

Der kartellrechtlich geschützte Wettbewerb umfasst sowohl den horizontalen Wettbewerb zwischen Unternehmen auf derselben Marktstufe als auch den vertikalen Wettbewerb zwischen Akteuren auf vor- und nachgelagerten Marktstufen.[44] Dazu gehören beispielsweise Preisgestaltung, Produktauswahl, Forschung und Entwicklung, Vertriebswege u. v. m.[45] Auch der potenzielle Wettbewerb wird durch das Kartellrecht geschützt. Dabei kann es sich beispielsweise um die Erschwerung eines Markteintritts durch Vereinbarungen handeln.[46]

Eine Wettbewerbsbeschränkung kann entweder bezweckt oder bewirkt werden. Wenn das Ziel einer Maßnahme klar darauf abzielt, den Wettbewerb einzuschränken, ist keine weitere Auswirkungsprüfung erforderlich. Typische Beispiele sind Preisabsprachen oder die Aufteilung von Märkten, vgl. Art. 101 Abs. 1 lit. a), c) AEUV. Bei einer bewirkten Wettbewerbsbeschränkung hingegen muss eine Marktanalyse zeigen, dass die Maßnahme wahrscheinlich negative Auswirkungen auf den Wettbewerb hat, etwa auf Preise oder Produktionsmengen.[47]

c. Freistellungsmöglichkeiten

Vereinbarungen, die eine Wettbewerbsbeschränkung bezwecken oder bewirken, können unter bestimmten Voraussetzungen nach Art. 101 Abs. 3 AEUV vom Kartellverbot ausgenommen werden, wenn ihre positiven Auswirkungen die negativen Auswirkungen überwiegen, so etwa durch die Verbesserung der Produktion oder die Förderung des technischen Fortschritts.[48] Der europäische Gesetzgeber hat dazu verschiedene Gruppenfreistellungsverordnungen (GVO) erlassen, wie die Vertikal-GVO,[49] die

44 *Stockenhuber* (Fn.36), Rn. 132.
45 Ebd. Rn. 126.
46 Ebd. En. 134.
47 Leitlinien zur Anwendung von Artikel 81 Absatz 3 EG-Vertrag, (2004/C 101/08), Rn. 24 ff.
48 Ebd. Rn. 33.
49 Verordnung (EU) 2022/720 der Kommission vom 10.05.2022 über die Anwendung des Artikels 101 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union auf Gruppen von vertikalen Vereinbarungen und abgestimmten Verhaltensweisen (ABl. L 134 S. 4).

Forschungs-und-Entwicklungs-GVO[50] und die Technologie-Transfer Verordnung,[51] die erleichtern sollen, solche Ausnahmen zu identifizieren.

d. Kartellverstöße

Besonderes Risiko dafür, einen Kartellverstoß im Metaverse zu begründen, bieten solche Blockchains, die den Informationsaustausch zwischen Marktteilnehmern durch die öffentliche Einsehbarkeit fördern.[52] „*Hardcore*"-Verstöße können etwa in Preisabsprachen auf Metaverse-Plattformen, bei NFTs oder Kryptowährungen auftreten. Auch die Zusammenarbeit von Wettbewerbern auf horizontaler Ebene bei der Forschung und Entwicklung oder der Standardsetzung für Interoperabilität, z.B. etwa durch Verbände wie die *OpenMetaverseAlliance*,[53] birgt Risiken. Diese Standards sind jedoch entscheidend, um ein interoperables Metaverse überhaupt zu ermöglichen und den Wettbewerb zu fördern. Doch auch sie können unter Umständen einen Kartellverstoß begründen. Denkbar ist zudem die Freistellung nach Art. 101 Abs. 3 AEUV etwa dadurch, dass die Standardsetzungsprozesse Vorteile für den Markt und die Verbraucher bringen, indem sie technische Interoperabilität fördern.[54] Gleichzeitig muss dabei jedoch gewährleistet werden, dass diese Vereinbarungen nicht zu Marktabschottungen oder dem Ausschluss von Wettbewerbern führen. Dann wäre eine Freistellung gemäß Art. 101 Abs. 3 AEUV nicht weiter möglich.

50 Verordnung (EU) 2023/1066 der Kommission vom 01.06.2023 über die Anwendung des Artikels 101 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union auf bestimmte Gruppen von Vereinbarungen über Forschung und Entwicklung (ABl. L 143 S. 9).

51 Verordnung (EU) Nr. 316/2014 der Kommission vom 21.03.2014 über die Anwendung von Artikel 101 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union auf Gruppen von Technologietransfer-Vereinbarungen (ABl. L 93 S. 17).

52 *M. Holm-Hadulla/M. Raible/A. Schüssel*, Kartellrecht, in: *E. Wagner/M. Holm-Hadulla/M. Ruttloff* (Hrsg.), Metaverse und Recht, München 2023, S. 663 f. m.w.N.

53 Vgl. https://www.oma3.org, zuletzt abgerufen am 13.10.2024.

54 Zu den einzelnen Standards siehe *OpenMetaverseAlliance*, OMA3 – Portals Unleashed – Creating a teleportation standard to connect the metaverse, abrufbar unter https://assets-global.website-files.com/62a8cfee4d1b8a5209c0fd7b/652d49c3babc06adc2577c61_64cadf84bea1b9754676c2e1_OMA3%20Portals.pdf, zuletzt abgerufen am 13.10.2024, S. 7 ff.

2. Das Missbrauchsverbot nach Art. 102 AEUV

Das Missbrauchsverbot nach Art. 102 AUEV ist die zweite Säule des Kartellrechts. Art. 102 Abs. 1 AEUV erklärt die Fälle mit dem Binnenmarkt für unvereinbar und verboten, in denen ein oder mehrere Unternehmen auf einem bestimmten Markt oder auf einem wesentlichen Teil desselben eine beherrschende Stellung innehaben, diese missbräuchlich ausnutzen und dies dazu führen kann, dass der Handel zwischen den Mitgliedstaaten beeinträchtigt wird. Art. 102 Abs. 2 AEUV nennt als Regelbeispiele eines Missbrauchs insbesondere die unmittelbare oder mittelbare Erzwingung von unangemessenen Einkaufs- oder Verkaufspreisen oder sonstigen Geschäftsbedingungen (sog. Ausbeutungsmissbrauch, lit. a), die Einschränkung der Erzeugung, des Absatzes oder der technischen Entwicklung zum Schaden der Verbraucher (lit. b), die Anwendung unterschiedlicher Bedingungen bei gleichwertigen Leistungen gegenüber Handelspartner, wodurch diese im Wettbewerb benachteiligt werde (lit. c) und die an den Abschluss von Verträgen geknüpfte Bedingung, dass die Vertragspartner zusätzliche Leistungen annehmen, die weder sachlich noch nach Handelsbrauch in Beziehung zum Vertragsgegenstand stehen (sog. Koppelungsgeschäfte, lit. d).

a. Marktabgrenzung im Metaverse

Die Marktabgrenzung im Metaverse erfordert die Identifizierung und Abgrenzung der relevanten sachlichen und räumlichen Märkte, um zu ermitteln, welchen Wettbewerbskräften Unternehmen ausgesetzt sind. Grundlage hierfür ist das „Bedarfsmarktkonzept". Der jeweils zu betrachtende sachlich relevante Produktmarkt umfasst danach sämtliche Erzeugnisse und/oder Dienstleistungen, die von den Verbrauchern hinsichtlich ihrer Eigenschaften, Preise und ihres vorgesehenen Verwendungszwecks als austauschbar oder substituierbar angesehen werden.[55] Die Europäische Kommission greift dabei oft auf den „*SSNIP*"-Test („*small but significant and nontransitory increase in price*") zurück, um die Reaktion der Verbraucher auf eine hypothetische Preiserhöhung zu analysieren. Handelt es sich allerdings um digitale Märkte mit unentgeltlichen Leistungen („*zero-price*"-Märkte), ist

55 Arbeitsunterlagen der Kommissionsdienststellen zur Evaluation der Bekanntmachung über die Definition des relevanten Marktes, SWD(2021) 199 final Rn. 2.

dieser Test nur schwierig anzuwenden.[56] Digitale Plattformen, insbesondere mehrseitige Märkte, erschweren dabei nämlich die Abgrenzung aufgrund von Netzwerkeffekten.[57] Dies trifft besonders auch auf Digitale Ökosysteme zu, da sie die Natur des Wettbewerbs in Bezug auf die einzelnen Dienstleistungen, die diese gebündelten Angebote integrieren, verändern.[58] Dabei spielen auch solche Faktoren wie die Offenheit bzw. Geschlossenheit und Interoperabilität eine wichtige Rolle. Geringe Interoperabilität führt nämlich regelmäßig zu hohen Wechselkosten sowie *Lock-in*-Effekte der Verbraucher.[59] Offene Ökosysteme ermöglichen grundsätzlich größere Wettbewerbseffekte, da sie mehr Zugang und Kompatibilität zwischen den Komponenten bieten. Geschlossene Systeme können hingegen Innovation durch bessere Nutzerkoordination und technische Kompatibilität fördern.[60] Es liegt daher nahe, insbesondere auf solche Effekte wie die Offenheit bzw. Geschlossenheit und die Interoperabilität, aber auch die Zentralisierung bzw. Dezentralisierung, als zentrale Kriterien für die sachliche Marktabgrenzung zurückzugreifen.

In Bezug auf die räumliche Marktabgrenzung ist beim Metaverse regelmäßig ein globaler Markt oder jedenfalls binnenmarktweiter Markt anzunehmen, insbesondere bei offenen und interoperablen Plattformen. Eine engere räumliche Abgrenzung ist jedoch möglich, etwa wenn Produkte oder Dienstleistungen spezifisch geografische Zielgruppen ansprechen und sich von anderen Zielgruppen unterscheiden.

b. Marktbeherrschende Stellung

Nachdem der sachlich und räumlich relevante Markt abgegrenzt wurde, wird die Marktmacht der Unternehmen untersucht. Hierbei werden Marktgröße, Verkaufszahlen, Markteintrittsschranken und Marktanteile berück-

56 *A. Fuchs*, in: *U. Immenga/E. Mestmäcker* (Hrsg.), Wettbewerbsrecht, Band 1, Art. 102 AEUV, München 2019, Rn. 51, 52.
57 *Holm-Hadulla*, Metaverse und Recht (Fn. 49), Rn. 683.
58 Definition des relevanten Marktes (Fn. 56), S.14, 81.
59 *European Commission – Directorate-General for Competition*, Support study accompanying the evaluation of the Commission notice on the definition of relevant market for the purposes of Community competition law, Brüssel 2021, S. 82 ff.
60 *CMA/Autorité de la Concurrence*, Joint Paper: The economics of open and closed systems, London 2014, S. 12.

sichtigt.[61] Nach § 18 Abs. 1 GWB wird ein Unternehmen als marktbeherrschend angesehen, wenn es ohne wesentlichen Wettbewerb auf dem Markt agiert oder eine überragende Marktstellung hat. Marktanteile über 40 % begründen die Vermutung einer marktbeherrschenden Stellung, vgl. § 18 Abs. 4 GWB.

Im digitalen Bereich sind auch auf dieser Ebene zusätzlich Faktoren wie Netzwerkeffekte, Größenvorteile und „*Lock-in*"-Effekte wichtig. Bei „*zero-price*"-Märkten, wie Suchmaschinen oder sozialen Netzwerken, kann zudem die Bewertung anhand von Marktanteilen eingeschränkt sein.[62] Laut § 18 Abs. 3a GWB müssen auch direkte und indirekte Netzwerkeffekte, die parallele Nutzung mehrerer Dienste und der Wechselaufwand für die Nutzer, Größenvorteile im Zusammenhang mit Netzwerkeffekten sowie der Zugang zu Daten und innovationsgetriebener Wettbewerbsdruck berücksichtigt werden. Die Bewertung der Marktmacht im digitalen Sektor erfordert daher oft flexible, einzelfallorientierte Methoden.

Dies gilt auch für das Metaverse. Hier kann die Marktmacht in geschlossenen Ökosystemen leichter konzentriert sein, während offene, interoperable Systeme tendenziell mehr Wettbewerb und damit eine geringere Marktkonzentration zulassen.

c. Verhaltenspflichten nach dem DMA

Der DMA führt spezifische Verhaltenspflichten für sog. „Torwächter" ein. Torwächter sind nach Art. 3 Abs. 1 DMA Unternehmen, die erheblichen Einfluss auf den Binnenmarkt haben (lit. a), einen zentralen Plattformdienst bereitstellen, der gewerblichen Nutzern als wichtiges Zugangstor zu Endnutzern dient (lit. b) und die hinsichtlich ihrer Tätigkeiten eine gefestigte und dauerhafte Position innehaben oder absehbar ist, dass sie eine solche Position in naher Zukunft erlangen werden (lit. c). Zu zentralen Plattformdiensten gehören beispielsweise Suchmaschinen, Soziale Netzwerke und Online-Werbung, vgl. Art. 2 Ziff. 1, 2 DMA. Eine vermutete Torwächter-Stellung bestimmt sich nach Art. 3 Abs. 2 DMA.

Die Verhaltenspflichten der Art. 5 und 6 DMA umfassen unter anderem das Verbot der Zusammenführung personenbezogener Daten aus verschie-

61 Definition des relevanten Marktes (Fn. 56), S. 53 f.
62 *Holm-Hadulla*, Metaverse und Recht (Fn. 49), Rn. 684.

denen Quellen, das Verbot von Paritätsklauseln und die Verpflichtung zur Ermöglichung von Interoperabilität und Datenportabilität.

Im Metaverse könnte das Anwenden dieser Regeln schwerer sein, insbesondere bei offenen und interoperablen Systemen, wo die genaue Bestimmung von Markteinfluss und Umsatzschwellen eine Herausforderung sein könnte. Bei geschlossenen digitalen Ökosystemen bleiben die Vorschriften jedoch weiterhin relevant.

d. Verhaltenspflichten nach § 19a GWB

§ 19a GWB erlaubt dem Bundeskartellamt, bei Unternehmen mit überragender marktübergreifender Bedeutung gezielt Maßnahmen zu ergreifen. § 19a GWB ermöglicht eine Missbrauchsaufsicht, auch wenn das Unternehmen noch keinen dominanten Marktanteil erlangt hat. Die Behörde kann aber aufgrund von dessen Stellung nach § 19a Abs. 2 GWB Einzelmaßnahmen wie das Verbot der Selbstbevorzugung, die Untersagung der Behinderungen auf Beschaffungs- oder Absatzmärkten und die Untersagung der Beeinträchtigung der Interoperabilität anordnen. Wie beim DMA könnte auch hier die Anwendung auf Metaverse-Kontexte und geschlossene digitale Ökosysteme durchaus schwierig werden.

3. Die Fusionskontrolle

Die kartellbehördliche Fusionskontrolle als dritte Säule des Kartellrechts wird immer dann relevant, wenn ein Unternehmen durch den Erwerb von Vermögen, Kontrollrechten, Anteilen oder sonstigen Verbindungen einen beherrschenden Einfluss erwerben möchte, vgl. Art. 3 Abs. 1 FKVO und § 37 Abs. 1 GWB. Ziel von Art. 2 Abs. 2, 3 FKVO und § 36 Abs. 1 GWB ist es nämlich zu verhindern, dass durch einen solchen Unternehmenszusammenschluss der Wettbewerb erheblich behindert würde, insbesondere durch die Begründung oder Verstärkung einer marktbeherrschenden Stellung, wenn dadurch nicht Effizienzen generiert werden, die die Behinderung des Wettbewerbs überwiegen.

Die Anwendung europäischer oder nationaler Fusionskontrollvorschriften einschließlich ihrer Anmeldepflichten hängt davon ab, ob einerseits eine gemeinschaftsweite Bedeutung vorliegt, die zur Zuständigkeit der Europäischen Kommission führt, und wenn diese Voraussetzung nicht er-

füllt ist, ob die Aufgreifschwellenwerte nach nationalen Vorschriften erfüllt sind. Ein Unternehmenszusammenschluss hat nach Art. 1 Abs. 2 FKVO grundsätzlich dann gemeinschaftsweite Bedeutung, wenn ein weltweiter Gesamtumsatz aller beteiligten Unternehmen zusammen von mehr als EUR 5 Mrd. und ein gemeinschaftsweiter Gesamtumsatz von mindestens zwei beteiligten Unternehmen von jeweils mehr als EUR 250 Mio. erzielt wird. Alternativ liegt eine gemeinschaftsweite Bedeutung dann nach Art. 1 Abs. 3 FKVO vor, wenn der weltweite Gesamtumsatz aller beteiligten Unternehmen zusammen mehr als EUR 2,5 Mrd. beträgt (lit. a), der Gesamtumsatz aller beteiligten Unternehmen in mindestens drei Mitgliedstaaten jeweils EUR 100 Mio. übersteigt (lit. b), in jedem von mindestens drei von lit. b erfassten Mitgliedstaaten der Gesamtumsatz von mindestens zwei beteiligten Unternehmen jeweils mehr als EUR 25 Mio. beträgt (lit. c) und der gemeinschaftsweite Gesamtumsatz von mindestens zwei beteiligten Unternehmen jeweils EUR 100 Mio. übersteigt. Seit der 9. GWB-Novelle werden auch „*Killer Acquisitions*" erfasst, bei denen von dem Zielunternehmen zwar keine hohen Umsätze erreicht, aber bei denen potenziell innovativere zukünftige Wettbewerber frühzeitig aufkauft werden.

Im Metaverse steht auch die Fusionskontrolle vor einigen Herausforderungen. So erschwert unter anderem die globale Zugänglichkeit und anonyme Nutzung von Metaverse-Plattformen die Feststellung des relevanten Marktes und der regionalen Zuständigkeit von Kartellbehörden. Während bei traditionellen Unternehmen der Tätigkeitsort oft am Standort der Kunden bestimmt wird, ist dies bei dezentralen Metaverse-Plattformen komplizierter. Hier könnte primär das europäische Fusionskontrollregime zum Einsatz kommen.

Auch können im Metaverse relevante Fusionen in Form von „*Chainmergers*" auftreten, bei denen Blockchain-Plattformen ihre Transaktionshistorien zusammenlegen.[63] Ebenso die perfekte Interoperabilität zwischen verschiedenen Metaverse-Plattformen oder die Übernahme der gesamten Infrastruktur einer virtuellen Welt könnte eine kartellrechtlich relevante Fusion darstellen, wenn diese dadurch faktisch zu einem einzelnen digitalen Ökosystem verschmelzen.[64] Diese Besonderheiten erfordern möglicherweise Anpassungen der Fusionskontrollvorschriften, um den spezifischen Gegebenheiten im Metaverse gerecht zu werden.

63 *Holm-Hadulla*, Metaverse und Recht (Fn. 49), Rn. 775.
64 Ebd. m.w.N.

D. Ergebnis

Das Metaverse stellt die gesamte Rechtsordnung vor bislang nicht gekannte Herausforderungen und verschiebt abermals die Grenzen des Konflikts zwischen Recht und Technologie. Während das Recht bislang maßgeblich auf die Anknüpfungspunkte der Territorialität und der Staatsangehörigkeit setzt, kommt es mit dem Metaverse, jedenfalls in seiner dezentralisierten, offenen Form möglicherweise dazu, dass diese Anknüpfungspunkte für Sachverhalte im Metaverse neu gedacht werden müssen. Dies zieht sich von der Rolle des Staates, über die Rechtsgestaltung und -durchsetzung bis hin zu dem Konzept von Eigentum im Metaverse und der Verantwortlichkeit von Nutzern sowie verschiedenen Aspekten des Rechts. Diese Diskrepanzen können nicht durch einzelne staatliche Akteure gelöst und weltweit Staaten wie Nutzern auferlegt werden, sondern brauchen eine Kooperation vieler Staaten, um einen Anspruch auf Geltung erlangen zu können. Hierbei gilt es jedoch aufzupassen, nicht zu früh zu stark einzugreifen, sondern den Unternehmen genügend Spielraum für die eigene Entwicklung von Geschäftsmodellen zu geben. Gleichwohl sollten die notwendigen Rahmenbedingungen rechtzeitig geschaffen werden, um die bestehenden rechtlichen konzeptionellen Diskrepanzen frühzeitig angehen und lösen zu können.

Die weitere Entwicklung des Metaverse hat eine besondere Bedeutung für den Wettbewerb. Besonders gilt es zu verhindern, dass einzelne große Technologieunternehmen, die schon heute Torwächterstellungen haben, diese verstärken und auch im Metaverse aufbauen. Sollten sie ihre Marktstellung bewahren können, könnten sie im Metaverse die Macht erlangen, einseitig und *de facto* Standards setzen zu können sowie für hohe Markteintrittsschwellen zu sorgen und sich einen *Lock-in*-Effekt ihrer Nutzer in ihren Ökosystemen zu eigen zu machen. Bevorstehende Herausforderungen, das Metaverse rechtlich erfassen zu können, zeigen sich in allen Bereichen des Kartellrechts. Auch hier wird man sich noch lange mit dem Metaverse auseinandersetzen müssen, um alle wettbewerblichen Auswirkungen zu verstehen und sodann einordnen zu können.

Normadressaten bei der Regulierung von Decentralized Autonomous Organizations (DAOs) – am Beispiel der Decentraland DAO[1]

Martin Meier

A. Problemaufriss

Das Jahr 2022 gilt als das Jahr der DAOs, so belegen aktuelle Statistiken, dass sich das gehaltene Vermögen der führenden DAOs auf rund 30 Milliarden USD beläuft.[2] Als digitale Unternehmen ohne jeden Geschäftsführer und Unternehmenssitz wird DAOs das Potential zugeschrieben, die traditionelle Unternehmensorganisation hin zu einer meritokratischen Teilhabe zu verändern.[3] Die Idee einer dezentralen Unternehmensstruktur geht auf das Whitepaper von *Christopher Jentzsch* zurück.[4] Sowohl die Blockchain-Technologie als auch die Idee von DAOs wurden von der Community rund um das Metaversum bzw. Web3 aufgenommen, um ein gesamtgesellschaftliches Leben in einer einzigen virtuellen Welt zu erschaffen, die insbesondere durch ihre Interoperabilität herausstechen soll.[5] Der wohl am weitesten entwickelte Prototyp einer DAO ist das auf der Ethereum-Blockchain basierende *Decentraland*, mit dem eine vollständig dezentralisierte virtuelle Welt und mit der *Decentraland DAO* auch eine eigene Governance-Struktur samt Mitbestimmungsrechten für seine Nutzer etabliert worden sind.[6] Die Problemstellungen auf gesellschaftsrechtlicher Ebene von DAOs liegen auf

1 Alle Internet-Quellen wurden zuletzt abgerufen am 09.10.2024.

2 *F. Holtermann/M. Müller*, DAO: Wie dezentrale Unternehmen ohne Manager jetzt die Kryptowelt erobern, Handelsblatt v. 12.10.2021, https://www.handelsblatt.com/technik/insight-innovation-dao-wie-dezentrale-unternehmen-ohne-manager-jetzt-die-kryptowelt-erobern/27686480.html.

3 *C. Hahn*, Die Decentralised Autonomous Association (DAA), NZG 2022, 684 (684).

4 *C. Jentzsch*, Decentralized Autonomous Organisation to Automate Governance, 2016, https://lawofthelevel.lexblogplatformthree.com/wp-content/uploads/sites/187/2017/07/WhitePaper-1.pdf.

5 *M. Martini/J. Botta*, Der Staat und das Metaversum, MMR 2023, 887 (888 f.).

6 Decentraland DAO, https://decentraland.org/dao/.

der Hand.[7] Demgegenüber bedürfen sowohl aufsichtsrechtliche als auch gefahrenabwehrrechtliche Maßnahmen eines geeigneten Normadressaten, der bei dezentralisierten Organisationen zu fehlen scheint.

Um sich dieser Problematik anzunähern, soll zunächst in die technischen Hintergründe (B.) eingeführt werden. Darauf aufbauend soll untersucht werden, ob und ggf. inwieweit DAOs taugliche Normadressaten (C.) sein können und ob eine Regulierung *de lege ferenda* (D.) notwendig erscheint.

B. Technischer Hintergrund

Zunächst bedarf es einer Analyse der bestehenden technischen Strukturen, um eine präzise juristische Bewertung vornehmen zu können. Dazu sollen nachfolgend die Blockchain-Technologie (I.) und Smart Contracts (II.) dargestellt werden, um so dann die Charakteristika und Eigenschaften von DAOs (III.) zu analysieren. Zu deren Veranschaulichung soll die *Decentraland DAO* (IV.) herangezogen werden. Weiterhin soll eine Bestandsaufnahme vollständig dezentraler DAOs (V.) erfolgen.

I. Blockchain-Technologie

Die Blockchain-Technologie entstand in Folge der Finanzkrise 2007/2008 als dezentrale Systemarchitektur für Kryptowährungen, um eine von zentralen Intermediären wie Banken und Staaten unabhängige Komplementärwährung zu schaffen.[8] Im Vergleich zu klassischen Datenbanken zeichnet sich die Blockchain insbesondere durch ihre Dezentralität, Disintermediation und Unveränderbarkeit aus.[9] Als informationstechnologische Systemarchitektur werden sämtliche Daten nicht zentral bei einer Entität, sondern dezentral bei allen Nutzern (Nodes) des Systems gespeichert.[10] Die Disintermediation dient der Vermeidung des *Single Point of Failure*, also dem

7 *B. Mienert*, Dezentrale autonome Organisationen (DAOs) und Gesellschaftsrecht, Tübingen 2022, S. 77 ff.

8 *S. Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf.

9 *D. Paulus*, Was ist eigentlich … eine Blockchain?, JuS 2019, 1049 (1049 f.).

10 *P. De Filippi/A. Wright*, Blockchain and the Law: The Rule of Code Paperback, Cambridge 2018, S. 49.

zentralen Systemausfall durch einen einzigen Intermediär.[11] Die Dezentralität der gespeicherten Daten bietet eine hohe Fälschungssicherheit, da der gesamte Datenbestand bei jedem Node gespeichert und so die Authentizität und Vollständigkeit der Daten gewährleistet wird.[12] Die Blockchain besteht aus einzelnen Datenblöcken, die mithilfe der Kryptographie dergestalt miteinander verknüpft werden, dass eine nachträgliche Änderung nahezu ausgeschlossen ist, was zur namensgebenden Verkettung und gleichzeitig zu einer grundsätzlichen Unveränderbarkeit der gespeicherten Daten (Token) führt.[13] Diese Token sind ausschließlich, einzigartig und nicht vervielfältigbar,[14] sodass mit ihnen unterschiedliche Rechte und Funktionen verknüpft werden können.[15] Ursprünglich noch als Komplementärwährung gedacht, haben sich in wirtschaftlicher Hinsicht neben Currency-Token auch Investment-Token und Utility-Token herausgebildet.[16] Weiterhin kann zwischen austauschbaren (*fungible*) Token, wie Bitcoin oder Ether, und einzigartigen (*non-fungible*) Token (NFTs), die eine digitale Abbildung etwa von Eigentumsverhältnissen ermöglichen, unterschieden werden.[17] Um eine Transaktion auszulösen, braucht es ein kryptografisches Schlüsselpaar (Public-Key/Private-Key),[18] das regelmäßig in digitalen Geldbörsen (Wallets) verwahrt wird.[19] Um die Fälschungssicherheit zu gewährleisten, insbesondere das Problem der doppelten Ausgabe von Token (sog. Double-Spending)[20] zu vermeiden, überprüfen sämtliche Nodes die in die Blockchain einzupfle-

11 *M. Fromberger/P. Zimmermann*, in: P. Maume/L. Maute/M. Fromberger (Hrsg.), München 2020, Rechtshandbuch-Kryptowerte, § 1 Rn. 5.

12 *M. Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (505).

13 *P. Maume/L. Haffke/P. Zimmermann*, Bitcoin vs. Bargeld – Die geldwäscherechtliche Verpflichtung von Güterhändlern bei Zahlungen mit Kryptowährungen, CCZ 2019, 149 (150).

14 *M. Kaulartz/R. Matzke*, Die Tokenisierung des Rechts, NJW 2018, 3278 (3278).

15 *Fromberger/Zimmermann* (Fn. 11), § 1 Rn. 68.

16 Es wird auch zwischen intrinsischen und extrinsischen Token unterschieden, siehe dazu *S. Möllenkamp*, in: T. Hoeren/U. Sieber/B. Holznagel (Hrsg.), Handbuch Multimedia Recht, Werkstand: 61. EL März 2024, Teil 13.6 Blockchain, Kryptowährungen und Token, Rn. 39, 60.

17 *M. Denga*, Non-Fungible Token im Bank- und Kapitalmarktrecht, BKR 2022, 288, 288 ff.

18 *Fromberger/Zimmermann* (Fn. 11), § 1 Rn. 15.

19 *M. Fromberger/L. Haffke/P. Zimmermann*, Kryptowerte und Geldwäsche, BKR 2019, 377 (378).

20 *H. Bechtolf/N. Vogt*, Datenschutz in der Blockchain – Eine Frage der Technik, ZD 2018, 66 (67).

genden Transaktionen anhand eines Algorithmus, der einen mehrheitlichen Konsens von mehr als 50 % verlangt.[21] Eine nachträgliche Änderung der in der Blockchain gespeicherten Daten ist grundsätzlich durch die algorithmische Kryptografie ausgeschlossen. Denkbar ist jedoch zum einen, dass ein „Angreifer" mehr als 50 % der an der Blockchain beteiligten Nodes stellt (Brute-Force-Attack).[22] Zum anderen besteht die Möglichkeit einer sog. Hard-Fork (engl. für Gabel), bei der die Programmierer eine neue Softwareversion der Blockchain aufsetzen.[23] Die einzelnen Nodes entscheiden letztlich jedoch selbst, ob sie die neue Version annehmen oder es zu einer endgültigen Zweiteilung kommt.[24] So hat sich beispielsweise Bitcoin Cash von Bitcoin mit einer Hard-Fork abgespalten, bei der die Skalierung der Blockgröße von 32 Megabyte auf 128 Megabyte angehoben und somit mehr Transaktionen in einem Block validiert werden konnten.[25] Derartige Änderungen werden regelmäßig der Community bekannt gegeben und ihr zur Abstimmung gestellt.[26]

II. Smart Contracts

Die technische Grundlage für DAOs bilden Smart Contracts, die im Jahr 1993 begrifflich von *Nick Szabo* geprägt wurden und ein Modell zur automatisierten Vertragsabwicklung beschreiben, bei dem in einem computerbasierten Transaktionsprotokoll die Bedingungen eines Vertrages implementiert sind.[27] Konzeptionell handelt es sich um Algorithmen, die automatisiert rechtlich vordefinierte Vertragsbestimmungen (Wenn-/Dann-Mechanismus) ausführen.[28] Es brauchte jedoch erst ein öffentliches

21 *A. Blunk*, in: H. Steege/K. Chibanguza (Hrsg.), Metaverse Rechtshandbuch, Baden-Baden 2023, § 22 Rn. 6.
22 *De Filippi/Wright*, Blockchain and the Law (Fn. 10), S. 49.
23 *P. Roßbach*, in: F. Möslein/S. Omlor (Hrsg.), FinTech-Handbuch, 1. Aufl. München 2019, § 4 Rn. 53.
24 *Bechtolf/Vogt* (Fn. 20), Datenschutz in der Blockchain, 70.
25 *N. Reiff*, All About the Bitcoin Cash Hard Fork, 24.3.2024, https://www.investopedia.com/news/all-about-bitcoin-cash-hard-fork/.
26 *Roßbach* (Fn. 23), § 4 Rn. 53 f.
27 *N. Szabo*, Formalizing and Securing Relationships on Public Networks, First Monday 1997, https://firstmonday.org/ojs/index.php/fm/article/view/548/469-publisher=First.
28 *N. Bilski*, Blockchain-Technologie, Smart Contracts und selbstvollziehende Verträge, S. 23 m.w.N., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3425805.

und fälschungssicheres Netzwerk wie die Blockchain.[29] Daher hat sich die Terminologie der Smart Contracts erst mit Entwicklung der Ethereum-Blockchain durch *Vitalik Buterin* durchgesetzt.[30] Da ein Smart Contract über die Blockchain operiert, ist auch der Smart Contract fälschungssicher und grundsätzlich unveränderbar wie die Blockchain selbst – auch für die Entwickler.[31]

III. Charakteristika und Eigenschaften von DAOs

Bei DAOs handelt es sich um auf Dauer angelegte Organisationen, die aus einer Vielzahl von Smart Contracts bestehen, welche über die Blockchain (on chain) dezentral verwaltet und ausgeführt werden.[32] So werden durch die Smart Contracts bei entsprechendem Bedingungseintritt Transkationen über die Blockchain abgewickelt oder Ereignisse in Gang gesetzt, wie z. B. bei einer Gesellschafterversammlung („Wenn die Bedingung eines Zustimmungsquorum von ¾ aller Mitglieder eingetreten ist, dann wird die Operation eines vorab definierten Gesellschafterbeschlusses ausgeführt").[33] Mit der ersten dezentralen Organisation *TheDAO* wurde noch ein Vehikel zur Kapitalbeschaffung avisiert, dabei können mit einer solchen Infrastruktur auch Forschungsnetzwerke[34], Social-Media-Plattformen[35] oder Finanzdienstleistungen[36] umgesetzt werden.[37]

Charakteristisch für eine DAO ist ihre Dezentralität. So wird die Organisation nach den in den Smart Contracts vordefinierten Regeln unmittelbar und direkt durch die Gesamtheit der Mitglieder verwaltet.[38] Die Governance der DAO ergibt sich dabei aus dem Geflecht an Smart Con-

29 *Bilski*, Blockchain-Technologie (Fn. 28), S. 24.
30 *V. Buterin*, Ethereum Whitepaper, https://ethereum.org/de/whitepaper/.
31 *C. Teichmann*, Digitalisierung und Gesellschaftsrecht, ZfPW 2019, 247 (267) spricht davon, dass „(n)ach der Installation des Smart Contracts (…) dessen Schöpfer ebenso an ihn gebunden (sind) wie alle anderen".
32 *Hahn*, DAA (Fn. 3), 684.
33 *Hahn*, DAA (Fn. 3), 685.
34 Vgl. ResearchHub, https://www.researchhub.com/about.
35 Vgl. Steemit, https://steem.com/SteemWhitePaper.pdf.
36 Vgl. MakerDAO, https://makerdao.com/en/.
37 *G. Langheld/C. Haagen*, Decentralized Autonomous Organizations, NZG 2021, 724 (725).
38 *M. Mann*, in: T. Braegelmann/M. Kaulartz (Hrsg.), Rechtshandbuch Smart Contracts, München 2019, 17. Kap. Rn. 1.

tracts.[39] Die Dezentralität von DAOs sorgt auch dafür, dass ein zentrales Geschäftsleitungsorgan fehlt und die Unternehmensentscheidungen vielmehr durch sämtliche Mitglieder mittels Mehrheitsprinzips gefasst und durch die Smart Contracts automatisiert vollzogen werden.[40] Um einer DAO beitreten zu können, müssen bestimmte Einheiten eines nativen Token (z. B. Ether) an die Wallet der DAO transferiert werden, für die ein äquivalenter Token (sog. Equity-Token) als Gegenleistung ausgegeben wird, welcher die Stimmanteile und Mitgliedschaftsrechte verkörpert.[41] Im Unterschied zu „klassischen" Geschäftsanteilen können Equity-Token nicht nur durch die Bereitstellung von Kapital, sondern auch durch klassische bzw. kreative Dienstleistungen oder anderer Beitragsformen erworben und allokiert werden.[42] Unterschieden wird insoweit zwischen „wrapped" und „non-wrapped" DAOs, ob also die Entwickler die DAO in eine bestimmte Rechtsform „verpacken" wollen.[43] Dies ist sehr anschaulich im Eckpunktepapier der britischen Law Commission dargestellt:[44]

39 *Langheld/Haagen*, DAOs (Fn. 37), 724.
40 *Langheld/Haagen*, DAOs (Fn. 37), 724 f.
41 *Langheld/Haagen*, DAOs (Fn. 37), 725.
42 *Hahn*, DAA (Fn. 3), 685.
43 Siehe dazu ausführlich bei *F. Möslein/D. Ostrovski*, Legal personality of Decentralized Autonomous Organizations (DAOs): Privilege or Necessity?, in: M. Oliveira/A. Rolo (Hrsg.), Decentralised Autnomous Organisation (DAO) Regulation, 2024.
44 Law Commission, Decentralised autonomous organisations (DAOs) A scoping paper, S. 91, 95, https://lawcom.gov.uk/document/decentralised-autonomous-organisations-scoping-paper/.

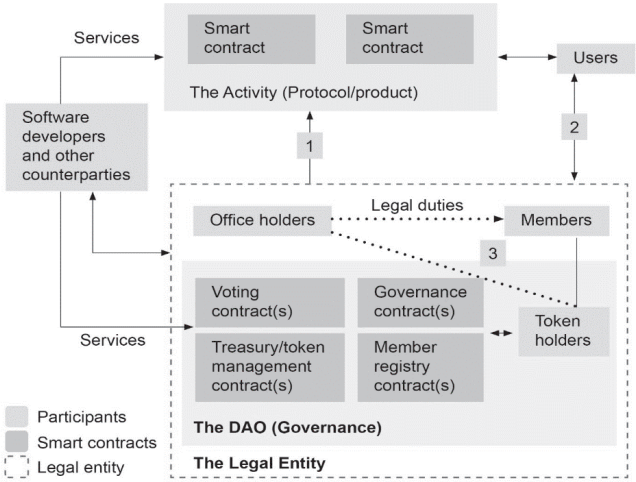


Abbildung 1: eine vollständig verpackte DAO („wrapped“)

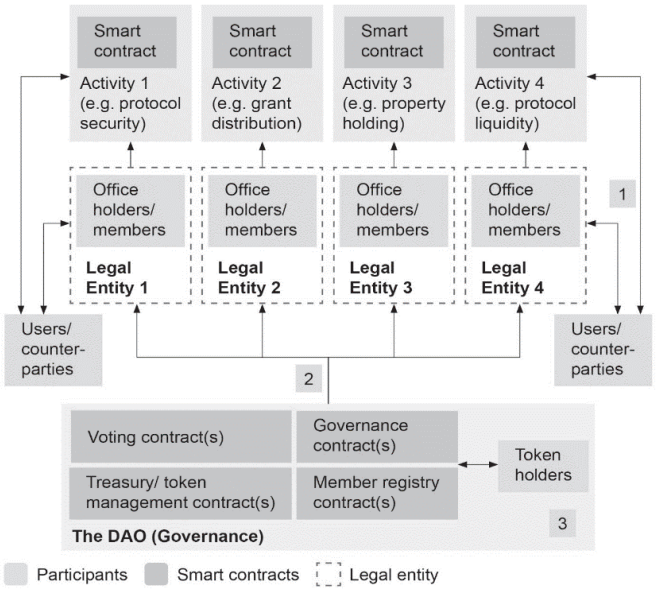


Abbildung 2: eine nicht verpackte DAO („non-wrapped“)

IV. Beispiel: Die *Decentraland DAO* als semi-dezentrale Organisation

Decentraland ist ein Anbieter im Metaverse und besteht als Plattform aus der *Decentraland DAO*, einem DAO-Fond und der Decentraland Foundation.[45] Dieses Metaverse ist ein Virtual-Reality-Ökosystem, in dem u. a. virtuelle Grundstücke und digitale Objekte als NFTs gehandelt werden können.[46] Erwirbt ein Netzwerkteilnehmer einen NFT über ein virtuelles Grundstück, so kann er frei und unabhängig von der DAO darüber verfügen.[47] Neben dem virtuellen Immobilienhandel haben sich auch andere Marktzweige etabliert, wie dem virtuellen Kunsthandel, verschiedenen Computerspielerlebnissen und anderen innovativen Anwendungen.[48] Der „Beitritt" zur Gesellschaft ist nur durch den Erwerb der Token MANA, NAMES oder LAND möglich, die sowohl die Teilnahme an internen Abstimmungen als auch die Unterbreitung eigener Vorschläge ermöglichen.[49] Die Governance der *Decentraland DAO* besteht aus einem DAO-Committee, einem Security Advisory Board sowie einzelnen Unter-Committees und Squads.[50] Das DAO-Committee besteht aus drei gewählten Mitgliedern, die jeder über einen Private-Key für ein Multi-Signature-Wallet verfügen, um Abstimmungen on-chain zu speichern, Personen zu bannen, einzelne Points-of-Interests zu setzen oder Governance-Vorschläge zu machen.[51] Bei einem solchen Multi-Signature-Wallet werden zwei oder mehr Private-Keys benötigt, um eine einzelne Transaktion freizugeben, was die Sicherheit erhöht – vergleichbar mit einem aus zwei Schlössern bestehenden Tresor, der nur mit zwei Schlüsseln geöffnet werden kann.[52]

Sollen Änderungen an der Governance und damit an den von der *Decentraland DAO* zugrundeliegenden Smart Contracts vorgenommen werden, so finden zunächst Abstimmungen der Mitglieder außerhalb der

45 Decentraland, The DAO Fund, https://docs.decentraland.org/player/general/dao/overview/the-dao-fund/.
46 *M. Kaulartz/A. Schmid/F. Müller-Eising*, Das Metaverse – eine rechtliche Einführung, RDi 2022, 521 (527).
47 *Kaulartz/Schmid/Müller-Eising*, Das Metaverse (Fn. 46), 527.
48 Vgl. https://coinmetro.com/price/mana.
49 Decentraland, Participation Requirements, https://docs.decentraland.org/player/general/dao/overview/what-do-you-need-to-participate/.
50 Decentraland, How the DAO works, https://docs.decentraland.org/player/general/dao/overview/how-does-the-dao-work/.
51 Decentraland, How the DAO works (Fn. 50).
52 *M. Gollrad*, in: D. Kipker (Hrsg.), Cybersecurity, 2. Aufl. München 2023, Kap. 20.2 Rn. 66 ff.

Blockchain (off-chain) in einem Internetforum statt, um hohe Transaktionskosten zu vermeiden.[53] Sodann läuft der Abstimmungsprozess in drei Stufen ab: Als erstes findet eine Umfrage für Vorschläge statt (Pre-Proposal Poll), als zweites wird ein Vorschlag entworfen und ausgearbeitet (Draft Proposal) und als drittes wird final mit einfacher Mehrheit über den Vorschlag abgestimmt (Governance Proposal).[54] Sind Änderungen an den Smart Contracts durch Abstimmungen beabsichtigt, führt entweder das DAO-Committee oder das Security-Advisory Board die Aktualisierung des Smart Contracts durch.[55] Das Security Advisory Board, bestehend aus fünf gewählten Mitgliedern, beaufsichtigt das DAO-Committee und hat die Möglichkeit, jede vom Komitee durchgeführte Aktion innerhalb von 24 Stunden anzuhalten oder abzubrechen.[56] Letztlich werden die Governance-Vorschläge aber durch das DAO-Committee in Kraft gesetzt.[57]

An diesem Aufbau wird deutlich, dass es sich bei der *Decentraland DAO* nur um eine semi-dezentralisierte Organisation handelt, da nur einzelne Unternehmenselemente automatisiert durch die Smart Contracts vollzogen werden, wichtige Kompetenzen und Entscheidungsbefugnisse aber weiterhin bei dem DAO-Committee verbleiben. Zudem steht der *Decentraland DAO* die Decentraland Foundation als Stiftung vor, die für die Gemeinschaft als Ganzes handelt.[58]

V. Bestandsaufnahme vollständig dezentraler DAOs

Offen bleibt die Frage, ob es derzeit vollständig dezentrale Unternehmensgebilde gibt. Auch wenn viele DAOs damit werben, ein solches komplett dezentralisierte System zu bilden, so handelt es sich bei den meisten doch nur um semi-dezentrale Organisationen.[59] Bei dem Open-Source Protokoll von *Compound* – einem FinTech-Unternehmen – besteht z. B. die

53 Decentraland, https://forum.decentraland.org/.
54 Decentraland, What you can do with the DAO, https://docs.decentraland.org/player/general/dao/overview/what-can-you-do-with-the-dao/.
55 Decentraland, What you can do with the DAO (Fn. 54).
56 Decentraland, How the DAO works (Fn. 50).
57 Decentraland, User Guide, https://docs.decentraland.org/player/general/dao/dao-userguide/.
58 Decentraland, Terms of Use, https://decentraland.org/terms/#2-disclaimer-and-modification-of-terms-of-use.
59 *M. Machacek*, Die Anwendung der neuen MiCA-Verordnung auf Dezentrale Finanzanwendungen, EuZW 2021, 923 (927).

Möglichkeit, von einem zentralen Administrator aktualisiert zu werden.[60] Auch die Smart Contracts der *Maker-DAO* werden von der gleichnamigen Maker-Stiftung kontrolliert, die im November 2020 einen neuen Token namens *Multi Collateral Dai* (MCD) emittierte,[61] was zeigt, dass die Stiftung noch die Protokolle der Smart Contracts mit Administratorenrechten kontrollieren konnte. Ebenso hatte bei der Emission des Governance-Token der dezentralen Tauschbörse *Uniswap* (UNI) das ursprüngliche Entwicklerteam die Freigabe und Verteilung dieser Token koordiniert und damit kontrolliert.[62] Das bis dato einzig vollständig dezentrale Geschäftsmodell ist – mangels dem Entwickler zustehender Administratorenrechte – die Bitcoin-Blockchain,[63] deren technisches Netzwerk aber nicht aus Smart Contracts, sondern allein aus der Blockchain besteht.[64] Deutlich wird, dass Administratorenrechte jedweder Art ein Indikator dafür sind, dass es sich nicht um ein vollständig dezentrales System handelt.

C. DAOs als taugliche Normadressaten

Dieses technische Begriffsverständnis von DAOs zugrunde gelegt, gilt es nunmehr zu untersuchen, inwieweit bei solchen Gesellschaftsstrukturen ein tauglicher Normadressaten für hoheitliche Maßnahmen gefunden werden kann. Dies ist vor dem Hintergrund von besonderer Bedeutung, dass auf dem Sekundärmarkt Risiken hinsichtlich der Finanzmarktregulierung bestehen können, wie etwa im Hinblick auf die Finanzmarktstabilität, die Währungssouveränität, den Verbraucherschutz und die Geldwäscheprävention.[65] Dies wird insbesondere am ersten Prototyp von *TheDAO* deutlich, bei dem es einem Hacker gelang 50 Millionen USD „zu stehlen".[66]

60 Bitkom e.V., Decentralized Finance (DeFi) – A new FinTech Revolution?, 2020, S. 16, https://www.bitkom.org/sites/default/files/2020-07/200729_whitepaper_decentralized-finance.pdf.

61 *Machacek*, MiCA (Fn. 59), 927.

62 CoinDesk, Uniswap Launches Governance Token in Bid to Keep Up With Rival AMM SushiSwap, 17.9.2020, https://www.coindesk.com/uniswap-token.

63 *Machacek*, MiCA (Fn. 59), 927.

64 Insoweit wird zwischen der Layer-1-Ebene und Layer-2-Ebene unterschieden, siehe dazu *T. von Poser*, Haftungsadressaten in DLT-Netzwerken, in: S. Omlor/F. Möslein (Hrsg.), Blockchain und Recht, Tübingen 2024, S. 100.

65 Vgl. dazu *M. Meier*, Geldwäsche-Compliance für Kryptowerte, Jena 2022, S. 159 ff.

66 *V. Tosovic*, Der DAO-Hack – und die Konsequenzen für die Blockchain, in: D. Burgwinkel (Hrsg.), Blockchain Technology, Berlin 2016, S. 1.

Zunächst soll für die Ausgangsfrage die Rechtssubjektivität von DAOs nach zivilrechtlichen Grundsätzen (I.) untersucht werden, ob diese Unternehmensgebilde einer *numerus clausus*-Rechtsform des Gesellschaftsrechts zugeordnet werden können. Anhand dessen soll dann eine Eigenschaft als Adressat nach verwaltungsrechtlichen und polizeirechtlichen Grundsätzen (II.) und anschließend eine Regulierung von DAOs als Normadressaten nach dem Aufsichtsrecht *de lege lata* (III.) beleuchtet werden.

I. Rechtssubjektivität von DAOs nach zivilrechtlichen Grundsätzen

Allgemein werden Gesellschaften in Körperschaften und Personengesellschaften differenziert, deren Unterschied traditionell in ihrer Rechtsfähigkeit und insbesondere in dem Bestand ihrer Mitglieder besteht.[67]

1. Körperschaft des Privatrechts

Für Körperschaften des Privatrechts ist der Verein i. S. d. §§ 21 ff. BGB die Grundform.[68] Daneben bestehen die Gesellschaftsformen der Kapitalgesellschaften. DAOs sammeln regelmäßig Kapital ein und verwalten dieses, womit eine Einordnung als Kapitalgesellschaft naheliegt. Eine Einordnung als Aktiengesellschaft, Gesellschaft mit beschränkter Haftung oder Unternehmergesellschaft scheitert jedoch zum einen an der notariellen Beurkundung ihrer Satzung und Handelsregistereintragung,[69] zum anderen an der fehlenden Geschäftsleitung.[70] Eine Qualifizierung von DAOs als Verein, Stiftung oder Genossenschaft scheidet ebenfalls aus formellen Gründen aus – es fehlt entweder an einer Eintragung in einem öffentlichen Register, an

67 *C. Behme*, in: B. Gsell/W. Krüger/S. Lorenz/C. Reymann (Hrsg.), beck.online.GROSSKOMMENTAR, Stand: 01.06.2024, BGB § 1 Rn. 36 f.

68 *Mienert*, DAOs und Gesellschaftsrecht (Fn. 7), S. 117.

69 Vgl. §§ 2 Abs. 1 S. 1, 11 Abs. 1 GmbHG, §§ 23 Abs. 1 S. 1, 41 Abs. 1 S. 1 AktG; siehe dazu *M. Mann*, Die Decentralized Autonomous Organization – ein neuer Gesellschaftstyp?, NZG 2017, 1014 (1017).

70 Vgl. § 6 Abs. 1 GmbHG, § 30 AktG; siehe dazu *Mann*, DAO (Fn. 69), 1017; *Mann* (Fn. 38), Kap. 17 Rn. 13; *S. Schwemmer*, Dezentrale (autonome) Organisationen, AcP 221 (2021), 555 (574); *H. Fleischer*, Ein erstes Rechtskleid für die Decentralized Autonomous Organization: Die Wyoming DAO LLC – Vorbild auch für Deutschland?, ZIP 2021, 2205 (2207).

der Anerkennung durch einen Hoheitsträger[71] oder einem Errichtungsakt.[72] Insoweit wird eine Anerkennung von Algorithmen als Gesellschaftsorgan *de lege ferenda* erwogen.[73] *De lege lata* scheidet eine Einordnung von DAOs als Körperschaft aus den o.g. Gründen aber aus.

2. Personengesellschaften

Personengesellschaften sind durch ihre vertragliche Verbundenheit geprägt und im Unterschied zu Körperschaften abhängig vom Bestand ihrer Mitglieder.[74] Die Einordnung einer DAO als Kommanditgesellschaft (KG) scheidet von vornherein aus zweierlei Gründen aus: Zum einen muss die die KG prägende Haftungsbeschränkung des Kommanditisten im Handelsregister eingetragen sein (§ 176 Abs. 1 HGB),[75] zum anderen ist eine DAO – wie auch die Blockchain – grundsätzlich als Peer-to-Peer-Netzwerk gleichrangig ausgestaltet; eine KG weist demgegenüber eine ungleiche Struktur zwischen Komplementär und Kommanditist auf.[76]

Die gesetzlichen Grundtypen sind die Gesellschaft bürgerlichen Rechts (GbR), die auf die Erreichung eines gemeinsamen Zwecks gerichtet ist, sowie die offene Handelsgesellschaft (oHG), die eine handelsgewerbliche Tätigkeit verfolgt,[77] und damit die Auffangrechtsnormen für sämtliche Personengesellschaften bilden.[78]

---

71 Vgl. § 21 BGB, § 80 Abs. 2 S. 1 BGB i.V.m. § 4 StiftBTG; *Langheld/Haagen*, DAOs (Fn. 37), 725.

72 Vgl. §§ 5, 10 GenG.

73 *F. Möslein*, Digitalisierung im Gesellschaftsrecht: Unternehmensleitung durch Algorithmen und künstliche Intelligenz?, ZIP 2018, 204 (206 f.); *Mienert*, DAOs und Gesellschaftsrecht (Fn. 7), S. 119.

74 *R. Stürner*, in: Jauernig (Hrsg.), Bürgerliches Gesetzbuch, 19. Aufl. 2023, BGB § 705 Rn. 1.

75 *Mienert*, DAOs und Gesellschaftsrecht (Fn. 7), S. 140; *Mann*, DAO (Fn. 69), 1017.

76 *Mienert*, DAOs und Gesellschaftsrecht (Fn. 7), S. 140.

77 Die oHG unterscheidet sich von der GbR entweder durch den Zweck des Handelsgewerbes (§ 105 Abs. 1 HGB) oder durch die Eintragung als Formkaufmann im Handelsregister (§ 105 Abs. 2 HGB). Zum Begriff des Gewerbes siehe *M. Roth*, in: A. Baumbach/K. Hopt (Hrsg.), HGB, 42. Aufl. 2023, § 105 Rn. 14. Ob eine DAO ein Handelsgewerbe ausübt, kann nicht pauschal, sondern muss, wie bei jeder anderen Gesellschaft, anhand des Einzelfalls beurteilt werden, siehe dazu *Mienert*, DAOs und Gesellschaftsrecht (Fn. 7), S. 137.

78 *K. Schmidt*, Gesellschaftsrecht, 4. Aufl., Köln 2002, § 5 II 3 b; 58 I b.

Auch wenn eine DAO aus Smart Contracts besteht, so sind die Contracts entgegen ihrer Begrifflichkeit keine Verträge im zivilrechtlichen Sinne,[79] da sie nicht auf einen rechtlichen Erfolg gerichtet sind, sondern lediglich eine faktische Änderung herbeiführen.[80] Daher ist vielmehr zu erwägen, ob die Mitglieder der DAO hinter dem Geflecht an Smart Contracts eine vertragliche Bindung eingehen wollten.[81] Dies ist durch objektive Auslegung anhand des entscheidenden Kriteriums zu ermitteln – dem Rechtsbindungswillen der Beteiligten.[82]

Gegen das Vorliegen eines solchen Willens spricht, dass Smart Contracts die DAO faktisch vollziehen.[83] Smart Contracts werden auch nicht verhandelt oder vereinbart,[84] so können unbestimmte Rechtsbegriffe, wie *angemessen* oder *erforderlich* nicht in einen Smart Contract aufgenommen werden, da eine technische Determinierung in einem Binärcode nicht zwangsläufig mit einer rechtlichen Lösungsumsetzung kongruieren muss.[85]

Für die Annahme eines Rechtsbindungswillen spricht allerdings, dass die DAO-Mitglieder die Regeln der durch die Smart Contracts abgesteckten Governance kennen und sich ihr entweder bewusst unterworfen haben,[86] oder um mögliche Fehler im Programmcode in rechtlicher Hinsicht auszugleichen.[87] Auch der in der Programmiersprache festgelegte Durchsetzungsmechanismus spricht für einen rechtlichen Bindungswillen.[88]

Nicht notwendig ist, dass Willenserklärungen in einer dem konkreten Empfänger natürlichen bzw. verständlichen Sprache niedergelegt werden,[89]

---

79 Vgl. *M. Kaulartz/J. Heckmann*, Smart Contracts – Anwendungen der Blockchain-Technologie, CR 2016, 618 (624).

80 *Mann*, DAO (Fn. 69), 1016 vergleicht die herbeigeführte faktische Änderung durch Smart Contracts mit Warenautomaten.

81 Zu den gesellschaftsrechtlichen Implikationen, wie dem Erwerb oder Verlust der Mitgliedschaft, der Beitragspflicht und der Haftung, siehe *Langheld/Haagen*, DAOs (Fn. 37), 726 ff.

82 *C. Schäfer*, in: MüKoBGB, 9. Aufl. 2024, BGB § 705 Rn. 28.

83 *Mann*, DAO (Fn. 69), 1016; *Teichmann* (Fn. 31), Digitalisierung und Gesellschaftsrecht, 268 f.

84 *Teichmann* (Fn. 31), Digitalisierung und Gesellschaftsrecht, 269.

85 *M. Meier*, „Code is Law?" – am Beispiel von Smart Contracts, in: M. Hilgard (Hrsg.), Englisch, Gender-Deutsch oder Maschinen-Code – Brauchen wir eine neue Rechtssprache?, Coburg 2023, S. 53.

86 *Langheld/Haagen*, DAOs (Fn. 37), 725.

87 Zu einem technischen Ausgleich als „Programmierte Schiedsstelle", siehe *Kaulartz/Heckmann*, Smart Contracts (Fn. 79), 623.

88 *Langheld/Haagen*, DAOs (Fn. 37), 725.

89 Vgl. *Kaulartz/Heckmann*, Smart Contracts (Fn. 79), 621 f.

womit auch der Programmcode eines Smart Contracts tauglicher Inhalt eines Gesellschaftsvertrages sein kann.[90] Ebenfalls nicht notwendig ist, dass sich die DAO-Mitglieder im Sinne einer personenrechtlichen Verbundenheit kennen, da die Vielzahl an rein kapitalistisch beteiligten Mitgliedern auf die von der Rechtsprechung anerkannte Gesellschaftsform der Publikumsgesellschaft ausgerichtet ist.[91]

Eine abschließende Beurteilung, ob eine DAO als GbR eingeordnet werden kann, ist insoweit nicht möglich, sondern muss anhand des Einzelfalls ermittelt und abgewogen werden, insbesondere anhand des erklärten Willens der Parteien und der äußeren Umstände.[92] Teilweise wird vertreten, dass bei Vorliegen eines Rechtsbindungswillen DAOs nur als Innengesellschaften bürgerlichen Rechts zu qualifizieren wären, da die der DAO zugrundeliegenden Smart Contracts nicht den Unternehmensträger, sondern den virtuellen Rahmen für die Unternehmensstrukturierung und die Willensbildung der Mitglieder bilden.[93] Überzeugender scheint es dagegen, eine teilrechtsfähige (Außen-)GbR anzunehmen, da sich die Willensbildung der einzelnen Mitglieder nicht auf eine reine Errichtung einer DAO beschränkt, sondern vielmehr auch ein rechtsgeschäftliches Auftreten intendiert ist, wie z. B. der Emission von Token. Das hat zur Folge, dass sämtliche Mitglieder der DAO nunmehr nach der MoPeG-Reform[94] gem. § 721 Abs. 1 BGB n.F. als Gesellschafter unmittelbar, primär und gesamtschuldnerisch haften,[95] was den meisten DAO-Mitgliedern wohl nicht bekannt sein dürfte.[96]

Für die *Decentraland DAO* ergibt sich dabei folgendes Bild: Als gemeinsamer Zweck der Gesellschaft ist die Bereitstellung und Unterstützung

90 *Bilski*, Blockchain-Technologie (Fn. 28), S. 53 m.w.N.

91 Vgl. statt vieler BGH NJW 1973, 1604; NJW 1975, 1318; NJW 1977, 2311; *B. Mienert*, Wyomings DAO-Gesetz, RDi 2021, 384 (387); dazu kritisch für Investments in der Realwirtschaft *G. Spindler*, Blockchaintypen und ihre gesellschaftsrechtliche Einordnung, RDi 2021, 309 (313).

92 *Mann*, DAO (Fn. 69), 1017; ebenso für eine Einordnung als Publikums-GbR siehe *Fleischer*, Die Wyoming DAO LLC (Fn. 70), 2207; *Spindler*, Blockchaintypen (Fn. 91), 313.

93 *Teichmann* (Fn. 31), Digitalisierung und Gesellschaftsrecht, 269.

94 Gesetz zur Modernisierung des Personengesellschaftsrechts, BGBl. 2021 I, S. 3436.

95 Nach alter Rechtslage haben BGB-Gesellschafter nach § 128 HGB analog gehaftet, vgl. *Fleischer*, Die Wyoming DAO LLC (Fn. 70), 2207.

96 *Mienert*, Wyomings DAO-Gesetz (Fn. 91), 384.

des Metaverse anzusehen.[97] Die Token MANA, NAMES, LAND können gegen andere native Token erworben werden und ermöglichen es so, der DAO „beizutreten" sowie an internen Abstimmungen teilzunehmen und eigene Vorschläge für Abstimmungen zu unterbreiten.[98] Durch diese Abstimmungen kann die Gemeinschaft in der DAO Zuschüsse erteilen, die Liste von gebannten Personen ändern, Points of Interest erstellen und neue Mitglieder für einen Server (sog. catalyst node) zulassen.[99] Damit sind diese Token als Equity-Token zu qualifizieren, die einen Gesellschaftsanteil repräsentieren. All dies spricht für eine Einordnung der *Decentraland DAO* als (Publikums-)GbR nach nationalem Recht.[100]

II. Adressat nach verwaltungsrechtlichen und polizeirechtlichen Grundsätzen

Die Fähigkeit, Rechtssubjekt im Sinne des Verwaltungsverfahrensgesetzes zu sein, richtet sich nach der Beteiligten- und Handlungsfähigkeit der §§ 11, 12 VwVfG. Diese Vorschriften regeln die Voraussetzungen, damit ein Rechtssubjekt im Verwaltungsverfahren aktiv teilnehmen und passiv durch eine Behörde ein Verfahren gegen dieses Rechtssubjekt wirksam durchgeführt werden kann.[101] Nach § 11 Nr. 1 Alt. 2 VwVfG sind neben natürlichen Personen auch juristische Personen beteiligtenfähig. Gleichgestellt sind Vereinigungen und Organisationen, denen durch Gesetz oder gewohnheitsrechtlich eine Prozessfähigkeit zuerkannt ist, also im eigenen Namen klagen oder verklagt werden können.[102] Da die Außen-GbR im Sinne des Zivilprozessrechts für uneingeschränkt parteifähig erklärt wor-

97 *J. Brukhmann/et. al.*, Decentraland White paper, https://decentraland.org/whitepaper.pdf.

98 Decentraland, Participation Requirements (Fn. 49).

99 Decentraland, What is the DAO, verfügbar unter: https://docs.decentraland.org/player/general/dao/overview/what-is-the-dao/.

100 So im Allgemeinen für DAOs *Poser*, Haftungsadressaten in DLT-Netzwerken (Fn. 64), S. 100 f.

101 *B. Gerstner-Heck*, in: J. Bader/M. Ronellenfitsch (Hrsg.), BeckOK VwVfG, 64. Edition Stand: 01.07.2024, VwVfG § 11 Rn. 1.

102 *Gerstner-Heck* (Fn. 101), VwVfG § 11 Rn. 10.

den ist,[103] ist sie auch konsequenterweise als beteiligtenfähig im Sinne des Verwaltungsverfahrensrechts nach Nr. 1 anzusehen.[104]

Auch der Adressat eines polizeilichen Verwaltungsakts, der sog. Störer, ist Beteiligter des Verwaltungsverfahrens.[105] Zur Inanspruchnahme einer juristischen Person des Privatrechts muss die Organisation, unabhängig ob sie rechtsfähig oder nichtrechtsfähig ist, ein Mindestmaß an Organisation aufweisen sowie auf gewisse Dauer angelegt sein,[106] was bei DAOs im Regelfall zu bejahen ist. Die Eigenschaft als Störer knüpft an die verschuldensunabhängige Verursachung einer Gefahr, die nach den drei polizeirechtlichen Kausalitätstheorien ermittelt wird.[107] Dies ist eine Frage von Zurechnung(-skriterien).[108] Eine Inanspruchnahme einer DAO als Störer muss sich neben den Kriterien des Ermessens (faktisch effektivste Beseitigung, „Greifbarkeit" durch die Behörden und finanzielle Leistungsfähigkeit) zudem am Grundsatz der Verhältnismäßigkeit messen lassen.[109]

Problematisch ist die Auswahl des Störers, da ein einzelnes DAO-Mitglied für sich allein genommen eine Gefahr nur beseitigen kann, wenn er über die Mehrheit der Equity-Token (> 50 %) verfügen würde, um entsprechende Mehrheitsbeschlüsse der Gesellschaft zu fassen, was der intendierten Dezentralität einer DAO zuwiderlaufen würde.[110] Handelt es sich, wie bei DAOs regelmäßig, um eine rechtsfähige Personengesellschaft, so sind nicht die persönlich haftenden Gesellschafter, sondern die Gesellschaft selbst ist Adressat der Anordnung.[111] Die einzelnen Gesellschafter

103 BGHZ 146, 341 (343, 347) = NJW 2001, 1056.
104 *M. Geis*, in: F. Schoch/J. Schneider (Hrsg.), Verwaltungsrecht, Werkstand: 4. EL November 2023, VwVfG § 11 Rn. 26a.
105 *W. Schenke*, Polizei- und Ordnungsrecht, 12. Aufl. 2023, Rn. 549.
106 *Schenke* (Fn. 105), Rn. 304.
107 Dies sind die Äquivalenztheorie, die Adäquanztheorie sowie die Theorie der unmittelbaren Verursachung, siehe dazu *Schenke* (Fn. 105), Rn. 313 ff. m.w.N.
108 Siehe ausführlich zu Zurechnung im öffentlichen Recht, *A. Hobusch*, Zurechnung im Recht, 2023, S. 158.
109 *A. Klaas*, Geldwäsche und dezentrale autonome Organisationen (DAO), BKR 2023, 162 (169) m.w.N.
110 Sofern der Beitrag eines einzelnen Mitglieds überhaupt die Gefahrenschwelle überschreiten würde, *Klaas* (Fn. 109), 167 spricht von singulären Handlungsbeiträgen.
111 BVerwG, Urt. v. 24. 2. 2010 – 8 C 10/09 = NZG 2011, 114, Rn. 20 ff.

stehen dann als Störermehrheit[112] nach § 721 Abs. 1 BGB persönlich für die regulatorischen Pflichten der Publikums-GbR ein.[113]

III. DAOs als Normadressaten im Aufsichtsrecht *de lege lata*

Das Aufsichtsrecht knüpft verschiedene Dienstleistungen an eine Erlaubnispflicht: „*Wer*" Bankgeschäfte oder Finanzdienstleistungen nach § 1 KWG erbringen will, bedarf der Erlaubnis der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) nach § 32 KWG,[114] gleiches gilt gem. §§ 10, 11 ZAG für Zahlungsdienste und E-Geld-Geschäfte.[115] Diese Konzessionspflichten brauchen jedoch eine natürliche oder juristische Person als geeigneten Adressaten.[116] Als Pendant zur Konzessionspflicht stehen der BaFin gefahrenabwehrrechtliche Befugnisse nach § 37 KWG bzw. § 6 Abs. 3 KWG zur Verfügung. So kann die BaFin durch formlose Information oder Aufforderung die sofortige Einstellung des Geschäftsbetriebs mit der Folge anordnen, dass die Erlaubnis erlischt und das Institut abzuwickeln ist.[117]

Die BaFin kann dabei dem Wortlaut des § 37 Abs. 1 KWG nach nur Maßnahmen gegenüber *dem Unternehmen und den Mitgliedern seiner Organe* als unmittelbar Verantwortliche ergreifen.[118] Darüber hinaus kann die BaFin ihre Maßnahmen gegen Internetprovider und sonstige Dritte richten, die zum Betrieb der unerlaubten Geschäfte beitragen.[119] Selbiges gilt für unerlaubte Zahlungsdienste und unerlaubte E-Geld-Geschäfte, bei der der BaFin im Unterschied zu § 37 KWG die Befugnisse gem. § 7 Abs. 1 S. 1 ZAG auch gegenüber den Gesellschaftern zustehen.[120]

---

112 Siehe ausführlich zur Mehrheit von Störern *T. Kingreen/R. Poscher*, Polizei- und Ordnungsrecht, 12. Aufl. 2022, § 9 Rn. 87 f.

113 Noch zur alten Rechtslage des § 128 S. 1 HGB analog, aber inhaltlich insoweit übereinstimmend, *Klaas* (Fn. 109), 162 (168).

114 Nach § 32 Abs. 1 KWG können natürliche und juristische Personen („Wer") einen Erlaubnisantrag stellen, siehe dazu *A. Schwennicke*, in: A. Schwennicke/D. Auerbach (Hrsg.), KWG, 4. Aufl. 2021, KWG § 32 Rn. 16.

115 Ausführlich bei *D. Walter*, in: M. Casper/M. Terlau (Hrsg.), ZAG, 2. Aufl. 2020, ZAG § 10 Rn. 16.

116 *Schwennicke* (Fn. 114), KWG § 32 Rn. 16.

117 *R. Fischer/K. Krolop*, in: R. Fischer/H. Schulte-Mattler (Hrsg.), KWG, 6. Aufl. 2023, KWG § 37 Rn. 8.

118 *Schwennicke* (Fn. 114), KWG § 37 Rn. 8.

119 *Fischer/Krolop* (Fn. 117), KWG § 37 Rn. 7.

120 *Schwennicke* (Fn. 114), ZAG § 7 Rn. 7.

Wird der Zweck der Gefahrenabwehr – der Schutz der Ordnungsmäßigkeit der Finanzwirtschaft[121] – nicht erreicht, so kann die BaFin nach dem Grundsatz der Opportunität im Rahmen ihres Auswahlermessens auch eine Untersagungsverfügung als förmlichen Verwaltungsakt erlassen.[122] Das Gesetz ist dabei weitgehend offengehalten, um der BaFin ein flexibles Vorgehen gegen unerlaubte Geschäfte zu ermöglichen.[123] Aber auch hier gilt der Grundsatz der Verhältnismäßigkeit, insbesondere muss das mildeste, zur Zweckerreichung geeignete Mittel angewendet werden.[124]

Neben den Befugnissen aus § 37 KWG steht der BaFin die Generalklausel nach § 6 Abs. 3 KWG zur Verfügung, wonach sie in ihren gesetzlich zugewiesenen Aufgaben diejenigen Anordnungen treffen kann, die geeignet und erforderlich sind, um Verstöße gegen aufsichtsrechtliche Bestimmungen zu verhindern oder zu unterbinden.[125] Adressat ist hier nach S. 1 das Institut oder ihre Geschäftsleiter. Nach S. 2 kann die BaFin Maßnahmen auch *„gegenüber den Personen (anordnen), die die Geschäfte dieser Gesellschaften tatsächlich führen*". Auch diese Anordnungen sind nach Auffassung des Gesetzgebers grundsätzlich als Verwaltungsakte anzusehen, um eine Entscheidung im Widerspruchsverfahren und ggf. im gerichtlichen Wege überprüfen zu können.[126] Fraglich ist daher, wie man allein bei normativer Auslegung des § 6 Abs. 3 S. 2 KWG ermitteln kann, welche Person die Geschäfte bei einer DAO tatsächlich führt. Insoweit lässt sich der Adressatenbegriff in formeller und materieller Hinsicht differenzieren:

Der Gesetzgeber hat mit dem Gesetz über elektronische Wertpapiere (eWpG)[127] für Emittenten von Kryptowertpapieren einen formellen Adressatenbegriff zugrunde gelegt.[128] Bei Kryptowertpapierregistern wird gem. § 16 Abs. 2 eWpG die Benennung einer „registerführenden Stelle" gefordert, um einen verantwortlichen Pflichtenadressaten bestimmen zu können.[129] Unterbleibt eine Benennung einer solchen Stelle, *gilt* der Emittent als registerführende Stelle – es handelt sich insoweit um eine gesetzliche Fiktion,

121 *Fischer/Krolop* (Fn. 117), KWG § 32 Rn. 5.
122 *Fischer/Krolop* (Fn. 117), KWG § 37 Rn. 8, 10.
123 Mit Beispielen zu einzelnen Maßnahmen, siehe *Schwennicke* (Fn. 114), KWG § 37 Rn. 9.
124 *Fischer/Krolop* (Fn. 117), KWG § 37 Rn. 9.
125 Siehe ausführlich *Schäfer* (Fn. 117), KWG § 6 Rn. 61.
126 *Habetha* (Fn. 114), KWG § 6 Rn. 49.
127 BGBl. I 2021, S. 1423.
128 BT-Drs. 19/26925, S. 60.
129 *B. Kell*, in: M. Müller/C. Pieper (Hrsg.), eWpG, München 2022, § 16 Rn. 53.

um die Situation zu vermeiden, dass kein verantwortliches Rechtssubjekt bzw. kein Adressat existent ist.[130] Aus dieser Konzeption lässt sich ableiten, dass man Adressaten allein aus ihrer formalen Benennung als Verantwortliche heranziehen kann.

Demgegenüber kann man auch einen materiellen Adressatenbegriff zugrunde legen. Bezogen auf das Beispiel von Smart Contract gesteuerten Dienstleistungen bedeutet dies, dass bei einem konkret zu bestimmenden Beitrag eines Initiators oder Projektbeteiligten des Smart Contracts ein Adressat identifiziert werden kann, z. B. wenn einem Beteiligten Administratorenrechte zustehen, um einzelne Dienstleistungen und Entscheidungen zu steuern bzw. anderweitig Einfluss darauf ausüben zu können,[131] oder er eine Provision bei der Abwicklung einer Dienstleistung erhält.[132]

Überträgt man diese Gedanken für eine Inanspruchnahme der *Decentraland-DAO*, so müsste konsequenterweise das DAO-Committee als Störer in Anspruch genommen werden, da dieses unmittelbar auf die Smart Contract Governance-Struktur der DAO einwirken kann und damit in materieller Hinsicht nach obigen Ausführungen als Störer angesehen werden kann.

Legt man eine formelle Betrachtung zugrunde, so könnte man bei der *Decentraland-DAO* die Decentraland Foundation als potenzieller Störer herangezogen werden. Es werden regelmäßig Decentralized Autonomous Association (DAA) als eine Art „rechtliche Schicht" auf die Blockchain-Schicht einer DAO (on-chain) als ein Idealverein oder eine Kapitalgesellschaft „aufgesetzt", um so einen Adressaten in formeller Hinsicht (als eine Art Benennung eines verantwortlichen Rechtssubjekts) zu schaffen.[133] So tritt eine solche DAA quasi in die Stellung eines Geschäftsleitungsorgan im Außenverhältnis. Mit *DAO.Link* wurde z. B. für die *TheDAO* eine Gesellschaft nach schweizerischem Recht als Treuhänderin im Außenverhältnis gegründet.[134] Bei der *Decentraland DAO* gibt es die Decentraland Foundation als Stiftung, die 20 % aller Token mit Stimmrechten hält und so die DAO schützen soll.[135]

---

130 *J. Reiter*, in: C. Conreder/J. Meier (Hrsg.), eWpG, Berlin 2023, § 16 Rn. 27.

131 *L. Auffenberg*, DeFi im Aufwärtstrend – Endstation für die Finanzmarktregulierung, 8. Februar 2021, https://fin-law.de/2021/02/08/defi-im-aufwaertstrend-endstation-fuer-die-finanzmarktregulierung/.

132 *Meier* (Fn. 65) Geldwäsche-Compliance, S. 158. So zum Beispiel bei der Dai, siehe dazu *Holtermann/Müller*, DAO (Fn. 2).

133 Siehe dazu ausführlich *Hahn*, DAA (Fn. 3), 686 ff.

134 *Spindler*, Blockchaintypen (Fn. 91), 311.

135 Vgl. https://smartvalor.com/de/decentraland.

D. Regulierung von DAOs de lege ferenda

Die Europäische Union sieht einen fragmentarischen Rechtsrahmen bei der Regulierung von DAOs und hat eine Studie zur Aufsicht über dezentralisierte Finanzdienstleistungen in Auftrag für eine Regulierung *de lege ferenda* gegeben.[136] In Wyoming gilt seit dem 1.7.2021 ein neues Gesetz mit dem sich DAOs als Limited Liability Company (LLC) registrieren lassen können.[137] Einen ähnlichen Ansatz verfolgt das kommentierte Mustergesetz „*Model Law for Decentralized Autnomous Organizations (DAOs)*.[138] Der Vorteil der Haftungsbeschränkung für DAOs liegt auf der Hand.[139] Die Geschäftsführung einer solchen DAO LLC kann dabei entweder durch ihre Mitglieder oder einen Smart Contract übernommen werden, wobei im letzteren Falle, einer algorithmenbasierten Geschäftsführung, die zugrundeliegenden Smart Contracts aktualisierbar und modifizierbar bleiben müssen.[140] Vor dem Hintergrund der Ausgangsfrage wird damit deutlich, dass die Erweiterung des LLC Act in Wyoming den Weg einer Rechtsformvariante, statt einer Rechtsformneuschöpfung geht,[141] welches sich konzeptionell ins deutsche Recht übertragen ließe. So müssten folglich die Entwickler oder Projektbeteiligten sich a priori Einwirkungsmöglichkeiten in Form von Administratorenrechten offenhalten, was diese auch zu Adressaten im Sinne einer effektiven Gefahrenabwehr macht, im Gegenzug aber der eigentlichen Intention von Dezentralisation, also einer Vermeidung einer zentralen Geschäftsführung, zuwiderläuft.

E. Zusammenfassung

1. DAOs sind auf Dauer angelegte *Organisationen*, die aus einer Vielzahl von Smart Contracts bestehen, die über die Blockchain *dezentral* abgewickelt werden. Da die Geschäftsleitungsorgane durch Smart Contracts

136 *E. Naudts*, Occasional Paper Series No. 331 The future of DAOs in finance In need of legal status, S. 24, verfügbar unter: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op331~a03e416045.en.pdf.
137 Wyoming Decentralized Autonomous Organization Supplement, SF0038, 66th Leg., Gen. Sess. 2021.
138 Coalition of Automated Legal Applications (COALA), 2021, https://coala.global/wp-content/uploads/2022/03/DAO-Model-Law.pdf.
139 Siehe dazu ausführlich *Fleischer*, Die Wyoming DAO LLC (Fn. 70), 2207.
140 *Fleischer*, Die Wyoming DAO LLC (Fn. 70), 2211.
141 *Fleischer*, Die Wyoming DAO LLC (Fn. 70), 2213.

ersetzt wurden, sind solche Organisationen aufgrund der Algorithmen *autonom* und werden durch ihre Mitglieder selbst und unmittelbar verwaltet. Bei der *Decentraland DAO* handelt es sich allerdings nur eine semi-dezentrale Organisation. Indikator dafür, ob ein System dezentral oder nur semi-dezentral ist, bilden Administratorenrechte.

2. *De lege lata* sind DAOs gesellschaftsrechtlich regelmäßig als Publikums-GbRs zu qualifizieren und damit auch beteiligtenfähig im Verwaltungsverfahren. Gehen von einer komplett dezentral organisierten DAO Gefahren aus, so können die einzelnen Mitglieder der DAO als Mehrheit von (Verhaltens-)Störern in Anspruch genommen werden.

3. Aufsichtsrechtlich können bei DAOs taugliche Normadressaten in formeller und materieller Hinsicht ermittelt werden, indem entweder ein Rechtssubjekt der DAO formell „vorgeschaltet" ist oder den Initiatoren bzw. Projektbeteiligten der DAO noch materiell Administratorenrechte zustehen.

4. Zweckmäßig erscheint eine Regulierung *de lege ferenda* – am Beispiel von Wyoming oder dem Model Law Mustergesetz – bei der Projektbeteiligten oder Initiatoren von DAOs Administratorenrechte vorbehalten bleiben müssen, auf die dann im Sinne einer effektiven Gefahrenabwehr zurückgegriffen werden kann.

Immersion, Interoperabilität und Inhaltsmoderation: Welche Auswirkungen hat der Digital Services Act auf virtuelle Welten?

Daniel Hauck

A. Einführung

Virtuellen Welten werden zahlreiche Potentiale zugeschrieben. Während analoge Begegnungsorte, an denen Bürger im Alltag aus ihren gewohnten Milieus ausbrechen, durch das Internet zunehmend abgelöst werden,[1] können virtuelle Welten, wie sie etwa das Metaverse verspricht, neue Begegnungsmöglichkeiten schaffen. Außerdem versprechen sie, wirtschaftliche Prozesse effizienter zu gestalten sowie die Entwicklung und den Handel mit virtuellen Gütern, Arbeitsplätze, Sport, Kultur, Bildung, Therapie, Tourismus, Stadtplanung, Medien und Formen sozialer Interaktion neu zu erschließen.[2] Es leuchtet deshalb ein, dass u.a. große Tech-Konzerne zunächst hohe Investitionen in ihre Entwicklung tätigten. Nach einer ersten Welle der Begeisterung auf Seiten der Investoren wurden einige Initiativen indes wieder eingestellt oder deren Finanzierung verringert, da sie von Nutzern

1 *L. Jacobsen*, Öffentlicher Raum: Bloß nicht noch ein Begegnungscafé!, Die Zeit, 19.08.2024.

2 Zahlreiche Anwendungsfelder bei *J. Broschart et al.*, § 1 Definition und Bedeutung des „Metaverse", in: H. Steege/B. Chibanguza/M. Bagratuni (Hrsg.), Metaverse, Baden-Baden 2023, S. 41 (Rn. 64); *Y. Dwivedi et al.*, Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy, International Journal of Information Management 66 (2022), 1 (6 f.); *M. Jacobides et al.*, Building synthetic worlds: lessons from the excessive infatuation and oversold disillusionment with the metaverse, Industry and Innovation 2024, 105 (114); *M. Quent*, Demokratische Kultur und das nächste Internet: Chancen und Risiken virtueller immersiver Erfahrungsräume im Metaverse, in: Institut für Demokratie und Zivilgesellschaft (Hrsg.), Wissen schafft Demokratie. Schwerpunkt Netzkulturen und Plattformpolitiken, Jena 2023, S. 30 (34 f.).

nicht erwartungsgemäß angenommen wurden.[3] Nichtsdestotrotz glauben manche weiterhin an das Potenzial virtueller Welten.[4]

Verschiedene Anwendungsfälle machen deutlich, dass virtuelle Welten Vorteile für demokratische Gesellschaften mit sich bringen und z.B. demokratiefördernd wirken können: Die Nichtregierungsorganisation Reporter ohne Grenzen, die sich weltweit für die Pressefreiheit engagiert, ermöglicht mit dem Projekt „The Uncensored Library" der Bevölkerung in autoritären Staaten über das Computerspiel Minecraft Zugang zu gesperrten journalistischen Inhalten.[5] Darüber hinaus verheißen virtuelle Welten, bestimmten Personengruppen die gesellschaftliche Teilhabe gegenüber der analogen Welt zu erleichtern.[6]

Jedoch bergen virtuelle Welten auch Risiken. Sie drohen, den direkten Kontakt zwischen Menschen zu ersetzen, zur Bildung von Echokammern und so zur zunehmenden Isolierung innerhalb der Gesellschaft beizutragen.[7] Bestehende soziale Ungleichheiten können im digitalen Raum reproduziert werden – insb. muss hinterfragt werden, ob virtuelle Welten ein inklusiver Raum sein können, zu dem alle gleichberechtigt Zugang haben.[8] Darüber hinaus können Hassrede und Desinformationen ihre destruktive Wirkkraft[9] stärker entfalten.[10] Neuen Formen digitaler Gewalt und anderen Risiken virtueller Welten durch wirksame Moderationsmechanismen zu begegnen, stellt Plattformbetreiber und Gesetzgeber vor eine große Herausforderung.[11] Schließlich werden privaten Unternehmen neue Einflussmög-

3 *Jacobides et al.*, Synthetic (Fn. 2), 106, 112 f., 120 f.; *F. Maschewski/A. Nosthoff*, § 4 Jenseits immersiver Demokratie: digitalkapitalistische und soziopolitische Dimension des Metaverse, in: H. Steege/B. Chibanguza/M. Bagratuni, (Hrsg.), Metaverse Baden-Baden 2023, S. 87 (Rn. 2, 7).

4 *Jacobides et al.,* Synthetic (Fn. 2), 106, 122, 129.

5 https://www.reporter-ohne-grenzen.de/aktivitaeten/kampagnen/the-uncensored-library-1

6 *Dwivedi et al.,* Hype (Fn. 2), 9; *I. Hermann*, Demokratische Werte nach Europäischem Verständnis im Metaverse, Berlin 2022, S. 1 (10); *M. Kaulartz et al.*, Das Metaverse – eine rechtliche Einführung, RDi 2022, 521 (523).

7 *L. Floridi*, Metaverse: A Matter of eXperience, Philosophy & Technology 35, 73 (2022), 1 (6, 9).

8 *Maschewski/Nosthoff,* § 4 (Fn. 3), Rn. 20.

9 *B. Steinrötter*, § 1 Einleitung, in: B. Steinrötter (Hrsg.), Europäische Plattformregulierung, Baden-Baden 2023, S. 23 (Rn. 8); kritisch *A. Peukert*, Desinformationsregulierung in der EU – Überblick und offene Fragen, JZ 2023, 278 (285).

10 *I. Trauthig/S. Woolley*, Addressing Hateful and Misleading Content in the Metaverse, Journal of Online Trust and Safety 1:5 (2023), 1 (4 ff.).

11 Vgl. *Dwivedi et al.,* Hype (Fn. 2), 1; *Trauthig/Woolley,* Content (Fn. 10), 4.

lichkeiten auf Nutzer eröffnet, wodurch im Bereich der Plattformökonomie bestehende Machtstrukturen sich weiter zu festigen drohen.[12] Sie sind deshalb zurecht Gegenstand rechtswissenschaftlicher und politischer Debatten.[13]

Vor diesem Hintergrund sollen im Folgenden die Anwendbarkeit und Wirksamkeit des Digital Services Act (DSA)[14], der u.a. die Regulierung sozialer Medien in den Blick nimmt, hinsichtlich der Inhaltsmoderation in sozialen virtuellen Welten, wie dem Metaverse, untersucht werden. Besonderes Augenmerk liegt auf den technischen Besonderheiten virtueller Welten.

B. Virtuelle Welten

Es wird eine Vielzahl virtueller Welten diskutiert, die sich zum Teil deutlich unterscheiden. Ideen wie das Metaverse befinden sich noch im Entwicklungsstadium,[15] andere Projekte, wie das Computerspiel Fortnite oder die virtuelle Welt Decentraland, die als „Vorstufe" des Metaverse bezeichnet werden,[16] sind bereits realisiert.

I. Das „Metaverse"

Inbegriff virtueller Welten ist die Idee des Metaverse. Das Metaverse wird im Wesentlichen als virtuelle Welt beschrieben, die auf dem täglichen Leben basiert und in die Nutzer bspw. mittels eines Avatars eintauchen, um an politischen, wirtschaftlichen, sozialen oder kulturellen Aktivitäten

12 Vgl. *L. Rosenberg,* Regulation of the Metaverse: A Roadmap, in: Association for Computing and Machinery (Hrsg.), 6th International Conference on Virtual and Augmented Reality Simulations, New York 2022, S. 21 (22).

13 Zur Strategie der EU-Kommission Pressemitteilung v. 11.7.2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3718.

14 Verordnung (EU) 2022/2065, Abl. L 277/1 v. 27.10.2022.

15 *F. Buchholz et al.*, There's more than one metaverse, Journal of Interactive Media 2022, 313 (319); *M. Martini/J. Botta*, Der Staat und das Metaversum, MMR 2023, 887 (888); *D. Robertson,* How to regulate a universe that doesn't exist, https://www.politico.com/newsletters/digital-future-daily/2023/02/08/how-to-regulate-a-universe-that-doesnt-exist-00081895.

16 *Martini/Botta,* Staat (Fn. 15), 888 f.

teilnehmen zu können[17] – quasi eine „begehbare Version des Internets".[18] Diese besteht aus einer Vielzahl miteinander verknüpfter virtueller Räume.[19] Innerhalb dieser Räume können Unternehmen und Entwickler (kommerzialisierbare) Inhalte erschaffen. Software-Anbieter stellen die nötigen Werkzeuge für die Erstellung und den Betrieb der virtuellen Umgebung, einschließlich Blockchain- und „Zwillingstechnologien", bereit. Die erforderliche Infrastruktur wird von Plattformbetreibern unterhalten.[20]

Die Diskussion entspinnt sich allerdings primär an einem Schlagwort der Absatzwirtschaft.[21] Ein Blick auf die an der Entwicklung des Metaverse beteiligten Unternehmen verdeutlicht, dass es sich bei virtuellen Welten oft um ein „Update für das Geschäftsmodell"[22] großer Konzerne handelt, die bereits in anderen Sektoren über Marktmacht verfügen.[23] Ein prominentes Bsp. ist der Meta-Konzern, welcher mit seinen Diensten wie Facebook und Instagram eine solche Vormachtstellung im Bereich sozialer Medien innehat[24] und nun mit neuen Produkten wie der Virtual Reality-Software Horizon Worlds und dem Meta Quest-Headset im Bereich virtueller Welten auf den Markt drängt. Im Übrigen fällt auf, dass bisher überwiegend entweder Unternehmen aus der Unterhaltungsbranche, die mit Werbung hohe Einnahmen erzielen und daher ein hohes ökonomisches Interesse an der umfangreichen Verarbeitung personenbezogener Daten zum Zwecke zielgerichteter Werbung haben,[25] oder große Digitalkonzerne an der Umsetzung virtueller Welten mitgewirkt haben. Exemplarisch genannt seien Google, Microsoft, Apple, Samsung, Nvidia, HTC, Roblox und Disney.[26]

17 *M. Ball,* The Metaverse: What It Is, Where to Find it, and Who Will Build It, https://www.matthewball.co/all/themetaverse; *Rosenberg,* Roadmap (Fn. 12), S. 22; *Quent,* Kultur (Fn. 2), S. 34.

18 *N. Höfler/H. Krolle*, Was hinter dem Metaverse-Hype steckt, Handelsblatt, 23.02.2023.

19 *Buchholz et al.,* More (Fn. 15), 319; *Kaulartz et al.,* Einführung (Fn. 6), 523; *Quent,* Kultur (Fn. 2), S. 34.

20 *Jacobides et al.,* Synthetic (Fn. 2), 115 f. Technische Grundlagen bei *Broschart et al.,* § 1 (Fn. 2), Rn. 13–45.

21 Kritisch zum Begriff Metaverse *Ball,* Metaverse (Fn. 17).

22 *Maschewski/Nosthoff,* § 4 (Fn. 3), Rn. 8.

23 Vgl. *Jacobides et al.,* Synthetic (Fn. 2), 124, 129.

24 *Floridi,* eXperience (Fn. 7), 1; *Maschewski/Nosthoff,* § 4 (Fn. 3), Rn. 8.

25 Vgl. *V. Xynogalas/M. Leiser*, The Metaverse: searching for compliance with the General Data Protection Regulation, International Data Privacy Law 2024, 89 (102).

26 *Dwivedi et al.,* Hype (Fn. 2), 5; *Broschart et al.,* § 1 (Fn. 2), Rn. 53-57; *Jacobides et al.,* Synthetic (Fn. 2), 110, 112, 118.

Die Umsetzung des Metaverse hängt stark von der künftigen technischen Entwicklung von Virtual Reality (VR)- und Augmented Reality (AR)-Technologien, dem Ausbau von 5G und deutlich erhöhter Rechenleistung der erforderlichen Hardware ab.[27] Daher ist unklar, wie das Metaverse schlussendlich ausgestaltet sein wird oder ob es sich überhaupt durchsetzt.

II. Konstitutive Eigenschaften virtueller Welten

Deshalb bietet sich ein rechtsguts- oder gefahrbezogenes Verständnis, anknüpfend an die besonderen Gefahren ausgehend von Immersion und Interoperabilität als den besonderen Eigenschaften virtueller Welten an.[28]

1. Immersion

Immersion bedeutet, dass die gleichen physiologischen und psychologischen Reaktionen ausgelöst werden wie in der analogen Welt.[29] Hierdurch unterscheiden sich virtuelle Welten maßgeblich von „klassischen" Internetanwendungen wie sozialen Medien.[30]

Die Immersion wird durch datenintensive VR- und AR-Technologien ermöglicht.[31] VR meint einen scheinbar in Echtzeit generierten computergestützten Raum, der entweder die Wirklichkeit oder eine Fiktion abbildet. AR meint dagegen die computergestützte Erweiterung der Wahrnehmung der analogen Welt. D.h. es wird keine vollständige virtuelle Welt generiert, sondern ein kombiniert real-virtueller Raum[32] geschaffen. Zugang hierzu erlangen Nutzer mittels verschiedener Hardware, etwa einer VR-Brille, Kinect-Systemen, „Wearables" oder eines Smartphones.[33]

Wie tief Nutzer in die (teil-)virtuelle Realität eintauchen, hängt von einer Vielzahl von Faktoren ab, insb. Realismus und zeitlicher Synchronität der erzeugten Welt, Leistungsfähigkeit der verwendeten Hardware sowie

27 *Martini/Botta,* Staat (Fn. 15), 888.
28 Vgl. *Rosenberg,* Roadmap (Fn. 12), S. 22.
29 *E. Hine*, Content Moderation in the Metaverse Could Be a New Frontier to Attack Freedom of Expression, Philosophy & Technology 36, 43 (2023), 1 (2); *Trauthig/Woolley,* Content (Fn.10), 2.
30 *Quent,* Kultur (Fn. 2), S. 34.
31 *Trauthig/Woolley,* Content (Fn. 10), 5.
32 AR-Technologien werden deshalb gelegentlich auch als Mixed Reality bezeichnet.
33 Vgl. *Kaulartz et al.,* Einführung (Fn. 6), 523.

der verwendeten Technologie und der hierdurch angesprochenen Sinne.[34] Dabei gibt es noch technisch bedingte Limitierungen, etwa bei der Wahrnehmung von Berührungen, Schwerkraft, Geschmäckern und Gerüchen.[35]

2. Interoperabilität

Eine immersive Erfahrung im Metaverse i.S. eines plattformübergreifenden Kosmos virtueller Welten setzt die nahtlose Verbindung der einzelnen Welten voraus. Nutzer sollen Gegenstände und Währungen von einem Element ins Nächste mitnehmen können.[36] Der unionale Gesetzgeber beschreibt eine solche Interoperabilität im Digital Markets Act (DMA)[37] als die Fähigkeit, Informationen auszutauschen und die über Schnittstellen oder andere Lösungen ausgetauschten Informationen beiderseitig zu nutzen, sodass alle Hardware- oder Softwarekomponenten mit anderer Hardware und Software auf die vorgesehene Weise zusammenwirken und bei Nutzern auf die vorgesehene Weise funktionieren (Art. 2 Nr. 29 DMA). Auf diese Legaldefinition kann nur zurückgegriffen werden, soweit der DMA anwendbar ist, also ein zentraler Plattformdienst i.S. der Art. 1 Abs. 2, 2 Nr. 2 DMA vorliegt. Dies dürfte hinsichtlich einzelner sozialer virtueller Welten der Fall sein, wenn diese als „Online-Dienste sozialer Netzwerke" i.S. von Art. 2 Nr. 2 lit. c), 7 DMA eingeordnet werden können. Im Übrigen sind neue Anwendungen virtueller Welten nicht erfasst. Die EU-Kommission kann gem. Art. 19 Abs. 1 DMA zwar neue Dienste als zentralen Plattformdienst vorschlagen, den abschließenden Katalog in Art. 2 Nr. 2 DMA aber nicht durch einen delegierten Rechtsakt ändern. Dieser muss im Wege des ordentlichen Gesetzgebungsverfahrens erweitert werden, da es sich um einen wesentlichen Teil der Verordnung handelt (vgl. Art. 290 Abs. 1 UAbs. 1 AEUV).[38] Die Vorschrift kann aber als Vorbild für die spätere Regulierung des Metaverse hinsichtlich der Beschreibung seiner Eigenschaften dienen.

---

34 *Quent,* Kultur (Fn. 2), S. 34 f.

35 Vgl. *Dwivedi et al.,* Hype (Fn. 2), 4; *Floridi,* eXperience (Fn. 7), 6; *Kaulartz et al.,* Einführung (Fn. 6), 523.

36 *Ball,* Metaverse (Fn. 17); *Höfler/Krolle,* Metaverse-Hype (Fn. 18); *Martini/Botta,* Staat (Fn. 15), 888; *Quent,* Kultur (Fn. 2), S. 34. Dagegen *Rosenberg,* Roadmap (Fn. 12), S. 22.

37 Verordnung (EU) 2022/1925, Abl. L 265/1 v. 12.10.2022.

38 *M. Kettemann/M. Müller*, § 7 Plattformregulierung, in: H. Steege/B. Chibanguza/M. Bagratuni (Hrsg.), Metaverse, Baden-Baden 2023, S. 135 ff. (Rn. 34).

Technisch setzt Interoperabilität voraus, dass Informationen, Daten und Metadaten derart miteinander vernetzt werden, dass eine effiziente Kommunikation zwischen den beteiligten Systemen gewährleistet ist.[39] Welche technischen Standards oder Schnittstellen letztlich dafür erforderlich sein werden, bleibt abzuwarten.[40] Die Verknüpfung verschiedener virtueller Welten mit ihren eigenen Regeln und technischen Gesetzen stellt aktuell jedenfalls eine große Herausforderung bei der Umsetzung des Metaverse dar.[41] Jenseits der technischen Herausforderungen ist zudem fraglich, ob die Plattformbetreiber eine enge Zusammenarbeit überhaupt anstreben. Die Vergangenheit hat gezeigt, dass Unternehmen wie Apple oder Microsoft Interoperabilität nicht aus Eigenmotivation anstreben, um von Lock-In- und Netzwerkeffekten zu profitieren.[42] Dieses Problem ließe sich gesetzgeberisch über Interoperabilitätsvorschriften wie Art. 6 Abs. 4 und 7, 7 DMA lösen.

3. Digitale Identitäten

Die Idee des Metaverse und anderer virtueller Welten wird oft derart beschrieben, dass Nutzer sie mittels eines digitalen Abbilds ihrer selbst betreten. Avatare oder andere digitale Identitäten sind dabei typisch, aber keineswegs zwingendes Kriterium. Vielmehr sind auch nicht Avatar-basierte Realitäten denkbar, insb. im Bereich der AR-Anwendungen.[43]

III. Risiken virtueller Welten

Aufgrund dieser Eigenschaften bergen virtuelle Welten Risiken.

1. Immersionsbezogene Risiken

Abhängig vom Grad der Immersion können Nutzer emotional und kognitiv direkter adressiert werden. Dadurch, dass virtuelle Welten realistischer als das heutige Internet wirken, können neue Manipulationsmöglichkeiten ge-

39 *Broschart et al.,* § 1 (Fn. 2), Rn. 14.
40 *Kaulartz et al.,* Einführung (Fn. 6), 524; kritisch *Floridi,* eXperience (Fn. 7), 5.
41 *Dwivedi et al.,* Hype (Fn. 2), 12; *Jacobides et al.,* Synthetic (Fn. 2), 115.
42 Vgl. *Jacobides et al.,* Synthetic (Fn. 2), 112, 123.
43 Vgl. *Ball,* Metaverse (Fn. 17).

genüber Verbrauchern (sog. Dark Patterns),[44] politisches Microtargeting, die Entstehung von Echokammern, innerhalb derer sich Nutzer radikalisieren oder isolieren, Überwachungsmechanismen, „Zensur", Desinformationen, Hassrede und andere Formen digitaler Gewalt, wie sexuelle Belästigung, ihr destruktives Potential stärker entfalten.[45]

Denn Nutzer erleben VR-Anwendungen multisensorisch, Wort und Schrift stehen nicht zwingend als Kommunikationsmedium im Mittelpunkt. Maßgeblich ist das gesamte Verhalten der digitalen Identität, d.h. Bewegung, Ton, Sprache und Artikulation. Echtzeitkommunikation sowie nonverbale Äußerungsmöglichkeiten können Plattformbetreiber bei der Moderation der Inhalte vor neue Herausforderungen stellen, da sie schwieriger auf problematische Inhalte untersucht werden können als textbasierte Beiträge.[46]

Die stärkere emotionale Erreichbarkeit der Nutzer rührt auch daher, dass diese sich mit ihrem Avatar identifizieren können[47] und die zum Betrieb virtueller Welten erforderliche Verarbeitung sensibler Daten und ggf. deren Verknüpfung mit bereits gespeicherten Daten[48] genauere Rückschlüsse auf Nutzer und somit deren noch persönlichere Ansprache ermöglicht.[49]

Die Ansprache kann daher psychologisch potenter sein als auf klassischen Plattformen.[50] Formen der Belästigung etwa können sich grundlegend unterscheiden. Erfahrungsberichte schildern sexuelle Belästigungen in virtuellen Welten eindrücklich.[51] Erste empirische Befunde deuten darauf hin, dass Des- und Fehlinformationen durch die Immersion schwieriger zu erkennen sind.[52] Denkbar sind auch von sog. Fake-Avataren ausgehende

44 *M. Gertz et al.*, Dark Patterns – eine interdisziplinäre Analyse, LTZ 2023, 3.
45 *C. Nehring*, Manipulation und Desinformation im Metaverse, Berlin 2023, S. 1 (2 f.); *Quent,* Kultur (Fn. 2), S. 36; *Rosenberg,* Roadmap (Fn. 12), S. 23.
46 Vgl. *Quent,* Kultur (Fn. 2), S. 35.
47 *J. Wolfendale*, My avatar, my self: Virtual harm and attachment, Ethics Inf Technol 2007, 111.
48 Umfassend zur datenschutzrechtlichen Bewertung *L. Bender-Paukens/S. Werry*, Datenschutz im Metaverse, ZD 2023, 127; *Xynogalas/Leiser,* Compliance (Fn. 25), 93 f., 102.
49 Vgl. *Maschewski/Nosthoff,* § 4 (Fn. 3), Rn. 21.
50 Vgl. *Trauthig/Woolley,* Content (Fn. 10), 5 f., 7.
51 *E. Kühl*, Horizon Worlds: Kaum eingeloggt, schon angegrapscht, Die Zeit, 17.12.2021; *Maschewski/Nosthoff,* § 4 (Fn. 3), Rn. 16.
52 *Hermann,* Werte (Fn. 6), S. 9; *Trauthig/Woolley,* Content (Fn. 10), 5 f.

Gefahren, hinter denen eine andere Person als die vermeintliche oder gar ein Programm steckt.[53]

All dies betrifft Rechtsgüter Einzelner sowie demokratische Prozesse insgesamt. Setzten sich virtuelle Welten in der breiten Öffentlichkeit durch, kann sich der gesellschaftliche Diskurs weiter ins Digitale verlagern. Der demokratische Willensbildungsprozess ist dadurch noch stärker nach privatwirtschaftlichen Prinzipien organisierten Plattformen und den ökonomischen Interessen ihrer Betreiber ausgesetzt.[54]

2. Interoperabilitätsbezogene Risiken

Die beschriebene Interoperabilität kann Probleme bei der Ermittlung des räumlichen Anwendungsbereichs von Rechtsakten, der grenzüberschreitenden Inhaltsmoderation und der Durchsetzung von Moderationsentscheidungen bereiten. Schwierigkeiten sind insb. bei der Identifikation von Nutzern zur Durchsetzung von Ansprüchen, etwa wegen Verletzungen des allgemeinen Persönlichkeitsrechts, vorstellbar.[55]

3. Teilhabebezogene Risiken

Ferner muss das Versprechen virtueller Welten, eine inklusive und gleichberechtigte Welt zu sein, kritisch hinterfragt werden. Bspw. können auf der Plattform Decentraland Nutzer über die Entwicklung und Verwaltung dieser virtuellen Welt abstimmen. Das Stimmgewicht hängt jedoch vom Guthaben der digitalen Währung ab. Stimmen derjenigen, die in der digitalen Welt „reicher" sind, zählen mehr als die Stimmen weniger wohlhabender Nutzer. Dies ist mit dem für staatliche Wahlen geltenden demokratischen Grundprinzip der Zählwertgleichheit von Stimmen unvereinbar[56] und verdeutlicht, dass virtuelle Welten keinesfalls gleichberechtigt sein müssen. Ferner können bestimmte Bevölkerungsgruppen z.B. mangels finanzieller Mittel von der Nutzung der kostspieligen Technologien ausgeschlossen sein.

---

53 *Kaulartz et al.,* Einführung (Fn. 6), 525; *Maschewski/Nosthoff,* § 4 (Fn. 3), Rn. 17.
54 *Hermann,* Werte (Fn. 6), S. 3 f.
55 *Hine,* Moderation (Fn. 29), 1 ff.
56 *Quent,* Kultur (Fn. 2), S. 41.

Außerdem besteht die Gefahr, dass im Bereich der Plattformregulierung existierende Vollzugsdefizite auch im Metaverse bestehen.[57] Diesen Risiken muss der Gesetzgeber aufgrund des Vorsorgeprinzips begegnen, wenn das geltende Recht sie nicht bereits adäquat adressiert.

C. Regulierung virtueller Welten durch den DSA

Auf Unionsebene soll der DSA die Voraussetzungen für ein sicheres Online-Umfeld schaffen, in welchem Innovationen gefördert, Grundrechte wirksam geschützt und damit ein Beitrag zum reibungslosen Funktionieren des Binnenmarktes geleistet wird (Art. 1 Abs. 1, ErwG 3 DSA). Der DSA nimmt u.a. soziale Medien in den Blick. Da virtuelle Welten als „dreidimensionale soziale Netzwerke" ähnliche Risiken bergen und nach einem vergleichbaren Geschäftsmodell betrieben werden, liegt es nahe, ihre Regulierung durch den DSA zu untersuchen.

I. Anwendbarkeit des DSA

Während der europäische Gesetzgeber davon ausgeht, das Metaverse bei Erlass des Regulierungspakets bestehend aus DSA und DMA nicht erfasst zu haben,[58] sind sich weite Teile der Literatur einig, dass der DSA teilweise auf virtuelle Welten Anwendung findet – jedenfalls soweit es sich um Vermittlungsdienste i.S. des Art. 2 Abs. 1 DSA handelt, die Nutzern in der EU angeboten werden.[59] Der räumliche Anwendungsbereich ist regelmäßig

57 *Maschewski/Nosthoff,* § 4 (Fn. 3), Rn. 23.

58 Vgl. *Rat der Europäischen Union*, Metaverse – Virtual World, Real Challenges, Council Research Paper, 2022, S. 1 (12), https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf. Der wissenschaftliche Dienst des Europäischen Parlaments hält die Frage nach der Anwendbarkeit der Moderationsvorschriften des DSA auf rechtswidrige oder schädliche Inhalte in virtuellen Welten nicht für abschließend geklärt *Wissenschaftlicher Dienst*, Metaverse – Opportunities, risks and policy implications, 2022, S. 1 (7), https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf.

59 Ohne Begründung *Bender-Paukens/Werry,* Datenschutz (Fn. 48), 130; *Hermann,* Werte (Fn. 6), S. 8; *J. Jaursch*, Der DSA gilt auch „im Metaverse", Tagesspiegel Background, 14.12.2022; *Kaulartz et al.,* Einführung (Fn. 6), 529; *M. Kettemann et al.*, Ordnungsansätze für immersive Welten: eine Einführung in die Regulierung der Metaverse, 2023, S. 3; *Martini/Botta,* Staat (Fn. 15), MMR 2023, 895; *H. Strobl*, Virtuelle

eröffnet, da virtuelle Welten auch Nutzern mit Niederlassungsort oder Sitz in der EU angeboten werden. Maßgeblich ist die physische Präsenz im Unionsgebiet.[60]

Vermittlungsdienste sind Dienstleistungen der Informationsgesellschaft i.S. von Art. 3 lit. a) DSA i.V.m. Art. 1 Abs. 1 lit b) Richtlinie (EU) 2015/1535, namentlich Access-, Caching- und Hosting-Provider (Art. 3 lit. g) DSA). Hierunter fallen jedenfalls die sozialen Medien ähnlichen Funktionen virtueller Welten. Der EuGH hat das Netzwerk Facebook bereits als Hostingdienst i.S. der E-Commerce-Richtlinie[61] eingeordnet.[62] Es liegt nahe, dass der DSA als deren Nachfolgeregelwerk dem inhaltlich entspricht.[63] Die erbrachte Dienstleistung besteht darin, die von Nutzern über die beschriebenen VR- und AR-Geräte individuell bereitgestellten Informationen über verbale sowie non-verbale Kommunikationsinhalte, die Ausgestaltung des Avatars, Bewegungen, die Übertragung virtueller Gegenstände u.a. Handlungsformen zu speichern und anderen Nutzern darzustellen, also den Austausch von Inhalten ohne gleichzeitige physische Anwesenheit zu ermöglichen. Hierbei operieren Betreiber virtueller Welten regelmäßig werbungs- oder datenfinanziert. Sie sind daher als Hosting-Dienste i.S. von Art. 3 lit. g) iii) DSA einzuordnen.

Fraglich ist aber, ob es sich – je nach Nutzerzahl – um (sehr große) Online-Plattformen i.S. der Art. 3 lit. i), 33 Abs. 1 DSA handelt, abhängig davon, ob sie mehr als 45 Millionen aktive monatliche Nutzer in der EU haben. Für die Einordnung als Online-Plattform kommt es entscheidend darauf an, ob die nutzergenerierten Inhalte öffentlich verbreitet werden und die Verbreitung nicht lediglich eine unbedeutende untrennbar verbundene Nebenfunktion oder untergeordnete Funktion des Hauptdienstes darstellt. Die beschriebenen gespeicherten Inhalte, wie die Ausgestaltung des Avatars und dessen Verhalten, sind im virtuellen Raum für andere Nutzer wahrnehmbar, also einem potenziell unbegrenzten Personenkreis zugänglich (Art. 3 lit. k) DSA). Diese öffentliche Verbreitung der durch die Nutzer bereitgestellten Inhalte steht jedenfalls bei sozialen virtuellen Welten im Fokus, sodass es sich nicht um eine bloße Nebenfunktion handelt.

Welten, reale Rechte: Die Durchsetzung des Urheberrechts im Metaverse, ZUM 2023, 492 (495 f.).

60 Vgl. *Kaulartz et al.,* Einführung (Fn. 6), 525.

61 Richtlinie (EG) 2000/31, Abl. L 178/1 v. 17.7.2000.

62 EuGH NJW 2019, 3287 (Rn. 22).

63 *Steinrötter/Schauer*, § 2 (Fn. 74), Rn. 16.

Virtuelle Welten sind daher regelmäßig als Online-Plattformen adressiert, für welche neben Art. 11–18 DSA auch die zentralen Vorschriften für Online-Plattformen (Art. 19–32 DSA) und sehr große Online-Plattformen (Art. 34 f. DSA) gelten. Durch diese werden Betreibern abhängig von ihrer Reichweite, und der damit einhergehenden systemischen Bedeutung für den Meinungsbildungsprozess, abgestuft Pflichten auferlegt.[64]

II. Regulierungsstrukturelle Probleme in Bezug auf virtuelle Welten

Der DSA wählt einen Ansatz der privaten Rechtsdurchsetzung und Selbstregulierung. Im Kern verpflichtet der DSA Plattformbetreiber dazu, innerhalb eines Melde- und Abhilfeverfahrens Moderationsentscheidungen über rechtswidrige Inhalte zu treffen (Art. 16 DSA). Dabei haften sie grundsätzlich nicht für rechtswidrige Inhalte ihrer Nutzer (Art. 4–6 DSA).[65] Hinsichtlich der Inhaltsmoderation ergeben sich für virtuelle Welten mit traditionellen sozialen Medien vergleichbare regulierungsstrukturelle Probleme.

1. Der Rechtswidrigkeitsmaßstab

Bereits der Maßstab für die Illegalität der durch die Nutzer bereitgestellten Inhalte ist unklar. Die EU-Kommission fürchtete angesichts zunehmend divergierender nationaler Regelungen, dass grenzüberschreitende digitale Leistungen erschwert und der Binnenmarkt dadurch beeinträchtigt würde (ErwG. 2 S. 1 f. DSA). Der DSA stellt daher auf das Unionsrecht und das gesamte Recht aller Mitgliedsstaaten ab (Art. 3 lit. t DSA)). Dies führt jedoch entweder zu einem unübersichtlich umfangreichen Maßstab. Oder es ergeben sich Beurteilungsschwierigkeiten im Bereich grenzüberschreitender Moderationsentscheidungen, da die nationalen Regelungen sich im Detail, jenseits rechtsvereinheitlichender europäischer Rechtsakte, teilweise voneinander unterscheiden.[66] Insb. im für die Meinungsfreiheit besonders

64 *S. Kuhlmann/H. Trute*, Die Regulierung von Desinformationen und rechtswidrigen Inhalten nach dem neuen Digital Services Act, GSZ 2022, 115.

65 Umfassend zur Regulatorik des DSA *S. Gerdemann/G. Spindler*, Das Gesetz über digitale Dienste (Digital Services Act) (Teil 1) GRUR 2023, 3; *S. Gerdemann/G. Spindler*, Das Gesetz über digitale Dienste (Digital Services Act) (Teil 2), GRUR 2023, 115.

66 *Kuhlmann/Trute,* Regulierung (Fn. 64), 118 f.

relevanten Bereich der Äußerungs- und Verhetzungsdelikte bestehen im europäischen Vergleich Unterschiede.[67] Auch im Urheberrecht können sich wegen des dort geltenden Schutzland- und Territorialitätsprinzips Unterschiede für die Darstellung der virtuellen Welt ergeben.[68] Die unterschiedliche rechtliche Realität in den Mitgliedsstaaten kann sich auch in virtuellen Welten auswirken und steht der Idee des immersiven gemeinsamen Erlebens diametral entgegen. Denn virtuelle Welten zeichnen sich gerade dadurch aus, dass Personen verschiedener Jurisdiktionen zusammentreffen, aber gemeinsam eine virtuelle Umgebung wahrnehmen. Das Szenario, dass Nutzer aus verschiedenen Ländern zwar im Metaverse nebeneinander stehen, aber unterschiedliche Welten wahrnehmen oder dass die Maßstäbe für (noch) zulässige Inhalte sich am Recht der strengsten Jurisdiktion orientieren und so die Meinungsfreiheit in den übrigen Mitgliedsstaaten einschränken, ist leicht vorstellbar.[69] Denn bei der Moderation von Inhalten stehen Anbieter vor der Herausforderung, die jeweils löschpflichtigen Inhalte für jeden Mitgliedsstaat gesondert zu identifizieren. Dies birgt die Gefahr, dass sie den Fokus zur Vereinheitlichung künftig vermehrt auf Allgemeine Geschäftsbedingungen legen und in Ausübung ihres „digitalen Hausrechts" vielerorts über die gesetzlichen Vorgaben hinausgehen.[70] So würden Anbieter in weiten Teilen der EU einen über das jeweilige nationale Recht hinausgehenden Maßstab etablieren und damit die Grenze zulässiger Inhalte dauerhaft verschieben.

Offen lässt der DSA auch, wie vorzugehen ist, wenn es zu einer Auseinandersetzung über behördliche Anordnungen gem. Art. 9 DSA kommt, etwa Anbieter der Anordnung nicht nachkommen oder Rechtsschutz suchen. Besonders bei grenzüberschreitenden Sachverhalten, die eher der Regelfall als die Ausnahme sein dürften, erlangt dies Relevanz. Auch wenn die Erwägungen des Verordnungsgebers dafür sprechen, dass sich Vollstreckung und mögliche Rechtsbehelfe nach dem jeweiligen Recht des anordnenden Staats richten sollen (vgl. ErwG 29 DSA), verhält sich der verfügende Teil des DSA dazu nicht konkret, obwohl die Erfahrungen zeigen, wie voraus-

67 Trotz des Harmonisierungsversuchs durch den EU-Rahmenbeschluss 2008/913/JI stellte die EU-Kommission fest, dass sich die vorhandenen mitgliedsstaatlichen Verhetzungstatbestände und deren Interpretation durch Gerichte im Detail unterscheiden, COM(2014) 27 final, S. 4 ff. Eine Übersicht liefert *B. Weiler*, Der Tatbestand „Volksverhetzung" im europäischen Vergleich, Hamburg 2012, S. 157 ff.

68 Vgl. *Strobl,* Durchsetzung (Fn. 59), 494 f.

69 *Hine,* Moderation (Fn. 29), 1, 2, 4.

70 Vgl. BGHZ 230, 347 (Rn. 78 ff.) – juris.

setzungsvoll und schwierig sich grenzüberschreitende Rechtsdurchsetzung im Einzelfall gestaltet.[71]

2. Die Durchsetzung von Moderationsentscheidungen

Ein weiteres Problem ergibt sich mit Blick auf die Meldefunktion nach Art. 16 DSA. Im Zuge der Meldung rechtswidriger Inhalte soll zum Zweck ihrer Identifikation die URL-Adresse des Posts angegeben werden. Eine solche gibt es in einer voll interoperablen virtuellen Welt aber nicht zwingend. Zwar reichen nach Art. 16 Abs. 2 S. 2 lit. b Alt. 2 DSA auch andere „zweckdienliche Angaben zur Ermittlung des rechtswidrigen Inhalts".[72] Zu denken ist hier an Bildschirmaufnahmen, die Identifikation der Inhalte über die dem Metaverse zugrundeliegende Blockchain-Technologie oder anhand ihrer Transkription. Technische Lösungen wie die App „Netzbeweis"[73] können Abhilfe schaffen, indem sie unveränderbare PDF-Kopien bspw. von Chats erstellen und so Beweise sichern. Denkbar ist auch, dass die Informationen über sämtliche soziale Interaktion für eine begrenzte Zeit lokal, z.B. auf der VR-Brille, gespeichert werden und – falls z.B. ein Übergriff gemeldet wird – von Moderatoren überprüft werden.[74] Hierdurch wird die Identifikation rechtswidriger Inhalte jedoch aufwändiger. Zudem ist das umfangreiche Speichern von Informationen über das Nutzerverhalten auf Vorrat datenschutzrechtlich bedenklich.

Wegen der Interoperabilität stellt sich im Einzelfall auch die Frage, wie die Vorschriften des DSA und Moderationsentscheidungen effektiv vollzogen werden können. Offen bleibt wie vorübergehende Sperren nach Art. 23 Abs. 1 DSA für den Fall, dass Nutzer wiederholt rechtswidrige Inhalte bereitstellen oder Inhalte häufig missbräuchlich melden, durchgesetzt werden sollen. Da Avatare virtuelle Welten plattformübergreifend nutzen können (sollen) und die Grenzen zwischen den verschiedenen Diensten zunehmend verschwinden (sollen) muss genau festgelegt werden, wie weit eine solche Sperre reichen darf.[75] Ein vollständiger und genereller Ausschluss vom Zutritt zu virtuellen Welten ist – gemessen am Maßstab der Verhältnismäßigkeit – nur in Ausnahmefällen denkbar. Zur technischen Umsetzung

71 *Kuhlmann/Trute,* Regulierung (Fn. 64), 118.
72 *Martini/Botta,* Staat (Fn. 15), 896.
73 https://www.netzbeweis.com/.
74 *Kühl*, Angegrapscht (Fn. 51).
75 *Martini/Botta,* Staat (Fn. 15), 897.

bedarf es eines eindeutig zuordenbaren Nexus zwischen analoger und digitaler Identität, da es anders als im plattformzentrierten Internet keinen Account für die jeweiligen Dienste geben soll.

Beispiele für faktisch bestehende Vollzugsdefizite bzgl. der Inhaltsmoderation gibt es bereits: Ein Team von Journalisten entwickelte in Metas Horizon Worlds einen virtuellen Raum (das sog. Qniverse), in dem auf Facebook und Instagram gesperrte Desinformationen, Verschwörungstheorien und extremistische Inhalte geteilt wurden. Das Qniverse existierte trotz mehrfacher Meldung durch die Journalisten tagelang, Meta blieb zunächst untätig.[76]

3. Transparenz und Dark Patterns

Probleme bestehen auch hinsichtlich der Plattformbetreibern auferlegten Transparenzpflichten (z.B. Art. 10, 15, 17, 24 DSA). Die Verfügbarkeit von Informationen verspricht besseren Schutz von Betroffenenrechten und Diskurs, dadurch dass das Moderationsverhalten besser nachvollzogen und kontrolliert werden kann. Zu viele Informationen können jedoch überfordern und dadurch das Gegenteil bewirken.[77]

Zudem können Angaben, etwa die bzgl. Werbung gem. Art. 26 Abs. 1 lit. d) DSA zu erteilenden Informationen, das immersive Erlebnis in virtuellen Welten stören. Anzeigen können, vergleichbar mit den aus dem Datenschutzrecht bekannten „Cookie-Bannern", virtuelle Elemente der generierten Welt überlagern.

Des Weiteren verbietet Art. 25 Abs. 1 DSA Online-Plattformen, ihre Online-Schnittstellen so zu konzipieren, dass Nutzer manipuliert werden. Hierdurch sollen Dark Patterns vermieden werden (ErwG 67 DSA).[78] Die Kontrolle dessen dürfte sich schwierig gestalten.

76 *E. Baker-White,* Meta Wouldn't Tell Us How It Enforces Its Rules In VR, So We Ran A Test To Find Out, https://www.buzzfeednews.com/article/emilybakerwhite/meta-facebook-horizon-vr-content-rules-test.

77 *Martini/Botta,* Staat (Fn. 15), 895; *Trauthig/Woolley,* Content (Fn. 10), 9.

78 Umfassend *M. Martini et al.,* Dark Patterns im Scheinwerferlicht des Digital Services Act, MMR 2023, 323.

4. Aufsicht

Bzgl. der Aufsicht über die Einhaltung der Regeln des DSA stellen sich mit dem Datenschutzrecht vergleichbare Vollzugsprobleme, da der europäische Gesetzgeber das unter der Datenschutz-Grundverordnung (DSGVO)[79] geltende Herkunftslandprinzip, wonach die nationalen Behörden am jeweiligen Niederlassungsort der Anbieter für deren Aufsicht zuständig sind, in Art. 49 Abs. 2, 56 Abs. 1 DSA grundsätzlich übernommen hat. Die Aufsicht über die Einhaltung der Vorgaben des DSA übernehmen für sehr große Online-Plattformen die EU-Kommission (Art. 56 Abs. 2, 3 DSA) und im Übrigen der Koordinator für digitale Dienste im jeweiligen Mitgliedsstaat (Art. 56 Abs. 1, 49 Abs. 1 DSA). In Deutschland ist dies grundsätzlich die Bundesnetzagentur (§ 12 Abs. 1 DDG).

Den bereits in Bezug auf die DSGVO vorgebrachten Einwänden,[80] insb. Durchsetzungsdefiziten bei grenzüberschreitenden Verstößen, begegnete der Verordnungsgeber, indem er beim DSA das Herkunftslandprinzip modifizierte: Er sieht für die Bearbeitung grenzüberschreitender Anfragen Fristen vor (Art. 57 Abs. 3 DSA) und zentriert die Aufsicht über die spezifischen Pflichten sehr großer Online-Plattformen bei der EU-Kommission (Art. 56 Abs. 3 DSA), was die Gefahr einer Machtkonzentration auf EU-Ebene birgt.[81]

D. Lösungsvorschläge

Nach alledem gibt es auch für die Inhaltsmoderation in virtuellen Welten einen anwendbaren Rechtsrahmen. Insb. gelten die zentralen Vorgaben des DSA für (sehr große) Online-Plattformen. Virtuelle Welten sind kein rechtsfreier Raum. Aber: Es drohen chronische Vollzugsdefizite – gerade bei der grenzüberschreitenden Moderation von Inhalten –,[82] die vermieden werden müssen.

79 VO (EU) 2016/679, Abl. L 119/1 v. 4.5.2016.

80 *R. Achleitner*, § 8 Durchsetzung: Befugnisse von und Zusammenarbeit mit Behörden, in: B. Steinrötter (Hrsg.), Europäische Plattformregulierung, Baden-Baden 2023, S. 222 (Rn. 13); dazu *M. Ebers/K. Sein,* Data-driven Technologies – Challenges for Privacy and EU Data Protection Law, in: M. Ebers/K. Sein (Hrsg.), Privacy, Data Protection and Data-driven Technologies, London 2024, Chapter 1, S. 1 (9 ff.).

81 *Achleitner,* § 8 (Fn. 82), Rn. 57.

82 *Hine,* Moderation (Fn. 29), 2; *Trauthig/Woolley,* Content (Fn. 10), 7.

I. Technische Lösungen

Teilweise wird vorgeschlagen, auf Erfahrungen aus der Videospielbranche zurückzugreifen.[83] Technische Lösungen sind in Gestalt von „World-Building" zur Bekämpfung von Hassrede und digitaler Gewalt grundsätzlich vorstellbar. Denn 3D-Engines wie die Grafik-Engine Unreal 5 ermöglichen die Darstellung realistischer und komplexer Umgebungen, die dynamisch angepasst werden können.[84] Zur Vermeidung sexueller Belästigung sieht etwa Metas Horizon Worlds einen Mindestabstand zwischen Avataren vor, der einen Übergriff gar nicht erst zulässt bzw. eine Sicherheitszone, die auf Knopfdruck die Interaktion mit anderen Nutzern unterbrechen kann.[85]

Auch zum Zweck des Jugendschutzes sind verschiedene technische Lösungen vorstellbar. Effektive Altersverifizierungsmechanismen, die nicht leicht umgangen werden können, unterliegen jedoch besonderen datenschutzrechtlichen Anforderungen.[86]

Technische Lösungen bergen jedoch ein hohes Missbrauchspotenzial. Zensurszenarien und der Ausschluss aus virtuellen Welten sind denkbar. Zudem sind sie zum Teil situativ nicht praktikabel und verlagern die Verantwortung für den Umgang mit schädlichen Inhalten alleine auf die Nutzer.[87] Nutzerinnen schilderten etwa, dass sie im Moment eines Übergriffs zu geschockt waren, um die Sicherheitszone zu aktivieren.[88]

II. Verhaltensmoderation und „immersive Rechte"

Wegen der Unzulänglichkeiten technikbasierter Lösungsansätze wird teilweise eine professionelle Verhaltensmoderation gefordert, d.h. dass geschulte Moderatoren schnell eingreifen, um rechtswidriges und schädliches Verhalten zunächst nachzuweisen und anschließend zu sanktionieren. Dies erinnert an die Aufgaben, welche die Polizei in der analogen Welt wahrnimmt. Zurecht wird darauf hingewiesen, dass diese Form der Verhaltens-

83 *Martini/Botta,* Staat (Fn. 15), 895.
84 *Broschart et al.,* § 1 (Fn. 2), Rn. 43; *Quent,* Kultur (Fn. 2), S. 35.
85 *Martini/Botta,* Staat (Fn. 15), 891.
86 *M. Lück/P. Vogel*, Rechtmäßige Verarbeitung personenbezogener Daten Minderjähriger, in: C. Heinze/B. Steinrötter (Hrsg.), KI und Daten: Digitalregulierung auf dem Höhepunkt?, Edewecht 2024, S. 163 ff.
87 *Maschewski/Nosthoff,* § 4 (Fn. 3), Rn. 15 f.
88 *Kühl*, Angegrapscht (Fn. 51); *Maschewski/Nosthoff,* § 4 (Fn. 3), Rn. 15 ff.

moderation legitimiert und kontrolliert werden muss, um „Over-Policing" zu vermeiden.[89] Möglicherweise können das vom DSA vorgesehene interne Beschwerdemanagement (Art. 20 DSA), v.a. aber die außergerichtlichen Streitbeilegungsmechanismen (Art. 21 DSA), diese Aufgaben bis zu einem gewissen Grad wahrnehmen – und sich hieraus dann Standards für die Moderationspraxis entwickeln.[90]

Teilweise werden „immersive Rechte" gegenüber Plattformbetreibern vorgeschlagen: So sollen physische Mikroexpressionen sowie sensible, biometrische Daten nicht gespeichert bzw. nicht für kommerzielle Zwecke verwendet werden dürfen. Ein Recht auf authentische immersive Erfahrungen soll sicherstellen, dass Nutzer platzierte Anzeigen erkennen können.[91] Dies übersieht, dass die durch Grundrechte verbürgten Garantien mittelbar auch im virtuellen Raum gelten, dort jedoch einer konsequenten Umsetzung bedürfen.[92] Zudem wird der Ansatz individueller Rechte, den die DSGVO wählte, kritisiert, weil die Geltendmachung individueller Rechte nur den Anschein von Kontrolle erweckt. Sie vermag Nutzer, die sich einer umfassenden, regelmäßig automatisierten Datenverarbeitung durch Großkonzerne bei ungleicher Verteilung der ökonomischen Ressourcen zur Rechtsdurchsetzung ausgesetzt sehen, nicht in die Lage zu versetzen, frei über die Datenverarbeitung zu entscheiden.[93] Der Fokus sollte daher weniger auf die Durchsetzung individueller Ansprüche gerichtet werden, sondern auf den Schutz europäischer Verbraucher vor systematischen Risiken, die mit der Nutzung virtueller Welten und sozialer Medien einhergehen – diesen Ansatz hat der DSA gewählt.

III. Dezentrales Identitätsmanagement

Als Nexus zwischen digitaler und analoger Identität wird ein dezentrales Identitätsmanagement vorgeschlagen. Die Identifikation soll danach unabhängig von einer spezifischen virtuellen Welt, auch unter verschiedenen

89 *Maschewski/Nosthoff,* § 4 (Fn. 3), Rn. 18.
90 Vgl. *H. Ruschemeier et al.,* Brave New World, 2024, https://verfassungsblog.de/ods-dsa-user-rights-content-moderatin-out-of-court-dispute-settlement/.
91 *L. Rosenberg*, Migration to the metaverse: We need guaranteed basic Immersive Rights, https://venturebeat.com/virtual/metaverse-we-need-guaranteed-basic-immersive-rights/.
92 *Maschewski/Nosthoff,* § 4 (Fn. 3), Rn. 25.
93 *Ebers/Sein,* Challenges (Fn. 82), S. 4 f.

Pseudonymen und trotz unterschiedlicher Avatare möglich sein. Eine Klarnamenpflicht, die teilweise für mit § 19 Abs. 2 TTDSG unvereinbar erachtet wird,[94] ist nicht zwingend. Es muss politisch entschieden werden, ob auch künftig vor Gerichten (oder außergerichtlichen Schlichtungsstellen) um die Identifikation gestritten werden muss. Die Identifikation sollte aber grundsätzlich technisch ermöglicht werden, um Ansprüche in virtuellen Welten durchsetzen zu können.

E. Fazit

Das Metaverse muss sein Potential als disruptive Technologie noch unter Beweis stellen. Nach Einschätzung einiger Experten wird sich innerhalb der kommenden zehn bis 15 Jahre zeigen, ob das Metaverse ein Nischenprodukt bleibt oder nicht.[95]

Von virtuellen Welten gehen wegen ihrer spezifischen Charakteristika potenziell bestimmte Gefahren aus, auf die der Gesetzgeber eine adäquate Antwort finden muss. Dies darf nicht darüber hinwegtäuschen, dass die Probleme eng mit den in der Plattformökonomie bestehenden Machtstrukturen verknüpft sind.[96] Konzerneigene Narrative von virtuellen Welten als inklusiven Diskursräumen müssen deshalb kritisch hinterfragt werden, damit Fehler wie beim Umgang mit sozialen Medien nicht wiederholt werden.[97] Das Metaverse sollte daher rechtlich adressiert werden, bevor Plattformbetreiber Fakten schaffen. Die Frage nach dem adäquaten regulatorischen Umgang mit sozialen Medien verdeutlicht eindrucksvoll, wie schwierig sich die rechtliche Einhegung flächendeckend umgesetzter und ubiquitär genutzter Technologien gestaltet.

Weil virtuelle Welten bzw. das Metaverse noch nicht flächendeckend umgesetzt sind, hat der Gesetzgeber die Chance, nicht durch die Technik abgehängt zu werden.[98] Indem er – anders als im Recht der Plattformen – frühzeitig und vorausschauend tätig wird, kann er Rechtsgüter effektiv schützen.[99] Es ist deshalb begrüßenswert, dass die EU-Kommission die

94 *Kaulartz et al.,* Einführung (Fn. 6), 523, 525.
95 Kritisch *Floridi,* eXperience (Fn. 7), 9; *Hermann,* Werte (Fn. 6), S. 2.
96 *Rosenberg,* Roadmap (Fn. 12), S. 22.
97 Vgl. *Maschewski/Nosthoff,* § 4 (Fn. 3), Rn. 12, 26.
98 Dazu *Emborg,* The EU's Pacing Problem, 2023, https://verfassungsblog.de/the-eus-pacing-problem/.
99 *Kettemann et al.,* Ordnungsansätze (Fn. 59), S. 6; *Martini/Botta,* Staat (Fn. 15), 892.

Schaffung internationaler Standards für virtuelle Welten in Kooperation mit anderen Akteuren der Internet-Governance auf ihrer Agenda hat.[100] Sie sollte dabei nicht zu lange abwarten und sich durch andere Akteure ausbremsen lassen. Die EU kann auch in Bezug auf das Metaverse und andere virtuelle Welten als Vorreiterin im Bereich der Tech-Regulierung auftreten.[101] Der DSA ist hierfür grundsätzlich ein guter Ausgangspunkt, findet jedoch nicht für alle hinsichtlich der Inhaltsmoderation in virtuellen Welten aufgeworfenen Fragen eine adäquate Antwort.

100 Pressemitteilung EU-Kommission v. 11.7.2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3718.

101 *Trauthig/Woolley,* Content (Fn. 10), 12.

„Sachlich, bitte!“ – Zur Regelung von Nutzerverhalten in virtuellen Diskursräumen des Staates

Franziskus Horn

„*Was verbinden Sie mit Johann Wolfgang von Goethe? Welches Werk haben Sie gern gelesen?*“,[1] fragt das Bundespresseamt die Nutzer[2] seiner Facebook-Seite und begrüßt sie in seinen „*Hinweise[n] und Regeln für die Kommentierung*“[3] mit dem Ziel, „*konstruktive und sachliche Diskussionen*“ führen zu wollen. Entsprechend ermöglichen unterschiedlichste staatliche Stellen Grundrechtsträgern, sich untereinander und mit der staatlichen Stelle internetbasiert auszutauschen. Künftig ist zu erwarten, dass solche Begegnungen auch in komplexen virtuellen Welten stattfinden werden, die begrifflich als sogenannte „*Metaversen*“ diskutiert werden. Bereits jetzt befinden sich die Diskursräume aber in einem Umfeld, das grundsätzlich anfällig ist für äußerungsbasierte Rechtsverletzungen und Diskursbeiträge, die auch unter der Schwelle der Rechtswidrigkeit sozial unangemessen sind, wie etwa Hass, Hetze und Desinformationen. Die Betreiber der Diskursräume begegnen dem mit Benutzungsregeln. Nachfolgend soll betrachtet werden, ob und gegebenenfalls wie sich dies in teilhabe- und abwehrrechtlichen Grundrechtsdimensionen auswirkt und welche Anforderungen an entsprechende Regeln zu stellen sind. Dafür werden zunächst die derzeitigen und die künftigen virtuellen Diskursräume des Staates unter der Perspektive der staatlichen Öffentlichkeitsarbeit vorgestellt (A.). Sodann wird der rechtliche Rahmen dargestellt, in dem die staatlichen Stellen das Nutzerverhalten in

1 Presse- und Informationsamt der Bundesregierung, Beitrag v. 28.8.2024, https://www.facebook.com/Bundesregierung/posts/pfbid0H47F6EbGdfMFW9HnkExnAzskzctBpnDRy7iqQKAEeNdWQeypRSXZ6Ga7e4K8gxYRl (alle Links wurden zuletzt am 12.12.2024 abgerufen); vgl. auch *H. Mandelartz*, Öffentlichkeitsarbeit der Regierung, DÖV 2009, 509 (512 f.).

2 Zugunsten der besseren Lesbarkeit wird in diesem Beitrag ausschließlich das generische Maskulinum verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

3 Presse- und Informationsamt der Bundesregierung, Über Bundesregierung, https://www.facebook.com/Bundesregierung/about_details.

ihren Diskursräumen derzeit regeln und künftig regeln werden (B.). Weiter wird erörtert, welche Rolle es für diesen Rahmen spielen kann, wenn Dritte auf die staatlichen Angebote einwirken können (C.), um sodann mit einem Fazit zu schließen (D.).

A. Virtuelle Diskursräume des Staates

Staatliche Stellen informieren Grundrechtsträger im Internet über ihre Aufgabenerfüllung und ermöglichen Nutzern, sich in Kommentarbereichen primär textbasiert dazu zu äußern. Derzeit geschieht dies insbesondere in Social-Media-Auftritten, die die staatlichen Stellen z. B. auf Facebook, X und YouTube eröffnen.[4] Sie nutzen zudem eigene Plattformen, die ihnen häufig zugleich dazu dienen, Umfragen oder Beteiligungsverfahren durchzuführen.[5] Letzteres ist teils gesetzlich determiniert.[6] Sie betonen jeweils, dass sie einen Dialog zwischen und mit den Nutzern ermöglichen bzw. fördern möchten.[7]

I. Öffentlichkeitsarbeit und Aufgabenerfüllung des Staates

Solche staatlich induzierten Diskursformate könnten einem nach Art. 20 Abs. 2, 38 Abs. 1 GG vorausgesetzten freiem öffentlichen Meinungs- und Willensbildungsprozess des Volkes entgegenstehen. Ausdruck des demokratischen Staatswesens nach dem Grundgesetz ist, dass die demokratische

4 Vgl. die Auflistung der Social-Media-Accounts der Bundesregierung in BT-Drs. 19/4796, S. 2 ff.

5 Bspw. Freistaat Sachsen, Beteiligungsportal, https://buergerbeteiligung.sachsen.de/portal/egov/startseite.

6 Vgl. z. B. § 9 PetG Bremen; § 14a Abs. 7 S. 2 ThürPetG; § 13 EGovG SL; § 18 EGovG NRW; § 14 EGovG Bln; § 11 BremEGovG; § 12 EGovG LSA; § 15 EGovG RP; § 24 ThürEGovG; vgl. z. B. auch § 3 Abs. 2 BauGB.

7 Vgl. VG Mainz BeckRS 2018, 10857 Rn. 60; weiter die Hinweise der BReg (Fn. 1); *„Auf diese Weise soll ein direkter Kontakt und Austausch mit interessierten Bürgerinnen und Bürgern gefördert werden.“*, BMFSFJ, Social Media Netiquette, bmfsfj.de, https://www.bmfsfj.de/bmfsfj/social-media-netiquette-111694; *„Wir laden Sie auf dem Beteiligungsportal des Freistaates Sachsen herzlich ein zum Dialog über Themen aus Politik und Gesellschaft, zur Teilnahme an Umfragen sowie zur Mitwirkung an formellen Beteiligungsverfahren.“*, Freistaat Sachsen, Beteiligungsportal, https://buergerbeteiligung.sachsen.de/portal/sachsen/informationen/benutzerregeln.

Gesellschaft ihre Werte und Entscheidungen in einem offenen Diskurs selbst findet.[8] Dafür erfolgt die Willensbildung frei, offen, nicht reglementiert und „*staatsfrei*" vom Volk zu den Staatsorganen. Dies gipfelt im Wahlakt, der seinerseits durch den vorgelagerten freien Prozess zu legitimieren ist.[9] Eine staatliche Einflussnahme darauf bedarf der verfassungsrechtlichen Rechtfertigung.[10]

Aus dem Demokratieprinzip ergibt sich, dass staatliche Stellen in gewissem Maße dafür werben sollen, dass der Einzelne Akzeptanz für den Staat und seine Ordnung aufbringt, um einen Grundkonsens im Volk zu erhalten.[11] Auch mit Blick auf die demokratische Funktion des Willensbildungsprozesses haben sie zu einer größeren Transparenz und daher einem informierten Prozess beizutragen, vgl. § 1 Abs. 2 RhPf LTranspG. Ihr kommunikatives Nachaußentreten kann weiter Rückkoppelungseffekte ermöglichen, aufgrund derer sich auch abseits von Wahlen der Staatswille entlang des Volkswillens bilden kann. Zudem kann es rechtsstaatlich legitimiert als Basis der Kontrolle staatlichen Handelns dienen.[12] Daraus folgt, dass eine entsprechende Öffentlichkeitsarbeit nicht nur gerechtfertigt werden kann, sondern sie vielmehr Teil der Aufgabenerfüllung jeder staatlichen Stelle ist.[13]

Darüber hinaus bestehen weitere, stellenspezifische Sachaufgaben, die es bedingen, auf die Willensbildung des Volkes einzuwirken. Dies kann z. B. in Betracht kommen, wenn förmliche Beteiligungsverfahren durchgeführt oder Aufgaben der Öffentlichkeitswarnung[14] oder der Staatsleitung[15] wahrgenommen werden.

---

8 *F. Drefs,* Die Öffentlichkeitsarbeit des Staates und die Akzeptanz seiner Entscheidungen, Frankfurt a. M. 2018, S. 169.

9 BVerwG NVwZ 2018, 433 Rn. 28, 31 mwN.; OVG Niedersachsen, Beschl. v. 16.9.2024, Az. 10 LA 84/24; *T. Hinderks*, Staatliche Kommunikation in den neuen Medien, ZUM 2023, 26 (31).

10 BVerfGE 20, 56 (99 f.); 44, 125 (139 f.); *M. Brenner,* in: K. Stern/H. Sodan/M. Möstl (Hrsg.), Staatsrecht, Bd. 1, 2. Aufl., München 2022, § 14 Rn. 46.

11 BVerfGE 44, 125 (147); 63, 230 (243); 138, 102 (114); *C. Gramm*, Aufklärung durch staatliche Publikumsinformation, Der Staat 30 (1991), 51 (76).

12 BVerfGE 44, 125 (147 f.); 105, 252 (269 f.); *M. Kloepfer*, Informationszugangsfreiheit und Datenschutz, DÖV 2003, 221 (221 f.).

13 So auch *M. Petit,* Notwendigkeit und Zulässigkeit justizieller Öffentlichkeitsarbeit in Sozialen Medien, NJW 2024, 2666 (2667 mwN).

14 Vgl. etwa die (Landes-) Umweltinformationsgesetze oder § 28a GenTG.

15 BVerfGE 105, 252 (270); 138, 102 (113 f.); *F. Schürmann,* Regierungsamtliche Öffentlichkeitsarbeit im Wahlkampf, NVwZ 1992, 852 (852 f.).

II. Diskursräume als derzeitige und künftige Mittel

In den von staatlichen Stellen derzeit betriebenen Online-Auftritten werden diese insbesondere tätig, indem sie zu ihrer Aufgabenerfüllung informieren. Die Diskursräume zeichnet aus, dass sich Nutzer daran anknüpfend untereinander und mit der staatlichen Stelle in dafür eröffneten Kommentarbereichen textbasiert austauschen können. Die Kommentarfunktionen stehen grundsätzlich jedem offen. Diese unmittelbare dialogische Auseinandersetzung zwischen dem Staat und Bürgern kann für die oben genannten Zwecke zuträglich sein. Im Vergleich zur lediglich neutralen Information über Intermediäre kann sie möglicherweise sogar in höherem Maße informierend, integrierend und konsensfördernd wirken. Ohne festzulegen, wann die Art und Weise der Öffentlichkeitsarbeit die Grenzen des Zulässigen überschreitet, ist festzustellen, dass jedenfalls der Betrieb solcher Präsenzen als Mittel verfassungsrechtlich legitimierter Öffentlichkeitsarbeit und Aufgabenerfüllung zulässig sein kann.

Als künftiges Mittel dafür könnten Diskursräume in einem sogenanntem *Metaversum* angeboten werden. Begrifflich wird damit die Zielvorstellung eines gemeinsamen Raums erfasst, in dem technisch ermöglicht wird, eine virtuelle und erweiterte Realität zu schaffen, die teils eigenständig wahrnehmbar ist und teils mit der realen Welt ineinandergreift.[16] Innerhalb dessen sollen virtuelle, interoperable Räume geschaffen werden, die unterschiedliche Zweck- und Funktionsbestimmungen haben. Diese können wiederum von Personen, denen eine virtuelle Identität, ein sogenannter Avatar, zugeordnet ist, genutzt werden.[17] Aus der Kombination einer realitätserweiternden Wahrnehmbarkeit und der Interoperabilität verschiedener virtueller und realer Räume sollen wirtschaftlich und sozial relevante Interaktions- und Anwendungsmöglichkeiten erwachsen.[18]

16 Zur näheren Erläuterung wird verwiesen auf *M. Martini/J. Botta, Der Staat und das Metaversum,* MMR 2023, 887 (888 ff.); *M. Kaulartz/A. Schmid/F. Müller-Eising,* Das Metaverse – eine rechtliche Einführung, RDi 2022, 521 (522 ff.); *E. Wagner/M. Holm-Hadulla/M. Ruttloff,* in: dies. (Hrsg.), Metaverse und Recht, München 2023, Vorwort; *V. Borkmann/P. Ciziroglou/I.Pantzartzis,* Metaverse: Chancen und Herausforderungen für Kommunen, Stuttgart, Fraunhofer IAO, 2023 S. 5 f.

17 Dazu *Martini/Botta*, Metaversum (Fn. 16), 888; *Kaulartz/Schmid/Müller-Eising*, Metaverse (Fn. 16), Rn. 5 ff.

18 *Borkmann/Ciziroglou/Pantzartzis*, Metaverse (Fn. 16), S. 5 f.; *Martini/Botta*, Metaversum (Fn. 16), 888 ff.

In als Vorstufen davon begriffenen Angeboten sind bislang nur abgeschlossene virtuelle Welten nutzbar, in denen Nutzer dreidimensionale Bereiche und Räumlichkeiten digital begehen, miteinander interagieren und die dortigen Funktionen nutzen können.[19] International werden entsprechende Angebote staatlicherseits bereits genutzt. So werden virtuelle Räumlichkeiten betrieben, um z. B. einzelne Verwaltungsleistungen anzubieten oder für den Tourismus zu werben.[20] In dem *„Metaverse Seoul"* der Stadt Seoul konnten Bürger sich unter anderem virtuell treffen und austauschen, Informationsangebote wahrnehmen, virtuelle Abbilder von Sehenswürdigkeiten besuchen oder Verwaltungsleistungen in Anspruch nehmen, wie etwa Beschwerden einreichen, Dokumente beantragen oder lokale Steuern zahlen.[21] Andere staatliche Stellen greifen teils auch auf die „*Metaversen*" privater Anbieter zurück.[22]

Diese Vorbilder und die Aussicht darauf, einer Vielzahl von Personen in einem Metaversum begegnen zu können, lassen den Schluss zu, dass ein Metaversum insbesondere auch als Mittel der staatlichen Öffentlichkeitsarbeit und für Beteiligungsverfahren in Betracht kommen kann, sofern dort eine entsprechende Kommunikation ermöglicht wird und Bürger das Medium tatsächlich nutzen. Auch die EU-Kommission stellt in ihrer Strategie für virtuelle Welten heraus, dass diese dazu dienen sollen, öffentliche Dienste anzubieten. Sie könnten die demokratische Teilhabe und Interaktion der Bürger in Konsultationsprozessen verbessern.[23] Eine leicht zugängliche und immersivere Auseinandersetzung zwischen Staat und Bürger könnte die oben genannten Zwecke staatlicher Öffentlichkeitsarbeit sogar noch

19 *Wagner/Holm-Hadulla/Ruttloff*, Metaverse (Fn. 16), Vorwort; s. zu einigen *Martini/Botta*, Metaversum (Fn. 16), 888 f.

20 *Borkmann/Ciziroglou/Pantzartzis*, Metaverse (Fn. 16), S. 17; Arab News, Kingdom launches heritage metaverse initiative, 24.2.2024, https://www.arabnews.com/node/2465806/saudi-arabia.

21 Seoul Metropolitan Government, Official release of Metaverse Seoul, 25.1.2023, https://english.seoul.go.kr/official-release-of-metaverse-seoul/.

22 Vgl. *J. Stephen,* Tokyo's Government Launches Promo Metaverse on Roblox, XR Today, 22.2.2024, https://www.xrtoday.com/virtual-reality/tokyos-government-launches-promo-metaverse-on-roblox/.

23 EU-Kommission, EU-Initiative für das Web 4.0 und virtuelle Welten, EU COM(2023) 442/final, 11.7.2023, S. 2; dies., Towards the next technological transition: Commission presents EU strategy to lead on Web 4.0 and virtual worlds, 11.7.2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3718; i. d. S. auch *N. Kshetri/Y. Dwivedi/M. Janssen,* Metaverse for advancing government: Prospects, challenges and a research agenda, Government Information Quarterly, S. 10; dafür grds. auch *Martini/Botta*, Metaversum (Fn. 16), 902.

fördern. Mit Blick auf die potenziell vielfältigen Anwendungsmöglichkeiten sind auch in virtuellen Welten Diskursräume auf Basis textbasierter oder anderweitig verkörperter Nutzerinhalte denkbar, die einen dezentralen und zeitlich voneinander unabhängigen Austausch ermöglichen. Ein in einem Metaverse angelegter staatlicher Diskursraum wäre aber nicht zwingend textbasiert auszugestalten. Die Akteure würden in einem Metaversum in Form von Avataren aufeinandertreffen. Insofern wäre auch ein unmittelbarer avatarbasierter Austausch denkbar, der, gegebenenfalls per Voice-Chat, einen virtuellen Diskurs sprachbasiert ermöglichen und damit eher an klassische Bürgerbeteiligungsformate wie Bürgersprechstunden erinnern würde. Auch der Betrieb von Diskursräumen in einem Metaverse kann daher als Mittel staatlicher Öffentlichkeitsarbeit und zur Aufgabenerfüllung zulässig sein. Mit Blick auf den verfassungsrechtlichen Auftrag zur Öffentlichkeitsarbeit würde sich die Mittelauswahl zugunsten eines solchen Betriebs umso mehr anbieten, je intensiver ein Metaverse von den Bürgern als Ort des Austauschs genutzt wird.

B. Regelung von Nutzerverhalten in den Diskursräumen

Das Nutzerverhalten in internetbasierten Diskursräumen ist Gegenstand vielfältiger Regulierung. Neben den Anforderungen, die die Rechtsordnung allgemein an entsprechende Inhalte aus straf- und zivilrechtlicher Perspektive stellt, werden insbesondere die Plattformbetreiber in die Pflicht genommen, nutzergenerierte Inhalte zu moderieren.[24] Diese stellen ihre Dienstleistungen zur Verfügung, sofern Nutzer einen Plattformnutzungsvertrag mit ihnen schließen.[25] Hierin erlegen sie ihren Nutzern Verhaltenspflichten auf, die deren Äußerungsmöglichkeiten über das grundsätzlich rechtlich Zulässige hinaus beschränken.[26] Bei Verstößen behalten Plattformbetreiber sich vor, die Nutzerinhalte zu moderieren bzw. Vertragsrechte zu beschränken. Sie schützen insofern ihre wirtschaftlichen Interessen daran, Nutzern und Werbepartnern ein zuträgliches Umfeld zu schaffen.[27] Mit Blick auf die

24 Vgl. dazu *A. Grünwald/J. Hackl,* Inhaltemoderation bei Online-Plattformen, MMR 2024, 532 (532 ff.).

25 Vgl. Meta Platforms Ireland Limited, Nutzungsbedingungen, Fassung vom 12.1.2024, https://www.facebook.com/legal/terms/; Twitter International Unlimited Company, AGB, Fassung v. 15.11.2024, https://x.com/de/tos.

26 Vgl. BGH NJW 2021, 3179 Rn. 59, 73.

27 Vgl. BGH NJW 2021, 3179 (3179 f., Rn. 72 f.).

Pflicht, systemische Risiken zu identifizieren und ihnen entgegenzuwirken, wird dies unionsrechtlich zumindest goutiert, vgl. Art. 34 Abs. 2 S. 2 lit. c, 35 Abs. 1 S. 2 lit. c DSA.

I. Benutzungsregeln staatlicher Stellen

Nutzerverhalten in den eigenen Angeboten selbstständig moderieren zu können, ist auch ein Anliegen staatlicher Stellen, die eigene Diskursräume betreiben. Sie binden dort Benutzungsregeln bzw. sogenannte Netiquetten[28] ein, die das Nutzerverhalten zumindest teilweise eingrenzen sollen. So behalten sich die staatlichen Stellen insbesondere vor, bei Verstößen Nutzerinhalte zu löschen und Nutzeraccounts zu sperren. Die Maßnahmen werden u. a. an rechtswidrige und strafbare Inhalte geknüpft, Inhalte, die nicht sach- und themenbezogen sind, werbliche Inhalte, Verlinkungen, Beiträge, die Spam und Trolling enthalten sowie Kommentare, die nicht in deutscher Sprache verfasst sind. Zudem wird typischerweise ein sachliches und seriöses Nutzerverhalten gefordert.[29]

Ein entsprechendes Bedürfnis ist absehbar, wenn staatliche Stellen Präsenzen in einem Metaversum eröffnen, um darin Diskursräume zugunsten ihrer Öffentlichkeitsarbeit zu betreiben bzw. um Beteiligungsverfahren durchzuführen. Das dortige Nutzerverhalten wäre schließlich nicht nur auf Äußerungen in Form von Kommentaren beschränkt. Auch ein Verhalten, das der Nutzer über seinen Avatar steuert, könnte störend wirken. Zugleich ist denkbar, dass Nutzer virtuelle Gegenstände, die sie im Metaverse erstehen, erschaffen oder jedenfalls verwenden können,[30] aufgrund der interoperablen Funktionalitäten auch in dem staatlichen Diskursraum störend nutzen werden. Nutzerverhalten auch staatlicherseits zu moderieren, könnte daher sogar noch relevanter werden.

II. Rechtfertigungsbedürftigkeit

Die staatlich gewährte Möglichkeit, sich in einen Diskurs zu begeben, wird insofern bereits in den derzeitigen Angeboten an staatliche Verhaltensvor-

28 Zum Begriff *P. Jung*, Die Bedeutung der Selbstregulierung für das Lauterkeitsrecht in internationalen Computernetzwerken, GRUR Int. 1998, 841 (841 ff. mwN.).

29 Dazu unten B.II.2.c); vgl. OVG Bautzen BeckRS 2020, 26143 Rn. 2, 25; VG Hamburg BeckRS 2021, 24254 Rn. 4.

30 Vgl. *Kaulartz/Schmid/Müller-Eising*, Metaverse (Fn. 16), Rn. 44 ff.

gaben geknüpft, die die Äußerungsmöglichkeiten von Grundrechtsträgern betreffen. Mit Blick auf die vielfältigen Möglichkeiten von Nutzern, ihren Avatar in einem Metaverse zu steuern, müssten diese noch erweitert werden. Die Benutzungsregeln, die die staatlichen Stellen formulieren, könnten, je nachdem aus welcher Grundrechtsdimension sie zu betrachten sind, rechtfertigungsbedürftig sein.

1. Teilhabe und Freiheitsausübung

Staatliche Stellen wenden Mittel auf, um die Diskursräume zu betreiben, dort fortwährend zu informieren, zu kommunizieren und die Nutzerinhalte zu moderieren, damit Nutzer diese zweckgemäß und innerhalb der Benutzungsregeln verwenden können.[31] Sie betätigen sich insofern in der Leistungsverwaltung. Zugleich begründen sie damit eine auf den Leistungsvorgang bezogene Verwaltungspraxis, an die sie aufgrund der Gesetzesmäßigkeit der Verwaltung, Art. 20 Abs. 3 GG, gleichheitsrechtlich gebunden sind, Art. 3 Abs. 1 GG.[32] Von dieser kann die jeweilige Stelle nicht ermessensfehlerfrei zu Lasten des Einzelnen und ohne dies sachlich zu rechtfertigen abweichen.[33] Die Nutzer haben daran anknüpfend ein derivatives Teilhaberecht auf eine gleichheitsgerechte Entscheidung über ihre Nutzung aus Art. 3 Abs. 1 GG i. V. m. der Selbstbindung der Verwaltung.

Zugleich sieht der Leistungsvorgang vor, dass Grundrechtsträger sich in den eröffneten Diskursräumen äußern und sich darin informieren. Ihre dortigen Meinungsäußerungen können insofern von der Meinungsfreiheit, Art. 5 Abs. 1 S. 1 Alt. 1 GG, geschützt sein. Der Schutzbereich ist ihnen unabhängig von einem vermeintlichen Niveau der Äußerung eröffnet und wird ohne einen spezifischen Raumbezug dort gewährleistet, wo ein Äußernder tatsächlich Zugang findet bzw. wo er sich befindet.[34] Weiter stellen die Informationen, die die staatlichen Stellen in ihren Angeboten veröffentlichen, aber auch die nutzergenerierten Inhalte grundsätzlich allgemein zugängli-

31 Vgl. VG Hamburg BeckRS 2021, 24254 Rn. 3; *A. Ingold,* Behördliche Internetportale im Lichte des allgemeinen Verwaltungsrechts, Die Verwaltung 48 (2015), 525 (533 f.).

32 Vgl. BVerwG BeckRS 2013, 56435 Rn. 39; *M. Geis,* in: F. Schoch/J. Schneider (Hrsg.), VwVfG, Bd. 3, 5. EL, München 2023, § 40 Rn. 75 mwN.; *J. Milker/S. Schuster,* Keine Diskussion, kein Problem?, NVwZ 2021, 377 (378 f.).

33 Dazu sogleich unten B.II.2.b); *S. Boysen,* in: I. v. Münch/P. Kunig (Hrsg.), Grundgesetz-Kommentar, 7. Aufl., München 2021, Art. 3 Rn. 74 ff.

34 BVerfGE 128, 226 (265); 90, 241 (247).

che Informationsquellen dar, deren ungehinderte Nutzung zur Unterrichtung von der Informationsfreiheit, Art. 5 Abs. 1 S. 1 Alt. 2 GG, geschützt ist. Sofern in einem Metaverse noch hinzutritt, dass Nutzern ermöglicht wird, weitere diskursbegünstigende Handlungen vorzunehmen, wie z. B. sich zwischen Diskursräumen zu bewegen, würde der Leistungsvorgang zumindest auch die Ausübung der allgemeinen Handlungsfreiheit, Art. 2 Abs. 1 GG, erfordern.[35] Je nach Thematik könnten Grundrechtsträger auch in Ausübung weiterer Freiheiten teilnehmen, wie z. B. Art. 12 Abs. 1 GG, wenn ihnen ermöglicht wird, gewerblich in staatlichen Räumlichkeiten tätig zu werden.[36]

Der den Nutzern eröffnete Diskursraum, wird insofern im Wege des Teilhabeverhältnisses zur Freiheitsausübung bereitgestellt.[37] Der Charakter der Freiheitsrechte ändert sich dabei allerdings nicht. Regelungen und Einzelanordnungen, die den Grundrechtsgebrauch der Nutzer beschränken, können die jeweiligen Freiheitsrechte abwehrrechtlich betreffen.[38] In beiden Verhältnissen müsste das Verwaltungshandeln daher insbesondere mit höherrangigem Recht vereinbar sein, Art. 1 Abs. 3, 20 Abs. 3 GG.

2. Beschränkungen des Nutzerverhaltens

Wird das Nutzerverhalten entlang der Benutzungsregeln beschränkt, könnte sich dies auf das Teilhabeverhältnis sowie die Freiheitsausübung des Nutzers auswirken. In derzeitigen Angeboten würde sich etwa die Löschung eines Nutzerinhalts dahingehend auswirken, dass dieser nicht mehr abrufbar wäre. Wird ein Nutzer gesperrt, kann dieser typischerweise nicht mehr in dem staatlichen Auftritt kommentieren. Teils ist das Angebot für ihn auch nicht mehr abrufbar und bzw. oder sämtliche seiner Nutzerbeiträge werden gelöscht. Potenzielle Moderationsmaßnahmen in einem Metaverse könnten dies entsprechend umsetzen. Zugleich ist denkbar, dass anlässlich des vielgestaltigen Nutzerverhaltens ein einzelfallspezifisches Einwirken möglich wird, wie die Sperre lediglich einzelner Funktionalitäten oder virtueller Gegenstände.

35 Vgl. *D. Murswiek*, in: J. Isensee/P. Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. 9, 3. Aufl., Heidelberg 2011, § 193 Rn. 87.
36 Vgl. BVerwG NVwZ 2014, 527 Rn. 24.
37 Vgl. *Murswiek*, HdbStR (Fn. 35), § 193 Rn. 86 ff.
38 *Murswiek*, ebenda Rn. 86 f.; vgl. auch *A. Knierim,* Belastende Benutzungsregelungen, Berlin 2021, S. 175 ff.

a) Eingriffe in Freiheitsrechte

Solche Beschränkungen könnten eingreifend wirken. In derzeitigen Angeboten werden sie überwiegend als Realakte vorgenommen.[39] Die Löschung eines Nutzerbeitrags beschränkt grundsätzlich die jeweilige Meinungsäußerung und -verbreitung nachträglich und final. Die in den Benutzungsregeln angekündigten Maßnahmen sowie auch die in die Zukunft gerichtete Sperre knüpfen zudem nachteilige Rechtsfolgen an die Ausübung der Meinungsfreiheit. Bereits aufgrund der Ankündigung in den Benutzungsregeln ist davon auszugehen, dass Nutzer davon absehen werden, den Schutzbereich auszuschöpfen, wenn sie damit rechnen müssen, dass ihre Äußerung als unerwünscht bzw. untersagt eingeordnet werden könnten.[40] Weiter verhindert das Löschen, dass die in dem betroffenen Nutzerkommentar enthaltenen Informationen von Grundrechtsträgern entgegengenommen werden und sie sich anhand dieser unterrichten können. Die Nutzer sind dadurch unmittelbar in ihrer Informationsfreiheit betroffen. Sofern Nutzer überdies gesperrt und insofern von der Informationsquelle ausgeschlossen werden, erfolgt dies ebenfalls eingreifend.[41] Können sie die Maßnahme umgehen und sich die Informationen, z. B. ohne Anmeldung mit ihrem gesperrten Account verschaffen, kann dies die Eingriffsintensität verringern.[42] Entsprechende Eingriffe in Art. 5 Abs. 1 GG sind jedenfalls nach Art. 5 Abs. 2 GG rechtfertigungsbedürftig. Die Durchsetzungsmaßnahmen und die zugrundeliegenden Benutzungsregeln bedürften somit einer Ermächtigungsgrundlage, die den Anforderungen des Art. 5 Abs. 2 GG, insbesondere hinsichtlich der Rechtssatzqualität,[43] genügt und die im Einzelfall verfassungsgemäß angewendet werden kann.

39 BVerwG NVwZ 2023, 602 Rn. 18, 31, 36; VG Mainz BeckRS 2018, 10857 Rn. 69; *M. Libertus*, Sperren und Löschen von User-Content durch öffentlich-rechtliche Rundfunkanstalten auf deren Social Media-Präsenzen, CR 2019, 262 (265); *F. Kalscheuer/A. Jacobsen*, Zu der Rechtsnatur und den Rechtmäßigkeitsvoraussetzungen eines behördlichen Hausverbots, NVwZ 2020, 370 (371); a. A. *J. Milker,* Die Polizei auf Twitter – Brauchen wir ein Social-Media-Gesetz für staatliche Stellen?, NVwZ 2018, 1751 (1756).

40 Vgl. *G. Warg,* Meinungsfreiheit zwischen Zensur und Selbstzensur, DÖV 2018, 473 (475, 480).

41 VG Hamburg BeckRS 2021, 24254 Rn. 50; *M. Bilsdorfer,* Polizeiliche Öffentlichkeitsarbeit in sozialen Netzwerken, Saarbrücken 2019, S. 185 f.

42 Vgl. VG Hamburg BeckRS 2021, 24254 Rn. 95.

43 BVerwG NVwZ 2023, 602 Rn. 59.

Dies gälte entsprechend für staatliche Diskursräume im Metaverse. Auch sofern Benutzungsregeln die Nutzeräußerungen aufgreifen, die über Voice-Chat vermittelt werden, würden diese meinungsspezifische Wirkung entfalten können, die gegebenenfalls einer Rechtfertigung im Rahmen des Art. 5 Abs. 2 GG bedürfte. Sofern die dort weitergehend ermöglichte Grundrechtsausübung beschränkt würde, kämen noch vielfältigere Eingriffskonstellation in Betracht. Die oben genannte Beschränkung der virtuellen Gegenstände eines Nutzers könnte etwa an seiner Eigentumsfreiheit, Art. 14 Abs. 1 GG, zu messen sein.

Für die derzeit angebotenen staatlichen Diskursräume wurden bislang lediglich vereinzelt spezifische Befugnisse einfachgesetzlich gefasst.[44] Die Benutzungsregeln an sich sind typischerweise allenfalls als untergesetzliche Rechtsnormen ausgestaltet, wenn nicht lediglich als veröffentlichte interne Verwaltungsvorschriften oder öffentlich-rechtliche Willenserklärungen.[45] Unter zutreffender Kritik[46] hat sich im Übrigen die Ansicht in Rspr. und Lit. herausgebildet,[47] dass ein an das öffentlich-rechtliche Hausrecht angelehntes virtuelles öffentlich-rechtliches Hausrecht als Ermächtigungsgrundlage im Sinne des Art. 5 Abs. 2 GG genügen könnte. Sofern bereits mit Blick auf die derzeitigen Benutzungsregeln Zweifel daran bestehen, ob diese auf einer hinreichenden Rechtsgrundlage beruhen, dürfte es die absehbare zunehmende Komplexität potenzieller Grundrechtsausübungen in den virtuellen Diskursräumen des Staates unabdingbar machen, die staatliche Moderation im Metaversum formalgesetzlich zu begleiten.

b) Ausschluss des Teilhaberechts

Wird eine Maßnahme zulasten eines Benutzers ergriffen, könnte dies sein derivativ gewährtes Teilhaberecht an der Benutzung der staatlichen Angebote beschränken oder es gar ausschließen. Zudem könnte er im Vergleich mit anderen Nutzern in gleichheitsrechtlich relevanter Weise benachteiligt werden. Dies kann dann gerechtfertigt sein, wenn das jeweilige Unterscheidungskriterium ermessensfehlerfrei ausgewählt, sachlich gerechtfertigt und

44 Siehe etwa § 31a JustG NRW; § 9 PetG Bremen; zur polizeilichen Generalklausel VG Hamburg BeckRS 2021, 24254 Rn. 51.
45 Vgl. BVerwG NVwZ 2023, 602 Rn. 58 ff.
46 Kritisch BVerwG NVwZ 2023, 602 Rn. 68.
47 Vgl. nur VG Köln BeckRS 2021, 15277 mwN.

i. Ü. verhältnismäßig ist. Neben dem Grundsatz der Verhältnismäßigkeit ergibt sich der jeweilige Prüfungsmaßstab dabei insbesondere aus den jeweils betroffenen Sach- und Regelungsbereichen, insbesondere auch aus der Betroffenheit der einzelnen Freiheitsrechte.[48] Sofern die staatliche Stelle in den Benutzungsregeln entsprechende Kriterien vorformuliert, sind an diese dieselben Anforderungen zu stellen.[49] Ein Ausschluss von Nutzern kann insofern gerechtfertigt sein, wenn ein – gegebenenfalls eine Wiederholungsgefahr begründender – Verstoß gegen die Benutzungsregeln oder das geltende Recht vorliegt und der Ausschluss auch im Übrigen verhältnismäßig ist.[50] Ermessensfehler kommen aber insbesondere dann in Betracht, wenn die Benutzungsregeln nicht mit höherrangigem Recht, den von der staatlichen Stelle verfolgten Zwecken und, sofern die Benutzungsregeln untergesetzliche sind, mit einfachem Recht vereinbar sind.[51] Dies steht insbesondere in Frage, wenn die jeweilige Benutzungsregel über einen funktionalen Zusammenhang mit dem Leistungsvorgang hinaus eine eigenständige Belastungswirkung entfaltet.[52] Für die Benutzungsregeln in derzeitigen Angeboten ist dem folgend insbesondere maßgeblich, ob sie mit Art. 5 Abs. 1, 2 GG vereinbar sind.

Auch kapazitative Erwägungen können hinzuzuziehen sein. Würde ein staatlicher Diskursraum in einem Metaversum etwa in einem Format betrieben, das einer Bürgersprechstunde ähnelt, könnte die Anzahl der Diskutanten staatlicherseits zugunsten des Leistungsvorgangs zweckgemäß beschränkt werden.[53] Unter mehreren Benutzungsanwärtern bedürfte es insofern einer ermessensfehlerfreien Auswahlentscheidung, soweit Einzelnen die Teilhabe versagt werden soll.

48 BVerfG NVwZ 2011, 1316 Rn. 77 f. mwN.; insgesamt zur Rechtfertigung *U. Kischel,* in: V. Epping/C. Hillgruber (Hrsg.), BeckOK Grundgesetz, 59. Ed., München 2024, Art. 3 Rn. 28 ff.

49 Vgl. *Geis* (Fn. 32), § 40 Rn. 75.

50 Vgl. OVG Münster BeckRS 2015, 46869; VG Mainz MMR 2018, 556 Rn. 98 ff.; *T. Frevert/O. Wagner*, Rechtliche Rahmenbedingungen behördlicher Internetauftritte, NVwZ 2011, 76 (78 f.).

51 Dazu *Knierim* (Fn. 38), S. 223 ff.; auch *K. Lange,* Kommunale öffentliche Einrichtungen im Lichte der neueren Rechtsprechung, DVBl 2014, 753 (756).

52 *Knierim* (Fn. 38), S. 175 ff., 223 ff.

53 Vgl. *S. Ott/B. Ramming*, Anspruch auf Aufnahme in eine kommunale Linkliste, BayVBl. 2003, 454 (461); vgl. auch OVG Saarlouis NVwZ-RR 2010, 972 (973).

c) Beispiel: Forderung sachlicher und seriöser Inhalte

In diesem Zusammenhang ist auch die hier beispielhaft herausgegriffene Benutzungsregel zu bewerten, nach der Nutzer sich seriös und sachlich zu verhalten haben. Sie taucht teils maßnahmenbewehrt,[54] teils als Aufforderung[55] in den Benutzungsregeln staatlicher Internetpräsenzen auf.

Die Seriosität und die Sachlichkeit sind ausfüllungsbedürftige Begriffe. Ihr objektiver Gehalt ist aus einer objektivierten Adressatensicht entsprechend § 133 BGB zu bestimmen, in der die erkennbare Interessenslage und die Begleitumstände zu berücksichtigen sind.[56] Die Benutzungsregel steht zunächst im Kontext der erläuterten staatlichen Aufgabenerfüllung und soll dafür ein bestimmtes Nutzerverhalten fördern. Sie weist insofern ein Diskursniveau aus,[57] das nach den staatlichen Vorstellungen ihrer Aufgabenerfüllung zuträglich ist. Aus der Adressatensicht sollen Beiträge insofern eine gewisse Objektivität in der Form und im Inhalt mit dem Bemühen um Richtigkeit aufweisen.[58] Damit verbunden ist eine Mäßigungs- und Zurückhaltungsaufforderung in der staatlichen Sphäre,[59] die sich in einer gewissen Nüchternheit und Distanz ohne überschießende Emotionalität und Schärfe ausdrücken soll. Somit enthält die Benutzungsregel eine an die Meinungsäußerungen der Nutzer gerichtete materielle Verhaltensanforderung, die zugleich ein Unterlassungsgebot für abweichende Nutzerinhalte enthält und auf ein staatlich vorgegebenes Diskursniveau abzielt. Sie ist auch i. V. m. den daran geknüpften Lösch- und Sperrmaßnahmen an Art. 5 Abs. 1, 2 GG zu messen.

---

54 *„Rassistische, sexistische, unsachliche, beleidigende oder in ähnlicher Form unangebrachte Kommentare (z.B. mit personenbezogenen Daten, obszöner Sprache oder Werbung) werden verborgen oder gelöscht, sofern es dem Social Media Team technisch möglich ist (Facebook, Instagram, Youtube, LinkedIn).*" heißt es bei der Polizei Hamburg, Social Media Team & "Netiquette", https://www.polizei.hamburg/das-social-media-team-793728.

55 *„Wir freuen uns über konstruktive und sachliche Diskussionen.*" heißt es bei dem Presse- und Informationsamt der Bundesregierung, Netiquette v. 8.4.2024, https://www.bundesregierung.de/breg-de/themen/netiquette-2268818.

56 BVerwG NVwZ 2023, 602 Rn. 59 mwN.

57 So VG Hamburg BeckRS 2021, 24254 Rn. 34.

58 Sinngemäß so wohl auch VG Hamburg BeckRS 2021, 24254 Rn. 55 f., 64 f., 73.

59 Vgl. dazu auch die Mäßigungspflichten von Beamten *T. Masuch,* Vom Maß der Freiheit – Der Beamte zwischen Meinungsfreiheit und Mäßigungsgebot, NVwZ 2021, 520 (523 f.).

Die oben dargelegten Grenzen dafür, ob und inwieweit der freie Meinungsbildungsprozess staatlicherseits beeinflusst werden kann, entfalten sich diesbezüglich aber insbesondere daran, dass Art. 5 Abs. 1 GG gerade eine Niveaukontrolle ausschließt, die anhand eines Idealbilds von Diskursen und staatlichen Wertvorstellungen zwischen geschützten und im Meinungsprozess grundsätzlich gleichrangigen Äußerungen differenziert.[60] Auch im Sinne eines Minderheitenschutzes ist die Meinungsfreiheit nicht allgemein und ohne tatbestandliche Eingrenzung unter den Vorbehalt zu stellen, dass die Äußerungsinhalte herrschenden sozialen oder ethischen Auffassungen entsprechen; wie es in polizeilichen Normen etwa mit dem Tatbestandsmerkmal der öffentlichen Ordnung erfolgt.[61] Eine entsprechende Niveaukontrolle wäre aber mit der geforderten Seriosität und Sachlichkeit verbunden, sofern deren Inhalt lediglich von ausführenden staatlichen Stelle auszufüllen wäre. Es könnte insofern relevant werden, ob Inhalte wertvoll oder wertlos, emotional oder rational sind. Dies wäre wiederum mit dem besondere Bedürfnis an der Machtkritik nicht vereinbar, aufgrund dessen Art. 5 GG gerade eine Vermutung zugunsten der freien Rede vorsieht, nach der auch polemische Schärfen und Übersteigerungen im öffentlichen Meinungskampf zu dulden sind.[62] In diesem Rahmen sind auch Bestimmungen, die an die Zulässigkeit öffentlicher Kritik oder an die Sorgfaltspflichten bei Tatsachenmitteilungen überhöhte Anforderungen stellen, mit Art. 5 Abs. 1 GG unvereinbar.[63] Mangels einer Bestimmtheit wäre die Benutzungsregel auch keiner verfassungskonformen Auslegung zugänglich.[64] Eine maßnahmenbewehrte Benutzungsregel, nach der sich Nutzer seriös und sachlich zu äußern haben, ist daher nicht zu rechtfertigen. Entsprechend kann auch das Teilhaberecht nicht ermessensfehlerfrei durch sie beschränkt werden.

60 Vgl. *Warg* (Fn. 40), 474 f.
61 BVerfGE 111, 147 (156).
62 Vgl. BVerfGE 7, 198 (208 f.); BVerfG NVwZ-RR 2022, 561 Rn. 12, 18.
63 BVerfGE 42, 163 (170 f.); *D. Grimm,* Die Meinungsfreiheit in der Rechtsprechung des Bundesverfassungsgerichts, NJW 1995, 1697 (1701).
64 Vgl. BVerfGE 107, 104 (128 f).

C. Einwirkungen Dritter in den Leistungsvorgang

Wählt die staatliche Stelle ein Metaverse oder ein soziales Netzwerk als Infrastruktur, um dort ihre Diskursräume zu betreiben, geschieht dies grundsätzlich in den technischen und gegebenenfalls vertraglichen Gegebenheiten, die dort vorliegen. Diese werden in einem sozialen Netzwerk von dem privaten Plattformbetreiber bestimmt. In einem Metaversum ist es zwar Teil der Zielvorstellung, dass dieses keiner Verfügungsgewalt unterliegt. Absehbar ist aber auch insofern, dass ein Verantwortlicher zumindest auf die technischen Gegebenheiten Einfluss nehmen können wird. Insbesondere in seinen Vorstufen würden entsprechende Angebote in der Hand Privater liegen und wären insofern wohl auf vertraglicher Basis nutzbar.[65] In beiden Fällen würde die staatliche Stelle daher für Teilaspekte der staatlichen Aufgabenerfüllung auf die Mittel Dritter zurückgreifen.

Dies ist grundsätzlich nicht neu. Im Wege der funktionalen Privatisierung nutzen staatliche Stellen in analogen Konstellationen z. B. Räumlichkeiten privater Anbieter, die sie mieten[66] oder sie nutzen die Dienstleistungen privater Hardware- und Softwareanbieter.[67] Allerdings ist damit stets die Problematik verbunden, dass sich die staatliche Stelle in ihrer Leistungsgewährung davon abhängig macht, dass der private Dritte seine Dienste so erbringt, dass die staatliche Stelle den von ihr gewährten Leistungsvorgang aufrecht erhalten kann. Dies gilt umso mehr, als sie nach oben erläutertem Vorbild z. B. derivative Teilhaberechte gegenüber den jeweils Benutzungsberechtigten zu erfüllen hat. Die staatliche Stelle hat insofern in ihrer Mittelauswahl und Organisationsentscheidung zu berücksichtigen, dass sie ihren verfassungsrechtlichen und einfachgesetzlichen Verpflichtungen entsprechen kann.[68] Könnte das Handeln eines in die staatliche Aufgabenerfüllung einbezogenen Privaten dem entgegenstehen, ist es erforderlich, dass sich die staatliche Stelle Einwirkungs- und Weisungsrechte vorbehält, um die zweckgemäße Benutzung aufrechterhalten

65 Vgl. auch i. Ü. zur Zusammenarbeit mit Privaten *Kshetri/Dwivedi/Janssen,* Metaverse (Fn. 23), S. 9.

66 Vgl. OVG Lüneburg NVwZ-RR 2004, 777 (778).

67 So schon *H. Kube,* in: J. Isensee/P. Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. 4, 3. Aufl., Heidelberg 2006, § 91 Rn. 67; *M. Frey*, Kommunale öffentliche Einrichtungen im Internet, DÖV 2005, 411 (413 f.).

68 Vgl. VG Neustadt a.d. Weinstraße BeckRS 2019, 4885 Rn. 27.

zu können.[69] Die staatliche Stelle trifft insofern eine Gewährleistungsverantwortung. Dieser kann sie insbesondere im Wege vertraglicher Abreden mit dem Privaten nachkommen.

In derzeitigen Angeboten kommt eine solche Situation in Betracht, wenn die staatliche Stelle einen ihr zugeordneten Diskursraum in einem sozialen Netzwerk eröffnet und sowohl die Nutzer als auch die Stelle lediglich den plattformtypischen Nutzungsvertrag schließen. Durch ihn wird der private Plattformbetreiber vertraglich berechtigt, dass Nutzerverhalten auch in dem staatlichen Diskursraum zu moderieren und zwar sogar über das hinaus, zu was der Gesetzgeber die staatliche Stelle ermächtigen könnte. Eine solche Konstellation könnte auch in einem Metaverse auftreten.

Weiter kommt auch in einem Metaverse in Betracht, dass nicht nur der Betreiber auf den staatlichen Diskursraum zweck- oder rechtswidrig einwirken kann, sondern andere Nutzer oder Betreiber von virtuellen Räumlichkeiten ebenfalls. Auch insofern trifft die staatliche Stelle die Gewährleistungsverantwortung dazu, den staatlich gewährten Leistungsvorgang aufrechtzuerhalten und den Benutzungsberechtigen die Benutzung zu ermöglichen. In diesem Sinne besteht bereits die Forderung danach, dass auch in einem Metaverse Rechtsverletzungen zivil- und strafrechtlich begegnet werden können muss.[70] Aus teilhaberechtlicher Perspektive ist zu dem gleichen Schluss zu kommen.

Damit verbunden ist weiter, dass ein nicht reguliertes Metaverse, das z. B. keinen zentralen Betreiber hat und in dem sich eine staatliche Stelle nicht die für ihre Anforderungen passende Räumlichkeit erstellen bzw. ihren Betrieb sichern kann, nicht ermessensfehlerfrei als Mittel staatlicher Aufgabenerfüllung ausgewählt werden kann.

D. Zusammenfassung und Fazit

Eine dem verfassungsrechtlichen Öffentlichkeitsauftrag folgende staatliche Öffentlichkeitsarbeit hat ein Interesse daran, ihren Adressaten an die Orte zu folgen, an denen sie erreichbar sind. Sind dies derzeit noch die sozialen Netzwerke, könnten schon bald Formen eines Metaverses gängig werden. Schon in den derzeitigen Diskursräume entsteht für staatliche Stellen das

69 *M. Burgi,* in: D. Ehlers/H. Pünder (Hrsg.), Allgemeines Verwaltungsrecht, 16. Aufl., Heidelberg 2022, § 10 Rn. 34.

70 *Kaulartz/Schmid/Müller-Eising*, Metaverse (Fn. 16), Rn. 57 f.

Bedürfnis, missliebiges Nutzerverhalten zu beschränken. Dies könnte in einem Metaversum noch wachsen. Anders als die privaten Anbieter haben die staatlichen Stellen aber ihrer unmittelbaren Grundrechtsbindung zu genügen. Eine Moderation nach privatem Vorbild und daher auch bestimmte Benutzungsregeln sind ihnen versperrt. Zudem haben die staatlichen Stellen in beiden Medien so weit berechtigt zu sein, dass sie die von ihnen eröffneten Leistungsgewährungen aufrechterhalten können und die Teilhaberechte der Benutzungsberechtigten nicht durch die Einwirkungen Dritter beschränkt werden. Hinsichtlich beider Anforderungen scheinen schon die derzeitigen staatlichen Diskursräume nicht hinreichend einfachgesetzlich ausgestaltet.

Personenverzeichnis

Dr. Jonas Botta ist Forschungsreferent am Deutschen Forschungsinstitut für öffentliche Verwaltung und Habilitand an der Deutschen Universität für Verwaltungswissenschaften Speyer.

Dr. Alexander Brade, LL.M. (Harvard) ist wissenschaftlicher Mitarbeiter am Bundesverfassungsgericht und Habilitand an der Universität Leipzig.

Martin Feldhaus ist Forschungsreferent am Deutschen Forschungsinstitut für öffentliche Verwaltung.

Dr. Katharina Goldberg ist wissenschaftliche Mitarbeiterin/PostDoc an der Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg.

Jun.-Prof. Dr. Jennifer Grafe, LL.M. ist Juniorprofessorin für Kriminologie und Strafrecht an der Universität Tübingen.

Daniel Hauck ist wissenschaftlicher Mitarbeiter an der Johannes-Gutenberg-Universität Mainz und der FernUniversität in Hagen.

Dr. Sarah Hartmann ist akademische Rätin a.Z. und Habilitandin an der Universität Münster.

Prof. Dr. Simon Heetkamp, LL.M. ist Professor für Wirtschaftsrecht, Mobilitäts- und Versicherungsrecht an der TH Köln und Mitgründer der „digitalen richterschaft".

Franziskus Horn ist wissenschaftlicher Mitarbeiter bei Spirit Legal und promoviert an der Universität Leipzig.

Carolin Kemper ist Forschungsreferentin am Deutschen Forschungsinstitut für öffentliche Verwaltung.

Dr. Luise Lautenbach ist Rechtsanwältin bei Noerr im Bereich Data, Tech & Telecom (Berlin).

Dr. Martin Meier ist wissenschaftlicher Mitarbeiter und Habilitand an der Universität Erfurt.

Armin Mozaffari Jovein, Maître en Droit ist Rechtsanwalt bei RWT (Reutlingen) im Bereich IT-Recht, Datenschutzrecht und Gewerblicher Rechtsschutz und promoviert an der Eberhard Karls Universität Tübingen.

Prof. Dr. Peter Parycek ist Vizerektor der Donau-Universität Krems und leitet das Kompetenzzentrum Öffentliche IT am FOKUS Berlin.

Maximilian Petras ist wissenschaftlicher Mitarbeiter an der Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg und promoviert an der Christian-Albrechts-Universität zu Kiel.

Nik Roeingh ist Forschungsreferent am Deutschen Forschungsinstitut für öffentliche Verwaltung.

Nitharshini Santhakumar, LL.M. (Speyer) ist wissenschaftliche Mitarbeiterin an der Technischen Universität Darmstadt.

Dr. David M. Schneeberger ist Senior Researcher & Consultant beim Research Institute, Digital Human Rights Center in Wien.

Nicolas Ziegler ist wissenschaftlicher Mitarbeiter an der Technischen Universität München.

Jaouhara Zouagui ist wissenschaftliche Mitarbeiterin am Fraunhofer Institut für offene Kommunikationssysteme (FOKUS) und promoviert an der Donau-Universität Krems.