



DIGITALLOTSE **WIRTSCHAFT 4.0** XR-TECHNOLOGIEWERKSTATT

XR- UND METAVERSE-RECHT

Ein Leitfaden.

Stand: v03. 22.01.2025

Gefördert von



Baden-Württemberg

MINISTERIUM FÜR WIRTSCHAFT, ARBEIT UND TOURISMUS

Inhaltsverzeichnis

1. Einleitung	4
1.1 Rechtsfelder	4
1.2 Ratschläge für den Umgang mit rechtlichen Fragestellungen im Metaverse	6
2. Regulierung	7
2.1 Digital Markets Act (DMA)	7
2.2 Digital Services Act (DSA)	9
2.3 General Data Protection Regulation (GDPR)	12
2.4 European Data Act (EDA)	15
2.5 electronic IDentification, Authentication and trust Services (eIDAS)	18
2.6 Artificial Intelligence Act (AI Act)	20
2.7 Net Neutrality Regulation	23
2.8 EU Fitness Check on Digital Fairness	25
3. Rechtsgebiete	28
3.1 Anwaltliches Berufsrecht	28
3.2 Arbeitsrecht	30
3.3 Bank- und Kapitalmarktrecht	32
3.4 Strafrechtliche Verantwortlichkeit	34
3.5 Cyber Security	34
3.6 Datenschutz	37
3.7 Designrecht	38
3.8 Digitale Identitäten	39
3.9 Finanzaufsichtsrecht	41
3.10 Finanztransaktionen	43
3.11 Gaming und eSport	44
3.12 Gesellschaftsrecht	46
3.13 Glücksspielrecht	47
3.14 Handelsrecht	49
3.15 Intellectual Property / Geistiges Eigentum	51
3.16 Internationales Privatrecht	52
3.17 Lauterkeitsrecht	54

3.18 Lieferkettengesetz	55
3.19 Markenrecht.....	57
3.20 Medienrecht	58
3.21 Medizin- und Medizinproduktrecht	60
3.22 Miet- und Wohneigentumsrecht.....	61
3.23 Normennutzung: rechtliche Implikationen.....	63
3.24 Patentrecht.....	64
3.25 Persönlichkeitsrecht	66
3.26 Polizeirecht und staatliche Kontrolle	68
3.27 Rechtsschutz und gerichtliche Zuständigkeit.....	69
3.28 Steuerrecht.....	71
3.29 Urheberrecht.....	72
3.30 Verbraucherschutzrecht.....	73
3.31 Versicherungsrecht	75
3.32 Vertragsrecht.....	76
3.33 Werberecht	78
3.34 Wettbewerbs- und Kartellrecht.....	79
4. Literatur	80
5. Impressum.....	82
6. Förderhinweis.....	82

1. Einleitung

Das Metaverse, ein Begriff, der in den letzten Jahren sowohl in technologischen als auch gesellschaftlichen Diskussionen an Bedeutung gewonnen hat, beschreibt eine neue Dimension der digitalen Welt. Es handelt sich um eine virtuelle Realität, in der Menschen durch Avatare interagieren, digitale Güter kaufen, verkaufen oder handeln, und sogar ganze Geschäftsmodelle in einem virtuellen Raum entwickeln können. Diese immersive, oft dezentral organisierte Umgebung bietet nahezu unbegrenzte Möglichkeiten für Kreativität, Innovation und wirtschaftliches Wachstum. Doch mit diesen Chancen gehen auch erhebliche Herausforderungen einher, insbesondere im rechtlichen Bereich.

Recht ist im Metaverse nicht weniger wichtig als in der physischen Welt – es ist vielmehr essenziell, um Vertrauen, Sicherheit und Fairness zu gewährleisten. Ohne klare Regelungen könnten Unternehmen, Entwickler und Nutzer gleichermaßen rechtlichen Risiken ausgesetzt sein, die von Datenschutzverletzungen bis hin zu Konflikten um Eigentumsrechte reichen. Zudem zeigt die globale und dezentrale Natur des Metaverse, dass nationale Rechtssysteme allein oft nicht ausreichen, um die vielfältigen rechtlichen Fragen zu beantworten, die in diesem digitalen Ökosystem entstehen.

1.1 Rechtsfelder

In diesem Rechtsratgeber zum Metaverse möchten wir Ihnen die wichtigsten rechtlichen Themenfelder vorstellen, die in dieser neuen Welt relevant sind. Jedes dieser Themen spielt eine entscheidende Rolle, um die rechtlichen Herausforderungen und Chancen im Metaverse besser zu verstehen.

Vertragsrecht im Metaverse: Verträge bilden die Grundlage für viele Transaktionen im Metaverse, sei es der Kauf virtueller Grundstücke, die Nutzung von NFTs oder die Bereitstellung von Dienstleistungen. Die besonderen Herausforderungen liegen in der Definition der Vertragsparteien, der Einhaltung digitaler Vertragsformen und der Durchsetzung von Rechten und Pflichten in einer virtuellen Umgebung.

Urheberrecht und geistiges Eigentum: Kreative Werke, digitale Kunst, Musik oder Avatare: Das Urheberrecht schützt die Rechte der Schöpfer und regelt, wie diese Werke genutzt, geteilt und

monetarisiert werden können. Gleichzeitig stellen KI-generierte Inhalte und die Reproduktion realer Objekte in der virtuellen Welt das klassische Urheberrecht vor neue Herausforderungen.

Datenschutz und Privatsphäre: Das Metaverse ist datenintensiv. Jede Interaktion, jede Transaktion und jede Bewegung eines Avatars können aufgezeichnet und analysiert werden. Der Schutz dieser Daten, insbesondere in einem globalen und oft anonymen Umfeld, ist eine der zentralen rechtlichen Fragen. Die DSGVO und andere internationale Datenschutzregelungen bieten hier Leitplanken, müssen aber an die speziellen Anforderungen des Metaverse angepasst werden.

Strafrechtliche Verantwortlichkeit: Vergehen wie Betrug, Belästigung oder Identitätsdiebstahl nehmen auch im Metaverse eine bedrohliche Form an. Die Frage der strafrechtlichen Zuständigkeit und Durchsetzbarkeit wird durch die Anonymität und Dezentralität des Metaverse erschwert. Wie können Täter identifiziert werden, und welche nationalen Gerichte sind zuständig?

Wettbewerbs- und Kartellrecht: Marktmacht und Monopolisierung durch große Plattformbetreiber sind im Metaverse ein zentrales Thema. Gatekeeper-Plattformen, die den Zugang zu virtuellen Märkten kontrollieren, stehen ebenso im Fokus wie Fragen zur Interoperabilität und fairen Wettbewerbsbedingungen für kleinere Anbieter.

Finanz- und Steuerrecht: Virtuelle Währungen, NFTs und andere digitale Vermögenswerte werfen Fragen zur Besteuerung und Regulierung auf. Wie werden Einkünfte aus dem Handel mit digitalen Gütern versteuert, und welche Regeln gelten für die Abwicklung internationaler Transaktionen?

Verbraucherschutz: Das Metaverse ist auch ein Marktplatz, und Verbraucher müssen vor Täuschung, unfairen Geschäftsbedingungen und unsicheren Produkten geschützt werden. Themen wie Widerrufsrechte, Garantien und Informationspflichten sind hier von zentraler Bedeutung.

Medizin- und Gesundheitsrecht: Virtuelle Anwendungen im Gesundheitswesen, wie VR-Therapien oder digitale Diagnosetools, eröffnen neue Möglichkeiten, werfen aber auch Fragen nach der Zulassung, Haftung und dem Datenschutz auf.

Polizeirecht und staatliche Kontrolle: Auch die öffentliche Sicherheit spielt eine Rolle: Wie können illegale Aktivitäten im Metaverse überwacht und geahndet werden? Welche Befugnisse haben staatliche Behörden, und wie wird der Schutz von Grundrechten gewährleistet?

1.2 Ratschläge für den Umgang mit rechtlichen Fragestellungen im Metaverse

Um rechtliche Probleme im Metaverse zu vermeiden oder zu lösen, sollten Nutzer, Entwickler und Unternehmen folgende Ratschläge beachten:

Rechtsberatung einholen: Das Metaverse ist ein rechtliches Neuland. Spezialisierte Rechtsanwälte und Berater können helfen, komplexe Fragen zu klären.

Verträge und Nutzungsbedingungen sorgfältig prüfen: Insbesondere bei Transaktionen mit virtuellen Gütern oder Dienstleistungen sollten Verträge und Bedingungen klar definiert sein.

Datenschutz ernst nehmen: Unternehmen sollten sicherstellen, dass sie die Anforderungen der DSGVO oder anderer relevanter Datenschutzgesetze einhalten, um Bußgelder und Reputationsschäden zu vermeiden.

Bewusstsein für Risiken schaffen: Nutzer und Unternehmen sollten sich der rechtlichen Risiken bewusst sein, die im Metaverse bestehen, und sich entsprechend vorbereiten.

Zusammenarbeit und Austausch fördern: Internationale Kooperationen und der Austausch zwischen Regulierungsbehörden, Entwicklern und Nutzern sind entscheidend, um ein gerechtes und sicheres Metaverse zu schaffen.

Dieses Vorwort soll Ihnen einen ersten Überblick über die rechtlichen Herausforderungen und Chancen im Metaverse geben. Im weiteren Verlauf dieses Rechtsratgebers gehen wir auf jedes dieser Themen detailliert ein, um Ihnen praxisnahe und fundierte Informationen an die Hand zu geben. Die Kapitel sind im Anschluss in alphabetischer Reihenfolge in Rechtsgebiete geordnet. Gemeinsam können wir dazu beitragen, das Metaverse als sicheren und fairen digitalen Raum zu gestalten.

2. Regulierung

2.1 Digital Markets Act (DMA)

Der Digital Markets Act (DMA) ist ein bedeutendes regulatorisches Instrument der Europäischen Union, das entwickelt wurde, um faire Wettbewerbsbedingungen in digitalen Märkten zu schaffen und die Macht großer Online-Plattformen einzuschränken. Seine Einführung markiert einen wichtigen Meilenstein in der digitalen Gesetzgebung und hat weitreichende Auswirkungen auf verschiedene Aspekte der digitalen Wirtschaft, einschließlich des aufstrebenden Konzepts des Metaverse. In diesem Beitrag soll untersucht werden, wie der DMA das Metaverse beeinflusst, wobei zunächst die Grundzüge des Gesetzes erläutert und dann seine allgemeinen Bedeutungen diskutiert werden, bevor die spezifischen Auswirkungen auf das Metaverse analysiert werden.

2.1.1 Grundzüge des Digital Markets Act (DMA)

Der DMA zielt darauf ab, sogenannte „Gatekeeper“ in digitalen Märkten zu regulieren. Gatekeeper sind Unternehmen, die eine erhebliche Marktstellung innehaben, eine wichtige Plattform für Geschäfts- oder Endnutzer bereitstellen und in mehreren EU-Mitgliedsstaaten tätig sind. Beispiele für solche Plattformen sind Suchmaschinen, soziale Netzwerke, Betriebssysteme, Online-Marktplätze und Cloud-Dienste. Der DMA legt eine Reihe von Verpflichtungen und Verbotskatalogen fest, um den Wettbewerb zu schützen und Innovationen zu fördern.

Zu den zentralen Verpflichtungen gehören unter anderem:

- Interoperabilität und Datenzugang: Gatekeeper müssen sicherstellen, dass ihre Dienste mit denen von Wettbewerbern kompatibel sind.
- Transparenzanforderungen: Unternehmen müssen klare und faire Bedingungen für Geschäfts- und Endnutzer schaffen.
- Verbot wettbewerbswidriger Praktiken: Dazu gehört unter anderem das Verbot, eigene Dienste auf der Plattform zu bevorzugen (Selbstbegünstigung).
- Nutzerkontrolle: Nutzer müssen die Freiheit haben, vorinstallierte Apps zu deinstallieren und alternative Anwendungen zu nutzen.

Der DMA wird von der Europäischen Kommission überwacht und sieht empfindliche Strafen für Verstöße vor, die bis zu 10 % des weltweiten Jahresumsatzes eines Unternehmens betragen können.

2.1.2 Bedeutung des DMA im Allgemeinen

Der DMA stellt eine der ehrgeizigsten Gesetzesinitiativen dar, um die Macht der digitalen Riesen zu zähmen und faire Wettbewerbsbedingungen zu schaffen. In den letzten Jahren haben Unternehmen wie Google, Meta, Amazon und Apple zunehmend Kritik wegen ihrer dominanten Marktposition und ihrer monopolähnlichen Praktiken auf sich gezogen. Der DMA adressiert diese Problematik, indem er Mechanismen schafft, die Innovationen und Wettbewerb begünstigen sollen.

Ein zentraler Aspekt des DMA ist die Stärkung der Rechte von kleinen und mittleren Unternehmen (KMU) sowie der Verbraucher. KMU erhalten durch die Verpflichtung der Interoperabilität und des fairen Zugangs zu Daten neue Möglichkeiten, in den digitalen Märkten zu konkurrieren. Verbraucher profitieren von mehr Auswahlmöglichkeiten und einer besseren Kontrolle über ihre digitalen Interaktionen. Der DMA wirkt somit nicht nur wettbewerbsfördernd, sondern auch schützend gegenüber der Konzentration von Macht in wenigen Händen.

Die Bedeutung des DMA liegt jedoch nicht allein in der Marktkontrolle. Er setzt weltweit Standards für die Regulierung digitaler Plattformen und könnte andere Regionen inspirieren, ähnliche Gesetze einzuführen. Dies könnte zu einer Harmonisierung der globalen digitalen Gesetzgebung führen, was wiederum die Komplexität und die Kosten für Unternehmen reduziert, die in verschiedenen Regionen tätig sind.

2.1.3 Auswirkungen des DMA auf das Metaverse

Das Metaverse ist ein aufstrebendes digitales Ökosystem, das immersive virtuelle Realität (VR) und erweiterte Realität (AR) kombiniert, um neue Formen der Interaktion und des Wirtschaftens zu ermöglichen. Als eine Plattform, die potenziell von wenigen großen Unternehmen dominiert werden könnte, steht das Metaverse bereits im Fokus regulatorischer Diskussionen. Der DMA könnte entscheidend dazu beitragen, wie sich das Metaverse entwickelt und welche Akteure es dominieren:

- **Interoperabilität als Schlüssel zum offenen Metaverse:** Eine der größten Herausforderungen im Metaverse ist die Fragmentierung. Verschiedene Unternehmen entwickeln proprietäre Plattformen, die oft nicht miteinander kompatibel sind. Der DMA könnte dies ändern, indem er Interoperabilität vorschreibt. Nutzer wären dadurch in der Lage, Avatare, digitale Güter oder Währungen nahtlos zwischen verschiedenen Plattformen zu bewegen, was die

Nutzererfahrung erheblich verbessern würde. Gleichzeitig würde dies kleinen Anbietern ermöglichen, sich in das Metaverse-Ökosystem zu integrieren und neue Dienste anzubieten.

- **Datenzugang und -kontrolle:** Das Metaverse basiert stark auf Daten—von Nutzerinteraktionen über Bewegungs- und Sprachdaten bis hin zu biometrischen Informationen. Der DMA stellt sicher, dass Unternehmen, die als Gatekeeper fungieren, keinen exklusiven Zugriff auf diese Daten haben. Stattdessen würden eine gerechte Verteilung und Kontrolle von Daten die Grundlage für Innovationen und Datenschutz schaffen. Nutzer hätten mehr Kontrolle darüber, wie ihre Daten verwendet werden, und könnten entscheiden, welche Plattformen Zugriff erhalten.
- **Verhinderung monopolistischer Strukturen:** Das Metaverse birgt das Risiko, von wenigen dominanten Unternehmen beherrscht zu werden, die ähnlich wie heute im Bereich der sozialen Medien und Online-Marktplätze agieren. Der DMA könnte durch seine Verpflichtungen zur Transparenz und zum fairen Wettbewerb sicherstellen, dass keine Plattform ungerechtfertigte Vorteile erlangt. Insbesondere das Verbot der Selbstbegünstigung könnte verhindern, dass Unternehmen ihre eigenen VR-Geräte oder -Dienste bevorzugen und Konkurrenten benachteiligen.
- **Förderung von Innovation und Wettbewerb:** Ein offenes Metaverse, das durch den DMA gefördert wird, würde die Eintrittsbarrieren für neue Unternehmen senken. Start-ups und KMU könnten kreative Lösungen entwickeln und von einer gerechteren Verteilung von Ressourcen profitieren. Dies würde nicht nur zu einer größeren Vielfalt im Metaverse beitragen, sondern auch die Innovationsdynamik stärken.
- **Schutz der Nutzerrechte:** Der DMA sorgt dafür, dass Nutzer eine bessere Kontrolle über ihre digitalen Identitäten und Vermögenswerte im Metaverse haben. Funktionen wie die Freiheit, Dienste zu wechseln oder vorinstallierte Anwendungen zu entfernen, würden auch im Metaverse gelten. Dies fördert die Selbstbestimmung der Nutzer und reduziert die Abhängigkeit von einzelnen Plattformen.

2.2 Digital Services Act (DSA)

Der Digital Services Act (DSA) ist eine zentrale Gesetzesinitiative der Europäischen Union, die darauf abzielt, die Verantwortung und Rechenschaftspflicht digitaler Plattformen zu stärken und die Rechte der Nutzer im digitalen Raum zu schützen. Als Schwesterinitiative des Digital Markets Act (DMA) fokussiert sich der DSA primär auf Inhalte, Transparenz und Verbraucherschutz in digitalen Dienstleistungen. In der Diskussion um die Zukunft des Metaverse nimmt der

DSA eine zunehmend wichtige Rolle ein. Dieser Beitrag beleuchtet die Grundzüge des DSA, seine allgemeine Bedeutung und die spezifischen Auswirkungen auf das Metaverse.

2.2.1 Grundzüge des Digital Services Act (DSA)

Der Digital Services Act wurde eingeführt, um die bestehende E-Commerce-Richtlinie von 2000 zu modernisieren. Mit dem exponentiellen Wachstum des Internets und der Digitalisierung seit der Jahrtausendwende haben sich auch die Herausforderungen im Bereich der Plattformregulierung stark verändert. Der DSA zielt darauf ab, klare Regeln für die Verantwortung von Online-Plattformen festzulegen und gleichzeitig Innovation und wirtschaftliches Wachstum zu fördern.

Zu den wichtigsten Aspekten des DSA gehören:

- Verantwortung von Plattformen: Plattformen müssen Mechanismen zur Moderation von Inhalten einrichten, um illegale Inhalte zu entfernen und Missbrauch zu verhindern. Dies umfasst Hassrede, Falschinformationen, illegale Waren und Dienstleistungen.
- Transparenzpflichten: Digitale Plattformen müssen offenlegen, wie ihre Algorithmen Inhalte priorisieren, und Nutzern klare Informationen über Werbung und Datenverarbeitung bereitstellen.
- Unterschiedliche Pflichten für verschiedene Plattfortmtypen: Der DSA unterscheidet zwischen kleinen Unternehmen, mittleren Plattformen und sehr großen Online-Plattformen (VLOPs). Letztere unterliegen strengeren Regeln, da sie aufgrund ihrer Reichweite und ihres Einflusses ein erhöhtes Risiko für gesellschaftliche Schäden bergen.
- Rechte der Nutzer: Der DSA stärkt die Rechte der Nutzer, etwa durch Mechanismen, um Entscheidungen von Plattformen zu Inhalten anzufechten oder personalisierte Werbung abzulehnen.
- Schutz von Minderjährigen: Besondere Bestimmungen sollen sicherstellen, dass Minderjährige vor schädlichen Inhalten und invasiver Datenerfassung geschützt werden.

2.2.2 Bedeutung des DSA im Allgemeinen

Der DSA hat das Potenzial, das digitale Ökosystem grundlegend zu verändern. Er stellt sicher, dass Plattformen nicht nur von ihren wirtschaftlichen Vorteilen profitieren, sondern auch eine soziale Verantwortung übernehmen. Dies ist besonders wichtig angesichts der zunehmenden Verbreitung von Falschinformationen, der Polarisierung durch algorithmische Empfehlungsdienste und des Missbrauchs von Online-Diensten für illegale Aktivitäten.

Der DSA schafft einen Rahmen, der Plattformen zur Rechenschaft zieht, ohne Innovationen zu behindern. Insbesondere kleine und mittlere Unternehmen (KMU) profitieren davon, dass die Anforderungen je nach Größe und Wirkung der Plattform skaliert werden. Dies fördert einen fairen Wettbewerb und vermeidet übermäßige Bürden für kleinere Anbieter.

International setzt der DSA Maßstäbe, die auch außerhalb der EU Beachtung finden. In einer globalisierten digitalen Wirtschaft könnte er als Blaupause für ähnliche Gesetzgebungen weltweit dienen, insbesondere in Regionen, die mit den Herausforderungen digitaler Plattformen ähnlich konfrontiert sind.

2.2.3 Auswirkungen des DSA auf das Metaverse

Das Metaverse stellt eine neue digitale Dimension dar, in der physische und virtuelle Realität miteinander verschmelzen. Es bietet unzählige Möglichkeiten für soziale Interaktion, Handel, Bildung und Unterhaltung. Gleichzeitig birgt es erhebliche Risiken, die vom Missbrauch personenbezogener Daten über illegale Inhalte bis hin zu Fragen der Fairness und Transparenz reichen. Der DSA spielt eine entscheidende Rolle dabei, wie diese Risiken im Metaverse adressiert werden können:

- **Inhaltsmoderation im Metaverse:** Die Moderation von Inhalten wird im Metaverse eine immense Herausforderung darstellen. Anders als traditionelle Plattformen bietet das Metaverse eine immersive und dynamische Umgebung, in der Inhalte in Echtzeit generiert und geteilt werden. Der DSA könnte Plattformen dazu verpflichten, robuste Mechanismen zur Inhaltsmoderation zu entwickeln, die in der Lage sind, illegale Inhalte schnell zu identifizieren und zu entfernen, ohne die Meinungsfreiheit unverhältnismäßig einzuschränken.
- **Transparenz und algorithmische Entscheidungen:** Im Metaverse spielen Algorithmen eine zentrale Rolle, beispielsweise bei der Empfehlung von Inhalten, der Platzierung von virtuellen Anzeigen oder der Organisation sozialer Interaktionen. Der DSA verlangt, dass Plattformen Transparenz über ihre Algorithmen schaffen. Nutzer müssen verstehen, wie Inhalte kuratiert werden und warum bestimmte Informationen priorisiert werden. Dies wird entscheidend dafür sein, Vertrauen im Metaverse zu schaffen und Manipulation durch undurchsichtige Algorithmen zu verhindern.
- **Schutz der Nutzerrechte:** Im Metaverse sind digitale Identitäten und Vermögenswerte von zentraler Bedeutung. Der DSA könnte sicherstellen, dass Nutzer umfassende Rechte über ihre Daten und digitalen Besitztümer haben. Dies umfasst das Recht, ihre Daten zu portieren, sowie den Schutz vor invasiver Werbung und Überwachung. Zudem würde der Schutz

von Minderjährigen besondere Bedeutung erlangen, da das immersive Umfeld des Metaverse neue Risiken birgt.

- Verantwortung der Plattformen: Plattformen, die das Metaverse betreiben, würden unter die strengen Regeln des DSA fallen, insbesondere wenn sie als sehr große Online-Plattformen (VLOPs) eingestuft werden. Dies bedeutet, dass sie umfassende Risikobewertungen vornehmen und Mechanismen zur Schadensbegrenzung entwickeln müssen. Dadurch wäre sichergestellt, dass das Metaverse nicht zu einem Raum für illegale oder schädliche Aktivitäten wird.
- Interoperabilität und Vielfalt: Ein zentraler Punkt des DSA ist die Forderung nach Transparenz und Fairness im Umgang mit Wettbewerbern. Für das Metaverse könnte dies bedeuten, dass Plattformen dazu angehalten werden, interoperabel zu sein, sodass Nutzer zwischen verschiedenen virtuellen Welten wechseln können. Dies würde nicht nur die Vielfalt und Innovation fördern, sondern auch verhindern, dass einzelne Anbieter eine monopolartige Kontrolle über das Metaverse ausüben.

2.3 General Data Protection Regulation (GDPR)

Die General Data Protection Regulation (GDPR), im Deutschen als Datenschutz-Grundverordnung (DSGVO) bekannt, ist ein grundlegendes Gesetz der Europäischen Union, das den Datenschutz und die Privatsphäre für alle Personen innerhalb der EU regelt. Seit ihrem Inkrafttreten im Mai 2018 hat die GDPR globale Auswirkungen gehabt und Standards für den Umgang mit personenbezogenen Daten gesetzt. In einer Zeit, in der digitale Technologien zunehmend komplexer werden, gewinnt die GDPR noch mehr an Bedeutung, insbesondere für das aufstrebende Konzept des Metaverse. Dieser Beitrag beleuchtet die Grundzüge der GDPR, ihre allgemeine Bedeutung und die Auswirkungen auf das Metaverse.

2.3.1 Grundzüge der GDPR

Die GDPR wurde eingeführt, um einheitliche Datenschutzstandards innerhalb der EU zu schaffen und die Rechte der Bürger in einer digitalisierten Welt zu stärken. Sie regelt, wie personenbezogene Daten erhoben, verarbeitet, gespeichert und genutzt werden dürfen. Die Verordnung ist für alle Unternehmen verbindlich, die Daten von Personen innerhalb der EU verarbeiten, unabhängig davon, wo das Unternehmen ansässig ist.

Zu den wichtigsten Grundzügen der GDPR gehören:

- Einwilligung und Transparenz: Personenbezogene Daten dürfen nur mit ausdrücklicher Zustimmung der Betroffenen erhoben und verarbeitet werden. Unternehmen müssen klar und transparent darlegen, wofür die Daten verwendet werden.
- Rechte der Betroffenen: Die GDPR gewährt Einzelpersonen umfassende Rechte, darunter das Recht auf Auskunft, Berichtigung, Löschung („Recht auf Vergessenwerden“) und Datenportabilität.
- Privacy by Design und by Default: Unternehmen müssen Datenschutz in ihre Systeme und Prozesse integrieren, und zwar von Beginn an. Datenschutzfreundliche Voreinstellungen müssen der Standard sein.
- Meldepflicht bei Datenschutzverletzungen: Unternehmen sind verpflichtet, Datenschutzverstöße innerhalb von 72 Stunden den zuständigen Behörden zu melden.
- Strenge Strafen: Verstöße gegen die GDPR können mit Geldstrafen von bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes eines Unternehmens geahndet werden.

2.3.2 Bedeutung der GDPR im Allgemeinen

Die GDPR hat die Art und Weise, wie Unternehmen weltweit mit personenbezogenen Daten umgehen, revolutioniert. Sie hat Datenschutz zu einer zentralen Frage in der digitalen Wirtschaft gemacht und Unternehmen gezwungen, ihre Praktiken anzupassen. Die Verordnung hat sowohl Verbraucher als auch Unternehmen sensibilisiert und ein Bewusstsein für die Bedeutung von Datenschutz geschaffen.

Für Verbraucher bietet die GDPR ein hohes Maß an Schutz und Kontrolle über ihre persönlichen Daten. Sie haben die Gewissheit, dass ihre Daten sicher und transparent behandelt werden. Gleichzeitig ermöglicht die GDPR, Verstöße einfacher zu melden und rechtliche Schritte einzuleiten.

Für Unternehmen stellt die GDPR eine Herausforderung dar, die jedoch auch Chancen bietet. Datenschutz wird zu einem Wettbewerbsvorteil, da Kunden zunehmend auf die Einhaltung von Datenschutzstandards achten. Unternehmen, die in Datenschutz investieren, können Vertrauen aufbauen und langfristig ihre Marktposition stärken.

Die GDPR hat auch Auswirkungen auf den globalen Kontext. Viele Länder und Regionen, darunter Kalifornien mit dem California Consumer Privacy Act (CCPA), haben ähnliche Gesetze

eingeführt, die von der GDPR inspiriert wurden. Damit setzt die Verordnung einen weltweiten Standard für Datenschutz.

2.3.3 Auswirkungen der GDPR auf das Metaverse

Das Metaverse ist ein aufkommendes digitales Ökosystem, das immersive virtuelle Realität (VR) und erweiterte Realität (AR) kombiniert, um neue Formen der Interaktion und des Wirtschaftens zu ermöglichen. Es verspricht grenzenlose Möglichkeiten, bringt jedoch auch erhebliche Datenschutzrisiken mit sich. Die GDPR spielt eine entscheidende Rolle dabei, wie diese Risiken bewältigt werden können:

- **Umgang mit personenbezogenen Daten:** Im Metaverse werden enorme Mengen an personenbezogenen Daten erhoben, darunter biometrische Daten (wie Gesichtsausdrücke und Bewegungen), Kommunikationsdaten und Nutzungsgewohnheiten. Die GDPR stellt sicher, dass diese Daten nur mit Zustimmung der Nutzer erhoben und verarbeitet werden dürfen. Unternehmen müssen transparente Mechanismen schaffen, um die Nutzer darüber zu informieren, welche Daten gesammelt werden und zu welchem Zweck.
- **Rechte der Nutzer im Metaverse:** Die Rechte der Betroffenen nach der GDPR gelten auch im Metaverse. Nutzer haben das Recht, Auskunft über die Verwendung ihrer Daten zu verlangen, diese Daten zu korrigieren oder löschen zu lassen. Dies wird besonders wichtig in einer Umgebung, in der digitale Identitäten und Vermögenswerte eine zentrale Rolle spielen. Plattformen im Metaverse müssen Mechanismen implementieren, die es Nutzern ermöglichen, diese Rechte effektiv auszuüben.
- **Privacy by Design im Metaverse:** Die GDPR verpflichtet Unternehmen, Datenschutz von Beginn an in ihre Systeme zu integrieren. Im Metaverse bedeutet dies, dass Plattformen von Anfang an sicherstellen müssen, dass personenbezogene Daten geschützt werden. Beispielsweise könnten Plattformen datenschutzfreundliche Voreinstellungen bieten, die standardmäßig aktiviert sind, und Nutzern die Möglichkeit geben, ihre Einstellungen individuell anzupassen.
- **Schutz vor Überwachung und Profilbildung:** Das Metaverse bietet Unternehmen die Möglichkeit, umfangreiche Profile über das Verhalten und die Präferenzen der Nutzer zu erstellen. Die GDPR schützt Nutzer vor invasiver Profilbildung und Überwachung, indem sie klare Regeln für die Verarbeitung personenbezogener Daten aufstellt. Plattformen im Metaverse müssen sicherstellen, dass sie diese Regeln einhalten und keine Daten ohne ausdrückliche Zustimmung der Nutzer verarbeiten.

- Herausforderungen bei grenzüberschreitender Datenverarbeitung: Das Metaverse ist ein globales Phänomen, das Nutzer und Unternehmen aus verschiedenen Regionen miteinander verbindet. Die GDPR regelt den grenzüberschreitenden Datenverkehr streng und stellt sicher, dass personenbezogene Daten von EU-Bürgern auch außerhalb der EU denselben Schutz genießen. Unternehmen, die im Metaverse tätig sind, müssen sich an diese Anforderungen halten, was eine erhebliche Herausforderung darstellt.
- Schutz von Minderjährigen: Das Metaverse zieht auch Minderjährige an, die besonders schutzbedürftig sind. Die GDPR enthält spezielle Bestimmungen für den Schutz von Kindern und Jugendlichen. Plattformen im Metaverse müssen sicherstellen, dass sie diese Vorgaben einhalten, etwa durch die Einholung der Zustimmung der Eltern und den Schutz vor schädlichen Inhalten.

2.4 European Data Act (EDA)

Der European Data Act (EDA) ist ein zentrales Regulierungsvorhaben der Europäischen Union, das darauf abzielt, die Nutzung und den Austausch von Daten in der digitalen Wirtschaft zu fördern und gleichzeitig faire Bedingungen für alle Marktteilnehmer zu schaffen. In einer zunehmend datengetriebenen Welt spielt der EDA eine entscheidende Rolle, insbesondere in Hinblick auf das Metaverse, das als ein potenziell dominierendes digitales Ökosystem der Zukunft angesehen wird. Dieser Beitrag beleuchtet die Grundzüge des EDA, seine allgemeine Bedeutung und die spezifischen Auswirkungen auf das Metaverse.

2.4.1 Grundzüge des European Data Act (EDA)

Der European Data Act wurde von der EU entwickelt, um ein klareres und gerechteres Regelwerk für den Zugang und die Nutzung von Daten zu schaffen. Ziel ist es, eine Ökonomie zu fördern, in der Daten nicht nur gesammelt, sondern auch effektiv und sicher geteilt werden können. Der EDA berücksichtigt dabei sowohl die Interessen der Dateninhaber als auch derjenigen, die Daten nutzen möchten.

Zu den zentralen Elementen des EDA gehören:

- Zugangsrechte zu Daten: Der EDA regelt, dass Unternehmen und Nutzer Zugang zu den Daten erhalten, die von Produkten und Dienstleistungen generiert werden, die sie besitzen oder nutzen. Dies ermöglicht eine bessere Nutzung von IoT-Daten (Internet of Things) und anderen datenintensiven Technologien.

- Datenteilung zwischen Unternehmen: Der EDA schafft klare Regeln für die freiwillige und verpflichtende Datenteilung zwischen Unternehmen. Ziel ist es, wettbewerbswidrige Praktiken zu verhindern und Innovationen zu fördern.
- Datenschutz und Sicherheit: Obwohl der EDA den Datenaustausch erleichtert, stellt er sicher, dass die Datenschutzstandards der GDPR (Datenschutz-Grundverordnung) eingehalten werden. Der Schutz sensibler Daten bleibt eine Priorität.
- Fairness für KMU: Der EDA legt besonderen Wert darauf, kleine und mittlere Unternehmen (KMU) zu unterstützen. Er verhindert missbräuchliche Vertragsbedingungen von großen Marktteilnehmern und schafft gleiche Wettbewerbsbedingungen.
- Interoperabilität und Standards: Der EDA fördert die Entwicklung technischer Standards, die die Interoperabilität zwischen verschiedenen Systemen und Plattformen erleichtern. Dies ist entscheidend für eine reibungslose Datennutzung.

2.4.2 Bedeutung des European Data Act im Allgemeinen

Der EDA hat eine weitreichende Bedeutung für die digitale Wirtschaft der EU und darüber hinaus. Er stellt sicher, dass Daten als eine wesentliche Ressource des 21. Jahrhunderts effizient genutzt werden können, ohne dass einzelne Akteure die Kontrolle über große Datenmengen monopolartig ausüben. Dies fördert Innovationen, Wettbewerbsfähigkeit und Chancengleichheit.

Ein zentraler Vorteil des EDA liegt in der Demokratisierung von Daten. Unternehmen und Organisationen erhalten Zugang zu Daten, die sie vorher nur schwer oder gar nicht nutzen konnten. Dies ermöglicht die Entwicklung neuer Produkte und Dienstleistungen, insbesondere in Bereichen wie Künstliche Intelligenz (KI), maschinelles Lernen und Smart Cities.

Gleichzeitig stärkt der EDA die Rechte von Verbrauchern und Unternehmen, indem er sicherstellt, dass Datennutzungspraktiken transparent und fair sind. Die Förderung der Interoperabilität und die Schaffung technischer Standards erleichtert die Zusammenarbeit zwischen verschiedenen Akteuren und verringert Abhängigkeiten von einzelnen Plattformen oder Technologien.

2.4.3 Auswirkungen des EDA auf das Metaverse

Das Metaverse, eine virtuelle Welt, die physische und digitale Realität verschmelzen lässt, ist ein datenintensives Ökosystem. Es basiert auf der Erfassung, Verarbeitung und Analyse riesiger Datenmengen, die aus Nutzerinteraktionen, Bewegungen, Transaktionen und digitalen

Inhalten generiert werden. Der European Data Act könnte die Entwicklung und das Funktionieren des Metaverse in vielfacher Hinsicht beeinflussen:

- **Zugänglichkeit von Daten im Metaverse:** Im Metaverse werden große Datenmengen von Plattformen und Geräten generiert. Der EDA stellt sicher, dass Nutzer und Unternehmen Zugang zu diesen Daten erhalten. Beispielsweise könnten Nutzer Informationen über ihre Bewegungen, virtuelle Transaktionen oder erstellte Inhalte anfordern und für eigene Zwecke nutzen. Unternehmen könnten diese Daten nutzen, um neue Anwendungen oder Dienstleistungen im Metaverse zu entwickeln.
- **Interoperabilität und technische Standards:** Eine der größten Herausforderungen im Metaverse ist die Interoperabilität zwischen verschiedenen Plattformen. Der EDA fördert die Entwicklung einheitlicher technischer Standards, die es Nutzern ermöglichen, nahtlos zwischen verschiedenen virtuellen Welten zu wechseln oder digitale Güter und Währungen plattformübergreifend zu nutzen. Dies würde ein offeneres und inklusiveres Metaverse schaffen.
- **Verhinderung von Datenmonopolen:** Im Metaverse besteht die Gefahr, dass wenige große Unternehmen die Kontrolle über die wichtigsten Datenströme erlangen. Der EDA wirkt dem entgegen, indem er klare Regeln für den Datenzugang und die Datenteilung schafft. Plattformen könnten verpflichtet werden, Daten mit kleineren Unternehmen oder Entwicklern zu teilen, was den Wettbewerb fördert und Innovationen begünstigt.
- **Schutz von Nutzerdaten:** Obwohl der EDA den Datenaustausch erleichtert, achtet er darauf, dass der Datenschutz nicht vernachlässigt wird. Im Metaverse wären personenbezogene Daten wie biometrische Informationen, Sprachdaten oder Nutzungsverhalten besonders sensibel. Der EDA stellt sicher, dass diese Daten sicher und im Einklang mit der GDPR behandelt werden.
- **Förderung kleiner und mittlerer Unternehmen (KMU):** Das Metaverse bietet immense Möglichkeiten für Start-ups und KMU, innovative Dienste und Produkte zu entwickeln. Der EDA stellt sicher, dass diese Akteure nicht durch unfaire Praktiken großer Plattformen benachteiligt werden. Klare Regeln für Datenzugang und faire Vertragsbedingungen schaffen gleiche Wettbewerbsbedingungen.
- **Neue Möglichkeiten für Verbraucher:** Für Nutzer des Metaverse bedeutet der EDA mehr Kontrolle über ihre Daten. Sie könnten beispielsweise entscheiden, wie ihre Daten genutzt werden, oder ihre Daten zwischen verschiedenen Plattformen portieren. Dies stärkt das Vertrauen in das Metaverse und fördert dessen Akzeptanz.

2.5 electronic IDentification, Authentication and trust Services (eIDAS)

Die Verordnung über elektronische Identifizierung, Authentifizierung und Vertrauensdienste (eIDAS) ist ein zentrales Regulierungsvorhaben der Europäischen Union, das darauf abzielt, ein rechtliches und technisches Rahmenwerk für elektronische Identitäten und Vertrauensdienste zu schaffen. Diese Verordnung spielt eine entscheidende Rolle bei der Digitalisierung und Integration von Dienstleistungen in Europa. Mit dem Aufkommen neuer Technologien wie dem Metaverse gewinnt die eIDAS-Verordnung an neuer Relevanz, da sie dazu beiträgt, Vertrauen und Sicherheit in dieser neuen digitalen Umgebung zu etablieren. Im Folgenden werden die Grundzüge der eIDAS-Verordnung, ihre allgemeine Bedeutung sowie ihre potenziellen Auswirkungen auf das Metaverse dargelegt.

2.5.1 Grundzüge der eIDAS-Verordnung

Die eIDAS-Verordnung wurde im Jahr 2014 von der Europäischen Union verabschiedet, um einen einheitlichen rechtlichen Rahmen für elektronische Identitäten, Authentifizierungsmethoden und Vertrauensdienste zu schaffen. Ziel der Verordnung ist es, die grenzüberschreitende Nutzung elektronischer Identitäten und Vertrauensdienste innerhalb der EU zu erleichtern, um den Binnenmarkt zu stärken und die Digitalisierung zu fördern.

Die Verordnung umfasst mehrere zentrale Elemente:

- **Elektronische Identitäten (eIDs):** Mitgliedsstaaten der EU sind verpflichtet, nationale elektronische Identitätssysteme zu entwickeln, die interoperabel sind und von anderen EU-Ländern anerkannt werden. Dies erleichtert die grenzüberschreitende Authentifizierung.
- **Vertrauensdienste:** eIDAS regelt die Bereitstellung von Vertrauensdiensten wie elektronische Signaturen, elektronische Siegel, Zeitstempel, elektronische Zustelldienste und Website-Zertifikate. Diese Dienste garantieren die Integrität, Authentizität und Vertraulichkeit von digitalen Transaktionen.
- **Rechtliche Anerkennung:** Elektronische Signaturen und andere Vertrauensdienste, die gemäß eIDAS erstellt wurden, haben die gleiche rechtliche Gültigkeit wie ihre papierbasierten Äquivalente.
- **Interoperabilität:** eIDAS legt Standards für die Interoperabilität zwischen verschiedenen elektronischen Identitäts- und Vertrauensdienstsystemen fest, um die grenzüberschreitende Nutzung zu gewährleisten.
- **Sicherheitsanforderungen:** Die Verordnung stellt hohe Anforderungen an die Sicherheit und Zuverlässigkeit der Dienste, um Missbrauch und Manipulation zu verhindern.

2.5.2 Bedeutung der eIDAS-Verordnung im Allgemeinen

Die eIDAS-Verordnung hat weitreichende Auswirkungen auf die digitale Transformation in Europa. Sie fördert das Vertrauen in digitale Dienste, indem sie einen rechtlich verbindlichen Rahmen für elektronische Identitäten und Vertrauensdienste schafft. Dadurch erleichtert sie den grenzüberschreitenden Zugang zu digitalen Diensten und stärkt den digitalen Binnenmarkt.

Ein zentraler Vorteil der eIDAS-Verordnung liegt in ihrer Förderung von Effizienz und Kosteneinsparungen. Unternehmen und Öffentliche Verwaltungen können durch die Nutzung elektronischer Signaturen und anderer digitaler Dienste Prozesse beschleunigen und Papierkosten reduzieren. Gleichzeitig profitieren Bürger von einer vereinfachten Interaktion mit Behörden und Unternehmen.

Die eIDAS-Verordnung dient auch als globaler Standard. Sie hat dazu beigetragen, das Bewusstsein für die Bedeutung von digitalen Identitäten und Vertrauensdiensten zu schärfen und hat andere Regionen und Länder inspiriert, ähnliche Regelwerke einzuführen.

2.5.3 Auswirkungen der eIDAS-Verordnung auf das Metaverse

Das Metaverse ist ein aufstrebendes digitales Ökosystem, das immersive virtuelle Realität (VR) und erweiterte Realität (AR) kombiniert, um neue Formen der Interaktion, des Handels und der sozialen Vernetzung zu ermöglichen. In einer solchen Umgebung ist die sichere und vertrauenswürdige Verwaltung von Identitäten und Transaktionen von entscheidender Bedeutung. Die eIDAS-Verordnung könnte das Metaverse in mehrfacher Hinsicht beeinflussen:

- **Sichere digitale Identitäten im Metaverse:** Im Metaverse spielen digitale Identitäten eine zentrale Rolle, da sie den Nutzern Zugang zu virtuellen Welten und Dienstleistungen ermöglichen. Die eIDAS-Verordnung könnte dazu beitragen, dass diese Identitäten sicher und interoperabel sind. Nutzer könnten ihre nationalen elektronischen Identitäten (eIDs) nutzen, um sich im Metaverse auszuweisen, was die Sicherheit und das Vertrauen in digitale Interaktionen erhöhen würde.
- **Vertrauensdienste für Transaktionen:** Das Metaverse wird voraussichtlich eine Vielzahl von wirtschaftlichen Aktivitäten umfassen, darunter digitale Transaktionen, virtuelle Immobilienkäufe und Verträge. Die eIDAS-Verordnung bietet durch elektronische Signaturen und Siegel eine rechtlich anerkannte Möglichkeit, solche Transaktionen sicher und verbindlich abzuschließen. Dies würde das Vertrauen in wirtschaftliche Aktivitäten im Metaverse stärken.

- **Schutz vor Identitätsdiebstahl und Betrug:** Da das Metaverse eine intensive Nutzung digitaler Identitäten erfordert, besteht ein hohes Risiko für Identitätsdiebstahl und Betrug. Die eIDAS-Verordnung stellt sicher, dass hohe Sicherheitsstandards für die Verwaltung und Authentifizierung von Identitäten gelten. Dies würde dazu beitragen, solche Risiken zu minimieren und die Integrität der digitalen Identitäten zu gewährleisten.
- **Interoperabilität zwischen virtuellen Welten:** Das Metaverse besteht aus einer Vielzahl von Plattformen und virtuellen Welten, die oft von unterschiedlichen Unternehmen betrieben werden. Die eIDAS-Verordnung könnte durch die Förderung von Standards und Interoperabilität sicherstellen, dass Nutzer ihre Identitäten und Vertrauensdienste plattformübergreifend verwenden können. Dies würde die Benutzerfreundlichkeit und Zugänglichkeit des Metaverse erheblich verbessern.
- **Rechtssicherheit im Metaverse:** Ein zentrales Anliegen im Metaverse ist die Frage der rechtlichen Verbindlichkeit von digitalen Interaktionen und Vereinbarungen. Durch die Anerkennung elektronischer Signaturen und anderer Vertrauensdienste bietet die eIDAS-Verordnung eine Grundlage für rechtssichere Transaktionen. Nutzer und Unternehmen könnten sicher sein, dass ihre digitalen Handlungen rechtsverbindlich sind.
- **Förderung der Nutzerautonomie:** Die eIDAS-Verordnung gibt den Nutzern mehr Kontrolle über ihre digitalen Identitäten und die Art und Weise, wie diese verwendet werden. Im Metaverse könnten Nutzer selbst entscheiden, welche Informationen sie teilen und wie sie sich authentifizieren, was ihre Autonomie und Privatsphäre stärkt.

2.6 Artificial Intelligence Act (AI Act)

Der Artificial Intelligence Act (AI Act) der Europäischen Union ist eine wegweisende Gesetzesinitiative, die darauf abzielt, die Nutzung von künstlicher Intelligenz (KI) zu regulieren und ein ausgewogenes Verhältnis zwischen Innovation, Sicherheit und ethischen Standards zu schaffen. Da KI eine zentrale Rolle im Metaverse spielt, hat der AI Act potenziell weitreichende Auswirkungen auf dessen Entwicklung und Nutzung. Dieser Beitrag beleuchtet die Grundzüge des AI Act, seine allgemeine Bedeutung sowie die spezifischen Auswirkungen auf das Metaverse.

2.6.1 Grundzüge des AI Act

Der AI Act wurde von der Europäischen Kommission im April 2021 vorgestellt und soll einen rechtlichen Rahmen schaffen, um die Entwicklung und Anwendung von KI-Systemen in der EU zu regulieren. Die Verordnung basiert auf einem risikobasierten Ansatz, der KI-Systeme je nach

ihrem potenziellen Risiko für Einzelpersonen und die Gesellschaft in verschiedene Kategorien einteilt:

- **Verbotene KI-Systeme:** Diese umfassen KI-Anwendungen, die als unvertretbar angesehen werden, wie z. B. Systeme zur manipulativen Verhaltensänderung oder solche, die soziale Bewertungssysteme wie in autoritären Regimen implementieren.
- **Hochrisiko-KI-Systeme:** Hierzu gehören Anwendungen, die in sensiblen Bereichen wie der Gesundheitsversorgung, der Strafverfolgung oder der kritischen Infrastruktur eingesetzt werden. Solche Systeme müssen strengen Anforderungen in Bezug auf Transparenz, Genauigkeit und Sicherheitskontrollen genügen.
- **KI mit geringem Risiko:** KI-Systeme, die Interaktionen wie Chatbots oder Empfehlungssysteme betreffen, unterliegen weniger strikten Regeln, müssen jedoch Transparenzpflichten erfüllen.
- **Minimales Risiko:** Anwendungen wie KI-basierte Spiele oder Spam-Filter fallen in diese Kategorie und unterliegen kaum regulatorischen Anforderungen.
- Zusätzlich legt der AI Act Anforderungen an die Datenqualität, Transparenz, menschliche Aufsicht und Cybersicherheit fest. Ziel ist es, sicherzustellen, dass KI-Systeme fair, sicher und im Einklang mit den Grundrechten genutzt werden.

2.6.2 Bedeutung des AI Act im Allgemeinen

Der AI Act ist die weltweit erste umfassende gesetzliche Regelung für KI und hat das Potenzial, globale Standards zu setzen. Die Verordnung zielt darauf ab, das Vertrauen in KI-Systeme zu stärken und gleichzeitig Innovationen zu fördern. Indem sie klare Regeln und Anforderungen schafft, bietet sie Unternehmen eine Orientierungshilfe und reduziert rechtliche Unsicherheiten.

Eine wichtige Errungenschaft des AI Act ist der Schutz grundlegender Rechte. Die Verordnung stellt sicher, dass KI-Systeme die Menschenwürde, Privatsphäre und Gleichberechtigung respektieren. Dies ist besonders wichtig angesichts der zunehmenden Verbreitung von KI in sensiblen Bereichen.

Darüber hinaus unterstützt der AI Act Unternehmen dabei, KI ethisch und nachhaltig zu entwickeln. Er fordert eine verantwortungsvolle Innovationskultur, die sowohl den wirtschaftlichen als auch den gesellschaftlichen Nutzen von KI maximiert. Gleichzeitig hilft er, Missbrauch und Risiken zu minimieren.

Durch seine Vorreiterrolle könnte der AI Act auch internationale Gesetzgebungsprozesse beeinflussen. Andere Regionen, wie die USA oder China, könnten ähnliche Regelungen entwickeln, um die Anforderungen des EU-Marktes zu erfüllen und Wettbewerbsvorteile zu sichern.

2.6.3 Auswirkungen des AI Act auf das Metaverse

Das Metaverse ist ein digitales Ökosystem, das immersive Technologien wie virtuelle Realität (VR), erweiterte Realität (AR) und KI kombiniert, um neue Formen der Interaktion, des Handels und der Unterhaltung zu schaffen. KI spielt eine Schlüsselrolle im Metaverse, indem sie z. B. virtuelle Assistenten, personalisierte Inhalte, Verhaltensanalyse und automatisierte Moderation ermöglicht. Der AI Act hat das Potenzial, die Entwicklung und Nutzung von KI im Metaverse maßgeblich zu beeinflussen:

- **Regulierung von KI-gestützten Inhalten und Interaktionen:** KI im Metaverse wird oft eingesetzt, um realistische virtuelle Umgebungen zu schaffen, die auf die Präferenzen und Verhaltensmuster der Nutzer abgestimmt sind. Der AI Act könnte sicherstellen, dass diese Systeme transparent sind und keine manipulativen oder diskriminierenden Algorithmen verwenden. Beispielsweise müssten Empfehlungssysteme, die Inhalte im Metaverse kuratieren, offenlegen, wie Entscheidungen getroffen werden, und sicherstellen, dass sie keine Vorurteile verstärken.
- **Schutz der Privatsphäre und Datenqualität:** Im Metaverse werden große Mengen personenbezogener Daten generiert und verarbeitet, darunter biometrische Daten, Bewegungsprofile und Kommunikationsmuster. Der AI Act stellt sicher, dass diese Daten in Übereinstimmung mit strengen Datenschutzstandards verwendet werden. Dies würde den Missbrauch sensibler Daten verhindern und das Vertrauen der Nutzer in das Metaverse stärken.
- **Moderation und ethische Nutzung von KI:** Virtuelle Welten im Metaverse könnten von hochentwickelten Moderationssystemen profitieren, die KI einsetzen, um illegale oder unangemessene Inhalte zu erkennen und zu entfernen. Der AI Act würde sicherstellen, dass solche Systeme fair und transparent arbeiten, ohne die Meinungsfreiheit unverhältnismäßig einzuschränken. Dies wäre entscheidend, um das Metaverse zu einem sicheren Raum für alle Nutzer zu machen.
- **Regulierung von Hochrisiko-KI im Metaverse:** Einige Anwendungen von KI im Metaverse könnten als hochriskant eingestuft werden, insbesondere wenn sie in sensiblen Bereichen wie Gesundheitsdiensten, Finanztransaktionen oder der biometrischen Authentifizierung eingesetzt werden. Der AI Act würde sicherstellen, dass solche Systeme strengen Prüfungen

unterzogen werden, bevor sie in Betrieb genommen werden. Dies würde nicht nur die Sicherheit erhöhen, sondern auch die Haftung und Verantwortlichkeit der Betreiber klären.

- **Innovationsförderung im Metaverse:** Während der AI Act strenge Regeln für Hochrisiko-KI setzt, bietet er auch Flexibilität für Anwendungen mit geringem Risiko. Dies könnte Innovationen im Metaverse fördern, indem es Start-ups und kleinen Unternehmen erleichtert wird, neue KI-gestützte Dienste zu entwickeln und bereitzustellen. Gleichzeitig würde der rechtliche Rahmen dazu beitragen, dass solche Innovationen ethisch und nachhaltig gestaltet werden.
- **Grenzüberschreitende Zusammenarbeit und Interoperabilität:** Das Metaverse ist ein globales Phänomen, das verschiedene Jurisdiktionen und regulatorische Ansätze verbindet. Der AI Act könnte dazu beitragen, Standards für KI im Metaverse zu harmonisieren und die grenzüberschreitende Zusammenarbeit zu erleichtern. Dies würde nicht nur den Handel und die Innovation fördern, sondern auch sicherstellen, dass Nutzer weltweit von den gleichen hohen Sicherheits- und Ethikstandards profitieren.

2.7 Net Neutrality Regulation

Die Netzneutralitätsverordnung (Net Neutrality Regulation) ist ein zentrales Prinzip der Internetregulierung, das darauf abzielt, den freien und gleichen Zugang zu digitalen Inhalten und Diensten sicherzustellen. Sie verpflichtet Internetdiensteanbieter (ISPs) dazu, alle Daten im Internet gleich zu behandeln, ohne sie zu blockieren, zu drosseln oder zu priorisieren. In einer Zeit, in der digitale Technologien und Plattformen wie das Metaverse zunehmend an Bedeutung gewinnen, hat die Netzneutralität erhebliche Auswirkungen auf dessen Entwicklung. Dieser Beitrag beleuchtet die Grundzüge der Netzneutralität, ihre allgemeine Bedeutung und die spezifischen Auswirkungen auf das Metaverse.

2.7.1 Grundzüge der Netzneutralitätsverordnung

Die Netzneutralitätsverordnung wurde in der Europäischen Union mit der Verordnung (EU) 2015/2120 eingeführt, um sicherzustellen, dass das Internet ein offener und fairer Raum bleibt. Die wichtigsten Grundsätze dieser Verordnung sind:

- **Gleichbehandlung von Daten:** ISPs dürfen keine diskriminierenden Praktiken anwenden, die bestimmte Inhalte, Dienste oder Anwendungen bevorzugen oder benachteiligen.
- **Verbot von Blockierung und Drosselung:** Datenverkehr darf nicht blockiert oder verlangsamt werden, es sei denn, es liegen spezifische rechtliche oder technische Gründe vor, wie z. B. die Bekämpfung illegaler Inhalte oder die Vermeidung von Netzüberlastungen.

- Keine bezahlte Priorisierung: ISPs dürfen keine bezahlten Abkommen mit Anbietern von Inhalten oder Diensten eingehen, um deren Datenverkehr zu bevorzugen.
- Transparenzanforderungen: ISPs müssen ihren Kunden klare und transparente Informationen über die Geschwindigkeit und Qualität ihrer Dienste bereitstellen.

2.7.2 Bedeutung der Netzneutralität im Allgemeinen

Die Netzneutralität hat grundlegende Auswirkungen auf die Struktur und Funktionsweise des Internets. Sie stellt sicher, dass das Internet ein offenes und inklusives Medium bleibt, das Innovationen und Wettbewerb fördert. Ohne Netzneutralität könnten ISPs entscheiden, welche Dienste oder Inhalte bevorzugt behandelt werden, was zu einer Dominanz großer Anbieter führen und Start-ups sowie kleinere Unternehmen benachteiligen würde.

Für Verbraucher bedeutet Netzneutralität, dass sie freien Zugang zu allen Inhalten und Diensten im Internet haben, ohne dass deren Qualität oder Verfügbarkeit von finanziellen Absprachen zwischen ISPs und Inhaltenanbietern abhängt. Dies fördert die Meinungsfreiheit, den Zugang zu Informationen und die Vielfalt digitaler Inhalte.

Auf globaler Ebene hat die Netzneutralität auch politische und wirtschaftliche Bedeutung. Sie unterstützt den fairen Wettbewerb und verhindert die Konzentration von Macht bei wenigen großen Unternehmen. Gleichzeitig dient sie als Modell für andere Regionen und Länder, die ähnliche Regelungen implementieren wollen.

2.7.3 Auswirkungen der Netzneutralität auf das Metaverse

Das Metaverse, eine virtuelle Welt, die immersive Technologien wie Virtual Reality (VR) und Augmented Reality (AR) nutzt, ist stark auf eine stabile und diskriminierungsfreie Internetinfrastruktur angewiesen. Die Netzneutralitätsverordnung hat erhebliche Auswirkungen auf die Entwicklung und Nutzung des Metaverse:

- Gleicher Zugang zu virtuellen Welten: Im Metaverse existieren zahlreiche Plattformen und Dienste, die von unterschiedlichen Unternehmen betrieben werden. Netzneutralität stellt sicher, dass keine Plattform bevorzugt oder benachteiligt wird. Nutzer könnten auf alle virtuellen Welten und Inhalte zugreifen, ohne Einschränkungen oder Zusatzkosten durch ISPs befürchten zu müssen. Dies fördert Vielfalt und Chancengleichheit im Metaverse.
- Förderung von Innovation und Wettbewerb: Das Metaverse bietet immense Chancen für Start-ups und kleine Unternehmen, innovative Dienste und Anwendungen zu entwickeln. Netzneutralität verhindert, dass große Plattformen ihre Marktstellung durch bezahlte

Priorisierung ausnutzen, und schafft so gleiche Wettbewerbsbedingungen. Dies ist entscheidend, um Innovationen im Metaverse zu fördern und Monopolbildungen zu vermeiden.

- **Sicherstellung von Nutzererfahrungen:** Die Qualität der Nutzererfahrung im Metaverse hängt stark von einer stabilen und schnellen Internetverbindung ab. Netzneutralität stellt sicher, dass alle Daten im Metaverse gleichbehandelt werden, was eine gleichbleibend hohe Qualität der Dienste gewährleistet. Ohne Netzneutralität könnten ISPs die Geschwindigkeit oder Qualität bestimmter Dienste drosseln, was die Nutzererfahrung erheblich beeinträchtigen würde.
- **Schutz vor Monopolisierung:** Ohne Netzneutralität besteht das Risiko, dass große Unternehmen mit ISPs exklusive Abkommen treffen, um ihre Dienste im Metaverse zu priorisieren. Dies könnte dazu führen, dass kleinere Anbieter und Plattformen im Wettbewerb benachteiligt werden. Die Netzneutralität wirkt dem entgegen, indem sie gleiche Bedingungen für alle Anbieter schafft.
- **Stärkung der Nutzerrechte:** Netzneutralität gibt Nutzern die Freiheit, Inhalte und Dienste im Metaverse ohne Einschränkungen zu erkunden. Dies fördert nicht nur die Kreativität und Innovation, sondern auch die individuelle Autonomie und Selbstbestimmung der Nutzer in der virtuellen Welt.

2.8 EU Fitness Check on Digital Fairness

Der EU Fitness Check on Digital Fairness ist eine Initiative der Europäischen Union, die darauf abzielt, die Fairness und Transparenz in digitalen Geschäftsmodellen und Plattformen zu bewerten. Dieser „Fitness Check“ analysiert bestehende Rechtsvorschriften und untersucht, ob diese ausreichen, um Verbraucherrechte, Wettbewerb und Chancengleichheit in der digitalen Wirtschaft zu gewährleisten. Mit der zunehmenden Bedeutung des Metaverse als neues digitales Ökosystem gewinnt der Fitness Check weiter an Relevanz. Im Folgenden werden die Grundzüge des EU Fitness Check on Digital Fairness, seine allgemeine Bedeutung und die spezifischen Auswirkungen auf das Metaverse beleuchtet.

2.8.1 Grundzüge des EU Fitness Check on Digital Fairness

Der EU Fitness Check on Digital Fairness wurde ins Leben gerufen, um sicherzustellen, dass die europäischen Verbraucherrechte und wettbewerbsrechtlichen Standards in einer sich schnell entwickelnden digitalen Welt weiterhin wirksam sind. Im Kern geht es darum, bestehende Gesetzgebungen, wie die Richtlinie über unlautere Geschäftspraktiken, die Verbraucherrechte-

Richtlinie und die Preisangabenrichtlinie, auf ihre Effektivität und Angemessenheit in der digitalen Ära zu überprüfen.

Zentrale Aspekte des Fitness Checks umfassen:

- Transparenz in digitalen Plattformen und Geschäftsmodellen: Sicherstellung, dass Nutzer klare Informationen über Preise, Vertragsbedingungen und die Funktionsweise von Algorithmen erhalten.
- Bekämpfung unlauterer Geschäftspraktiken: Verhinderung manipulativer Techniken, wie beispielsweise „Dark Patterns“, die Verbraucher dazu verleiten, unbewusst Entscheidungen zu treffen, die nicht in ihrem Interesse liegen.
- Schutz vor Diskriminierung: Sicherstellung, dass Algorithmen keine diskriminierenden Entscheidungen treffen, sei es auf Basis von Herkunft, Geschlecht oder anderen Faktoren.
- Förderung von Wettbewerb und Chancengleichheit: Gewährleistung, dass alle Marktteilnehmer, insbesondere kleine und mittlere Unternehmen (KMU), gleiche Chancen in der digitalen Wirtschaft erhalten.

Der Fitness Check setzt dabei auf umfassende Konsultationen mit Verbrauchern, Unternehmen und anderen Stakeholdern, um ein ausgewogenes Bild der aktuellen Herausforderungen und Möglichkeiten zu erhalten.

2.8.2 Bedeutung des EU Fitness Check on Digital Fairness im Allgemeinen

Im Kontext der digitalen Transformation hat der Fitness Check eine grundlegende Bedeutung für die europäische Wirtschaft und Gesellschaft. Er stellt sicher, dass der digitale Binnenmarkt transparent, fair und wettbewerbsorientiert bleibt. Mit der ständigen Entwicklung neuer Technologien wie Künstlicher Intelligenz (KI), Big Data und personalisierter Werbung ist es entscheidend, dass rechtliche Rahmenbedingungen Schritt halten und Missbrauch verhindern.

Die Initiative stärkt die Rechte der Verbraucher, indem sie sicherstellt, dass diese in der digitalen Welt informierte Entscheidungen treffen können. Gleichzeitig schafft sie gleiche Wettbewerbsbedingungen für Unternehmen, indem sie unlautere Praktiken und Marktmissbrauch bekämpft. Dies fördert Innovationen und Vertrauen in digitale Plattformen und Geschäftsmodelle.

Darüber hinaus hat der Fitness Check globale Auswirkungen. Als Vorreiter in der Regulierung der digitalen Wirtschaft setzt die EU Standards, die oft von anderen Regionen und Ländern übernommen werden. Dies schafft nicht nur Klarheit für internationale Unternehmen, die auf

dem EU-Markt tätig sind, sondern treibt auch die Harmonisierung globaler digitaler Standards voran.

2.8.3 Auswirkungen des EU Fitness Check on Digital Fairness auf das Metaverse

Das Metaverse ist eine dynamische und komplexe digitale Umgebung, in der Nutzer interagieren, handeln und Inhalte erstellen können. Es ist eine Mischung aus virtuellen Welten, die stark auf Technologien wie Virtual Reality (VR), Augmented Reality (AR) und KI basieren. Der EU Fitness Check on Digital Fairness hat erhebliche Implikationen für die Entwicklung und Nutzung des Metaverse:

- **Transparenz in virtuellen Geschäftsmodellen:** Im Metaverse gibt es zahlreiche Geschäftsmodelle, von virtuellen Marktplätzen bis hin zu abonnementbasierten Diensten. Der Fitness Check stellt sicher, dass Nutzer klare und transparente Informationen über Preise, Vertragsbedingungen und die Funktionsweise digitaler Produkte erhalten. Dies ist entscheidend, um Verbrauchertäuschung und undurchsichtige Praktiken zu verhindern.
- **Bekämpfung manipulativer Techniken:** Das Metaverse bietet Unternehmen neue Möglichkeiten, Nutzer zu beeinflussen, beispielsweise durch immersive Werbung oder „Dark Patterns“, die die Entscheidungsfreiheit einschränken. Der Fitness Check hilft, solche manipulativen Praktiken zu identifizieren und zu regulieren, um sicherzustellen, dass Nutzer im Metaverse frei und informierte Entscheidungen treffen können.
- **Schutz vor algorithmischer Diskriminierung:** Im Metaverse spielen Algorithmen eine zentrale Rolle, sei es bei der Personalisierung von Inhalten, der Moderation von Communities oder der Platzierung von Werbung. Der Fitness Check stellt sicher, dass solche Algorithmen fair und diskriminierungsfrei gestaltet sind. Dies ist besonders wichtig, um die Chancengleichheit zu wahren und Diskriminierung zu verhindern.
- **Förderung von Wettbewerb und Innovation:** Das Metaverse bietet großen Plattformen die Möglichkeit, dominante Positionen einzunehmen. Der Fitness Check stellt sicher, dass Wettbewerb und Chancengleichheit gefördert werden, insbesondere für kleinere Unternehmen und Start-ups. Dies ist entscheidend, um ein vielfältiges und innovatives Ökosystem im Metaverse zu schaffen.
- **Stärkung des Verbrauchervertrauens:** Das Metaverse steht noch am Anfang seiner Entwicklung, und viele Nutzer stehen dieser neuen Technologie mit Skepsis gegenüber. Der Fitness Check trägt dazu bei, Vertrauen aufzubauen, indem er sicherstellt, dass die Rechte der Verbraucher gewahrt bleiben und digitale Plattformen fair und transparent agieren.

3. Rechtsgebiete

3.1 Anwaltliches Berufsrecht

3.1.1 Rechtsvorschriften im Rechtsgebiet

Das anwaltliche Berufsrecht im Metaverse unterliegt in Deutschland primär der Bundesrechtsanwaltsordnung (BRAO), der Berufsordnung für Rechtsanwälte (BORA) und dem Rechtsdienstleistungsgesetz (RDG). Für grenzüberschreitende Sachverhalte ist die Rom-I-Verordnung (Rom I-VO) entscheidend, die das anwendbare Recht bei Verträgen regelt. In digitalen Kontexten ist zudem das Telemediengesetz (TMG) relevant, insbesondere wenn Rechtsdienstleistungen über das Metaverse erbracht werden. Ergänzend gelten die Datenschutz-Grundverordnung (DS-GVO) und nationale Datenschutzgesetze, da Anwälte im Metaverse mit sensiblen Daten umgehen. Zudem können Plattform-AGBs das Vertragsverhältnis beeinflussen.

3.1.2 Geltende Grundprinzipien

Die anwaltliche Verschwiegenheit gemäß § 43a Abs. 2 BRAO ist zentral, auch im digitalen Raum. Anwälte sind zur Wahrung der Vertraulichkeit verpflichtet, was technische Sicherheitsmaßnahmen im Metaverse erfordert. Das Prinzip der Unabhängigkeit (§ 3 Abs. 1 BRAO) bleibt auch im virtuellen Raum essenziell, um die Freiheit der Mandatsbearbeitung zu gewährleisten. Ebenso gilt das Prinzip der Parteiautonomie, welches durch die Rom I-VO abgesichert wird. Bei der Leistungserbringung im Metaverse muss zusätzlich die Personenauthentifizierung erfolgen, um sicherzustellen, dass Verträge tatsächlich mit der identifizierten Partei abgeschlossen werden. Die Anforderungen an Transparenz und Fairness, etwa in Bezug auf die Gestaltung von Wahlklauseln, bleiben unverändert.

3.1.3 Prioritäre juristische Fragestellungen im Kontext anwaltliches Berufsrecht

Im Metaverse stehen mehrere Fragen im Vordergrund: Wie kann die Authentifizierung von Mandanten sichergestellt werden, da Interaktionen oft über Avatare erfolgen? Welches Recht gilt für im Metaverse abgeschlossene Verträge – insbesondere bei grenzüberschreitenden Mandaten? Welche rechtlichen Anforderungen bestehen an die Nutzung von Smart Contracts? Außerdem sind Fragen der Datensicherheit und des Mandantenschutzes im virtuellen Raum besonders relevant. Ein weiteres Thema ist die Einhaltung anwaltlicher Pflichten in einer Umgebung, die stark von Plattformbetreibern beeinflusst wird. Schließlich wird diskutiert, wie anwaltliche Tätigkeiten – etwa Prozessvertretungen – digital in Übereinstimmung mit geltenden Verfahrensregeln durchgeführt werden können.

3.1.4 Wichtigste rechtliche Risiken

Zentrale Risiken umfassen Datenschutzverletzungen, da die Nutzung des Metaverse umfangreiche personenbezogene Daten erfasst, einschließlich biometrischer Daten. Eine unzureichende Authentifizierung kann dazu führen, dass sensible Informationen in falsche Hände gelangen. Weiterhin können Konflikte über das anwendbare Recht entstehen, insbesondere bei grenzüberschreitenden Mandaten. Verstöße gegen anwaltliche Verschwiegenheitspflichten durch Sicherheitslücken sind ein weiteres Risiko. Auch die Einhaltung der Formvorschriften bei Verträgen, etwa bei Grundstückskäufen oder Vollmachten, ist problematisch, da derzeitige Regelungen oft auf analoge Prozesse ausgerichtet sind. Die Gefahr rechtlicher Auseinandersetzungen mit Plattformbetreibern, etwa bei der Durchsetzung von Mandantenrechten, besteht ebenfalls.

3.1.5 Best Practice

Gesetzeskonform sind Handlungen, die bestehende berufliche Pflichten beachten und auf den sicheren Umgang mit Mandantendaten abzielen. Dazu zählt die Implementierung sicherer Authentifizierungsmechanismen, wie Zwei-Faktor-Authentifizierung oder biometrische Verfahren. Ebenso gehört die transparente Gestaltung von Verträgen, einschließlich der Einbindung von Rechtswahlklauseln gemäß Rom I-VO, zu gesetzeskonformen Handlungen. Die Nutzung von Smart Contracts ist erlaubt, solange sie den allgemeinen Rechtsgrundsätzen entsprechen und keine zwingenden Formvorschriften verletzen. Anwälte müssen ihre Leistungen so gestalten, dass die Anforderungen des TMG und RDG eingehalten werden, insbesondere wenn sie Mandate vollständig über das Metaverse abwickeln.

3.1.6 Worst Practice

Gesetzeswidrig sind Handlungen, die gegen Verschwiegenheitspflichten verstoßen, wie die Nutzung unsicherer Kommunikationswege. Ebenso unzulässig ist die Erbringung von Rechtsdienstleistungen ohne die erforderlichen Zulassungen oder ohne Einhaltung der Vorgaben des RDG. Verstöße gegen Datenschutzgesetze, etwa durch die unbefugte Verarbeitung biometrischer Daten, sind ebenfalls verboten. Die Missachtung der Formvorschriften bei Vertragsabschlüssen, wie der Schriftform bei Grundstücksverträgen (§ 311b BGB), ist problematisch. Zudem sind Rechtswahlklauseln in Verbraucherverträgen, die gegen Art. 6 Rom I-VO verstoßen, unzulässig. Schließlich sind unzureichende Sicherheitsmaßnahmen, die eine Verletzung anwaltlicher Pflichten ermöglichen, rechtlich nicht zulässig.

3.2 Arbeitsrecht

3.2.1 Rechtsvorschriften im Rechtsgebiet

Das Arbeitsrecht im Metaverse basiert auf bestehenden nationalen Vorschriften, da es keine spezifischen internationalen Regelungen gibt. In Deutschland gelten insbesondere das Arbeitszeitgesetz (ArbZG), das Maßnahmen zur Regelung von Arbeits- und Pausenzeiten vorschreibt, und das Arbeitsschutzgesetz (ArbSchG), das den Schutz der physischen und psychischen Gesundheit von Arbeitnehmern verlangt. Auch das Bundesdatenschutzgesetz (BDSG) und die Datenschutz-Grundverordnung (DSGVO) spielen eine zentrale Rolle, insbesondere bei der Verarbeitung der im Metaverse generierten personenbezogenen Daten. Mitbestimmungsrechte von Betriebsräten gemäß dem Betriebsverfassungsgesetz (BetrVG) sind ebenfalls relevant, insbesondere wenn XR-Technologien eingeführt oder genutzt werden.

3.2.2 Geltende Grundprinzipien

Im Metaverse gelten grundlegende Prinzipien des Arbeitsrechts, darunter die Fürsorgepflicht des Arbeitgebers, der für sichere und gesunde Arbeitsbedingungen sorgen muss, auch in der virtuellen Realität. Das Direktionsrecht des Arbeitgebers erlaubt es, den Inhalt, Ort und die Zeit der Arbeitsleistung zu bestimmen, jedoch nur im Rahmen billigen Ermessens. Der Arbeitnehmerdatenschutz verlangt eine strenge Kontrolle über die Verarbeitung personenbezogener Daten. Schließlich sind Mitbestimmungsrechte der Arbeitnehmervertretungen bei der Einführung neuer Technologien zu wahren, um die Rechte und Interessen der Belegschaft zu schützen.

3.2.3 Prioritäre juristische Fragestellungen im Kontext Arbeitsrecht

Drei zentrale Fragestellungen ergeben sich im Zusammenhang mit dem Metaverse. Erstens ist unklar, wie XR-Arbeitsplätze rechtskonform und sicher gestaltet werden können. Zweitens stellt sich die Frage, wie flexible Arbeitszeitmodelle implementiert werden können, ohne dass Arbeit und Freizeit verschwimmen. Drittens ist der Umgang mit den umfangreichen Daten, die im Metaverse generiert werden, ein kritisches Thema, insbesondere im Hinblick auf den Schutz der Privatsphäre und die rechtliche Zulässigkeit von Leistungskontrollen.

3.2.4 Wichtigste rechtliche Risiken

Mit der Nutzung des Metaverse gehen auch rechtliche Risiken einher. Datenschutzverletzungen sind ein großes Risiko, da die erhobenen Daten oft sehr umfassend und sensibel sind. Darüber hinaus können übermäßige Nutzung von VR-Technologien oder schlechte Arbeitsbedingungen im Metaverse physische und psychische Gesundheitsprobleme verursachen. Ein weiteres Risiko

besteht in der Entgrenzung von Arbeit und Freizeit, wenn keine klaren Regelungen zu Arbeitszeiten und Pausen bestehen.

3.2.5 Best Practice

Im Metaverse umfasst gesetzestkonformes Handeln verschiedene Maßnahmen, die den bestehenden arbeitsrechtlichen Vorgaben entsprechen. Ein zentrales Beispiel ist die Durchführung von Gefährdungsbeurteilungen, die gemäß § 3 ArbSchG verpflichtend sind. Diese Beurteilungen stellen sicher, dass Arbeitnehmer durch die Nutzung von XR-Technologien keine gesundheitlichen Schäden erleiden, etwa durch Belastungen wie Motion Sickness oder die Langzeitnutzung von VR-Brillen. Zudem können Arbeitgeber Leitlinien für das Verhalten im Metaverse einführen, um Fehlverhalten wie Mobbing, Belästigungen oder respektlose Interaktionen zu vermeiden. Solche Leitlinien sind nicht nur Teil der Fürsorgepflicht des Arbeitgebers, sondern auch ein effektives Mittel, um das Arbeitsklima im virtuellen Raum zu wahren. Schließlich gehört die Einhaltung datenschutzrechtlicher Vorgaben, wie in der DSGVO und dem BDSG festgelegt, zu den gesetzestkonformen Handlungen. Dies umfasst Maßnahmen wie die Minimierung der Datenerhebung, transparente Kommunikation über die Nutzung der erhobenen Daten und die Sicherstellung, dass nur befugte Personen Zugriff auf die Daten haben.

3.2.6 Worst Practice

Gesetzeswidriges Handeln im Metaverse betrifft vor allem Verstöße gegen Arbeits- und Datenschutzvorschriften. Eine permanente Überwachung von Arbeitnehmern, etwa durch die kontinuierliche Erfassung von Bewegungen, Reaktionen oder biometrischen Daten, verstößt gegen § 26 BDSG. Solche Maßnahmen sind nur in sehr engen Grenzen zulässig, beispielsweise wenn sie für das Arbeitsverhältnis erforderlich und verhältnismäßig sind, was häufig nicht gegeben ist. Ebenso ist die einseitige Anordnung einer ausschließlichen Tätigkeit im Metaverse ohne vertragliche Grundlage unzulässig. Eine solche Anordnung stellt eine wesentliche Änderung der Arbeitsbedingungen dar und erfordert die Zustimmung des Arbeitnehmers oder entsprechende vertragliche Vereinbarungen, wie etwa eine Versetzungsklausel. Auch die Missachtung gesetzlicher Arbeitszeitregelungen, wie im Arbeitszeitgesetz festgelegt, ist ein häufiges Problem. Im Metaverse kann es dazu kommen, dass die Grenzen zwischen Arbeit und Freizeit verschwimmen, wenn keine klaren Regelungen zu Arbeitszeiten und Pausen bestehen. Das Fehlen von Ruhezeiten oder die Überschreitung der täglichen Höchstarbeitszeit sind klare Verstöße, die rechtliche Konsequenzen nach sich ziehen können.

Die Einhaltung der gesetzlichen Vorgaben ist entscheidend, um sowohl die Rechte der Arbeitnehmer zu schützen als auch potenzielle Haftungsrisiken für Arbeitgeber zu minimieren. Arbeitgeber sollten daher proaktiv Maßnahmen ergreifen, um die gesetzlichen Anforderungen zu erfüllen und Verstöße zu vermeiden.

3.3 Bank- und Kapitalmarktrecht

3.3.1 Rechtsvorschriften im Rechtsgebiet

Das Bank- und Kapitalmarktrecht im Kontext des Metaverse wird von verschiedenen regulatorischen Rahmenwerken beeinflusst. Zentral sind hier das Kreditwesengesetz (KWG), das Zahlungsdienstleistungsaufsichtsgesetz (ZAG), das Wertpapierinstitutsgesetz (WpIG) sowie die europäische Markets in Crypto-Assets Regulation (MiCAR). Diese Gesetze regeln Bankgeschäfte, Finanzdienstleistungen und den Umgang mit Kryptowerten. Ergänzt werden sie durch das Wertpapierprospektgesetz (WpPG) und das Gesetz über elektronische Wertpapiere (eWpG), die die Emission und den Handel von Finanzinstrumenten und Kryptowerten betreffen. Für grenzüberschreitende Transaktionen gelten zudem die Vorschriften der EU-Finanzmarktregulierung, insbesondere MiFID II. Die BaFin spielt bei der Anwendung dieser Gesetze eine Schlüsselrolle und stellt Richtlinien bereit, um die Erlaubnispflichten für Finanzdienstleister zu konkretisieren.

3.3.2 Geltende Grundprinzipien

Im Bank- und Kapitalmarktrecht stehen die Prinzipien der Rechtssicherheit, der Anleger- und Verbraucherschutz sowie die Marktintegrität im Vordergrund. Anbieter von Finanzdienstleistungen sind verpflichtet, klare und transparente Informationen bereitzustellen. Das Gebot der Verhältnismäßigkeit gilt bei der Ausgestaltung regulatorischer Anforderungen, insbesondere für innovative Technologien wie Blockchain und Kryptowährungen. Zudem wird das Prinzip der Technologieneutralität betont, um sicherzustellen, dass neue digitale Produkte wie NFTs oder Stablecoins nicht diskriminiert werden. Ein weiteres wichtiges Grundprinzip ist die Überwachung durch unabhängige Behörden wie die BaFin, um Missbrauch und Marktverzerrungen zu verhindern.

3.3.3 Prioritäre juristische Fragestellungen im Kontext Bank- und Kapitalmarktrecht

Im Metaverse ergeben sich zentrale Fragen zur Regulierung virtueller Vermögenswerte. Wie werden Kryptowährungen, NFTs und andere digitale Vermögenswerte rechtlich kategorisiert? Welche Anforderungen gelten für die Ausgabe, Verwahrung und den Handel solcher

Vermögenswerte? Besondere Herausforderungen bestehen bei der grenzüberschreitenden Erbringung von Finanzdienstleistungen und der Frage, wie das nationale Aufsichtsrecht anzuwenden ist, wenn Anbieter außerhalb Deutschlands agieren. Weiterhin stellt sich die Frage, ob bestehende Vorschriften wie die MiCAR ausreichen, um neue Produkte und Märkte im Metaverse zu regulieren. Auch die Abgrenzung zwischen erlaubnisfreien und erlaubnispflichtigen Tätigkeiten ist zentral.

3.3.4 Wichtigste rechtliche Risiken

Die Risiken im Bank- und Kapitalmarktrecht des Metaverse sind vielfältig. Ein zentrales Risiko ist die unzureichende Regulierung und Überwachung von Anbietern, die virtuelle Vermögenswerte herausgeben oder handeln. Dies kann zu Betrug, Geldwäsche oder Marktmanipulation führen. Weiterhin bestehen Unsicherheiten bei der Kategorisierung von Produkten wie NFTs, die je nach Ausgestaltung als Kryptowert, Finanzinstrument oder Vermögensanlage eingestuft werden könnten. Auch der Schutz der Anleger vor intransparenten oder hochriskanten Angeboten ist eine Herausforderung. Technologische Risiken, etwa durch Cyberangriffe oder technische Fehler in Smart Contracts, stellen ebenfalls eine Bedrohung dar.

3.3.5 Best Practice

Gesetzeskonform sind Handlungen, die den bestehenden gesetzlichen Anforderungen entsprechen. Dazu gehört die Einholung der erforderlichen Erlaubnisse bei der BaFin, wenn Finanzdienstleistungen oder Bankgeschäfte im Metaverse angeboten werden. Die ordnungsgemäße Prospektierung bei der Ausgabe von Kryptowerten oder Finanzinstrumenten sowie die Einhaltung der Anforderungen der MiCAR und anderer relevanter Gesetze sind ebenfalls notwendig. Anbieter, die ihre Dienstleistungen transparent gestalten und für ausreichende Sicherheitsmaßnahmen sorgen, bewegen sich im rechtlichen Rahmen. Auch die Nutzung von Technologien wie Blockchain ist erlaubt, solange sie den gesetzlichen Vorgaben entspricht.

3.3.6 Worst Practice

Gesetzeswidrig sind Handlungen, die gegen die oben genannten regulatorischen Anforderungen verstoßen. Dazu gehört die Erbringung erlaubnispflichtiger Dienstleistungen ohne Genehmigung, etwa der Handel mit Kryptowerten ohne BaFin-Erlaubnis. Die Ausgabe von Finanzinstrumenten oder Kryptowerten ohne Prospektierung oder die Verletzung von Transparenzanforderungen sind ebenfalls unzulässig. Aktivitäten, die auf Marktmanipulation oder Geldwäsche

abzielen, sind streng verboten. Zudem ist die Nichteinhaltung technischer und organisatorischer Sicherheitsanforderungen, die den Schutz der Anleger gefährden, gesetzeswidrig.

3.4 Strafrechtliche Verantwortlichkeit

3.4.1 Rechtsvorschriften im Rechtsgebiet

Im Metaverse finden die allgemeinen Vorschriften des deutschen Strafgesetzbuches (StGB) Anwendung, insbesondere die Bestimmungen zu Vermögensdelikten (§§ 242 ff. StGB), Betrug (§ 263 StGB), Computerbetrug (§ 263a StGB) und Datenveränderung (§ 303a StGB). Zudem sind internationale Regelungen und Abkommen, wie die Budapester Konvention über Cyberkriminalität, relevant. Das Telemediengesetz (TMG) und Datenschutzvorschriften, insbesondere die DSGVO, greifen ergänzend ein, insbesondere bei der Verarbeitung personenbezogener Daten und der Plattformbetreiberhaftung. § 9 StGB regelt die Zuständigkeit bei Taten mit internationalem Bezug, etwa durch Avatare in virtuellen Räumen.

3.5 Cyber Security

3.5.1 Rechtsvorschriften im Rechtsgebiet

Die Cybersicherheit im Metaverse unterliegt einer Vielzahl bestehender Vorschriften. In der EU gelten die DSGVO und das BSI-Gesetz, ergänzt durch die NIS2-Richtlinie und den geplanten Cyber Resilience Act (CRA), der verbindliche Mindeststandards für digitale Produkte vorsieht. Betreiber kritischer Infrastrukturen müssen nach § 8a BSI-Gesetz erhöhte Sicherheitsanforderungen erfüllen, falls XR-Technologien Teil dieser Systeme sind. Auch Smart Contracts und Blockchain-Technologien fallen zunehmend unter rechtliche Rahmenbedingungen.

3.5.2 Geltende Grundprinzipien

Grundprinzipien der Cybersicherheit umfassen die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Systemen. Diese Prinzipien gelten auch im Metaverse, wo der Schutz vor Datenlecks und Manipulationen durch dezentrale Sicherheitslösungen, wie Blockchain, verstärkt werden kann. Verantwortlichkeiten innerhalb der Sicherheitsinfrastruktur müssen klar zugewiesen werden, um interoperable Plattformen sicher zu gestalten. Präventive Maßnahmen und Sensibilisierung spielen dabei eine zentrale Rolle.

3.5.3 Prioritäre juristische Fragestellungen im Kontext Cyber Security

Die wichtigsten Fragestellungen betreffen den Schutz der Avataren-Integrität, da Identitätsdiebstahl und Avatar-Duplizierung Risiken darstellen. Ein weiteres Thema ist die Sicherstellung sicherer Interoperabilität zwischen Plattformen, was technische und rechtliche

Herausforderungen aufwirft. Schließlich sind Smart Contracts und deren rechtliche Sicherheit, insbesondere bei Transaktionen, entscheidend, um Betrug und Manipulation zu verhindern.

3.5.4 Wichtigste rechtliche Risiken

Zu den rechtlichen Risiken zählen die Unsicherheit über die Verantwortlichkeit bei Angriffen, insbesondere bei Plattforminteroperabilität, der Missbrauch von biometrischen Daten, wie sie in XR-Anwendungen oft verwendet werden, und die Gefahr durch neuartige Angriffe wie „Man-in-the-Room“-Hacks oder Deepfakes. Diese Risiken machen deutliche Sicherheitsmaßnahmen und rechtliche Klarheit erforderlich.

3.5.5 Best Practice

Gesetzeskonforme Handlungen umfassen die Implementierung technischer und organisatorischer Maßnahmen gemäß Art. 32 DSGVO, die Durchführung von Sicherheitsbewertungen, um Risiken zu minimieren, sowie die Einführung internationaler Standards für digitale Authentifizierung, etwa durch Blockchain-basierte Lösungen. Diese Maßnahmen helfen, Sicherheit und Vertrauen im Metaverse zu fördern.

3.5.6 Worst Practice

Gesetzeswidrig hingegen sind Verstöße gegen Datenschutzgesetze, wie das unautorisierte Sammeln und Verwenden personenbezogener Daten. Ebenso unzulässig ist die unzureichende Absicherung digitaler Infrastrukturen, die zu Datenlecks führen können. Schließlich ist die bewusste Umgehung von Sicherheitsvorschriften, etwa durch die Implementierung unsicherer Protokolle oder mangelhafter Sicherheitsstandards, rechtswidrig.

3.5.7 Geltende Grundprinzipien

Das Strafrecht orientiert sich an den Prinzipien der individuellen Verantwortlichkeit und der Tatbezogenheit. Handlungen eines Avatars im Metaverse werden der steuernden natürlichen Person zugerechnet. Kausalität, Adäquanz und objektive Zurechnung bilden die Grundlage für die Bewertung von Taten. Das Territorialitätsprinzip (§ 3 StGB) und das Schutzprinzip (§ 5 StGB) definieren, wann deutsches Strafrecht bei internationalen Sachverhalten greift. Ein zentrales Prinzip ist auch die Vermeidung von Doppelbestrafung (ne bis in idem), das durch internationale Abkommen geregelt wird.

3.5.8 Prioritäre juristische Fragestellungen im Kontext strafrechtlicher Verantwortlichkeit

Im Metaverse stellen sich Fragen zur strafrechtlichen Bewertung virtueller Handlungen. Beispielsweise: Wann ist das Verhalten eines Avatars strafbar? Wie werden Vermögensdelikte durch die Nutzung von NFTs oder Kryptowährungen bewertet? Welche Verantwortung tragen Plattformbetreiber? Ein weiteres Thema ist der grenzüberschreitende Vollzug des Strafrechts: Welches Recht gilt, wenn Täter und Opfer aus verschiedenen Ländern stammen? Schließlich sind die Anforderungen an Sicherheitsvorkehrungen zur Verhinderung strafbarer Handlungen zentral.

3.5.9 Wichtigste rechtliche Risiken

Zentrale Risiken umfassen Vermögensdelikte wie Betrug und Phishing, bei denen virtuelle Werte wie Kryptowährungen oder NFTs betroffen sind. Die mangelnde Transparenz und Anonymität im Metaverse erhöhen die Gefahr von Geldwäsche (§ 261 StGB) und Identitätsdiebstahl. Ebenso birgt die Plattformhaftung Risiken, da Betreiber verpflichtet sind, rechtswidriges Verhalten zu unterbinden, etwa Hassrede oder Kinderpornographie. Technische Schwächen, etwa Sicherheitslücken in Smart Contracts, können weitere Probleme schaffen.

3.5.10 Best Practice

Gesetzeskonform sind Handlungen, die den gesetzlichen Vorgaben entsprechen, wie die rechtmäßige Nutzung virtueller Vermögenswerte und die Einhaltung von Datenschutz- und Sicherheitsvorgaben. Die Erbringung von Dienstleistungen, etwa der Verkauf von NFTs, ist erlaubt, sofern dies transparent und ohne Täuschung erfolgt. Plattformbetreiber müssen Mechanismen einrichten, um illegale Aktivitäten zu verhindern, und rechtliche Rahmenbedingungen wie das Jugendschutzgesetz (JuSchG) einhalten.

3.5.11 Worst Practice

Gesetzeswidrig sind unter anderem Phishing-Angriffe, bei denen Nutzer zur Preisgabe von Passwörtern oder Schlüsseln zu Wallets verleitet werden, sowie Manipulationen in der virtuellen Welt, die Vermögensschäden verursachen. Auch das Betreiben von nicht genehmigten Bankgeschäften im Zusammenhang mit Kryptowährungen oder das Ignorieren von Sicherheitsanforderungen durch Plattformbetreiber ist illegal. Straftaten wie Nötigung, Bedrohung oder Verleumdung über Avatare fallen ebenso unter strafrechtliche Verfolgung.

3.6 Datenschutz

3.6.1 Rechtsvorschriften im Rechtsgebiet

Die datenschutzrechtliche Rechtslage im Metaverse basiert hauptsächlich auf der DSGVO und ergänzenden Regelungen wie dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG). Die DSGVO gilt für jede Verarbeitung personenbezogener Daten, einschließlich biometrischer und sensibler Daten, wie sie in XR- und Metaverse-Anwendungen häufig vorkommen. Das TTDSG ergänzt diese Vorschriften, insbesondere durch Regelungen zur Privatsphäre bei Endeinrichtungen und Kommunikation. Eine besondere Herausforderung ist der internationale Datentransfer, etwa in unsichere Drittstaaten wie die USA.

3.6.2 Geltende Grundprinzipien

Die Grundprinzipien umfassen Transparenz, Zweckbindung und Datenminimierung. Unternehmen müssen sicherstellen, dass Nutzer klar und verständlich über die Verarbeitung informiert werden, dass Daten nur für festgelegte Zwecke verwendet und so sparsam wie möglich erhoben werden. Sensible Daten wie Gesundheits- oder Bewegungsdaten erfordern spezielle Schutzmaßnahmen und oft eine ausdrückliche Einwilligung. Auch das Recht auf Löschung ist essenziell und im Metaverse technisch anspruchsvoll umzusetzen.

3.6.3 Prioritäre juristische Fragestellungen im Kontext Datenschutz

Wichtige Fragestellungen betreffen die Verantwortlichkeit bei dezentralen Strukturen, etwa wer bei Blockchain-Nutzung als Verantwortlicher gilt, sowie die Einhaltung der Betroffenenrechte wie Löschung und Portabilität in komplexen, grenzüberschreitenden Umgebungen. Auch die sichere Verarbeitung sensibler Daten, etwa aus biometrischen oder emotionalen Messungen, wirft erhebliche Fragen auf, insbesondere in Hinblick auf Missbrauch und Datenschutzfolgenabschätzungen.

3.6.4 Wichtigste rechtliche Risiken

Zu den Risiken zählen die Unsicherheit über Verantwortlichkeiten bei der Datenverarbeitung in dezentralen Strukturen, die erhöhte Gefahr von Datenmissbrauch durch umfassende Datenerfassung, und potenzielle Verstöße gegen das Recht auf Vergessenwerden durch irreversible Daten auf Blockchains. Weiterhin problematisch ist die mangelnde Transparenz vieler Systeme, die Nutzerrechte erschwert.

3.6.5 Best Practice

Gesetzeskonformes Handeln umfasst die Einholung spezifischer Einwilligungen für jede Datenverarbeitung, die Implementierung von Privacy-by-Design-Prinzipien und die transparente Kommunikation aller datenschutzrechtlichen Vorgänge. Unternehmen müssen zudem Datenschutzfolgenabschätzungen durchführen, wenn Risiken für Betroffene bestehen, und sicherstellen, dass personenbezogene Daten pseudonymisiert oder anonymisiert werden.

3.6.6 Worst Practice

Gesetzeswidrig sind die Sammlung personenbezogener Daten ohne Einwilligung, die Speicherung irreversibler Daten in Blockchains ohne Lösungsmechanismen und das Nicht-Einhalten von Betroffenenrechten wie Zugang oder Löschung. Ebenso ist die nicht autorisierte Nutzung sensibler Daten oder die Weitergabe an Dritte ohne spezifische Einwilligung ein klarer Verstoß gegen geltendes Recht.

3.7 Designrecht

3.7.1 Rechtsvorschriften im Rechtsgebiet

Die Rechtslage zum Designrecht im Metaverse basiert auf dem deutschen Designgesetz (DesignG) und der EU-Verordnung über Gemeinschaftsgeschmacksmuster (GGV). Diese schützen zweidimensionale und dreidimensionale Erscheinungsformen von Erzeugnissen, einschließlich virtueller Objekte wie Benutzeroberflächen oder NFTs, sofern sie neu sind und eine Eigenart besitzen. Die Eintragung eines Designs ist erforderlich, wobei nicht eingetragene Designs in der EU einen dreijährigen Schutz genießen. Die Vorschriften werden ergänzt durch internationale Abkommen wie die WIPO-Leitlinien, die jedoch oft an ihre Grenzen stoßen.

3.7.2 Geltende Grundprinzipien

Grundprinzipien des Designrechts umfassen die Schutzzfähigkeit neuer und eigenartiger Designs sowie die territoriale Begrenzung des Schutzes. Anders als im Markenrecht ist der Schutz unabhängig von der Art der Verwendung oder der Notwendigkeit einer Benutzung. Designs können sowohl physische als auch rein virtuelle Objekte umfassen, solange sie eine klare ästhetische Erscheinung haben. Dies schließt auch bewegte Designs ein, deren Registrierung jedoch technisch anspruchsvoll ist.

3.7.3 Prioritäre juristische Fragestellungen im Kontext Designrecht

Wichtige Fragestellungen im Metaverse betreffen die Eintragungsfähigkeit dynamischer Designs, da animierte Objekte derzeit nur eingeschränkt registrierbar sind. Zudem stellt sich die

Frage, wie das Territorialprinzip bei global verfügbaren Metaverse-Plattformen angewendet wird. Schließlich ist die Durchsetzung von Designrechten problematisch, insbesondere aufgrund der Anonymität in dezentralen Netzwerken wie Blockchains.

3.7.4 Wichtigste rechtliche Risiken

Zu den Risiken gehören die unklare Rechtsdurchsetzung bei anonymen Verletzern, etwa bei der Verwendung geschützter Designs durch unbekannte Akteure im Metaverse. Das Territorialprinzip kann dazu führen, dass Rechteinhaber Schwierigkeiten haben, ihre Ansprüche außerhalb ihrer Registrierungsgebiete geltend zu machen. Darüber hinaus besteht die Gefahr, dass dynamische Designs aufgrund technischer Hürden keinen umfassenden Schutz genießen.

3.7.5 Best Practice

Gesetzeskonform sind die Eintragung eines Designs gemäß den Anforderungen des DesignG, der GGV, die Einhaltung der vorgeschriebenen Rechte der Designer bei der Nutzung ihrer Werke sowie die transparente Lizenzierung und Nutzung geschützter Designs durch Dritte. Unternehmen können auch Mechanismen der Plattformen nutzen, um verletzende Inhalte zu melden.

3.7.6 Worst Practice

Gesetzeswidrig ist die Verwendung geschützter Designs ohne Zustimmung des Rechteinhabers, insbesondere wenn diese im Metaverse ohne Lizenz reproduziert werden. Die Manipulation oder unerlaubte Veränderung eines registrierten Designs sowie die Nutzung von dynamischen Designs ohne korrekte Darstellung und Eintragung stellen ebenfalls Verstöße dar. Schließlich ist auch die nicht deklarierte kommerzielle Nutzung fremder Designs unzulässig.

3.8 Digitale Identitäten

3.8.1 Rechtsvorschriften im Rechtsgebiet

Digitale Identitäten im Metaverse werden durch eine Vielzahl von Rechtsvorschriften geregelt. Zentrale Regelungen auf europäischer Ebene sind die eIDAS-Verordnung (VO EU Nr. 910/2014) und deren geplante Reform durch die eIDAS 2.0, die digitale Identifizierungsdienste standardisieren und eine europäische digitale Identitäts-Wallet einführen sollen. National gelten das Telemediengesetz (TMG) und das Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG), die pseudonyme und anonyme Nutzungen sowie Datenschutzaspekte regeln. Ergänzend kommen das Bürgerliche Gesetzbuch (BGB) für allgemeine vertragliche Regelungen und das Geldwäschegesetz (GwG) bei Transaktionen mit Identitätsnachweis zur Anwendung. In Bereichen

mit internationalem Bezug können weitere Vorschriften, wie der Digital Markets Act (DMA), relevant sein.

3.8.2 Geltende Grundprinzipien

Die Gestaltung und Nutzung digitaler Identitäten orientiert sich an den Prinzipien der Rechtmäßigkeit, Zweckbindung und Datenminimierung, wie sie in der DS-GVO festgelegt sind. Dabei ist besonders wichtig, dass die digitale Identität nur jene Informationen preisgibt, die für den jeweiligen Zweck erforderlich sind. Anonymität und Pseudonymität stehen im Vordergrund, um den Nutzern im Metaverse größtmögliche Privatsphäre zu gewährleisten. Gleichzeitig greift das Know-Your-Customer-Prinzip (KYC) in Fällen, in denen Identitätsprüfungen gesetzlich vorgeschrieben sind, wie bei Finanztransaktionen oder im Glücksspiel. Einheitliche Standards für digitale Identitäten, wie sie in der geplanten EUid-Wallet vorgesehen sind, sollen außerdem Interoperabilität und Sicherheit gewährleisten.

3.8.3 Prioritäre juristische Fragestellungen im Kontext digitaler Identitäten

Im Metaverse ergeben sich diverse Fragestellungen: Wie kann die Authentifizierung der Nutzer sicher, aber datenschutzfreundlich erfolgen? Ist die Nutzung von Pseudonymen ausreichend oder erfordert die Rechtsordnung in bestimmten Fällen Klarnamen? Welche Standards sind erforderlich, um Avatare über verschiedene Plattformen hinweg eindeutig zuzuordnen? Zudem stellt sich die Frage, wie der grenzüberschreitende Einsatz digitaler Identitäten reguliert wird, insbesondere bei international tätigen Plattformen. Auch die Frage, wie eine Identitätsprüfung durch technologische Verfahren wie Blockchain oder Videoidentifizierung rechtskonform gestaltet werden kann, ist von zentraler Bedeutung. Schließlich müssen Konflikte zwischen Datenschutz und Identitätsprüfungsanforderungen, beispielsweise im Finanzsektor, gelöst werden.

3.8.4 Wichtigste rechtliche Risiken

Zu den rechtlichen Risiken gehört die Verletzung von Datenschutz- und Datensicherheitsvorschriften, insbesondere bei der Speicherung und Weitergabe von Identitätsdaten. Ein weiteres Risiko besteht in der unzureichenden Authentifizierung, die Identitätsdiebstahl und Betrug ermöglicht. Die Fragmentierung des Marktes und das Fehlen einheitlicher Standards führen zu Interoperabilitätsproblemen und erschweren die Durchsetzung von Rechten. Ein Risiko stellt auch die unklare rechtliche Zuweisung von Verantwortlichkeiten dar, etwa wenn Plattformbetreiber die Identitätsprüfung delegieren. Technologische Schwachstellen in Blockchain- oder

Videoidentifikationssystemen können ebenfalls genutzt werden, um Sicherheitsvorkehrungen zu umgehen.

3.8.5 Best Practice

Gesetzeskonform ist die Nutzung digitaler Identitäten, wenn diese auf den Grundsätzen der Rechtmäßigkeit, Datenminimierung und Transparenz beruhen. Eine ordnungsgemäße Implementierung des KYC-Prinzips, etwa bei Finanztransaktionen, durch sichere Technologien wie Videoident oder Blockchain, ist erlaubt. Plattformbetreiber können Nutzern Anonymität gewähren, solange dies technisch möglich und rechtlich zulässig ist. Die Einhaltung einheitlicher Standards, wie sie in der eIDAS-Verordnung und künftig in der eIDAS 2.0 vorgesehen sind, ist ebenfalls gesetzeskonform. Die Bereitstellung von pseudonymisierten Identitäten und deren Verwaltung durch Nutzer selbst, wie im Konzept der Self-Sovereign Identity (SSI) vorgesehen, entspricht den geltenden Regelungen.

3.8.6 Worst Practice

Gesetzeswidrig ist jede Nutzung digitaler Identitäten, die gegen Datenschutzvorschriften verstößt, etwa die Verarbeitung sensibler Identitätsdaten ohne Rechtsgrundlage. Unzulässig ist auch die Durchsetzung einer Klarnamenpflicht, wenn dies gegen das TTDSG oder den Datenschutz verstößt. Ebenso problematisch sind unzureichende Sicherheitsmaßnahmen, die Identitätsdiebstahl oder Datenmissbrauch ermöglichen. Verstöße gegen das KYC-Prinzip, etwa durch eine unzureichende Prüfung der Identität bei Transaktionen, sind ebenfalls rechtswidrig. Schließlich ist die Bereitstellung digitaler Identitätsdienste ohne Berücksichtigung der geplanten eIDAS 2.0-Vorgaben und ohne Gewährleistung von Interoperabilität mit europäischen Standards unzulässig.

3.9 Finanzaufsichtsrecht

3.9.1 Rechtsvorschriften im Rechtsgebiet

Die Rechtslage zum Finanzaufsichtsrecht im Metaverse wird von bestehenden nationalen und EU-weiten Vorschriften bestimmt. In Deutschland greifen das Zahlungsdiensteaufsichtsgesetz (ZAG), das Kreditwesengesetz (KWG) und das Wertpapierinstitutsgesetz (WpIG), die Anforderungen für Zahlungsdienste, Kreditinstitute und Finanzdienstleister regeln. EU-weit gelten zusätzliche Bestimmungen wie die MiCA-Verordnung für Kryptowerte und die PSD2-Richtlinie, die den Zahlungsverkehr betreffen. Diese Regularien decken Themen wie die Erlaubnispflicht, Eigenkapitalanforderungen und Risikomanagement ab.

3.9.2 Geltende Grundprinzipien

Grundprinzipien des Finanzaufsichtsrechts sind Transparenz, Verbraucherschutz und Marktintegrität. Anbieter von Finanzdienstleistungen im Metaverse müssen sicherstellen, dass ihre Tätigkeiten klar reguliert sind, um Vertrauen zu schaffen und Missbrauch zu verhindern. Das Territorialprinzip und die Zielmarkttheorie bestimmen die Anwendbarkeit nationaler Vorschriften auf grenzüberschreitende Dienstleistungen. Darüber hinaus erfordert die digitale Natur des Metaverse innovative Ansätze für Identifikation und Transaktionssicherheit.

3.9.3 Prioritäre juristische Fragestellungen im Kontext Finanzaufsichtsrecht

Drei zentrale Fragestellungen umfassen die Regulierung dezentraler Finanzsysteme (DeFi), wie Stablecoins und Smart Contracts, sowie die Einhaltung von Geldwäschevorschriften in anonymen Umgebungen. Zudem stellt sich die Frage, wie traditionelle Finanzaufsichtsregeln auf neuartige digitale Vermögenswerte und Plattformen angewandt werden können, insbesondere bei globalen Transaktionen und interoperablen Systemen.

3.9.4 Wichtigste rechtliche Risiken

Rechtliche Risiken im Metaverse betreffen vor allem unzureichende Kontrollmechanismen bei der Emission und dem Handel von Kryptotoken, die mögliche Anonymität und Intransparenz bei Finanztransaktionen sowie die Gefahr von Verstößen gegen geldwäscherechtliche Vorschriften. Auch das Fehlen klarer Haftungsregelungen bei dezentralisierten Plattformen birgt erhebliche rechtliche Unsicherheiten.

3.9.5 Best Practice

Gesetzeskonform sind die Beantragung einer Lizenz für Finanzdienstleistungen gemäß den Vorgaben der BaFin, die Einhaltung von Geldwäschevorschriften durch KYC-Verfahren sowie die Registrierung und Dokumentation von Transaktionen nach den Anforderungen von MiCA und ZAG. Unternehmen können durch Compliance-Maßnahmen rechtliche Sicherheit gewährleisten.

3.9.6 Worst Practice

Gesetzeswidrig sind hingegen die Emission von Kryptowerten oder Stablecoins ohne die erforderliche Genehmigung, die Umgehung von Geldwäschevorschriften durch anonyme Transaktionen sowie die Irreführung von Nutzern durch falsche Angaben zu finanziellen Produkten. Verstöße gegen diese Vorschriften können zu erheblichen Sanktionen führen.

3.10 Finanztransaktionen

3.10.1 Rechtsvorschriften im Rechtsgebiet

Die Rechtslage zu Finanztransaktionen im Metaverse wird stark von bestehenden Regelungen wie dem Zahlungsdiensteaufsichtsgesetz (ZAG), der MiCA-Verordnung und der EU-Geldwäscherichtlinie geprägt. Insbesondere Kryptowährungen und NFTs spielen im Metaverse eine zentrale Rolle, wobei ihre Nutzung oft als E-Geld oder Finanzinstrument reguliert ist. Zusätzlich gelten je nach Transaktionsart Vorschriften des Kreditwesengesetzes (KWG) oder des Wertpapierinstitutsgesetzes (WpIG), wenn Finanzdienstleistungen im Metaverse erbracht werden.

3.10.2 Geltende Grundprinzipien

Grundprinzipien im Finanztransaktionsrecht umfassen Transparenz, Nachverfolgbarkeit und Sicherheit. Diese Prinzipien sollen den Schutz von Verbrauchern gewährleisten und illegale Aktivitäten wie Geldwäsche oder Terrorismusfinanzierung verhindern. Zudem müssen Finanzdienstleister eine starke Kundenauthentifizierung sowie Datensicherheitsmaßnahmen umsetzen, um die Integrität der Transaktionen sicherzustellen. Das Territorialprinzip der Regulierung bleibt ein zentraler Punkt, auch bei globalen Plattformen.

3.10.3 Prioritäre juristische Fragestellungen im Kontext Finanztransaktionen

Die wichtigsten Fragestellungen betreffen die rechtliche Einordnung von Kryptowährungen und NFTs, die Sicherstellung von Geldwäscheprävention bei dezentralen Transaktionen und die Einhaltung internationaler Regularien bei grenzüberschreitenden Finanzaktivitäten. Ebenso ist die Interoperabilität zwischen Plattformen und die technische Integration von Zahlungsdiensten eine bedeutende Herausforderung.

3.10.4 Wichtigste rechtliche Risiken

Zu den rechtlichen Risiken gehören die unsichere rechtliche Einordnung von virtuellen Währungen, insbesondere bei der Definition als E-Geld oder Finanzinstrument, sowie die mangelnde Nachverfolgbarkeit von Transaktionen, was Geldwäsche und Betrug begünstigen kann. Zusätzlich bestehen Haftungsrisiken bei der Nutzung dezentraler Technologien, wenn technische oder sicherheitsrelevante Probleme auftreten.

3.10.5 Best Practice

Gesetzeskonform ist die Einhaltung der Vorgaben für die Erlaubnispflicht bei der Ausgabe von E-Geld gemäß ZAG, die Implementierung robuster KYC-Verfahren zur Geldwäscheprävention

und die transparente Kommunikation über Transaktionskosten und Risiken. Auch die Nutzung genehmigter Plattformen und Technologien kann rechtliche Sicherheit bieten.

3.10.6 Worst Practice

Gesetzeswidrig sind die Durchführung von Finanztransaktionen ohne die erforderliche Lizenz, die Verletzung von Geldwäschevorschriften durch fehlende Identitätsprüfung und die Irreführung von Nutzern durch unklare oder fehlerhafte Informationen zu Kosten oder Risiken. Ebenso problematisch ist die Manipulation oder der Missbrauch von Zahlungssystemen, beispielsweise durch betrügerische Aktivitäten.

3.11 Gaming und eSport

3.11.1 Rechtsvorschriften im Rechtsgebiet

Im Bereich Gaming und eSport im Metaverse gelten diverse Rechtsvorschriften, die sowohl nationale als auch internationale Dimensionen abdecken. National sind dies das Jugendschutzgesetz (JuSchG), der Glücksspielstaatsvertrag (GlüStV) sowie das Bürgerliche Gesetzbuch (BGB), insbesondere in Bezug auf Verträge über digitale Inhalte. Ergänzend greifen datenschutzrechtliche Bestimmungen wie die Datenschutz-Grundverordnung (DS-GVO). Auf europäischer Ebene haben die Markets in Crypto-Assets Regulation (MiCA) und die eIDAS-Verordnung Bedeutung, insbesondere wenn es um die Authentifizierung und den Handel mit NFTs oder In-Game-Assets geht. Bei internationalen Aspekten spielen Regelungen zur grenzüberschreitenden Nutzung digitaler Inhalte und Plattformbetreiberpflichten eine Rolle.

3.11.2 Geltende Grundprinzipien

Zentrale Prinzipien im Gaming- und eSport-Recht sind der Schutz von Verbrauchern und Jugendlichen sowie die Gewährleistung von Fairness und Transparenz. Diese Prinzipien manifestieren sich in klaren Regelungen zu In-Game-Käufen, Lootboxen und Datenschutz. Das Prinzip der Zweckbindung ist in Bezug auf Datenverarbeitung wichtig, während das Know-Your-Customer-Prinzip (KYC) bei Plattformen mit Finanztransaktionen zentral ist. Für die Anerkennung des eSports als Sport sind die Prinzipien der Chancengleichheit, der Fairness und des Wettbewerbs entscheidend. Schließlich spielt das Jugendschutzrecht eine bedeutende Rolle bei der Begrenzung jugendgefährdender Inhalte.

3.11.3 Prioritäre juristische Fragestellungen im Kontext Gaming und eSport

Im Metaverse treten neue Fragestellungen auf: Wie werden Lootboxen rechtlich bewertet, insbesondere im Hinblick auf Glücksspielregelungen? Welche Anforderungen bestehen an die

Authentifizierung und den Schutz minderjähriger Nutzer? Wie können digitale Assets wie NFTs und Kryptowährungen in Spielen rechtssicher gehandelt werden? Im eSport stellt sich die Frage, ob die Kriterien für eine Anerkennung als Sport, etwa die motorische Aktivität, durch die Nutzung von VR-Technologien erfüllt werden können. Darüber hinaus ist zu klären, welche rechtlichen Rahmenbedingungen für „Play-to-Earn“-Spiele gelten und wie Plattformbetreiber ihre Pflichten erfüllen können.

3.11.4 Wichtigste rechtliche Risiken

Ein großes Risiko ist die unklare Abgrenzung zwischen Gaming und Gambling, insbesondere bei Lootboxen. Dies kann zu regulatorischen und rechtlichen Unsicherheiten führen. Weitere Risiken betreffen den Datenschutz, insbesondere durch die umfassende Datensammlung und den Handel mit NFTs und Kryptowährungen. Die grenzüberschreitende Natur des Metaverse erschwert die Durchsetzung nationaler Vorschriften. Technologische Risiken, etwa Sicherheitslücken in Blockchain-Systemen, können zu Missbrauch und Rechtsverletzungen führen. Plattformbetreiber können für unzureichende Kontrollmechanismen und Verstöße gegen das Jugendschutzrecht haftbar gemacht werden.

3.11.5 Best Practice

Gesetzeskonform ist die Nutzung von digitalen Assets und In-Game-Mechanismen, wenn sie den bestehenden regulatorischen Anforderungen entsprechen. Dazu gehört die Bereitstellung transparenter Informationen über Lootboxen und In-Game-Käufe. Plattformen müssen sicherstellen, dass jugendgefährdende Inhalte durch technische Maßnahmen wie Altersverifikationen begrenzt werden. Auch die Einhaltung der Datenschutzbestimmungen, insbesondere durch die pseudonymisierte Verarbeitung von Nutzerdaten, ist zentral. Anbieter von „Play-to-Earn“-Spiele können gesetzeskonform agieren, wenn sie klare Geschäftsbedingungen formulieren und finanzrechtliche Regelungen beachten.

3.11.6 Worst Practice

Gesetzeswidrig sind Handlungen wie der Vertrieb von Lootboxen ohne Beachtung glücksspielrechtlicher Vorschriften. Verstöße gegen Datenschutzbestimmungen, etwa die unbefugte Weitergabe personenbezogener Daten, sind ebenfalls unzulässig. Das Angebot jugendgefährdender Inhalte ohne geeignete Schutzmaßnahmen verstößt gegen das JuSchG. Plattformbetreiber, die keine ausreichenden Sicherheitsmaßnahmen gegen Betrug oder Datenmissbrauch

implementieren, handeln ebenfalls rechtswidrig. Schließlich ist die Nutzung von „Play-to-Earn“-Mechanismen ohne Berücksichtigung der Finanzaufsichtsgesetze unzulässig.

3.12 Gesellschaftsrecht

3.12.1 Rechtsvorschriften im Rechtsgebiet

Die Rechtslage zum Gesellschaftsrecht im Metaverse orientiert sich an bestehenden Vorschriften des deutschen und internationalen Gesellschaftsrechts, wobei sich spezifische Herausforderungen durch die Einführung dezentraler autonomer Organisationen (DAOs) ergeben. DAOs, die oft als Organisationseinheiten im Metaverse fungieren, sind rechtlich schwer einzuordnen, da sie weder über einen festen Verwaltungssitz noch über eine zentrale Geschäftsleitung verfügen. In Deutschland können sie, abhängig von ihrer Ausgestaltung, als Gesellschaft bürgerlichen Rechts (GbR) oder offene Handelsgesellschaft (OHG) angesehen werden, was persönliche Haftung der Mitglieder nach sich zieht.

3.12.2 Geltende Grundprinzipien

Grundprinzipien des Gesellschaftsrechts im Metaverse umfassen die Autonomie der Organisation, die durch Smart Contracts verwaltet wird, sowie die Verteilung von Entscheidungsbefugnissen auf alle Token-Inhaber. Die Rechtsverhältnisse werden durch programmierte Regeln bestimmt, was neue Fragen zur Haftung und rechtlichen Qualifikation aufwirft. Das Territorialprinzip und die Wahl des anwendbaren Rechts sind zentrale Herausforderungen, insbesondere bei grenzüberschreitenden Konstellationen.

3.12.3 Prioritäre juristische Fragestellungen im Kontext Gesellschaftsrecht

Wichtige Fragestellungen betreffen die rechtliche Einordnung und Registrierung von DAOs, die Haftung der Mitglieder bei fehlerhaften oder nicht genehmigten Aktionen sowie die Anwendung des deutschen Gesellschaftsrechts auf virtuelle Organisationen. Die dezentrale Struktur erschwert die klare Zuordnung von Verantwortlichkeiten, was neue gesetzliche Regelungen erfordert.

3.12.4 Wichtigste rechtliche Risiken

Rechtliche Risiken bestehen in der unklaren Haftungsregelung für DAOs, der Gefahr von Manipulationen durch zentrale Einflussnahmen trotz des dezentralen Ansatzes und der fehlenden rechtlichen Absicherung von Smart Contracts. Hinzu kommen mögliche Konflikte durch internationale Regelungslücken und fehlende Standards.

3.12.5 Best Practice

Gesetzeskonforme Handlungen umfassen die transparente Kommunikation über DAO-Regeln, die ordnungsgemäße Registrierung einer DAO in Staaten, die solche Strukturen anerkennen, und die Durchführung von Abstimmungen gemäß den programmatischen Vorgaben der Smart Contracts. Diese Schritte minimieren rechtliche Unsicherheiten.

3.12.6 Worst Practice

Gesetzeswidrig ist die Gründung einer DAO ohne Beachtung der geltenden Anforderungen an Rechtsformen oder die Nutzung von Smart Contracts für illegale Transaktionen. Ebenso ist die vorsätzliche Umgehung von Transparenzvorschriften oder die Missachtung der Rechte von Mitgliedern durch manipulative Abstimmungsprozesse unzulässig. Dies kann zu rechtlichen Konsequenzen für die Beteiligten führen.

3.13 Glücksspielrecht

3.13.1 Rechtsvorschriften im Rechtsgebiet

Das Glücksspielrecht im Metaverse wird von bestehenden Regelungen wie dem Glücksspielstaatsvertrag (GlüStV) dominiert, ergänzt durch Landesausführungsgesetze und internationale Abkommen. Der GlüStV regelt insbesondere die Veranstaltung, Vermittlung und Bewerbung von Glücksspielen. Weiterhin sind spezifische Regelungen wie das Strafgesetzbuch (StGB, §§ 284 ff.), das Geldwäschegesetz (GwG), sowie Bestimmungen zu Online-Zahlungen im Zahlungsdiensteaufsichtsgesetz (ZAG) von Relevanz. Auf europäischer Ebene können weitere Vorgaben durch die geplante EU-KI-Verordnung und Datenschutzvorschriften (DS-GVO) greifen. Die Einordnung von Glücksspielen im Metaverse stellt jedoch eine Herausforderung dar, da das Metaverse eine neue Dimension zwischen terrestrischen und Internet-Glücksspielen schafft.

3.13.2 Geltende Grundprinzipien

Das Glücksspielrecht basiert auf den Prinzipien des Spieler- und Jugendschutzes, der Vermeidung von Spielsucht sowie der Sicherstellung eines fairen und transparenten Marktes. Der GlüStV verfolgt ein präventives Verbot mit Erlaubnisvorbehalt: Glücksspiel ist grundsätzlich verboten, es sei denn, es wurde explizit genehmigt. Ein weiteres Prinzip ist die Kanalisierung: Durch klare Regulierung soll der Schwarzmarkt eingedämmt werden. Besondere Anforderungen gelten für die Identifizierung der Teilnehmer sowie für die Überwachung und Begrenzung von Spielgewohnheiten, um verantwortungsvolles Spielen zu fördern.

3.13.3 Prioritäre juristische Fragestellungen im Kontext Glücksspielrecht

Die Hauptfragen betreffen die rechtliche Einordnung von Glücksspielen im Metaverse. Dazu gehört, ob diese als „Internetglücksspiel“ oder als eigenständige Kategorie gelten. Die Möglichkeit zur vollständigen Anonymität im Metaverse wirft Fragen zur Identifizierung von Spielern und Anbietern auf, insbesondere im Hinblick auf den Jugendschutz und Geldwäscheprävention. Auch die technische Umsetzbarkeit bestehender Vorschriften, etwa zur Spielersperrdatei oder Verlustlimits, stellt eine Herausforderung dar. Zusätzlich gilt es zu klären, wie KI-basierte Werbung und neue Spielformen wie virtuelle Pferderennen oder Avatar-Wettkämpfe reguliert werden sollen.

3.13.4 Wichtigste rechtliche Risiken

Zentrale Risiken umfassen die Entstehung eines unregulierten Schwarzmarktes, der durch die Anonymität und internationale Struktur des Metaverse begünstigt wird. Die fehlende Anpassung bestehender Vorschriften birgt die Gefahr, dass wichtige Schutzmechanismen, wie Verlustlimits oder der Ausschluss minderjähriger Spieler, nicht greifen. Technologische Schwächen, etwa in der Zahlungsabwicklung mit Kryptowährungen, können zu Compliance-Problemen führen. Weiterhin besteht die Gefahr von Missbrauch durch KI-gestützte Werbung, die gezielt besonders vulnerable Spieler anspricht, sowie rechtliche Unsicherheiten bei der Einordnung neuer Spielformen.

3.13.5 Best Practice

Gesetzeskonform sind Handlungen, die den bestehenden regulatorischen Anforderungen entsprechen. Dazu gehört die Beantragung von Genehmigungen für erlaubnisfähige Glücksspiele gemäß GlüStV und die Implementierung von Mechanismen zur Spieleridentifikation und Altersverifikation. Transparente Werbung, die keine vulnerable Zielgruppen anspricht, sowie die Einhaltung von Vorschriften zum Zahlungsverkehr sind ebenfalls rechtmäßig. Betreiber sollten Maßnahmen ergreifen, um bestehende Schutzmechanismen, wie die Spielersperrdatei und Verlustlimits, auch im Metaverse anzuwenden.

3.13.6 Worst Practice

Gesetzeswidrig sind insbesondere die Veranstaltung und Vermittlung von Glücksspielen ohne Genehmigung. Ebenso unzulässig ist die Nutzung von Kryptowährungen für Glücksspiele, solange diese nicht den Anforderungen des ZAG genügen. Verstöße gegen Werbungsvorschriften, etwa durch direkte Ansprache Minderjähriger oder die Verwendung von KI-Avataren ohne

Kennzeichnung, sind ebenfalls verboten. Schließlich ist auch die Missachtung bestehender Schutzmaßnahmen, wie der Spielersperre oder der Verlustlimits, rechtswidrig.

3.14 Handelsrecht

3.14.1 Rechtsvorschriften im Rechtsgebiet

Im Metaverse finden die allgemeinen Regelungen des deutschen Handels- und Vertragsrechts Anwendung. Dazu zählen das Bürgerliche Gesetzbuch (BGB), insbesondere die Vorschriften zu Fernabsatzverträgen (§§ 312c ff. BGB) und digitale Inhalte (§§ 327 ff. BGB), sowie das Handelsgesetzbuch (HGB). Für digitale Güter wie NFTs oder Token ist die Einordnung als „digitale Inhalte“ gemäß § 327 BGB zentral. Auf europäischer Ebene sind die Markets in Crypto-Assets Regulation (MiCA) und die eIDAS-Verordnung relevant, die den Handel und die Sicherheit digitaler Vermögenswerte regeln. Weitere Regelungen wie die Richtlinie über Verbraucherschutz in der EU (Consumer Rights Directive) greifen ebenfalls. Die Einhaltung steuerlicher Vorschriften und Bestimmungen zum Datenschutz (DS-GVO) ist ebenfalls essenziell.

3.14.2 Geltende Grundprinzipien

Das Handelsrecht basiert auf den Grundprinzipien der Vertragsfreiheit und Rechtssicherheit. Im Kontext des Metaverse wird dies durch die Regeln zu Fernabsatzverträgen ergänzt, den Verbrauchern umfangreiche Rechte einräumen, etwa das Widerrufsrecht. Das Prinzip der Transparenz ist für den Handel im Metaverse von besonderer Bedeutung, insbesondere bei der Bereitstellung von Informationen über die Beschaffenheit und Nutzung digitaler Güter. Zusätzlich gilt das Prinzip der Verhältnismäßigkeit, um die Interessen von Unternehmen und Verbrauchern auszugleichen, und die Technologieneutralität, um Innovationen wie NFTs oder Smart Contracts in bestehende rechtliche Strukturen einzubinden.

3.14.3 Prioritäre juristische Fragestellungen im Kontext Handelsrecht

Im Metaverse entstehen neue Fragestellungen: Wie werden digitale Güter wie NFTs oder virtuelle Dienstleistungen rechtlich eingestuft? Handelt es sich hierbei um einen klassischen Kaufvertrag, der Eigentum überträgt, oder um Lizenzverträge, die Nutzungsrechte einräumen? Besonders relevant ist die Frage, wie Gewährleistungsrechte und das Widerrufsrecht bei rein virtuellen Gütern ausgestaltet sind. Zudem stellt sich die Herausforderung, wie steuerliche und aufsichtsrechtliche Pflichten, etwa im Hinblick auf Token als potenziell regulierte Finanzprodukte, erfüllt werden können. Auch die Verknüpfung physischer und digitaler

Vertragsgegenstände, beispielsweise beim Erwerb eines virtuellen und physischen Produkts, bedarf rechtlicher Klarheit.

3.14.4 Wichtigste rechtliche Risiken

Die rechtlichen Risiken umfassen Unsicherheiten bei der Einordnung virtueller Güter, insbesondere NFTs, die je nach ihrer Funktion als Finanzinstrumente reguliert werden könnten. Fehlende Transparenz bei Vertragsabschlüssen oder unzureichende Informationen über digitale Produkte können zu Verbraucherschutzverstößen führen. Ein weiteres Risiko besteht in der mangelnden Absicherung von Nutzungsrechten, etwa wenn eine Plattform den Zugang zu erworbenen digitalen Gütern beschränkt oder einstellt. Zudem können Streitigkeiten über das anwendbare Recht auftreten, da das Metaverse international und dezentral organisiert ist. Technologische Schwachstellen, wie unsichere Smart Contracts, können ebenfalls rechtliche Probleme verursachen.

3.14.5 Best Practice

Gesetzeskonform ist der Handel mit digitalen und physischen Gütern, sofern die gesetzlichen Anforderungen eingehalten werden. Dazu gehören die Bereitstellung klarer Vertragsbedingungen, die Einhaltung von Widerrufsrechten bei Verbraucherverträgen und die korrekte Ausgestaltung von Lizenzbedingungen bei digitalen Gütern. Unternehmen müssen sicherstellen, dass sie den Verbraucherschutz wahren, beispielsweise durch klare Angaben zu den Eigenschaften und Nutzungsrechten von NFTs. Auch die Implementierung von Smart Contracts kann rechtmäßig sein, wenn diese den Anforderungen an Transparenz und Sicherheit entsprechen.

3.14.6 Worst Practice

Gesetzeswidrig sind Handlungen, die gegen Verbraucherschutzrechte verstoßen, etwa die Nichtbereitstellung von Informationen über die Beschaffenheit und Nutzung von digitalen Gütern. Unzulässig ist es, digitale Produkte anzubieten, die gegen die Vorgaben zur Gewährleistung oder das Widerrufsrecht verstoßen. Ebenso problematisch sind intransparente Vertragsbedingungen oder die unzureichende Absicherung von Nutzungsrechten, die zu Benachteiligungen von Verbrauchern führen. Verstöße gegen steuerliche oder aufsichtsrechtliche Pflichten, etwa bei der Emission von Token ohne Einhaltung der MiCA-Vorgaben, sind ebenfalls rechtswidrig.

3.15 Intellectual Property / Geistiges Eigentum

3.15.1 Rechtsvorschriften im Rechtsgebiet

Die Rechtslage zu geistigem Eigentum im Metaverse basiert auf bestehenden Normen des Urheberrechts, Markenrechts und gewerblicher Schutzrechte, ergänzt durch internationale Regelungen wie das TRIPS-Abkommen und das EU-Recht. In Deutschland regeln das Urheberrechtsgesetz (UrhG) und das Markengesetz (MarkenG) die wesentlichen Aspekte, während auf EU-Ebene die Verordnung über Gemeinschaftsmarken und das Designrecht anwendbar sind. Diese Vorschriften gelten auch für Werke und Marken, die ins Metaverse übertragen werden..

3.15.2 Geltende Grundprinzipien

Grundprinzipien im Bereich des geistigen Eigentums umfassen das Territorialitätsprinzip, wonach Schutzrechte auf die jeweilige Jurisdiktion beschränkt sind, sowie das Erfordernis der Originalität und Schöpfungshöhe für den Schutz durch das Urheberrecht. Im Metaverse ist eine markenmäßige Nutzung erforderlich, um den Schutz geltend zu machen, wobei der kommerzielle Effekt und die Zielrichtung entscheidend sind. Rechteinhaber müssen zudem aktiv gegen Verstöße vorgehen.

3.15.3 Prioritäre juristische Fragestellungen im Kontext Intellectual Property

Wichtige Fragestellungen betreffen die Durchsetzung territorial begrenzter Schutzrechte in einer global zugänglichen virtuellen Welt, die Frage, ob digitale Designs und Marken spezifische Anpassungen in bestehenden Rechtsvorschriften erfordern, und die Verantwortlichkeit in dezentralen Metaverse-Strukturen, bei denen kein zentraler Betreiber existiert. Dies betrifft insbesondere die Rolle der Nutzer als potenziell Verantwortliche für Rechtsverletzungen.

3.15.4 Wichtigste rechtliche Risiken

Rechtliche Risiken ergeben sich aus der schwierigen Durchsetzung von Schutzrechten in einem dezentralen Metaverse, der möglichen Umgehung territorialer Grenzen durch Plattformbetreiber oder Nutzer sowie aus dem Fehlen technischer Mechanismen, die eine effektive Sperrung oder Unterbindung von Rechtsverletzungen gewährleisten. Insbesondere die Verletzung von Urheberrechten durch nicht genehmigte Kopien oder Modifikationen stellt eine häufige Herausforderung dar.

3.15.5 Best Practice

Gesetzeskonform ist die Nutzung von urheberrechtlich geschützten Inhalten mit ausdrücklicher Genehmigung der Rechteinhaber, die Eintragung von Marken und Designs für spezifische

digitale Anwendungen und die Einhaltung der Anforderungen für den rechtmäßigen Einsatz von geschützten Werken oder Marken im Metaverse. Dies umfasst auch die transparente Lizenzierung und angemessene Vergütung.

3.15.6 Worst Practice

Gesetzeswidrig sind hingegen die unerlaubte Nutzung oder Vervielfältigung geschützter Werke, die Nachahmung oder Verletzung eingetragener Marken und die Umgehung technischer Schutzmaßnahmen, wie Uploadfilter oder DRM-Systeme. Ebenfalls unzulässig ist die vorsätzliche Manipulation von geschützten Inhalten oder Designs, um den Ursprung zu verschleiern und Rechteinhaber zu täuschen.

3.16 Internationales Privatrecht

3.16.1 Rechtsvorschriften im Rechtsgebiet

Im internationalen Privatrecht für das Metaverse gelten zahlreiche Regelwerke, darunter die Rom-I-VO für vertragliche Schuldverhältnisse und die Rom-II-VO für außervertragliche Ansprüche. Für spezifische Vertragsarten, wie den Kauf von Waren, ist das UN-Kaufrecht (CISG) maßgeblich. Die Bestimmung der Zuständigkeit richtet sich häufig nach der Brüssel-Ia-Verordnung (EU-Verordnung Nr. 1215/2012) und ggf. nach dem Haager Gerichtsstandsübereinkommen. National kommen ergänzend die Regelungen des EGBGB zur Anwendung, insbesondere bei der Rechtswahl und bei Verbraucherverträgen. Im Metaverse erlangt das Kollisionsrecht besondere Bedeutung, da die meisten Interaktionen und Transaktionen einen grenzüberschreitenden Charakter haben.

3.16.2 Geltende Grundprinzipien

Das internationale Privatrecht basiert auf den Prinzipien der Parteiautonomie und der engsten Verbindung. Die Parteiautonomie erlaubt es den Vertragspartnern, das anwendbare Recht im Voraus zu bestimmen. Gleichzeitig wird durch objektive Anknüpfungsregeln, wie sie in der Rom-I-VO oder der Rom-II-VO formuliert sind, eine sachgerechte Zuordnung des anwendbaren Rechts gewährleistet. Weitere Prinzipien sind der Schutz schwächerer Parteien, wie Verbraucher oder Arbeitnehmer, sowie die Vorhersehbarkeit und Rechtssicherheit im internationalen Handel. Besondere Bedeutung hat der Grundsatz der gegenseitigen Anerkennung, der in der EU durch harmonisierte Vorschriften gestärkt wird.

3.16.3 Prioritäre juristische Fragestellungen im Kontext internationales Privatrecht

Im Metaverse ergeben sich zahlreiche neue Fragestellungen: Wie wird das anwendbare Recht bestimmt, wenn die Parteien anonym oder über Avatare agieren? Welche Rechtsordnung gilt bei grenzüberschreitenden Transaktionen, insbesondere wenn Kryptowährungen oder NFTs im Spiel sind? Wie wird der Schutz von Verbrauchern gewährleistet, wenn Verträge mit Plattformbetreibern oder anderen Nutzern geschlossen werden? Ein weiteres Problem ist die Bestimmung der Gerichtszuständigkeit, insbesondere wenn die Interaktionen vollständig virtuell erfolgen und keine physische Adresse vorliegt. Auch die Frage, wie man Datenschutzregelungen und Verbraucherschutz im globalen Kontext effektiv durchsetzt, ist zentral.

3.16.4 Wichtigste rechtliche Risiken

Die größten Risiken liegen in der Unbestimmtheit des anwendbaren Rechts und der Schwierigkeiten bei der Durchsetzung von Ansprüchen. Die Anonymität der Nutzer kann dazu führen, dass weder Gerichtsstand noch anwendbares Recht leicht ermittelbar sind. Ein weiteres Risiko besteht in der Möglichkeit, dass Rechtswahlklauseln in den AGB großer Plattformbetreiber den Verbraucherschutz aushöhlen. Auch die Nutzung von Smart Contracts und Blockchain-Technologien kann rechtliche Probleme aufwerfen, etwa wenn automatisierte Prozesse geltendes Recht verletzen oder bei Konflikten keine klare Lösung vorliegt. Schließlich birgt die mangelnde Harmonisierung internationaler Vorschriften ein erhebliches Risiko für die Rechtssicherheit.

3.16.5 Best Practice

Gesetzeskonform ist die Nutzung von Rechtswahlklauseln in Verträgen, sofern diese den Verbraucherschutz beachten und klar kommuniziert werden. Ebenso ist die Anwendung der Rom-I-VO und der Rom-II-VO auf grenzüberschreitende Verträge und außervertragliche Schuldverhältnisse gesetzeskonform. Plattformbetreiber, die transparente AGB bereitstellen und die Verbraucherrechte gemäß den europäischen Vorschriften respektieren, handeln rechtmäßig. Die Implementierung von Smart Contracts kann ebenfalls rechtlich unproblematisch sein, wenn diese den gesetzlichen Anforderungen genügen und Konfliktlösungsmechanismen vorsehen.

3.16.6 Worst Practice

Gesetzeswidrig sind Handlungen wie die Missachtung zwingender Verbraucherschutzvorschriften oder die Verwendung intransparenter Rechtswahlklauseln, die den Verbraucher über seine Rechte täuschen. Ebenso unzulässig ist die Vernachlässigung von Sorgfaltspflichten bei der Identifikation der Vertragspartner, insbesondere wenn dies zu Rechtsunsicherheit führt.

Verstöße gegen internationale Kollisionsnormen, wie die Rom-Verordnungen, sind ebenfalls problematisch. Schließlich können automatisierte Vertragsprozesse, die grundlegende rechtliche Anforderungen nicht berücksichtigen, zu Rechtsverstößen führen.

3.17 Lauterkeitsrecht

3.17.1 Rechtsvorschriften im Rechtsgebiet

Die Rechtslage zum Lauterkeitsrecht im Metaverse wird durch das Gesetz gegen unlauteren Wettbewerb (UWG) bestimmt, das auch auf virtuelle Umgebungen Anwendung findet. § 3 UWG verbietet unlautere geschäftliche Handlungen, während § 4 Nr. 4 UWG gezielte Mitbewerberbehinderungen untersagt. Ergänzend gilt die Rechtsprechung zu Werbeformen wie standortbezogener Werbung, die durch AR-Technologien im Metaverse an Bedeutung gewinnt und spezifische Herausforderungen birgt.

3.17.2 Geltende Grundprinzipien

Grundprinzipien umfassen den Schutz vor unlauterem Wettbewerb, die Sicherstellung fairer Marktpraktiken und die Vermeidung von Irreführung und Belästigung. Im Metaverse wird dies auf kontextabhängige Werbung übertragen, bei der Plattformbetreiber darauf achten müssen, Mitbewerber nicht gezielt zu behindern. Auch die sich verändernde Verkehrsanschauung spielt bei der Bewertung von Wettbewerbspraktiken eine Rolle.

3.17.3 Prioritäre juristische Fragestellungen im Kontext Wettbewerbs-, Kartell- und Lauterkeitsrecht

Zentrale Fragestellungen betreffen die Zulässigkeit von kontextabhängiger AR-Werbung, die Abgrenzung zwischen zulässiger Werbung und unlauterem Abwerben sowie die Verantwortung von Plattformbetreibern für rechtswidrige Handlungen Dritter. Insbesondere bei globalen Plattformen entstehen durch unterschiedliche Rechtsauffassungen rechtliche Unsicherheiten.

3.17.4 Wichtigste rechtliche Risiken

Rechtliche Risiken bestehen in der gezielten Behinderung von Mitbewerbern durch standort- oder blickwinkelabhängige Werbung, der Irreführung von Verbrauchern durch unklare Werbepraktiken und der möglichen Haftung von Plattformbetreibern für unlautere Handlungen auf ihren Plattformen. Diese Risiken können zu Abmahnungen oder rechtlichen Sanktionen führen.

3.17.5 Best Practice

Gesetzeskonform sind transparente Werbemaßnahmen, die keine Mitbewerber behindern, sowie die Einhaltung von Informationspflichten und Kennzeichnungsvorschriften. Auch die Nutzung von AR-Technologien ist erlaubt, wenn sie fair und ohne Manipulation eingesetzt wird. Plattformbetreiber sollten klare Richtlinien für Nutzer erstellen.

3.17.6 Worst Practice

Gesetzeswidrig sind die gezielte Behinderung von Mitbewerbern, etwa durch verdeckte Einflussnahme auf Kaufentscheidungen, die bewusste Irreführung von Verbrauchern und das Verschleiern von Werbezwecken. Solche Praktiken können rechtliche Konsequenzen nach sich ziehen und das Vertrauen der Nutzer beeinträchtigen. Rechtliche Expertise ist bei neuen Technologien wie AR unerlässlich, um unlautere Praktiken zu vermeiden.

3.18 Lieferkettengesetz

3.18.1 Rechtsvorschriften im Rechtsgebiet

Das Lieferkettensorgfaltspflichtengesetz (LkSG), das am 1. Januar 2023 in Kraft getreten ist, regelt die menschenrechtlichen und umweltbezogenen Sorgfaltspflichten für bestimmte Unternehmen in Deutschland. Es betrifft inländische Unternehmen mit mindestens 3.000 Mitarbeitern (ab 2024: 1.000 Mitarbeitern) sowie ausländische Unternehmen mit Zweigniederlassungen in Deutschland, die diese Schwellenwerte erfüllen. Das LkSG umfasst alle Schritte einer Lieferkette, vom Rohstoffabbau bis zur Lieferung an den Endkunden. Im Kontext des Metaverse greifen auch allgemeine zivilrechtliche Regelungen (z. B. §§ 823 ff. BGB) und internationale Rechtsvorschriften, die auf Lieferketten in virtuellen Umgebungen anwendbar sind.

3.18.2 Geltende Grundprinzipien

Das LkSG basiert auf den Prinzipien der Prävention und Risikominimierung im Hinblick auf menschenrechtliche und umweltbezogene Gefahren. Unternehmen müssen angemessene Maßnahmen ergreifen, um Risiken in ihrer Lieferkette zu identifizieren, zu minimieren und im besten Fall zu vermeiden. Diese Verpflichtungen erstrecken sich nicht nur auf den eigenen Geschäftsbereich, sondern auch auf unmittelbare und mittelbare Zulieferer. Weitere Prinzipien sind die Angemessenheit und Bemühungspflichten, die sicherstellen, dass Unternehmen ihre Sorgfaltspflichten im Rahmen ihrer Möglichkeiten erfüllen.

3.18.3 Prioritäre juristische Fragestellungen im Kontext Lieferkettengesetz

Im Metaverse ergeben sich komplexe Fragestellungen, insbesondere ob und wie digitale Güter wie NFTs oder Dienstleistungen in die Definition einer Lieferkette nach § 2 Abs. 5 LkSG fallen. Ist die Erstellung oder der Handel mit NFTs als Teil einer Lieferkette zu verstehen? Wie werden die Verantwortlichkeiten von Plattformbetreibern oder dezentralen autonomen Organisationen (DAOs) rechtlich eingeordnet? Zudem stellt sich die Frage, wie Unternehmen menschenrechtliche und umweltbezogene Risiken in einer digitalen Umgebung identifizieren können, insbesondere angesichts der oft anonymen und dezentralen Natur von Akteuren im Metaverse.

3.18.4 Wichtigste rechtliche Risiken

Ein zentrales Risiko besteht in der Schwierigkeit, die Identität von Vertragspartnern oder Zulieferern im Metaverse zu ermitteln. Dies erschwert die Durchführung von Risikoanalysen (§ 5 LkSG) und die Verankerung von Präventionsmaßnahmen (§ 6 LkSG). Zudem birgt die Anonymität im Metaverse das Risiko, dass Verstöße gegen menschenrechtliche oder umweltbezogene Verpflichtungen nicht verfolgt werden können. Für DAOs besteht das Problem, dass sie oft keine zentrale Managementstruktur besitzen, was die Einhaltung von Sorgfaltspflichten erschwert. Unternehmen riskieren hohe Bußgelder oder den Ausschluss von öffentlichen Ausschreibungen, wenn sie ihre Pflichten nach dem LkSG nicht angemessen erfüllen.

3.18.5 Best Practice

Gesetzeskonform sind Handlungen, die den Anforderungen des LkSG entsprechen, wie die Durchführung angemessener Risikoanalysen, die Dokumentation von Maßnahmen und die Einführung eines Beschwerdeverfahrens. Unternehmen, die im Metaverse tätig sind, sollten sicherstellen, dass sie menschenrechtliche und umweltbezogene Risiken entlang ihrer digitalen Lieferketten berücksichtigen. Hierzu zählt die Integration von Schutzklauseln in Verträgen mit Partnern, die beispielsweise Server oder Hardware für das Metaverse bereitstellen. Auch die Einführung von Maßnahmen zur Transparenz und die Einhaltung von Berichtspflichten gemäß § 10 LkSG sind gesetzeskonform.

3.18.6 Worst Practice

Gesetzeswidrig sind unterlassene Maßnahmen zur Erfüllung der Sorgfaltspflichten, insbesondere bei offensichtlichen menschenrechtlichen oder umweltbezogenen Risiken. Unternehmen, die keine Risikoanalysen durchführen oder unzureichende Präventions- und Abhilfemaßnahmen umsetzen, verstoßen gegen das LkSG. Auch die Zusammenarbeit mit anonymen Partnern

oder Plattformen im Metaverse ohne angemessene Aufklärung der Identität birgt Rechtsverstöße. Der Abschluss von Verträgen, die keine menschenrechtlichen und umweltbezogenen Erwartungen enthalten, ist ebenfalls rechtswidrig, da dies den Anforderungen des § 6 LkSG widerspricht.

3.19 Markenrecht

3.19.1 Rechtsvorschriften im Rechtsgebiet

Die Rechtslage zum Markenrecht im Metaverse basiert auf dem deutschen Markengesetz (MarkenG) und der EU-Unionsmarken-Verordnung (UMVO), die einen harmonisierten Rahmen für den Markenschutz schaffen. Diese Gesetze schützen Marken, die für virtuelle Güter und Dienstleistungen verwendet werden, wobei auch neue Technologien wie NFTs berücksichtigt werden. Das Territorialitätsprinzip begrenzt den Markenschutz jedoch auf die jeweilige Jurisdiktion, so dass global tätige Unternehmen oft mehrere Markenregistrierungen benötigen..

3.19.2 Geltende Grundprinzipien

Zu den Grundprinzipien des Markenrechts gehört der Schutz der Unterscheidungskraft, die Sicherstellung der Herkunftsfunktion und die Verhinderung von Verwechslungsgefahr. Marken müssen eindeutig einem Anbieter zuordenbar sein und dürfen nicht rein beschreibend oder dekorativ verwendet werden. Für virtuelle Marken und NFTs gelten dieselben Anforderungen wie für physische Marken, jedoch mit zusätzlichen Spezifizierungsanforderungen, um die Klarheit des Schutzzumfangs zu gewährleisten.

3.19.3 Prioritäre juristische Fragestellungen im Kontext Markenrecht

Wichtige Fragestellungen umfassen die Anerkennung virtueller Marken als eigenständige Schutzobjekte, die Abgrenzung zwischen virtuellen und physischen Gütern bei der Beurteilung der Verwechslungsgefahr sowie die rechtliche Durchsetzbarkeit von Markenrechten in globalen und oft anonymen virtuellen Umgebungen. Insbesondere der Schutz von Marken in dezentralen Plattformen stellt eine Herausforderung dar.

3.19.4 Wichtigste rechtliche Risiken

Rechtliche Risiken ergeben sich aus der mangelnden internationalen Harmonisierung, wodurch Konflikte über die Gültigkeit und Durchsetzung von Markenrechten entstehen können. Weiterhin besteht das Risiko von Verwechslung oder Missbrauch virtueller Marken, etwa durch imitierte NFTs, sowie die Gefahr der Haftung von Plattformbetreibern bei unzureichender Kontrolle über markenrechtliche Verstöße in virtuellen Räumen.

3.19.5 Best Practice

Gesetzeskonform ist die korrekte Eintragung einer Marke für virtuelle Waren oder Dienstleistungen, die Einhaltung der Anforderungen an die Nutzung von Marken als Herkunftshinweis und die transparente Kommunikation über Markenrechte und Lizenzen. Die Anwendung klarer Richtlinien für die Nutzung virtueller Marken schafft zusätzliche Rechtssicherheit.

3.19.6 Worst Practice

Gesetzeswidrig sind die unerlaubte Nutzung geschützter Marken, die Umgehung des Territorialitätsprinzips durch illegale Nutzung in anderen Jurisdiktionen und die missbräuchliche Registrierung von Marken, etwa in bösgläubiger Absicht. Ebenso ist die Nutzung einer Marke ohne Zustimmung des Rechteinhabers im Metaverse, insbesondere zu kommerziellen Zwecken, eine klare Verletzung des Markenrechts.

3.20 Medienrecht

3.20.1 Rechtsvorschriften im Rechtsgebiet

Das Medienrecht im Metaverse wird durch eine Vielzahl von Vorschriften geregelt, darunter das Jugendschutzgesetz (JuSchG), der Jugendmedienschutz-Staatsvertrag (JMStV), das Telemediengesetz (TMG), sowie strafrechtliche Normen des Strafgesetzbuches (StGB). Auf europäischer Ebene sind die Datenschutz-Grundverordnung (DS-GVO), die E-Commerce-Richtlinie und die Audiovisuelle Mediendienste-Richtlinie (AVMD-RL) relevant. Für grenzüberschreitende Inhalte sind das Herkunftslandprinzip und kollisionsrechtliche Regelungen von zentraler Bedeutung. Plattformbetreiber im Metaverse, die Inhalte hosten oder verbreiten, müssen die Vorschriften zur Alterskennzeichnung und technischen Zugangsbeschränkungen beachten.

3.20.2 Geltende Grundprinzipien

Wichtige Grundprinzipien des Medienrechts sind der Schutz von Kindern und Jugendlichen vor schädlichen Inhalten, der Schutz der Menschenwürde und das Verbot strafbarer Inhalte wie Kinderpornografie oder Gewaltverherrlichung. Zugleich spielt die Meinungsfreiheit eine zentrale Rolle, die im Rahmen der Rechtsvorschriften geschützt bleibt. Das Prinzip der Selbstregulierung ermöglicht Plattformbetreibern, durch freiwillige Maßnahmen und Mitgliedschaft in anerkannten Selbstkontrolleinrichtungen (z. B. FSM, USK) Verantwortung für den Jugendschutz zu übernehmen. Ein weiteres Prinzip ist die Technologieneutralität, die sicherstellt, dass neue Technologien wie Virtual Reality (VR) ebenfalls unter das bestehende Recht fallen.

3.20.3 Prioritäre juristische Fragestellungen im Kontext Medienrecht

Im Metaverse entstehen neue Fragestellungen wie die rechtliche Bewertung von VR-Inhalten, die Erfordernisse von Alterskennzeichnungen und die Verantwortung der Plattformbetreiber für nutzergenerierte Inhalte. Es stellt sich die Frage, wie Jugendschutzmaßnahmen technisch umgesetzt werden können, etwa durch Altersverifikationssysteme. Auch die Einordnung von In-Game-Werbung und Lootboxen sowie die Rolle von Künstlicher Intelligenz bei der Moderation von Inhalten sind entscheidende Themen. Schließlich bleibt zu klären, wie das Herkunftslandprinzip in einem grenzüberschreitenden virtuellen Raum umgesetzt werden kann und welche Zuständigkeiten nationale Behörden haben.

3.20.4 Wichtigste rechtliche Risiken

Die Risiken im Medienrecht des Metaverse umfassen die Verbreitung strafbarer Inhalte wie Kinderpornografie, das Versäumnis jugendschutzrechtlicher Maßnahmen und die mögliche Haftung von Plattformbetreibern für nutzergenerierte Inhalte. Eine unzureichende Altersverifikation oder fehlende Kennzeichnung von Inhalten kann zu Bußgeldern oder Sperrungen führen. Auch grenzüberschreitende Inhalte bergen Risiken, insbesondere wenn Plattformen die Anforderungen der Länder, in denen ihre Dienste verfügbar sind, nicht erfüllen. Zudem bestehen Datenschutzrisiken durch unzureichende Pseudonymisierung und die Erhebung sensibler Nutzerdaten.

3.20.5 Best Practice

Gesetzeskonform ist der Betrieb von Plattformen, die technische Maßnahmen wie Altersverifikationssysteme und Jugendschutzprogramme implementieren, um den Zugang zu entwicklungsbeeinträchtigenden oder jugendgefährdenden Inhalten zu regeln. Auch die Kennzeichnung von Inhalten gemäß den Vorgaben des JuSchG und JMStV sowie die Mitgliedschaft in Selbstkontrolleinrichtungen tragen zur Gesetzeskonformität bei. Plattformen können durch die Bereitstellung transparenter Nutzungsbedingungen und datenschutzfreundlicher Technologien die rechtlichen Anforderungen erfüllen.

3.20.6 Worst Practice

Gesetzeswidrig sind die Verbreitung und der Zugriff auf Inhalte, die gegen den Jugendschutz oder strafrechtliche Bestimmungen verstoßen, wie Gewalt- oder pornografische Darstellungen ohne ausreichende Schutzmaßnahmen. Die Missachtung der Alterskennzeichnungspflichten oder das Angebot von Lootboxen ohne entsprechende Einschränkungen können ebenfalls als

Rechtsverstöße gewertet werden. Plattformbetreiber, die unzureichende Maßnahmen gegen Belästigungen, Cybergrooming oder andere Formen von Missbrauch ergreifen, laufen Gefahr, gegen das geltende Recht zu verstoßen.

3.21 Medizin- und Medizinprodukterecht

3.21.1 Rechtsvorschriften im Rechtsgebiet

Im Medizin- und Medizinprodukterecht im Metaverse gelten die Vorschriften der europäischen Medizinprodukteverordnung (MDR, EU 2017/745) und des Medizinprodukterecht-Durchführungsgesetzes (MPDG). Ergänzend greifen nationale Regelungen zur Telemedizin sowie Datenschutzbestimmungen wie die Datenschutz-Grundverordnung (DS-GVO). Für digitale Anwendungen sind zudem die spezifischen Regelungen der Software-Risikoklassifizierung der MDR, insbesondere Regel 11, von Bedeutung. Internationale Vorgaben, etwa durch die FDA oder vergleichbare Institutionen anderer Länder, haben Einfluss auf grenzüberschreitende medizinische Dienstleistungen und Produkte im Metaverse.

3.21.2 Geltende Grundprinzipien

Das Medizin- und Medizinprodukterecht beruht auf den Prinzipien der Patientensicherheit, der Transparenz und der Wirksamkeitsprüfung. Produkte und Dienstleistungen müssen den Grundsätzen der Zweckbestimmung entsprechen und in klar definierten Zulassungsverfahren auf Sicherheit und Leistungsfähigkeit geprüft werden. Ein weiteres Prinzip ist die Risikoklassifizierung, bei der Produkte entsprechend ihrer Gefährdungspotenziale eingestuft werden. Im Metaverse spielt zudem der Schutz vor Fehlinformationen und die Einhaltung von Datenschutzvorgaben eine zentrale Rolle.

3.21.3 Prioritäre juristische Fragestellungen im Kontext Medizin- und Medizinprodukterecht

Zentrale Fragestellungen betreffen die Einordnung virtueller medizinischer Produkte und Dienstleistungen: Handelt es sich bei VR- oder AR-basierten Therapien um Medizinprodukte? Welche Anforderungen gelten für digitale Zwillinge und deren Verwendung? Ein weiterer Schwerpunkt liegt auf der Zulassung und Risikoklassifizierung solcher Produkte, insbesondere bei innovativen Anwendungen wie virtuellen Operationstrainings. Die Frage nach der Haftung bei fehlerhaften digitalen Therapien oder Diagnosen und die Sicherstellung des Datenschutzes bei der Verarbeitung sensibler Gesundheitsdaten sind ebenfalls entscheidend.

3.21.4 Wichtigste rechtliche Risiken

Rechtliche Risiken bestehen vor allem in der unklaren Abgrenzung zwischen Medizin- und Lifestyle-Produkten. Die fehlerhafte Klassifizierung oder unzureichende Prüfung eines Produkts kann zu Haftungsproblemen führen. Datenschutzverletzungen, insbesondere bei der Verarbeitung sensibler Daten durch KI-gestützte Diagnosetools oder digitale Zwillinge, bergen erhebliche Sanktionen. Ein weiteres Risiko besteht in der unzureichenden Einbindung der genutzten Hardware (z. B. VR-Brillen) in den Zulassungsprozess. Die globale Natur des Metaverse erschwert zudem die Rechtsdurchsetzung und Regulierungsüberwachung.

3.21.5 Best Practice

Gesetzeskonform sind die Zulassung und Nutzung von VR- und AR-Produkten, wenn sie gemäß MDR und nationalen Vorschriften geprüft und zertifiziert wurden. Telemedizinische Dienstleistungen, die Datenschutz- und Sicherheitsanforderungen erfüllen, können ebenfalls rechtmäßig angeboten werden. Gesetzeskonform ist die Verwendung von Software, die korrekt klassifiziert wurde und die Zweckbestimmung des Produkts unterstützt. Darüber hinaus können Ausnahmen wie die „Inhouse-Herstellung“ unter bestimmten Bedingungen rechtmäßig genutzt werden.

3.21.6 Worst Practice

Gesetzeswidrig ist die Nutzung oder der Vertrieb von medizinischen Anwendungen, die keine ordnungsgemäße Zulassung nach MDR oder vergleichbaren Standards haben. Auch die Missachtung von Datenschutzvorgaben bei der Verarbeitung von Patientendaten im Metaverse ist unzulässig. Der Einsatz von Produkten, die bewusst als Lifestyle-Tools deklariert werden, um regulatorische Anforderungen zu umgehen, verstößt ebenfalls gegen das Medizinprodukte-recht. Schließlich sind falsche oder irreführende Werbeversprechen, die medizinische Wirkungen suggerieren, ohne diese nachweisen zu können, rechtswidrig.

3.22 Miet- und Wohneigentumsrecht

3.22.1 Rechtsvorschriften im Rechtsgebiet

Die Rechtslage zum Miet- und Wohneigentumsrecht im Metaverse basiert auf bestehenden Regelungen des BGB und der EU-Richtlinie über digitale Inhalte (Digitale-Inhalte-RL). Virtuelle Grundstücke und Immobilien werden rechtlich als digitale Produkte betrachtet, wodurch die §§ 327 ff. BGB für digitale Verträge Anwendung finden. Das Wohnungseigentumsgesetz ist nicht

anwendbar, da NFTs und virtuelle Grundstücke keine Sachen im Sinne des § 90 BGB sind und lediglich Lizenzrechte darstellen..

3.22.2 Geltende Grundprinzipien

Grundprinzipien umfassen das Äquivalenzprinzip, das eine angemessene Beziehung zwischen Leistung und Gegenleistung sicherstellen soll, sowie die Anwendung von Mietrecht analog für digitale Produkte. Die Rechte des Mieters, wie Minderungs- und Kündigungsrechte, und die Pflichten des Vermieters werden in digitalen Mietverträgen auf die Eigenschaften digitaler Produkte angepasst. Das Territorialitätsprinzip ist hier weniger relevant, da das Metaverse global operiert.

3.22.3 Prioritäre juristische Fragestellungen im Kontext Miet- und Wohneigentumsrecht

Wichtige Fragestellungen betreffen die rechtliche Qualifikation virtueller Grundstücke und NFTs, die Geltung mietrechtlicher Vorschriften bei digitalen Produkten und die Durchsetzung von Rechten bei Mängeln oder Ausfällen im Metaverse. Dabei ist zu klären, wie weit Miet- oder Kaufrecht greift und welche spezifischen Rechte und Pflichten daraus folgen.

3.22.4 Wichtigste rechtliche Risiken

Zu den rechtlichen Risiken zählen unklare Haftungsregelungen bei Serverausfällen, die mangelnde Beständigkeit virtueller Grundstücke durch plattformspezifische Abhängigkeiten und die Gefahr von Manipulationen oder unzureichendem Schutz durch Lizenzbedingungen. Insbesondere bei internationalen Plattformen ergeben sich Unsicherheiten durch unterschiedliche Rechtsordnungen.

3.22.5 Best Practice

Gesetzeskonform ist die vertragliche Gestaltung von Mietverhältnissen im Metaverse nach den §§ 327 ff. BGB, die transparente Kommunikation der Lizenzbedingungen und die Gewährleistung der Nutzungsmöglichkeit durch technische Stabilität. Rechte und Pflichten müssen klar geregelt sein, um Mängel oder Streitigkeiten zu minimieren.

3.22.6 Worst Practice

Gesetzeswidrig ist die Verwendung irreführender oder unklarer Lizenzbedingungen, die bewusste Einschränkung von Nutzerrechten entgegen der vertraglichen Vereinbarung und die Nichtgewährung von Rückerstattungen bei dauerhafter Nichterfüllung. Auch das Verschweigen

wesentlicher Eigenschaften der virtuellen Grundstücke oder NFTs kann rechtliche Konsequenzen haben.

3.23 Normennutzung: rechtliche Implikationen

3.23.1 Rechtsvorschriften im Rechtsgebiet

Bei der Entwicklung und Inverkehrbringung von Metaverse-Produkten gelten nationale und internationale Regelungen. In Deutschland sind insbesondere das Produktsicherheitsgesetz (ProdSG), das Bürgerliche Gesetzbuch (BGB) und das Gesetz gegen den unlauteren Wettbewerb (UWG) relevant. Auf europäischer Ebene kommen die Verordnung (EU) 2019/1020 über die Marktüberwachung und das Inverkehrbringen von Produkten sowie die Datenschutz-Grundverordnung (DS-GVO) zum Tragen. Technische Standards, etwa ISO-Normen oder DIN-Vorgaben, sind nicht rechtlich bindend, gelten jedoch als anerkannte Regeln der Technik und spielen bei der Haftung und Produktsicherheit eine zentrale Rolle.

3.23.2 Geltende Grundprinzipien

Die Einhaltung von Normen und Standards orientiert sich an den Grundprinzipien der Produktsicherheit, der Transparenz und des Verbraucherschutzes. Hersteller und Anbieter sind verpflichtet, Produkte so zu gestalten, dass sie keine Gefahren für Nutzer darstellen (§ 3 ProdSG). Zudem gilt der Grundsatz der Verkehrssicherungspflicht, nach dem potenzielle Risiken vorhersehbar und minimierbar sein müssen. Standards und Normen dienen als Referenz, um den Stand der Technik zu bestimmen und rechtliche Anforderungen zu erfüllen.

3.23.3 Prioritäre juristische Fragestellungen im Kontext Patentrecht

Wichtige Fragen umfassen die Anwendung bestehender Normen auf virtuelle Produkte und Dienstleistungen. Wie wird Produktsicherheit bei Metaverse-Software oder Hardware wie VR-Brillen bewertet? Welche Standards gelten für Interoperabilität, Datenschutz und KI-basierte Anwendungen? Die Rolle von international anerkannten Normen (z. B. ISO 27001 für Informationssicherheitsmanagement) und deren Anpassung an digitale Produkte ist ebenfalls eine zentrale Fragestellung. Zudem stellt sich die Frage, wie Verstöße gegen Sicherheits- oder Datenschutzvorgaben im globalen Kontext geahndet werden können.

3.23.4 Wichtigste rechtliche Risiken

Ein Hauptproblem besteht in der Haftung bei Nichteinhaltung von Normen und Standards. Produkte, die nicht den anerkannten Regeln der Technik entsprechen, können als mangelhaft eingestuft werden, was Schadensersatzansprüche nach sich zieht (§§ 823, 831 BGB). Die

Missachtung von Sicherheitsstandards, insbesondere bei Hardware-Produkten, kann zu Produkthaftungsfällen führen. Im digitalen Bereich erhöhen Verstöße gegen Datenschutzstandards oder die Nutzung unsicherer Algorithmen die Gefahr von Bußgeldern und Reputationsverlusten.

3.23.5 Best Practice

Gesetzeskonform ist die Entwicklung von Produkten, die den geltenden Normen und Standards entsprechen, insbesondere in Bezug auf Produktsicherheit und Datenschutz. Die transparente Offenlegung von Produktinformationen und die Einhaltung von Datenschutzanforderungen gemäß DS-GVO sind ebenfalls rechtlich erforderlich. Unternehmen, die internationale Normen wie ISO-Standards freiwillig anwenden, handeln im Einklang mit den Erwartungen an die Verkehrssicherungspflicht.

3.23.6 Worst Practice

Rechtswidrig ist die Inverkehrbringung von Produkten, die nicht den Sicherheitsanforderungen entsprechen oder bei denen relevante Standards missachtet wurden. Dazu zählen unsichere Softwarelösungen, die potenzielle Gefahren für Nutzer darstellen, sowie VR-Geräte oder Plattformen, die gesundheitliche Risiken erhöhen könnten. Ebenso unzulässig ist die Verarbeitung personenbezogener Daten ohne Einhaltung der Datenschutzstandards, was Bußgelder nach sich ziehen kann. Schließlich gilt auch die Irreführung von Verbrauchern über die Eigenschaften oder Sicherheit eines Produkts als rechtswidrig.

3.24 Patentrecht

3.24.1 Rechtsvorschriften im Rechtsgebiet

Das Patentrecht im Metaverse wird durch nationale und internationale Regelwerke wie das deutsche Patentgesetz (PatG) und das Europäische Patentübereinkommen (EPÜ) geregelt. Insbesondere sind die Artikel 52 ff. EPÜ und § 1 PatG relevant, die den Schutz technischer Erfindungen regeln. Computerimplementierte Erfindungen und Algorithmen sind grundsätzlich ausgeschlossen, es sei denn, sie lösen ein technisches Problem mit technischen Mitteln. Zudem sind Blockchain-Technologien, VR-Hardware und -Software sowie Datenfolgen durch das deutsche und europäische Patentrecht reguliert, sofern sie technische Voraussetzungen erfüllen. Internationale Regelungen, wie die Richtlinien des Europäischen Patentamts (EPA), sind ebenfalls von Bedeutung.

3.24.2 Geltende Grundprinzipien

Das Patentrecht basiert auf den Prinzipien der Technizität, Neuheit, erfinderischen Tätigkeit und gewerblichen Anwendbarkeit. Der Schutz ist auf technische Erfindungen beschränkt, die einen konkreten technischen Erfolg erzielen. Computerprogramme sind grundsätzlich vom Patentschutz ausgeschlossen, es sei denn, sie erzeugen eine „zusätzliche technische Wirkung“. Auch Daten können geschützt werden, wenn sie ein unmittelbares Verfahrenserzeugnis eines patentierten Verfahrens darstellen. Im Metaverse werden diese Prinzipien durch die Anforderungen an Virtualisierungen, Blockchain-Implementierungen und Datenstrukturen ergänzt.

3.24.3 Prioritäre juristische Fragestellungen im Kontext Patentrecht

Im Metaverse ergeben sich spezifische Fragestellungen: Können Virtualisierungen, wie digitale Abbilder oder Avatare, als technische Erfindungen eingestuft werden? Wie wird der Patentschutz auf computerimplementierte Erfindungen angewandt, insbesondere bei Algorithmen und Simulationen? Eine weitere Herausforderung ist die Durchsetzung von Patentrechten, insbesondere wenn patentgeschützte Produkte oder Verfahren virtuell imitiert oder angeboten werden. Auch die Patentierung von Blockchain-Technologien und die Einordnung von Datenfolgen als Verfahrenserzeugnisse stellen zentrale Fragen dar.

3.24.4 Wichtigste rechtliche Risiken

Ein zentrales Risiko liegt in der unklaren Abgrenzung zwischen patentierbaren und nicht patentierbaren Erfindungen, insbesondere bei Software und Algorithmen. Die Virtualisierung realer Produkte im Metaverse kann Patentrechtsverletzungen begründen, wenn patentierte technische Merkmale imitiert werden. Die globale Natur des Metaverse erschwert zudem die Rechtsdurchsetzung, insbesondere wenn Plattformen in Ländern ohne angemessenen Patentschutz betrieben werden. Risiken bestehen auch in der Patentierung von Technologien, die nicht eindeutig technischer Natur sind, was zu rechtlichen Unsicherheiten führen kann.

3.24.5 Best Practice

Gesetzeskonform sind Handlungen, die patentrechtlich geschützte Technologien mit entsprechender Lizenz nutzen. Die Entwicklung von computerimplementierten Erfindungen, die technische Probleme lösen, und die Einreichung von Patentanmeldungen, die die Voraussetzungen der Technizität, Neuheit und erfinderischen Tätigkeit erfüllen, sind ebenfalls zulässig. Das Anbieten von virtuellen Produkten im Metaverse, sofern keine patentierten Merkmale verletzt

werden, ist rechtlich unproblematisch. Auch die Nutzung von Blockchain-Technologien, die den Anforderungen des Patentschutzes genügen, ist erlaubt.

3.24.6 Worst Practice

Gesetzeswidrig ist die Nutzung oder das Anbieten von patentgeschützten Technologien ohne Zustimmung des Rechteinhabers, insbesondere durch virtuelle Nachbildungen oder Simulationen. Die Verwendung von Software oder Algorithmen, die patentierte Verfahren imitieren, ohne technische Neuerungen zu implementieren, kann ebenfalls eine Verletzung darstellen. Auch das Anbieten von Datenfolgen, die durch patentierte Verfahren erzeugt wurden, ohne Lizenzvereinbarung ist unzulässig. Schließlich ist die Anmeldung von Erfindungen, die nicht den Anforderungen der Technizität entsprechen, rechtswidrig.

3.25 Persönlichkeitsrecht

3.25.1 Rechtsvorschriften im Rechtsgebiet

Im Bereich des Persönlichkeitsrechts im Metaverse sind sowohl nationale Regelungen wie Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, die das allgemeine Persönlichkeitsrecht schützen, als auch die Datenschutz-Grundverordnung (DS-GVO) von zentraler Bedeutung. Weitere Vorschriften wie § 22 und § 23 KUG (Recht am eigenen Bild) sowie §§ 185 ff. StGB (Schutz vor Beleidigung und übler Nachrede) kommen ergänzend zur Anwendung. Im virtuellen Raum erweitern internationale Vereinbarungen und Nutzungsbedingungen der Plattformen diese Regelungen. Die Frage nach der Jurisdiktion richtet sich nach kollisionsrechtlichen Vorschriften wie der Rom-II-Verordnung.

3.25.2 Geltende Grundprinzipien

Das Persönlichkeitsrecht im Metaverse basiert auf den Grundsätzen des Schutzes der Menschenwürde, der informationellen Selbstbestimmung und der Privatsphäre. Es umfasst auch das Recht am eigenen Bild und den Schutz vor unberechtigter kommerzieller Nutzung persönlicher Merkmale wie Avataren oder digitalen Repräsentationen. Das Recht auf freie Entfaltung der Persönlichkeit gilt auch in digitalen Kontexten und zielt darauf ab, Nutzer vor übermäßiger Überwachung, Identitätsdiebstahl oder Belästigung zu schützen. Gleichzeitig besteht ein Spannungsfeld zwischen Meinungsfreiheit und dem Schutz der individuellen Würde.

3.25.3 Prioritäre juristische Fragestellungen im Kontext Persönlichkeitsrecht

Im Metaverse stellen sich Fragen zur rechtlichen Bewertung von Avataren und deren Schutz als digitale Repräsentation. Welche Rechte hat ein Nutzer, wenn sein Avatar in einer Weise genutzt

wird, die gegen seine Wünsche verstößt? Wie wird der Schutz persönlicher Daten gewährleistet, wenn Plattformbetreiber Nutzerdaten erheben und verwenden? Auch die Abwägung zwischen Meinungsfreiheit und dem Schutz vor Belästigung ist eine zentrale Herausforderung. Schließlich ist die Frage relevant, wie das postmortale Persönlichkeitsrecht auf die digitalen Hinterlassenschaften eines Verstorbenen angewendet wird.

3.25.4 Wichtigste rechtliche Risiken

Die Risiken liegen vor allem in der Verletzung des Persönlichkeitsrechts durch die unerlaubte Nutzung von Avataren oder personenbezogenen Daten. Ein weiteres Risiko ist die unklare Verantwortlichkeit bei Rechtsverstößen, insbesondere wenn Plattformen in unterschiedlichen Rechtsräumen agieren. Identitätsdiebstahl, Cybermobbing und die Manipulation oder Diffamierung von Avataren sind konkrete Bedrohungen. Schließlich besteht die Gefahr, dass Nutzungsbedingungen der Plattformen Persönlichkeitsrechte der Nutzer beschneiden.

3.25.5 Best Practice

Gesetzeskonform sind die Erstellung und Nutzung eines Avatars, wenn diese im Einklang mit den Nutzungsbedingungen der Plattform stehen und keine Rechte Dritter verletzen. Ebenso erlaubt ist die Verarbeitung personenbezogener Daten durch Plattformbetreiber, wenn sie die Vorgaben der DS-GVO einhalten. Die Nutzung von Avataren für kommerzielle Zwecke ist rechtmäßig, sofern der Avatar-Inhaber ausdrücklich zustimmt. Plattformen, die Mechanismen zum Schutz vor Belästigung und Identitätsdiebstahl implementieren, agieren im Rahmen des rechtlich Erlaubten.

3.25.6 Worst Practice

Gesetzeswidrig sind die unerlaubte Nutzung von Avataren oder persönlichen Daten ohne Zustimmung des Nutzers sowie die Veröffentlichung oder Verbreitung von Inhalten, die die Würde oder Privatsphäre anderer verletzen. Identitätsdiebstahl, die kommerzielle Nutzung eines Avatars ohne Zustimmung und Cybermobbing stellen ebenfalls Rechtsverstöße dar. Plattformbetreiber, die keine wirksamen Maßnahmen zum Schutz der Persönlichkeitsrechte ergreifen oder Nutzungsbedingungen durchsetzen, die Persönlichkeitsrechte einschränken, handeln ebenfalls rechtswidrig.

3.26 Polizeirecht und staatliche Kontrolle

3.26.1 Rechtsvorschriften im Rechtsgebiet

Das Polizeirecht im Metaverse wird primär durch nationale Polizeigesetze (wie die Landespolizeigesetze und das Bundespolizeigesetz) sowie die Strafprozessordnung (StPO) geregelt. Auf europäischer Ebene ist die Datenschutzrichtlinie für Justiz und Inneres (JI-Richtlinie) relevant, ergänzt durch die Datenschutz-Grundverordnung (DS-GVO). Internationale Abkommen, wie die Europäische Menschenrechtskonvention (EMRK), beeinflussen die Grenzen polizeilichen Handelns. Zunehmend spielen die Vorschriften zur Regulierung Künstlicher Intelligenz, wie der EU-KI-Verordnungsentwurf, eine zentrale Rolle, da polizeiliche Maßnahmen im Metaverse stark auf KI-basierte Systeme angewiesen sind.

3.26.2 Geltende Grundprinzipien

Das Polizeirecht ist vom Grundsatz der Verhältnismäßigkeit geprägt. Eingriffe in Grundrechte müssen geeignet, erforderlich und angemessen sein. Im Metaverse gilt dies besonders für digitale Überwachungsmaßnahmen, die etwa durch Art. 2 Abs. 1 i.V.m. Art. 1 GG (informationelle Selbstbestimmung) und Art. 10 GG (Telekommunikationsgeheimnis) begrenzt sind. Ein weiteres Grundprinzip ist die Abgrenzung zwischen Gefahrenabwehr und Strafverfolgung. Im Metaverse erweitern internationale Prinzipien wie das Diskriminierungsverbot und der Schutz der Meinungsfreiheit den Handlungsspielraum der Polizei.

3.26.3 Prioritäre juristische Fragestellungen im Kontext Polizeirecht

Die zentralen Fragen umfassen: Wie können die Polizei und Strafverfolgungsbehörden im Metaverse effektiv agieren, ohne übermäßige Grundrechtseingriffe vorzunehmen? Welche rechtliche Grundlage gibt es für die Verwendung polizeilicher Avatare und KI-Systeme? Weitere Herausforderungen sind die Abgrenzung von Jurisdiktionen, da Straftaten im Metaverse häufig grenzüberschreitend sind. Auch die rechtliche Bewertung von Metakriminalität (etwa Betrug durch NFTs) und die Einbindung privater Plattformbetreiber in die Gefahrenabwehr stellen neue Fragestellungen dar.

3.26.4 Wichtigste rechtliche Risiken

Ein Hauptproblem ist die unklare Abgrenzung der Zuständigkeiten nationaler und internationaler Strafverfolgungsbehörden im dezentralen Metaverse. Risiken bestehen auch in der unzureichenden Regulierung polizeilicher KI-Systeme, die zu unverhältnismäßigen Eingriffen führen könnten. Verstöße gegen Datenschutzvorgaben, insbesondere bei der Verarbeitung

personenbezogener Daten, können zu erheblichen rechtlichen Konsequenzen führen. Zusätzlich birgt die fehlende technische Absicherung von polizeilichen Maßnahmen das Risiko von Missbrauch und Hackerangriffen.

3.26.5 Best Practice

Gesetzeskonform ist die präventive Gefahrenabwehr und Strafverfolgung, die sich auf nationale Polizeigesetze stützt und die Grundsätze der Verhältnismäßigkeit einhält. Die Verwendung von KI-Systemen ist zulässig, sofern diese transparent betrieben werden und den Anforderungen der EU-KI-Verordnung genügen. Auch der Einsatz von polizeilichen Avataren zur Informationsbereitstellung und verdeckten Ermittlungen ist erlaubt, wenn gesetzliche Grundlagen vorhanden sind. Die Kooperation mit Plattformbetreibern, etwa zur Umsetzung von Community-Richtlinien, ist ebenfalls rechtlich zulässig.

3.26.6 Worst Practice

Unzulässig sind unverhältnismäßige Eingriffe in Grundrechte, insbesondere die ungerechtfertigte Überwachung oder Speicherung personenbezogener Daten. Der Einsatz von KI-Systemen ohne adäquate Transparenz- und Kontrollmechanismen verstößt gegen geltende Datenschutzrichtlinien. Auch das Überschreiten nationaler Zuständigkeiten, etwa durch Maßnahmen außerhalb der deutschen Jurisdiktion, ist problematisch. Schließlich sind polizeiliche Maßnahmen ohne gesetzliche Grundlage, wie die verdeckte Nutzung von Avataren zur Überwachung, rechtswidrig.

3.27 Rechtsschutz und gerichtliche Zuständigkeit

3.27.1 Rechtsvorschriften im Rechtsgebiet

Im Bereich des Rechtsschutzes und der gerichtlichen Zuständigkeit im Metaverse kommen nationale Vorschriften wie die Zivilprozessordnung (ZPO) sowie europäische Verordnungen wie die Brüssel Ia-Verordnung (EuGVVO) zum Tragen, die die internationale Zuständigkeit regeln. Ergänzend gelten spezifische Vorschriften für digitale Streitbeilegung, darunter die Regelungen zu Smart Contracts und Online-Schiedsverfahren. Internationale Übereinkommen wie das New Yorker Übereinkommen über die Anerkennung und Vollstreckung ausländischer Schiedssprüche sind ebenso relevant, insbesondere bei grenzüberschreitenden Streitigkeiten.

3.27.2 Geltende Grundprinzipien

Das Rechtsschutzsystem im Metaverse basiert auf den Prinzipien der Verfahrensgerechtigkeit, des Zugangs zu Gerichten und der Effektivität von Streitbeilegung. Das Prinzip der Territorialität

prägt die gerichtliche Zuständigkeit und kollidiert im Metaverse häufig mit der globalen Reichweite virtueller Plattformen. Ebenso gilt das Prinzip der Parteiautonomie, insbesondere in Bezug auf die Wahl von Gerichtsständen oder Schiedsgerichten. Ein weiteres Grundprinzip ist der Schutz vor Missbrauch durch Anonymität, das durch Anforderungen an die Identifizierbarkeit der Parteien gestützt wird.

3.27.3 Prioritäre juristische Fragestellungen im Kontext Rechtsschutz und gerichtliche Zuständigkeit

Im Metaverse stellen sich Fragen wie: Welche Gerichte sind zuständig, wenn Streitigkeiten zwischen anonymen Parteien oder über digitale Güter wie NFTs entstehen? Wie können Smart Contracts rechtlich durchgesetzt werden, und welche Beweismittel sind im digitalen Raum zulässig? Eine weitere Herausforderung ist die Vollstreckung von Urteilen und Schiedssprüchen, wenn digitale Vermögenswerte oder Avatare betroffen sind. Zudem ist zu klären, wie Online-Schiedsverfahren effektiv gestaltet werden können und ob neue Formen wie Blockchain-basierte Schiedsgerichtsbarkeit rechtswirksam sind.

3.27.4 Wichtigste rechtliche Risiken

Ein zentrales Risiko besteht in der mangelnden Klarheit über die internationale Zuständigkeit, insbesondere wenn Plattformen globale Nutzerbasis haben und unterschiedliche Rechtsordnungen kollidieren. Die Nutzung von Anonymität im Metaverse birgt das Risiko, dass rechtliche Ansprüche nicht effektiv durchgesetzt werden können. Die Durchsetzbarkeit von Entscheidungen und Schiedssprüchen ist ein weiteres Problem, insbesondere wenn Parteien ihre Identität verschleiern oder Vermögenswerte schwer greifbar sind. Die Unsicherheiten bei der Anerkennung von digitalen Schiedssprüchen und Smart Contracts erhöhen die Komplexität.

3.27.5 Best Practice

Gesetzeskonform ist die Nutzung von vertraglichen Vereinbarungen über Gerichtsstände und Schiedsverfahren, die mit den Anforderungen der ZPO und der EuGVVO übereinstimmen. Die Durchführung von Online-Verfahren, einschließlich digitaler Beweiserhebung, ist zulässig, solange die gesetzlichen Vorgaben eingehalten werden. Auch die Integration von Smart Contracts in rechtliche Prozesse ist zulässig, sofern diese die Anforderungen an Transparenz und Nachvollziehbarkeit erfüllen. Plattformen können Nutzungsbedingungen etablieren, die Streitbeilegungsmechanismen vorsehen, wenn diese nicht gegen zwingendes Recht verstoßen.

3.27.6 Worst Practice

Gesetzeswidrig sind die Durchführung von Verfahren ohne ausreichende Identifikation der Parteien, da dies gegen das Prinzip der Rechtsstaatlichkeit verstößt. Ebenso unzulässig ist die Umgehung nationaler Zuständigkeitsregelungen durch plattformseitige Klauseln, die unzulässige Gerichtszuständigkeiten festlegen. Schiedssprüche, die ohne ordnungsgemäße Anerkennung der Identität der Parteien oder ohne Transparenz erstellt werden, könnten unwirksam sein. Schließlich verstößt die Vollstreckung von Smart Contracts, die rechtswidrige Inhalte automatisieren, gegen geltendes Recht.

3.28 Steuerrecht

3.28.1 Rechtsvorschriften im Rechtsgebiet

Die Rechtslage zum Steuerrecht im Metaverse wird durch bestehende nationale und internationale Vorschriften wie das Einkommensteuergesetz (EStG), die Umsatzsteuer-Systemrichtlinie (MwStSystRL) und das Körperschaftsteuergesetz (KStG) geregelt. Einnahmen aus Kryptowährungen und NFTs können je nach Nutzung verschiedenen Einkunftsarten im Sinne von § 2 EStG zugeordnet werden, wie Einkünften aus Gewerbebetrieb, privaten Veräußerungsgeschäften oder Kapitalvermögen. Umsätze im Metaverse, etwa durch den Handel mit NFTs oder die Vermietung virtueller Grundstücke, unterliegen potenziell der Umsatzsteuer gemäß § 1 UStG, wobei die steuerliche Qualifikation komplex bleibt.

3.28.2 Geltende Grundprinzipien

Grundprinzipien des Steuerrechts im Metaverse umfassen das Welteinkommensprinzip, nach dem weltweit erzielte Einkünfte in Deutschland steuerpflichtig sein können, und das Leistungsfähigkeitsprinzip, das sicherstellen soll, dass Steuerpflichtige entsprechend ihrer wirtschaftlichen Kapazität besteuert werden. Zudem sind Grundsätze wie der Leistungsaustausch und die Nachhaltigkeit zentral, um steuerbare Vorgänge zu identifizieren.

3.28.3 Prioritäre juristische Fragestellungen im Kontext Steuerrecht

Zentrale Fragestellungen betreffen die ertragsteuerliche Qualifikation von Einnahmen aus virtuellen Welten, die umsatzsteuerliche Behandlung von digitalen Gütern und Dienstleistungen sowie die Anwendung und Einhaltung von Doppelbesteuerungsabkommen bei grenzüberschreitenden Transaktionen. Besonders der Übergang von virtuellen zu realen Märkten, etwa bei der Umwandlung virtueller Währungen, wirft komplexe Fragen auf.

3.28.4 Wichtigste rechtliche Risiken

Zu den rechtlichen Risiken zählen Unsicherheiten in der steuerlichen Einordnung virtueller Transaktionen, die Gefahr von Steuerumgehung durch anonyme oder dezentrale Plattformen und die Unklarheit über steuerliche Pflichten bei der Nutzung von Kryptowährungen. Zudem können Missverständnisse oder Unklarheiten bei der Umsatzsteuerpflicht von virtuellen Gütern zu rechtlichen Konflikten führen.

3.28.5 Best Practice

Gesetzeskonforme Handlungen umfassen die ordnungsgemäße Deklaration von Einkünften aus dem Metaverse, die Einhaltung von KYC-Vorschriften bei steuerpflichtigen Transaktionen und die fristgerechte Abführung der Umsatzsteuer. Klare Verträge und vollständige Aufzeichnungen helfen ebenfalls, steuerliche Pflichten zu erfüllen.

3.28.6 Worst Practice

Gesetzeswidrig sind die absichtliche Verschleierung von Einkünften, das Unterlassen der Umsatzsteueranmeldung bei steuerpflichtigen Vorgängen und die Nutzung von Steuerparadiesen zur Umgehung der Steuerpflicht. Solche Handlungen können zu erheblichen steuerlichen Nachforderungen und Strafen führen.

3.29 Urheberrecht

3.29.1 Rechtsvorschriften im Rechtsgebiet

Die Rechtslage zum Urheberrecht im Metaverse stützt sich auf das Urheberrechtsgesetz (UrhG), das urheberrechtlichen Schutz für Werke gewährleistet, die als persönliche geistige Schöpfungen gelten. Dazu zählen Software, grafische Darstellungen, Musik und andere digitale Inhalte. Besondere Beachtung finden auch § 16 UrhG (Vervielfältigungsrecht) und § 19a UrhG (Recht auf öffentliche Zugänglichmachung), die auf digitale Schöpfungen im Metaverse anwendbar sind. Der Schutz gilt unabhängig von der physischen oder virtuellen Natur des Werks.

3.29.2 Geltende Grundprinzipien

Grundprinzipien umfassen die Schöpfungshöhe, die geistige Eigenleistung des Urhebers und den Schutz der Verwertungsrechte. Urheberpersönlichkeitsrechte wie das Recht auf Namensnennung oder Schutz vor Entstellung spielen ebenfalls eine wichtige Rolle. Im Metaverse bleibt das Territorialitätsprinzip relevant, sodass nationale Rechte nur bei lokalem Bezug greifen. Auch die Übertragbarkeit von Nutzungsrechten wird streng geregelt, um den Schutz des Urhebers zu gewährleisten.

3.29.3 Prioritäre juristische Fragestellungen im Kontext Urheberrecht

Die zentralen Fragestellungen betreffen die urheberrechtliche Einordnung von NFTs und digitalen Zwillingen, die Frage nach der Schutzfähigkeit neuer digitaler Kreationen und die Durchsetzung von Urheberrechten in globalen, oft anonymen virtuellen Umgebungen. Die Abgrenzung zwischen originärer Schöpfung und Nutzung fremder Werke ist dabei besonders komplex, insbesondere wenn Werke digital nachgebildet oder transformiert werden.

3.29.4 Wichtigste rechtliche Risiken

Rechtliche Risiken bestehen in der Verletzung von Verwertungsrechten durch unautorisierte Nutzung oder Nachahmung, der mangelnden Durchsetzbarkeit von Rechten in dezentralen Plattformen und Unsicherheiten in der Einordnung virtueller Werke. Hinzu kommt die Gefahr, dass unklare Lizenzbedingungen zu Streitigkeiten führen, insbesondere bei der Nutzung von NFTs und digitalen Inhalten.

3.29.5 Best Practice

Gesetzeskonforme Handlungen umfassen die Nutzung urheberrechtlich geschützter Werke mit entsprechender Lizenz, die Einhaltung der Bedingungen für die öffentliche Zugänglichmachung und die Schaffung originärer Werke, die die erforderliche Schöpfungshöhe erreichen. Die transparente Lizenzierung von Werken im Metaverse ist ebenfalls ein wesentlicher Bestandteil rechtmäßigen Handelns.

3.29.6 Worst Practice

Gesetzeswidrig sind unautorisierte Vervielfältigungen und die öffentliche Zugänglichmachung urheberrechtlich geschützter Werke ohne Zustimmung des Rechteinhabers. Ebenfalls unzulässig ist die Verwendung geschützter Werke in digitalen Zwillingen oder NFTs ohne entsprechende Lizenz. Manipulationen oder Missbrauch durch die Umgehung technischer Schutzmaßnahmen stellen weitere häufige Verstöße dar.

3.30 Verbraucherschutzrecht

3.30.1 Rechtsvorschriften im Rechtsgebiet

Die Rechtslage zum Verbraucherschutzrecht im Metaverse wird durch bestehende Vorschriften des BGB, insbesondere die §§ 312 ff., geregelt, die Fernabsatzverträge und elektronische Vertriebsformen betreffen. Zusätzlich greifen die neuen Regelungen der §§ 327 ff. BGB, die auf digitale Produkte anwendbar sind. Europäische Vorschriften wie die Verbraucherrechte-Richtlinie und der Digital Services Act (DSA) ergänzen den Schutzrahmen. Der Betrieb von Metaverse-

Plattformen fällt regelmäßig unter diese Normen, da es sich um digitale Dienstleistungen handelt.

3.30.2 Geltende Grundprinzipien

Grundprinzipien des Verbraucherschutzrechts umfassen Transparenz, Informationspflichten und den Schutz vor Übervorteilung. Verbraucher haben Anspruch auf klare Informationen über Vertragsbedingungen, Preise und Rechte wie das Widerrufsrecht. Anbieter müssen sicherstellen, dass digitale Produkte mangelfrei bereitgestellt werden und die Nutzerrechte uneingeschränkt gewahrt bleiben. Technologische Entwicklungen wie virtuelle Avatare und immersive Umgebungen dürfen die Entscheidungsfreiheit der Verbraucher nicht beeinträchtigen.

3.30.3 Prioritäre juristische Fragestellungen im Kontext Verbraucherschutzrecht

Die wichtigsten Fragestellungen umfassen die Anwendbarkeit des Verbraucherschutzrechts auf virtuelle Güter, die Gewährleistung eines effektiven Widerrufsrechts und die Einhaltung der Informationspflichten durch Plattformbetreiber. Zudem stellt sich die Frage, wie personalisierte Werbung und mögliche Überrumpelungsgefahren in virtuellen Welten reguliert werden können, um die Rechte der Verbraucher zu wahren.

3.30.4 Wichtigste rechtliche Risiken

Rechtliche Risiken ergeben sich aus der mangelnden Transparenz bei Verträgen über digitale Güter, der potenziellen Manipulation durch personalisierte Werbung und der unzureichenden Umsetzung von Gewährleistungsrechten bei Mängeln virtueller Produkte. Zudem können die dezentralen und oft anonymen Strukturen des Metaverse die Durchsetzung von Verbraucherrechten erschweren.

3.30.5 Best Practice

Gesetzeskonform sind Handlungen wie die Bereitstellung umfassender Informationen über digitale Produkte gemäß Art. 246a EGBGB, die transparente Gestaltung von Vertragsbedingungen und die Einhaltung der Vorschriften zur Gewährleistung. Plattformbetreiber können auch durch technische Maßnahmen sicherstellen, dass Verbraucherrechte leicht ausgeübt werden können.

3.30.6 Worst Practice

Gesetzeswidrig sind die bewusste Täuschung oder Irreführung von Verbrauchern, etwa durch intransparente Geschäftsbedingungen oder die Umgehung von Informationspflichten. Ebenso

unzulässig ist die Einschränkung von Gewährleistungsrechten oder die Manipulation von Kaufentscheidungen durch sogenannte Dark Patterns. Diese Praktiken können zu rechtlichen Konsequenzen für Anbieter und Plattformbetreiber führen.

3.31 Versicherungsrecht

3.31.1 Rechtsvorschriften im Rechtsgebiet

Das Versicherungsrecht im Metaverse basiert auf den allgemeinen Regelungen des Versicherungsvertragsgesetzes (VVG) und den aufsichtsrechtlichen Vorgaben der BaFin, insbesondere den „Versicherungsaufsichtsrechtlichen Anforderungen an die IT“. Zusätzlich gelten internationale Regelungen wie die Datenschutz-Grundverordnung (DS-GVO), die Anforderungen an den Umgang mit personenbezogenen Daten im Metaverse stellt. Für Cyberversicherungen sind die „Allgemeinen Versicherungsbedingungen für die Cyberrisiko-Versicherung (AVB Cyber)“ des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) relevant. Zudem ist der Vorschlag der EU-KI-Verordnung für Versicherer, die KI-Systeme im Metaverse einsetzen, von Bedeutung.

3.31.2 Geltende Grundprinzipien

Das Versicherungsrecht im Metaverse folgt den Grundsätzen der Transparenz, Fairness und Sicherheit. Versicherer müssen Risiken präzise bewerten und transparent darstellen. Der Schutz der Versicherungsnehmer vor übermäßigen technischen oder rechtlichen Hürden bei Schadensmeldungen oder Vertragsabschlüssen ist essenziell. Versicherungsunternehmen sind verpflichtet, Risiken wie Cyberangriffe und Datenverluste durch umfassende Policen abzudecken. Das Prinzip der Datenminimierung und der Schutz personenbezogener Daten spielen im Metaverse eine besondere Rolle.

3.31.3 Prioritäre juristische Fragestellungen im Kontext Versicherungsrecht

Die zentralen Fragen umfassen die Versicherbarkeit von Risiken im Metaverse, insbesondere durch Cyberversicherungen, die Deckung von Schäden bei virtuellen Objekten wie NFTs und die Einbindung von digitalen Zwillingen in die Risikobewertung. Welche Haftungsfragen ergeben sich bei Hackerangriffen oder Manipulationen im Metaverse? Wie können Versicherungsunternehmen KI-gestützte Technologien rechtssicher einsetzen, und wie lässt sich die Identifikation von Versicherungsnehmern gewährleisten? Die Anwendung bestehender Vorschriften auf virtuelle Schadensfälle und die Gestaltung neuer Versicherungsprodukte sind weitere wesentliche Themen.

3.31.4 Wichtigste rechtliche Risiken

Ein zentrales Risiko liegt in der Unsicherheit über die rechtliche Einordnung virtueller Vermögenswerte und deren Versicherungsschutz. Hackerangriffe auf VR-Systeme oder NFTs können zu Datenverlusten führen, die oft schwer zu bewerten sind. Die Nutzung KI-basierter Systeme kann bei unzureichender Regulierung oder Transparenz zu rechtlichen Konflikten führen. Zudem besteht die Gefahr, dass Versicherer durch nicht standardisierte Bedingungen oder uneinheitliche Vertragsgestaltung rechtliche Probleme bei der Schadensregulierung bekommen.

3.31.5 Best Practice

Gesetzeskonform sind die Entwicklung und der Vertrieb von Versicherungsprodukten, die den Anforderungen des VVG und der BaFin entsprechen. Dazu gehören Cyberversicherungen mit klar definierten Deckungsbereichen für Risiken im Metaverse, etwa den Verlust digitaler Vermögenswerte. Versicherer, die Metaverse-Technologien für Kundens Schulungen oder Schadensabwicklungen einsetzen, müssen datenschutzrechtliche Vorgaben wie die DS-GVO beachten. Die transparente Kommunikation von Versicherungsbedingungen, etwa über digitale Avatare, ist ebenfalls rechtmäßig.

3.31.6 Worst Practice

Rechtswidrig ist die unzureichende Abdeckung von Risiken in Policen, die explizit im Metaverse auftreten können, wie etwa Schäden durch VR-Hardware oder NFTs. Auch die Verarbeitung personenbezogener Daten ohne Zustimmung oder die nicht transparente Nutzung von KI-Systemen im Versicherungsprozess verstoßen gegen geltende Regelungen. Versicherungsverträge, die keine ausreichenden Informationen über ihre Bedingungen enthalten oder auf intransparente Weise zustande kommen, sind ebenfalls unzulässig.

3.32 Vertragsrecht

3.32.1 Rechtsvorschriften im Rechtsgebiet

Die Rechtslage zum Vertragsrecht im Metaverse orientiert sich an bestehenden Normen des BGB, insbesondere den Regelungen zu Dienst-, Werk-, Kauf- und Mietverträgen, angepasst durch die §§ 327 ff. BGB für digitale Inhalte und Dienstleistungen. Verträge im Metaverse betreffen typischerweise Nutzungsverhältnisse zwischen Plattformanbietern und Nutzern sowie Erwerbsverhältnisse, etwa bei NFTs oder virtuellen Objekten. Die dezentrale Organisation vieler Plattformen, etwa durch DAOs, erschwert die eindeutige Identifikation von Vertragspartnern und die Rechtsdurchsetzung.

3.32.2 Geltende Grundprinzipien

Grundprinzipien umfassen die Vertragsfreiheit, den Schutz des Verbrauchers und die Erfüllung der vereinbarten Leistung. Nutzer erhalten oft lediglich ein zeitlich begrenztes Nutzungsrecht, was einen Unterschied zu klassischen Kaufverträgen darstellt. Transparenz und klare Vertragsgestaltung sind essenziell, um die Interessen der Parteien zu wahren. Die Gültigkeit von Verträgen ist trotz virtueller Natur der Gegenstände gewährleistet, solange die rechtlichen Voraussetzungen erfüllt sind.

3.32.3 Prioritäre juristische Fragestellungen im Kontext Vertragsrecht

Wichtige Fragestellungen betreffen die Qualifikation von Verträgen über NFTs und digitale Güter, die Rechte der Nutzer bei Störungen, etwa Serverausfällen, und die Verbindlichkeit von Vereinbarungen in anonymen oder dezentral organisierten Systemen wie DAOs. Insbesondere die Durchsetzung von Ansprüchen gegen internationale Plattformbetreiber stellt eine Herausforderung dar.

3.32.4 Wichtigste rechtliche Risiken

Rechtliche Risiken bestehen in der unsicheren Einordnung der Vertragstypen, was zu Streitigkeiten über Rechte und Pflichten führen kann, in der Schwierigkeit der Durchsetzung von Rechten bei Ausfall des Metaverse und in mangelnder Transparenz bei den Bedingungen für digitale Güter und Dienstleistungen. Nutzer können bei unklaren Regelungen leicht benachteiligt werden.

3.32.5 Best Practice

Gesetzeskonforme Handlungen umfassen die transparente Gestaltung und Dokumentation von Nutzungsbedingungen, die Einhaltung der §§ 327 ff. BGB für digitale Inhalte und die Nutzung der Plattformen im Rahmen der vereinbarten Rechte. Verträge sollten klare Angaben über die Nutzungsdauer und -bedingungen enthalten, um Konflikte zu vermeiden.

3.32.6 Worst Practice

Gesetzeswidrig sind die unklare oder irreführende Gestaltung von Nutzungsbedingungen, die ungerechtfertigte Einschränkung von Nutzungsrechten durch Plattformbetreiber und die Nutzung manipulativer Techniken, um Nutzer zu Vertragsabschlüssen zu drängen. Solche Praktiken können rechtliche Konsequenzen nach sich ziehen und das Vertrauen der Nutzer in die Plattformen schädigen.

3.33 Werberecht

3.33.1 Rechtsvorschriften im Rechtsgebiet

Das Werberecht im Metaverse wird durch bestehende nationale und europäische Vorschriften geregelt. In Deutschland sind das Gesetz gegen den unlauteren Wettbewerb (UWG) und das Telemediengesetz (TMG) zentral. Auf europäischer Ebene greift der Digital Services Act (DSA), der insbesondere Transparenzanforderungen an Plattformen und Werbetreibende stellt. Zusätzlich gelten spezifische Regelungen zur Kennzeichnung von Werbung, beispielsweise aus der EU-Richtlinie über unlautere Geschäftspraktiken. Internationale Regelungen sind ebenfalls relevant, da das Metaverse global agiert und Werbetreibende nationale Besonderheiten berücksichtigen müssen.

3.33.2 Geltende Grundprinzipien

Die Grundprinzipien des Werberechts umfassen die Transparenz, Fairness und Vermeidung von Irreführung. Werbung muss klar als solche gekennzeichnet werden, um Schleichwerbung zu verhindern. Die Angaben in Werbeaussagen dürfen weder irreführend noch unzutreffend sein, müssen jedoch gleichzeitig alle für eine Kaufentscheidung wesentlichen Informationen enthalten. Ein weiteres Prinzip ist der Schutz des Wettbewerbs, um Monopolbildung oder gezielte Behinderungen anderer Marktteilnehmer zu verhindern. Auch kulturelle Sensibilitäten gewinnen im internationalen Kontext des Metaverse an Bedeutung.

3.33.3 Prioritäre juristische Fragestellungen im Kontext Werberecht

Im Metaverse ergeben sich neue Fragestellungen: Wie lässt sich sicherstellen, dass Werbung transparent und eindeutig gekennzeichnet ist, insbesondere bei immersiven Formaten wie Virtual Reality oder In-Game-Werbung? Welche Standards gelten für Influencer-Marketing, wenn Avatare Produkte bewerben? Auch die Berücksichtigung internationaler Unterschiede, etwa bei der rechtlichen Zulässigkeit bestimmter Werbeinhalte, ist entscheidend. Zudem stellt sich die Frage, wie datengetriebene Werbung im Einklang mit Datenschutzvorschriften gestaltet werden kann, insbesondere wenn KI-basierte Systeme verwendet werden.

3.33.4 Wichtigste rechtliche Risiken

Ein zentrales Risiko besteht in der fehlenden oder unzureichenden Kennzeichnung von Werbung, die zu Schleichwerbung führen kann. Irreführende Werbeaussagen oder das gezielte Ausnutzen von Nutzerunwissenheit durch „Dark Patterns“ bergen rechtliche Konflikte. Internationale Werbung kann zu Haftungsrisiken führen, wenn Inhalte in einem Land erlaubt, in einem

anderen jedoch verboten sind. Auch datenschutzrechtliche Verstöße, etwa durch personalisierte Werbung ohne Einwilligung, stellen ein erhebliches Risiko dar.

3.33.5 Best Practice

Gesetzeskonform ist die transparente Kennzeichnung von Werbung, beispielsweise durch klare Hinweise oder Markierungen in virtuellen Umgebungen. Die Einhaltung der Anforderungen des UWG und DSA, wie die Offenlegung von Sponsoring oder Produktplatzierungen, ist ebenfalls erforderlich. Plattformbetreiber, die Mechanismen zur Kontrolle und Überwachung von Werbeeinhalten implementieren, agieren rechtmäßig. Werbetreibende können rechtmäßige datengetriebene Werbung schalten, wenn die Anforderungen der DS-GVO, insbesondere zur Einwilligung, erfüllt sind.

3.33.6 Worst Practice

Gesetzeswidrig ist jede Form von Schleichwerbung oder intransparenter Werbung, etwa das Verstecken von Sponsoring-Informationen. Irreführende Werbeaussagen oder das Verschweigen wesentlicher Informationen verstoßen ebenfalls gegen das UWG. Unzulässig ist die gezielte Manipulation von Nutzern durch irreführende Designelemente („Dark Patterns“). Schließlich sind Verstöße gegen Datenschutzanforderungen, wie die nicht autorisierte Verarbeitung personenbezogener Daten für Werbezwecke, ebenfalls rechtswidrig.

3.34 Wettbewerbs- und Kartellrecht

3.34.1 Rechtsvorschriften im Rechtsgebiet

Die Rechtslage zum Wettbewerbs- und Kartellrecht im Metaverse wird durch europäische und nationale Vorschriften geprägt, insbesondere durch die Art. 101 und 102 AEUV, die das Kartellverbot und das Missbrauchsverbot regeln, sowie die §§ 1 und 19 GWB, die ähnliche Prinzipien auf nationaler Ebene anwenden. Ergänzt werden diese durch den Digital Markets Act (DMA) und das GWB-Digitalisierungsgesetz, die Plattformbetreiber stärker regulieren, und durch Vorgaben zur Fusionskontrolle wie der EU-Fusionskontrollverordnung.

3.34.2 Geltende Grundprinzipien

Grundprinzipien umfassen den Schutz des freien Wettbewerbs, die Verhinderung von Marktverzerrungen und die Sicherstellung von Innovation und Verbraucherschutz. Unternehmen dürfen ihre marktbeherrschende Stellung nicht missbrauchen, und Vereinbarungen, die den Wettbewerb beschränken, sind unzulässig. Besondere Bedeutung hat die Interoperabilität, um Lock-in-Effekte und eine Dominanz weniger Plattformen zu verhindern.

3.34.3 Prioritäre juristische Fragestellungen im Kontext Wettbewerbs- und Kartellrecht

Wichtige Fragestellungen betreffen die Abgrenzung relevanter Märkte im Metaverse, etwa bei der Bewertung neuer Geschäftsmodelle oder Plattformen, die Regulierung von Fusionsvorhaben wie „Killer-Akquisitionen“, bei denen Konkurrenten aufgekauft werden, und die Einhaltung von Interoperabilitätsstandards, um offene Märkte und Innovation zu fördern.

3.34.4 Wichtigste rechtliche Risiken

Zu den rechtlichen Risiken zählen die Gefahr der Monopolisierung durch große Plattformbetreiber, die gezielte Behinderung von Mitbewerbern durch exklusive Standards und die Verstärkung von Marktverzerrungen durch ungerechte Vorteile für marktbeherrschende Unternehmen, etwa durch Self-Preferencing oder den Zugang zu Big Data.

3.34.5 Best Practice

Gesetzeskonform sind Kooperationen zur Standardisierung, sofern sie Effizienzgewinne fördern und den Wettbewerb nicht einschränken, die Einhaltung der Vorgaben des DMA durch Plattformbetreiber und die transparente Gestaltung von Fusionen unter Berücksichtigung kartellrechtlicher Vorgaben. Interoperabilität fördert zudem den fairen Wettbewerb.

3.34.6 Worst Practice

Gesetzeswidrig sind Absprachen, die den Wettbewerb beschränken, etwa Preisabsprachen oder exklusive Zugangsbarrieren, der Missbrauch einer marktbeherrschenden Stellung, etwa durch Diskriminierung von Mitbewerbern, und der Aufbau geschlossener Standardsysteme, die Innovation und den Marktzugang neuer Akteure verhindern. Solche Verstöße führen oft zu erheblichen Sanktionen und Auflagen.

4. Literatur

- [01] Beck; Roggel, ArbRAktuell 2022, 631: Arbeitsrecht im Metaverse, in: ArbRAktuell 2022, 631
- [02] Bender-Paukens; Werry, ZD 2023, 127: Datenschutz im Metaverse, in: ZD 2023, 127
- [03] Engelhardt, C.; at al.: Metaverse – ein neuer Rechtsraum. Aktuelle Regelungen, Herausforderungen und Lösungsansätze. Baker Tilly, Düsseldorf, 2022
- [04] von Fuchs, GRUR-Prax 2019, 104: Die Marke in der virtuellen Realität, GRUR-Prax 2019, 104

- [05] Gaff, L.: Datenschutz bei Virtual und Augmented Reality, 2022
- [06] Gola P.; Heckmann D.: DS-GVO DS-GVO BDSG, 3. Aufl. 2022
- [07] Günther; Böglmüller; Gerigk: NZA 2022, 1509: Arbeitsrechtliche Herausforderungen des Metaverse, in: NZA 2022, 1509
- [08] Hilgert, CR 2017, 472 Augmented Reality, CR 2017, 472
- [09] Leupold; Wiebe; Glossner; Hilgert: IT-Recht, Teil 17 Hilgert, in: Leupold/Wiebe/Glossner, IT-Recht, 4. Aufl. 2021, Teil 17: Augmented Reality
- [10] Kaulartz; Schmid; Müller-Eising: RD 2022, 521 Das Metaverse – eine rechtliche Einführung, in: RD 2022, 521
- [11] Madiega, T.; Car, P.; Niestadt, M.: Metaverse. Opportunities, risks and policy implications. EPRS | European Parliamentary Research Service, European Union: Strasbourg, 2022
- [12] Tann, GRUR 2022, 1644
- [13] Markenrechtlicher Schutz im Metaverse, in: GRUR 2022, 1644
- [14] Günther; Böglmüller; Gerigk: NZA 2022, 1509: Arbeitsrechtliche Herausforderungen des Metaverse, in: NZA 2022, 1509
- [15] Council of the European Union: Metaverse - Virtual World, Real Challenges, March 2022
- [16] Bundesnetzagentur: Metaverse. Status, Perspektiven für die Standardisierung und Regulierung, July 2023
- [17] European Commission: Next Generation Virtual Worlds, July 2023
- [18] Rosenberg, Louis B. (Chief Scientist, Unanimous AI): Regulation of the Metaverse: A Roadmap, March 2022
- [19] Roth, M.; Just, K.: Luther Whitepaper 02.2023. Metaverse. Unyer Global Advisors, Luther Rechtsanwaltsgesellschaft mbH, Köln, 2023
- [20] Steege, Chibanguza: Metaverse Rechtshandbuch. Nomos-Verlag, Baden-Baden: 2023
- [21] Wagner; Holm-Hadulla; Ruttloff: Metaverse und Recht. Vahlen / C.H. Beck, München: 2023
- [22] Völzow, C.: Rechtsmonitor XR für die Unternehmenspraxis. Studie Stand: Juli 2023. Anwendungen der Virtual und Augmented Reality und rechtliche Anforderungen – ein Praxischeck. vbw Vereinigung der Bayerischen Wirtschaft e. V., München, 2023
- [23] Wenzel, G.; Manca, T.; Braun, S.: Regulierung des Metaversums. Analyse rechtlicher Aspekte virtueller und erweiterter Realitäten aus Innovationsperspektive. Riedel, O.; Hölzle, K.; Bauer, W. (Hrsg.), Fraunhofer IAO, Stuttgart, 2024

5. Impressum

Verantwortlich für die Inhalte dieser Publikation ist das Virtual Dimension Center (VDC). Die Inhalte wurden mit größter Sorgfalt erstellt. Für die Richtigkeit, Vollständigkeit und Aktualität der Inhalte kann jedoch keinerlei Gewähr übernommen werden. Die Inhalte unterliegen dem deutschen Urheberrecht. Die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung außerhalb der Grenzen des Urheberrechts bedürfen der schriftlichen Zustimmung des Erstellers.

Verantwortlich für den Inhalt:

Virtual Dimension Center (VDC) Fellbach

Kompetenzzentrum für Virtuelle Realität und kooperatives Engineering w.V.

Prof. Dr.-Ing. Dipl.-Kfm. Christoph Runde

Ioannis Alexiadis, M.Sc.

Auberlenstr. 13

70736 Fellbach

URL: www.vdc-fellbach.de

VIRTUAL DIMENSION CENTER



Kontakt:

Tel.: +49(0)711 58 53 09-0

Fax : +49(0)711 58 53 09-19

Email: info@vdc-fellbach.de

6. Förderhinweis

Die vorgestellten Arbeiten entstanden im Rahmen des Projekts "*Digitallotse Wirtschaft 4.0 - Technologiewerkstatt*" welches durch das Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg gefördert wird.