C. Rechtliche Untersuchung von Interoperabilität

Mark D. Cole/Christina Etteldorf

Bevor eine eingehende Analyse des geltenden Rechtsrahmens für unterschiedliche Interoperabilitätsvorgaben erfolgt, wird ein Überblick vorangestellt, der sich mit den **relevanten Rahmenbedingungen** befasst, die unabhängig von den jeweils in unterschiedlichen Rechtsgebieten verankerten Interoperabilitätsbestimmungen gelten. Interoperabilität kann nämlich nicht losgelöst von primärrechtlichen Rahmenbedingungen der EU, verfassungsrechtlichen Grundsätzen oder anderen Bestimmungen im jeweils betroffenen Rechtsgebiet geschaffen werden, was mögliche Begrenzungen der Nutzbarkeit von Interoperabilität als Lösung für die oben beschriebenen Schieflagen bedeuten kann. Da dies auch für die Förderung von Interoperabilitätslösungen auf freiwilliger Basis gelten kann, sind die Rahmbedingungen und ihre Auswirkungen auch im Hinblick auf die Effektivität und Umsetzbarkeit möglicher Interoperabilitätsregeln oder -ansätze – auch unter dem Gesichtspunkt der Medienvielfalt – mitzudenken.

Im Anschluss an die Darstellung der rechtlichen Grenzen bzw. Voraussetzungen von Interoperabilitätsanforderungen erfolgt eine umfassende Analyse des **geltenden rechtlichen Rahmens zur Interoperabilität**. Dabei werden diejenigen Bestimmungen und Bereiche untersucht, in denen tatsächlich eine Interoperabilität von Systemen angeordnet wird. Datenportabilität wird insoweit als Teilaspekt von Interoperabilität betrachtet.[139] Untersucht werden eingehend die relevanten Regeln des Wettbewerbsrechts, des Telekommunikationsrechts und des Datenschutzrechts. Dazu werden auch rechtsvergleichend die Bestimmungen und Ansätze außerhalb des nationalen Rahmens einbezogen, sodass jeder Teilbereich unterteilt ist in den Rechtsrahmen der USA, der EU und Deutschlands. Dem zuerst dargestellten Wettbewerbsrecht, insbesondere den Regeln auf EU-Ebene, kommt besondere Bedeutung zu, da es Weichenstellungen enthält, die auch auf nationaler Ebene sowie in anderen Staaten aufgegriffen werden. Im Anschluss an die drei vornehmlich relevanten Rechtsgebiete werden ergän-

139 Zur Erläuterung des Zusammenhangs vgl. unten C.IV.

zend Einblicke in andere Rechtsgebiete und Sektoren gegeben, in denen Interoperabilität ebenfalls eine Rolle spielt. Abschließend werden nach der Analyse geltender Bestimmungen wichtige **aktuelle Diskussionsansätze bzw. Legislativvorhaben** dargestellt, da aus diesen wiederum Erkenntnisse für mögliche weitere Vorschläge in der Zukunft abgeleitet werden können. Neben den USA und dem Vereinigten Königreich sind es Entwicklungen in Frankreich, Australien und China, die hervorgehoben werden, bevor ein Überblick über die Diskussionslage in Deutschland hinsichtlich möglicher neuer rechtlicher Verankerungen von Interoperabilitätsvorgaben erfolgt.

I. Rechtliche Grenzen und Voraussetzungen von Interoperabilitätsanforderungen

1. Primär- und verfassungsrechtliche Implikationen

Auf unionsprimär- und verfassungsrechtlicher Ebene betreffen rechtliche Rahmenbedingungen zunächst grundrechtlich und grundfreiheitlich geschützte Interessen. Die Herstellung von Interoperabilität zwischen zwei oder mehr Systemen erfordert eine Zusammenarbeit zwischen diesen, womit eine wechselseitige Einwirkung auf Rechtspositionen einhergehen kann. Aufgrund der vielgestaltigen denkbaren Konstellationen im medienrechtlichen Zusammenhang sind möglicherweise Grundrechte und Grundfreiheiten ebenfalls in vielfältiger Weise betroffen.

Die Herstellung von Interoperabilität durch Vermittlungsdienste – ob horizontal untereinander oder vertikal mit anderen Dienstarten – kann die Anbieter dieser Dienste zunächst in ihrer Eigentumsfreiheit bzw. unternehmerischen Freiheit und Berufsfreiheit, inklusive der vertraglichen Freiheit, tangieren, die in Art. 12 und 14 des Grundgesetzes (GG)[140], Art. 15, 16 und 17 der Charta der Grundrechte der Europäischen Union (Grundrechtecharta, GRC)[141] und auch Art. 1 des Protokolls Nr. 1 zur

140 Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100–1, veröffentlichten bereinigten Fassung, das zuletzt durch Art. 1 des Gesetzes vom 19. Dezember 2022 (BGBl. I S. 2478) geändert worden ist.

141 Charta der Grundrechte der Europäischen Union, OJ C 202, 7.6.2016, S. 389–405.

Europäischen Menschenrechtskonvention (EMRK)[142] gewährleistet sind.[143] Grundfreiheitliche Implikationen betreffen vor allem die Dienstleistungsfreiheit nach Art. 56 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)[144], die den freien Verkehr auch von Vermittlungsdiensten im Binnenmarkt schützt. Die wie auch immer gestaltete Öffnung einer Schnittstelle oder die Nutzung eines bestimmten Standards kann auch mit der Offenbarung von Geschäftsgeheimnissen oder sonstigen unternehmenseigenen Daten verbunden sein. Auch hat Interoperabilität Kostenfolgen, ggf. können auch Lizenzierungsverpflichtungen die Eigentumsfreiheit berühren. Betrachtet werden muss die Frage der Einschränkung auch hinsichtlich der von den Anbietern verfolgten Geschäftsmodelle, die diese grundsätzlich frei wählen dürfen. Interoperabilitätsanforderungen können die Refinanzierbarkeit und Innovationspotenziale beeinträchtigen. Gerade im hier interessanten Markt richten sich, wie noch detaillierter aufgezeigt wird, gewinnorientierte Geschäftsstrategien der Anbieter regelmäßig auf die gegenteilige Situation von Interoperabilität, nämlich den Ausbau von Netzwerkeffekten und „walled gardens", um eigene Produkte und Dienstleistungen voranzutreiben, was grundsätzlich aber ebenfalls dem Schutz von Grundrechten und Grundfreiheiten unterliegt.

Auch Medienanbieter – als Wirtschaftsteilnehmer – können sich auf die eben genannten Rechte berufen. Der Schutz von Urheberrechten spielt dabei nicht nur im technischen Bereich eine Rolle, sondern ist stärker ausgeprägt, wenn es um die von ihnen erstellten oder lizenzierten Inhalte geht. Medienanbieter können sich zudem auch auf den Schutz der Medienfreiheit nach Art. 5 Abs. 1 GG, Art. 11 GRC und Art. 10 EMRK stützen, die insoweit spezieller zu den Unternehmensrechten steht, als es um (auch) redaktionelle Tätigkeiten geht. Nicht nur kann Interoperabilität dabei die Vorgabe einer bestimmten Art der Ausspielung bedeuten, sondern möglicherweise greift die Orientierung an einem verbindlichen (homogenen) Standard auch in redaktionelle Freiheiten ein. Dabei ist insbesondere die Rolle von

142 Europäische Menschenrechtskonvention, BGBl. 1952 II, S. 685, ber. 953. Die Berufsfreiheit wird hier nicht als einzelnes Recht gewährleistet, findet aber innerhalb der anderen Grundrechte, insbesondere der Eigentumsfreiheit und der Meinungsfreiheit, ihren Ausdruck; vgl. *Blanke*, in: Stern/Sachs, Art. 15, Rn. 14.

143 Im Folgenden wird auf eine Unterscheidung zwischen den unterschiedlichen Rechtsinstrumenten des GG, der GRC und der EMR verzichtet, da sie für die überblickhafte Darstellung der Grundrechtsrelevanz nicht erforderlich ist. Die einzelnen Rechte sind hier ähnlich, und sie sind ähnlich stark gewährleistet.

144 Konsolidierte Fassungen des Vertrags über die Arbeitsweise der Europäischen Union, EU ABl. C 202, 7.6.2016, S. 47–200.

Medien als „public watchdog" – wie sie der Europäische Gerichtshof für Menschenrechte (EGMR) in ständiger Rechtsprechung hervorhebt – zu bedenken. Zur Illustration möglicher Probleme soll eine Situation dienen, bei der z. B. ein Fernsehveranstalter eine bestimmte Reportage kürzen müsste, um einem vorgegebenen (weil interoperablen) Videostandard auf einer der davon erfassten Plattformen zu entsprechen, oder bei der ein Presseverlag die inhaltlichen Richtlinien des die Plattform betreibenden Unternehmens zwingend im Rahmen seiner Beiträge berücksichtigen müsste. Die äußere Beeinflussung aufgrund rechtlicher Vorgaben könnte in solchen Konstellationen in die grundrechtlich geschützte Unabhängigkeit der Berichterstattung eingreifen.

Schließlich können auch Nutzer durch Interoperabilität in ihren Grundrechten betroffen sein. Je nach Anknüpfungspunkt kann sich, wenn es etwa um Interoperabilität von Telekommunikation geht, eine entsprechende Umsetzung auf das Fernmeldegeheimnis auswirken. Art. 10 GG schützt das Recht des Einzelnen gegenüber dem Staat auf Abschirmung der nichtöffentlichen Kommunikation, um den unbeobachteten Austausch und die Weitergabe von Tatsachen, Meinungen und Gedanken zu ermöglichen. Entsprechendes gilt auch für den „Transportprozess" bei Interoperabilität. Das betrifft also einerseits den freien Gedankenaustausch von Individuen ohne Befürchtung einer Offenbarung im Lichte auch der Meinungsfreiheit und andererseits Aspekte der Privatsphäre. Ebenjene Rechte sind ebenfalls gesondert als Grundrechte gewährleistet und können von Interoperabilität betroffen werden. Die Meinungs- und Informationsfreiheit nach Art. 5 GG, Art. 11 Abs. 1 GRC und Art. 10 EMRK erfasst das Recht, seine Meinung frei in Bezug auf Ort und Format zu äußern und sich aus öffentlich zugänglichen Quellen frei zu informieren. Sie erstreckt sich aber auch auf das Recht, seine Meinung nicht (in einem bestimmten Format oder Dienst) zu äußern oder sich nicht aus bestimmten Quellen zu informieren. So kann es der Wahrnehmung der Meinungs- und Informationsfreiheit auch entsprechen, wenn ein Nutzer bspw. auf einem sozialen Netzwerk aktiv sein möchte, seine Inhalte aber nicht innerhalb eines anderen Netzwerks teilen oder Informationen von dort erhalten möchte, weil ihm bspw. die dort geltenden Inhalterichtlinien oder schlicht die Tonalität des Diskurses nicht zusagen.

Das allgemeine Persönlichkeitsrecht nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, das Recht auf Achtung des Privat- und Familienlebens aus Art. 7 GRC und Art. 8 EMRK sowie das Recht auf Schutz personenbezogener Daten aus Art. 8 GRC fokussieren auf Aspekte der Privatsphäre. Die Herstellung von Interoperabilität hängt – je nach Dienst – häufig auch mit der Notwen-

digkeit der Übermittlung personenbezogener Daten zusammen. Bei der Interoperabilität von Messenger-Diensten oder dem netzwerkübergreifenden Posten innerhalb sozialer Netzwerke ist offensichtlich, dass in bestimmtem Umfang auch solche Daten an den Empfangsdienst übermittelt werden müssen. Auch bei anderen Konstellationen, wie etwa einer Interoperabilität von Mediatheken, spielen personenbezogene Daten eine Rolle, wenn Werbung oder redaktionelle Inhalte durch den Dienst personalisiert werden oder der Nutzer entsprechende Profilinformationen vorgegeben hat.

Ob diese Grundrechte tatsächlich beeinträchtigt werden, hängt stark von der rechtlichen Ausgestaltung möglicher Interoperabilitätslösungen ab. So greift ein Anreizsystem oder eine Förderung von Interoperabilität auf freiwilliger Basis, ob durch regulatorische Impulse oder aus der Industrie heraus, bereits nicht oder nur geringfügig in Grundrechte von Medienanbietern oder Vermittlern ein. Für Nutzer käme es – ggf. über eine mittelbare Grundrechtsbindung der Dienste – dann auf die Ausgestaltung solcher freiwilligen Systeme an, insbesondere darauf, ob die Interoperabilität auch aus Sicht der Nutzer freiwillig ist. Gesetzliche Interoperabilitätspflichten hingegen stellen einen intensiven Eingriff in Grundrechte und Grundfreiheiten dar. Sie bedürfen daher auch einer entsprechenden Rechtfertigung, also eines Schutzziels von allgemeinem öffentlichen Interesse bzw. eines gesellschaftlichen Bedürfnisses. Als solche Ziele sind anerkannt worden der Verbraucherschutz – wie er zumindest vorrangig auch den Regeln zu Interoperabilität und Datenportabilität aus dem Telekommunikations- und dem Datenschutzrecht zugrunde liegt – und der Schutz des Wettbewerbs bzw. des Funktionierens des (Binnen-)Markts – wie er die Basis der Regeln im Wettbewerbsrecht bildet.

Insbesondere Vielfaltssicherung ist ein solches dem Gemeinwohl dienendes Ziel, mit dem Eingriffe gerechtfertigt werden können.[145] Der EGMR etwa leitet den Schutz der Medienvielfalt als Grundbedingung aus der Medienfreiheit ab[146] und weist auf die Grundbedingung von Pluralismus

145 Eingehend dazu *Ukrow/Cole/Etteldorf*, Zur Kompetenzverteilung zwischen der Europäischen Union und den Mitgliedstaaten im Mediensektor, Kapitel C.

146 Vgl. hierzu den Standard, den der EGMR aus der EMRK abgeleitet hat und der sich auch im EU- und im nationalen Kontext widerspiegelt: EGMR, Nr. 37374/05, *Társaság a Szabadságjogokért / Ungarn*; Nr. 17207/90, *Informationsverein Lentia u. a. / Österreich*; Nr. 24699/94, *VgT Verein gegen Tierfabriken / Schweiz*; Nr. 13936/02, *Manole u. a. / Moldova*; Nr. 48876/08, *Animal Defenders International / Vereinigtes Königreich*.

für die Demokratie hin[147]. Die Medienvielfaltssicherung hat dabei nicht nur eine abwehrrechtliche Dimension, vielmehr begreift der EGMR die Konventionsstaaten als „ultimative Garanten" des Pluralismus in den Medien, sodass sie einen rechtlichen und praktischen Rahmen schaffen müssen, der den Zugang der Öffentlichkeit zu unparteiischen Informationen und einem Spektrum von Meinungen und Debatten sicherstellt und der u. a. die Vielfalt der politischen Ansichten innerhalb des jeweiligen Staates widerspiegelt.[148] Auch der EuGH erkennt an, dass der Pluralismus der Medien in einem Zusammenhang mit der durch Art. 10 EMRK und Art. 11 GRC garantierten Meinungsfreiheit steht und dass insbesondere eine Kulturpolitik, die das Ziel der Pluralismussicherung als zwingenden Grund des Allgemeininteresses verfolgt, Beschränkungen der Dienstleistungsfreiheit rechtfertigen kann.[149] Eine entscheidende Bedeutung der Ausgestaltung des vielfaltssichernden Rechtsrahmens, insbesondere im Bereich des Rundfunks, ist auch vom Bundesverfassungsgericht (BVerfG) in der Auslegung des Grundgesetzes eindeutig und mit besonderer Betonung anerkannt.[150] Das spielt insbesondere vor dem Hintergrund einer sich rapide verändernden Medienlandschaft fortwährend eine Rolle.[151]

Die Schaffung von Interoperabilitätspflichten muss neben einer entsprechenden Zielrichtung allerdings auch dem Grundsatz der Verhältnismäßigkeit entsprechen; insbesondere muss sie zur Erreichung des Ziels geeignet, erforderlich und angemessen sein. Das verlangt nicht nur eine eingehende Untersuchung der in Aussicht genommenen Regel entlang ihres tatsächlichen Nutzens für Verbraucherschutz, Markt oder Vielfalt, da die Effektivität ein Kriterium der Eignungsprüfung ist. Es erfordert auch eine Gewichtung der widerstreitenden grundrechtlich geschützten Interessen, wobei es

147 EGMR, Nr. 13936/02, *Manole u. a. / Moldova*, Rn. 95

148 EGMR, Nr. 13936/02, *Manole u. a. / Moldova*, Rn. 107.

149 Vgl. hierzu EuGH, Rs. 353/89 – *Kommission / Niederlande*, Rn. 30; Rs. C-288/89 – *Stichting Collectieve Antennevoor-ziening Gouda u. a. / Commissariaat voor de Media*, Rn. 23; Rs. C-148/91 – *Vereniging Veronica Omroep Organisatie / Commissariaat voor de Media*, Rn. 9; Rs. C-23/93 – *TV10 SA / Commissariaat voor de Media*, Rn. 18; Rs. C-368/95 – *Vereinigte Familiapress Zeitungsverlags- und vertriebs GmbH / Heinrich Bauer Verlag*, Rn. 19; Rs. C-250/06 – *United Pan-Europe Communications Belgium SA u. a. / État belge*, Rn. 41; Rs. C-336/07 – *Kabel Deutschland Vertrieb und Service GmbH & Co. KG / Niedersächsische Landesmedienanstalt für privaten Rundfunk*, Rn. 37; Rs. C-87/19 – *TV Play Baltic AS / Lietuvos radijo ir televizijos komisija*, Rn. 38.

150 Zum Rundfunk etwa maßgeblich BVerfGE 73, 118 (118).

151 BVerfG, Urteil des Ersten Senats vom 18. Juli 2018 – 1 BvR 1675/16 –, Rn. 79.

maßgeblich auch darauf ankommt, welche Art von Interoperabilität umgesetzt werden soll und wie. Vor allem spielt hier die Unterscheidung zwischen symmetrischen und asymmetrischen Vorgaben eine Rolle: Während etwa das Marktversagen auch asymmetrische Pflichten nur an bestimmte Anbieter, die wesentlich zum Marktversagen beitragen, zu rechtfertigen vermag (wie im DMA und im europäischen Kodex für die elektronische Kommunikation; vgl. eingehend unten C.II.2.c und C.III.2.a), könnte eine symmetrische und verbindliche Pflicht häufig vor allem für kleine Anbieter unterverhältnismäßig sein.[152] Auch eine partielle oder eine vollständige Interoperabilität wären in der Verhältnismäßigkeit unterschiedlich zu gewichten, da erstere regelmäßig weit weniger einschneidend für unternehmerische Interessen sowie möglicherweise auch für Nutzerinteressen ist. Zudem wäre bei nationalen Ansätzen oder solchen in föderalen Untergliederungen im Rahmen des Unionsrechts zu beachten, dass der EuGH in verschiedenen Zusammenhängen jüngst den Handlungsspielraum der Mitgliedstaaten im Rahmen von Dienstleistungsfreiheitseinschränkungen eher restriktiv ausgelegt hat, wobei sich das für medienvielfaltsbezogene Regelungen anders darstellen kann.[153]

2. Implikationen aus EU-Sekundärrecht und nationalem Recht

Die dargestellten Grundrechte finden regelmäßig auch eine einfachgesetzliche und daher konkretisierende Ausgestaltung im sekundären EU- und im nationalen Recht. Die wichtigsten Aspekte werden daher überblickhaft dargestellt werden, da sie nicht nur den Rechtsrahmen für Interoperabilitätsregeln bestimmen, sondern auch häufig deren Reichweite und Effektivität bedingen.

152 *Monopolkommission*, Telekommunikation 2021, S. 91.

153 EuGH, Urt. v. 3.2.2021, C-555/19 – *Fussl Modestraße Mayr*, ECLI:EU:C:2021:89; wegen sekundärrechtlich entgegenstehender Bedingungen vgl. insbesondere EuGH, Urt. v. 9.11.2023, C-376/22 – *Google Ireland u. a.*, ECLI:EU:C:2023:835. Vgl. aber allgemein zur Problematik der Kompetenzverteilung im Kontext von Medienvielfaltssicherung *Cole/Ukrow/Etteldorf*, Zur Kompetenzverteilung zwischen der Europäischen Union und den Mitgliedstaaten im Mediensektor; *Cole*, in: AfP, 2021, S. 1, 1 ff.

a. Anforderungen aus dem Wettbewerbsrecht

Das Wettbewerbsrecht enthält, wie unten (C.II.) näher ausgeführt wird, selbst Möglichkeiten, von Anbietern mit bestimmter Marktmacht eine Interoperabilität ihrer Dienste zu fordern, und zwar sowohl als Maßnahmenentscheidung im Einzelfall als auch im Wege der Ex-ante-Regulierung.[154] Gleichzeitig sind aber für interoperable Strukturen auch Grenzen aus dem Wettbewerbsrecht zu beachten. Das betrifft vor allem solche aus dem Kartellrecht. Während marktdominante Akteure sich etwa dadurch wettbewerbswidrig verhalten können, dass sie ihre Dienste abschotten, und deshalb nach den Regeln des Wettbewerbsrechts zu Interoperabilität verpflichtet werden können, kann umgekehrt die Interoperabilität nur bestimmter Dienste auch kartellrechtlich bedenklich sein. Das betrifft einerseits das dadurch mögliche Entstehen von „Super-Apps", die (vertikal) zentralisiert Zugriff auf unterschiedliche Dienste ermöglichen, andererseits die Kompatibilität nicht aller, sondern nur bestimmter Dienste (in horizontaler oder vertikaler Richtung).

Dass nur bestimmte Dienste interoperabel sind, kann dabei unterschiedliche Ursachen haben. Wenn eine Interoperabilitätspflicht nicht gesetzlich und neutral vorgegeben ist, sondern die Entscheidung zur Öffnung des Dienstes vom Anbieter selbst kommt, so kann dieser sich in Ausübung seiner unternehmerischen Freiheit dazu entschließen, nur bestimmten anderen Anbietern Schnittstellen zu öffnen, die bspw. bestimmten inhaltlichen Standards entsprechen oder zu bestimmten Unternehmensgruppen gehören. Denkbar ist aber auch, dass Integrationskosten für den interoperablen Standard von einigen, vor allem kleinen Unternehmen nicht getragen werden können (oder wollen) und sie deshalb nicht davon profitieren können. Insoweit ergeben sich aus den unten (E.I.) näher dargestellten Regeln gleichermaßen Grenzen für die Ausgestaltung von Interoperabilität, insbesondere um die Einhaltung von FRAND-Bedingungen[155] sicherzustellen. Zudem erfordert Interoperabilität immer auch ein gewisses Maß an

154 Dazu unten C.II.2. Der DMA auf EU-Ebene wird wegen seiner engen Verbindung und Anknüpfung an Marktverhältnisse im Rahmen dieser Publikation dem Wettbewerbsrecht zugeordnet, obwohl er die Harmonisierung im Rahmen der Binnenmarktregulierung als Rechtsgrundlage hat.

155 Der Begriff der FRAND-Bedingungen (Fair, Reasonable and Non-Discriminatory, also fair, angemessen und diskriminierungsfrei) kommt originär aus dem Patentrecht und beschreibt die Art der Einräumung von Lizenzbedingungen. Er findet aber mittlerweile auch im weiteren Wettbewerbsrecht Erwähnung und Anknüpfungspunkte.

Koordinierung und Kooperation zwischen den beteiligten Unternehmen, was wiederum auch den Bereich kartellrechtswidriger Absprachen betreffen kann, die das Kartellrecht verhindern soll. Finden solche zwischen marktstarken Akteuren statt – wie es bspw. bei einer Interoperabilität sozialer Netzwerke der Fall sein könnte –, könnte das in Konflikt mit Art. 101 AEUV und § 1 UWG geraten.

b. Anforderungen aus dem Telekommunikationsrecht

Neben möglichen Verpflichtungen zur Herstellung von Interoperabilität und zur Zusammenschaltung von Telekommunikationsdiensten (dazu unten E.II.) enthält das Telekommunikationsrecht vor allem auch Sicherheitsanforderungen an die Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste. Sie ergeben sich vorrangig aus Titel V des EKEK und sind auch in Kapitel 10 des deutschen TKG umgesetzt. Auch im Rahmen der Herstellung von Interoperabilität sind sie einzuhalten.

Betreiber sind danach verpflichtet, die Sicherheit ihrer Netze und Dienste zu gewährleisten und Sicherheitsvorfälle zu verhindern bzw. deren Auswirkungen zu minimieren. Diese Maßnahmen sollen unter Berücksichtigung des Standes der Technik ein Sicherheitsniveau der Netze und Dienste gewährleisten, das angesichts des bestehenden Risikos angemessen ist. Das betrifft die physische Sicherheit und Sicherheit des Umfelds und des Materials sowie die Kontrolle des Zugangs zu Netzen und die Netzintegrität, aber auch Mechanismen zur Bewältigung von Sicherheitsvorfällen. Die erfassten Anbieter haben ihre Nutzer kostenlos über besondere und erhebliche Sicherheitsbedrohungen und über Maßnahmen zum Schutz von Kommunikationsinhalten, die sie betreffen können, zu informieren, z. B. über den Einsatz spezieller Software oder von Verschlüsselungsverfahren. Gefördert werden sollen auch eine Ende-zu-Ende-Verschlüsselung sowie erforderlichenfalls die datenschutzfreundliche Ausgestaltung von Voreinstellungen und der Technik insgesamt. Sicherheitsanforderungen erstrecken sich seit der Reform durch den EKEK 2018 auch auf die Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste (u. a. Messenger-Dienste)[156] – dort aber nur begrenzt, weil sie üblicherweise keine tatsächliche Kontrolle der Signalübertragung über die Netze ausüben. Auch sie

156 Zum Begriff unten C.III.2.a(2).

haben aber ein Sicherheitsniveau zu gewährleisten, das dem bestehenden Risiko angemessen ist.

Gerade im Zusammenhang mit der technischen Umsetzung von Interoperabilität bei Messenger-Diensten ist die Aufrechterhaltung der Sicherheit der Dienste, insbesondere der Ende-zu-Ende-Verschlüsselung mit Blick auf die notwendige Entschlüsselung bei der Übertragung, ein vielfach kritisierter Aspekt.[157] Bedenken bestehen also vorwiegend im Hinblick auf die Interoperabilität von Kommunikationsinhalten sowie solchen Inhalten, die (auch) über Telekommunikationsinfrastrukturen übertragen werden.

c. Anforderungen aus dem Datenschutzrecht

Die Herstellung von Interoperabilität zwischen Diensten – ob vertikal oder horizontal – ist regelmäßig mit der Übertragung von Daten verbunden, da Dienste nur auf diesem Weg miteinander kommunizieren können. Weisen solche Daten einen Personenbezug auf, gelten in der EU hierfür die besonderen Regeln zum Schutz solcher Daten nach der DS-GVO und, wenn es um den Datenschutz in der elektronischen Kommunikation geht, nach der e-Privacy-Richtlinie[158] und den nationalen Umsetzungen. In Deutschland gelten ergänzend bzw. konkret diese Regeln umsetzend das Bundesdatenschutzgesetz (BDSG)[159] und das Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG)[160].

157 Dazu auch unten C.II.2.c(9)(d).

158 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), EU ABl. L 201, 31.7.2002, S. 37–47, in der Fassung der Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, EU ABl. L 337, 18.12.2009, S. 11–36.

159 Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Art. 10 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 414) geändert worden ist.

160 Telekommunikation-Telemedien-Datenschutz-Gesetz vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Art. 4 des Gesetzes vom 12. August 2021 (BGBl. I S. 3544; 2022 I S. 1045) geändert worden ist.

Relevant ist das Datenschutzrecht daher in jedem Fall, wenn es um die Interoperabilität von Diensten geht, in deren Zentrum die Kommunikation zwischen Nutzern steht, wie Messenger-Dienste, Chats, soziale Netzwerke oder die unterschiedlichen Arten von Diskussionsforen.[161] Aber auch in solchen Diensten, in deren Rahmen es vorrangig um den Inhaltekonsum geht, etwa bei Video-Sharing-Plattformen, Mediatheken oder anderen Anwendungen von Medienanbietern (bspw. Streaming-Apps, Webradio etc.), sind personenbezogene Daten relevant. So kann es um die Account-Daten (bspw. Name, E-Mail-Adresse etc.), vom Anwender erhobene Nutzerdaten (Gerätedaten, IP-Adressen), beobachtete Daten (bspw. Suchverlauf für Empfehlungssysteme) oder vom Nutzer personalisierte Daten (bspw. Favoriten, Playlists, eingestellte Interessen etc.) gehen, die zum Betrieb des Dienstes oder für Empfehlungen bzw. personalisierte Werbung verwendet werden. Dass auch solche Daten in interoperablen Systemen eine Rolle spielen, also mitübertragen werden, kann jedoch gerade im Interesse der Anbieter und ggf. auch der Nutzer liegen.

Die Grundregeln im Datenschutzrecht setzen für die Verarbeitung solcher Daten – dazu gehört auch deren Übermittlung an einen anderen Verantwortlichen – zunächst eine Rechtsgrundlage voraus. Im Rahmen der mit Interoperabilität verbundenen Datenübertragung kommen dabei insbesondere zwei Rechtsgrundlagen in Betracht: Die Verarbeitung ist aufgrund vertraglicher Zwecke erforderlich oder der Nutzer hat eine wirksame Einwilligung erteilt.[162] Ersteres würde erfordern, dass Interoperabilität fester und wesentlicher Bestandteil des jeweiligen Dienstes ist, der Dienst also ohne Interoperabilitätsfunktion nicht genutzt werden könnte. Soll Interoperabilität bei bestehenden Diensten hergestellt werden (als nachgebesserte Funktion), ist das bereits schwierig. Wenn sogar besondere Kategorien personenbezogener Daten (bspw. solche zur politischen Gesinnung, ethnischen Herkunft, sexuellen Orientierung oder biometrische Daten) übertragen werden, wäre die Berufung auf die Vertragsgrundlage

161 Vgl. zu diesem Komplex auch die Untersuchung des *BKartA*, Sektoruntersuchung Messenger- und Video-Dienste, die sich ausführlich mit den technischen und rechtlichen Rahmenbedingungen für Messenger- und Video-Dienste befasst und dabei einen besonderen Schwerpunkt auf Datenschutz- und Datensicherheitsfragen legt. Umgekehrt wird dabei auch der Frage nachgegangen, ob Interoperabilität zu einem Vorteil hinsichtlich dieser Aspekte führen kann.

162 Dass in diesem Zusammenhang andere Tatbestände greifen, insbesondere die Wahrnehmung berechtigter Interessen (hier: an Interoperabilität) seitens der Anbieter, scheint eher fernliegend.

ausgeschlossen. Die Übertragung solcher besonders geschützter Daten ist jedoch häufig Bestandteil von Individualkommunikation und kann auch bei den anderen genannten Beispielfällen nicht ausgeschlossen werden. Für die elektronische Kommunikation gilt Ähnliches, wonach die Verarbeitung von Daten möglich ist, wenn sie zum Betrieb eines Dienstes zwingend erforderlich ist (bspw. Sicherheits-Cookies) oder der Betroffene eingewilligt hat. Die Datenübertragung könnte dabei nur zum Zwecke der Interoperabilität zwingend erforderlich sein, aber nicht zum Betrieb des gesamten Dienstes. Im Ergebnis bedeutet dies aber, dass regelmäßig eine Einwilligung des Nutzers erforderlich sein wird, die den Bedingungen des Datenschutzrechts entspricht und insbesondere freiwillig und informiert erfolgen muss. Diese Schlussfolgerung deckt sich auch mit den Ausführungen des EuGH in der Rechtssache *Meta platforms*[163], in denen (sogar) für die Datenzusammenführung innerhalb eines Konzerns (hier zwischen Facebook und WhatsApp) das Vorliegen einer Einwilligung vorgegeben wurde. Ob Interoperabilität etabliert werden kann, würde also in den meisten Fällen von einer aktiven Entscheidung des Nutzers abhängig sein, selbst wenn die Infrastrukturen bereits vom Verantwortlichen angeboten werden. Insofern müsste auf der Basis des Datenschutzrechts auch gefordert werden, dass die Interoperabilitätsfunktion innerhalb eines Dienstes aktiv eingeschaltet werden kann bzw. muss,[164] wenn sie individuell gewünscht ist.

Eine solche Einwilligung aktiv einzuholen oder eine Aktivierungsfunktion für Interoperabilität zu integrieren, scheint zunächst ohne großen Aufwand durch den jeweiligen Dienst des konkreten Nutzers umsetzbar. Problematisch ist aber, dass diese Einwilligung sich auch auf die Datenverarbeitung durch den anderen Dienst (im datenschutzrechtlichen Sinn: eines anderen Verantwortlichen) erstrecken muss. Diese Konstellation kann rechtlich konstruiert werden, wie bereits die Regelung zur Datenportabilität nach Art. 20 DS-GVO zeigt.[165] Auch kann die Einwilligung von einem anderen als dem Verantwortlichen eingeholt werden, solange sie dem Verantwortlichen dann zu Beweiszwecken (Art. 7 Abs. DS-GVO) vorliegt, wobei ggf. entsprechende Auftragsverarbeitungsverträge abgeschlossen werden müssten, weil Interoperabilität im Vergleich zu Datenportabilität ein

163 EuGH, C-252/21 – *Meta Platforms*, ECLI:EU:C:2023:537 – Rn. 86 ff. Vgl. zu diesem Verfahren, das seinen Ursprung in einer Entscheidung des BKartA hat, im Detail unten C.II.3.b(3)(d).

164 Das entspricht der Rechtsprechung des EuGH zur Erforderlichkeit einer aktiven Einwilligung; vgl. EuGH, C-673/17 – *Planet 49*, ECLI:EU:C:2019:801.

165 Dazu unten C.IV.2.a.

deutliches „Mehr" bzw. eine komplexere Konstellation betrifft. Allerdings kann sich in dem Zusammenhang als problematisch erweisen, dass verschiedene Dienste auch einen möglicherweise sogar sehr unterschiedlichen Umgang mit der Privatsphäre ihrer Nutzer aufweisen, die „Privacy Policies" also keinesfalls identisch sind. So könnte z. B. der den Messenger-Dienst Threema verwendende Nutzer mit den Verarbeitungszwecken von WhatsApp gerade nicht einverstanden sein, wenn diese Dienste interoperabel wären, oder der Mastodon-Nutzer gerade nicht wollen, dass Instagram seine Daten auf eine bestimmte Art nutzt. Komplexer wird die Situation dadurch, dass einer der interoperablen Dienste Daten außerhalb des EWR verarbeiten könnte, wofür wiederum Sonderregeln gelten, die die Gewährleistung eines Datenschutzniveaus fordern, das dem in der EU geltenden entspricht. Insofern bedürfte es hier zum einen bereits einer informierten Einwilligung, die den Nutzer des „Sendedienstes" genau über die Bedingungen der Datenverarbeitung im Zieldienst informiert. Des Weiteren gelten Transparenzbestimmungen im Datenschutzrecht, also auch außerhalb des Erfordernisses einer informierten Einwilligung, die verlangen, dass der Nutzer bei der Datenerhebung auch über den Umfang und die Zwecke der Verarbeitung seiner Daten zu informieren ist.

Neben diesen Aspekten könnte die grundsätzlichere Frage aufgeworfen werden, ob eine Einwilligung noch freiwillig sein kann, wenn der Nutzer „gezwungen" ist, die Bedingungen auch der Zieldienste zu akzeptieren, um von Interoperabilität zu profitieren. Vergleichbar ist das mit der Diskussion im Wettbewerbsrecht, in der es darum geht, ob die Kopplung der Nutzung eines Dienstes (insb. sozialer Netzwerke) an für den Nutzer einschneidende Privatsphäreneinstellungen (z. B. Zahlen mit Daten) deshalb ein missbräuchliches Verhalten darstellt, weil der Nutzer keine echte Wahl hat, wenn er die Partizipation an diesem Dienst aus Gründen sozialer Interaktion nicht vollständig aufgeben kann.[166] Sehr umstritten ist dabei auch im Datenschutzrecht die Frage, ob und wann Betroffene überhaupt in ein niedrigeres Datenschutzniveau einwilligen können, z. B. um von einer Leistung zu profitieren, die ansonsten datenschutzrechtlich unzulässig wäre. Das Merkmal der erforderlichen „Freiwilligkeit" der Einwilligung liegt dann nicht vor, wenn der Betroffene keine echte Wahl hat. Ein Beispiel wäre etwa das Versenden von Gesundheitsdaten per E-Mail seitens eines Arztes, damit der Patient möglichst schnell seine Untersuchungsergebnisse

166 Dazu unten C.IV.2.a.

erhält. Während das OLG Düsseldorf eine solche Übermittlung, basiert sie auf einer ausdrücklichen Einwilligung, als zulässig betrachtet hat,[167] will die Konferenz der deutschen Datenschutzbehörden eine Einwilligung in ein geringeres Datenschutzniveau oder gar einen Verzicht auf technische und organisatorische Schutzmaßnahmen nur in eng umgrenzten Ausnahmefällen zulassen,[168] insbesondere wenn es um besondere Kategorien personenbezogener Daten wie Gesundheitsdaten geht.

Um eine solche Folge zu vermeiden, müssten entsprechende Schutzvorkehrungen bei Interoperabilitätslösungen vorgesehen werden. Bei bestehenden Interoperabilitätsvorschriften etwa im DMA sind Vorgaben zur Schaffung von Kohärenz mit dem Datenschutzrecht bereits gesetzlich vorgesehen. Möglich wäre es zunächst, den Umfang der Verarbeitung und der verarbeiteten Daten durch den Empfangsdienst zu beschränken. Das würde sich dann innerhalb von Datenschutzbestimmungen auf das „zur Herstellung von Interoperabilität erforderliche Maß" beschränken, was jedoch ohnehin als Grenze bereits aus der DS-GVO ableitbar sein dürfte. Zudem könnte eine Beschränkung der Interoperabilität auf nur bestimmte Funktionen – also eine partielle Interoperabilität – zu diesem Ziel beitragen. Umgekehrt können aber stärkere Einschränkungen zugunsten des Datenschutzes dazu führen, dass weniger Funktionen interoperabel sind und damit die Interoperabilität weniger effektiv oder sinnvoll ist.[169] Diese Auswirkung hängt aber vom jeweiligen Dienst und von der Art von Interoperabilität ab. So wäre etwa die Interoperabilität der Basisfunktionen von Messenger-Diensten einfacher umzusetzen als die Interoperabilität von sozialen Netzwerken oder Empfehlungssystemen, die gerade wesentlich mit personenbezogenen Daten gesteuert werden. Eine weitergehende Möglichkeit wäre die Einigung interoperabler Dienste nicht nur auf einen Interoperabilitätsstandard, sondern auch auf einen gemeinsamen Datenschutzstandard. Abgesehen von der vorhersehbaren Kollision mit Geschäftsmodellen

167 OLG Düsseldorf, 28.10.2021, 16 U 275/20 – MDR 2022, 435.

168 Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DS-GVO auf ausdrücklichen Wunsch betroffener Personen, 24. November 2021, https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf.

169 Eine bislang eher geringe praktische Wirksamkeit des Rechts auf Datenportabilität, das ein Weniger im Vergleich zu Interoperabilität darstellt, lässt sich aufgrund der notwendigen datenschutzrechtlichen Sicherungsbedingungen beobachten. Eingehend dazu unten C.IV.2.a.

(sowohl der mehr datengetriebenen Dienste als auch derer, die sich durch das Angebot besonderer Datensicherheit und Privatsphäre hervorheben), könnte es dadurch zu einem „privacy race to the bottom" kommen. Solche Bedenken über das Absinken des Datenschutzniveaus insgesamt, weil der niedrigste gemeinsame Standard gewählt wird, wurden bereits im Kontext der Schaffung des Rechts auf Datenportabilität geäußert.[170]

Selbst bei Beachtung einer informierten und freiwilligen Einwilligung des Betroffenen, also des Dienste-Nutzers, stellt sich ein weiteres Problem, wenn die personenbezogenen Daten, zu deren Verarbeitung eingewilligt werden muss, nicht nur ihn, sondern auch Dritte betreffen. Hier geht es bei der Interoperabilität von Kommunikationsprozessen vor allem um Kontakt- oder Freundeslisten, wenn diese auch von der Interoperabilität erfasst sein sollen. Eine Interoperabilität von Messenger-Diensten etwa wäre praktisch nicht effektiv, wenn der Nutzer von Dienst A zwar Kontaktdaten von einem anderen Nutzer hätte (bspw. eine Mobilfunknummer), diesen aber bei Dienst B nicht erreichen könnte, weil die beiden Dienste zwar interoperabel sind, aber Kontaktinformationen nicht austauschen können, oder wenn auch Chatverläufe nicht innerhalb beider Dienste abrufbar wären. Auch ein netzwerkübergreifendes Posten in sozialen Netzwerken hat nur dann einen Mehrwert, wenn der Postende seine Freunde/Follower/Abonnenten auch innerhalb anderer Netzwerke erreicht, die sozialen Netzwerke also über diese Daten Informationen austauschen. Dabei ist aber bereits die Information, dass entsprechende Kontakte bestehen, ein personenbezogenes Datum. Um diese Prozesse also datenschutzkonform umzusetzen, wären jeweils beidseitig Einwilligungen erforderlich: Sowohl der Empfänger als auch der Sender müssten sich aktiv für die Interoperabilität entscheiden.

Daneben enthält das Datenschutzrecht Vorschriften zur Gewährleistung von Datensicherheit ähnlich wie bei der Telekommunikation, die sich an alle datenverarbeitenden Unternehmen unabhängig von der Branche richten. Mit Interoperabilität – unabhängig davon, wie diese umgesetzt wird – ist jedenfalls in einem gewissen Maß eine Öffnung von Schnittstellen verbunden, die auch in bösgläubiger Absicht genutzt werden können und

170 Vgl. etwa *Grimmelmann*, in: Iowa Law Review, 2009, S. 1137, 1194, der konstatiert, dass durch Datenportabilität zwar möglicherweise das Ungleichgewicht in vertikalen Machtstrukturen verringert werden kann, aber gleichsam horizontale Privatsphärenproblematiken geschaffen werden.

Dienste daher z. B. für Phishing-Attacken angreifbarer machen.[171] Unberechtigte Datennutzungen wie z. B. im Skandal um Cambridge Analytica oder Hackerangriffe im Facebook-Scraping-Fall von 2021[172] hätten in interoperablen Systemen potenziell weitreichendere Auswirkungen.[173] Art. 32 DS-GVO verpflichtet Verantwortliche und Auftragsverarbeiter dazu, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Das kann u. a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen. Diese Pflicht erstreckt sich sowohl auf den Empfangs- und den Zieldienst bei Interoperabilität als auch auf den Transportvorgang, was gerade in Bezug auf die Verschlüsselung von Kommunikation erhebliche Probleme bereiten dürfte, da sowohl Empfänger als auch Sender über die entsprechenden Schlüssel zur Entschlüsselung verfügen müssten. Im Übrigen unterliegt das erforderliche Niveau an Datensicherheit aber einer gewissen Flexibilität hinsichtlich der zu treffenden Vorkehrungen, was insbesondere unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu beurteilen ist. Im Hinblick auf Interoperabilität könnte sich dabei insbesondere das Instrument der Zertifizierungsverfahren als nützlich erweisen. Betrifft Interoperabilität die elektronische Kommunikation, sind außerdem weitere Anforderungen zu beachten, insbesondere ist die Gewährleistung des Fernmeldegeheimnisses (§ 3 TTDSG) sicherzustellen.

171 Dazu auch eingehend *Barczentewicz*, Privacy and Security Implications of Regulation of Digital Services in the EU and in the US, S. 4 ff.

172 Im April 2021 veröffentlichten Unbekannte die Daten von etwa 500 Millionen Facebook-Nutzern im Darknet, darunter Namen und Telefonnummern. Die Daten hatten die Unbekannten zuvor über einen längeren Zeitraum zunächst unter Ausnutzung der seinerzeitigen Suchfunktionen von Facebook gesammelt, über die es damals wegen einer Sicherheitslücke möglich war, eine Person einer Telefonnummer zuzuordnen, selbst wenn die Anzeige der eigenen Telefonnummer bei Facebook nicht aktiviert war. Vgl. dazu etwa die Sachverhaltsdarstellungen in den vielfach anhängigen und teils bereits entschiedenen Schadensersatzklagen, bspw. OLG Hamm, Urt. v. 15.8.2023 – Az. 7 U 19/23, NJW 2024, 92.

173 So *Doctorow/Cyphers*, Privacy Without Monopoly, S. 28.

d. Anforderungen aus der Netz- und Informationssicherheit

Im Zentrum der Gewährleistung von Netz- und Informationssicherheit, auch als Cybersicherheit bezeichnet, steht die Resilienz von (kritischen) Infrastrukturen gegen Cyberangriffe. Im Dezember 2020 legten die Europäische Kommission und der Europäische Auswärtige Dienst eine neue EU-Strategie für die Cybersicherheit vor.[174] Mit dieser Strategie soll die Widerstandsfähigkeit Europas gegenüber Cyberangriffen gestärkt und gewährleistet werden, damit alle Bürger und Unternehmen in vollem Umfang von vertrauenswürdigen und zuverlässigen Diensten und digitalen Instrumenten profitieren können. Sie basiert auf drei Säulen: (1.) der Resilienz, technologischen Souveränität und Führung; (2.) der operativen Fähigkeit zur Verhinderung, Abschreckung und Reaktion; und (3.) der Zusammenarbeit zur Förderung eines globalen und offenen Cyberspace. Gegenstand der Strategie sind u. a. auch vernetzte Objekte, wie sie im Kontext von Interoperabilitätserwägungen ebenfalls eine Rolle spielen.

Das Thema digitale Souveränität und Resilienz hat im Kontext der geopolitischen Lage u. a. zwischen den USA, China und Europa eine zunehmend internationale Dimension erhalten. Aspekte hiervon spielen auch im Zusammenhang mit Interoperabilität eine Rolle.[175] Sicherheitsbedenken bei Interoperabilität, vorrangig wenn es um Kommunikationsinhalte geht, stehen zwar vorrangig im Kontext der Sicherheit und des Schutzes von Daten natürlicher Personen. Sie lassen sich am Beispiel der Diskussionen um Datentransfers außerhalb des EWR ablesen, insbesondere im Kontext der fortwährenden Streitigkeiten um die richtigen Prozeduren bei Angemessenheitsbeschlüssen und Datenschutzabkommen mit den USA.[176] Einige Aspekte können aber auch die Ebene europäischer und nationaler Sicherheit

174 Joint Communication: The EU's Cybersecurity Strategy for the Digital Decade, JOIN/2020/18 final, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018. Vgl. auch die Übersicht bei *Schmitz-Berndt/Cole*, in: Cybersecurity & Internet Governance, 1, 1, 2022, S. 1–17.

175 Vgl. *WIK-Consult,* Interoperabilitätsvorschriften für digitale Dienste, S. 55. Vgl. dazu auch den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen, COM(2023) 209 final, auf den sich das Europäische Parlament und der Rat bereits Anfang März 2024 geeinigt haben (vgl. Pressemitteilung der Europäischen Kommission vom 6.2.2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1332).

176 Dazu etwa *Gottschalk*, in: EDPL, 2023, S. 448, 448 ff.

betreffen. Die potenziellen sicherheitstechnischen Bedrohungen – und damit korrespondierend auch das Niveau an Sicherheitspflichten – hängt zu einem großen Teil davon ab, wie Interoperabilität ausgestaltet wird. Offene Schnittstellen, wie sie aus der Perspektive des Wettbewerbs wünschenswert sind, sind besonders anfällig für Cybersicherheitsattacken.[177] Durch die bei Interoperabilität erforderliche Öffnung (bspw. bei der Verschlüsselung von Kommunikation) können Sicherheitsstandards gesenkt werden.

Wesentlicher Aspekt in diesem Zusammenhang ist die Nutzung von nicht in der EU angesiedelten Cloud-Diensten und anderen digitalen Infrastrukturen, die von einer Vielzahl digitaler Plattformen verwendet werden. Je nachdem, wo diese Dienste niedergelassen sind, unterliegen sie unterschiedlichen Regeln. In den USA fallen etwa Cloud-Dienste unter den Clarifying Lawful Overseas Use of Data Act (CLOUD Act)[178], der u. a. US-Behörden Zugriff auf gespeicherte Daten einräumt – selbst dann, wenn die Speicherung nicht in den USA erfolgt. Auch in China hat die Regierung umfassende Zugangsrechte zu Daten.[179] In der EU unterfallen Cloud-Dienste der Richtlinie über die Netz- und Informationssicherheit (NIS-Richtlinie)[180], die 2016 eingeführt wurde und u. a. Sicherheitspflichten für Anbieter „kritischer" digitaler Dienste enthält. Durch die NIS-2-Richtlinie[181], die am 16. Januar 2023 in Kraft getreten ist und die NIS-Richtlinie zum 18. Oktober 2024 aufheben bzw. ersetzen wird, wurde die Richtlinie bereits umfassend überarbeitet. Anwendung finden die erweiterten Regeln u. a. auf Cloud-Computing-Dienste und öffentlich zugängliche elektronische Kommunikationsdienste als Sektoren mit hoher Kritikalität, die besonders strengen Pflichten unterliegen. Erfasst werden aber auch „sonstige kritische Sektoren" mit weniger strengen Cybersicherheitspflichten, darunter digitale

177 *Bourreau/Krämer/Buiten*, Interoperability in Digital Markets, S. 40.

178 18 USC 1 note, Public Law 115–141 v. 23. März 2018, 132 STAT. 1213, https://www.govinfo.gov/content/pkg/PLAW-115publ141/pdf/PLAW-115publ141.pdf#page=867.

179 Vgl. zum chinesischen Sicherheitsgesetz etwa die Ausarbeitung des Wissenschaftlichen Dienstes des Deutschen Bundestages, WD 10 – 3000 – 077/19.

180 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, EU ABl. L 194 vom 19.7.2016, S. 1–30. Vgl. dazu umfassend *Schmitz/Cole*, Kommentar zur NIS-Richtlinie.

181 Richtlinie (EU) 2022/2555 vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), EU ABl. L 333, 27.12.2022, S. 80–152.

Dienste in Form von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke. Zum Pflichtenkatalog gehören u. a. Multi-Faktor-Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie Kryptografie und ggf. Verschlüsselung. Bedeutsam sind insoweit auch die Zertifizierungssysteme unter dem Rechtsakt zur Cybersicherheit[182], zu denen die Mitgliedstaaten wesentliche Einrichtungen verpflichten können. Jüngst angenommen wurde außerdem auf EU-Ebene auch eine Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen.[183]

In Deutschland sind diese Vorgaben u. a. im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)[184] sowie ergänzend in der BSI-Kritisverordnung[185] umgesetzt. Hervorzuheben ist in diesem Zusammenhang, dass der Sektor Medien und Kultur zwar nicht vom BSIG erfasst ist, aber auf der Basis einer Bund-Länder AG auf Arbeitsebene im sog. UP KRITIS auch den Branchenarbeitskreis (BAK) Medien gegründet hat.[186] Dort werden regelmäßig Themen aus dem Bereich der Sicherstellung von Mediendienstleistungen angesprochen, wobei ein wesentlicher Punkt der Schutz vor Gefahren aus dem Cyberraum ist. Als kritische Dienstleistungen werden in der Arbeitsgruppe insbesondere die Warnung und Alarmierung, die Versorgung mit Informationen und die Herstellung von Öffentlichkeit im Rundfunk und in der (gedruckten und elektronischen) Presse gesehen.

Dieser Cybersicherheitsrahmen muss auch innerhalb von Interoperabilitätsbestimmungen berücksichtigt und sichergestellt werden. Zu bemerken

182 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit), EU ABl. L 151 vom 7.6.2019, S. 15–69.

183 Vorschlag für eine Verordnung des Europäischen Parlaments und Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020, COM(2022) 454 final. Die Legislativorgane haben sich auf einen Kompromiss dazu geeinigt, und das Parlament hat in erster Lesung am 12.3.2024 zugestimmt, sodass nur noch die förmliche Annahme durch den Rat aussteht; vgl. https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2022/0272(COD).

184 BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Art. 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist.

185 BSI-Kritisverordnung vom 22. April 2016 (BGBl. I S. 958), die zuletzt durch Art. 1 der Verordnung vom 29. November 2023 (BGBl. 2023 I Nr. 339) geändert worden ist.

186 Dazu eingehend *Etteldorf*, in AfP, 2018, S. 114, 114 ff.

ist allerdings, dass kleine und mittelständische Unternehmen[187] teilweise nicht unter die genannten Regeln fallen, was bei einer Einbeziehung in Interoperabilitätslösungen zu weiteren Sicherheitsrisiken führen oder der vorgesehenen Interoperabilität bereits entgegenstehen könnte.

e. Anforderungen aus dem Geschäftsgeheimnisschutz

Der Schutz von Geschäftsgeheimnissen ist eine wichtige Ausprägung unternehmerischer Freiheit und von Eigentumsrechten. Innovation und technische Entwicklungen, die teils mit erheblichem Personal- und Kostenaufwand verbunden sind, sollen grundsätzlich vor dem Zugriff durch andere Unternehmen oder die Öffentlichkeit geschützt werden. Die Schaffung von Interoperabilität kann solche Geschäftsgeheimnisse auf unterschiedlichen Ebenen tangieren, etwa wenn es um die Öffnung von Schnittstellen geht, die den Zugang zu unternehmenseigenen Systemen oder Daten bedingt oder auch technische Anwendungen wie algorithmische Systeme betrifft.

Eine sekundärrechtliche Ausprägung hat der Geschäftsgeheimnisschutz auf EU-Ebene in der Richtlinie über Geschäftsgeheimnisse gefunden.[188] Diese legt Vorschriften für den Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb, rechtswidriger Nutzung und rechtswidriger Offenlegung fest. Der Begriff des Geschäftsgeheimnisses ist dabei weit und erfasst alle Informationen, die geheim sind, einen kommerziellen Wert haben, weil sie geheim sind, und die Gegenstand von Geheimhaltungsmaßnahmen durch den Inhaber sind. Das trifft auch auf eine Vielzahl an technischen Funktionalitäten zu, wie etwa APIs oder algorithmische Systeme. Der Geschäftsgeheimnisschutz kann von Unternehmen zudem vorrangig selbst sichergestellt werden, indem sie etwa Geheimhaltungsvereinbarungen, einschließlich eines Verbots des Reverse Engineering, in ihren Lizenzvereinbarungen niederlegen oder die Zahl der möglichen Lizenzen insgesamt begrenzen. Ausnahmen vom Geschäftsgeheimnisschutz können zum Schutz eines legitimen Interesses im Unionsrecht oder nationalen Recht vorgesehen werden (Art. 5 der Richtlinie über Geschäftsgeheimnisse). Diese Aus-

187 Also solche, die die in der Empfehlung 2003/361/EG genannten Schwellenwerte nicht überschreiten, Art. 3 Abs. 1 lit. a) NIS2-Richtlinie.

188 Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, EU ABl. L 157 vom 15.6.2016, S. 1–18.

nahmen müssen jedoch den oben genannten Grenzen der Einschränkung von Grundrechten und Grundfreiheiten entsprechen.

In Deutschland sind die Regeln im Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)[189] umgesetzt. Anders als auf EU-Ebene ist Voraussetzung für den Geschäftsgeheimnisschutz zusätzlich ein berechtigtes Interesse an Geheimhaltung, das aber in Bezug auf die Integrität eigener Systeme ohne weiteres vorliegen dürfte.

f. Anforderungen aus dem Immaterialgüterrecht

Immaterialgüterrechte wie das Urheberrecht, aber ebenso das Patent- oder Markenrecht, sind im vorliegenden Kontext von Interoperabilität an zwei Stellen relevant.

Zunächst kann das Immaterialgüterrecht bei der technischen Umsetzung von Interoperabilität Schranken setzen. Insbesondere können (bislang geschlossene) Schnittstellen nicht nur unter den Geschäftsgeheimnisschutz fallen, sondern auch nach immaterialgüterrechtlichen Regeln (Patente, Urheberrechte) Schutz genießen.[190] Eine Öffnung oder Lizenzierung dieser Schnittstellen bedarf also einer Zustimmung des Inhabers der Immaterialgüterrechte oder einer gesetzlichen Rechtfertigung und ist ggf. angemessen zu vergüten.

Für urheberrechtlich geschützte Computerprogramme[191] existiert eine solche gesetzliche Rechtfertigung für eine Reihe von urheberrechtlich relevanten Nutzungshandlungen (Vervielfältigungen, Bearbeitungen, öffentliche Verbreitung, Übersetzung in Codeform etc.) in Art. 6 Abs. 1 der EU-Richtlinie über den Rechtsschutz von Computerprogrammen[192] bzw. in dessen Umsetzung in Art. 69e des deutschen Urheberrechtsgesetzes (UrhG)[193]. Danach ist eine Zustimmung des Urhebers zu diesen Handlungen nicht erforderlich, eine Nutzung also möglich, um die erforderlichen Informationen zur „Herstellung der Interoperabilität eines unabhängig ge-

189 Gesetz zum Schutz von Geschäftsgeheimnissen vom 18. April 2019 (BGBl. I S. 466).

190 *Bourreau/Krämer/Buiten*, Interoperability in Digital Markets, S. 41.

191 Wenn sie individuelle Werke in dem Sinne darstellen, dass sie das Ergebnis der eigenen geistigen Schöpfung ihres Urhebers sind.

192 Richtlinie 2009/24/EG des Europäischen Parlaments und des Rates vom 23. April 2009 über den Rechtsschutz von Computerprogrammen (kodifizierte Fassung), EU ABl. L 111 vom 5.5.2009, S. 16–22.

193 Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), das zuletzt durch Art. 25 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858) geändert worden ist.

schaffenen Computerprogramms mit anderen Programmen zu erhalten". Erforderlich ist aber, dass die Handlungen vom Lizenznehmer oder einem sonstigen Berechtigten vorgenommen werden sowie die notwendigen Informationen nicht ansonsten schon zugänglich sind und sich auf das beschränken, was zur Herstellung von Interoperabilität notwendig ist. Gewonnene Informationen dürfen – und das deckt sich mit dem Geschäftsgeheimnisschutz – aber nicht weitergegeben oder zu anderen Zwecken verwendet werden. Angesichts der Reichweite des Begriffs der Computerprogramme (Programme in jeder Gestalt, einschließlich des Entwurfsmaterials) dürfte das auch für eine Reihe von Anwendungen (Betriebsprogramme oder Anwendungsprogramme) im vorliegenden Kontext gelten. Wichtig ist der Zusatz in Art. 6 Abs. 3 der Richtlinie, wonach zur Wahrung der Übereinstimmung mit den Bestimmungen der Berner Übereinkunft zum Schutz von Werken der Literatur und der Kunst die Bestimmungen des Artikels nicht dahingehend ausgelegt werden dürfen, dass die rechtmäßigen Interessen des Rechteinhabers in unvertretbarer Weise beeinträchtigt werden oder im Widerspruch zur normalen Nutzung des Computerprogramms stehen.

Das Urheberrecht ist vor allem des Weiteren bei der Interoperabilität medialer Inhalte relevant, also vorrangig für Fragen im Kontext horizontaler oder vertikaler Integration von Medienanbietern, weniger dagegen bezüglich der Kommunikationsinhalte[194]. Mediale Inhalte – seien es Filme aus Mediatheken, Podcasts aus Audiotheken, journalistische Wortbeiträge in Foren, Memes auf sozialen Netzwerken, Videos auf Video-Sharing-Plattformen – sind regelmäßig umfassend urheberrechtlich geschützt. Ihre Nutzung darf also nur in den Schranken erfolgen, die der Urheber (durch Zustimmung oder Lizenzierung) oder das Gesetz (über Schranken- und Ausnahmeregeln) vorgeben. Interoperabilität führt insoweit zu einer Erweiterung der ursprünglichen Nutzung oder sogar zu einer anderen Nutzungsart, kann etwa mit zusätzlichen Vervielfältigungshandlungen oder einer (neuen) öffentlichen Wiedergabe eines Werkes verbunden sein.[195]

194 Das Urheberrecht ist daneben in diesem Rahmen relevant, wenn z. B. urheberrechtlich geschütztes Material im Kommunikationsvorgang versandt wird. Dies betrifft aber nicht den Aspekt der Interoperabilität, sondern ist ein allgemeines Phänomen beim Vorgang.

195 Das Urteil das EuGH in der Rs. C-161/17 – *Land Nordrhein-Westfalen / Dirk Renckhoff*, ECLI:EU:C:2018:634 – zeigt deutlich die Komplexität von Nutzungshandlungen vor allem im Internet. Der Gerichtshof sah hier in dem Upload eines Bildes auf einer Schulwebseite eine eigenständige Handlung der öffentlichen Wiedergabe, obwohl das Bild auf der Webseite eines Reisemagazins im Internet frei und mit Zu-

Das ist einerseits bei der legalen Verbreitung solcher Inhalte zu beachten. Eine gesetzlich verbindliche, horizontale und vollständige Interoperabilität von Mediatheken, Audiotheken oder Video-Sharing-Plattformen wäre aus urheberrechtlicher Sicht nur denkbar, wenn sie unter die Bedingung der Zustimmung der Urheber (ggf. für einzelne Inhalte) gestellt wird. Alternativ müsste eine allgemeine „Interoperabilitätsschranke" in das Urheberrecht eingeführt werden, vergleichbar zu der bei Computerprogrammen, was aber mit Blick auf die Grundsätze der Verhältnismäßigkeit und des Schutzes der berechtigten Interessen von Urhebern schwierig erscheint und EU-rechtlich vorgegeben werden müsste. Das gilt selbst dann, wenn sie mit einer angemessenen Vergütung verbunden wäre.[196] Problematisch ist eine Zustimmung des Urhebers, wenn Medienanbieter und Urheber nicht identisch sind, also Erstere nur Verwerter oder Nutzungsrechteinhaber sind – bspw. bei eingekauften Produktionen in Mediatheken oder bei nutzergeneriertem Content auf Plattformen. In einer solchen Konstellation den Verwerter oder Nutzungsrechteinhaber zu Interoperabilität zu verpflichten, würde ihn zur Einholung entsprechender Lizenzen zwingen.

Dieser Gedanke ist dem EU-Urheberrecht zwar nicht fremd. Zum Beispiel findet er sich teilweise in Art. 17 der DSM-Richtlinie[197], der Diensteanbieter (bspw. bei Video-Sharing-Plattformen) – vereinfacht ausgedrückt – dazu verpflichtet, in Bezug auf nutzergenerierte Inhalte alle Anstrengungen zu unternehmen, um die notwendigen Erlaubnisse für auf ihren Plattformen verbreitetes urheberrechtlich geschütztes Material einzuholen. Anders als beim Lizenzeinkauf, den man bei einer entsprechenden Interoperabilitätspflicht fordern müsste, ist das aber keine losgelöste oder mitenthaltene Verpflichtung, sondern führt „nur" dazu, dass die Anbieter, wenn sie die-

stimmung des Urhebers zur Verfügung stand. Nach Auffassung des EuGH richtete sich der Upload an ein neues Publikum, das von der ursprünglichen Zustimmung des Urhebers nicht gedeckt gewesen sei.

196 Schrankenregelungen, die eine gesetzlich erlaubte Nutzung vorsehen, werden häufig mit einer angemessenen Vergütungspflicht verbunden, um dem Verhältnismäßigkeitsgrundsatz Rechnung zu tragen. Eine solche im Kontext von Interoperabilität anzuwenden, könnte aber auch urheberpersönlichkeitsrechtliche Interessen wegen des Kontrahierungszwangs gefährden. Unabhängig davon ist zu beachten, dass die Mehrkosten dann entweder beim Verbreiter oder bei den Nutzern entstehen würden.

197 Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17. April 2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG, EU ABl. L 130 vom 17.5.2019, S. 92–125 (Copyright in the Digital Single Market (DSM)-Richtlinie).

se Anstrengungen unterlassen haben, nach den Regeln des Urheberrechts auch als bloße Vermittler haften. In der umfassenden Diskussion zu dieser Regelung, die auch unter dem Stichwort „Upload-Filter" geführt wurde, wurden Bedenken geäußert, dass Plattformen im Zweifel dazu übergehen könnten, möglichst weitreichend Inhalte vor der Veröffentlichung zu blockieren, um Haftungsrisiken zu entgehen. Im vorliegenden Kontext wäre eine solche Befürchtung, dass Medienanbieter weniger Fremdinhalte in ihren Mediatheken aufnehmen, weil sie eine Lizenzierung nicht sicherstellen können, entweder wegen der damit verbundenen Kosten aufgrund der weiteren Verbreitung oder weil der Urheber dem nicht zustimmt.

Ein anderes Beispiel, in dem gesetzliche Vorgaben eine urheberrechtliche „Öffnung" zur Folge haben, ist die EU-Portabilitätsverordnung[198]. Sie betrifft das Problem des Geoblockings insbesondere bei audiovisuellen Inhalten in kostenpflichtigen Bezugsverhältnissen, das auch im vorliegenden Kontext relevant sein kann. Anbieter entgeltlicher (z. B. Abonnement-)Online-Inhalte-Dienste (audiovisuelle Mediendienste und VoD-Dienste) werden verpflichtet, die grenzüberschreitende Portabilität von Inhalten sicherzustellen, es Nutzern also zu ermöglichen, abonnierte Inhalte auch bei Auslandsaufenthalten in anderen als dem Heim-EU-Mitgliedstaat abzurufen. Anbieter unentgeltlicher entsprechender Dienste werden lediglich „berechtigt", eine solche Portabilität zu ermöglichen. Für die Ermöglichung der grenzüberschreitenden Nutzung fingiert Art. 4 der Portabilitätsverordnung den Leistungsort: Die Bereitstellung eines Online-Inhalte-Dienstes für einen Abonnenten, der sich vorübergehend in einem Mitgliedstaat aufhält, sowie der Zugriff auf diesen Dienst und seine Nutzung durch den Abonnenten gelten als ausschließlich im Wohnsitzmitgliedstaat des Abonnenten erfolgt. Folglich können Urheber insoweit die Verbreitung ihrer Werke nicht mehr rechtswirksam geografisch einschränken, unabhängig von einer hierfür einzuräumenden angemessenen Vergütung. Sehen Lizenzverträge eine geografische Beschränkung vor – wie das bislang gängiger Praxis entspricht –, wären sie in Bezug auf unter die Portabilitätsverordnung fallende Konstellationen wegen der Fiktionsregel (jedenfalls insoweit)

198 Verordnung (EU) 2017/1128 des Europäischen Parlaments und des Rates vom 14. Juni 2017 zur grenzüberschreitenden Portabilität von Online-Inhaltediensten im Binnenmarkt, EU ABl. L 168 vom 30.6.2017, S. 1–11.

nicht durchsetzbar.[199] Hintergrund der EU-Portabilitätsverordnung ist, dass die Vergabe geografisch limitierter Lizenzen, die im Urheberrecht und im Markenrecht übliche Praxis ist, ein Hindernis für die Entstehung eines einheitlichen audiovisuellen Binnenmarkts darstellt(e).[200] Auch für Interoperabilität kann dies ein Problem sein. Im Gegensatz zur Portabilitätsverordnung, die nur den geografischen Aspekt der Lizenzierung betrifft, würden entsprechende „Kontrahierungszwänge" aber bei der Interoperabilität deutlich weiter reichen. Die Fiktion müsste sich daher darauf beziehen, dass der „Leistungsort" hier auch dann nur der eine (Ursprungs-)Mediendienst ist, wenn tatsächlich Inhalte in einem interoperablen Netzwerk bei mehreren Diensten abrufbar sind. Selbst wenn diese Fiktion mit dem Verhältnismäßigkeitsgrundsatz für vereinbar gehalten würde, wären Mehrkosten von den Diensteanbietern zu tragen, die auf die Nutzer umgelegt werden könnten. Gleiches gilt auch für eine partielle Interoperabilität (bspw. von Suchfunktionen) in Bezug auf die jeweilige Nutzungshandlung (bspw. Darstellung von Vorschaubildern in einem gemeinsamen Katalog), wobei dies in der Lizenzierungspraxis eher denkbar wäre.

Andererseits betreffen durch Interoperabilität generierte weitere Nutzungsarten auch die illegale Verbreitung urheberrechtlich geschützter Inhalte. So könnte bspw. das netzwerkübergreifende Posten eines geschützten Lichtbilds ohne Zustimmung des Urhebers mehrere Verletzungshandlungen (in jedem weiteren Dienst) darstellen. Das wirft weitergehend Fragen nach der Haftung bzw. ihrer Verteilung auf, auf die im Folgenden allgemeiner eingegangen wird. Für Nutzungsrechteinhaber, die bereits unter nicht-interoperablen Verhältnissen mit der massiven (ggf. nicht-autorisierten) Verbreitung ihrer Inhalte im Internet konfrontiert sind, dürfte das jedenfalls einen deutlichen Mehraufwand zur Folge haben.

Daran knüpft sich die nicht leicht zu beantwortende Folgefrage an, wie bspw. mit den bereits genannten Pflichten von Diensteanbietern für das Teilen von Online-Inhalten (bspw. soziale Netzwerke, Video-Sharing-Plattformen) aus Art. 17 der DSM-Richtlinie bzw. dem deutschen Urhe-

199 Art. 3 und Art. 6 der Portabilitätsverordnung regeln nicht explizit das Verhältnis zwischen Mediendiensteanbieter und Urheber, sondern nur das Verhältnis zwischen Rezipient und Mediendiensteanbieter.

200 So *Janik*, in: Geppert/Schütz, § 75 TKG, Rn. 6, im telekommunikationsrechtlichen Kontext.

ber-Diensteanbieter-Gesetz[201] innerhalb von interoperablen Systemen umzugehen wäre. Um sich weiterhin auf eine Haftungsprivilegierung berufen zu können, wenn illegal urheberrechtlich geschützte Inhalte von Dritten (Nutzern) über ihre Plattform verbreitet werden, müssen Diensteanbieter alles in ihrer Macht Stehende tun, um notwendige Lizenzen einzuholen. Ob die Zielplattform eines interoperablen Inhalts sich dann abgeleitet auf eine eingeholte Lizenz berufen kann oder (wahrscheinlicher) diese nochmal selbst einholen muss oder ob sie mithaftet, wenn die entsprechende Anstrengung nicht erfolgt ist, die Zielplattform sich aber darauf verlassen hatte, regelt die DSM-Richtlinie nicht. Insoweit wäre, wie im folgenden Abschnitt näher erläutert wird, bei strikter Anwendung geltenden Rechts von einem Verlust von Haftungsprivilegien für Diensteanbieter auszugehen, was durchaus möglich ist und wiederum nach Ansicht mancher bei einem eventuellen Overblocking zu Vielfaltsgefährdungen[202] führen kann.

g. Anforderungen aus der Plattformregulierung und dem Haftungsrecht

Auch in einem weiteren Zusammenhang ist zu bedenken, dass die Einführung von Interoperabilitätsverpflichtungen in einem Widerspruch zu bestehenden gesetzlichen Pflichten stehen könnte und daher mit der Einfügung entsprechender Ausnahmen verbunden sein müsste. Bei Haftungsfragen, die sich aus der Plattformregulierung ergeben, wäre dabei zu klären, ob weitere Ausnahmen in Bezug auf bspw. bestehende Regelungen zum Jugendschutz oder gegen die Verbreitung illegaler Inhalte gesellschaftlichen und demokratischen Interessen entgegenlaufen würden.

In Bezug auf Haftungsregeln gilt zunächst der allgemeine Grundsatz, dass für eigene Inhalte gehaftet wird. Vermittlungsdienste hingegen können sich unter bestimmten Voraussetzungen auf Haftungsprivilegien berufen, die nunmehr in den Art. 12 ff. DSA in Fortführung der entsprechenden Begrenzungen aus der e-Commerce-Richtlinie EU-weit unmittelbar bindend festgelegt sind. In interoperablen Strukturen müssten die Rechtsverhältnisse aber neu bewertet werden. Dieses Problem ergibt sich bereits bei der

201 Gesetz über die urheberrechtliche Verantwortlichkeit von Diensteanbietern für das Teilen von Online-Inhalten (Urheberrechts-Diensteanbieter-Gesetz – UrhDaG), BGBl. I S. 1204, 1215.

202 Vgl. dazu etwa *Weiden*, Mehr Freiheit und Sicherheit im Netz, S. 17 ff.

Datenportabilität nach der DS-GVO[203], gestaltet sich bei Interoperabilität aber noch komplexer. So müsste etwa bei horizontaler Interoperabilität zwischen Medienanbietern (bspw. Mediatheken) gefragt werden, ob alle beteiligten Anbieter für alle Inhalte als eigene Inhalte haften oder ob sie für „Fremdinhalte" nur Vermittlungsdienste sind (wenn sie z. B. Kontrolle über die Benutzeroberfläche ausüben können), selbst wenn die Benutzeroberfläche sich aus Nutzersicht als einheitlich darstellt. Soweit für diese Konstellation die Vorgaben für Hosting-Dienste zur Anwendung kämen, würde sich die Folgefrage stellen, unter welchen Umständen bei den weiteren Diensten von einer Kenntnis bzw. einem Kennenmüssen der Illegalität eines Inhalts auszugehen wäre. Im Zusammenhang mit dem Recht auf Datenportabilität ist als Vergleich dazu anerkannt, dass derjenige, der die portablen Daten bereitstellt, nicht für deren Weiterverwendung durch die betroffene Person oder den anderen Verantwortlichen, an den die Daten weitergegeben werden, haftet.[204] Bei Datenportabilität handelt es sich aber um einen einseitigen Austausch, anders als bei wechselseitiger Interoperabilität, bei der die „Daten" in mehreren Systemen vorhanden sind.

Insoweit erschiene es sinnvoll, soweit dies technisch überhaupt umsetzbar wäre, zusammen mit der Umsetzung etwaiger Interoperabilitätsanforderungen auch eine Automatisierung des Umgangs mit bestimmten Inhalten einzuführen, z. B. mit der diensteübergreifenden Entfernung von (illegalen) Inhalten. Wenn bspw. ein Inhalt unter Verstoß gegen das Urheberrecht in einem sozialen Netzwerk geteilt wird, würde seine Löschung dort auch eine Löschung im gesamten interoperablen Geflecht nach sich ziehen. Soweit die Illegalität sich aber aus nationalen Vorschriften ergibt, könnten sich eventuelle Probleme bei grenzüberschreitenden Aktivitäten von Diensten daraus ergeben, dass nicht alle Dienste in dem interoperablen System den gleichen rechtlichen Regelungen unterliegen. Als Beispiel kann das Posten eines verfassungsfeindlichen Symbols herangezogen werden, das vielleicht nur im deutschen Verbreitungsgebiet als rechtswidrig eingestuft wird, damit aber zugleich einen Verbreitungsraum betrifft, den möglicherweise nicht alle (interoperabel gemachten) sozialen Netzwerke adressieren.

Gleiches gilt für Regeln zum Jugendmedienschutz, die zwar in der EU für bestimmte Diensteanbieter und bestimmte Angebote einer Mindestharmonisierung unterliegen, aber in der nationalen Umsetzung und Anwen-

203 *Brüggemann*, in: DSRITB 2017, S. 1, 10.
204 *Artikel-29-Arbeitsgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, S. 6.

dung unterschiedlich gehandhabt werden. Auch gelten Altersbeschränkungen bei Online-Diensten in der EU weder gesetzlich noch tatsächlich[205] einheitlich. Eine Löschpflicht würde sich also möglicherweise bei separater Betrachtung nicht für alle Dienste innerhalb eines interoperablen Systems ergeben, gleichwohl würde eine Automatisierung dieser Löschung nach den jeweils strengsten Regeln aber zu dieser Folge führen. Komplexer wird die Situation bei nicht rechtswidrigen, aber aus anderen Gründen schädlichen Inhalte. So unterscheiden sich bspw. die Community-Standards der unterschiedlichen Dienste teils erheblich, mindestens aber in bestimmten Teilbereichen. So ist auf der Streaming-Plattform Twitch bereits das Suggerieren von Nacktheit nach den Nutzungsrichtlinien[206] untersagt, während dies bei YouTube nicht explizit der Fall ist. Die Bindung des Nutzers an diese Standards erfolgt aber auf zivilrechtlicher (vertraglicher) Ebene nur in Bezug auf den jeweiligen Dienst, bei dem der Nutzer registriert ist, nicht aber (automatisch) in Bezug auf alle Dienste, wenn sie in einem interoperablen Netzwerk integriert sind.

Diese Probleme sind nicht unüberwindbar,[207] bedürfen aber bei der Diskussion von Interoperabilität mitgedachter Lösungen wegen fehlender allgemeingültiger Standards sowohl in rechtlicher als auch in geschäftsmodellbezogener Hinsicht. Ohne die „Zentralisierung" durch ein einheitliches Moderationsregime[208], das mithin einschneidend für die unternehmerische Freiheit und möglicherweise auch nicht sinnvoll für auf bestimmte Nutzer oder Inhalte ausgerichtete Plattformen wäre, wäre Interoperabilität demnach mit der Beantwortung komplexer Haftungsfragen verbunden.

---

205 Die meisten sozialen Netzwerke und ähnlichen Online-Dienste knüpfen die Registrierung an die Bedingung eines Mindestalters von 13 Jahren. Das ist der unteren Vorgabe für rechtswirksame Einwilligungen unter der DS-GVO geschuldet, stellt aber keinen verbindlichen gesetzlichen Standard dar. Vgl. dazu *Cole/Etteldorf*, The Implementation of the GDPR in Member States' Law and Issues of Coherence and Consistency, S. 138 ff.

206 https://safety.twitch.tv/s/article/Community-Guidelines?language=de, Unterpunkt „Kleidung – Standardrichtlinien".

207 *Doctorow*, Interoperable Facebook, konstruiert etwa verschiedene Möglichkeiten einer nutzergesteuerten Moderation („User Republic") von Inhalten, in der Nutzer wählen können, welche „Standards" sie für ihren Feed anwenden, von wem sie Inhalte angezeigt erhalten oder wer an von ihnen gestarteten Diskussionen teilnehmen kann.

208 Zu dieser Idee und für eine Interoperabilität sozialer Netzwerke s. *La Quadrature du Net*, Pour l'interopérabilité des réseaux sociaux.

Abgesehen von Haftungsfragen besteht diese Komplexität auch in Bezug auf die Durchsetzung der Pflichten von Diensten in interoperablen Systemen. Solche Pflichten können sowohl von der Niederlassung oder der Marktausrichtung eines Dienstes abhängen als auch von der Dienstart oder Größe des Dienstes. So existieren mit dem Digital Services Act EU-weit einheitliche Regeln für Plattformen als Intermediäre, die aber einem abgestuften Pflichtenansatz entlang der Art und Reichweite einer Online-Plattform (Anzahl aktiver Nutzer) folgen. In einem interoperablen System hätte eine sehr große Online-Plattform ihren strengeren Pflichten ohne gesetzliche Anpassung auch bei der Inhaltemoderation nachzukommen, ggf. auch in Bezug auf Inhalte, die von Nutzern anderer (nicht in die Kategorie sehr großer Online-Plattformen fallender) Intermediäre generiert werden, also im Dienst von Anbietern, die weniger strengen Pflichten unterliegen oder als Kleinst- oder Kleinunternehmen sogar davon befreit sind. Auch bei Empfehlungssystemen gilt nach dem DSA kein einheitlicher Standard etwa in Bezug auf Transparenz und Einstellungsoptionen, sodass bei interoperablen Empfehlungssystemen die strengeren Regeln als Standard angelegt werden müssten, obwohl keine korrespondierende Pflicht einer (nicht sehr großen) Online-Plattform hierzu besteht. In interoperablen Systemen werden gerade – als Ausdruck von Vielfaltssicherungserwägungen bei der Schaffung solcher Lösungen – Unternehmen unterschiedlicher Größe beteiligt sein, sodass das Problem einer Abstufung von Pflichten, das auch anderen relevanten Regelungswerken bekannt ist,[209] sich auf jeden Fall stellen würde.

Wenn es darum geht, Diensten der Informationsgesellschaft[210] (bspw. soziale Netzwerke, Video-Sharing-Plattformen etc.) durch einen Mitgliedstaat Interoperabilitätspflichten aufzuerlegen, sind im Übrigen auch die Regeln der e-Commerce-Richtlinie[211] zum Herkunftslandprinzip zu bedenken. Art. 3 dieser Richtlinie, der auch nach Inkrafttreten des DSA weiter be-

209 Vgl. etwa auch die Vorschriften für Medienintermediäre nach dem MStV, die nach § 91 MStV nur ab einer bestimmten Nutzerreichweite gelten.

210 Vgl. die Definition in Art. 1 Abs. 1 lit. b) der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft, EU ABl. L 241, 17.9.2015, S. 1–15.

211 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), EU ABl. L 178, 17.07.2000, S. 1–16.

steht, ist dabei eine besondere Ausprägung der grundfreiheitlich geschützten Dienstleistungsfreiheit. Nach dessen Abs. 2 dürfen die Mitgliedstaaten den freien Verkehr von Diensten der Informationsgesellschaft aus einem anderen Mitgliedstaat nicht aus Gründen einschränken, die in den koordinierten Bereich der e-Commerce-Richtlinie fallen. Sie können nach Abs. 4 lediglich Maßnahmen im Hinblick auf „einen bestimmten" Dienst ergreifen, wenn das aus bestimmten Gründen (u. a. Jugendschutz oder Bekämpfung von Hass) erforderlich und angemessen ist. Vielfaltssicherung als expliziten Abweichungsgrund nennt Art. 3 Abs. 4 e-Commerce-Richtlinie nicht. Allerdings bezieht sich das Verbot einschränkender Maßnahmen auch nur auf den von der e-Commerce-Richtlinie koordinierten Bereich. Art. 1 Abs. 6 e-Commerce-Richtlinie statuiert hierzu, dass Maßnahmen auf gemeinschaftlicher oder einzelstaatlicher Ebene, die unter Wahrung des Gemeinschaftsrechts der Förderung der kulturellen und sprachlichen Vielfalt und dem Schutz des Pluralismus dienen, von der Richtlinie ohnehin unberührt bleiben. Mitgliedstaatliche Regelungen zur Vielfaltssicherung bleiben damit von der e-Commerce-Richtlinie bereits aus kompetenziell-systematischen Gründen unberührt[212] bzw. fallen nicht in den von der Richtlinie koordinierten Bereich[213]. Eine nicht EU-weit einzuführende Interoperabilitätspflicht könnte daher auf der Basis der Vielfaltssicherung begründet werden, müsste aber auch diese Ausrichtung haben, um nicht der Begrenzung durch Art. 3 e-Commerce-Richtlinie zu unterfallen.[214] In einer jüngeren Entscheidung zum österreichischen Kommunikationsplattformen-Gesetz hat der EuGH außerhalb von Vielfaltssicherungsregeln ein eher enges Verständnis der Vorschrift gezeigt, soweit es um mitgliedstaatliche Handlungsspielräume geht.[215] Die in Art. 3 Abs. 4 der e-Commerce-Richtlinie vorgesehene Möglichkeit, vom Grundsatz des freien Verkehrs von Diensten der Informationsgesellschaft abzuweichen, sei nicht dazu gedacht, den Mitgliedstaaten zu erlauben, *generell-abstrakte* Maßnahmen zur Regelung einer *gesamten Kategorie von Anbietern von Diensten der Informationsgesellschaft* zu ergreifen, selbst wenn mit solchen Maßnahmen Inhalte bekämpft werden sollen, die die in Art. 3 Abs. 4 Buchst. a Ziff. i der Richtlinie genannten Schutzziele in schwerwiegender Weise beeinträchti-

212 Ausführlich *Ukrow/Cole/Etteldorf*, Zur Kompetenzverteilung zwischen der Europäischen Union und den Mitgliedstaaten im Mediensektor, S. 175 ff., 571 ff.

213 So etwa *Paal*, Intermediäre: Regulierung und Vielfaltssicherung, S. 38.

214 Dabei sind aber die oben bereits unter dem primär- und verfassungsrechtlichen Rahmen dargestellten Bedingungen einzuhalten.

215 EuGH, Urt. v. 9.11.2023, Rs. C-376/22 – *Google Ireland u. a.*, ECLI:EU:C:2023:835.

gen, wobei diese Auslegung auch damit erklärt werden kann, dass auf EU-Ebene entsprechende Harmonisierungsbestrebungen bestehen.

h. Anforderungen aus dem Medienrecht

Wenn es um Interoperabilität im Kontext von Medienvielfaltssicherung geht, sind schließlich auch diejenigen Vorschriften von besonderer Relevanz, die Medienanbieter sowie in Teilen auch diesen vergleichbare Dienste adressieren.

Hierzu gehören vor allem die Vorschriften aus dem nationalen Medienrecht, in Deutschland also insbesondere die Bestimmungen aus den Länderstaatsverträgen MStV, JMStV und den Mediengesetzen der einzelnen Länder. Auch die dort enthaltenen Pflichten müssten ohne gesetzliche Anpassung innerhalb interoperabler Systeme eingehalten werden. Das bereits im vorigen Abschnitt aufgezeigte Problem, dass unterschiedliche Pflichten für unterschiedliche Anbieter bestehen, gilt auch in diesem Zusammenhang. Für den JMStV würden sich insbesondere Fragen in Bezug auf die Gewährleistung von geschlossenen Benutzergruppen und zu einheitlichen Altersverifikationsmechanismen stellen, deren Antwort aber in einer einheitlichen Anbindung an das bisherige System in Kooperation mit den Selbstregulierungseinrichtungen liegen könnte. Ferner sind die durch den Rechtsrahmen gegebenen Garantien etwa der redaktionellen Freiheit und Unabhängigkeit des Rundfunks zu beachten, die nicht durch Standardisierung im Zusammenhang mit Interoperabilität verkürzt werden sollten. In Bezug auf den öffentlich-rechtlichen Rundfunk wäre zudem gesondert zu beachten, ob die Herstellung von Interoperabilität vom Auftrag gedeckt ist.

Auf EU-Ebene ist im medienrechtlichen Zusammenhang die AVMD-Richtlinie von Relevanz, die ihre Umsetzung im MStV, JMStV und TMG[216] findet. Dort gibt es einen ähnlichen Mechanismus wie unter der e-Commerce-Richtlinie, der Mitgliedstaaten Restriktionen auferlegt, wenn sie im eigenen Recht Interoperabilitätspflichten auf Anbieter audiovisueller Mediendienste anwenden wollen. Nach Art. 3 Abs. 1 AVMD-Richtlinie gewährleisten die Mitgliedstaaten den freien Empfang und behindern nicht die Weiterverbreitung von audiovisuellen Mediendiensten aus anderen Mitgliedstaaten in ihrem Hoheitsgebiet aus Gründen, die Bereiche betref-

216 Zukünftig im Digitale-Dienste-Gesetz; vgl. Art. 36 des Entwurfs, BT-Drs. 20/10031.

fen, die durch die AVMD-Richtlinie „koordiniert" sind. Die Mitgliedstaaten können allerdings unter bestimmten Bedingungen hiervon abweichen (Art. 3 Abs. 2, 3 und 5 AVMD-Richtlinie) oder strengere Regeln für unter die eigene Rechtshoheit fallende Anbieter erlassen (Art. 4 AVMD-Richtlinie).[217] Zentral ist wiederum die Frage nach dem von der Richtlinie koordinierten Bereich, dessen Beurteilung sich im Einzelfall als schwierig herausstellen kann.[218] In der Rechtssache Fussl Modestraße Mayr hatte der EuGH 2021 die Regeln zum „Verbot" regionalisierter Werbung nach dem MStV zu beurteilen[219] und entschied, dass § 7 Abs. 11 RStV a. F. zwar in einen von der AVMD-Richtlinie „erfassten Bereich" falle, nämlich den der Fernsehwerbung, allerdings einen speziellen Bereich betreffe, der durch keine der Richtlinien-Vorschriften geregelt wird. Damit fielen die nationalen Vorschriften nicht in den „koordinierten" Bereich und unter die Herkunftslandmechanismen. Das dürfte auch für Interoperabilitätsverpflichtungen gelten, die keinen Anknüpfungspunkt in der AVMD-Richtlinie finden. Diese wäre dann allerdings – wie auch die nationale Regelung im Fall Fussl Modestraße Mayr – an der primärrechtlichen Dienstleistungsfreiheit (oder anderem Sekundärrecht) zu messen.

Abschließend ist auf den EMFA hinzuweisen, der jüngst veröffentlicht worden ist. Während Interoperabilität mit dem Ziel der Vielfaltssicherung auch die Zielsetzung des darin enthaltenen Art. 3 EMFA (Recht von Rezipienten auf Zugang zu einer Vielfalt an redaktionell unabhängigen Medieninhalten) stützen und befördern könnte, müssten die vom EMFA aufgestellten Pflichten in interoperablen Systemen sichergestellt bleiben. Interoperabilitätspflichten müssten also so ausgestaltet sein, dass sie die redaktionelle Freiheit nicht verkürzen. Wenn Interoperabilität bei sozialen Netzwerken oder anderen Online-Plattformen angestrebt wird, dürfte auch die Umsetzung des „Medienprivilegs" aus Art. 17 EMFA eine Herausforderung sein.

217 Im Detail dazu *Cole/Etteldorf*, Future Regulation of Cross-border Audiovisual Content Dissemination, S. 127 ff.

218 *Cole/Etteldorf*, Future Regulation of Cross-border Audiovisual Content Dissemination, S. 156.

219 EuGH, Urt. v. 3.2.2021, Rs. C-555/19 – *Fussl Modestraße Mayr*, ECLI:EU:C:2021:89.

II. Geltender Rechtsrahmen zur Interoperabilität: Wettbewerbsrecht

Die Gefahren, die aus dem Fehlen von Interoperabilität resultieren (können),[220] beziehen sich zu einem großen Teil auf bedenkliche Marktentwicklungen in Form von Marktverzerrungen durch die Dominanz einiger weniger großer Anbieter und dadurch verringerten Marktzutrittschancen anderer Anbieter. Solche problematischen Entwicklungen zu adressieren und ihnen gegenzusteuern, ist maßgeblich Aufgabe des Wettbewerbs- und insbesondere des Kartellrechts. Das betrifft zunächst die gesetzlichen Regeln, die regelmäßig allgemein formuliert sind und für alle Wirtschaftssektoren gleichermaßen gelten. Mehr noch betrifft es aber deren Ausfüllung durch die jeweiligen Kartellbehörden sowohl durch Einzelfallentscheidungen als auch mit konkretisierenden Leitlinien. Im Folgenden wird daher untersucht, inwieweit Interoperabilitätserwägungen in der wettbewerbsrechtlichen Regulierungspraxis in die Betrachtung einbezogen wurden und welche Rückschlüsse daraus gezogen werden können. Vor dem Hintergrund der Zielsetzung des Gutachtens wird dabei jeweils auch darauf eingegangen, ob Aspekte der Vielfaltssicherung, die durch eine aus Marktmacht resultierende Meinungsmacht gefährdet werden kann, aufgegriffen wurden oder grundsätzlich aufgegriffen werden könn(t)en.

1. USA

Im US-amerikanischen Wettbewerbsrecht sind im Zusammenhang mit Interoperabilität drei Gesetze, die im Folgenden beleuchtet werden, zentral: der Sherman Antitrust Act, der Federal Trade Commission Act und der Clayton Antitrust Act. Sie dienen dem Schutz vor Missbrauch einer marktbeherrschenden Stellung und der Verhinderung der Bildung von Monopolen. Auch wenn Interoperabilität nicht ausdrücklich geregelt wird, könnte sie im Rahmen dieser Gesetze dazu geeignet sein, den freien Wettbewerb zwischen technischen Plattformen und Dienstleistungen wiederherzustellen oder sich als praktische Konsequenz aus der Zerschlagung eines Monopols ergeben.

220 Vgl. dazu eingehend oben unter B.

a. Sherman Antitrust Act

Der Sherman Antitrust Act of 1890[221] (nachfolgend Sherman Act) ist das erste US-Gesetz zum Schutz des freien Wettbewerbs durch die Beschränkung von Monopolen und Kartellen. Kern des Gesetzes ist das in Section 1 enthaltene Verbot unangemessener Handelsbeschränkungen,[222] das etwa Preisabsprachen und Marktaufteilungen unter Marktteilnehmern ausnahmslos untersagt, und das in Section 2 normierte Monopolverbot, das zur Anwendung kommt, wenn ein Unternehmen den Wettbewerb durch die Erlangung oder Aufrechterhaltung eines Monopols verdrängt oder behindert.Dabei ist bereits der Versuch der Monopolisierung untersagt („attempt to monopolize"). Der Anwendungsbereich des Sherman Act unterscheidet sich von der in der EU geltenden Regelung des Art. 102 AEUV, der das Entstehen eines Monopols nicht regelt (dazu C.II.2.a).[223]

Auf der Grundlage von Section 2 Sherman Act könnte mit dem Ziel der Verhinderung oder Auflösung eines Monopols ein Unternehmen zur Öffnung seiner Dienste und zur Herstellung von horizontaler Interoperabilität gezwungen werden.[224] Am Beispiel eines sozialen Netzwerks könnte so der Austausch von Daten und Inhalten mit Wettbewerbern erzwungen werden, die auf dieser Grundlage technisch kompatible Dienste anbieten könnten. Auf diesem Weg wäre es möglich, eine Monopolstellung eines sozialen Netzwerks aufzubrechen und Wettbewerb wiederherzustellen.[225] Um den Tatbestand der Monopolisierung nach Section 2 Sherman Act zu erfüllen, muss eine von drei Voraussetzungen vorliegen. Ein Marktteilnehmer (1) muss ein Monopol erlangen oder (2) den Versuch unternehmen, ein Monopol zu erlangen, oder (3) sich mit anderen Marktteilnehmern verabreden, ein Monopol zu erlangen. Der Oberste Gerichtshof der Vereinigten Staaten stellte klar, dass nur vorsätzlich erlangte Monopolstellungen mit dem Ziel der Ausnutzung der Marktmacht erfasst sind, während die nicht intendierte Erlangung eines Monopols – etwa durch ein überlegenes Produkt oder die Beendigung der Tätigkeit eines Mitbewerbers – grundsätzlich

221 Sherman Antitrust Act of 1890, 15 U.S. Code § 1–7.

222 Das in Section 1 ursprünglich enthaltene absolute Verbot von Handelsbeschränkungen wurde später vom US Supreme Court auf unangemessene Handelsbeschränkungen reduziert; siehe US Supreme Court, Standard Oil Co. of New Jersey v. United States, 211 U.S. 1 (1911).

223 *Scholz*, in: Wiedemann KartellR-HdB, § 22 Rn. 14.

224 *Palka*, in: Seton Hall Law Review, 2021, S. 1193, 1234 f.

225 *Palka*, in: Seton Hall Law Review, 2021, S. 1193, 1198.

zulässig ist.[226] Darüber hinaus muss der Nachweis einer bestehenden Wettbewerbsbeeinträchtigung erbracht werden können.[227]

Die Rechtsdurchsetzung des Sherman Act obliegt vorrangig dem Justizministerium der Vereinigten Staaten, dem US Department of Justice (DOJ), das Verstöße zivilrechtlich mit Geldbußen von bis zu USD 100 Millionen für Unternehmen und bis zu USD 1 Million für natürliche Personen ahnden kann. Darüber hinaus sind Haftstrafen von bis zu zehn Jahren möglich. Allerdings wurde in den USA u. a. vor dem Hintergrund der zunehmenden Globalisierung von Märkten die Wettbewerbsaufsicht in den letzten Jahrzehnten reduziert. Insbesondere wenden Gerichte und Wettbewerbsbehörden das Monopolisierungsverbot nur zurückhaltend an, und es wird nur selten erfolgreich eingesetzt.[228] Auch wenn die hohen Tatbestandsvoraussetzungen erfüllt und eine Wettbewerbsbeeinträchtigung tatsächlich nachgewiesen werden könnte, erscheint eine erfolgreiche Anwendung der Norm zur Herstellung von Interoperabilität zum jetzigen Zeitpunkt in den USA zwar grundsätzlich möglich, aber nicht naheliegend.[229] Die seit den 1970er Jahren im Wettbewerbsrecht der USA vorherrschende Strömung der Chicago School, deren zentraler Anknüpfungspunkt die Frage ist, ob sich unternehmerisches Handeln letztlich in höheren Verbraucherpreisen niederschlägt, wird erst seit etwa einem Jahrzehnt kritisch hinterfragt. Dabei fordern Anhänger der sog. New Brandeis School bei der Anwendung des US-Kartellrechts die Berücksichtigung von Fairness, sozialen Interessen, Qualität und der Möglichkeit von Konsumenten, zwischen verschiedenen Wettbewerbern zu wählen.[230] Dies spiegelt sich in zahlreichen Verfahren aus jüngerer Zeit gegen Big-Tech-Unternehmen auf der Grundlage des Sherman Act wider, wenngleich nicht davon auszugehen ist, dass diese alle aus Sicht des Justizministeriums erfolgreich ausgehen werden.[231] Wichtige Fälle werden im Folgenden im Überblick dargestellt.

226 US Supreme Court, United States v. Aluminum Co. of America, 148 F.2d 416 (1945); *Fuchs*, in: Immenga/Mestmäcker, Art. 102 AEUV, Rn. 40.

227 US Supreme Court, United States v. E. I. du Pont de Nemours & Co., 353 U.S. 586, 597 (1957).

228 *Bueren/Crowder*, in: ZHR, 186, 2022, S. 788, 793, 802 ff.; *Fuchs*, in: Immenga/Mestmäcker, Art. 102 AEUV, Rn. 40a.

229 *Palka*, in: Seton Hall Law Review, 2021, S. 1193, 1234 f.

230 *Bueren/Crowder*, in: ZHR, 186, 2022, S. 788, 802 ff. m. w. N.

231 Vgl. z. B. *McCabe/Grant*, in: The New York Times v. 24.1.2023.

(1) Microsoft Internet Explorer

Das wohl bekannteste US-Wettbewerbsverfahren zur Herbeiführung von Interoperabilität betraf Microsoft. Um die Jahrtausendwende ging das DOJ unter Anwendung von Section 2 Sherman Act gegen Microsoft vor.[232]

In den 1990er Jahren monopolisierte Microsoft den Markt für Internetbrowser, indem es das eigene Produkt Internet Explorer bevorzugte und Wettbewerber wie Netscape bewusst verdrängte. Dazu war der Internet Explorer auf dem damals nahezu monopolartig verbreiteten eigenen Betriebssystem Windows vorinstalliert, und Anwendern wurde die vollständige Entfernung des Browsers nahezu unmöglich gemacht. Zusätzlich hatte Microsoft zentrale Schnittstellen im Betriebssystem Windows für Drittentwickler derart eingeschränkt, dass Browser von Drittanbietern im Vergleich zum Internet Explorer technisch benachteiligt wurden. Durch die Einschränkung dieser Programmierschnittstellen in Windows wurden die Interoperabilität des Betriebssystems mit Browsern von Drittherstellern und darüber hinaus deren Funktionalität erheblich begrenzt. Aus Anwendersicht verloren Browser von Drittanbietern damit erheblich an Attraktivität. Zusätzlich traf Microsoft wettbewerbswidrige Vereinbarungen mit PC-Herstellern, die einerseits dazu gedrängt wurden, den Internet Explorer als Verknüpfung auf dem Windows-Desktop voreinzustellen (sog. Desktop Icon). Andererseits wurde es PC-Herstellern durch Microsoft untersagt, Browser von Drittherstellern wie Netscape vorzuinstallieren.[233] Konkurrenzprodukte konnten sich so nicht erfolgreich am Markt etablieren.

Durch diese Handlungen konnte Microsoft die Marktmacht für Internetbrowser erfolgreich erlangen und absichern. Der über zehn Jahre andauernde Fall endete mit einer Vereinbarung zwischen Microsoft und dem DOJ,[234] in der sich Microsoft u. a. dazu verpflichtete, Programmierschnittstellen im Betriebssystem Windows für Drittanbieter von Internetbrowsern zu öffnen – und damit Interoperabilität herzustellen – und sonstiges wettbewerbswidriges Verhalten, wie das Verbot der Installation von Drittbrowsern, einzustellen. Der Fall Microsoft zeigt, wie die Einschränkung von Interoperabilität durch einen marktstarken Anbieter den Wettbewerb beeinflussen kann, und macht zugleich deutlich, wie die Anwendung des Sherman Act zu einer technischen Interoperabilität führen kann.

232 Für einen Überblick zum Fall siehe *Cohen*, in: Berkeley Technology Law Journal, 2004, S. 333.

233 *Cohen*, in: Berkeley Technology Law Journal, 2004, S. 333, 340 ff.

234 United States v. Microsoft Corp., Final Judgement, 98-CV-1232 (D.D.C. 12.11.2002).

(2) Google AdTech

Microsoft ist nicht das einzige Big-Tech-Unternehmen, das durch die Anwendung wettbewerbsrechtlicher Instrumente in seinem Marktverhalten korrigiert werden sollte.[235] Vielmehr wurden in den vergangenen Jahren zahlreiche Verfahren initiiert, in denen es zumindest mittelbar um die Interoperabilität digitaler Plattformen geht und die auch Ausdruck der sich verschiebenden Schwerpunktsetzung bei den Zielen des US-Wettbewerbsrechts sind. So laufen derzeit bspw. verschiedene Verfahren gegen Google wegen Wettbewerbsverletzungen im Online-Werbemarkt.

Im Jahr 2020 haben Texas und 14 weitere Bundesstaaten ein Verfahren gegen Google wegen der Monopolisierung des Online-Werbemarktes auf der Grundlage von Section 1 und 2 Sherman Act eingeleitet.[236] Google wird vorgeworfen, Produkte und Dienstleistungen im Bereich des Display Advertising monopolisiert zu haben, die von Publishern und Werbetreibenden eingesetzt werden. Display Advertising betrifft das Ausspielen grafischer Werbemittel, also etwa Werbebanner auf Webseiten. Ebenfalls auf der Grundlage von Section 2 Sherman Act ist seit 2020 ein Verfahren gegen Google wegen der Monopolisierung von Online-Suchmaschinen und des Online-Werbemarktes im Kontext von Online-Suchmaschinenanfragen anhängig.[237] Anders als im erstgenannten Verfahren sind hier nicht nur grafische Werbeanzeigen im Display Advertising, sondern auch Textanzeigen erfasst, die etwa im Kontext von Suchmaschinenergebnissen ausgespielt werden. Darüber hinaus wurde im November 2023 ein weiteres Verfahren gegen Google wegen wettbewerbswidriger Praktiken im Google Play Store vorläufig durch einen Vergleich beigelegt. Google wurde vorgeworfen, für Apps im mobilen Betriebssystem Android andere App-Stores als den Google Play Store für die Verbreitung zu verbieten, im Google Play Store eine bestimmte Zahlungsart vorzuschreiben und Transaktionsgebühren von bis zu 30 % für In-App Käufe zu erheben.[238] Die Bedingungen des Vergleichs sind noch nicht bekannt. Ferner muss der Vergleich noch gerichtlich bestätigt werden.[239]

235 *McGabe/Grant*, in: The New York Times v. 24.1.2023.
236 Texas and Plaintiff States v. Google LLC, Complaint 16.12.2020.
237 U.S. and Plaintiff States v. Google LLC, Complaint 20.10.2020.
238 Utah and Plaintiff States v. Google, Complaint 7.7.2021.
239 *Sisco*, in: Politico.com v. 6.9.2023.

Das jüngste, im Jahr 2023 vom DOJ und acht weiteren Bundesstaaten gegen Google eingeleitete Verfahren ähnelt dem zuvor genannten Fall des Display Advertising.[240] Gestützt auf Section 1 und 2 Sherman Act wird Google vorgeworfen, ein Monopol im Online-Werbemarkt erlangt zu haben und die erlangte Marktmacht in unrechtmäßiger Weise auszunutzen. Dies äußere sich einerseits darin, dass der Wettbewerb im Online-Werbemarkt gezielt von Google behindert werde, indem das Unternehmen Wettbewerber aufkaufe und so vom Markt verdränge. Dadurch habe das Unternehmen eine Position erlangt, aus der es die im Online-Werbemarkt eingesetzte Technologie zum Nachteil von Werbetreibenden und Publishern betreiben und so den größten Online-Werbemarktplatz etablieren und kontrollieren könne.[241] Konkret habe Google die Möglichkeit, die für Online-Werbung eingesetzte Technologie auf Verkäuferseite (Publisher), Käuferseite (Werbetreibende) sowie den Handelsplatz dafür (Ad Exchange, „AdX") zu kontrollieren.[242] Dadurch bestimme Google nicht nur über Transaktionsgebühren, sondern auch über die eingesetzte Technologie. Auch wenn diese für Online-Werbung in der Form interoperabel ist, dass neben den von Google bereitgestellten Tools weitere technische Werkzeuge, Plattformen und Handelsplätze eingesetzt werden können, habe sich Google durch die Kontrolle des größten AdX einen ökonomischen Vorteil verschafft. Google habe die Interoperabilität mit anderen AdX erschwert, sodass Publisher daran gehindert worden seien, ihre Werbeplätze auf anderen AdX zu günstigeren Preisen anzubieten.[243] Ferner erhöhe Google die Ausschüttungen für Publisher auf Kosten der Werbetreibenden.[244] Dadurch werde ein Anreiz für Publisher geschaffen, Transaktionen primär auf der von Google bereitgestellten Plattform abzuwickeln, woraus wiederum Google profitiere. Tatsächlich sei Google durch die Kontrolle aller Komponenten der Online-Werbetechnologie und des größten Online-Marktplatzes in der Lage, bis zu 35 % an Transaktionskosten für Online-Werbetransaktionen einzubehalten.[245] Die von Google bestimmten Transaktionskosten für Publisher seien jedoch bedeutend höher als bei Wettbewerbern, sodass trotz der höheren Ausschüttungen und damit Einnahmen auch Publisher

240 *McCabe/Grant*, in: The New York Times v. 24.1.2023.
241 U.S. and Plaintiff States v. Google LLC [2023], Complaint 24.1.2023, Rn. 6 f., https://www.justice.gov/atr/case/us-and-plaintiff-states-v-google-llc-2023.
242 U.S. and Plaintiff States v. Google LLC [2023], Complaint 24.1.2023, Rn. 17.
243 U.S. and Plaintiff States v. Google LLC [2023], Complaint 24.1.2023, Rn. 21, 136.
244 U.S. and Plaintiff States v. Google LLC [2023], Complaint 24.1.2023, Rn. 20.
245 U.S. and Plaintiff States v. Google LLC [2023], Complaint 24.1.2023, Rn. 39.

langfristig einen Nachteil davontrügen.[246] Dieses Geschäftsgebaren behindere den freien Wettbewerb.

Entsprechend fordert das DOJ, dass Google große Teile des Werbemarktplatzes abstoßen solle. Interoperabilität steht damit nicht im Zentrum dieses Falls. Dennoch zeigt das Verfahren exemplarisch, dass zum einen Googles Wettbewerber keine Möglichkeit haben, die von Google getroffenen technischen Entscheidungen und damit die Anforderungen an die Interoperabilität der Werbetechnologie mitzubestimmen. Zum anderen bevorzugt Google die eigene Plattform (*self-preferencing*) etwa durch das Erschweren des Handels mit anderen Handelsplätzen, womit für Werbetreibende und Publisher der Wechsel zu von Wettbewerbern betriebenen Plattformen behindert wird. Dieses Verfahren vergegenwärtigt, dass eine technisch vorhandene Interoperabilität durch das Verhalten von Marktteilnehmern unterlaufen werden kann und daher die technische Voraussetzung allein unter Umständen nicht ausreicht, um Fehlentwicklungen am Markt zu beheben.

b. Federal Trade Commission Act

(1) Untersuchungsbefugnisse der unabhängigen Behörde FTC

Der Sherman Antitrust Act wurde durch den Federal Trade Commission Act of 1914[247] und den Clayton Antitrust Act of 1914 ergänzt. Mit dem Federal Trade Commission Act wurde die unabhängige US-Bundesbehörde Federal Trade Commission (FTC) errichtet, die für die Durchsetzung von Wettbewerbs- und Verbraucherschutzgesetzen zuständig ist. Geführt wird die Behörde von fünf politisch gewählten Beauftragten (den sog. Commissioners), die vom US-Präsidenten nominiert und vom US-Senat bestätigt werden. Maximal drei der fünf Commissioners dürfen derselben politischen Partei angehören.[248] Neben der Errichtung der FTC enthält der Federal Trade Commission Act Vorschriften zur Untersagung unlauterer

246 U.S. and Plaintiff States v. Google LLC [2023], Complaint 24.1.2023, Rn. 126 ff., 262 ff.
247 Federal Trade Commission Act of 1914, 15 U.S. Code §§ 41–58, as amended.
248 15 U.S. Code § 41.

Wettbewerbsmethoden sowie unlauterer oder betrügerischer geschäftlicher Handlungen oder Praktiken:[249]

> *15 U.S. Code § 45 – Unfair methods of competition unlawful; prevention by Commission*
> *(a) Declaration of unlawfulness; power to prohibit unfair practices; inapplicability to foreign trade*
> *(1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.*

Zu den Aufgaben der FTC gehören die Verhinderung von unlauterem Wettbewerb, die Kontrolle von Unternehmensfusionen und die Bekämpfung von betrügerischen oder irreführenden Geschäftspraktiken. Die Durchsetzung des Wettbewerbsrechts auf US-Bundesebene erfolgt in Form von branchenweiten Verordnungen (sog. Rulemaking) der FTC, der Einleitung von verwaltungsgerichtlichen Verfahren sowie der Erhebung von Zivilklagen. Die FTC verfügt, anders als das US DOJ, nicht über strafrechtliche Befugnisse.

(2) Der Fall Meta

Jeder Verstoß gegen den Sherman Antitrust Act stellt gleichzeitig auch einen Verstoß gegen den FTC Act dar.[250] Deshalb kann die FTC auch unternehmerische Handlungen im Anwendungsbereich des Sherman Act verfolgen.[251] Vor diesem Hintergrund versuchte die FTC zusammen mit 46 US-Bundesstaaten, dem District of Columbia und dem US-Außengebiet Guam im Jahr 2020 auf der Grundlage von Section 2 Sherman Act gegen Facebook (bzw. den Mutterkonzern Meta) vorzugehen, weil es durch die Zukäufe von WhatsApp und Instagram ein Monopol im Bereich sozialer Netzwerke erlangt habe. Dadurch sei der Wettbewerb im Online-Werbe-

249 15 U.S. Code § 45. Daneben sind weitere unlautere Handlungen wie irreführende Produktetiketten untersagt; siehe 15 U.S. Code §§ 45a-45f, 52–54.

250 Konkret gegen das Verbot unlauterer Wettbewerbsmethoden; siehe 15 U.S. Code § 45(a).

251 Federal Trade Commission, The Antitrust Laws, https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/antitrust-laws.

markt sozialer Netzwerke verzerrt worden.[252] Die FTC begehrte, dass Meta die Zukäufe Instagram und WhatsApp abstoßen solle. Gleichzeitig warf die FTC Facebook vor, Drittentwicklern den Zugriff auf von Facebook bereitgestellte Schnittstellen zu entziehen, sobald Drittanwendungen zu direkten Konkurrenten von Facebook würden. Dadurch werde die Interoperabilität von Drittanwendungen mit Facebook zum Nachteil von Nutzern eingeschränkt.

Der Fall wurde zunächst vom Gericht abgewiesen, weil die von der FTC vorgelegten Beweise nicht ausreichten.[253] Die FTC startete kurz darauf einen zweiten Anlauf.[254] Hierauf beantragte Meta eine Klageabweisung und stellte einen Befangenheitsantrag gegen die Vorsitzende der FTC, Lina Khan, weil sie sich in der Vergangenheit öffentlich negativ über Facebook geäußert habe.[255] Beide Anträge wurden 2022 gerichtlich abgewiesen. Gleichzeitig sah das Gericht keine ausreichenden Beweise für den Facebook vorgeworfenen Umgang mit der Interoperabilität von Drittentwicklern, etwa weil Facebook die angegriffene Regelung bereits 2018 aufgegeben hatte. Damit kann das Verfahren zumindest bezüglich der Unternehmenskäufe von Instagram und WhatsApp weitergeführt werden.[256] Sein Ausgang ist zwar ungewiss,[257] für die Interoperabilitätsfrage jedoch nicht entscheidend.

252 FTC v. Facebook, Complaint 9.12.2020. Zum Verfahrensgang siehe auch https://www.ftc.gov/legal-library/browse/cases-proceedings/191-0134-facebook-inc-ftc-v.

253 FTC v. Facebook, Order, 20-CV-3590 (D.D.C. 28.6.2021); FTC v. Facebook, Memorandum Opinion, 20-CV-3590 (D.D.C. 28.6.2021); *Bueren/Crowder*, ZHR, 186, 2022, S. 788, 810 ff.

254 FTC v. Facebook, First Amended Complaint for Injunctive and Other Equitable Relief, 20-CV-03590-JEB (D.D.C. 19.8.2021).

255 FTC v. Facebook, First Amendment Complaint for Injunctive and Other Equitable Relief, 20-CV-03590-JEB (D.D.C. 19.8.2021).

256 FTC v. Facebook, Order, 20-CV-03590-JEB (D.D.C. 11.1.2022); FTC v. Facebook, Memorandum Opinion, 20-CV-03590-JEB (D.D.C. 11.1.2022).

257 *Bueren/Crowder*, in: ZHR, 186, 2022, S. 788, 813.

c. Clayton Antitrust Act

(1) Die Bedeutung für die Fusionskontrolle

Neben dem Federal Trade Commission Act wurde auch der Clayton Antitrust Act[258] (nachfolgend Clayton Act) als Ergänzung des Sherman Act erlassen. Der Clayton Act zielt insbesondere auf die Bekämpfung wettbewerbsschädigender Handlungen, die nicht vom Sherman Act erfasst werden. Das Gesetz verbietet u. a. die wettbewerbsschädigende Preisdiskriminierung (Section 2) und den Wettbewerb erheblich einschränkende Exklusiv- und Kopplungsgeschäfte (Section 3). Zentral für das Wettbewerbsrecht ist die Fusionskontrolle in Section 7, um die Erlangung von Monopolen durch Unternehmenskäufe und -fusionen (Mergers and Acquisitions und Joint Ventures) zu verhindern:[259]

> *15 U.S. Code § 18 – Acquisition by one corporation of stock of another*
> *No person engaged in commerce or in any activity affecting commerce shall acquire, directly or indirectly, the whole or any part of the stock or other share capital and no person subject to the jurisdiction of the Federal Trade Commission shall acquire the whole or any part of the assets of another person engaged also in commerce or in any activity affecting commerce, where in any line of commerce or in any activity affecting commerce in any section of the country, the effect of such acquisition may be substantially to lessen competition, or to tend to create a monopoly.*
> *No person shall acquire, directly or indirectly, the whole or any part of the stock or other share capital and no person subject to the jurisdiction of the Federal Trade Commission shall acquire the whole or any part of the assets of one or more persons engaged in commerce or in any activity affecting commerce, where in any line of commerce or in any activity affecting commerce in any section of the country, the effect of such acquisition, of such stocks or assets, or of the use of such stock by the voting or granting of proxies or otherwise, may be substantially to lessen competition, or to tend to create a monopoly.*
> *[…]*

258 Clayton Antitrust Act of 1914, 15 U.S. Code §§ 12–27, 29 U.S. Code §§ 52–53.
259 Clayton Antitrust Act of 1914 § 7, 15 U.S. Code § 18.

Danach ist der Erwerb eines Unternehmens oder eines Unternehmensanteils (*stocks*), aber auch von Vermögenswerten (*assets*)[260] durch Unternehmen und Privatpersonen untersagt, wenn dies eine wesentliche Einschränkung des Wettbewerbs oder die Bildung eines Monopols zur Folge haben könnte. Ein wichtiger Unterschied zum Sherman Act ist, dass auf der Grundlage von Section 7 Clayton Act nicht tatsächliche Wettbewerbsbeeinträchtigungen nachgewiesen, sondern nur wahrscheinliche Auswirkungen auf den Wettbewerb glaubhaft gemacht werden müssen.[261] Dafür muss der räumlich und sachlich relevante Markt bestimmt werden, auf dem der Wettbewerb geschädigt werden könnte. Unternehmen, die große Zusammenschlüsse planen, müssen die FTC und das US DOJ vorab informieren (*pre-merger notification*).[262] Beide Behörden sind primär für die Durchsetzung des Clayton Act auf Bundesebene zuständig. Sie müssen sich daher bei der Einleitung entsprechender Wettbewerbsverfahren abstimmen.[263] Auf der Grundlage von Section 16 Clayton Act kann eine zivilgerichtliche Durchsetzung des Gesetzes auch durch Generalstaatsanwälte auf der Ebene der US-Bundestaaten sowie durch Privatpersonen erfolgen.

Section 7 Clayton Act kennt keine unmittelbare Entsprechung im EU-Recht, lässt sich jedoch am ehesten mit Art. 2 EU-Fusionskontrollverordnung (FK-VO)[264] zur Beurteilung von Unternehmenszusammenschlüssen vergleichen. Durch Anwendung des Clayton Act könnte verhindert werden, dass über Unternehmenstransaktionen neue Monopolisten entstehen, die wiederum die Interoperabilität einschränken oder verhindern könnten.[265]

(2) Ticketmaster/Live Nation

Ob und inwieweit dieses primär zur Fusionskontrolle gedachte Instrument in der Praxis auf die Schaffung von horizontaler Interoperabilität gerichtet werden kann, ist bei Betrachtung eines wichtigen Anwendungsfalls allerdings fraglich, wie sich beispielhaft an der Fusion von Ticketmaster/Live

260 Dies schließt immaterielle Vermögenswerte ein, z. B. Patente, Marken oder vertragliche Rechte; vgl. United States v. Lever Brothers Company, 216 F. Supp. 887 (S.D.N.Y. 1963).
261 US Supreme Court, Brown Shoe Co., Inc v. United States, 370 U.S. 294, 317 (1962).
262 Die *pre-merger notification* ist eingeführt worden mit dem Hart-Scott-Rodino Antitrust Improvements Act of 1976, 15 U.S. Code § 18a.
263 *Körber*, in: Immenga/Mestmäcker, FK-VO vor Art. 1 Rn. 169.
264 Verordnung (EG) 139/2004, EU ABl. L 024, 29.1.2001, S. 1–22.
265 *Palka*, in: Seton Hall Law Review, 2021, S. 1193, 1235.

Nation im Jahr 2010 zeigt. Ticketmaster ist ein US-Anbieter von Veranstaltungskarten, Live Nation ein Veranstalter von Konzerten sowie Sport- und Kulturveranstaltungen. Aus der Fusion beider Unternehmen ist die Muttergesellschaft Live Nation Entertainment entstanden.

Der Zusammenschluss wurde auf der Grundlage von Section 7 Clayton Act durch das DOJ jedoch nur unter Auflagen genehmigt.[266] So durfte Live Nation Entertainment für zehn Jahre keine Maßnahmen gegen Veranstalter – etwa Betreiber von Konzerthallen oder Stadien – ergreifen, die mit anderen Anbietern für Eintrittskarten als Ticketmaster zusammenarbeiten. Zu solchen Maßnahmen würden bspw. Verpflichtungen zählen, für von Live Nation organisierte Konzerte Eintrittskarten nur über Ticketnation zu vertreiben. Im Sinne der Angebotsvielfalt sollen Veranstaltungsbesucher vielmehr die Möglichkeit haben, entsprechende Karten von anderen Kartenanbietern als Ticketmaster zu kaufen und so von günstigeren Preisen zu profitieren. Infolgedessen musste Ticketmaster eine horizontale Interoperabilität zu anderen Anbietern von Veranstaltungskarten sowohl technisch als auch organisatorisch herstellen. Allerdings ist Ticketmaster derzeit nach wie vor der in den USA mit Abstand verbreitetste Anbieter von Veranstaltungskarten, sodass im Ergebnis die Interoperabilität nicht für eine umfassende Neuordnung im Markt für Eintrittskarten gesorgt hat.[267]

Jedoch stellte das DOJ im Jahr 2020 auch fest, dass Ticketmaster gegen die Auflagen der Unternehmensfusion verstoßen hatte. Live Nation machte bspw. gegenüber Betreibern von Veranstaltungsorten den exklusiven Vertrieb von Veranstaltungskarten über Ticketmaster bei der Buchung von Veranstaltungsorten zur Bedingung. Veranstaltungsorte haben sich diesen Bedingungen unterworfen, weil sie aufgrund der kommerziellen Bedeutung von Live Nation als Tourneeveranstalter befürchteten, weniger oder keine von Live Nation organisierten Konzerte mehr veranstalten zu können und dadurch kommerzielle Nachteile zu erleiden. Gleichzeitig hinderte das Vorgehen von Ticketmaster andere Anbieter von Eintrittskarten am Vertrieb von Karten für von Live Nation organisierte Veranstaltungen, was letztlich den Wettbewerb in diesem Bereich einschränkte. Aus diesem Grund wurden die ursprünglich bis 2020 befristeten Auflagen um weitere fünf Jahre

266 U.S. and Plaintiff States v. Ticketmaster Entertainment, Inc. and Live Nation Entertainment, Inc., Final Judgement 30.10.2010.

267 *Rubinfeld*, European Journal of Law and Economics, 2023, S. 1, 14.

verlängert.[268] Dieser Fall verdeutlicht, dass die technische Gewährleistung von Interoperabilität allein nicht unbedingt ausreicht, um tatsächliche Interoperabilität sicherzustellen.

2. EU

a. AEUV und relevante Wettbewerbsentscheidungen der Kommission

Auf der Ebene der Europäischen Union ist Art. 102 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)[269] die relevante Normierung im Wettbewerbsrecht. Danach ist die missbräuchliche Ausnutzung einer beherrschenden Stellung auf dem Binnenmarkt verboten, soweit dies dazu führen kann, dass der Handel zwischen Mitgliedstaaten beeinträchtigt wird. Die Bestimmung enthält drei Voraussetzungen, die für eine Sanktionierung durch die Europäische Kommission als dafür zuständige Kartellbehörde vorliegen müssen: marktbeherrschende Stellung, missbräuchliche Ausnutzung dieser Stellung und Eignung zur Handelsbeeinträchtigung.

(1) Marktbeherrschung

(a) Marktbeherrschung im Allgemeinen

Eine Definition der Kriterien für die Annahme einer marktbeherrschenden Stellung enthält der AEUV nicht. Vielmehr wird der unbestimmte Rechtsbegriff maßgeblich durch die Fallentscheidungspraxis der Kommission sowie die Rechtsprechung des EuGH ausgefüllt. Die gefestigte Rechtsprechung des EuGH umschreibt die Marktbeherrschung als wirtschaftliche Machtstellung eines Unternehmens, die dieses in die Lage versetzt, die Aufrechterhaltung eines wirksamen Wettbewerbs auf dem relevanten Teilmarkt zu verhindern, indem sie ihm die Möglichkeit verschafft, sich von seinen Wettbewerbern, seinen Abnehmern und schließlich den Verbrauchern gegenüber in einem nennenswerten Umfang unabhängig zu verhal-

268 U.S. and Plaintiff States v. Ticketmaster Entertainment, Inc. and Live Nation Entertainment, Inc., Amended Final Judgement 28.1.2020.

269 Vertrag über die Arbeitsweise der Europäischen Union, EU ABl. C 202, 7.6.2016, S. 47.

ten.[270] Dabei handelt es sich um eine Einzelfallentscheidung, die sich auf einen konkreten, abgrenzbaren Teilmarkt beziehen muss. Faktoren sind vor allem die Struktur des Marktes (inklusive bestehender Marktzutrittsbarrieren), bestimmte Unternehmenseigenschaften und das Verhalten eines Unternehmens im Wettbewerb. Der Marktanteil eines Unternehmens ist regelmäßig der wichtigste Indikator zur Bemessung von Marktmacht.[271] In den Strukturen der Internetökonomie, regelmäßig also auch in Bezug auf verschiedene Arten von Vermittlungsdiensten, spielen die herkömmlichen Beurteilungskriterien dagegen eine eher untergeordnete Rolle.[272] Vielmehr werden bei dieser Marktbetrachtung Aspekte aufgegriffen, die die oben angesprochenen Gefahren von Netzwerk- und Lock-in-Effekten, (fehlendem) Multi-Homing sowie Größen- und Datenvorteilen widerspiegeln.

(b) Charakteristika der Plattformökonomie

Die Charakteristika der Plattformökonomie – Vielseitigkeit von Diensten, Vielgestaltigkeit der Akteure, technischer Wandel, globales Agieren, Vernetzung, datengetriebene Geschäftsmodelle etc. – stellen das Wettbewerbs- und Kartellrecht regelmäßig bereits bei der Abgrenzung bzw. Bestimmung des Marktes vor große Herausforderungen. So ist eine geografische Abgrenzung bei global agierenden Unternehmen häufig nicht zielführend, ebenso wenig wie eine an sprachlichen Kriterien orientierte. Eine sehr kleinteilige Marktbestimmung wird nicht unbedingt der tatsächlichen Einflussreichweite eines Unternehmens gerecht, umgekehrt kann eine zu allgemeine oder zu weite Marktdefinition dazu führen, dass zu viele Akteure als mögliche Wettbewerber berücksichtigt werden. Das lässt sich am Beispiel von Online-Suchmaschinen[273] veranschaulichen: Die Definition eines „Suchmarktes" wirft die Frage auf, welche geografischen und sprachlichen Einschränkungen sinnvoll sind, wenn die möglichen Ergebnisse das gesamte Internet betreffen, welche Akteure auf diesem Markt agieren (nur allgemeine Suchmaschinen wie Google oder auch Produktsuchen wie bei Amazon oder Personensuchen wie bei Facebook) und aus welcher Perspektive

270 EuGH, Rs. C-27/76 – *United Brands/Kommission*, Slg. 1978, 207 Rn. 65.
271 *Eilmann/Kruis*, in: Streinz (Hrsg.), Art. 102 AEUV Rn. 21 f.
272 Hierzu und zum Folgenden auch *Eilmann/Kruis*, in: Streinz (Hrsg.), Art. 102 AEUV Rn. 25.
273 Eingehend *Dewenter/Rösch/Terschüren*, in: NZKart, 2014, S. 387, 387 ff.

dieser Markt zu definieren ist (der suchenden Verbraucher, der gesuchten Anbieter oder der Werbekunden).

Letzterer Aspekt steht in unmittelbarem Zusammenhang mit dem Spezifikum der indirekten Netzwerkeffekte, das bei der Marktabgrenzung ebenfalls problematisch ist.[274] Plattformen dienen verschiedenen Nutzergruppen, die aus unterschiedlichen Märkten oder Marktseiten stammen können, als Vermittler und bewegen sich daher innerhalb von mehrseitigen Märkten. Ein soziales Netzwerk ist bspw. Kommunikationsplattform für Endnutzer, aber auch Werbeplattform für Werbetreibende und Werbende.[275] Eine ähnliche Mehrseitigkeit gilt für Suchmaschinen[276] oder Sprachassistenten[277]. Ob und inwieweit mehrseitige Märkte zu einem Markt zusammengefasst werden können und dabei auch indirekte Netzwerkeffekte zwischen den Marktseiten zu berücksichtigen sind, ist noch nicht abschließend geklärt. Die Tendenz geht aber dahin, vernetzte Marktstrukturen weitreichender zu berücksichtigen. 2021 hat die Europäische Kommission ein Verfahren zur Überarbeitung ihrer bisherigen Bekanntmachung über die Definition des relevanten Marktes im Sinne des Wettbewerbsrechts der (damaligen) Europäischen Gemeinschaft von 1997[278] eingeleitet und ihren neuen Entwurf[279] Ende 2022 zur öffentlichen Konsultation gestellt. Dieser Entwurf enthält Spezifizierungen zur Marktabgrenzung bei mehrseitigen Plattformen und betont u. a., dass indirekte Netzwerkeffekte zwischen Nutzergruppen und inwieweit diese von den Plattformen internalisiert werden, Berücksichtigung finden sollen.[280]

274 Hierzu *Eilmann/Kruis*, in: Streinz (Hrsg.), Art. 101 AEUV Rn. 57 m. w. N.

275 Zur Mehrseitigkeit dieses Marktes *Graef*, in: Telecommunications Policy, 39, 6, 2015, S. 502, 505 ff.

276 Dazu *Dewenter/Rösch/Terschüren*, in: NZKart, 2014, S. 387, 387 ff.

277 Dazu *Rabassa/Sabri/Spaletta*, in: Technological Forecasting and Social Change, 2022–121292, S. 1, 6 ff.

278 Bekanntmachung der Kommission über die Definition des relevanten Marktes im Sinne des Wettbewerbsrechts der Gemeinschaft, EU ABl. C 372, 9.12.1997, S. 5–13.

279 Entwurf einer Bekanntmachung der Kommission über die Definition des relevanten Marktes im Sinne des Wettbewerbsrechts der Gemeinschaft, abrufbar unter https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6528.

280 Entwurf einer Bekanntmachung der Kommission über die Definition des relevanten Marktes im Sinne des Wettbewerbsrechts der Gemeinschaft, Rn. 94 ff.

(c) Microsoft-Entscheidungen

Im vorliegenden Zusammenhang beachtenswerte Entscheidungen betreffen das Unternehmen Microsoft. Während etwa ein beträchtlicher gemeinsamer Marktanteil von 90 % der Unternehmen Microsoft und Skype auf dem Videotelefonie-Markt ihrer Fusion nach Ansicht der Kommission nicht entgegenstand[281], stellte sie in der Rechtssache *Microsoft* von 2004[282] maßgeblich auf Netzwerkeffekte ab. Die Sun Microsystems, Inc., die insbesondere Server und Server-Betriebssysteme vertrieb, hatte Beschwerde bei der Europäischen Kommission mit der Begründung eingereicht, dass sich Microsoft geweigert habe, ihr die erforderlichen Informationen und die nötige Technologie zu übermitteln, um die Interoperabilität ihrer Betriebssysteme für Arbeitsgruppenserver mit dem Windows-Betriebssystem für Client-PCs zu ermöglichen. Kern des Verfahrens waren also Fragen der Interoperabilität sowie der erweiterten Schnittstellenoffenheit und ob deren Fehlen zu einem Wettbewerbsverstoß führen können. Die Kommission bejahte dies im Ergebnis, verhängte eine Geldbuße gegen Microsoft und ordnete bestimmte Abhilfemaßnahmen an, darunter auch die Verpflichtung von Microsoft, umfassende Interoperabilitätsinformationen an Interessierte herauszugeben.

Die beherrschende Stellung auf dem Markt der Betriebssysteme für Client-PCs wurde neben dem – hier als relevant angesehenen – Marktanteil von 90 % und einer anhaltenden Stabilität und Kontinuität[283] vor allem mit indirekten Netzwerkeffekten[284] begründet: Der Nutzen, den Verbraucher aus einem Client-PC-Betriebssystem zögen, hänge von den Anwendungen ab, die sie darauf nutzen könnten. Umgekehrt würden Softwareentwickler Anwendungen vor allem für die beliebtesten Betriebssysteme schreiben.

281 Entscheidung der Kommission vom 7. Oktober 2011 zur Vereinbarkeit eines Zusammenschlusses mit dem Gemeinsamen Markt (Fall COMP/M.6281 – *Microsoft / Skype*) gemäß der Verordnung (EG) Nr. 139/2004 des Rates, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32011M6281. Dazu näher unten C.II.2.b.

282 Entscheidung der Kommission vom 24. Mai 2004 in einem Verfahren gemäß Art. 82 EG-Vertrag und Art. 54 EWR-Abkommen gegen die Microsoft Corporation in der Sache COMP/C-3/37.792 — *Microsoft*, EU ABl. L 32, 6.2.2007, S. 23–28, Gesamtentscheidung abrufbar unter https://ec.europa.eu/competition/antitrust/cases/dec_docs/37792/37792_4177_1.pdf.

283 COMP/C-3/37.792 (Fn. 282), Rn. 430–435.

284 COMP/C-3/37.792 (Fn. 282), Rn. 448–464.

Beides beeinflusse und potenziere sich gegenseitig.[285] Dieser „indirekte Netzwerkeffekt" führe dazu, dass es zwar theoretisch möglich, aber „extrem schwierig, zeitaufwändig, riskant und teuer"[286] wäre, ein alternatives Betriebssystem zu entwickeln, wenn keine Anwendungen dafür programmiert würden. Im Prinzip wäre es daher nötig, die komplette Windows-Schnittstelle in ein alternatives Betriebssystem zu implementieren, was allerdings technisch nicht machbar sei. Wie Versuche (bspw. Linux und IBM) in der Vergangenheit gezeigt hätten, sei es auch nicht erfolgversprechend, Softwareentwickler von der Entwicklung ihrer Anwendungen für ein anderes Betriebssystem zu überzeugen, da ihnen der wirtschaftliche Anreiz fehle. Der „positive Feedback-Loop"[287] bewahre die hohen Marktanteile von Microsoft vor effektiver Konkurrenz. Das entspreche einer Marktzutrittsschranke für Wettbewerber. Deshalb könne das Unternehmen auch unabhängig von seinen Geschäfts- und Endkunden agieren. In Bezug auf den Markt der Betriebssysteme für Arbeitsgruppenserver komme zudem (u. a.) hinzu, dass es eine enge wirtschaftliche und technologische Verbindung zwischen dem letztgenannten Markt und dem Markt der Betriebssysteme für Client-PCs gebe.[288]

Die Klage auf Nichtigerklärung der Kommissionsentscheidung, die Microsoft vor dem Gericht der Europäischen Union (EuG) erhoben hatte, blieb erfolglos. Das EuG erkannte insbesondere Netzwerkeffekte als ein Bemessungskriterium der Marktbeherrschung an.[289]

(2) Missbrauch der marktbeherrschenden Stellung

Das Innehaben einer marktbeherrschenden Stellung allein kann wettbewerbsrechtlich nicht sanktioniert werden. Vielmehr bedarf es zusätzlich eines Missbrauchs dieser Stellung. Dabei wird gemeinhin zwischen Ausbeutungsmissbrauch, Behinderungsmissbrauch und Marktstrukturmissbrauch

285 Die Kommission beschreibt das als „self-reinforcing" („selbstverstärkend"); COMP/C-3/37.792 (Fn. 282), Rn. 458.
286 COMP/C-3/37.792 (Fn. 282), Rn. 453.
287 Was von der Kommission als indirekter Netzwerkeffekt beschrieben wird, wurde von Mircosoft-Entwickler Bill Gates 2002 im Rahmen einer Anhörung vor dem US-Kongress als „positiver Feedback-Loop" bezeichnet. Vgl. Direct Testimony of Bill Gates, Civil Action No. 98–1233, Rn. 25.
288 COMP/C-3/37.792 (Fn. 282), Rn. 526–540.
289 EuG, Rs. T-201/04 – *Microsoft Corp. / Kommission*, ECLI:EU:T:2007:289, Rn. 558.

unterschieden, die wiederum in unterschiedlichen Erscheinungsformen auftreten und auch Überschneidungen aufweisen können.[290] Sie können in unterschiedlichen Ausprägungen auch für Interoperabilitätsfragen Bedeutung erlangen. Art. 102 Abs. 2 AEUV listet als wohl wichtigste, aber nicht abschließende Regelbeispiele Sondertatbestände des Ausbeutungsmissbrauchs auf, von denen insbesondere Art. 102 Abs. 2 lit. b) im vorliegenden Zusammenhang relevant ist. Danach kann ein Missbrauch u. a. in der Einschränkung der Erzeugung, des Absatzes oder der technischen Entwicklung durch ein marktbeherrschendes Unternehmen zum Schaden der Verbraucher gesehen werden. Die Grenzen der einzelnen Missbrauchstatbestände sind aber häufig fließend, sodass eine Verhaltensweise mehreren Regelbeispielen zugeordnet werden oder jedenfalls unter die Generalklausel fallen kann. Gerade im digitalen Sektor, in dem wettbewerbsrelevante Verhaltensweisen eng mit technischen Möglichkeiten zusammenhängen, ist daher die Einzelfallbetrachtung nötig, die entlang allgemeiner Kriterien nach wettbewerbsschädigenden Auswirkungen des Verhaltens fragt.

Dieses zusätzliche Kriterium gilt auch bei der Frage nach der Wettbewerbsrelevanz von Interoperabilität. Eine mangelnde Schnittstellenoffenheit ist nicht per se von den Tatbeständen des Art. 102 AEUV erfasst. Es gibt aber verschiedene Fallgestaltungen, in denen das Fehlen von Interoperabilität oder damit in engem Zusammenhang stehende Verhaltensweisen als wettbewerbswidrig eingestuft werden können.[291] Kriterien und Grenzen sollen nachfolgend anhand von bereits entschiedenen Fällen dargestellt werden.

(a) IBM und Decca Navigator Systems

Einen Unterfall des technischen Behinderungsmissbrauchs kann es darstellen, wenn Mitbewerbern die notwendigen Informationen oder die Möglichkeit einer Kompatibilität ihrer Anlagen mit den Standards eines marktbe-

290 Dazu *Jung*, in: Grabitz/Hilf/Nettesheim/Jung (Hrsg.), Art. 102 AEUV Rn. 163 ff.; *Eilmansberger/Kruis*, in: Streinz (Hrsg.), Art. 102 AEUV Rn. 29 ff.; *Weiß*, in: Callies/Ruffert (Hrsg.), Art. 102 AEUV Rn. 24 ff.

291 Dazu auch eingehend *McMahon*, in Tulane Journal of Technology & Intellectual Property, 9/2007, S. 123, 123 ff.

herrschenden Unternehmens vorenthalten werden.[292] Beide Aspekte sind notwendige Bestandteile von Interoperabilität.

In der Rechtssache IBM, die allerdings ohne förmliche Entscheidung gegen entsprechende Zusagen von IBM eingestellt wurde, hat die Kommission bereits 1984 das Fehlen der Informationsbereitstellung als ein Wettbewerbsproblem festgestellt. IBM, zum damaligen Zeitpunkt der größte Computerhersteller der Welt und damit auch Inhaber einer marktdominanten Stellung in Bezug auf sein System/370 (Prozessoreinheit und Betriebssystem), wurde von der Kommission ein Marktmissbrauch vorgeworfen. Neben zwei anderen Punkten ging es darum, dass IBM anderen Herstellern nicht rechtzeitig die technischen Informationen zur Verfügung gestellt hatte, die erforderlich waren, um die Verwendung von Konkurrenzprodukten mit dem System/370 zu ermöglichen („Schnittstelleninformationen"). Zum anderen sah die Kommission die Tatsache, dass bestimmte Software-Installationsdienste für Benutzer von Nicht-IBM-Prozessoren nicht kompatibel waren, als missbräuchlich in Form einer Diskriminierung gegenüber Nutzern an.[293]

Ohne das Bestehen einer marktbeherrschenden Stellung oder deren Missbrauch einzuräumen, verpflichtete sich IBM u. a., zukünftig rechtzeitig ausreichende Schnittstelleninformationen offenzulegen, damit konkurrierende Unternehmen in der EWG sowohl Hardware- als auch Softwareprodukte an das System/370 anschließen könnten. Gebunden war das sogar an konkrete zeitliche Verpflichtungszusagen (für Schnittstellen zu Hardwareprodukten innerhalb von vier Monaten nach der Ankündigung des betreffenden Produkts und für Schnittstellen zwischen Softwareprodukten sofort bzw. sobald die Schnittstelle einigermaßen stabil ist, jeweils aber spätestens bei allgemeiner Verfügbarkeit des Produkts). Da die Kommission davon ausging, dass diese Verpflichtung auch zu einer wesentlichen Verbesserung der Stellung sowohl der Benutzer (diese könnten zu einem früheren Zeitpunkt zwischen verschiedenen Anbietern wählen) als auch der Wettbewerber (diese könnten sich auf Kompatibilität einstellen) führen würde, wurde das Verfahren jedoch eingestellt.

292 Dazu auch *Jung*, in: Grabitz/Hilf/Nettesheim/Jung (Hrsg.), Art. 102 AEUV Rn. 215 f.

293 Rs. IV/29.479. Eine Zusammenfassung des Falls sowie der Verpflichtungszusagen ist abgedruckt im 14. Bericht über die Wettbewerbspolitik der Kommission, abrufbar unter https://op.europa.eu/en/publication-detail/-/publication/3c93e6fa-934b-4fb9-b927-dc9fed71ccfe, S. 77 ff.

Im Fall Decca Navigator System ging es hingegen darum, dass ein Unternehmen, das im Nord-/Ostsee-Raum die Märkte für die Sendung und den Empfang von Navigationsfunksignalen kontrollierte, die Art seiner Signale dergestalt geändert hatte, dass sie von bislang kompatiblen Empfangsgeräten konkurrierender Hersteller nicht mehr empfangen werden konnten. Das führte entsprechend zu technischen und Lizenz- und Marktaufteilungsvereinbarungen mit Wettbewerbern, die keine andere Wahl hatten, als die jeweiligen Bedingungen anzunehmen, da es keine Alternative für die Schifffahrt in dem betreffenden Bereich gab, die die nötigen Standards erfüllte. Die Kommission entschied 1988, dass der Betreiber, Racal-Decca Marine Navigation Limited, seine beherrschende Stellung bei kommerziellen DNS-Empfangsgeräten auf wettbewerbsbeschränkende Weise genutzt hatte, indem der Zugang Dritter zu dem Markt für kommerzielle Empfangsgeräte und die Wahlfreiheit der Verbraucher eingeschränkt wurden.[294] Nicht nur die Vereinbarungen wurden dabei als Wettbewerbsverstoß gesehen, sondern auch die tatsächliche (technische) Änderung des Signals.

(b) Microsoft

Um einen ähnlichen Sachverhalt wie in der Rechtssache IBM ging es auch in der bereits im Zusammenhang mit der Marktabgrenzung (C.II.2.a(1)) erwähnten Microsoft-Entscheidung von 2004. Hier sah die Europäische Kommission einen Marktmissbrauch einerseits in der Weigerung von Microsoft, Interoperabilitätsinformationen[295] zu liefern und deren Nutzung zu gestatten, im Ergebnis also seine Schnittstelle nicht nur zu öffnen, sondern das System interoperabel zu machen (ohne aber den Quellcode dafür offenbaren zu müssen).[296] Dabei hob sie auch den Aspekt hervor, dass es sich bei der Weigerung um ein generelles Verhaltensmuster von

294 Entscheidung der Kommission vom 21. Dezember 1988 in einem Verfahren nach Art. 85 und 86 EWG-Vertrag (IV/30.979 und 31.394, *Decca Navigator System),* EU ABl. L 43 vom 15.02.1989, S. 27–48.

295 Darin sah die Kommission sehr weitgehend die „vollständigen und genauen Spezifikationen für alle Protokolle, die in Windows-Betriebssystemen für Arbeitsgruppenserver implementiert und von Windows-Arbeitsgruppenservern genutzt werden, um den Windows-Arbeitsgruppennetzwerken Daten- und Druckdienste sowie Gruppen- und Nutzerverwaltungsdienste einschließlich der Dienste Windows-Domänenkontrolle, Active Directory und Group Policy zur Verfügung zu stellen".

296 COMP/C-3/37.792 (Fn. 282), Rn. 560 ff.

Microsoft handle, das den Wettbewerb auf dem Markt der Betriebssysteme für Arbeitsgruppenserver auszuschalten drohe und sich negativ auf die technische Entwicklung und die Verbraucherinteressen auswirke.[297]

Anderseits wurde auch ein Marktmissbrauch in der Kopplung des Verkaufs des Windows-Betriebssystems für Client-PCs mit dem des Windows Media Players (WMP) gesehen.[298] Die Kommission setzte sich hier vertieft damit auseinander, dass angesichts der indirekten Netzwerkeffekte auf dem Markt für Medienabspielgeräte das allgegenwärtige Vorhandensein des WMP-Codes dieser Anwendung einen erheblichen Wettbewerbsvorteil verschaffe, der schädliche Auswirkungen auf die Struktur des Wettbewerbs auf diesem Markt haben könne. Auch das EuG bestätigte dies letztlich in seiner Entscheidung und hob insbesondere hervor, dass die Kommission „umso mehr berechtigt" gewesen sei, Maßnahmen zu ergreifen, weil der Markt durch erhebliche Netzwerkeffekte gekennzeichnet sei und die Ausschaltung des Wettbewerbs daher schwer rückgängig zu machen wäre.[299]

(c) Google Shopping

Um „Netzwerkeffekte", hier aber in einem anderen Wortsinn, geht es im Übrigen auch bei einer anderen möglichen und mit den vorherigen Ausführungen im Zusammenhang stehenden Form des Marktmissbrauchs: der sog. Selbstbevorzugung bzw. -präferenzierung (im engl. „self-preferencing"). Der Begriff beschreibt die Vorgehensweise von häufig bereits marktdominanten Akteuren, eigene oder bestimmte dritte Dienste (bspw. Dienste im gemeinsamen Mutterkonzern, Unterfunktionen eines multidimensionalen Dienstes oder in vertraglichen Beziehungen stehende Dienste) gegenüber anderen Diensten zu bevorzugen. Diese Vorgehensweise kann einen Marktmissbrauch darstellen, wenn dadurch Mitbewerber faktisch vom Wettbewerb um potenzielle Kunden ausgeschlossen werden. Die Selbstpräferenzierung ist dabei nicht deckungsgleich mit dem Fehlen von Interoperabilität, kann aber Überschneidungen damit aufweisen und basiert auf dem gleichen Hintergedanken zu wettbewerbsrechtlichen Implikationen.

297 COMP/C-3/37.792 (Fn. 282), Rn. 693–708.
298 COMP/C-3/37.792 (Fn. 282), Rn. 792 ff.
299 EuG, Rs. T-201/04 – *Microsoft Corp. / Kommission*, ECLI:EU:T:2007:289, Rn. 562.

Dies lässt sich etwa am Beispiel des Google-Shopping-Falls veranschaulichen.[300]

Dieser Fall bezog sich auf eine Form der Selbstpräferenzierung innerhalb der Suchmaschine Google, die bis mindestens 2014 anhielt: Bei der Eingabe von produktbezogenen Suchbegriffen sowohl in der allgemeinen Google-Suche als auch über den separaten Bereich der Produktsuche („Shopping"-Reiter im Menü) zeigte die Suchmaschine Produkte verschiedener Partnershops samt Preisen in einer vergleichenden Ansicht an. In der allgemeinen Suche waren diese in einem abgegrenzten Bereich „gesponserter Inhalte" oberhalb der eigentlichen Websuchergebnisse zu finden. Die Kommission entschied 2017, dass Google mit der spezifischen Gestaltung dieses Mechanismus gegen Art. 102 AEUV verstoßen hatte. Google habe seine Stellung als marktbeherrschendes Unternehmen auf den Märkten für allgemeine Online-Suchdienste und für Online-Vergleichsdienste in wettbewerbsrechtlicher Weise missbraucht, indem konkurrierende Preisvergleichsdienste zwar weiterhin in den Ergebnissen der allgemeinen Suche über Links und kurze Ausschnitte aus dem Inhalt ihrer Webseiten auftauchten. Allerdings wurden sie zum einen nicht wie bei Googles eigenem Preisvergleichsdienst in einer Box am oberen Rand der Suche hervorgehoben, sondern lediglich in den generischen Suchergebnissen angezeigt. Zum anderen wurde Letzteres zusätzlich durch die Anwendung sog. „Anpassungsalgorithmen" (des sog. „Panda-Algorithmus" im konkreten Fall) derart beeinflusst, dass konkurrierende Preisvergleichsdienste in der Rangfolge der allgemeinen Ergebnisse zurückgestuft wurden.

Diese Anpassungsalgorithmen waren (vereinfacht erklärt) so programmiert, dass sie die Merkmale einer Website analysierten und insbesondere solchen Websites eine geringere Relevanz und damit einen niedrigeren Ranking-Status zuwiesen, die keine „originären" Inhalte enthielten (was bei Preisvergleichs- und ähnlichen Diensten, die lediglich Inhalte Dritter sammeln und vergleichend darstellen, regelmäßig der Fall ist). Für Verbraucher, die von einer generischen Suche eine neutrale Darstellung geeigneter Inhalte im Internet erwarteten, war diese algorithmische (De-)Präferenzierung jedoch nicht transparent. Vielmehr verleitete die Ausgestaltung sie dazu, sich nur auf das „relevanteste" Angebot von Google Shopping zu

300 Decision C(2017) 4444 final relating to proceedings under Article 102 TFEU and Article 54 of the EEA Agreement (Case AT.39740 – Google Search (Shopping)), https://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf.

verlassen und nicht durch die niedriger „gerankten" Ergebnisse zu scrollen, um nach Alternativen zu suchen. Faktisch führte das zu einem Rückgang des Verkehrs auf Konkurrenzwebseiten und einer Zunahme des Verkehrs in Googles eigenem Dienst.

Nach Ansicht der Kommission nahm dies den konkurrierenden Diensten die Möglichkeit, die Nutzer von ihrem eigenen Angebot zu überzeugen, und es hinderte die Verbraucher in der EU daran, tatsächlich zwischen verschiedenen Diensten zu wählen und die Vorteile eines innovativen Wettbewerbs voll auszuschöpfen. Die Kommission verhängte daraufhin eine Geldbuße von 2,42 Milliarden Euro, die auch vom Gericht der Europäischen Union bestätigt wurde.[301] Die Schlussfolgerung für den vorliegenden Kontext ist, dass es jedenfalls aus wettbewerbsrechtlicher Sicht nicht nur auf die Interoperabilität eines Dienstes ankommt (die konkurrierenden Preisvergleichsdienste hatten Zugang über eine Schnittstelle), sondern auch darauf, wie diese ausgestaltet ist.

(d) Google AdTech

Den Konnex zwischen Selbstpräferenzierung und Netzwerkeffekten bzw. Interoperabilitätserwägungen veranschaulichen auch die wettbewerbsrechtlichen Verfahren zum Werbesystem von Google. Im Kern, obwohl mit unterschiedlichen Schwerpunkten, geht es dabei um die (Allein-)Stellung von Google im Online-Werbemarkt, die sich über verschiedene dem Unternehmen angehörige Dienste ergibt und mit der die Regeln für den Wettbewerb diktiert werden. Die Vorwürfe bezogen sich auf Selbstpräferenzierung, mangelnde Interoperabilität, Intransparenz und weitere diskriminierende Verhaltensweisen.[302]

Haupteinnahmequelle von Google ist Online-Werbung sowohl durch den Verkauf von Werbeflächen auf eigenen Websites und in eigenen Apps als auch als Vermittler zwischen Werbetreibenden und Publishern. Letzteres erfolgt maßgeblich über den Betrieb mehrerer AdTech-Dienste, darunter zwei Tools zum Anzeigenkauf für Werbetreibende („Google Ads" und „DV 360"), einen Ad-Server für Publisher („DoubleClick For Publishers (DFP)") und schließlich eine Anzeigenbörse („AdX"), über die letztlich der

301 EuG, Rs. T-612/17 – *Google and Alphabet v Commission (Google Shopping)*, ECLI:EU:T:2021:763.

302 Eingehend und weiterführend *Höppner/Piepenbrock*, Digitale Werbung und das Google Ökosystem.

Verkauf und Kauf von Werbeanzeigen in Form von Echtzeitauktionen stattfindet. AdX wird dabei insbesondere von den anderen genannten Diensten gespeist.

Neben den oben (C.II.1.a(2)) dargestellten Entwicklungen in den USA wurden wettbewerbsrechtliche Maßnahmen gegen die AdTech-Strategie von Google bereits in einigen EU-Mitgliedstaaten auf nationaler Ebene ergriffen. So hatte bspw. die französische Wettbewerbsbehörde (*Autorité de la concurrence*) im Juni 2021 ein Bußgeld in Höhe von 220 Millionen Euro verhängt.[303] Grund waren die von Google implementierten Praktiken zur Förderung seiner eigenen Werbevermittlungstechnologien: Der DFP-Ad-Server bevorzugte die Anzeigenbörse AdX, indem er ihr insbesondere den von konkurrierenden Publisher-Plattformen angebotenen Preis angab und AdX darauf basierend den Auktionsprozess (sprich: die Preise entlang der Wettbewerbsintensität) optimierte. AdX bevorzugte umgekehrt den DFP-Server dadurch, dass konkurrierenden Ad-Servern technische und vertragliche Beschränkungen auferlegt wurden, was sich auch auf die Interaktionsmöglichkeiten von deren Kunden negativ auswirkte. Zentral für den Marktmissbrauch war hier also wieder die Selbstpräferenzierung, die Serverbetreiber und deren Kunden (Werbetreibende und Publisher) benachteiligte. Erwähnenswert ist allerdings, dass im Zentrum des Verfahrens der französischen Behörde auch die eingeschränkte Interoperabilität von AdX mit Anzeigenservern von Dritten stand, die als maßgeblicher Faktor sowohl für die Einnahmen der Publisher aus ihren Werbeflächen als auch für die Attraktivität der Auktionsplattformen gesehen wurde. Google hatte allerdings im Verfahren die Verpflichtungszusage gemacht, Anzeigenservern von Drittanbietern eine Interoperabilitätsmethode mit dem DFP-Server zu bieten, die einen Leistungswettbewerb zwischen diesen und AdX beim Kauf von Inventar von Publishern, die DFP nutzen, ermöglicht. Auch hatte sich Google verpflichtet, Änderungen an bestehenden Konfigurationen (AdX Direct und nicht verkaufte Werbebuchungen) vorzunehmen, die es Publishern, die Ad-Server von Drittanbietern verwenden, ermöglichen, in Echtzeit auf die AdX-Nachfragen zuzugreifen.

Auch die Wettbewerbsbehörde *Competition and Markets Authority* (CMA) im Vereinigten Königreich hat im Mai 2022 eine umfassende Untersuchung eingeleitet, die allerdings noch nicht zu einem finalen Ergebnis

303 Décision n° 21-D-11 du 7 juin 2021 relative à des pratiques mises en œuvre dans le secteur de la publicité sur Internet, https://www.autoritedelaconcurrence.fr/sites/default/files/integral_texts/2021-06/21d11_0.pdf.

gekommen ist.[304] Einerseits geht es um Interoperabilität – die CMA prüft, ob die Praktiken von Google den Wettbewerb dadurch verzerren, dass das Unternehmen die Interoperabilität seines Anzeigenaustauschs mit Ad-Servern von Drittanbietern einschränkt und/oder diese Dienste vertraglich miteinander verknüpft – und andererseits um Selbstpräferenzierung – die CMA befürchtet, dass Google möglicherweise seinen Publisher-Ad-Server und seine Anzeigenkaufdienste genutzt hat, um illegal seine eigene Anzeigenbörse zu bevorzugen, und gleichzeitig Schritte unternommen hat, um die von Konkurrenten angebotenen Dienste auszuschließen.

Auf Unionsebene hat die Europäische Kommission bereits im Juni 2021 Untersuchungen gegen Google in Bezug auf wettbewerbswidriges Verhalten auf dem Online-Werbemarkt eingeleitet.[305] Im Juni 2023 hat sie eine Mitteilung von Beschwerdepunkten an das Unternehmen gerichtet – ein formeller Schritt bei mutmaßlichen Verstößen, der Stellungnahme- und weitere Verfahrensrechte des Adressaten einleitet, aber dem Untersuchungsergebnis noch nicht vorgreift.[306] Darin vertritt die Kommission die Auffassung, dass Google als marktbeherrschendes Unternehmen[307] gegen die EU-Kartellvorschriften verstoßen hat, indem es seine eigenen Online-Display-Werbetechnologiedienste zum Nachteil konkurrierender Anbieter von Werbetechnologiediensten, Werbetreibenden und Online-Publishern bevorzugt. Konkret – wie in der Entscheidung der französischen Wettbewerbsbehörde festgestellt – bevorzuge AdX den Google-eigenen Dienst DFP, indem beispielsweise im Voraus über den Wert des besten und damit zu schlagenden Gebots der Wettbewerber informiert werde. Außerdem werde wiederum die Anzeigenbörse AdX von den Anzeigenkauf-Tools Google Ads und DV360 bevorzugt, indem Gebote auf anderen Anzeigenbörsen überhaupt nicht abgegeben würden. Interessant ist aber vor allem die Rechtsfolge, die die Kommission in Aussicht stellt, sollten die Vorwürfe zutreffen und damit ein Verstoß gegen Art. 101, 102 AEUV vorliegen: Eine verhaltensbezogene Abhilfemaßnahme gegen die Selbstpräferenzierung sei wahrscheinlich un-

304 Vgl. zum Verfahren und zu den jüngsten Erweiterungen https://www.gov.uk/cma-cases/investigation-into-suspected-anti-competitive-conduct-by-google-in-ad-tech.

305 Vgl. die Pressemitteilung vom 22. Juni 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3143.

306 Vgl. die Pressemitteilung vom 14. Juni 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3207.

307 In Bezug auf Tools für den Anzeigenkauf für Werbetreibende (in diesem Fall „Google Ads“ und „DV 360“) sowie für Ad-Server für Publisher (in dem Fall „DFP“).

wirksam, da Google mit seinem Publisher-Ad-Server und seinen Anzeigenkauf-Tools auf beiden Seiten des Marktes aktiv und marktbeherrschend sei und daher ein inhärenter Interessenkonflikt vorliege. Die Kommission vertritt daher vorläufig die Auffassung, dass Google die Wettbewerbsbedenken nur durch die obligatorische Veräußerung eines Teils seiner Dienste ausräumen könnte.

(e) RTE und ITP

Während bereits das Vorenthalten technischer Informationen einen Marktmissbrauch darstellen kann, wie an den Fällen von IBM und Microsoft (oben C.II.2.a(2)(a)) gezeigt wurde, kann das unter Umständen auch beim Vorenthalten von Leistungen der Fall sein. Aus Art. 102 AEUV kann sich für marktbeherrschende Unternehmen die Verpflichtung ergeben, eigene Leistungen nicht willkürlich zurückzuhalten. Das betrifft zum einen Unternehmen, die eine allgemein benötigte Einrichtung oder Infrastruktur kontrollieren, zum anderen solche, die einen Markt für Vorprodukte beherrschen und Wettbewerb auf nachgelagerten Wirtschaftsstufen befürchten.[308]

Die Europäische Kommission wendet diese unter dem Stichwort der „essential facility doctrine" diskutierte Praxis bereits seit 1992 relativ breit verstanden an. Als missbräuchlich sieht sie in solchen Fällen ein Verhalten dann, wenn die Versagung der konkreten Leistung ein unübliches Geschäftsgebaren darstellt, das durch keinen objektiven wirtschaftlichen Grund gerechtfertigt ist und betroffenen Wettbewerbern erhebliche Nachteile aufbürdet.[309] Unter einer „wesentlichen Einrichtung" versteht die Kommission eine Einrichtung oder Infrastruktur, die wesentlich ist, um Kunden zu erreichen und/oder Wettbewerbern die Durchführung ihrer Geschäftstätigkeit zu ermöglichen, und die mit angemessenen Mitteln nicht

308 Hierzu und zum Folgenden eingehend *Jung*, in: Grabitz/Hilf/Nettesheim/Jung (Hrsg.), Art. 102 AEUV Rn. 238 ff., 254 ff.

309 Vgl. etwa Entscheidung der Kommission vom 18. Juli 1988 betreffend ein Verfahren nach Art. 86 des EWG-Vertrages (IV/30.178 – *Napier Brown/British Sugar*), EU ABl. L 284 v. 19.10.1988, S. 41–59. Allg. zum Konzept *Haus*, Zugang zu Netzen und Infrastruktureinrichtungen, speziell bezogen auf für Medien relevante Dienste S. 35 ff.

neu geschaffen werden kann.[310] Die europäischen Gerichte sind dagegen zurückhaltender und fordern insbesondere eine Unentbehrlichkeit der angebotenen Leistung und dass mit dem Vorenthalten jeglicher Wettbewerb (auf dem benachbarten Markt) ausgeschlossen werden kann.[311] Ein Missbrauch einer marktbeherrschenden Stellung in diesem Sinne kann auch im Vorenthalten urheberrechtlicher Lizenzen (als „Leistung") liegen und ist damit auf mehreren Ebenen auch für Interoperabilitätsfragen relevant.[312] So kann der Inhaber von für einen Marktzugang essenziellen Immaterialgüterrechten (bspw. Patente, die für die Einhaltung von Standards essenziell sind) nach Art. 102 AEUV verpflichtet werden, sich gegenüber Wettbewerbern an die sog. FRAND-Bedingungen (Fair, Reasonable And Non-Discriminatory) zu verhalten, im Ergebnis also seine Immaterialgüterrechte diesen anderen Marktteilnehmern zu diesen Bedingungen zu lizenzieren.[313]

Zur Veranschaulichung dieser Grundsätze können die verbundenen Rechtssachen Radio Telefis Eireann (RTE) und Independent Television Publications Ltd (ITP) angeführt werden, über die der EuGH 1995 in einem wettbewerbsrechtlichen Verfahren mit Medienbezug zu entscheiden hatte.[314] Ein unabhängiger Verlag – die Magill TV Guide Ltd – wollte zum damaligen Zeitpunkt einen gedruckten, umfassenden wöchentlichen Fernsehprogrammführer in Irland herausgeben. Das wurde ihm aber von irischen und britischen Fernsehanstalten (RTE, IPT und auch der britischen BBC) untersagt, indem die Einräumung von Lizenzen verweigert bzw. ge-

310 Vgl. etwa Entscheidung der Kommission vom 21. Dezember 1993 betreffend ein Verfahren nach Art. 86 EG-Vertrag (IV/34.689 – *Sea Containers gegen Stena Sealink*), EU ABl. L 15 v. 18.1.1994, S. 8–19.

311 Eingehend und m. w. N. *Jung*, in: Grabitz/Hilf/Nettesheim/Jung (Hrsg.), Art. 102 AEUV Rn. 258 ff.

312 In seinem IMH-Health-Urteil entschied das EuG etwa, dass ein Missbrauch durch Vorenthalten einer urheberrechtlichen Lizenz an nach Art. 4 Abs. 2 des deutschen Urheberrechtsgesetzes geschützten Datenbankstrukturen, die sich zum Marktstandard entwickelt haben und denen sich ein Wettbewerber anpassen muss, dann vorliegt, wenn die Verweigerung der Lizenz das Auftreten eines neuen Erzeugnisses verhindert, nach dem eine potenzielle Nachfrage der Verbraucher besteht, wenn die Verweigerung nicht gerechtfertigt ist und wenn sie geeignet ist, jeglichen Wettbewerb auf einem abgeleiteten Markt auszuschließen. Dazu auch *Weiß*, in: Callies/Ruffert, Art. 102 AEUV Rn. 43.

313 Grundlegend EuGH, Urt. v. 6.4.1995, Rs. C-241/91 P und C-242/91 P – *RTE und ITP / Kommission*, Slg. 1995 I-00743; Urt. v. 26.11.1998, Rs. C-7/97 – *Bronner*, ECLI:EU:C:1998:569; Urt. v. 29.4.2004, Rs. C-418/01 – *IMS Health*, ECLI:EU:C:2004:257.

314 Rs. C-241/91 P und C-242/91 P – *RTE und ITP / Kommission*, Slg. 1995 I-00743.

gen eine Verbreitung ohne entsprechende Lizenz vorgegangen wurde. Die Veranstalter veröffentlichten bis zu dem Zeitpunkt ihre Programme selbst und räumten auf Anfrage Tageszeitungen oder Zeitschriften unentgeltliche Lizenzen für die Nennung und Abbildung ihrer Programme ein. Diese waren aber auf bestimmte Programmteile (zeitlich nur 24 oder 48 Stunden im Voraus) begrenzt und standen unter bestimmten Bedingungen, wie die Inhalte dargestellt werden durften.

Die Kommission sah darin einen Wettbewerbsverstoß und wies die Fernsehanstalten 1989 insbesondere an, Dritten auf Anfrage ihre jeweiligen wöchentlichen Programmvorschauen auf nichtdiskriminierender Basis zur Verfügung zu stellen und die Wiedergabe durch Dritte zu gestatten. Weiter hieß es dort, dass ein Fernsehveranstalter bei einer Entscheidung zur Vergabe von Lizenzen für die Wiedergabe der Programminformationen die Lizenzgebühren angemessen gestalten müsse.[315] Sowohl das EuG[316] als auch der EuGH bestätigten diese Entscheidung.

Zwar ergebe sich aus der Eigenschaft als Inhaber eines Immaterialgüterrechts allein keine beherrschende Stellung. Jedoch seien die Grundinformationen über den Sendekanal, den Tag, die Uhrzeit und den Titel der Sendungen die notwendige Folge der Programmplanung der Fernsehanstalten, die damit für Unternehmen wie die Firma Magill, die diese Informationen zusammen mit Kommentaren oder Bildern veröffentlichen möchten, die einzige Informationsquelle seien. Daraus ergebe sich ein faktisches Monopol über diese Informationen. Die Ausübung des Ausschließlichkeitsrechts (hier: des Urheberrechts an diesen Informationen) könne „unter außergewöhnlichen Umständen" auch ein wettbewerbsrechtlich missbräuchliches Verhalten darstellen.[317] Maßgeblich berücksichtigt wurde die Tatsache, dass es keinen tatsächlichen oder potenziellen Ersatz für einen wöchentlichen Fernsehprogrammführer gab, der Informationen über die Programme der folgenden Woche enthielt – Verbraucher hatten also keine andere Möglichkeit, als sich die wöchentlichen Programmführer für jeden Sender zu kaufen und daraus selbst die Angaben zu entnehmen, die sie benötigten, um Vergleiche anzustellen. Durch dieses Verhalten behielten sich die Veranstalter einen abgeleiteten Markt — den der wöchentlichen Fernsehprogrammführer — vor, auf dem sie selbst gar nicht tätig waren (sie veröffentlichten

315 Case IV/31.851 — *Magill TV Guide/ITP, BBC und RTE*, EU ABl. 1989, L 78, S. 43.
316 EuGH, Rs. T-76/89 R, T-77/89 R und T-91/89 R – *RTE u. a./Kommission,* Slg. 1989, 1141.
317 *RTE und ITP / Kommission* (Fn. 314), Rn. 50.

nur Einzelprogramme ihrer Sender), indem sie jeden Wettbewerb auf diesem Markt ausschlossen und damit den Zugang zu den unentbehrlichen Grundinformationen verweigerten.

(f) Apple/Spotify

Schließlich kann ein Missbrauch einer marktbeherrschenden Stellung auch dann gegeben sein, wenn ein Zugang zwar grundsätzlich eingeräumt, diese Art von Interoperabilität aber an Bedingungen geknüpft ist, die einseitig vom marktbeherrschenden Unternehmen bestimmt werden. Das betrifft vorrangig das „Wie" der Interoperabilität, also deren Ausgestaltung. Es kann aber auch bereits das „Ob" betreffen, wenn die Bedingungen für den Zugang derart ungünstig sind, dass sich die Inanspruchnahme der Schnittstelle wirtschaftlich nicht oder nicht sinnvoll umsetzen lässt.

Als Beispiel für eine derartige Entwicklung im digitalen Sektor kann der App Store von Apple angeführt werden. Im Juni 2020 hat die Kommission ein förmliches Verfahren eingeleitet, in dessen Zentrum mögliche Wettbewerbsverstöße durch die App Store-Bedingungen für App-Entwickler und -Vertreiber stehen.[318] Auf Apple- bzw. iOS-Endgeräten ist der App Store zwingendes Zugangstor für die Installation von Anwendungen – eine Schnittstelle für dritte Bezugsquellen existiert herstellerseitig nicht. Apple prüft dabei, welche Anwendungen in den App Store gelangen können, und bindet diese an bestimmte Bedingungen. Im Verfahren der Kommission geht es dabei insbesondere um die verpflichtende Nutzung des Apple-eigenen In-App-Kaufsystems (IAP), wobei Apple App-Entwicklern eine Provision von 30 % auf alle Abonnementgebühren über IAP berechnet. Zudem geht es um Einschränkungen der Möglichkeit von Entwicklern, iPhone- und iPad-Nutzer über alternative, günstigere Kaufmöglichkeiten außerhalb von Apps zu informieren (sog. Anti-Steering). Zwar erlaubt Apple den Nutzern, an anderer Stelle (z. B. auf der Website des App-Entwicklers) erworbene Inhalte wie Musik, E-Books und Hörbücher auch in der App zu konsumieren, seine Regeln hindern Entwickler jedoch daran, Nutzer über solche Kaufmöglichkeiten zu informieren, die in der Regel günstiger

318 Vgl. Pressemitteilung vom 16.6.2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1073.

sind. Parallel läuft eine Untersuchung in Bezug auf Apple Pay insgesamt.[319] Anlass für die Untersuchungen waren Beschwerden des Musikstreaming-Dienstes Spotify und eines E-Book-/Hörbuch-Händlers über die Auswirkungen der App-Store-Regeln auf den Wettbewerb.[320] In den USA gibt es ähnliche Beschwerden im Verfahren zwischen Epic Games und Apple – der Entwickler des Online-Spiels Fortnite hatte seine Spieler im Spiel bewusst auf günstigere In-Game-Kaufbedingungen außerhalb des Apple-Kosmos hingewiesen, auch, um danach aufgrund der erwarteten Reaktion von Apple ein Verfahren anstrengen zu können.[321]

Das Verfahren ist zwar noch nicht abgeschlossen, die Kommission übermittelte aber am 30. April 2021 ihre Beschwerdepunkte an Apple.[322] Darin teilte sie ihr vorläufiges Untersuchungsergebnis mit, wonach Apple seine marktbeherrschende Stellung im Bereich des Vertriebs von Musikstreaming-Apps über seinen App Store missbraucht und dadurch den Wettbewerb auf dem Musikstreaming-Markt verfälscht habe. Das bezieht sich auf die Anwendung dieser Regeln auf alle Musikstreaming-Apps, die mit der Apple-eigenen Streaming-App „Apple Music" im EWR im Wettbewerb stehen. Die Kommission moniert, dass für App-Entwickler der App Store das einzige Zugangstor zu Verbrauchern sei, die Mobilgeräte von Apple mit dem Apple-Betriebssystem iOS nutzten. Die Geräte und die Systemsoftware von Apple bildeten ein „geschlossenes Ökosystem", in dem Apple alle Aspekte der Nutzererfahrung für iPhones und iPads steuere. Die Nutzer von Apple-Geräten blieben dieser Marke sehr treu und seien nicht so leicht dazu zu bewegen, zu einer anderen Marke zu wechseln. Für Entwickler führe daher kein Weg am App Store und den dort einseitig diktierten Bestimmungen vorbei, um diesen Markt zu erschließen. Diese Bedingungen hält die Kommission aber für missbräuchlich: Die obligatorische Nutzung von IAP für In-Game-Käufe sei durch die damit verbundene 30 %-Provision nicht nur für Entwickler missbräuchlich, sondern wirke sich zu Lasten der Verbraucher aus, da die Entwickler die Gebühr an die Nutzer weitergäben.

In Bezug auf das Anti-Steering befürchtet die Kommission nach ihren Untersuchungen, dass die Nutzer von Apple-Geräten deshalb deutlich

319 Vgl. Pressemitteilung vom 16.6.2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1075.

320 AT.40437, Verfahrensdokumentation abrufbar unter https://competition-cases.ec.europa.eu/cases/AT.40437.

321 Epic Games, Inc. v. Apple Inc., Az. 20-cv-05640-YGR.

322 Vgl. Pressemitteilung vom 30.4.2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2061.

höhere Gebühren für ihre Musikabonnements bezahlen oder bestimmte Abonnements nicht direkt in den Apps erwerben können. In einer Klarstellung vom 28. Februar 2023 teilte sie jedoch mit, dass das Verfahren in Bezug auf die IAP-Verpflichtung nicht mehr weiterverfolgt werde.[323] Demgegenüber wurden die Bedenken in Bezug auf das Anti-Steering nochmals konkretisiert: Diese Beschränkungen seien weder nötig noch verhältnismäßig für die Bereitstellung des App Stores, wirkten sich (auch finanziell) nachteilig auf die Nutzer sowie negativ auf die Interessen der Entwickler von Musik-Streaming-Apps aus, indem sie die effektive Auswahl für Verbraucher einschränkten. Das Verfahren, das derzeit noch läuft, dürfte sich durch die zwischenzeitlich erfolgte Aufnahme der Regeln zur Interoperabilität und Diskriminierungsfreiheit in App-Stores im DMA (dazu unten C.II.2.c(3)und C.II.2.c(4)) nochmals in neuer Gestalt darstellen.

(3) Eignung zur Beeinträchtigung des Handels in der EU

Das Wettbewerbsrecht der Union und damit auch die Zuständigkeit der Kommission ist allerdings nur dann einschlägig, wenn der Missbrauch auch den Handel bzw. den Wirtschaftsverkehr zwischen den Mitgliedstaaten beeinträchtigt. Es ist also ein Zwischenstaatsbezug erforderlich, der dann fehlen kann, wenn sich die Auswirkungen auf einen einzigen Mitgliedstaat beschränken.

In seiner ständigen Rechtsprechung geht der EuGH von einer möglichen Beeinträchtigung des zwischenstaatlichen Handels bereits dann aus, wenn sich anhand einer Gesamtheit objektiver rechtlicher oder tatsächlicher Umstände mit hinreichender Wahrscheinlichkeit voraussehen lässt, dass die Vereinbarung unmittelbar oder mittelbar, tatsächlich oder der Möglichkeit nach den Handelsverkehr zwischen Mitgliedstaaten beeinflussen kann.[324] Wenn die marktbeherrschende Stellung in einem Gebiet besteht, das über das Territorium eines Mitgliedstaates hinausreicht, und die betreffende Verhaltensweise gegenüber Abnehmern in mehreren Mitgliedstaaten prakti-

323 Vgl. Pressemitteilung vom 28.2.2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1217.

324 EuGH, Rs. C-56/65 – *Société Technique Minière / Maschinenbau Ulm*, Slg. 1966, S. 282, Rn. 17.

ziert wird, liegt ohne weiteres der geforderte Zwischenstaatsbezug vor.[325] Im medienbezogenen Zusammenhang agieren relevante marktdominante Akteure regelmäßig über nationale Grenzen hinweg, und das unter gleichen Bedingungen und mit gleichen Auswirkungen auf verschiedene Mitgliedstaaten. Im digitalen Umfeld ist die Einschlägigkeit dieses Kriteriums bei Vorliegen der zuvor genannten Voraussetzungen daher regelmäßig unproblematisch.

b. Fusionskontrolle

Ein weiteres Instrument des Wettbewerbsrechts auf EU-Ebene ist das Fusionskontrollrecht. Nach den Regeln der Fusionskontroll-Verordnung (FK-VO)[326] hat die Europäische Kommission die Aufgabe, Fusionen und Übernahmen von Unternehmen zu prüfen, deren Umsatz bestimmte Schwellenwerte überschreitet (Art. 1 FK-VO), und Zusammenschlüsse zu verhindern, die den wirksamen Wettbewerb im EWR oder in einem wesentlichen Teil davon erheblich behindern würden.

Die Fusionskontrolle spielt daher für Interoperabilitätsfragen zunächst eine vorgelagerte Rolle: Der Zusammenschluss oder Aufkauf von Unternehmen kann dazu führen (und führt vor allem in der Internetökonomie regelmäßig dazu), dass vormals unabhängige oder sogar konkurrierende Dienste in bestehende Multi-Konzernstrukturen ein- und an bestehende Dienste in irgendeiner Form angegliedert werden. Folgen sind häufig der Ausbau von Marktmacht und Datenvorteilen sowie damit verbunden Lock-in-Effekte und Selbstpräferenzierungen, was wiederum auch in Verbindung mit fehlender Schnittstellenoffenheit für dritte Dienste stehen kann. Das Fusionskontrollrecht ist zudem auch nachgelagert für Interoperabilitätsfragen relevant, da bei Bedenken gegen eine Fusion aufgrund der genannten Auswirkungen Verpflichtungszusagen der Unternehmen in Betracht kommen, die über eine ansonsten negative Bescheidung hinweghelfen. Die Kommission nimmt in ihren Fusionskontrollentscheidungen eine Gesamtbetrachtung der Auswirkungen von Zusammenschlüssen vor, die auch im

325 *Eilmansberger/Kruis*, in: Streinz (Hrsg.), Art. 102 Rn. 131 f.; *Jung*, in: Grabitz/Hilf/Nettesheim/Jung (Hrsg.), Art. 102 AEUV Rn. 361 ff.

326 Verordnung (EG) Nr. 139/2004 des Rates vom 20. Januar 2004 über die Kontrolle von Unternehmenszusammenschlüssen („EG-Fusionskontrollverordnung"), EU ABl. L 24 v. 29.1.2004, S. 1–22.

vorliegenden Zusammenhang relevante Aspekte aufgreift. Das soll an nachfolgenden Beispielfällen veranschaulicht werden.

(1) Microsoft/Skype

In der bereits erwähnten Fusionskontrollentscheidung Microsoft/Skype befasste sich die Kommission ebenfalls mit Netzwerkeffekten und der Frage nach verbleibenden Möglichkeiten des Multi-Homings. Am 7. Oktober 2011 erklärte sie die Übernahme von Skype durch Microsoft für mit dem Binnenmarkt und dem Abkommen über den Europäischen Wirtschaftsraum (EWR) vereinbar.[327] Im Zentrum stand der Markt für Kommunikationsdienste für Verbraucher. Trotz eines prognostizierten Marktanteils von 80 bis 90 % nach der Fusion (konkurrierend war zum damaligen Zeitpunkt lediglich Facebook mit einem Marktanteil von 5 bis 10 % sowie wenige „kleinere" Anbieter wie Yahoo, ooVoo, Google und AOL)[328] und trotz der Tatsache, dass mögliche Netzwerkeffekte im Raum standen (je mehr Nutzer ein Kommunikationsdienst hat, desto eher könne er auch seine Nutzerbasis weiter ausbauen),[329] wurde in der Fusion keine Gefährdung des Binnenmarkts gesehen. Grund hierfür waren laut Kommission verbleibende Möglichkeiten des Multi-Homings für Nutzer sowie der rapide und innovativ wachsende Markt für Kommunikationsdienste.[330] Netzwerkeffekte würden durch die Tatsache abgeschwächt, dass die meisten Nutzer von Kommunikationsdiensten den Großteil ihrer Sprach- und Videoanrufe mit einer kleinen Anzahl von Familienmitgliedern und Freunden führten, die ihren sog. „inneren Kreis" bildeten. Eine regelmäßige, wechselseitige Interaktion erfolge also nur mit vier bis sechs Personen, weshalb es für diese Gruppen nicht schwierig sei, zwischen Kommunikationsdiensten zu wechseln.

Unter Berufung auf von den Verfahrensbeteiligten vorgelegte Studien stellte die Kommission außerdem fest, dass die Verbraucher auch tatsächlich bis zu einem gewissen Grad zwischen verschiedenen Anbietern von Verbraucherkommunikationsdiensten wechselten. Schließlich seien Verbraucherkommunikationsdienste ein im Entstehen begriffener und rasch

327 COMP/M.6281 (Fn. 281).
328 COMP/M.6281 (Fn. 281).Rn. 109.
329 COMP/M.6281 (Fn. 281), Rn. 91.
330 COMP/M.6281 (Fn. 281), Rn. 92 ff.

wachsender Sektor, was den Eintritt in diese Märkte und deren Expansion erleichtern dürfte, wie auch von erfolgreichen Neueinsteigern – zum damaligen Zeitpunkt Facebook, Viber, Fring und Tango – dokumentiert werde. Die Entscheidung wurde in der Folge auch vom EuG bestätigt – geklagt hatten konkurrierende Anbieter von Internetkommunikationsdiensten und Internetkommunikationssoftware –, das hervorhob, die Kommission habe die fehlende Behinderung des Marktes durch das Vorhandensein von Multi-Homing ausreichend begründet.[331]

(2) Facebook/WhatsApp

Eine weitere relevante Entscheidung betraf den 2014 notifizierten Zusammenschluss von Facebook (heute Meta) und WhatsApp. In ihrer Entscheidung prüfte die Kommission die Auswirkungen der beabsichtigten Fusion auf drei Märkte: Verbraucherkommunikationsdienste, soziale Netzwerke und Online-Werbedienste.[332] Im Hinblick auf den ersten Markt war auch hier der Faktor (mit-)entscheidend, dass ein „signifikanter Grad an Multi-Homing" stattfand, Nutzer also verschiedene Kommunikations-Apps auf ihren Endgeräten simultan nutzten.[333] Der Facebook Messenger und WhatsApp wurden wegen ihrer unterschiedlichen Funktionen, die bei WhatsApp eher mit anderen unmittelbaren nummern- oder mailbasierten Kommunikationsdiensten wie Viber, beim Messenger dagegen hinsichtlich der Anbindung an ein soziales Netzwerk mit Google Hangouts und Twitter vergleichbar seien, auch nicht als „nahe" Wettbewerber eingeordnet.

Ein weiterer Faktor war hier zudem die Tatsache, dass weder der Facebook Messenger noch WhatsApp regelmäßig auf Endgeräten oder Betriebssystemen vorinstalliert waren, Facebook auch keine Kontrolle über ein Betriebssystem hatte. Dies wäre aber ein wichtiger Aspekt gewesen, denn eine solche Vorinstallation kann nach Ansicht der Kommission in wettbewerbsrechtlicher Hinsicht relevant sein, weil dadurch der Wechsel zwischen

331 EuG, Rs. T-79/12 – *Cisco Systems und Messagenet / Kommission*, ECLI:EU:T:2013:635, Rn. 81.

332 Entscheidung der Kommission vom 03/10/2014 zur Vereinbarkeit eines Zusammenschlusses mit dem Gemeinsamen Markt (Fall COMP/M.7217 – *Facebook / WhatsApp*) gemäß der Verordnung (EG) Nr. 139/2004 des Rates, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32014M7217.

333 COMP/M.7217 (Fn. 332) Rn. 105, 110.

Diensten erschwert werde und zu einem „status quo bias" führen könne.[334] Netzwerkeffekte sah die Kommission dagegen deutlich kritischer: Zwar begründeten diese „nicht a priori ein Wettbewerbsproblem", sie würden das aber zumindest dann tun, wenn sie Wettbewerber daran hinderten, ihre Kundenbasis zu erweitern.[335]

In der erforderlichen Einzelfallprüfung kam die Kommission jedoch zu dem Ergebnis, dass andere Faktoren die vorhandenen Netzwerkeffekte – ähnlich wie im Fall *Microsoft/Skype* – abschwächten: (1.) ein sich rasch entwickelnder und offener Sektor, (2.) Multi-Homing, das regelmäßig kostenfrei ist, und (3.) die fehlende gleichzeitige Kontrolle über ein Netzwerk- oder mobiles Betriebssystem, was Lock-in-Effekte vermeide.[336] Der Vollständigkeit halber hat die Kommission allerdings ebenfalls geprüft, ob das Vorhaben voraussichtlich zu einer fusionsspezifischen erheblichen Verstärkung der Netzwerkeffekte führen würde. Netzwerkeffekte könnten verstärkt werden, wenn die Transaktion die getrennten Nutzernetzwerke von WhatsApp und Facebook zu einem wesentlich größeren Netzwerk zusammenführte. Eine solche Kombination erforderte zwangsläufig eine gewisse Integration zwischen den Diensten der Parteien. Eine Integration, die etwa eine Kommunikation zwischen den beiden Messenger-Anwendungen ermöglichen würde, wurde aber im Ergebnis als unwahrscheinlich bewertet wegen technischer (die Nutzer-IDs müssten interoperabel gestaltet werden) und wirtschaftlicher (Facebook rechnete für ein solches Vorhaben mit Gegenwehr der Nutzer) Hürden.

Während auf dem Markt für soziale Netzwerke wegen der nur untergeordnet relevanten sozialen Netzwerkfunktionen von WhatsApp keine wettbewerbsrechtlichen Bedenken gesehen wurden, ist für den Online-Werbemarkt interessant, dass die Kommission auch mögliche Datenvorteile durch den Zusammenschluss in die Betrachtung einbezog. Während sie es für unwahrscheinlich hielt, dass WhatsApp in Zukunft selbst werbebasiert werden könnte, weil dies der Geschäftsstrategie entgegenlaufe, befasste sie sich eingehender damit, ob WhatsApp Facebook weitere Daten zuliefern könnte, die dann bei Facebook zur Verbesserung der Werbedienstleistungen genutzt werden könnten. Sowohl Facebook CEO Mark Zuckerberg[337] als auch

334 COMP/M.7217 (Fn. 332) Rn. 111.
335 COMP/M.7217 (Fn. 332) Rn. 130.
336 COMP/M.7217 (Fn. 332) Rn. 132–134.
337 Vgl. die Aussage von Mark Zuckerberg am Mobile World Congress 2014, zitiert bei *Gibbs*, in: The Guardian v. 24.2.2014.

WhatsApp CEO Jan Koum[338] hatten damals verkündet, dass WhatsApp auch nach dem Zusammenschluss unabhängig bleiben und insbesondere keine Zusammenführung von Daten erfolgen solle. Dieses Versprechen war spätestens mit der Ankündigung der Änderung von Nutzungsbedingungen im Jahr 2019 hinfällig,[339] hätte aber die Entscheidung der Kommission (aus damaliger Sicht) wohl auch nicht geändert. Diese vertrat nämlich die Auffassung, dass selbst bei einer Zusammenführung der Marktanteil von Facebook (damals) in der Werbeindustrie vergleichsweise gering sei (Google bei 33 %, Facebook bei 6,4 %, Adobe bei 1,3 %, Yahoo! bei 0,6 %, Microsoft bei 0,02 % und alle anderen zusammengefasst bei 58,7 %) und selbst bei einem Anstieg weiterhin gering bleiben würde. Wie im wirtschaftlichen Teil des Gutachtens noch auszuführen sein wird, stimmt diese Prognose rückblickend nicht mehr.

(3) Google/Fitbit

Im Fusionskontrollverfahren Google/Fitbit ging es konkret (auch) um Fragen der Interoperabilität vor einem wettbewerbsrechtlichen Hintergrund. 2020 notifizierte Google bei der Kommission seine Absicht, das amerikanische Unternehmen Fitbit zu übernehmen, das in der Entwicklung, Herstellung und im Vertrieb von tragbaren Geräten (sowohl Smartwatches als auch Fitness-Trackern) und vernetzten Waagen im Gesundheits- und Wellnessbereich sowie von zugehöriger Software tätig war.

Ein Aspekt der Untersuchung, die in einer sehr umfangreichen Entscheidung Ende 2020 mündete,[340] waren die Bedenken der Kommission, dass Google – als Betreiber des Betriebssystems Android – nach der Übernahme konkurrierende Anbieter von Smartwatches benachteiligen könnte, indem es deren Interoperabilität mit Android einschränke. Eine solche Einschränkung wäre für konkurrierende Anbieter eine extreme Marktzutrittsschranke, da sich Verbraucher beim Kauf einer Smartwatch an deren Kompatibilität mit ihrem Mobilgerät orientierten (und regelmäßig nicht

338 Jan Koum, Missverständnisse aus dem Weg räumen, WhatsApp Blog vom 17. März 2014, https://blog.whatsapp.com/setting-the-record-straight.

339 Dazu *Etteldorf*, in: NJW, 74, H21, 2021, NJW-aktuell, S. 19; näher dazu bereits oben C.I.2.c.

340 Entscheidung der Kommission vom 17. Dezember 2020 zur Feststellung der Vereinbarkeit eines Zusammenschlusses mit dem Binnenmarkt und dem EWR-Abkommen (COMP/M.9660 – *Google/Fitbit*), https://ec.europa.eu/competition/mergers/cases1/202120/m9660_3314_3.pdf.

umgekehrt). Zudem wurde befürchtet, dass die bislang weitgehend offene Web-API von Fitbit, auf die eine Reihe von Akteuren, insbesondere Start-ups, im Gesundheitssektor zugegriffen hatten, von Google beschränkt werden könnte. Schließlich sah die Kommission es auch als bedenklich an, dass Google durch die Übernahme mit dem Zugriff auf die umfassende Fitness-Datenbank seine Datenvorteile weiter ausbauen und ggf. sogar ähnliche Datenbanken entwickeln könnte. Durch die Vergrößerung der ohnehin schon riesigen Datenmenge, die Google für die Personalisierung von Anzeigen nutzen könnte, wäre es für Konkurrenten schwieriger, mit den Diensten von Google auf den Märkten für Online-Suchwerbung und Online-Display-Werbung und im gesamten „Ad-Tech"-Ökosystem mithalten zu können.

Die Fusion wurde letztlich von der Kommission freigegeben, allerdings auf der Grundlage einer Reihe verbindlicher Zusagen von Google. Im Hinblick auf die befürchteten wettbewerbsschädigenden Datenvorteile musste Google zusichern, Fitbit-Daten nicht für Werbung zu nutzen, die Daten von Fitbit und anderen Google-Diensten strikt in unterschiedlichen Datensilos zu halten und den Nutzern eine Auswahlmöglichkeit zu lassen, ihre Fitbit-Daten mit anderen Google-Diensten zusammenzuführen oder nicht. Auch der Web-API-Zugriff muss nach der Fusion aufrechterhalten werden. Einschneidender sind die Bedingungen zur Interoperabilität: Google muss Android-Originalgeräteherstellern weiterhin kostenlos die öffentlichen APIs lizenzieren, die alle aktuellen Kernfunktionen von Smartwatches zur Kompatibilität abdecken, und darf diese Auflage auch nicht umgehen, indem es die zentralen Interoperabilitäts-APIs außerhalb des Android Open Source Project dupliziert. Google muss außerdem sicherstellen, dass Android-Originalgerätehersteller Zugriff auf alle Android-APIs haben, die es Entwicklern von Android-Smartphone-Apps zur Verfügung stellt, einschließlich der APIs, die Teil von Google Mobile Services sind, und es darf diese Auflage auch nicht umgehen, indem es die Benutzererfahrung beim Tragen von Drittanbieter-Smartwatches dadurch verringert, dass etwa Warnmeldungen, Fehlermeldungen oder Erlaubnisanfragen in diskriminierender Weise angezeigt werden. Die Laufzeit der Zusagen beträgt zehn Jahre.

c. Digital Markets Act

(1) Überblick: Anwendungsbereich und Ziele

Mit dem Ende 2022 in Kraft getretenen Digital Markets Act (DMA)[341] wurden im Verordnungswege auf EU-Ebene bereits einige Fallgestaltungen aufgegriffen, die zuvor Gegenstand wettbewerbsrechtlicher Entscheidungen waren. Einige Aspekte aus den bereits dargestellten Fällen sind nunmehr unmittelbar im DMA adressiert,[342] insbesondere Regeln zur Interoperabilität und Selbstpräferenzierung. Anders als Art. 102 AEUV, der (lediglich) eine auf den konkreten Einzelfall bezogene Ex-post-Entscheidung der Kommission ermöglicht, ist der DMA aber ein Ex-ante-Regulierungsinstrument, legt also im Voraus Regeln zu teilweise sehr spezifischen Sachverhalten fest, an die sich die vom DMA adressierten Unternehmen halten müssen. Obwohl der DMA auf die Rechtsgrundlage der Binnenmarktklausel des Art. 114 AEUV und nicht auf wettbewerbsrechtliche Kompetenzen gestützt ist, ändert dies nichts an seiner Verwandtschaft und Ähnlichkeit mit dem Wettbewerbsrecht.[343] Das lässt sich bereits am Zweck der Verordnung erkennen, der darin liegt, zum reibungslosen Funktionieren des Binnenmarkts beizutragen, indem harmonisierte Vorschriften festgelegt werden, die in der gesamten Union zum Vorteil von gewerblichen Nutzern und Endnutzern für alle Unternehmen „bestreitbare und faire Märkte" im digitalen Sektor gewährleisten (Art. 1 Abs. 1 DMA). Wie das Wettbewerbsrecht adressiert auch der DMA nur bestimmte Akteure, die sich durch eine gewisse Dominanz auszeichnen, nämlich in der Verordnung sog. Torwächter (oder Gatekeeper), die bestimmte zentrale Plattformdienste betreiben.

An dieser Stelle zeigt sich der Unterschied zum Wettbewerbsrecht nach Art. 101, 102 AEUV, und auch die Begründung wird ersichtlich, warum auf EU-Ebene ein solches Ex-ante-Regulierungsinstrument als notwendig erachtet wurde: Die allgemeinen Regeln des Wettbewerbsrecht sind zwar

341 Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte) EU ABl. L 265 vom 12.10.2022, S. 1–66.

342 Für eine Gegenüberstellung bzw. Rückführung der Pflichtenkataloge des DMA auf die wettbewerbsrechtliche Fallpraxis der Kommission vgl. eingehend *Morton/Caffara*, The European Commission Digital Markets Act: A translation.

343 Dazu *Cole*, in: Cappello (Hrsg.), Unravelling the Digital Services Act package, S. 81 ff.

auf das Verhalten von Torwächtern anwendbar, jedoch nur auf bestimmte Arten von Marktmacht, z. B. auf spezifischen Märkten, und werden erst im Nachhinein nach einer umfassenden Untersuchung oft sehr komplexer Fakten in konkreten Fällen durchgesetzt, wenn die negative Marktsituation schon eingetreten ist.[344] Sowohl die spezifischeren Pflichten des DMA als auch das damit eingeführte Überwachungs- und Rechtsdurchsetzungssystem sind deshalb deutlich zeitsensibler als die starreren Strukturen des Wettbewerbsrechts.[345] Zudem begegnet der DMA auch Informationsasymmetrien, die die Europäische Kommission im Wettbewerbsrecht vor Herausforderungen gestellt haben, weil dort erst im Rahmen von bereits eingeleiteten förmlichen Untersuchungen eine geeignete Informationsbasis geschaffen werden konnte.[346]

Es bedurfte einer Festlegung von Vorabpflichten für Gatekeeper, die der DMA nun allgemeiner als solche Unternehmen definiert, die erheblichen Einfluss auf den Binnenmarkt haben, einen zentralen Plattformdienst bereitstellen, der gewerblichen Nutzern als wichtiges Zugangstor zu Endnutzern dient, und hinsichtlich ihrer Tätigkeiten eine gefestigte und dauerhafte Position innehaben oder absehbar in naher Zukunft innehaben werden. Zur Bestimmung dieser Begriffe werden zunächst bestimmte Schwellenwerte festgelegt, bei deren Erreichen eine Vermutung für die Eigenschaft als Gatekeeper besteht.[347] Gatekeeper werden in einem förmlichen Verfahren von der Kommission als solche benannt und sind erst dann – nach einer Übergangsfrist von sechs Monaten – zur Einhaltung der Regeln des DMA verpflichtet. Auch bei Nichterreichen der Schwellenwerte kann die Kom-

344 Erwgr. 5 DMA.

345 Dazu auch *Podszun/Bongartz/Langenstein*, in: EuCML, 2021, S. 60, 61.

346 *Podszun/Bongartz/Langenstein*, in: EuCML, 2021, S. 60, 61.

347 Ein erheblicher Einfluss auf den Binnenmarkt wird vermutet, wenn das Unternehmen in jedem der vergangenen drei Geschäftsjahre in der Union einen Jahresumsatz von mindestens 7,5 Mrd. EUR erzielt hat oder wenn seine durchschnittliche Marktkapitalisierung oder sein entsprechender Marktwert im vergangenen Geschäftsjahr mindestens 75 Mrd. EUR betrugen und es in mindestens drei Mitgliedstaaten denselben zentralen Plattformdienst bereitstellt; die Eigenschaft als zentrales Zugangstor wird vermutet, wenn das Unternehmen im vergangenen Geschäftsjahr mindestens 45 Millionen in der Union niedergelassene oder aufhältige monatlich aktive Endnutzer und mindestens 10.000 in der Union niedergelassene jährlich aktive gewerbliche Nutzer hatte, wobei die Ermittlung und Berechnung gemäß der Methode und den Indikatoren im Anhang erfolgt; die gefestigte Position wird vermutet, wenn die genannten Schwellenwerte in jedem der vergangenen drei Geschäftsjahre erreicht wurden.

mission Anbieter als Gatekeeper benennen, wenn diese nach ihrer Auffassung die Kriterien der Definition erfüllen. Die hierbei von der Kommission zu berücksichtigenden Kriterien spiegeln teilweise Gefahren wider, die bereits oben entlang der Gefahren beim Fehlen von Interoperabilität erwähnt wurden: Netzwerkeffekte und Datenvorteile, Skalen- und Verbundeffekte, Lock-in-Effekte und konglomeratsartige Unternehmensstruktur oder vertikale Integration. Solche Gefahren bzw. Merkmale von Gatekeepern bzw. zentralen Plattformdiensten waren die Hauptbeweggründe für die Verabschiedung des DMA.[348] Erwägungsgrund 2 nennt sehr starke Netzwerkeffekte, die durch die Mehrseitigkeit dieser Dienste bedingte Fähigkeit, viele gewerbliche Nutzer mit vielen Endnutzern in Verbindung zu bringen, die beträchtliche Abhängigkeit sowohl der gewerblichen Nutzer als auch der Endnutzer, Bindungseffekte (Lock-in-Effekte), fehlende Parallelverwendung mehrerer Dienste (Multi-Homing) der Endnutzer für denselben Zweck, vertikale Integration sowie Datenvorteile als Begründung für die Notwendigkeit der Verordnung.

Eine weitere Begrenzung neben dem eingeschränkten Adressatenkreis erfahren die Regeln des DMA dadurch, dass sie nur für sog. zentrale Plattformdienste gelten. Diese sind zunächst[349] abschließend im DMA aufgelistet und erfassen folgende Dienste:

- Online-Vermittlungsdienste
- Online-Suchmaschinen
- Online-Dienste sozialer Netzwerke
- Video-Sharing-Plattform-Dienste
- nummernunabhängige interpersonelle Kommunikationsdienste
- Betriebssysteme
- Webbrowser
- virtuelle Assistenten

348 Vgl. hierzu auch die Folgenabschätzung begleitend zum Vorschlag für einen DMA: Commission staff working document, impact assessment report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), SWD(2020) 363 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020SC0363, insb. Rn. 256.

349 Art. 19 DMA enthält Regeln über die Marktuntersuchung in Bezug auf neue Dienste und neue Praktiken, die die Kommission durchzuführen hat und die Aufschluss über Akteure und Praktiken geben soll, denen mit dem DMA (noch) nicht wirksam begegnet wird.

- Cloud-Computing-Dienste
- Online-Werbedienste

An dieser Auflistung zeigt sich die Relevanz des DMA für den Mediensektor.[350] Online-Vermittlungsdienste und Online-Suchmaschinen sind häufig Zugangstor und Vermittler für mediale Inhalte Dritter, entscheiden mithin über deren Zugänglichkeit, Auffindbarkeit und Sichtbarkeit. Zu den Vermittlungsdiensten gehören dabei insbesondere App-Stores, über die auch Anwendungen von Medienanbietern vertrieben werden. Diese Relevanz gilt auch für soziale Netzwerke sowie Video-Sharing-Plattformen, auf denen (auch) Medieninhalte stattfinden, die aber gleichzeitig unmittelbar in Konkurrenz mit Medienunternehmen um Aufmerksamkeit von Rezipienten und Werbekunden stehen. Eher „technische" Dienste wie Betriebssysteme, Webbrowser und virtuelle Assistenten sind nicht minder relevante Zugangstore für Medien und meinungsbildungsrelevante Inhalte insgesamt, weil sie die Basis für jedwede Online-Interaktion von Rezipienten sind. So können die in einem Betriebssystem vorinstallierten Anwendungen darüber entscheiden, ob es Schnittstellen oder eine Kompatibilität mit dem Angebot eines Mediendiensteanbieters gibt, oder die Voreinstellungen eines Webbrowsers darüber bestimmen, wie die Interaktion mit einer Mediathek stattfindet.

Zu den virtuellen Assistenten gehören Sprachassistenten, die vor allem für Radioanbieter als Schnittstelle von enormer Bedeutung sind. Schließlich sind Online-Werbedienste regelmäßig zentraler Bestandteil von Finanzierungsmodellen von Online-Medienangeboten.

Diesen zentralen Plattformdiensten (oder nur bestimmten von ihnen) erlegt der DMA eine Reihe von Pflichten auf bzw. der DMA listet, wie die Kommission es beschreibt, für diese Unternehmen „Do's" und „Don'ts".[351] Diese lassen sich überblickhaft zusammenfassen in Vorschriften über die (Grenzen der) Datennutzung und über Datenportabilität, Werbetransparenz, die Verbesserung von Interaktionsmöglichkeiten zwischen Endnutzern und Geschäftsnutzern, über Schnittstellenoffenheit, Interoperabilität, Multi-Homing sowie Fairness und Transparenz. Dabei ist an dieser Stelle

350 Dazu auch eingehend *Cole*, Overview of the impact of the proposed EU Digital Services Act Package on broadcasting in Europe.

351 Vgl. das Factsheet der Europäischen Kommission, The Digital Markets Act: ensuring fair and open digital markets, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

darauf hinzuweisen, dass nach Sinn und Zweck des DMA der Begriff des zentralen Plattformdienstes weit ausgelegt werden sollte und technologieneutral ist. Wie Erwägungsgrund 14 daher zutreffend bestimmt, können auch Dienste erfasst sein, die auf verschiedenen Medien oder Geräten oder über solche Medien und Geräte bereitgestellt werden, z. B. verbundene Fernsehgeräte oder eingebettete digitale Dienste in Fahrzeugen.

(2) Das System der Interoperabilität im DMA

Interoperabilität spielte bei der Schaffung des DMA insbesondere aus zwei Gesichtspunkten eine Rolle: zum einen vor dem Hintergrund, dass geschäftliche Nutzer marktstarker Vermittlungsdienste nur begrenzten oder keinen Zugriff auf Daten hätten und keine effektive Interoperabilität gewährleistet werde, um auf solche Daten ggf. zuzugreifen.[352] Zum anderen sollte der DMA wirksam der Tatsache begegnen, dass Torwächter den Zugang zu ihren Diensten oder die Interoperabilität ihrer Dienste oder einzelne Funktionen derselben bewusst für dritte Dienste beschränkten und damit nur ihren eigenen Diensten eine Anbindung ermöglichten.[353]

Beide Aspekte wurden in unterschiedlichen Bestimmungen in der finalen Fassung des DMA aufgegriffen. Dabei sind aber im vorliegenden Zusammenhang nicht nur die Vorschriften relevant, die sich unmittelbar auf Interoperabilität beziehen, sondern auch solche, die mittelbar für die Gewährleistung offener und nutzbarer Schnittstellen bedeutsam sind.

Dabei ist zunächst Art. 2 Nr. 29 DMA zu beachten, der eine Definition des Begriffs „Interoperabilität" enthält. Diese beschreibt

> *die Fähigkeit, Informationen auszutauschen und die über Schnittstellen oder andere Lösungen ausgetauschten Informationen beiderseitig zu nutzen, sodass alle Hardware- oder Softwarekomponenten mit anderer Hardware und Software auf die vorgesehene Weise zusammenwirken und bei Nutzern auf die vorgesehene Weise funktionieren.*

Damit wird dem DMA ein Verständnis von Interoperabilität zugrunde gelegt, das mehr an Zielvorstellungen und weniger an den konkreten technischen Bedingungen von Interoperabilität orientiert ist. Dies ist systematisch

352 SWD(2020) 363 final (Fn. 348), Rn. 44, hier bezugnehmend auf ein Beispiel des Verhältnisses zwischen App-Stores und App-Entwicklern.

353 SWD(2020) 363 final (Fn. 348), Rn. 49, hier bezugnehmend auf das Beispiel der (Nicht-)Einbindung externer Zahlungsdienste.

für den DMA folgerichtig, weil er sich auf sehr unterschiedliche (zentrale) Plattformdienste erstreckt und Interoperabilität auch an verschiedenen Stellen in unterschiedlichen Zusammenhängen aufgreift. Art. 2 Nr. 29 DMA beschreibt den gewünschten Zustand, dass Endnutzer über einen Dienst nahtlos Informationen austauschen können. Wie und inwieweit das technisch umzusetzen ist, ist entlang der konkreten materiellen Bestimmungen zu beurteilen.

Art. 6 Abs. 7 DMA ist dabei die zentrale Interoperabilitätsbestimmung, die aber ohne weitere Bestimmungen des DMA, wie etwa das Zugangsrecht nach Art. 6 Abs. 4 DMA auf Seiten der gewerblichen Nutzer sowie die Bestimmung des Art. 6 Abs. 12 DMA, wonach dieser Zugang fair und diskriminierungsfrei sein muss, nur begrenzt die Ziele des DMA für eine wirksame Interoperabilität erreichen könnte. Die Interoperabilität wäre zudem für gewerbliche Nutzer wertlos, wenn die Endnutzer sie nicht in Anspruch nehmen, weil sie es technisch nicht können oder keine Kenntnis von ihren Möglichkeiten haben. Zur Überwindung dieser Problematik dienen etwa die „Kontaktrechte" mit Endnutzern nach Art. 5 Abs. 4 und 5 DMA, die Pflichten zur Ermöglichung von Software-Wechseln bzw. -Abonnements (Art. 6 Abs. 6 DMA) sowie zur Anpassung von Standardeinstellungen (Art. 6 Abs. 3 UAbs. 2 S. 1 DMA) und das Recht auf Datenportabilität nach Art. 6 Abs. 9 DMA. Selbstbegünstigungs- und Diskriminierungsverbote nach Art. 6 Abs. 5 DMA, Kopplungsverbote nach Art. 5 Abs. 7 DMA sowie Datenzugangsrechte nach Art. 6 Abs. 10 DMA sind wiederum von Bedeutung für faire Bedingungen innerhalb interoperabler Systeme (das „Wie" der Interoperabilität). Diese Bestimmungen sollen daher nachfolgend eingehender und im systematischen Zusammenhang betrachtet werden.

(3) Vertikale Interoperabilität von Betriebssystemen, virtuellen Assistenten und Nebendiensten (Art. 6 Abs. 4 und 7 DMA)

Nach Art. 6 Abs. 4 DMA muss es der Torwächter gestatten (passiv) und technisch ermöglichen (aktiv), Software-Anwendungen Dritter (maßgeblich: Apps) und von Dritten betriebene Geschäfte für Software-Anwendungen (maßgeblich: App-Stores), die sein Betriebssystem nutzen oder mit diesem interoperieren,[354] zu installieren und effektiv zu nutzen (sog.

354 Die Bestimmung beschränkt sich also auf solche Anwendungen, die überhaupt für das jeweilige Betriebssystem programmiert sind. So wird etwa Apple dadurch nicht

„Side-Loading“[355]). Auch muss der Torwächter in gleicher Weise dafür sorgen, dass auf diese Apps und App-Stores auf anderem Wege als über die betreffenden zentralen Plattformdienste des Torwächters zugegriffen werden kann. Letzteres betrifft nicht nur die Bezugsquellen der App-Stores „kleinerer“ Anbieter wie Huawei App Market oder F-Droid sowie freie quelloffene Datenbanken wie GitHub, sondern kann sich auch auf das unmittelbare Anbieten von Apps zum Download durch Diensteanbieter erstrecken (bspw. der Webplayer eines Radiounternehmens, die Mediathek eines Fernsehsenders etc.).

Die Regelung verpflichtet aber nur Anbieter von Betriebssystemen[356], wird sich also voraussichtlich in Zukunft in der Implementierungs- und Durchsetzungspraxis (dazu unten C.II.2.c(11)) auf Apples iOS und Googles Android beschränken, die jedoch gemeinsam 99 % des Marktes für mobile Betriebssysteme ausmachen. Die Vorschrift greift damit vor allem Bedenken auf, die sich auch im oben (C.II.2.a(2)(f)) dargestellten Verfahren in Sachen App Store gezeigt haben. Ohne Bedeutung ist dabei aber die Hardware bzw. das Endgerät, auf dem das Betriebssystem läuft. Dabei ist auch an Smart-TV-Geräte und Entertainmentsysteme in Fahrzeugen[357] zu denken, wobei die installierten Systeme hier (noch) diverser sind als im Smartphone- oder PC-Bereich.[358] An dieser Stelle sei an Erwägungsgrund 14 erinnert, der eine weite Auslegung des Begriffs der zentralen Plattformdienste fordert und insbesondere auf verbundene Fernsehgeräte oder eingebettete digitale Dienste in Fahrzeugen hinweist.

Die Regelung fordert nicht nur ein Unterlassen von missbräuchlichem Verhalten, sondern einen aktiven Abbau von Interoperabilitätshindernissen und sogar den Aufbau von besseren technischen Voraussetzungen für ein Mindestmaß an Interoperabilität.[359] Dies ist sehr weitreichend gemeint, wie sich aus dem in Art. 6 Abs. 4 DMA aufgeführten Beispielfall einer

---

etwa verpflichtet, Android-Software interoperabel zu machen. Die Pflicht zur Herstellung technischer Kompatibilität bleibt also auf Seiten der App-Anbieter, nicht der Gatekeeper.

355 Zum Begriff *Podszun/Bongartz/Langenstein*, in: EuCML, 2021, S. 60, 64; *Herbers,* in: Podszun, Art. 6 Rn. 53.

356 Eine Systemsoftware, die die Grundfunktionen der Hardware oder Software steuert und die Ausführung von Software-Anwendungen ermöglicht, Art. 2 Nr. 10 DMA.

357 *Herbers,* in: Podszun, Art. 6 Rn. 60.

358 Neben Android TV und Google TV etwa Amazons Fire OS sowie herstellereigene Betriebssysteme wie Tizen (Samsung) und webOS von LG.

359 *Wielsch*, in: MKDS, Art. 6 DMA, Rn. 47.

solchen Verhinderungstaktik ablesen lässt: Der Torwächter darf nicht nur nicht verhindern, dass eine Drittanbieter-App danach fragt, ob der Nutzer diese App als Standard einrichten möchte (anstelle einer vergleichbaren App des Torwächters), vielmehr muss er sogar technisch ermöglichen, dass diese Einstellung dann auch wirksam umgesetzt wird und für den Endnutzer einfach vorzunehmen ist. Fraglich dürfte die Anwendbarkeit des Kriteriums bei Nudging-Techniken wie z. B. dem Verstecken solcher Einstellungsoptionen in komplizierten Einstellungspfaden, dem Anzeigen von Warnhinweisen bei der Installation einer Fremdanbieter-App oder der aufdringlichen Hervorhebung des eigenen vergleichbaren Dienstes sein, die in der Nutzung von Betriebssystemen verbreitete Praxis sind. Solche Techniken verhindern die Einstellung durch den Nutzer nicht „technisch", wie von Art.6 Abs. 4 UAbs. 1 DMA vorausgesetzt.[360] Jedoch wären dann zumindest solche Praktiken als unter das Umgehungsverbot fallend und daher als vom DMA untersagt anzusehen (dazu unten C.II.2.c(10)).

Grenze dieser umfassenden Interoperabilität sind der Integritätsvorbehalt in UAbs. 2 und der Sicherheitsvorbehalt in UAbs. 3.[361] Gatekeeper müssen dann keine Interoperabilität für Apps und App-Stores sicherstellen, wenn deren Integration die Integrität des eigenen Betriebssystems bzw. der Hardware gefährden würde. Sie dürfen auch Einstellungen (nicht aber: Standardeinstellungen) vornehmen, um die Sicherheit zu gewährleisten. Diese Einschränkung soll der Kritik begegnen, dass offene Systeme zu großen Risiken durch Schadsoftwareattacken führen könnten.[362] Solche Maßnahmen müssen nach der Vorgabe des DMA aber unbedingt erforderlich und angemessen sein, wobei den Gatekeeper eine Begründungspflicht trifft. Der Ausschluss bestimmter Anwendungen aufgrund rechtlicher Bedenken (illegale Apps bzw. Apps mit illegalen Inhalten) bleibt damit weiter möglich, der Torwächter muss ihn aber rechtfertigen. Nicht mehr möglich ist allerdings der Ausschluss aufgrund der Tatsache, dass eine App die Geschäftsinteressen des Torwächters gefährdet, bspw. weil sie seinen eigenen Angeboten ähnlich ist oder zu deren Umgehung führen könnte.

Die Pflicht nach Art. 6 Abs. 4 DMA ist in der Praxis nur dann für gewerbliche Nutzer wertvoll, wenn der Torwächter ihnen nicht den Zugang zu denjenigen seiner Schnittstellen verwehren kann, die sie zur Entwicklung entsprechender Apps benötigen. Dies ist durch Art. 6 Abs. 7 DMA

360 *Herbers*, in: Podszun, Art. 6 Rn. 71.
361 Zu den Begriffen *Wielsch*, in: MKDS, Art. 6 DMA, Rn. 64 f., 66 f.
362 Dazu *Herbers*, in: Podszun, Art. 6 Rn. 55, 72 ff. m. w. N.

vorgesehen, der daher im direkten Zusammenhang mit Abs. 4 gelesen werden muss. Nach Satz 1 ermöglicht der Torwächter Diensteanbietern und Anbietern von Hardware kostenlos eine wirksame Interoperabilität mit – und Zugang für Zwecke der Interoperabilität zu – denselben Hardware- und Software-Funktionen, die dem Torwächter selbst zur Verfügung stehen und auf die über das Betriebssystem oder den virtuellen Assistenten zugegriffen wird bzw. die über dieselben gesteuert werden. Anders als Satz 2 beschränkt sich Satz 1 daher auf die Möglichkeiten und steuerbaren Dienste des Torwächters. So könnte ein gewerblicher Nutzer in Bezug auf einen von ihm angebotenen Dienst (bspw. Spotify) von einem Torwächter (bspw. Apple) dann Zugang zu den Steuerungsfunktionen eines virtuellen Assistenten (bspw. Siri) verlangen, wenn das in Bezug auf einen eigenen Dienst des Torwächters (bspw. Apple Music) möglich ist, nicht aber dann, wenn das nicht der Fall ist.[363]

Satz 2 ist davon nicht abhängig. Danach muss der Torwächter gewerblichen Nutzern und alternativen Anbietern von Diensten, die zusammen mit zentralen Plattformdiensten oder zu deren Unterstützung erbracht werden, grundsätzlich kostenlos wirksame Interoperabilität mit – und Zugang für Zwecke der Interoperabilität zu – denselben Betriebssystem-, Hardware- oder Software-Funktionen ermöglichen, die er zur Verfügung hat oder verwendet. Das gilt unabhängig davon, ob die Funktionen Teil des Betriebssystems sind. Ziel der Verpflichtung ist es, konkurrierenden Dritten eine Interkonnektivität mit den jeweiligen Funktionen durch Schnittstellen oder ähnliche Lösungen zu gestatten, die ebenso wirksam ist wie bei den eigenen Diensten oder der eigenen Hardware des Torwächters.[364] Gewerbliche Nutzer sollen mittels Schnittstellen in die Lage versetzt werden, auf den Endgeräten der Torwächter gleichwertige Leistungen anzubieten. Begegnet wird damit der im digitalen Sektor zu beobachtenden Entwicklung von „walled gardens", in denen Gatekeeper eine Doppelrolle als Vermittler und Wettbewerber einnehmen,[365] indem dagegen eine Öffnung der Dienste und eine Gleichstellung angeordnet wird.[366] Die Vorschrift knüpft damit auch an die bestehende Wettbewerbspraxis bspw. aus dem oben dargestellten Fall zu Microsoft an.

363 Zu dem Beispiel *Wielsch*, in: MKDS, Art. 6 Rn. 102.
364 Erwgr. 57.
365 Dazu bereits oben B.I.1
366 *Herbers*, in: Podszun, Art. 6 Rn. 144 f.

Die Bezugnahme auf Hardware betrifft dabei insbesondere sog. Wearables (bspw. Smartwatches), mit denen sich die Kommission bereits eingehend in einer Sektoruntersuchung[367] befasst und bei deren Interoperabilität sie Mängel festgestellt hatte.[368] Was jedoch Dienste sind, „die zusammen mit zentralen Plattformdiensten oder zu deren Unterstützung erbracht werden", definiert der DMA nicht näher. Beispielhaft nennt Erwägungsgrund 44 etwa die bereits in Art. 5 Abs. 7 DMA unmittelbar adressierten Identifizierungsdienste, Webbrowser-Engines, Zahlungsdienste[369] oder technische Dienste zur Unterstützung der Erbringung von Zahlungsdiensten. Anders als Art. 5 Abs. 7 ist Art. 6 Abs. 7 UAbs. 1 S. 2 DMA jedoch nicht auf diese beschränkt.

Was diese Bestimmungen insgesamt nicht gewährleisten, ist ein vollständiger Zugang zu und eine vollständige Interoperabilität von Nebendienstleistungen („ancillary services") mit den Diensten des Torwächters. Eine solche umfassende Regelung wurde im legislativen Prozess als Option vor dem Vorschlag für den DMA diskutiert, aber letztlich verworfen.[370]

(4) Fairer Zugang zu App-Stores, Online-Suchmaschinen und sozialen Netzwerken (Art. 6 Abs. 12 DMA)

Art. 6 Abs. 12 DMA ergänzt die Abs. 4 und 7 der Vorschrift, obwohl es sich um einen eigenständigen Regelungstatbestand handelt, in gewisser Weise um aus dem Willkürverbot folgende Elemente. Der Torwächter soll für den Zugang gewerblicher Nutzer zu seinen App-Stores, Online-Suchmaschinen und sozialen Netzwerken faire, zumutbare und diskriminierungsfreie allgemeine Bedingungen anwenden, wie sie schon aus den FRAND-Bedingungen im Wettbewerbsrecht bekannt sind. Zu diesem Zweck hat er die Bedingungen, zu denen auch ein alternativer Streitbeilegungsmechanismus für Konfliktfälle gehören muss, zu veröffentlichen. Die Bedingungen unterliegen wiederum der Überprüfung durch die Kommission.

367 Vgl. dazu auch die Ergebnisse der Sektoruntersuchung zum Internet der Dinge der Europäischen Kommission, COM(2022) 19 final, Final report – sector inquiry into consumer Internet of Things.

368 Dazu eingehend *Herbers*, in: Podszun, Art. 6 Rn. 137.

369 Das in der Folgenabschätzung der Kommission formulierte Beispiel war relativ eindeutig auf ApplePay zugeschnitten; SWD(2020) 363 final (Fn. 348), S. 55.

370 SWD(2020) 363 final (Fn. 348), Rn. 156.

Der DMA gibt damit aber nicht selbst bestimmte Standards vor, denen die Bedingungen entsprechen müssen. Vielmehr ist die Bestimmung abstrakt formuliert und bezieht sich auf auslegungsbedürftige Grundsätze. Mit der Implementierung von Streitbeilegungsmechanismen[371] und der Überprüfungsmöglichkeit durch die Kommission wird deutlich, dass die Bestimmung auf die Erarbeitung von Standards in einem Dialog – mehr noch als im Rahmen von Art. 8 und 12 DMA (C.II.2.c(11)) – setzt. Insofern liegt es nahe, sie mit Systemen der regulierten Selbstregulierung zu vergleichen.[372] Erwägungsgrund 62 konkretisiert die Vorgabe nur insoweit, als preisliche oder andere allgemeine Zugangsbedingungen zumindest dann als unfair angesehen werden, wenn sie zu einem Ungleichgewicht zwischen Rechten und Pflichten, die den gewerblichen Nutzern auferlegt werden, führen, dem Torwächter einen unverhältnismäßigen Vorteil verschaffen oder umgekehrt die gewerblichen Nutzer benachteiligen. Als Kriterien hierfür werden etwa die Preise oder Bedingungen genannt, die andere Betreiber von App-Stores erheben. Auch soll es eine Rolle spielen, welche Preise und Bedingungen in Bezug auf Dienstleistungen, Nebendienste und unterschiedliche Regionen gelten und welche der Torwächter für seine eigenen Anwendungen ansetzt.

Wie Erwägungsgrund 62 ausdrücklich unterstreicht, gewährt Art. 6 Abs. 12 DMA jedoch kein Zugangsrecht. Auch wird damit keine Aussage über den Umgang der genannten Plattformdienste mit illegalen Anwendungen oder Inhalten getroffen. Letzteres ist auch nicht Zweck der Regel, die eher den Fall im Blick hat, dass der Torwächter durch die Ungleichbehandlung selbst einen Vorteil erlangt. Was den Begriff des Zugangs anbelangt, sollte er aber im Hinblick auf die Ziele des DMA (das einseitige Diktieren von Bedingungen aufgrund der Marktmacht soll durchbrochen werden) weit ausgelegt werden und insbesondere die Auffindbarkeit dem Fairnessgebot zuordnen.[373]

371 Nach Erwgr. 62 soll dieser leicht zugänglich, unparteiisch, unabhängig und für den gewerblichen Nutzer gebührenfrei sein. Er soll aber nicht der Inanspruchnahme anderer Mechanismen, insbesondere der Beschreitung von nationalen Rechtswegen, entgegenstehen.

372 So *Wielsch*, in: MKDS, Art. 6 Rn. 179.

373 So auch *Wielsch*, in: MKDS, Art. 6 Rn. 187; *Herbers*, in: Podszun, Art. 6 Rn. 298.

(5) Verbot von Selbstpräferenzierung und Gebot der Nicht-Diskriminierung (Art. 6 Abs. 5 DMA)

(a) Allgemeines

Art. 6 Abs. 5 DMA enthält sowohl ein Verbot der Selbstpräferenzierung (Satz 1) als auch ein Gebot der Nichtdiskriminierung (Satz 2) in Bezug auf Rankingsysteme. Bevor zwischen diesen beiden verschiedenen Tatbeständen unterschieden wird, ist erwähnenswert, dass diese Bestimmung in ihrem Anwendungsbereich zunächst nicht auf bestimmte Arten von zentralen Plattformdiensten und auf bestimmte Erscheinungsformen von Rankingsystemen beschränkt ist. Allerdings ist eine solche Beschränkung der zugrunde liegenden Definition des Rankings zu entnehmen. So ist nach Art. 2 Nr. 22 DMA Ranking

> *die relative Hervorhebung von Waren und Dienstleistungen, die über* ***Online-Vermittlungsdienste****,* ***Online-Dienste sozialer Netzwerke****,* ***Video-Sharing-Plattform-Dienste*** *oder* ***virtuelle Assistenten*** *angeboten werden, oder die Relevanz, die den Suchergebnissen von* ***Online-Suchmaschinen*** *mittels entsprechender Darstellung, Organisation oder Kommunikation durch die Unternehmen, die Online-Vermittlungsdienste, Online-Dienste sozialer Netzwerke, Video-Sharing-Plattform-Dienste, virtuelle Assistenten oder Online-Suchmaschinen anbieten, zugemessen wird, unabhängig von den für diese Darstellung, Organisation oder Kommunikation verwendeten technischen Mitteln und unabhängig davon, ob nur ein einziges Ergebnis dargestellt oder kommuniziert wird [Hervorhebung d. Verf.].*

Vereinfacht ausgedrückt bezeichnet der Begriff Listen, die typischerweise als Antwort auf eine Sucheingabe auf diesen Plattformen angezeigt werden. Für den Bereich der genannten Online-Vermittlungsdienste werden Hauptanwendungsfälle in der Regel also App-Stores und Online-Marktplätze sein, auf denen eine solche Auflistung bei Produktsuchen regelmäßig stattfindet. Bei Online-Suchmaschinen, Video-Sharing-Plattformen und virtuellen Assistenten (auch und vor allem: Sprachassistenten) kann es dagegen auch um eine Suche nach Inhalten gehen, da der Begriff der Dienstleistung in diesem Zusammenhang weit zu verstehen ist. Nicht verbunden ist aber vor allem der erste Halbsatz der Definition des Rankings mit einer aktiven Suchanfrage. Fraglich ist daher, ob auch von den Anbietern (ohne Zutun des Nutzers) hervorgehobene Inhalte wie Feeds auf sozialen Netzwerken oder die Startseite mit Empfehlungen auf Video-Sharing-Plattformen hier-

unter fallen. Das Europäische Parlament hatte in seiner Position die – im Kommissionsvorschlag nur auf Suchanfragen beschränkte – Vorschrift weiter fassen und auch „andere Einstellungen" erfassen wollen. Dieser Vorschlag hat sich nicht durchgesetzt und es wurden „nur" das Ranking und Crawling aufgenommen. Eine Gesamtschau der Erwägungsgründe spricht ebenfalls gegen die Annahme eines darüber hinausgehenden Anwendungsbereichs der Vorschrift.

Erwägungsgrund 52 beschreibt das Ranking näher als „relative Hervorhebung" und nennt beispielhaft das Anzeigen, die Beurteilung, das Verlinken oder die Sprachausgabe von Ergebnissen. Dabei macht es keinen Unterschied, ob dem Suchenden auch mehrere Ergebnisse oder tatsächlich nur ein Ergebnis präsentiert werden, solange die Anordnung im Hintergrund stattfindet – ein Beispiel hierfür wären Sprachassistenten, die regelmäßig nur die relevanteste Antwort ausgeben und nicht eine Auswahl. Interessanterweise hebt dieser Erwägungsgrund auch hervor – um sicherzustellen, dass diese Verpflichtung wirksam ist und nicht umgangen werden kann –, dass auch Maßnahmen mit „gleiche[r] Wirkung wie eine Differenzierung oder Vorzugsbehandlung beim Ranking" erfasst sind.

Dem Begriff des Rankings liegt ein technisches Verständnis zugrunde. In der Praxis der Online-Umgebung bestimmen regelmäßig Algorithmen die Listung, die zu einem gewissen Grad (maschinell) lernen oder auf Künstlicher Intelligenz basieren können.[374] Daher ist es sinnvoll, dass die Vorschrift des Art. 6 Abs. 5 DMA nicht nur das entsprechende Auflisten (also das Ergebnis) erfasst, sondern bereits die damit verbundenen und im Vorfeld stattfindenden Aktivitäten des Crawlings (das Suchen und Auffinden von neuen und aktualisierten Inhalten) und der Indexierung (die Speicherung und Ordnung dieser Inhalte).[375]

(b) Verbot der Selbstpräferenzierung (Art. 6 Abs. 5 S. 1 DMA)

Nach Art. 6 Abs. 5 S. 1 DMA darf der Torwächter von ihm selbst angebotene Dienstleistungen und Produkte beim Ranking sowie bei der damit verbundenen Indexierung und dem Auffinden gegenüber ähnlichen Dienstleistungen oder Produkten eines Dritten nicht bevorzugen. Damit werden Verhaltensweisen aufgegriffen, die bereits aus der Fallpraxis des Kartellrechts

374 Dazu eingehend *Hacker*, in: GRUR, 2022, S. 1278, 1281 ff.
375 Erwgr. 52 DMA.

bekannt waren. Allerdings wird die bestehende Praxis durch die explizite Regelung im DMA insoweit verstärkt, als ein Verstoß gegen das Verbot der Selbstpräferenzierung nicht mehr von einer Marktbestimmung und nicht mehr von der Feststellung einer Marktbeherrschung (diese ist durch die Benennung als Gatekeeper ersetzt) abhängt und keine separate Prüfung wettbewerbsschädigender Auswirkungen erfolgen muss. Letzteres bedeutet auch, dass etwaige positive Effekte (bspw. die tatsächlich für Verbraucher relevanteste Auswahl) oder die Marktlage (bspw. das Bestehen von Alternativdiensten) das Verbot nicht verändern.

Zu den eigenen Angeboten des Torwächters zählen auch die Angebote aller verbundenen Unternehmen, auf die er bestimmenden Einfluss ausübt (Art. 2 Nr. 1 i. V. m. Art. 2 Nr. 27, 28 DMA).[376] Das erfasst also nicht nur die unmittelbar eigenen Dienste eines Gatekeepers, sondern auch die Dienste von anderen gewerblichen Nutzern, die der Gatekeeper kontrolliert.[377]

Die Handlung der Präferenzierung ist weit zu verstehen. Ziel ist es, dass die Gatekeeper ihre Algorithmen so programmieren und die Anzeige in den jeweiligen Benutzeroberflächen so gestalten, dass die Unterscheidung in eigene oder fremde Produkte bzw. Dienstleistungen keine Rolle spielt.[378] Das erstreckt sich auf die rechtliche (z. B. Verankerung entsprechender Vorschriften in Allgemeinen Geschäftsbedingungen der zentralen Plattformdienste), kommerzielle (bspw. vertragliche Vereinbarung einer bevorzugten Behandlung gegen Entgelt) und rein technische (bspw. Anlernen von Algorithmen zur bevorzugten Behandlung eigener Dienste) Selbstpräferenzierung.[379] Im Hinblick auf diese Zielsetzung ist davon auszugehen, dass eine (verbotene) Selbstpräferenzierung auch dann vorliegt, wenn sie als solche oder gesondert gekennzeichnet ist, sich also von den übrigen Suchergebnissen optisch unterscheidet (bspw. „gesponserter Inhalt" „von/Verkauf und Versand durch XY"). Denn eine solche rein verbraucherschutzrechtliche Ausrichtung lässt sich Art. 6 Abs. 5 DMA nicht entnehmen, da die Vorschrift auch gewerbliche Nutzer schützt.[380]

Satz 1 beschränkt sich aber auf das Verbot der Präferenzierung eigener Angebote, schließt also zunächst (zu Satz 2 sogleich) „nur" die Zugehörig-

376 *Wielsch*, in: MKDS, Art. 6 DMA Rn. 81.
377 Erwgr. 52 DMA.
378 *Wielsch*, in: MKDS, Art. 6 DMA Rn. 82; dazu auch *Herbers*, in: Podszun, Art. 6 Rn. 97 ff.
379 Erwgr. 52 nennt explizit rechtliche, kommerzielle und technische Mittel.
380 *Wielsch*, in: MKDS, Art. 6 DMA Rn. 83, aber anders in Bezug auf die zulässigen Kriterien nach S. 2; *Herbers*, in: Podszun, Art. 6 Rn. 97.

keit zum Unternehmen als Kriterium für das Ranking aus. Über weitere Kriterien, ob und wie Produkte und Dienstleistungen angeordnet werden, trifft die Vorschrift keine Aussage. Insbesondere ist damit auch keine Bedingung für die Zugangseröffnung verbunden. Daran knüpft allerdings der im folgenden dargestellte Art. 6 Abs. 5 S. 2 DMA an.

(c) Gebot der Nichtdiskriminierung

Nach Art. 6 Abs. 5 S. 2 DMA muss der Torwächter das Ranking anhand transparenter, fairer und diskriminierungsfreier Bedingungen vornehmen.

Das Gebot der Transparenz beim Ranking dürfte sich jedoch für die vom DMA adressierten Dienste bereits aus der Platform-to-Business-(P2B-)Verordnung[381] ergeben. Deren Art. 5 legt bereits seit Juli 2020 verbindlich fest, dass Anbieter von Online-Vermittlungsdiensten und Online-Suchmaschinen die wichtigsten Parameter, die für die Auflistung oder das Ranking der Dienste ausschlaggebend sind, klar und transparent darstellen müssen. Bei Online-Suchmaschinen wird diese Transparenz dadurch konkretisiert, dass die Informationen in einer leicht und öffentlich zugänglichen Beschreibung in einfacher und verständlicher Sprache abgefasst werden müssen. Damit ist in gewisser Weise eine andere Art „Interoperabilität" angesprochen, deren Vorbedingung Transparenz ist: Gewerbliche Nutzer (für Verbraucher gibt es entsprechende Vorschriften in der durch die Mitgliedstaaten umzusetzenden Richtlinie (EU) 2019/2161[382]) sollen in die Lage versetzt werden, die Funktionsweise und Kriterien zu verstehen, die für das Ranking ihrer Angebote maßgeblich sind.[383] Das ist wichtig für ihre Auffindbarkeit und Sichtbarkeit, die durch die Interaktion mit Vermittlern bedingt wird.

Beschränkt ist die Transparenzpflicht aber auf die Offenlegung der „Hauptparameter". Insbesondere soll die Transparenz nicht so weit gehen,

381 Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten, EU ABl. L 186, 11.7.2019, S. 57–79.

382 Richtlinie (EU) 2019/2161 des Europäischen Parlaments und des Rates vom 27. November 2019 zur Änderung der Richtlinie 93/13/EWG des Rates und der Richtlinien 98/6/EG, 2005/29/EG und 2011/83/EU des Europäischen Parlaments und des Rates zur besseren Durchsetzung und Modernisierung der Verbraucherschutzvorschriften der Union, EU ABl. L 328, 18.12.2019, S. 7–28.

383 Hierzu und zum Folgenden auch *Etteldorf*, in: Cappello (Hrsg.), Algorithmische Transparenz und Rechenschaftspflicht bei digitalen Diensten, S. 48 ff.

dass dadurch eine Täuschung oder Schädigung von Verbrauchern durch die Manipulation von Suchergebnissen möglich gemacht wird (Art. 5 Abs. 6 P2B-Verordnung). Letzteres ist auch aus dem Blickwinkel der Meinungs- und Medienvielfaltssicherung wichtig, da es verhindern soll, dass mediale Angebote (nur) zum Zweck der Optimierung an den Algorithmus angepasst werden, statt sich an inhaltlicher Qualität und Relevanz für die Meinungsbildung zu orientieren. Was unter solchen Hauptparametern zu verstehen ist, konkretisiert die Bekanntmachung der Kommission zu den Leitlinien zur Transparenz des Rankings nach der P2B-Verordnung.[384] Danach sollen Anbieter bspw. bei der Bestimmung der transparent zu machenden Hauptparameter berücksichtigen, ob (und inwieweit) ihre Algorithmen auf einer Personalisierung und dem Verbraucherverhalten beruhen, inwieweit sie mit Zusatzdiensten verknüpft sind oder welche Maßnahmen die gerankten Ergebnisse gegen illegale Inhalte ergreifen bzw. nicht ergreifen. Erwägungsgrund 52 des DMA nimmt ausdrücklich Bezug auf diese Leitlinien, sodass sie auch in Zukunft unter Art. 6 Abs. 5 DMA relevant sein werden.

An dieser Stelle ist jedoch kritisch hervorzuheben, dass sich die praktische Wirksamkeit der Transparenzvorgaben der P2B-Verordnung bislang in Grenzen hält. Eine Evaluierungsstudie im Auftrag der Europäischen Kommission stellte fest, dass die Umsetzung durch die Plattformen „uneinheitlich und unzureichend" sei und dass die Anforderungen nur selten vollständig erfüllt würden.[385] Der Studie zufolge sind der geringe Bekanntheitsgrad und das Fehlen einer wirksamen Durchsetzung die Hauptgründe für diese geringe Wirksamkeit. Insbesondere in Bezug auf Art. 5 der P2B-Verordnung wird festgestellt, dass nur etwa ein Drittel der untersuchten Online-Vermittlungsdienste (96 von 290 oder 33,1 %) ihre Ranking-Parameter transparent machten. Aber auch soweit diese Vorgabe erfüllt wurde, konnten die Beschreibungen der Ranking-Praktiken nur bei einer relativ kleinen Zahl (73 Plattformen, also 25,2 % der untersuchten Dienste) als „gut erklärt" eingestuft werden. Eine später in Auftrag gegebene Studie zur Medienvielfalt im Internet untersuchte zwar nicht explizit die Auswirkungen der P2B-Verordnung, warf aber einen Blick auf die Medienlandschaft in Bezug auf

384 Leitlinien zur Transparenz des Rankings gemäß der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates (2020/C 424/01), EU ABl. C 424, 8.12.2020, S. 1–2.

385 *Gineikytė-Kanclerė/Klimavičiūtė/Kudzmanaitė et al.*, Study on evaluation of the Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services (the P2B Regulation).

Akteure, die der P2B-Verordnung unterliegen, wie etwa Suchmaschinen. Auch diese Studie bescheinigte der Transparenz von durch Algorithmen gesteuerten Rankingsystemen erheblichen Raum für Verbesserungen („ample space for improvement").[386] Diese Erfahrungswerte müssen in Zukunft auch beim DMA mitgedacht werden.

Während das Transparenzgebot des DMA keinen neuen materiellen Regelungsgehalt einführt, ist es aber nunmehr auch im DMA durchsetzbar und unterliegt der unmittelbaren Aufsicht der Kommission. Die Gebote von Fairness und Diskriminierungsfreiheit entfalten demgegenüber auch einen größeren eigenständigen Regelungsgehalt im Vergleich zu bestehenden Vorschriften. Der DMA unterwirft das Ranking einer Inhaltskontrolle.[387] Die Vorschrift etabliert den Gleichheitsgrundsatz für das Ranking und statuiert ein Willkürverbot. Eine ultimative Gleichstellung aller „gerankten" Angebote, wie sie etwa dem Prinzip der Netzneutralität zugrunde liegt,[388] ist damit nicht verbunden. Das würde auch dem Sinn eines Rankings, das die relevantesten oder für den Nutzer passendsten Angebote hervorheben will, zuwiderlaufen. Vielmehr geht es dabei um Chancengleichheit. Weiterhin sind die Torwächter also berechtigt, bestimmte Kriterien für die Bestimmung der Rangfolge anzuwenden und dabei bspw. auch Personalisierungsmethoden heranzuziehen oder nach Qualität oder Nutzerzufriedenheit der Produkte bzw. Dienstleistungen zu fragen. Sie unterliegen aber einer Rechtfertigungspflicht, wenn sie vergleichbare Produkte und Dienstleistungen unterschiedlich behandeln. Das geht über das Verbot der Selbstpräferenzierung und die bisherige wettbewerbsrechtliche Fallpraxis hinaus. Im Detail bleiben die Kriterien für eine sachliche Rechtfertigung bspw. Diskriminierungen noch unklar und sollten durch Leitlinien der Kommission ausgeformt werden.[389]

Inwieweit Art. 6 Abs. 5 S. 2 DMA in Zukunft das Ranking im Einzelfall beeinflussen bzw. verändern wird und insbesondere wie die Kommission darauf einwirken kann, ist bislang noch nicht abzusehen. Dies gilt auch für die Frage, wie mit bezahltem Ranking umgegangen wird und ob eine solche Praxis mit dem Gleichheitsgrundsatz vereinbar ist[390] oder welche Reichweite das Umgehungsverbot („Maßnahmen gleicher Wirkung") hat,

386 *Parcu/Brogi/Verza et al.*, Study on media plurality and diversity online, S. 75 ff.
387 *Herbers*, in: Podszun, Art. 6 Rn. 102.
388 *Wielsch*, in: MKDS, Art. 6 DMA Rn. 77, 87.
389 *Herbers*, in: Podszun, Art. 6 Rn. 137.
390 Zur Diskussion *Wielsch*, in: MKDS, Art. 6 DMA Rn. 87.

bspw. bei Methoden des Gatekeepers, die an sich sachliche Kriterien beeinflussen (bspw. Kundenbewertungen als sachliches Kriterium, die der Gatekeeper aber nur für bestimmte Dienste zulässt)[391]. Bemerkenswert ist aus medienrechtlicher Perspektive, dass durch dieses Gebot nicht mehr nur kommerzielle Interessen der Anbieter eine Rolle bei der Sichtbarkeit und Auffindbarkeit von Inhalten spielen, sondern auch öffentliche Interessen mit einfließen (durch Sicherstellung von Fairness und Nicht-Diskriminierung) ebenso wie diejenigen gewerblicher Nutzer.

Aus den Zielen und der Formulierung der Vorschrift lässt sich ableiten, dass es dabei nicht um Interoperabilität im Sinne eines gleichgestellten Zugangs zum Rankingsystem gehen kann, sondern um dessen Ausgestaltung.[392] Denkbar wäre es, aus der Bestimmung prozedurale Pflichten der Gatekeeper abzuleiten, wonach sie Beschwerden von Nutzern über mögliche Diskriminierungen nachgehen und die Ranking-Algorithmen entsprechend überprüfen müssen.[393]

(6) Kopplungsverbot bei Identifizierungsdiensten, Webbrowser-Engines und Zahlungsdiensten (Art. 5 Abs. 7 DMA)

Nach Art. 5 Abs. 7 DMA darf der Torwächter von Endnutzern oder gewerblichen Nutzern nicht verlangen, dass sie einen Identifizierungsdienst, eine Webbrowser-Engine oder einen Zahlungsdienst des Torwächters nutzen bzw. – im Falle von gewerblichen Nutzern -nutzen, anbieten oder mit ihnen interoperieren. Im Vordergrund der Bestimmung steht die Wahlfreiheit von Endnutzern, die von Multi-Homing profitieren sollen. Daneben profitieren aber auch gewerbliche Nutzer: einerseits von der eigenen Entscheidungsfreiheit, andererseits aber auch von der Entscheidungsfreiheit der Nutzer, was insbesondere mit dem Abbau von Lock-in-Effekten verbunden ist.[394] Abs. 7 etabliert ein striktes Kopplungsverbot, nicht aber eine Pflicht zur Öffnung von Schnittstellen für die jeweiligen genannten Dienste. Insoweit ist Ziel auch die Offenhaltung von Märkten.[395] Für Interoperabilität hat die Bestimmung dennoch aus der Perspektive der gewerblichen Nutzer

391 *Herbers*, in: Podszun, Art. 6 Rn. 106.
392 Zur Diskussion *Wielsch*, in: MKDS, Art. 6 DMA Rn. 88.
393 So etwa *Wielsch*, in: MKDS, Art. 6 DMA Rn. 88.
394 *Wielsch*, in: MKDS, Art. 5 DMA Rn. 146.
395 *Herbers*, in: Podszun, Art. 5 Rn. 138.

Bedeutung. Soweit ein Dienst (Webbrowser, Zahlung, Identifizierung) interoperabel ist, sei es aufgrund einer gesetzlichen Verpflichtung (auch aus dem DMA) oder einer wirtschaftlich gesteuerten Entscheidung des Torwächters, dann darf keine Kopplung dieses Dienstes an eigene Dienste des Torwächters erfolgen. Der Torwächter darf die Nutzung dieser weiteren Dienste nicht „verlangen", was jedenfalls zwingende Registrierungspflichten ausschließt, sich möglicherweise aber auch auf Nudging-Techniken und Dark Patterns erstreckt.[396]

Obwohl Art. 5 Abs. 7 DMA zwar für alle zentralen Plattformdienste gilt, dürfte sich die medienrechtliche Relevanz in Grenzen halten. Während es für Verbraucher sicherlich förderlich ist, nicht unbedingt an eine Apple-ID oder ein Google-Konto zu Identifizierungszwecken gebunden zu sein, profitieren gewerbliche Nutzer maßgeblich nur dann, wenn sie Browser-Engines, Zahlungsdienste oder Identifizierungsdienste selbst anbieten oder an bestimmte Dienste gebunden sind. Gleiches dürfte im Übrigen auch für das Kopplungsverbot zwischen verschiedenen zentralen Plattformdiensten (Art. 5 Abs. 8 DMA) gelten, das Registrierungszwängen entgegenwirkt (bspw. Google-Konto und YouTube oder die Kopplung zwischen Facebook und Instagram, die in der Praxis bereits erste Veränderungen aufgrund des DMA erfährt[397]).

(7) Datenportabilität (Art. 6 Abs. 9 DMA)

Art. 6 Abs. 9 DMA statuiert das Recht der Datenportabilität für Endnutzer der Gatekeeper. Diesen sowie von ihnen beauftragten Dritten soll auf ihren Antrag hin kostenlos die effektive Übertragbarkeit der Daten ermöglicht werden, die sie bereitgestellt oder im Zusammenhang mit der Nutzung des zentralen Plattformdienstes generiert haben. Insbesondere sollen ihnen kostenlos Instrumente, die die effektive Nutzung dieser Datenübertragbar-

396 Für ein weites Begriffsverständnis *Wielsch*, in: MKDS, Art. 5 DMA Rn. 161; wohl anders und mehr bezugnehmend auf eine technische Verhinderung oder Erschwerung *Herbers*, in: Podszun, Art. 5 Rn. 160. Für die Ausgestaltung von Benutzeroberflächen ohne Dark Patterns besteht im Übrigen eine Regelung im DSA für Online-Plattformen (Art. 25 DSA), die auch einen großen Teil der hier adressierten zentralen Plattformdienste erfassen dürfte.

397 Am. 22.1.2024 kündigte Meta an, seinen Nutzern vor dem Hintergrund des DMA ab sofort mehr Auswahlmöglichkeiten in Bezug auf ihre Nutzung von Meta-Produkten zu geben. Dazu gehört auch, dass die Verbindung zwischen Facebook und Instagram gelöst werden kann.

keit erleichtern, und ein permanenter Echtzeitzugang zu diesen Daten bereitgestellt werden.

Ein Recht auf Datenportabilität existiert innerhalb der DS-GVO bereits seit 2018 (dazu eingehend unten C.IV.2.a). Allerdings wollte der EU-Gesetzgeber mit dem DMA bewusst auf den Erfahrungen aus der DS-GVO aufbauen, das Recht an die technischen Gegebenheiten anpassen und die Möglichkeiten der Nutzer stärken. Damit soll der bestehende Schutz aus der DS-GVO erhöht und über die dortigen Regeln hinausgegangen werden.[398] Art. 6 Abs. 9 DMA ist daher weiter und konkreter als Art. 20 DS-GVO. Die Datenportabilität ist wichtige Voraussetzung für die Effektivität der (vertikalen und horizontalen) Interoperabilität, denn diese kann nur dann sinnvoll genutzt werden, wenn Endnutzer ihre Daten auch zu einem anderen Dienst „mitnehmen" bzw. „mitbringen" können.

Die Ausweitung der Rechtsposition betrifft zunächst die Art der erfassten Daten: Art. 20 DS-GVO ist auf personenbezogene Daten beschränkt, Art. 6 Abs. 9 DMA erfasst mangels einer solchen Beschränkung auch andere aggregierte Daten, die nicht unmittelbar zur Identifizierung einer Person herangezogen werden können. Voraussetzung ist lediglich deren Bereitstellung oder Generierung durch den Endnutzer „im Zusammenhang" mit seiner Nutzung des zentralen Plattformdienstes. Das kann aber angesichts der Erwägung, auf der Art. 6 Abs. 9 DMA (auch) basiert – nämlich, dass Torwächter von ihrem Zugang zu großen Datenmengen profitieren, die sie im Zuge des Betriebs der zentralen Plattformdienste sowie anderer digitaler Dienste erheben –, nicht auf Daten beschränkt sein, die der Endnutzer aktiv und vor allem bewusst generiert. Vielmehr sollten insgesamt solche Daten erfasst werden, die der Plattformdienst dem Nutzer zuordnet, unabhängig davon, wie und durch wessen Verhalten deren Generierung veranlasst wurde.[399] Dass hier, anders als in Art. 20 DS-GVO, auch von „generierten" Daten die Rede ist, spricht dafür, dass bewusst Auslegungsfragen, die sich bei Art. 20 DS-GVO als problematisch herausgestellt haben, vermieden werden sollten.[400] Insoweit dürften jedenfalls Ableitungen des

398 Erwgr. 59.

399 So auch *Wielsch*, in: MKDS, Art. 6 Rn. 130; ebenso für ein weites Verständnis *Herbers*, in: Podszun. Art. 6 Rn. 184, der allerdings die Grenze bei Auswertungen und Analysen zieht, die allein durch den Torwächter erfolgen.

400 Dazu unten C.IV.2.a.

Torwächters („beobachtete Daten") unter die Regelung fallen, fraglich wäre die Anwendbarkeit lediglich bei Analysen und Profilauswertungen.[401]

Ein weiterer großer Unterschied zur DS-GVO liegt in der Konkretisierung des (technischen) Übertragungsvorgangs. Der Endnutzer muss ein Format dieser Daten erhalten, das er tatsächlich für die Zwecke des Anbieterwechsels verwenden kann – anders als in der DS-GVO geht es im DMA nicht primär um die persönlichkeitsrechtlichen Aspekte der Verfügungsmacht über eigene Daten, sondern um die Verfügungsmacht über Daten im Wettbewerb (auch zugunsten von Wettbewerbern). Zudem muss ein kontinuierlicher Echtzeitzugang bereitgestellt werden, der in der Praxis auf die zwingende Zurverfügungstellung einer entsprechenden Anwendungsprogrammierschnittstelle hinauslaufen wird, die auch an die Datenverarbeitungssysteme des Torwächters angebunden ist. Im Rahmen der DS-GVO hatte der Gesetzgeber von einer solchen Konkretisierung noch Abstand genommen, hauptsächlich mit den Argumenten fehlender technischer Machbarkeit und zu großer Belastung für Datenverarbeiter.[402] Das zweite Argument trifft aber im Rahmen des DMA nicht zu, da im Gegensatz zur allgemeinen Anwendbarkeit der DS-GVO die im DMA adressierten Gatekeeper über entsprechende Mittel verfügen, wie sich aus den Schwellenwerten für die Benennung ergibt.

Nicht unproblematisch ist aber auch im DMA die technische Umsetzbarkeit der Bestimmung. Erwägungsgrund 59 verlangt „hochwertige, technische Maßnahmen", konkretisiert aber nicht, wie diese aussehen sollen. Ein einheitlicher Industriestandard wie z. B. im Mobilfunk bei SMS existiert zu den Datenpaketen, die nach Art. 6 Abs. 9 DMA zu übertragen sind, nicht. Je weiter der Begriff der „im Zusammenhang mit" einem Plattformdienst generierten Daten verstanden wird, desto schwieriger wird es, einen solchen Standard zu finden. Innerhalb der DS-GVO lassen sich dazu aus der Entscheidungspraxis und den bestehenden Initiativen einiger Plattformen bereits Ableitungen treffen (dazu unten C.IV.2.a(3)). Jedoch konnte im dortigen Zusammenhang anders als beim DMA nicht einbezogen werden, dass der Verarbeiter dem Datensubjekt „Instrumente" zur Portabilität bereitstellen muss. Im DMA wird es daher für den Umfang der Portabilität und das Maß an Benutzerfreundlichkeit maßgeblich auf die Ausgestaltung durch

401 Verneinend *Herbers*, in: Podszun, Art. 6 Rn. 184.

402 Vgl. die Folgenabschätzung zur DS-GVO, Commission staff working paper, SEC(2012) 72 final, S. 106, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072.

die Gatekeeper im Dialog mit der Kommission ankommen (siehe unten C.II.2.c(11)).

(8) Weitere relevante Bestimmungen zur Ausgestaltung der Interoperabilität

Weitere Elemente der Art. 5 und 6 des DMA befassen sich nicht unmittelbar mit der Interoperabilität zwischen Diensten im Sinne einer Ermöglichung des Zugangs. Dennoch sind weitere Regeln in die Betrachtung einzubeziehen, weil sie im Gesamtzusammenhang stehen. So verfolgen bestimmte „Do's" und „Dont's" nämlich solche (Teil-)Ziele, die entweder aus Nutzersicht auch ein gewünschtes (Teil-)Ergebnis bei einem Bestehen von Interoperabilität wären oder eine bestehende Interoperabilität erst effektiv machen würden.

Einerseits sind es Bestimmungen, die zwar nicht das Ob des Zugangs oder der Zugänglichkeit (Interoperabilität) vorschreiben, aber doch ein gewisses Maß an Interaktion zwischen Endnutzern und gewerblichen Nutzern auf dem zentralen Plattformdienst ermöglichen sollen. So sieht Art. 5 Abs. 4 DMA vor, dass Torwächter gewerblichen Nutzern Werbung gegenüber und Vertragsschlüsse mit Endnutzern ermöglichen müssen, die über den jeweiligen zentralen Plattformdienst akquiriert worden sind. Es muss also eine geeignete Kommunikationsmöglichkeit geschaffen werden:[403] Dienstleister und (potenzielle) Kunden dürfen nicht voneinander abgeschirmt werden.[404] Die medienrechtliche Relevanz dokumentiert das von der Kommission gewählte Beispiel solcher Anti-Steering-Maßnahmen in ihrer Folgenabschätzung zum DMA: Eine solche Maßnahme liege vor, wenn ein Torwächter technisch oder durch Vertragsbedingungen verhindere, dass ein Zeitungsverlag in der im App-Store des Torwächters verfügbaren App auf günstigere Abo-Konditionen auf der Website des Verlages selbst

403 Erwgr. 40 DMA.

404 Dieses nunmehr ausdrückliche Gebot im DMA folgt aus bereits vorher eingeleiteten kartellrechtlichen Verfahren z. B. gegenüber Apple (vgl. SWD(2020) 363 final (Fn. 348), Rn. 54). Sowohl in Bezug auf die Benachteiligung anderer Musik-Streamingdienste neben Apple Music (Verfahren der Europäischen Kommission AT.40437) als auch von In-App-Käufen bei Videospielen (US-amerikanisches Verfahren des Fortnite-Anbieters: Epic Games, Inc. v. Apple Inc., Az. 20-cv-05640-YGR) wurden kartellrechtliche Bedenken vorgebracht. Vgl. dazu eingehend *Wielsch*, in: MKDS, Art. 5 DMA Rn 97 f.

(statt in der App) hinweise.[405] Art. 5 Abs. 5 DMA erweitert das auf Inhalte, Abonnements, Funktionen und andere Elemente in Software-Anwendungen gewerblicher Nutzer: Torwächter müssen sicherstellen, dass Endnutzer Zugriffe auf diese auch innerhalb eines zentralen Plattformdienstes haben. „Software-Anwendung" meint in diesem Zusammenhang ein digitales Produkt oder eine digitale Dienstleistung, das bzw. die über ein Betriebssystem genutzt wird. Zentraler Anwendungsbereich beider Vorschriften sind also App-Stores und In-App-Käufe.

In einem ähnlichen Kontext, aber in Bezug auf den potenziellen Anwendungsbereich weiter gefasst, ist auch Art. 6 Abs. 3 UAbs. 2 S. 1 DMA zu sehen. Danach hat der Torwächter es Endnutzern zu gestatten und auch technisch zu ermöglichen, Standardeinstellungen des Betriebssystems, der virtuellen Assistenten und des Webbrowsers des Torwächters, die Endnutzer zu vom Torwächter angebotenen Produkten oder Dienstleistungen leiten oder lenken, auf einfache Weise zu ändern. Die Regelung ist daher eng mit den erwähnten Kopplungsverboten verzahnt (Art. 5 Abs. 7 und 8 DMA, siehe oben C.II.2.c(6)). Sie verbietet aber nicht die Vorinstallation von Anwendungen.

Nach Art. 6 Abs. 6 DMA dürfen zudem die Möglichkeiten von Endnutzern, zwischen verschiedenen Software-Anwendungen oder anderen Diensten zu wechseln oder solche zu abonnieren, nicht technisch oder anderweitig beschränkt werden. Das verpflichtet Torwächter aber nicht zur Schaffung eines entsprechenden Zugangs zu ihren Diensten, sondern betrifft nur ein Beschränkungsverbot. Während sich also Art. 6 Abs. 4 und 7 DMA auf die Öffnung von Schnittstellen vor allem für gewerbliche Nutzer beziehen (Interoperabilität bei Single-Homing), geht es bei Art. 6 Abs. 6 DMA um die Wettbewerber, da deren Dienste, die vergleichbar zu denen des Torwächters sind, nicht durch Behinderungsmaßnahmen vom Wettbewerb ausgeschlossen werden sollen (Ermöglichung von Multi-Homing). Deshalb ist die Vorschrift auch deutlich weiter gefasst („Software-Anwendungen und Dienste, auf die über die zentralen Plattformdienste des Torwächters zugegriffen wird") und erstreckt sich auf alle zentralen Plattformdienste, die solche Behinderungstaktiken anwenden könnten, etwa durch technische Sperren oder bestimmte Nudging-Techniken.

All diese Regeln, mit Ausnahme von Art. 5 Abs. 5 DMA im Hinblick auf Zusatzelemente, setzen jeweils voraus, dass eine Schnittstellenoffenheit bereits besteht, was wiederum weiterhin außerhalb der genannten verpflich-

405 SWD(2020) 363 final (Fn. 348), Rn. 53.

tenden Interoperabilitätsregeln von den Entscheidungen des Torwächters abhängt.

Andererseits sind auch solche Regeln relevant, die Transparenz gegenüber und Zugriff auf Daten durch gewerbliche Nutzer sicherstellen sollen. Neben Regeln zur Transparenz des Online-Werbeinventars (Art. 5 Abs. 9 und 10 DMA), die für die Finanzierung von (vor allem medialen) Online-Angeboten von erheblicher Bedeutung sein dürften, betrifft das vor allem Art. 6 Abs. 10 DMA. Danach gewährt der Torwächter gewerblichen Nutzern auf ihren Antrag hin kostenlos einen „effektiven, hochwertigen und permanenten Echtzeitzugang" zu von ihnen oder ihren Endnutzern generierten Daten. Das erstreckt sich auf (aggregierte und nicht-aggregierte) Daten, die im Zusammenhang mit der Nutzung der betreffenden zentralen Plattformdienste oder von Diensten, die zusammen mit den betreffenden zentralen Plattformdiensten oder zu deren Unterstützung erbracht werden, generiert werden. Die Vorschrift ist zwar nicht als unmittelbare Interoperabilitäts-, wohl aber als Zugangseröffnungspflicht zu verstehen,[406] gewährt also nicht Zugang zu einer Plattform, aber Zugang zu einem bestimmten Bereich dieser Plattform, der gewerblichen Nutzern bislang regelmäßig versperrt ist (namentlich zu den ihn betreffenden „Datensilos"[407]). Sie ist das Spiegelbild zur Datenportabilität für Nutzer nach Art. 6 Abs. 9 DMA.

Beschränkt ist dieser Zugang aus der Perspektive der gewerblichen Nutzer aber auf solche Daten, zu deren Aggregation sie zumindest beigetragen haben. Sie werden also insbesondere nicht in die gleiche Lage versetzt wie der Torwächter, der Daten aller Endnutzer und gewerblichen Nutzer hat und aus deren Weiterverarbeitung wiederum Rückschlüsse und Verwertungsmöglichkeiten ziehen kann. Der Torwächter muss die Nutzung der vorher genannten Daten ermöglichen, was die Bereitstellung entsprechend nutzbarer Formate voraussetzt. Bei personenbezogenen Daten ist das allerdings von der Einwilligung der Endnutzer abhängig. Wie beim Recht auf Datenportabilität ist die Ausgestaltung eines effektiven und hochwertigen Zugangs in seiner genauen Gestalt noch nicht absehbar, da auch hier bislang keine Standards für solche Datenzugänge bzw. Schnittstellen existieren.

406 *Wielsch*, in: MKDS, Art. 6 Rn. 139.
407 *Herbers*, in: Podszun, Art. 6 Rn. 205.

(9) Spezifische Vorgabe horizontaler Interoperabilität von Messenger-Diensten (Art. 7 DMA)

Art. 7 DMA ist eine in sich geschlossene Vorschrift, die bewusst losgelöst von den Art. 5 und 6 DMA aufgenommen wurde. Kern der Vorschrift ist Abs. 1, wonach Torwächter hinsichtlich ihrer Messenger-Dienste (in der telekommunikationsrechtlichen Begrifflichkeit, die im DMA aufgegriffen ist: nummernunabhängige interpersonelle Kommunikationsdienste) Interoperabilität der grundlegenden Funktionen dieser Dienste mit anderen Messenger-Diensten sicherstellen müssen. Zu diesem Zweck sind auf Antrag der dritten Anbieter kostenlos die hierzu erforderlichen technischen Schnittstellen oder ähnliche Lösungen bereitzustellen.

(a) Zweck und Gesetzgebungsprozess

Erwägungsgrund 64 verdeutlicht die Zwecksetzung von Art. 7 DMA mit der Erhöhung der Bestreitbarkeit der Märkte und der Senkung von Marktzutrittsschranken, die sowohl durch starke Netzwerkeffekte auf dem Markt für Messenger-Dienste als auch durch die Zugehörigkeit von interpersonellen Kommunikationsdiensten zu Plattformökosystemen geprägt sind. Gerade diese vernetzten Plattformstrukturen lassen sich durch die Förderung von Multi-Homing, die das Ziel zahlreicher anderer Bestimmungen des DMA ist, allein nicht aufbrechen.

Die Vorschrift wurde auf Vorschlag des Europäischen Parlaments in den Trilogprozess eingebracht.[408] Der Kommissionsvorschlag sah demgegenüber lediglich in Art. 6 Abs. 1 lit. f DMA-E vor, dass gewerblichen Nutzern und Anbietern von Nebendienstleistungen der Zugang zu und die Interoperabilität mit den gleichen Betriebssystemen, Hardware- oder Softwarefunktionen wie dem Gatekeeper zur Verfügung stehen sollen. Das Hauptziel dieser vorgeschlagenen „vertikalen" Interoperabilitätsvorschrift war es, diesen Anbietern die Möglichkeit zu geben, mit dem Betriebssystem des Gatekeepers und dessen Funktionen zu interoperieren, um die Bestreitbarkeit solcher Zusatzdienste sicherzustellen.

408 *Institut für Europäisches Medienrecht (EMR)*, DMA-Synopse (Version vom 08.01.2022), https://emr-sb.de/synopsis-dma/.

Gegen die vom Parlament vorgeschlagene „horizontale" Interoperabilität äußerte die Kommission im Trilog starke Bedenken.[409] Dabei sah sie die zusätzliche Interoperabilität bereits nicht als erforderlich an, weil es entsprechende andere Regelungen im DMA gebe, die die Bestreitbarkeit und Fairness adressieren und daher den vom Parlament als Grund für die Interoperabilitätsregel vorgebrachten Netzwerkeffekten entgegenwirken.[410] Auch wandte sie ein, dass eines der Hauptziele des DMA gerade das Multi-Homing sei, auf das eben diese Bestimmungen hinwirkten, was von horizontaler Interoperabilität, die von einem Torwächter-Dienst auszugehen habe, in gewisser Weise konterkariert werde.[411] Interoperabilität könnte demzufolge den gegenteiligen Effekt haben, dass Nutzer keinen Anreiz mehr hätten, von den marktführenden Diensten weg zu wechseln, und so die Netzwerkeffekte noch verstärken. Auch nannte die Kommission technische Probleme als Grund gegen die Einführung der Regel, darunter Datensicherheitsbedenken (insb. mit Blick auf die Verschlüsselung), den Grundsatz der Datenminimierung, die Heterogenität der verschiedenen Dienste und Problematiken bei der Inhaltemoderation. Vorgebracht wurden auch negative Einflüsse auf Innovationen und Investitionen, da die Regelung zu einer möglichst weitreichenden Homogenität aller Dienste führen würde, die sich an den Standards des Torwächters orientieren würde. Gerade kleine Dienste, die ihr Angebot gegen Entgelt erbrächten, würden von einer Interoperabilität mit großen kostenlosen Angeboten nicht profitieren, sondern eher ihren Marktanteil dadurch verlieren.

Die Kommission schlug daher verschiedene andere Optionen vor, um das Ziel des Parlaments zu erreichen (bspw. eine Verpflichtung der Kommission zur weiteren Untersuchung des Themas oder eine weitere Stärkung des Multi-Homings bei Messenger-Diensten im DMA). Letztlich setzte sich das Parlament aber mit der unmittelbaren Interoperabilitätsregelung für

409 Non-paper from the Commission services on interoperability for messenger services and online social networks in the DMA, https://www.lobbycontrol.de/wp-content/uploads/non_paper_interoperability_dma.pdf, S. 2 ff.

410 Non-paper from the Commission (Fn. 409), S. 2. Die Kommission nannte hier insbesondere das Verbot der Datenzusammenführung, die Kopplungsverbote von Diensten und Registrierungen, die Pflichten zur Ermöglichung der Deinstallation von Software und Einstellungsoptionen sowie die Regeln zur Datenportabilität von Endnutzern und zum Datenzugang von gewerblichen Nutzern.

411 Hier verweist die Kommission ausdrücklich auf die Studie der Bundesnetzagentur von 2021 (*BNetzA*, Interoperabilität von Messenger-Diensten, vgl. dazu unten C.VI.3.c).

Messenger-Dienste durch, ohne diese aber, wie ursprünglich ebenfalls in der Parlamentsposition vorgesehen, auch auf soziale Netzwerke zu erstrecken. Für soziale Netzwerke hätte die Position des Parlaments in Bezug auf die Zusammenschaltungsanforderungen bedeutet, dass Drittanbietern sozialer Netzwerke die Möglichkeit eingeräumt worden wäre, den Zugang und die Zusammenschaltung bei Merkmalen wie Text, Video, Stimme und Bild zu beantragen, wobei der Zugang und die Zusammenschaltung bei grundlegenden Merkmalen wie Posts, Likes und Kommentaren für Dienste sozialer Netzwerke grundsätzlich bereitzustellen gewesen wäre.[412] Der Vorschlag des Parlaments hinsichtlich der Messenger-Dienste ist auch damit zu erklären, dass im Messenger-Bereich eine sehr starke Konzentration zu beobachten ist,[413] die wiederum der Tatsache geschuldet ist, dass es bei solchen Diensten besonders im Nutzerinteresse liegt, eine möglichst große Zahl an Kontakten erreichen zu können, womit die Netzwerkeffekte für die Anbieter daher besonders wirkungsvoll sind.

(b) Nummernunabhängiger interpersoneller Kommunikationsdienst

Art. 2 Nr. 9 DMA verweist zur Definition des Begriffs nummernunabhängiger interpersoneller Kommunikationsdienst auf die Legaldefinition in Art. 2 Nr. 7 EKEK: ein interpersoneller Kommunikationsdienst, der weder eine Verbindung zu öffentlich zugeteilten Nummerierungsressourcen, nämlich Nummern nationaler oder internationaler Nummerierungspläne, herstellt noch die Kommunikation mit Nummern nationaler oder internationaler Nummerierungspläne ermöglicht.

Es geht also („nummernunabhängig") um Over-the-Top-(OTT-)Dienste, die nicht an einen bestimmten Anschluss wie eine Rufnummer gebunden sind, sondern eigene Zuordnungsmethoden verwenden. Der Begriff

412 Vgl. Erwgr. 52a der Parlamentsposition, Abänderungen des Europäischen Parlaments vom 15. Dezember 2021 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte) (COM(2020)0842 – C9–0419/2020 – 2020/0374(COD)), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0499_DE.html.

413 Ein Großteil der Nutzer vereint sich weltweit auf die drei Dienste WhatsApp, Facebook Messenger und WeChat (vor allem im asiatischen Raum); vgl. *Curry*, Messaging App Revenue and Usage Statistics (2023), 9.1.2023, https://www.businessofapps.com/data/messaging-app-market/, m. w. N.

„interpersoneller Kommunikationsdienst" beschreibt die Abgrenzung zu Massenkommunikationsdiensten wie dem Rundfunk. Ein elektronischer Kommunikationsdienst – diesen definiert der EKEK als gewöhnlich gegen Entgelt über elektronische Kommunikationsnetze erbrachte Dienste mit der Ausnahme von Diensten, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben – bietet keine Inhalte an und übt auch keine redaktionelle Kontrolle über die Kommunikation aus. Der Begriff des elektronischen Kommunikationsdienstes fügt sich somit in das System des europäischen Medienrechts, das – vereinfacht formuliert – zwischen der Bereitstellung der Technologie (Netzinfrastrukturen und Transportdienste) und des Inhalts (eigenes Angebot bzw. redaktionelle Kontrolle) unterscheidet.[414] In Abgrenzung zum linearen Rundfunk, zu Videoabrufdiensten, sozialen Netzwerken und Blogs umfassen interpersonelle Kommunikationsdienste nur die Kommunikation zwischen einer begrenzten Zahl von Personen.[415]

Stellt sich eine Kommunikationsfunktion (bspw. Instant Messages oder Chats) nur als Nebenfunktion dar, wie das auf vielen Online-Angeboten der Fall ist, dann wird der Dienst damit nicht zu einem Kommunikationsdienst. Messenger-Dienste wie WhatsApp, Messenger (Meta), Threema, Signal oder WeChat sind also zweifelsfrei interpersonelle Kommunikationsdienste, nicht aber Chats in Videospielen.[416] Unter die Vorschrift fallen darüber hinaus auch E-Mail- und VoIP- bzw. Videotelefonie-Dienste wie Gmail, Skype und Microsoft Teams.[417] Für andere Angebote gilt, dass sie, je umfassender die „Neben"-Funktion ausgestaltet und je relevanter sie für den Dienst ist, desto eher den Anforderungen des DMA unterfallen, wobei es zu Abgrenzungsschwierigkeiten kommen kann. Rechtssicherheit schafft jedoch, dass erst durch eine Benennung als Gatekeeper und die Auflistung als zentrale Plattformdienst eine Bindung an den DMA entsteht.

(c) Umfang der Interoperabilität

Die Interoperabilität für diese Dienste erstreckt sich nach Abs. 1 nur auf „grundlegende Funktionen". In einem zeitlich gestaffelten Ansatz beschreibt

414 *Oster*, in: MKDS, Art. 2 Rn. 33.
415 *Oster*, in: MKDS, Art. 2 Rn. 35.
416 Erwgr. 17 EKEK.
417 *Bongartz/Kirk*, in: Podszun, Art. 2 Rn. 54.

Abs. 2, was der DMA als grundlegende Funktionen versteht und wann diese zu gewährleisten sind: Unmittelbar nach Benennung sind dies Ende-zu-Ende-Textnachrichten inklusive Bild-, Sprach-, Video- und andere Dateien zwischen zwei Endnutzern, innerhalb von zwei Jahren dann der gleiche Umfang, aber innerhalb von Gruppen einzelner Nutzer, und nach spätestens vier Jahren auch Ende-zu-Ende-Sprach- und -Videoanrufe von Einzelnutzern und Gruppen. Prozedural hat der Torwächter hierzu ein Referenzangebot mit den technischen Einzelheiten und allgemeinen Bedingungen für die Interoperabilität zu veröffentlichen (Art. 7 Abs. 4 DMA). Auf dieses können interessierte Mitbewerber mit einem Antrag auf Zugang reagieren, der – bei Zumutbarkeit – innerhalb von drei Monaten vom Torwächter zu erfüllen ist (Art. 7 Abs. 5 DMA). Hierin zeigt sich auch die Flexibilität der Bestimmung, die im Wesentlichen das „Wie" der Umsetzung den Torwächtern überlässt und erst ex post eine Kontrolle durch die Kommission vorsieht.[418]

Diese Fristen können von der Europäischen Kommission ausnahmsweise weiter verlängert werden, wenn der Gatekeeper nachweist, dass dies notwendig ist, um eine wirksame Interoperabilität zu gewährleisten und das erforderliche Sicherheitsniveau, ggf. einschließlich einer Ende-zu-Ende-Verschlüsselung, aufrechtzuerhalten (Art. 7 Abs. 6 DMA). Die Kommission kann auch Verpflichtungen aussetzen, die aufgrund außergewöhnlicher Umstände, die sich der Kontrolle des Gatekeepers entziehen, die wirtschaftliche Tragfähigkeit seines Betriebs in der Union gefährden würden (Art. 9 DMA), oder einen Gatekeeper aus Gründen der öffentlichen Gesundheit oder der öffentlichen Sicherheit von der Verpflichtung freistellen (Art. 10 DMA).

Wichtige Bestimmungen, die den Umfang der Gewährleistung von Interoperabilität von Messenger-Diensten begrenzen und dabei auch auf die von der Kommission im Legislativprozess geäußerten Bedenken reagieren, finden sich in den weiteren Absätzen von Art. 7 DMA. So betreffen Abs. 3 und 9 Sicherheitsbedenken: Das Sicherheitsniveau, ggf. einschließlich der Ende-zu-Ende-Verschlüsselung, das der Torwächter seinen eigenen Endnutzern bietet, muss bei allen interoperablen Diensten beibehalten werden (Abs. 3). Auch das Referenzangebot muss die erforderlichen Einzelheiten zum Sicherheitsniveau und zur Ende-zu-Ende-Verschlüsselung enthalten. Das bedeutet, dass ein Dienst wie bspw. WhatsApp, der ausschließlich eine

418 Dazu *Wielsch*, in: MKDS, Art. 7 Rn. 11 f.

Ende-zu-Ende-Verschlüsselung anbietet, nicht verpflichtet ist, Funktionen einzuführen, die nicht Ende-zu-Ende-verschlüsselt sind. Zur Herstellung von Interoperabilität wird es daher voraussichtlich erforderlich sein, dass zumindest die verschlüsselten Metadaten (nicht aber die übermittelten Inhalte), auf die der Gatekeeper Zugriff hat und die benötigt werden, um Sicherheitsfunktionen zu betreiben (bspw. Anti-Phishing), auch Drittanbietern zur Verfügung stellen muss, sodass diese die Sicherheitsfunktionen ebenfalls aufrechterhalten können.[419] Zu weitgehend dürfte es allerdings sein, in technischer Hinsicht identische Sicherheitsvorkehrungen zu verlangen, sodass im Sinne einer effektiven Interoperabilität vielmehr äquivalente Maßnahmen zur Gewährleistung von Datensicherheit zu fordern sein dürften.[420] Der Torwächter ist zudem nicht daran gehindert, Maßnahmen zu ergreifen, um sicherzustellen, dass Drittanbieter die Integrität, die Sicherheit und den Schutz der Privatsphäre seiner Dienste nicht gefährden (Abs. 9). Diese Möglichkeit steht aber unter dem Vorbehalt der „unbedingten" Erforderlichkeit und Angemessenheit und unterliegt einer Begründungspflicht auf Seiten des Gatekeepers.

Während Abs. 9 bereits den Aspekt des Privatsphäreschutzes aufgreift, wird der Schutz der Endnutzer durch Abs. 7 und 8 vertieft. Diesen soll es zum einen freigestellt bleiben, ob sie die bereitgestellten interoperablen Funktionen nutzen (Abs. 7). Zum anderen dürfen Torwächter nur diejenigen personenbezogenen Daten von Endnutzern erheben und mit Drittanbietern austauschen, die für eine wirksame Interoperabilität unbedingt erforderlich sind (Abs. 8). Dabei sind die Torwächter unabhängig vom DMA an die Regeln der DS-GVO und der ePrivacy-Richtlinie (bzw. ihrer nationalen Umsetzungen) gebunden. Im Ergebnis läuft dies darauf hinaus, dass die tatsächliche Herstellung effektiver Interoperabilität nicht auf Seiten der Torwächter oder Drittanbieter liegt – diese müssen bzw. können nur die Bedingungen dazu schaffen. Vielmehr ist sie von einer aktiven Entscheidung des Endnutzers auf Empfänger- und Senderseite, im datenschutzrechtlichen Sinne also von einer Einwilligung abhängig.

419 Vgl. dazu und zum Folgenden auch *Brown*, Private Messaging Interoperability in the EU Digital Markets Act, S. 10 ff.

420 *WIK-Consult*, Interoperabilitätsvorschriften für digitale Dienste, S. 128.

(d) Herstellung von Interoperabilität

Art. 7 DMA spricht lediglich davon, dass der Torwächter die erforderlichen technischen Schnittstellen oder ähnliche Lösungen bereitzustellen hat. Obwohl der DMA den Begriff der Interoperabilität definiert (vgl. oben C.II.2.c(2)), kommt es auch an dieser Stelle darauf an, welche technischen Mittel gerade für Messenger-Dienste verfügbar sind und welche sich dazu eignen, die hinter der Interoperabilität liegenden Ziele – die nahtlose Kommunikation von Endnutzern verschiedener Messenger-Dienste – zu erreichen. Einheitliche Industriestandards gibt es, ähnlich wie bei den zuvor diskutierten Bestimmungen des DMA, jedoch noch nicht. Was die Schaffung von Interoperabilität und offene Standards betrifft, gibt es lediglich eine Reihe von privatwirtschaftlich organisierten Initiativen, an die angeknüpft oder die gefördert werden könnten. Zu nennen sind hier etwa die Engineering Task Force (IETF)[421] und das World Wide Web Consortium (W3C).

Die naheliegende Option der Umsetzung werden öffentliche, begrenzte Versionen von Anwendungsprogrammierschnittstellen (APIs) und verwandten Funktionen sein, die Gatekeeper bereits in ihren eigenen Systemen verwenden.[422] Auf diese könnten Drittanbieter dann zugreifen, wären aber auch in der Verantwortung, ihre Dienste im Hinblick auf die Kompatibilität mit der Schnittstelle auf dem neuesten Stand zu halten, was angesichts der möglichen Vielzahl an Drittdiensten nicht einfach umsetzbar scheint.

Ob sog. „Bridges", die als externer Dienst im Sinne eines Übersetzers fungieren würden, den Anforderungen von Art. 7 DMA entsprechen, erscheint zumindest fragwürdig.[423] Sie würden in gewisser Weise außerhalb des Plattformökosystems stehen, wären insbesondere nicht selbst zentraler Plattformdienst, würden aber allein vom Torwächter kontrolliert und wären maßgeblicher Faktor für das Funktionieren der Interoperabilität. Derzeit arbeiten die Messenger-Dienste noch auf der Basis unterschiedlicher Protokolle, die oftmals nicht miteinander kompatibel sind. Die Einrichtung von Bridges oder eines sonstigen unabhängigen, neutralen und vertrauenswürdigen Intermediärs als eine Art „Clearingstelle" stößt auch in techni-

421 Vgl. dazu insbesondere das Projekt More Instant Messaging Interoperability (mimi) https://datatracker.ietf.org/group/mimi/about/.

422 *Brown*, Private Messaging Interoperability in the EU Digital Markets Act, S. 12.

423 Hierzu eingehend *Wielsch*, in: MKDS, Art. 7 Rn. 18 f.; *BKartA*, Abschlussbericht Sektoruntersuchung Messenger- und Video-Dienste, S. 146 ff.

scher Hinsicht an Grenzen. Beispielsweise nutzen Dienste wie Threema keine Rufnummern, sondern anonymisierte Identifikationsnummern für ihr Adressierungsschema und speichern auch sonst keine weiteren IDs oder Metadaten, die das Senden und Empfangen über einen Intermediär ermöglichen könnten.[424] Auch wären Ende-zu-Ende-Verschlüsselungen über solche Übersetzer kaum umzusetzen.

Eine weitere Möglichkeit wäre die Entwicklung (offener) technischer Standards, damit Drittanbieter sich nicht an mehrere Schnittstellen verschiedener Torwächter anpassen müssen. Für eine solche Vereinfachung wird es aber voraussichtlich keinen Anreiz auf Seiten der Gatekeeper geben, und entsprechende Vorschläge, solche Standards verbindlich festzulegen, haben sich im Gesetzgebungsprozess zum DMA nicht durchgesetzt.[425]

(10) Umgehungsverbot (Art. 13 DMA)

Alle genannten Bestimmungen des DMA sind im Lichte des in Art. 13 DMA statuierten Umgehungsverbots zu sehen. Nach Abs. 2 der Vorschrift darf der Torwächter kein Verhalten an den Tag legen, das die wirksame Einhaltung der Verpflichtungen aus den Art. 5, 6 und 7 DMA untergräbt, unabhängig davon, ob das Verhalten vertraglicher, kommerzieller, technischer oder sonstiger Art ist oder in der Verwendung von Verhaltenslenkungsmethoden oder einer Schnittstellengestaltung besteht. Das lässt der Kommission die Möglichkeit, auf solche Taktiken (inklusive technischen Fortschritts) zu reagieren, die an sich nicht den Pflichten widersprechen, aber den Zielen des DMA zuwiderlaufen. Ist zur Einhaltung zudem eine Einwilligung von Nutzern zur Datenverarbeitung erforderlich, so fordert Art. 13 Abs. 5 DMA vom Gatekeeper, deren Erhalt mit angemessenen Mitteln zu unterstützten oder ggf. Daten zu anonymisieren.

Art. 13 Abs. 6 DMA geht noch einen Schritt weiter und bestimmt, dass der Torwächter die Bedingungen oder die Qualität der zentralen Plattformdienste für gewerbliche Nutzer oder Endnutzer, die von den in den Art. 5, 6 und 7 DMA festgelegten Rechten bzw. Möglichkeiten Gebrauch machen, nicht verschlechtern oder übermäßig erschweren darf. Dazu gehören auch Nudging-Techniken, also bspw. dass dem Endnutzer Wahlmöglichkeiten in einer nicht neutralen Weise angeboten oder seine Autonomie, Entschei-

424 *Monopolkommission*, Telekommunikation 2021, S. 88.
425 *Brown*, Private Messaging Interoperability in the EU Digital Markets Act, S. 14.

dungsfreiheit oder freie Auswahl durch die Struktur, Gestaltung, Funktion oder Art der Bedienung einer Benutzerschnittstelle untergraben werden.

(11) Umsetzung und Rechtsdurchsetzung des DMA

Die Umsetzung und Durchsetzung des neuen Regelungswerkes wird in Zukunft ein zentraler Punkt für seine Effektivität sein, auch und vor allem in Bezug auf die Interoperabilitätsvorschriften. Dazu bedarf es nach der in der Verordnung vorgesehenen Aufsichtsstruktur der Justierung zahlreicher „Stellschrauben". Zunächst sind die konkreten Adressaten des Regelungswerkes durch die Benennung zu bestimmen. Darüber hinaus sind einige Bestimmungen des DMA konkretisierungsfähig oder sogar -bedürftig. Dies gilt zuvorderst für den Art. 6 DMA. Für die weitere Konkretisierung sieht der DMA mehrere Möglichkeiten vor, u. a. einen „Dialog" der Torwächter mit der Kommission, Durchführungsrechtsakte, delegierte Rechtsakte und die Entwicklung von Standards. Erst auf dieser Basis kann die eigentliche Rechtsdurchsetzung erfolgen.

(a) Benannte Gatekeeper

Auf der Basis des in Kapitel II DMA näher bestimmten Benennungsverfahrens hat die Europäische Kommission am 6. September 2023 die ersten sechs Torwächter benannt, die die Pflichten des DMA – regelmäßig nach einer Übergangsfrist von sechs Monaten – zu erfüllen haben: Alphabet, Amazon, Apple, ByteDance, Meta und Microsoft.[426] Dienstbezogene Pflichten des DMA sind von den Gatekeepern aber nicht per se für alle ihre Dienste zu erfüllen, sondern nur in Bezug auf zentrale Plattformdienste, die sie betreiben. So notifizierte etwa Samsung bei der Kommission seine eigene Stellung als über den Schwellenwerten liegend, hatte aber keinen zentralen Plattformdienst in seinem Portfolio.[427] Zum derzeitigen Zeitpunkt (Stand Februar 2024) sind 22 Dienste in den unterschiedlichen Kategorien benannt:

426 Hierzu und zum Folgenden Europäische Kommission, Pressemitteilung v. 6.9.2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328.

427 Zwar wurden von Samsungs Internetbrowser die quantitativen Schwellenwerte erreicht, nicht aber die qualitativen als „essenzielles" Zugangstor.

- Vermittlungsdienste:
  - Google Maps
  - Google Play
  - Google Shopping
  - Amazon Marketplace
  - App Store (Apple)
  - Meta Marketplace
- Soziale Netzwerke:
  - TikTok (ByteDance)
  - Facebook (Meta)
  - Instagram (Meta)
  - LinkedIn (Microsoft)
- Online-Werbedienste:
  - Google Ads
  - Amazon Ads
  - Meta Ads
- Nummernunabhängige interpersonelle Kommunikationsdienste:
  - WhatsApp (Meta)
  - Messenger (Meta)
- Video-Sharing-Plattformen:
  - YouTube (Google)
- Suchmaschinen:
  - Search (Google)
- Webbrowser:
  - Chrome (Google)
  - Safari (Apple)
- Betriebssysteme:
  - Android (Google)
  - iOS (Apple)
  - Windows (Microsoft)

Interessanterweise hat die Europäische Kommission bislang weder Cloud-Dienste noch – was im vorliegenden Zusammenhang besonders relevant sein dürfte – virtuelle Assistenten als zentrale Plattformdienste benannt. Potenzielle Dienste, die von Torwächtern angeboten werden, wären Apples Siri, Amazons Alexa, Microsofts Copilot und der Google Assistant. Das kann damit zusammenhängen, dass erst durch das Europäische Parlament virtuelle Assistenten in den Regelungsbereich des DMA aufgenommen wurden, die „Vorbereitungszeit" hier also geringer war. Es ist aber

insofern verwunderlich, als die Europäische Kommission in einer Sektoruntersuchung zum Internet der Dinge von 2021 feststellte, dass die drei Sprachassistenten von Amazon (Alexa), Google (Assistant) und Apple (Siri) eine dominante Markposition innehaben, und starke Bedenken in Bezug auf fehlendes Multi-Homing, einseitige Standardeinstellungen, Datenakkumulation und Interoperabilität äußerte.[428] Damit sind allesamt Aspekte angesprochen, die der DMA adressiert. Die Kommission stellte weiter fest, dass „[d]ie Fähigkeit zur Vernetzung und Kommunikation mit den verschiedenen Komponenten eines Ökosystems, d. h. die Interoperabilität zwischen intelligenten Geräten, Sprachassistenten und Diensten im Bereich des IoT für Verbraucher, von entscheidender Bedeutung für die vollständige Einführung der Funktionen [ist], die ein Ökosystem im Bereich des IoT für Verbraucher den Nutzern bieten kann. Die Interoperabilität zwischen verschiedenen Marken ist ebenso wichtig, da sie es den Nutzern ermöglicht, mit heterogenen Produkten eigene Ökosysteme im Bereich des IoT für Verbraucher aufzubauen, wodurch die Verbraucher mehr Auswahl bekommen und verhindert wird, dass sie an die Produkte eines bestimmten Anbieters gebunden sind."[429]

Allerdings hat die Kommission bereits eine weitere Marktuntersuchung eingeleitet, die über die mögliche Benennung zusätzlicher Dienste Aufschluss geben soll. Das betrifft insbesondere solche Dienste, die zwar die quantitativen Schwellenwerte erreichen, aber möglicherweise nicht die qualitative Schranke, ein essenzielles Zugangstor zu sein, wie von Anbieterseite bspw. in Bezug auf Mircosofts Bing, Edge und MS Ads oder Apples iMessage vorgetragen. Es kann aber auch den umgekehrten Fall betreffen, in dem quantitative Schwellenwerte nicht erreicht werden, der Dienst sich aber als essenzielles Zugangstor darstellt, so bspw. bei Apples iPad OS.

Mit Ausnahme von Sprachassistenten sind allerdings die wichtigsten Dienste im Zusammenhang mit den Interoperabilitätsvorschriften des DMA benannt. Das betrifft insbesondere die App-Stores von Apple und Google sowie die Messenger-Dienste von Meta (nicht aber den iMessage-Dienst von Apple). Festzuhalten ist, dass diese Bestimmungen zunächst nur dazu führen, dass diese Dienste ihre Schnittstellen für Interoperabilität öffnen müssen (bspw. WhatsApp für Signal oder Telegram). Dass auch

428 Bericht der Kommission an den Rat und das Europäische Parlament, Endgültiger Bericht – Sektoruntersuchung zum Internet der Dinge für Verbraucher, COM(2022) 19 final, https://competition-policy.ec.europa.eu/system/files/2022-01/internet-of-things_final_report_2022_de.pdf.

429 COM(2022) 19 final (Fn. 428), Rn. 17.

Drittanbieter untereinander operabel sein müssen (bspw. Signal für Telegram und umgekehrt) bedeuten sie nicht. Das könnte sich lediglich als Folge entwickelter Schnittstellen und Standards ergeben, ist aber gesetzlich nicht vorgeschrieben.

(b) Einhaltung der Verpflichtungen durch Torwächter (Art. 8 DMA)

Art. 8 DMA enthält Bestimmungen dazu, wie die Verpflichtungen der Art. 5 bis 7 DMA von den Torwächtern einzuhalten sind, und sieht verschiedene Wege vor, darauf (nach-)steuernd einzuwirken. Für die Umsetzung und letztlich auch Effektivität der Regeln ist die Bestimmung besonders wichtig.

Abs. 1 statuiert zunächst eine Nachweispflicht auf Seiten der Gatekeeper, die die Maßnahmen, die sie in Umsetzung des DMA ergreifen, dokumentieren müssen. Zwar hat die Kommission auch Untersuchungsbefugnisse, jedoch sind diese von Ermittlungen abhängig, während die Nachweispflicht den Anbietern eine „Bringschuld" auferlegt. Von Bedeutung ist auch Abs. 3, wonach der Torwächter die Kommission ersuchen kann, die von ihm beabsichtigten Maßnahmen auf ihre Vereinbarkeit mit den „Do's" und „Dont's" zu überprüfen. Die Kommission entscheidet nach eigenem Ermessen und unter Wahrung der Grundsätze der Gleichbehandlung, der Verhältnismäßigkeit und der guten Verwaltungspraxis über die Einleitung eines solchen Verfahrens. Das ist insbesondere für die Pflichten aus Art. 6 DMA relevant, die möglicherweise noch einer näheren Konkretisierung bedürfen. Es wird also die Möglichkeit eines Dialogs eröffnet, mit der die Kommission steuernd auf beabsichtigte Maßnahmen einwirken und daraus auch neue Erkenntnisse gewinnen kann.

Ein förmlicheres Verfahren sehen die Abs. 2, 5 und 6 vor. Die Kommission kann von Amts wegen oder auf Antrag des Torwächters ein Verfahren nach Art. 20 DMA einleiten. Sie kann in diesem Rahmen Durchführungsrechtsakte erlassen, in denen die Maßnahmen festgelegt werden, die der betreffende Torwächter zu ergreifen hat, um den Verpflichtungen wirksam nachzukommen. Näheres dazu regeln Art. 46 und 50 DMA. Durchführungsrechtsakte können insbesondere Form, Inhalt und sonstige Einzelheiten der technischen Maßnahmen zur Umsetzung der Art. 5, 6 oder 7 DMA betreffen sowie die operativen und technischen Vorkehrungen im Hinblick auf die Umsetzung der Interoperabilität nach Art. 7 DMA. Das dabei zu beachtende Verfahren sieht eine Stellungnahme des Beratenden Ausschus-

ses für digitale Märkte vor, die die Kommission vor Erlass eines Durchführungsrechtsakts einzuholen hat. Der Ausschuss ist ein Beratungsgremium, in dem jeder Mitgliedstaat vertreten ist und dessen Delegation u. a. Sachverständige der zuständigen Behörden der Mitgliedstaaten umfassen kann, die über das einschlägige Fachwissen für die dem Ausschuss vorgelegten Fragen verfügen.[430] Damit hat auch die nationalen Ebene die Möglichkeit, auf die ausfüllungsbedürftigen Vorschriften des DMA mit Expertise aus praktischer Erfahrung einzuwirken.

Vor Erlass eines solchen Beschlusses gibt die Kommission dem Torwächter innerhalb von drei Monaten nach Einleitung des Verfahrens ihre vorläufige Beurteilung bekannt. In dieser vorläufigen Beurteilung erläutert die Kommission, welche Maßnahmen sie zu ergreifen beabsichtigt bzw. der betreffende Torwächter ihrer Ansicht nach ergreifen sollte, um der vorläufigen Beurteilung wirksam Rechnung zu tragen (Abs. 5). Um auch interessierten Dritten Gelegenheit zur Stellungnahme zu geben, veröffentlicht die Kommission bei Mitteilung ihrer vorläufigen Beurteilung eine nichtvertrauliche Zusammenfassung des Sachverhalts und der beabsichtigten Maßnahmen. Dadurch wird auch die Öffentlichkeit beteiligt.

Art. 8 Abs. 8 DMA sieht schließlich ein spezielles Verfahren für Art. 6 Abs. 11 und 12 DMA vor. Für die Zwecke der Festlegung der Verpflichtungen in Bezug auf einen fairen Zugang zu App-Stores, Online-Suchmaschinen und sozialen Netzwerken prüft die Kommission auch, ob die beabsichtigten bzw. durchgeführten Maßnahmen sicherstellen, dass kein Ungleichgewicht zwischen den Rechten und Pflichten der gewerblichen Nutzer besteht und dass die Maßnahmen dem Torwächter keinen Vorteil verschaffen, der in Anbetracht seiner Dienstleistung für die gewerblichen Nutzer unverhältnismäßig wäre. Für diese Bestimmung, die auch im Zusammenhang mit der Interoperabilität, wie oben gezeigt, besonders relevant ist, wird also eine gesonderte Prüfung angeordnet, die neben den sonstigen Befugnissen der Kommission steht.

(c) Aktualisierung der Verpflichtungen der Torwächter (Art. 12 DMA)

Art. 12 DMA ist eine weitere Besonderheit, die den DMA kennzeichnet. Der Kommission wird nach Abs. 1 die Befugnis übertragen, nach einer

430 Erwgr. 101 DMA.

Marktuntersuchung mit entsprechenden Ergebnissen delegierte Rechtsakte zu erlassen, um den DMA in Bezug auf die in den Art. 5 und 6 DMA festgelegten Verpflichtungen zu ergänzen. Die Ausgestaltung von Gesetzen durch verbindliche delegierte Rechtsakte wird von Art. 290 AEUV und der Rechtsprechung des EuGH[431] insoweit begrenzt, als es lediglich um eine „Ergänzung" des zugrunde liegenden Rechtsakts gehen darf, wesentliche Inhalte sich aber bereits aus dem demokratisch legitimierten Rechtsakt, hier also der Verordnung, selbst ergeben müssen.[432] Daher enthalten auch Art. 12 und 49 DMA entsprechende Beschränkungen. Insbesondere ist die Befugnis auf bestimmte, ausdrücklich in Abs. 2 genannte Bereiche beschränkt und betrifft u. a. die (genauere) Art und Weise, wie Torwächter ihre Pflichten erfüllen müssen, und eine Ausweitung von Pflichten auf weitere Dienste. Letzteres könnte auch Anknüpfungspunkt für eine Ausweitung von Interoperabilitäts- oder damit in Zusammenhang stehenden Vorschriften sein.

Ähnliches sehen Art. 12 Abs. 3 und 4 DMA auch für die Bestimmung des Art. 7 DMA vor. In delegierten Rechtsakten kann die Kommission die Liste grundlegender Funktionen (und damit die Reichweite der Interoperabilität) erweitern sowie die Art und Weise, wie sie umzusetzen sind, näher bestimmen.

Näheres zum Erlass delegierter Rechtsakte in diesem Sinne bestimmt Art. 49 DMA in Übereinstimmung mit den insoweit üblichen Verfahren. Neben einer Beteiligung des Europäischen Parlaments und Rates im förmlichen Verfahren sieht Art. 49 Abs. 4 DMA auch vor, dass die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen im Einklang mit den in der Interinstitutionellen Vereinbarung vom 13. April 2016[433] über eine bessere Rechtsetzung enthaltenen Grundsätzen zu konsultieren hat.

431 Vgl. etwa EuGH, C-286/14 – *Parlament / Kommission*, ECLI:EU:C:2016:183 – Rn. 41.

432 Kritisch zur Reichweite der Befugnis zu delegierten Rechtsakten im DMA *Ukrow*, Die Vorschläge der EU-Kommission für einen Digital Services Act und einen Digital Markets Act, S. 16 ff.; *Podszun/Bongartz/Langenstein*, in: EuCML, 2021, S. 60, 65.

433 Interinstitutionelle Vereinbarung zwischen dem Europäischen Parlament, dem Rat der Europäischen Union und der Europäischen Kommission über bessere Rechtsetzung, EU ABl. L 123/1, S. 1–14.

(d) Überwachung und Durchsetzung des DMA

In Kapitel IV des DMA steht der Kommission ein umfassendes Instrumentarium an Marktuntersuchungsbefugnissen zur Verfügung. Diese Befugnisse umfassen die Benennung von Torwächtern, Untersuchungen bei systematischer Nichteinhaltung des DMA und, vor allem, die Ermittlung, ob der DMA auf neue Dienste und neue Praktiken zu erstrecken ist. Dazu gehört, ob ein oder mehrere Dienste des digitalen Sektors in die Liste der zentralen Plattformdienste neu aufgenommen werden sollten, oder die Frage, ob es Praktiken gibt, die die Bestreitbarkeit zentraler Plattformdienste beschränken oder unfair sind und denen durch den DMA (noch) nicht wirksam begegnet wird. Ergebnisse dieser Ermittlung können dann, wie eben erwähnt, steuernd in einen delegierten Rechtsakt überführt werden.

Darüber hinaus regelt Kapitel V Untersuchungs-, Durchsetzungs- und Überwachungsbefugnisse. Diese reichen von Auskunfts-, Informations- und Nachprüfungsbefugnissen über einstweilige Maßnahmen und Verpflichtungszusagen der Gatekeeper bis hin zu Maßnahmen bei Nichteinhaltung. Bei Nichteinhaltung der Vorschriften riskiert ein Torwächter Geldbußen bis zu einem Höchstbetrag von 10 % seines weltweit erzielten Gesamtumsatzes, mögliche Geldbußen in Höhe von bis zu 20 % seines weltweit erzielten Gesamtumsatzes bei wiederholter Zuwiderhandlung, Zwangsgelder bis zu einem Höchstbetrag von 5 % seines durchschnittlichen Tagesumsatzes oder sogar nicht finanzielle strukturelle Abhilfemaßnahmen wie den Abverkauf von Teilen des Unternehmens als letztes Mittel bei systematischer Nichteinhaltung.

Die Europäische Kommission ist alleinige Durchsetzungsbehörde im DMA. Regeln zur Zusammenarbeit mit nationalen Behörden, insbesondere den zuständigen nationalen Wettbewerbsbehörden, finden sich in Art. 37 und 38 DMA. Die Rolle, die nationale Wettbewerbsbehörden innerhalb des DMA spielen, ist jedoch limitiert.[434] Hervorhebenswert ist auch, dass die Kommission von einem „Beratenden Ausschuss" (Art. 50 DMA) sowie einer „High Level Expert Group (HLEG)" beratend unterstützt wird. Diese HLEG ist in Art. 40 DMA näher konkretisiert. Im Einklang mit den dortigen Bestimmungen ist sie im März 2023 bestehend aus Vertretern des Gre-

434 Vgl. dazu aber *Hartmann-Rüppel/Horn*, The Digital Markets Act – how it will impact national competition authorities?, die auf verschiedene Beteiligungsmöglichkeiten hinweisen, die jedoch wiederum maßgeblich von einer entsprechenden Initiative der Kommission abhängen.

miums der europäischen Regulierungsbehörden für elektronische Kommunikation (GEREK), des Europäischen Datenschutzbeauftragten (EDPS) und des Europäischen Datenschutzausschusses (EDSA), des Europäischen Wettbewerbsnetzwerks (ECN), des Consumer Protection Cooperation Network (Verbraucherschutz-Zusammenarbeits-Netzwerk, CPC Network) und der European Regulators Group for Audiovisual Media Services (ERGA) eingerichtet worden.[435] Die HLEG soll die Kommission in allen mit dem DMA zusammenhängenden Aktivitäten beraten und bestehende Expertise in den Rechtsdurchsetzungsprozess mit einbringen.

Neben ihren Aufsichts- und Rechtsdurchsetzungsbefugnissen kann die Kommission auch Leitlinien herausgeben (Art. 47 DMA) sowie, soweit angemessen und erforderlich, die europäischen Normungsgremien beauftragen, die Umsetzung der im DMA festgelegten Verpflichtungen durch die Entwicklung geeigneter Normen zu erleichtern (Art. 48 DMA). Beides dürfte vor allem im Zusammenhang mit solchen Interoperabilitätsvorschriften besonders relevant sein, die technische Systeme zur Schnittstellenöffnung erfordern. In Bezug auf die Entwicklung von Standards dürfte dabei auch die Arbeit der HLEG zur Europäischen Standardisierung von Interesse sein.[436]

Möglichkeiten der privaten Rechtsdurchsetzung, insbesondere etwa durch gewerbliche Nutzer oder Endnutzer, sieht der DMA nicht vor. Denkbar ist es allerdings, die Grundsätze der privaten Durchsetzung aus dem EU-Wettbewerbsrecht auch auf den DMA anzuwenden.[437] Verschieden Autoren leiten die grundsätzliche Möglichkeit, dass der DMA auch durch private Parteien durchsetzbar sein muss, unmittelbar aus der Vorschrift zur Zusammenarbeit mit nationalen Gerichten ab.[438] Wenn die Bestimmungen der Art. 5 und 6 DMA als hinreichend konkret angenommen werden – dabei dürfte ein Unterschied zwischen den „direkten" Pflichten des Art. 5 DMA und den „zu konkretisierenden" Pflichten des Art. 6 DMA zu machen sein –, wäre eine Durchsetzung auf nationaler Ebene in einem zivilrechtlichen Verfahren (etwa in Anknüpfung an die Anspruchsgrundlage des § 194

435 Commission Decision of 23.3.2023 on setting up the High-Level Group for the Digital Markets Act, C(2023) 1833 final, https://competition-policy.ec.europa.eu/system/files/2023-03/High_Level_Group_on_the_DMA_0.pdf.

436 Commission decision C(2022) 6189 of 1.9.2022 setting up the group of experts 'High-Level Forum on European Standardisation'.

437 So etwa *Wielsch*, in: MKDS, Art. 5 Rn. 37 ff.; ebenfalls *Herbers*, in: Podszun, Art. 6 Rn. 104.

438 *Lahme/Ruster*, in: Podszun, Art. 39 Rn. 8 ff. m. w. N.

BGB) oder in einem wettbewerbsrechtlichen Verfahren (etwa in Anknüpfung an § 3a UWG) grundsätzlich möglich. Seit der 11. GWB-Novelle erstrecken sich die Beseitigungs-, Unterlassungs- und Schadensersatzansprüche auch auf Verstöße gegen den DMA, sind aber von der Feststellung eines Verstoßes abhängig und auf Mitbewerber und Marktteilnehmer beschränkt.[439]

3. Deutschland

a. Gesetz gegen Wettbewerbsbeschränkungen

(1) Einleitender Überblick zu den GWB-Novellen 2017, 2021 und 2023

Im Kontext der vorliegenden Studie ist auf nationaler Ebene das Gesetz gegen Wettbewerbsbeschränkungen (GWB)[440] vor allem hinsichtlich der jüngsten und umfassenden Novellen zu betrachten, die daher vorab im Überblick vorgestellt werden.

Das „Zeitalter der Digitalisierung" im Wettbewerbsrecht wurde mit der 9. GWB-Novelle eingeleitet, die vor allem auf internet- und datenbasierte Geschäftsmodelle reagierte und im Juni 2017 in Kraft trat.[441] Wesentliche Punkte waren die Ergänzung der Kriterien zur Annahme einer marktbeherrschenden Stellung, die mit den neuen §§ 18 Abs. 2a und 3a Besonderheiten bei Digitalkonzernen aufgriffen. Insbesondere wurde festgelegt, dass die Unentgeltlichkeit angebotener Leistungen – wie bei daten- und werbefinanzierten Geschäftsmodellen – nicht unerheblich für die Marktbestimmung ist, und ergänzend wurden neue Kriterien für die Bewertung von Marktmacht bei mehrseitigen Märkten und Netzwerken eingeführt. Andererseits betraf die Novelle Änderungen bei der Fusionskontrolle in Form von Anpassungen der Schwellenwerte, die auch dann im Gegensatz zur vorherigen Regelung eine Kontrolle von Zusammenschlüssen ermöglichen sollten, wenn Umsatzschwellen nicht erreicht werden. Diese Änderung ist eine Reaktion darauf, dass nach der früheren Regelung Start-ups durch etablierte Unternehmen übernommen werden konnten, ohne dass

439 Dazu unten C.II.3.b(2).

440 Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bekanntmachung vom 26. Juni 2013 (BGBl. I S. 1750, 3245), das zuletzt durch Art. 1 des Gesetzes vom 25. Oktober 2023 (BGBl. 2023 I Nr. 294) geändert worden ist.

441 Gesetz vom 01.06.2017 – BGBl. I 2017, Nr. 33 vom 08.06.2017, S. 1416.

eine Kontrolle durch die Kartellbehörden erfolgen und damit möglichen Marktbehinderungen durch die etablierten Unternehmen in Form der Verhinderung der Entstehung potenter Wettbewerber („killer acquisitions") begegnet werden konnte.

Der Koalitionsvertrag zwischen CDU/CSU und SPD sah bereits im März 2018 erneut Handlungsbedarf im Wettbewerbsrecht vor allem im Zusammenhang mit der Marktmacht von Digitalkonzernen.[442] Auf dieser Grundlage wurden zwei umfangreiche Gutachten erstellt, um den Bedarf näher zu analysieren. Das für das BMWi erstellte Gutachten „Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen"[443] und der Bericht „Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft"[444] der Wettbewerbskommission 4.0 sprachen jeweils Handlungsempfehlungen aus. Die notwendige Reform zur Umsetzung der ECNplus-Richtlinie[445] der EU wurde daher zum Anlass genommen, auch Ergebnisse aus diesen Untersuchungen aufzugreifen. Im Januar 2021 trat die 10. GWB-Novelle, das „Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer wettbewerbsrechtlicher Bestimmungen" oder auch „GWB-Digitalisierungsgesetz"[446] in Kraft. Damit verbunden waren wesentliche Änderungen für den Wettbewerbsschutz in der Digitalwirtschaft und insbesondere eine Modernisierung der Missbrauchsaufsicht. Neben Änderungen im Fusionskontrollrecht und der Umsetzung der ECNplus-Richtlinie betrifft das vor allem die Einführung von § 19a GWB, die auch im Kontext von Interoperabilität Bedeutung erlangen kann.

Diese Bestimmung adressiert „[m]issbräuchliches Verhalten von Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb" und gibt dem Bundeskartellamt (BKartA) erstmals frühzeitige Eingriffsbefugnisse, auch im Sinne von vorbeugenden Untersagungen und speziellen Befugnissen gegen das Kippen eines Marktes („market tipping").

442 Siehe dazu *Körber*, MMR, 2020, S. 290, 290.

443 *Kommission Wettbewerbsrecht 4.0*, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft.

444 *Schweitzer/Haucap/Kerber/Welker*, Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen.

445 Richtlinie (EU) 2019/1 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 zur Stärkung der Wettbewerbsbehörden der Mitgliedstaaten im Hinblick auf eine wirksamere Durchsetzung der Wettbewerbsvorschriften und zur Gewährleistung des reibungslosen Funktionierens des Binnenmarkts, EU ABl. L 11, 14.1.2019, S. 3–33.

446 Gesetz vom 18.01.2021 – BGBl. I 2021, Nr. 1 vom 18.01.2021, S. 2.

Aufgegriffen werden darin Gefahren der Digitallandschaft, wie z. B. Selbstpräferenzierung und Datenvorteilen, die bereits Gegenstand (langwieriger) Verfahren auf nationaler und EU-Ebene waren. Um schneller und praktisch effektiv auf aktuelle Entwicklungen in diesem Umfeld reagieren zu können, führte die 10. GWB-Novelle auch Verkürzungen des Rechtswegs ein – Beschwerden gegen § 19a-Entscheidungen des BKartA werden direkt vom BGH entschieden –, und die Voraussetzungen für einstweilige Maßnahmen wurden gesenkt. Begriffe und Gehalt verschiedener bereits existierender Bestimmungen – z. B. zur Marktmachtbestimmung – wurden vor dem Hintergrund besonderer Herausforderungen im digitalen Raum konkretisiert und aktualisiert.

Durch das Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen und anderer Gesetze vom 25. Oktober 2023[447] ist das GWB nur zwei Jahre später erneut novelliert worden. Im Zentrum dieser 11. GWB-Novelle standen einerseits neue Möglichkeiten für das BKartA in Form von Abhilfemaßnahmen, innerhalb derer – nach einer umfassenden Sektoruntersuchung – eine erhebliche und dauerhafte Störung des Wettbewerbs festgestellt und darauf basierend gegenüber einem Unternehmen die Beseitigung dieser Störung oder sogar als Ultima Ratio eine Entflechtung angeordnet werden kann. Diese von manchen als deutscher „Sonderweg"[448] bezeichnete Durchsetzungslösung, die es in anderen Staaten in dieser konkreten Form nicht gibt,[449] wurde im Rahmen des Gesetzgebungsverfahrens sehr kontrovers diskutiert.[450] Während einige die Klarheit der Regeln bemängelten und insbesondere die Reichweite des Begriffs der Wettbewerbsstörung oder die dem BKartA dadurch entstehenden „Designbefugnisse" des Marktes kritisierten, betrachteten andere dies als wichtigen und richtigen Schritt zur Belebung des Wettbewerbs und zur Flexibilisierung der Aufsicht. Andererseits wurde mit der Änderung die Durchsetzung des DMA durch einen neu eingefügten § 32g gestärkt, der es dem BKartA

447 BGBl. 2023 I Nr. 294 vom 06.11.2023.

448 Vgl. *Boettcher*, Stellungnahme zu BT-Drucksache 20/6824, https://www.bundestag.de/resource/blob/952840/9cb54a27c24b76932657549832e359ed/20-9-267_Stellungnahme-Dr-Boettcher.pdf.

449 Parallelen bestehen aber zu den Befugnissen der Wettbewerbsbehörde des Vereinigten Königreichs, die ebenfalls auf der Basis einer Untersuchung Abhilfemaßnahmen ergreifen kann.

450 Vgl. hierzu die Stellungnahmen von Fachexperten im Rahmen der öffentlichen Anhörung des Wirtschaftsausschusses am 14. Juni 2023, abrufbar unter https://www.bundestag.de/dokumente/textarchiv/2023/kw24-pa-wirtschaft-11-gwb-novelle-951258.

ermöglicht, Verstöße gegen die Art. 5–7 DMA zu untersuchen und so die Kommission als alleinig zuständige Durchsetzungsbehörde im DMA zu unterstützen.

Diese Novellen dienten der Anpassung des Wettbewerbsrechts an die Bedingungen der Online-Umgebung sowie einer Anbindung bzw. Anpassung an die Vorgaben der EU-Ebene.

(2) Marktbeherrschung und verbotenes Verhalten (§§ 18–20 GWB)

(a) Marktbeherrschung

Zentrale Vorschrift ist § 18 GWB, der die Voraussetzungen zur Feststellung einer Marktbeherrschung regelt. Anders als im AEUV ist im GWB die marktbeherrschende Stellung näher umschrieben.

Abs. 1 legt dazu die allgemeine Definition in dem Sinne fest, dass ein Unternehmen marktbeherrschend ist, soweit es als Anbieter oder Nachfrager einer bestimmten Art von Waren oder gewerblichen Leistungen auf dem sachlich und räumlich relevanten Markt entweder ohne Wettbewerber ist oder keinem wesentlichen Wettbewerb ausgesetzt ist oder eine im Verhältnis zu seinen Wettbewerbern überragende Marktstellung hat. § 20 GWB erweitert bestimmte Missbrauchstatbestände auch auf Unternehmen mit relativer oder überlegener Marktmacht. Hieraus ergibt sich bereits ein wesentlicher Unterschied zum EU-Recht: Während die Kommission Machtmissbräuchen erst dann entgegentreten kann, wenn sie von allein oder kollektiv marktbeherrschenden Unternehmen ausgehen, setzt das deutsche Recht in § 20 GWB bereits im Vorfeld der Marktbeherrschung an und erfasst auch Unternehmen mit relativer Marktmacht, d. h. solche, die zwar nicht über eine absolute, den ganzen Markt betreffende Machtstellung verfügen, von denen aber andere Unternehmen abhängig sind.[451]

Im Hinblick auf die Bestimmung des Marktes, insbesondere bezüglich der Herausforderungen in den Strukturen der Online-Umgebung, gilt im Wesentlichen bereits das oben zur EU-Ebene Erläuterte. Wichtig ist allerdings, dass nach Abs. 3 der räumlich relevante Markt weiter sein kann als der Geltungsbereich des GWB, der Markt sich also auch über Deutschland hinaus erstrecken kann. Zudem spielt es für die Bestimmung des Marktes

451 *Körber*, in: MMR, 2020, S. 290, 291.

nach Abs. 2a keine Rolle, ob eine Leistung unentgeltlich erbracht wird, was gerade bei mehrseitigen Märkten, vor allem also Netzwerkverflechtungen im Internet, die häufig auf unentgeltlicher, aber datenbasierter Nutzung beruhen, besonders bedeutsam ist.[452]

Im nationalen und medienrechtlichen Kontext ist zudem zu erwähnen, dass es bei Fernsehen und Hörfunk (mit Ausnahme von Pay-TV) nach der Praxis des BKartA keinen Zuschauermarkt gibt, sondern lediglich einen Werbemarkt. Dieser Werbemarkt ist aber bislang je nach Medium ein separat zu betrachtender Markt (Fernsehwerbemarkt, Online-Werbemarkt, Hörfunkwerbemarkt, Anzeigenmarkt bei der Presse), innerhalb dessen Anbieter nicht miteinander konkurrieren.[453] Diese Marktabgrenzung gilt gleichermaßen für werbetreibende Unternehmen wie für Medien, die die Werbung ausstrahlen. Anders als im Wettbewerbsrecht findet sich im Medienrecht (z. B. in der AVMD-Richtlinie) dagegen eine Anerkennung der Konkurrenz bspw. von Online-Medien und Fernsehen um Zuschauer und Werbetreibende, und es werden daher auch Angleichungen im Rechtsrahmen geschaffen, um ein Level-Playing-Field zu erreichen.[454] Im Bereich der Presse wird zwischen Lesermarkt und Anzeigenmarkt unterschieden, wobei sich letzterer wiederum je nach Art der Presseveröffentlichung z. B. bei Fachzeitschriften, Zeitungen, Publikumszeitschriften etc. unterscheidet und auch räumlich (in Bezug auf das Verbreitungsgebiet) sowie zeitlich (Tageszeitungen, Wochenzeitungen etc.) zu untergliedern ist.[455] Eine bereichsübergreifende Berücksichtigung wettbewerbsrechtlicher Problematiken ist insofern also schon innerhalb der bzw. zwischen den „klassischen" Medien sowie bei Verflechtungen zu „neuen" Medien und Vermittlungsdiensten schwierig. Eine Durchbrechung erfolgt nur teilweise innerhalb des Kriteriums der Marktbeherrschung.

Im Hinblick auf die Bestimmung der marktbeherrschenden Stellung sieht das GWB, ebenfalls anders als der AEUV, Kriterien vor, die dabei „insbesondere" zu berücksichtigen sind. Das sind nach Abs. 3 zunächst herkömmliche Kriterien wie Marktanteil, Finanzkraft oder Verflechtungen, aber auch seit der 10. GWB-Novelle der Zugang zu wettbewerbsrelevan-

452 Dazu *Paal*, in: Gersdorf/Paal, § 18 Rn. 4 f.

453 Eingehend *Kühnen*, in: LMRKM, § 18 Rn. 45 f. m. w. N.

454 So ausdrücklich etwa Erwgr. 4 der Richtlinie (EU) 2018/1808 mit der Feststellung, dass Video-Sharing-Plattformen (im Wettbewerbsrecht: Online-Werbemarkt) „um das gleiche Publikum und um die gleichen Einnahmen wie die audiovisuellen Mediendienste konkurrieren" (im Wettbewerbsrecht: Fernsehwerbemarkt).

455 *Kühnen*, in: LMRKM, § 18 Rn. 42 f. m. w. N.

ten Daten. Eine Vermutung für die Marktbeherrschung gilt nach Abs. 4 bei einem Marktanteil von mind. 40 %. Für die gemeinsame Marktbeherrschung mehrerer Unternehmen gelten die Abs. 5 bis 7. Bedeutsamer im vorliegenden Kontext sind die mit der 9. bzw. 10. GWB-Novelle eingefügten Abs. 3a und 3b, die neben Abs. 1 treten, diesen aber nicht ersetzen.[456] Diese Vorschriften sprechen Marktmachtstrukturen an, die auch im Zusammenhang mit (fehlender) Interoperabilität als problematisch angesehen werden.

§ 18 Abs. 3a GWB nennt Faktoren, die bei der Betrachtung mehrseitiger Märkte und Netzwerke zu berücksichtigen sind: direkte und indirekte Netzwerkeffekte, die parallele Nutzung mehrerer Dienste und der Wechselaufwand für die Nutzer, seine Größenvorteile im Zusammenhang mit Netzwerkeffekten, der Zugang zu wettbewerbsrelevanten Daten und der innovationsgetriebene Wettbewerbsdruck. Das ist nach dem Willen des Gesetzgebers insgesamt auf die Bewertung der Marktbeherrschung in der Digitalwirtschaft zu erstrecken, selbst wenn im Einzelfall kein mehrseitiger Markt festgestellt wird.[457] Solche Kriterien wurden bereits in der Entscheidungspraxis des BKartA entlang der allgemeinen Kriterien nach Abs. 3 berücksichtigt, wie unten anhand ausgewählter Entscheidungen gezeigt wird. In der Gesetzesbegründung zur Einführung dieser Kriterien finden sich nunmehr die relevanten Aspekte, die bereits oben bei der wettbewerbsrechtlichen Berücksichtigungsmöglichkeit auf EU-Ebene benannt wurden: Lock-in-Effekte, Multi-Homing, Markt-Tipping und Big Data.[458] Ein Abstellen auf die Interoperabilität von Diensten solcher Unternehmen oder deren Fehlen findet sich allerdings weder unmittelbar im Gesetz noch in der Begründung, jedenfalls nicht als Kriterium zur Beurteilung der marktbeherrschenden Stellung.

§ 18 Abs. 3b GWB bestimmt darüber hinaus, dass bei der Bewertung der Marktstellung eines Unternehmens, das als Vermittler auf mehrseitigen Märkten tätig ist, insbesondere auch die Bedeutung der von ihm erbrachten Vermittlungsdienstleistungen für den Zugang zu Beschaffungs- und Absatzmärkten zu berücksichtigen ist. Die Bestimmung etabliert das Konzept der sog. „Intermediationsmacht“[459] und trägt somit der wachsenden Bedeutung von Vermittlungsdiensten als Tor zu Inhalten, Dienstleistungen und Produkten Rechnung – ein Ansatz, auf dem auch der DMA basiert. Insoweit

456 *Paal*, in: Gersdorf/Paal, § 18 Rn. 8a m. w. N.
457 Regierungsentwurf, BT-Drs. 18/10207, S. 48.
458 Regierungsentwurf, BT-Drs. 18/10207; vgl. eingehend *Paal*, in: Gersdorf/Paal, § 18 Rn. 11 ff.
459 *Paal*, in: Gersdorf/Paal, § 18 Rn. 16.

kann das BKartA eine Marktmacht auch unabhängig von Marktanteilen auf einem spezifischen Markt darauf stützen, dass ein Unternehmen wesentliches Zugangstor für dritte Dienste ist. Das ist in gewisser Weise durchaus vergleichbar mit einer Meinungsmacht, wie sie im medienrechtlichen Kontext eine Rolle spielt, wenn es bei diesen Leistungen um mediale oder meinungsbildungsrelevante Inhalte geht.

Der mit der 9. GWB-Novelle (2017) eingeführte § 18 Abs. 8 GWB sieht für die Novellierungen des Gesetzes jeweils eine Evaluierung innerhalb von drei Jahren vor. Das Bundesministerium für Wirtschaft und Energie (nunmehr: Klimaschutz) soll den gesetzgebenden Körperschaften nach Ablauf von drei Jahren nach Inkrafttreten der Regelungen in den Abs. 2a und 3a über die Erfahrungen mit den Vorschriften berichten. Ein solcher Bericht steht allerdings noch aus, wobei die aus dem BMWK stammenden Entwürfe für weitere Novellen des GWB den Anpassungsbedarf bereits zum Ausdruck gebracht haben.

(b)Verbotenes Verhalten

Nach der Feststellung einer Marktbeherrschung unterliegen Unternehmen dem Missbrauchsverbot nach § 19 GWB sowie der Zusammenschlusskontrolle. Ein Kausalzusammenhang zwischen der Marktbeherrschung und dem missbilligten Verhalten (Verhaltenskausalität) muss nicht vorliegen. Vielmehr genügt eine Ergebniskausalität in dem Sinne, dass die Marktbeherrschung für das Marktergebnis kausal ist.[460] Ähnlich wie im AEUV legt Abs. 1 das Missbrauchsverbot fest, während Abs. 2 Regelbeispiele für verbotene Verhaltensweisen aufstellt. Für Interoperabilitätserwägungen mittelbar relevant, nämlich in Bezug auf die faire Ausgestaltung von interoperablen Systemen, sind neben dem allgemeineren Behinderungstatbestand in Nr. 1 die Nr. 2 (Fordern von Entgelten oder sonstigen Geschäftsbedingungen, die von denjenigen abweichen, die sich bei wirksamem Wettbewerb mit hoher Wahrscheinlichkeit ergeben würden) und Nr. 3 (Fordern ungünstigerer Entgelte oder sonstiger Geschäftsbedingungen, als sie das marktbeherrschende Unternehmen selbst auf vergleichbaren Märkten von gleichartigen Abnehmern fordert) relevant. Insoweit bestehen ebenfalls Parallelen zu den oben dargestellten Fallgestaltungen auf EU-Ebene.

Nr. 4 hingegen bestimmt, dass es eine verbotene Verhaltensweise darstellt, wenn sich ein marktbeherrschendes Unternehmen weigert, ein ande-

460 BGH, Urteil vom 23. Juni 2020, KVR 69/19 – Facebook. Kritisch dazu *Körber,* in: MMR, 2020, S. 290, 291.

res Unternehmen gegen angemessenes Entgelt mit einer Ware oder gewerblichen Leistung zu beliefern, insbesondere ihm Zugang zu Daten, zu Netzen oder anderen Infrastruktureinrichtungen zu gewähren, und die Belieferung oder die Gewährung des Zugangs objektiv notwendig ist, um auf einem vor- oder nachgelagerten Markt tätig zu sein, und wenn diese Weigerung den wirksamen Wettbewerb auf diesem Markt auszuschalten droht. Das steht unter der Ausnahme einer sachlichen Rechtfertigung für eine solche Verweigerung. Abs. 4 beschreibt die „essential facilities doctrine", die oben bereits erläutert wurde,[461] und wurde durch die 10. GWB-Novelle neu gefasst. Mit dieser Änderung wurde klargestellt, dass eine missbräuchliche Zugangsverweigerung nicht nur bei physischer Infrastruktur in Betracht kommt, sondern auch in einer Verweigerung des Zugangs zu Daten, Netzen oder anderen Infrastruktureinrichtungen bestehen kann, was der Rechtsanwendungspraxis auf EU-Ebene Rechnung trägt.[462] Ein solches Verhalten kann auch in der Verweigerung immaterialgüterrechtlicher Lizenzen liegen. Nach der Gesetzesbegründung sollte es vor allem um Fälle gehen, in denen ein marktbeherrschendes Unternehmen den Zugang zu den Nutzungsdaten einer bestimmten Person oder Maschine kontrolliert und ein anderes Unternehmen Zugang zu den individualisierten Nutzungsdaten benötigt, bspw. um Zusatzdienste anbieten zu können (Wartung, Reparatur oder innovatives komplementäres Angebot), oder ein Unternehmen Zugang zu den aggregierten Nutzungsdaten einer Vielzahl von Nutzern/Maschinen begehrt, etwa um Störungen einer Maschine oder Nutzerbedürfnisse besser vorhersagen zu können.[463] Datenschutzrechtliche Anforderungen bleiben davon unberührt; insbesondere ist weiterhin eine Rechtsgrundlage hierfür nötig. Auch wird weiterhin verlangt, dass es um eine „wesentliche Einrichtung" geht, was zuvor bspw. Unternehmen wie Energieversorger erfasste. Die Ausweitung auf digitale Prozesse bedeutet daher nicht, dass bspw. Nutzerdaten von Google oder Meta per se unter diese Bestimmung fallen, sondern erfordert eine sorgfältige Analyse einer die Wesentlichkeit begründenden Datenmacht.[464] Die Formulierung „gegen ein angemessenes Entgelt" ist dabei nicht so zu verstehen, dass eine von Nr. 4 beabsichtigte Zugangsöffnung immer unter der Bedingung eines Entgelts stehen muss,

461 Eingehend im Zusammenhang mit dem Fall RTE/IPTV oben C.II.2.a(2)(e).
462 *Paal*, in: Gersdorf/Paal, § 19 Rn. 7.
463 Regierungsentwurf, BT-Drs. 19/23492, S. 72.
464 *Körber*, in: MMR, 2020, S. 290, 292, mit Verweis auf KOM 11.3.2008, M.4731 – *Google/DoubleClick*, Rn. 364 ff.

denn je nach Fallgestaltung kann eine unentgeltliche Zugangsöffnung gerade geboten sein.[465] Obwohl in dieser Vorschrift – anders als in § 19a GWB – Interoperabilität nicht explizit angesprochen wird, bildet die Konstellation bewusst[466] diejenigen Fälle ab, die auf EU-Ebene in einen Zusammenhang mit Interoperabilität gesetzt wurden.

(3) Missbräuchliches Verhalten von Unternehmen mit überragender marktübergreifender Bedeutung (§ 19a GWB)

(a) Überblick und Zielsetzung

§ 19a GWB wurde mit der 10. GWB-Novelle ins Gesetz eingefügt und etabliert eine besondere Missbrauchsaufsicht, die dem BKartA eine effektivere Kontrolle über große Digitalkonzerne ermöglichen soll.[467] Die bisherigen Befugnisse, die an eine auf Einzelmärkten bereits vorliegende Marktbeherrschung und daraus entstehende Verhaltensspielräume anknüpfen, wurden als nicht mehr ausreichend angesehen, um Gefahren im digitalen Raum (Netzwerkeffekte, Datenvorteile und damit verbundene Selbstverstärkungseffekte, Größen- und Ressourcenvorteile) zu begegnen.[468] Daher erfolgt durch § 19a Abs. 1 GWB eine marktübergreifende Betrachtung der Positionierung eines Unternehmens, die mit der Feststellung einer überragenden marktübergreifenden Bedeutung durch das BKartA enden kann. Solche Feststellungsverfügungen hat das BKartA seit Inkrafttreten der Regelung bereits in einigen Fällen, etwa bezüglich Amazon, Meta und Apple, getroffen.[469]

Abs. 2 listet abschließend Missbrauchstatbestände auf, die nach Auffassung des Gesetzgebers mit einem hohen wettbewerblichen Schädigungspo-

465 Regierungsentwurf, BT-Drs. 19/23492, S. 72, stellt klar, dass die Formulierung nur der Klarstellung diene, dass es solche Fälle geben könne. Für eine möglicherweise unentgeltliche Zugangsgewährung wird hier der Fall des Zugangs auf wettbewerbsrelevante Daten beispielhaft genannt.

466 Im Regierungsentwurf, BT-Drs. 19/23492, S. 72 f., wird mehrfach darauf hingewiesen, dass mit der Änderung der Nr. 4 eine Anpassung an die Prioritäten und die Rechtspraxis der Kommission bezüglich Art. 102 AEUV erfolgen sollte.

467 Dazu eingehend und auch kritisch zur Reichweite *Körber*, MMR, 2020, S. 290, 290 f.; ebenso *Paal*, in: Gersdorf/Paal, § 19a Rn. 5 m. w. N. auch mit Blick auf die Verfassungskonformität von § 19a GWB.

468 Regierungsentwurf, BT-Drs. 19/23492, S. 73.

469 Dazu unten C.II.3.b(3)(e).

tenzial verbunden sind und daher der speziellen und flexibleren Norm des § 19a GWB unterliegen. Abs. 4 enthält eine Evaluierungspflicht, wonach das BMWK den gesetzgebenden Körperschaften nach Ablauf von vier Jahren nach Inkrafttreten über die Erfahrungen mit der Norm zu berichten hat.

(b) Feststellung der überragenden marktübergreifenden Bedeutung

§ 19a Abs. 1 GWB normiert die Kriterien, aufgrund derer das BKartA die überragende marktübergreifende Bedeutung eines Unternehmens feststellen kann. Das erfordert eine Gesamtwürdigung aller im Einzelfall relevanten Umstände und belässt der Behörde einen Ermessensspielraum. Erforderlich ist zunächst, dass ein Unternehmen in erheblichem Umfang auf Märkten im Sinne des § 18 Abs. 3a GWB tätig ist. Die Norm betrifft also mehrseitige Märkte oder Netzwerke. Satz 2 der Bestimmung nennt nicht abschließende („insbesondere") Kriterien, die dabei zu berücksichtigen sind: marktbeherrschende Stellung auf einem oder mehreren Märkten, Finanzkraft oder Zugang zu sonstigen Ressourcen, vertikale Integration und Tätigkeit auf verbundenen Märkten, Zugang zu wettbewerbsrelevanten Daten und Bedeutung der Tätigkeit für den Zugang Dritter zu Beschaffungs- und Absatzmärkten sowie der damit verbundene Einfluss auf die Geschäftstätigkeit Dritter (Intermediationsmacht).

Damit bestehen zwar Parallelen zur Marktmacht nach § 18 GWB, insbesondere ist es auch dort (anders als auf EU-Ebene) möglich, gegen ein Unternehmen mit nur relativer Marktmacht vorzugehen. Allerdings sind die Begriffe nicht gleichbedeutend, betreffen insbesondere nicht eine absolute Beherrschung eines bestimmten Marktes, sondern eher die strategische Positionierung des Unternehmens und sein Agieren im (übergreifenden) Gesamtmarkt. Ebenso wie der DMA geht es nach der Gesetzesbegründung darum, das Vorliegen einer Gatekeeper-Funktion zu adressieren.[470]

(c) „Missbrauchstatbestände"

§ 19a Abs. 2 GWB listet abschließend sieben Tatbestände auf, die das BKartA einem Unternehmen mit der festgestellten überragenden marktübergreifenden Bedeutung untersagen kann, weil sie als besonders wettbe-

470 Regierungsentwurf, BT-Drs. 19/23492, S. 73.

werbsschädlich zu qualifizieren sind. Diese Liste zeigt erneut, dass § 19a GWB vor allem auf marktübergreifende schädliche Entwicklungen abzielt.

Nr. 1 bezeichnet die Selbstpräferenzierung als ein solches wettbewerbsschädigendes Verhalten. Damit bestehen wiederum Parallelen zur Fallpraxis der Kommission und zu Art. 6 Abs. 5 DMA.[471] Allerdings geht das GWB darüber hinaus. Untersagt werden kann das Verhalten eines Unternehmens, das beim Vermitteln des Zugangs zu Beschaffungs- und Absatzmärkten die eigenen Angebote gegenüber denen von Wettbewerbern bevorzugt behandelt, insbesondere wenn es die eigenen Angebote bei der Darstellung bevorzugt oder ausschließlich eigene Angebote auf Geräten vorinstalliert oder anders integriert. Damit reicht das GWB (verallgemeinernde Regel) weiter als die einzelfallbezogene Praxis der Kommission (Verbot in Ausnahmefällen) und hat gegenüber dem DMA (beschränkt auf zentrale Plattformdienste) einen umfassenderen Anwendungsbereich (Beschaffungs- und Absatzmärkte). Da diese Vorschrift insgesamt das Verhalten auf Märkten erfasst, auf denen Unternehmen Produkte und Dienstleistungen kaufen und verkaufen können, ist sie potenziell auch für den Mediensektor an verschiedenen Stellen, nicht nur in Bezug auf App-Stores, relevant.

Nr. 2 beschreibt Maßnahmen als wettbewerbsschädigend, die andere Unternehmen in ihrer Geschäftstätigkeit auf Beschaffungs- oder Absatzmärkten behindern, wenn die Tätigkeit des Unternehmens mit marktübergreifender Bedeutung für den Zugang zu diesen Märkten Bedeutung hat. Als Regelbeispiele hierfür beschreibt der Tatbestand die Vorinstallation oder Integration eigener Angebote und die Erschwerung oder Verhinderung des Zugangs zu Abnehmern oder deren Behinderung bei der Bewerbung ihrer Angebote. Auch insoweit bestehen Parallelen zur Fallpraxis der Kommission[472] und zum DMA[473], die Vorschrift geht aber wie bei Nr. 1 in der Reichweite (Ausnahme/Regel) und dem Anwendungsbereich (bestimmte zentrale Plattformdienste/Absatz- und Beschaffungsmärkte) darüber hinaus.

Nr. 3 beschreibt die Fallgestaltung des Aufrollens, in der ein Unternehmen zwar noch keine marktbeherrschende Stellung hat, seine Position aber schnell ausbauen und deshalb andere Unternehmen behindern kann (bspw. indem es das neue Angebot an ein bestehendes bindet oder davon abhängig macht und damit die Wahlmöglichkeiten der Nutzer einschränkt). Parallelen gibt es wiederum zum DMA, etwa in Bezug auf dort angesprochene

471 Vgl. bereits oben C.II.2.a(2)(c) und C.II.2.c(5).
472 Vgl. *Apple/Spotify*, oben C.II.2.a(2)(f).
473 Vgl. Art. 6 Abs. 3 und 4 DMA, oben C.II.2.c(3).

Wechsel zwischen Systemen und die Kopplungsverbote, die aber im DMA nicht explizit im Kontext des „Aufrollens" genannt werden.

Nr. 4 betrifft den Datenzugang. Anders als im DMA, der von Geschäftsnutzern oder deren Endkunden generierten Daten spricht, wird im GWB als wettbewerbsschädigend eingestuft, wenn „wettbewerbsrelevante" Daten verarbeitet werden oder Geschäftsbedingungen eine solche Verarbeitung zwingend vorsehen und dadurch Marktzutrittsschranken errichtet oder spürbar erhöht werden. Wie § 19a Abs. 2 Nr. 4 lit. a) GWB zeigt, geht es dabei einerseits um die dienstübergreifende Zusammenführung von Nutzerdaten (entsprechend Art. 5 Abs. 2 DMA) und andererseits nach lit. b) um die Ausgrenzung von Geschäftsnutzern bezüglich dieser Daten (entsprechend Art. 6 Abs. 10 DMA). An dieser Stelle ist das GWB aber enger, der Anwendungsbereich („wettbewerbsrelevante Daten") könnte als weniger umfangreich als allgemein generierte Daten verstanden werden. Auch wird nicht per se ein Datenzugang allgemein eingeräumt oder eine Cross-Nutzung von Daten insgesamt verboten.

Nr. 6 beschreibt es als wettbewerbsschädigende Verhaltensweise, andere Unternehmen unzureichend über den Umfang, die Qualität oder den Erfolg der erbrachten oder beauftragten Leistung zu informieren oder ihnen in anderer Weise eine Beurteilung des Werts dieser Leistung zu erschweren. In der Reichweite findet sich eine vergleichbare Vorschrift im DMA nicht, dieser regelt aber zumindest Ähnliches in Bezug auf die Transparenz von Online-Werbung. Kritisch wird gegen diese sehr weite Transparenzbestimmung vorgebracht, dass sie eher ein vertragsrechtliches als ein wettbewerbsrechtliches Problem beschreibt.[474]

Nach Nr. 7 soll das BKartA zudem untersagen können, dass für die Behandlung von Angeboten eines anderen Unternehmens Vorteile gefordert werden, die in keinem angemessenen Verhältnis zum Grund der Forderung stehen. Insbesondere gilt das für Fälle, in denen für die Darstellung eines Angebots eines Dritten oder deren Qualität die Übertragung von Daten oder Rechten gefordert wird, die nicht zwingend erforderlich oder unverhältnismäßig sind.

Während alle diese Regelungen mittelbare Relevanz für Interoperabilitätserwägungen entfalten können, weil sie entweder Teilaspekte oder deren Ausgestaltung betreffen, so wie es bereits für die entsprechenden Bestimmungen des DMA dargelegt wurde, spricht § 19a Abs. 2 Nr. 5 GWB Interoperabilität und Datenportabilität explizit an. Danach kann das BKartA

474 *Körber*, in: MMR, 2020, S. 290, 294.

einem Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb untersagen, die Interoperabilität von Produkten oder Leistungen oder die Portabilität von Daten zu verweigern oder zu erschweren und damit den Wettbewerb zu behindern. Anders als bei einigen anderen Tatbeständen der Liste in § 19a Abs. 2 ist die Wettbewerbsbehinderung bei dieser Nummer ein selbstständig zu prüfendes Merkmal.

Dieses Verbot soll verhindern, dass Unternehmen mit überragender marktübergreifender Bedeutung einen ungerechtfertigten Wettbewerbsvorteil erlangen, indem sie die Interoperabilität von Produkten oder Leistungen behindern. Insoweit geht es einerseits deutlich über die Bestimmungen des DMA hinaus, die auf bestimmte zentrale Plattformdienste (maßgeblich Betriebssysteme, App-Stores, teils virtuelle Assistenten und Messenger-Dienste) beschränkt sind. Ausweislich der Gesetzesbegründung ist Interoperabilität wegen der Zielsetzung der Verhinderung von Lock-in-Effekten weit zu verstehen, und die Vorschrift erfasst alle Maßnahmen, die verhindern, dass Produkte miteinander arbeiten bzw. interagieren können.[475] Fehlende Interoperabilität kann Grundlage für Lock-in-Effekte sein, denen die GWB-Novelle begegnen will.[476] Auch die Wettbewerbskommission 4.0 hatte sich im Vorfeld der 10. GWB-Novelle für ein Aufgreifen von Interoperabilität ausgesprochen. In deren Bericht wurde aber eine Verankerung auf EU-Ebene als sinnvoller angesehen.[477]

Andererseits enthält der DMA positive Pflichten von Gatekeepern, während § 19a GWB von einer Untersagung im Einzelfall bei Wettbewerbsbehinderung abhängt, also keine vorab für bestimmte Adressaten bestehende Interoperabilitätspflicht begründet. Daher ist auch wegen der zeitlichen Beschränkung der Feststellung marktübergreifender Bedeutung fraglich, ob das BKartA Interoperabilität bspw. eines sozialen Netzwerks „positiv" anordnen könnte. Sind im konkreten Fall Schnittstellen tatsächlich vorhanden, werden aber bspw. nur bestimmten Unternehmen geöffnet, so scheint eine solche Anordnung in Form einer Untersagung der Behinderung von Interoperabilität denkbar. Damit ginge es um die Ausgestaltung einer grundsätzlich bestehenden Zugangsoffenheit. Das gilt regelmäßig für die vertikale Interoperabilität, kann aber auch für die horizontale Interoperabilität angenommen werden. Denkbar ist eine solche Anordnung auch für

475 Regierungsentwurf BT-Drs. 19/23492, S. 76, 77.
476 *Paal*, in: Gersdorf/Paal, § 19a GWB Rn. 27.
477 *Kommission Wettbewerbsrecht 4.0*, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft, Empfehlung 11, S. 55.

einzelne Funktionen grundsätzlich interoperabler Dienste, wie sie in Art. 6 Abs. 4 und 7 DMA mit Blick auf Betriebssysteme normiert wird. Eine mit Art. 7 DMA vergleichbare Anordnung einer horizontalen Interoperabilität durch das BKartA, ohne dass bereits Schnittstellen bestehen, dürfte aber mit der Konstruktion von § 19a GWB nicht funktionieren.

Im Hinblick auf die Datenportabilität adressiert die Untersagungsmöglichkeit, dass die Nutzung konkurrierender Angebote insbesondere auf mehrseitigen Märkten für Verbraucher und Geschäftsnutzer oft nur dann von Interesse ist, wenn die bei der Nutzung des bisherigen Angebots entstandenen Daten auch nach dem Wechsel zu einem Wettbewerber genutzt werden können. Es geht also um Systemwechsel- und Multi-Homing-Möglichkeiten. Wann eine Datenportabilität in diesem Sinne vorliegt, wird vom Gesetz nicht konkretisiert. Die Gesetzesbegründung verweist auf Aspekte, die denen der Datenportabilität nach Art. 20 DS-GVO entsprechen, und fordert insbesondere eine Zurverfügungstellung in einem „strukturierten, gängigen und maschinenlesbaren Format" oder aber „eine andere Form der Mitwirkung des datenverarbeitenden Unternehmens".[478]

Nach § 19a Abs. 2 S. 2 stehen alle vorgenannten Tatbestände als Grundlage für ein Untersagen unter der Einschränkung, dass die Verhaltensweise sachlich gerechtfertigt werden kann. Dazu trifft das Unternehmen aber dann die Darlegungs- und Beweislast. Bezüglich der Interoperabilitätsbestimmung hebt die Gesetzesbegründung hervor, dass bei der sachlichen Rechtfertigung die wettbewerbliche Ambivalenz von Interoperabilität berücksichtigt werden soll, dass also das Fehlen von Interoperabilität nicht per se wettbewerbsschädigend ist und begründet sein kann. Daher sollen auch mögliche Nachteile von Interoperabilität in die Betrachtung einbezogen werden, z. B., dass zugunsten von Wettbewerbern des Normadressaten wirkende Netzwerkeffekte geschwächt werden könnten. Maßnahmen zur Interoperabilität können nach der Gesetzesbegründung Produktgestaltungsmöglichkeiten einschränken und Innovation behindern. Schließlich könnten solche Maßnahmen dazu beitragen, dass der Normadressat durch ihre Nutzung Zugang zu (noch) mehr Daten erhält,[479] weshalb die Speisung von Datenvorteilen als möglicher Rechtfertigungsgrund für das Fehlen von Interoperabilität angesehen wird.[480]

478 Regierungsentwurf BT-Drs. 19/23492, S. 77.
479 Regierungsentwurf BT-Drs. 19/23492, S. 77.
480 *Paal*, in: Gersdorf/Paal, § 19a GWB Rn. 27.

b. Institutionelle Dimension

(1) Befugnisse des BKartA

Im Rahmen der allgemeinen Missbrauchsaufsicht (§§ 19 und 20) steht dem BKartA ein umfassendes Portfolio an Rechtsdurchsetzungsmöglichkeiten zur Verfügung (§§ 32 ff. GWB). Diese umfassen u. a. (auch einstweilige) Verpflichtungsanordnungen zur Abstellung von Verstößen, die auch Abhilfemaßnahmen verhaltensorientierter oder struktureller Art vorschreiben können. Hinzu treten Beseitigungs-, Unterlassungs- und Schadensersatzansprüche bei Verstößen gegen Teil 1 des GWB oder Verfügungen des BKartA, die Betroffenen (Mitbewerbern oder sonstigen beeinträchtigten Marktbeteiligten) zustehen. Das BKartA kann zudem unter den Bedingungen des § 81 GWB Bußgelder bei Verstößen gegen die §§ 19 und 20 oder gegen Anordnungen nach § 19a Abs. 2 GWB – wie im Übrigen auch beim DMA – verhängen. Zudem ist eine Vorteilsabschöpfung möglich.

§ 19a GWB ist aber insgesamt ein Sondertatbestand der Missbrauchsaufsicht, der es dem BKartA ermöglicht, durch eine Verfügung die überragende marktübergreifende Bedeutung eines Unternehmens für den Wettbewerb festzustellen und, darauf basierend, diesem Unternehmen zunächst bestimmte Verhaltensweisen zu untersagen. Das ist von der allgemeinen Missbrauchsaufsicht zu separieren, da die §§ 19 und 20 GWB nach § 19a Abs. 3 GWB ausdrücklich unberührt bleiben, ein Vorgehen in Bezug auf das gleiche Verhalten also parallel nach beiden Vorschriften möglich bleibt und mit anderen Rechtsfolgen verknüpft werden kann.[481] § 19a GWB ist mit anderen Folgen verbunden, die wiederum zeitlich befristet gelten. Die Feststellung der überragenden marktübergreifenden Bedeutung ist auf fünf Jahre zu befristen (§ 19a Abs. 1 S.3 GWB). Die Regeln zur Auferlegung von Abhilfemaßnahmen, einstweiligen Maßnahmen und Verpflichtungszusagen gelten entsprechend bei § 19a GWB.

Von besonderer Bedeutung für ein flexibles Reagieren auf Marktentwicklungen sind die Neuerungen, die mit der 11. GWB-Novelle ins Gesetz eingefügt wurden. Nach § 32e GWB kann das BKartA zur Untersuchung einzelner Wirtschaftszweige und Arten von Vereinbarungen eine Sektoruntersuchung einleiten, die auf eine Sollfrist von 18 Monaten ausgelegt ist. Verbunden sind damit entsprechende Auskunftsrechte. Die Sektoruntersuchung

481 *Paal*, in: Gersdorf/Paal, § 19a Rn. 39.

endet mit einem Abschlussbericht, an dessen Veröffentlichung eine weitere 18-monatige Frist für etwaige Folgemaßnahmen anknüpft. Im Anschluss an diese Sektoruntersuchung kann das BKartA nach § 32f GWB in einem zweiten Schritt eine „erhebliche und fortwährende" Wettbewerbsstörung[482] feststellen, soweit die Anwendung seiner sonstigen Befugnisse nach einer Prima-facie-Bewertung nicht ausreichen, um die Störung wirksam und dauerhaft zu beseitigen. In einem dritten Schritt besteht für das BKartA die Möglichkeit, gegenüber den Adressaten der zuvor getroffenen Feststellungsverfügung Abhilfemaßnahmen anzuordnen, um die Störung zu beseitigen oder zu verringern. Hierzu gehören alle Abhilfemaßnahmen verhaltensorientierter oder struktureller Art, die zur Beseitigung oder Verringerung der Störung des Wettbewerbs erforderlich sind. Insbesondere und ausdrücklich kann das nach § 32f Abs. 3 Nr. 1 GWB auch die Gewährung des Zugangs zu Daten, Schnittstellen, Netzen oder sonstigen Einrichtungen erfassen. In diesem Sinne hat das BKartA die Befugnis, Interoperabilität zumindest in Teilen anzuordnen. In Bezug auf Unternehmen nach § 19a Abs. 1 GWB ist weitergehend die Anordnung der Veräußerung von Unternehmensanteilen oder Vermögen möglich.

Eine grenzüberschreitende Zusammenarbeit, die vor allem im digitalen Bereich von besonderer Relevanz ist, ist im Netzwerk der europäischen Wettbewerbsbehörden vorgesehen. Regeln zu Ermittlungen, Zustellungen, zur Vollstreckung, zum Informationsaustausch und zur sonstigen Zusammenarbeit finden sich in §§ 50a ff. GWB. Eine Regelung zur Zusammenarbeit mit anderen (nationalen) Behörden ist in § 50f vorgesehen. Abs. 2 nennt insbesondere den Erkenntnisaustausch mit den Landesmedienanstalten und der Kommission zur Ermittlung der Konzentration im Medienbereich, soweit dies für die Erfüllung der jeweiligen Aufgaben erforderlich ist. Diese Bestimmung könnte auch im Kontext von Interoperabilität nutzbar gemacht werden.

(2) BKartA und DMA

Mit der 11. GWB-Novelle wurde das Gesetz an den DMA angepasst. Neben der Erweiterung von Beseitigungs-, Unterlassungs- und Schadensersatzansprüchen auch auf Verstöße gegen den DMA (§ 33 Abs. 1 GWB) ist vor allem die Untersuchung von möglichen Verstößen gegen den DMA durch

482 Die Bedingungen hierzu enthält § 32f Abs. 5 GWB.

das BKartA nach § 32g GWB relevant. Danach kann das BKartA eine Untersuchung bei einer möglichen Nichteinhaltung der Art. 5, 6 oder 7 DMA durch ein nach Art. 3 DMA benanntes Unternehmen durchführen. Hierzu kann es alle für die Untersuchung erforderlichen Ermittlungen durchführen.

Sofern die Ermittlungen einen möglichen Verstoß gegen Art. 7 DMA betreffen, also die Interoperabilität von Messenger-Diensten, soll der Bundesnetzagentur die Möglichkeit zur Stellungnahme gegeben werden. Verbunden ist das schließlich mit einer Berichterstattungspflicht des BKartA an die Kommission. Weitere Gesetzesänderungen erklären das BKartA auch zu einer für die Mitwirkung an Verfahren der Europäischen Kommission unter dem DMA zuständigen Wettbewerbsbehörde.

(3) Relevante Wettbewerbsentscheidungen des Bundeskartellamts

(a) Online-Vergleichsplattformen

Am 24. Juli 2015 und damit noch vor der 9. GWB-Novelle, die solche Kriterien unmittelbar ins Gesetz einführte, beurteilte das BKartA die Übernahme von Verivox durch die ProSiebenSat.1 Media AG (P7S1) auch entlang möglicher Netzwerkeffekte.[483] Im Hinblick auf die Marktabgrenzung stellte das BKartA fest, dass bei Transaktionsplattformen wie Verivox (als dem damals führenden Online-Vergleichsportal für die Vermittlung von Strom- und Gasverträgen in Deutschland) zwar ein typischer zweiseitiger Markt vorliege, aber anders als bei auf Werbefinanzierung beruhenden zweiseitigen Märkten nicht zwischen den verschiedenen Marktseiten (Verbraucher und Anbieter von Verträgen) zu trennen sei, weil die Verbundenheit der Gruppen durch wechselseitige positive indirekte Netzwerkeffekte zu einem weitgehend einheitlichen Bedarf führe.

Für die zu untersuchende Beeinträchtigung des Wettbewerbs war festzustellen, dass zwar zwischen den Geschäftstätigkeiten der Zusammenschlussbeteiligten keine nennenswerten horizontalen Überschneidungen bestanden. Allerdings warf die Übernahme die Frage auf, ob P7S1 dadurch künftig die Möglichkeit und den Anreiz habe, Verivox bessere Werbeplät-

483 *BKartA*, Fallbericht zu Az. B8–76/15, 5.8.2015, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Fusionskontrolle/2015/B8-76-15.pdf?__blob=publicationFile&v=3.

ze zu günstigeren Konditionen einzuräumen als den Wettbewerbern, und ob dadurch wirksamer Wettbewerb erheblich behindert würde. In seiner Pressemitteilung hatte P7S1 – neben der RTL-Gruppe der größte Anbieter von Fernsehwerbung – damals mitgeteilt, dass man die Marktposition von Verivox durch den Einsatz von Fernsehwerbung ausbauen wolle. Letztlich ließ das Vorhaben jedoch auch bei einer engen Marktabgrenzung eine solche erhebliche Behinderung, insbesondere durch ein sog. Markt-Tipping, nicht erwarten, und das BKartA genehmigte die Übernahme. Dafür führte es insbesondere an, dass, auch bei Gewährung einer bevorzugten Stellung in der Werbung, die Provisionsumsätze von Verivox einerseits und ein etwaiger Verlust von Werbeeinnahmen von P7S1 andererseits aus Sicht des Medienkonzerns in einem wirtschaftlichen Verhältnis stehen müsse. Auch bliebe anderen Vergleichsportalen die neben der Fernsehwerbung wichtigste Sichtbarkeitsquelle der Google-Platzierung.[484] Durch die Marktstärke des Vergleichsportals Check24, das in den meisten Sparten außer dem Energiebereich höhere Marktanteile habe, sei die Gefahr eines Tippings nicht so hoch. Tendenziell gegen ein Tipping spreche auch, dass die Anbieter im Energiebereich eher Multi-Homing als Single-Homing einsetzten, d. h. ihre Angebote jeweils auf mehreren Online-Vergleichsplattformen schalteten.

(b) Slack/Salesforce

In der Rechtssache *Slack/Salesforce* ging es um ein Fusionskontrollverfahren, das im Februar 2021 entschieden wurde.[485] Das BKartA genehmigte den beabsichtigten Erwerb der Slack Technologies, eines Anbieters von Kollaborationssoftware für den Austausch von Nachrichten, Dokumenten und Sprach-/Videoanrufen, durch die salesforce.com, Inc., den weltweit führenden Anbieter von Customer-Relationship-Management-(CRM-)Lösungen, weil keine erhebliche Wettbewerbsbehinderung zu befürchten sei.

Ein zentraler Punkt in der Untersuchung war dabei die Interoperabilität der Systeme. Hätte der Zusammenschluss zu einer Beschränkung der Interoperabilität der Anwendungen geführt, wäre dies bei der Untersuchung als wettbewerbsrechtlich problematisch einzustufen gewesen. Beide Unter-

484 Vgl. zu dieser Problematik oben die Entscheidung zu *Google Shopping*, C.II.2.a(2)(c).

485 *BKartA*, Fallbericht zu Az. B7–32/21, 12.3.2021, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Fusionskontrolle/2021/B7-32-21.pdf?__blob=publicationFile&v=2.

nehmen hatten aber im Verfahren und öffentlich bekundet, dass sie sich einer offenen Software-Architektur verpflichtet sähen und Slack weiterhin als Stand-alone-Version verfügbar sein solle. Zwar wurde die Beschränkung der Einbindungsmöglichkeit von Slack für kleinere CRM-Anbieter als möglich und dann auch als möglicher wettbewerblicher Nachteil für diese gesehen, allerdings sei für weitreichende Effekte Slacks Marktbedeutung in Deutschland und für den CRM-Bereich nicht groß genug, um einer Fusion entgegenzustehen.

(c) Eventim

In zwei Rechtssachen betreffend die CTS EVENTIM AG & Co. KGaA befasste sich das BKartA bereits im Vorfeld der relevanten GWB-Novellen mit dem Thema Interoperabilität. Eventim ist einer der größten Ticketing- und Live-Entertainment-Unternehmen und bietet insbesondere Agenturleistungen im Zusammenhang mit dem Vertrieb von Tickets für bspw. Konzerte oder andere Veranstaltungen über ein umfassendes Ticketsystem an. Dieses System schließt den Vertrieb über externe und konzerneigene stationäre Vorverkaufsstellen, diverse Reisebüros großer Reisebüroketten, konzerneigene Callcenter und konzerneigene Online-Shops, insbesondere die Webseite eventim.de, ein. Im ersten Verfahren, das mit Beschluss vom 23. November 2017 entschieden wurde, ging es um einen geplanten Zusammenschluss, bei dem Eventim Anteile an der Four Artists Booking Agentur GmbH und Four Artists Events GmbH erwerben wollte. Der Zusammenschluss wurde jedoch untersagt – eines der einschneidendsten Mittel, die im Fusionskontrollverfahren zur Verfügung stehen, wenn keine Auflagen oder Verpflichtungszusagen über die mit der geplanten Fusion verbundenen Wettbewerbsbeeinträchtigungen hinweghelfen könnten.[486]

Im zweiten Verfahren standen dagegen (auch) die Exklusivvereinbarungen im Vordergrund, die Eventim mit seinen Kunden (Künstlern, Konzertveranstaltern, Vorverkaufsstellen etc.) schloss. Neben einer Gebührenpflicht bzw. Provision für Eventim sahen die Klauseln eine Verpflichtung der Vertragspartner vor, entweder ausschließlich oder zu einem erheblichen Anteil nur das CTS-System EVENTIM.NET für den Vertrieb ihrer Tickets

486 *BKartA*, Beschluss zu Az. B 6 – 35/17, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Fusionskontrolle/2018/B6-35-17.pdf?__blob=publicationFile&v=2.

über Ticketsysteme zu nutzen. Weder die Veranstalter selbst noch andere Ticket-Vertriebsunternehmen konnten Ticketbestände selbst über eigene Kanäle verkaufen. Das BKartA sah diese Vorgehensweise als wettbewerbswidrig an und verpflichtete Eventim mit Entscheidung vom 4. Dezember 2017 dazu, künftig Veranstaltern und Vorverkaufsstellen zu erlauben, mindestens 20 % ihres pro Jahr für den Vertrieb über Ticketsysteme verfügbaren Ticketvolumens selbst oder über Dritte zu verkaufen, die Exklusivvereinbarung also deutlich zu relativieren.[487]

In beiden Fällen spielte die Interoperabilität von Ticketverkaufssystemen bzw. von deren Fehlen eine Rolle für die negative Bescheidung des BKartA.[488] Bei Ticketsystemen sei die Möglichkeit eines Multi-Homing für Veranstalter von vornherein nur beschränkt zu verwirklichen, da mangels Interoperabilität der Ticketsysteme nur vorab festgelegte Ticketkontingente auf die Systeme verteilt werden können. Es existierten bislang keine technischen Lösungen, etwa in Form der Live-Interoperabilität von Ticketdienstleistungssystemen verschiedener Anbieter, die es ermöglichen würden, eine Verwaltung der Kontingente über mehrere Vertriebsquellen zu steuern. Nur innerhalb des Kosmos eines Vertriebsdienstleisters sei das gewährleistet. Eine solche Lösung werde von den Ticketsystemen auch nicht angestrebt. Ein wirksames marktmachtbegrenzendes Multi-Homing könnte auf diesem Markt aus Sicht des BKartA daher grundsätzlich nur angenommen werden, wenn Veranstalter überwiegend mehrere Ticketsysteme mit vergleichbaren Ticketkontingenten bestücken würden. Das war aber vorliegend nicht der Fall. Die Untersuchungen des BKartA ergaben, dass im Untersuchungszeitraum nur etwa 10 % der Veranstalter überhaupt ein anderes System als Eventim nutzten. Insofern war das Fehlen von Interoperabilität und die mangelnde Bestrebung dazu einer der Gründe, die ein wettbewerbsrechtliches Einschreiten rechtfertigten.

(d) Facebook

In einer umfassenden Entscheidung vom 6. Februar 2016 untersagte das BKartA Facebook (heute Meta) im Wesentlichen die diensteübergreifende

487 *BKartA*, Beschluss zu Az. B 6 – 132/14–2, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Missbrauchsaufsicht/2018/B6-132-14-2.pdf?__blob=publicationFile&v=3.

488 B 6 – 35/17, Rn. 178, und B 6 – 132/14–2, Rn. 184.

Zusammenführung von Nutzerdaten innerhalb des Konzerns bzw. die Vorhaltung entsprechender Nutzungsbedingungen innerhalb seiner verschiedenen Netzwerke. Das betraf sowohl die Zusammenführung von Daten in den konzerneigenen Diensten wie Facebook, Instagram, WhatsApp, Masquerade und Oculus als auch den Zugriff auf Daten aus bestehenden Programmierschnittstellen (insb. Facebook-Business-Tools wie das beliebte Social-Media-Plugin, das Unternehmen in ihre Webseiten und Anwendungen einbinden können, um sich mit Nutzern auf den Meta-Netzwerken zu vernetzen). Nach Entscheidungen in mehreren Instanzen[489] entschied auch der EuGH in dieser Rechtssache. Dieses Urteil soll nicht im Detail betrachtet werden, da Interoperabilität nicht der Schwerpunkt war, aber ein materieller und ein prozeduraler Aspekt sind hervorzuheben.

In materieller Hinsicht ist die Entscheidung im vorliegenden Kontext insofern relevant, als sie einerseits die Gefahren von fehlender Interoperabilität und andererseits Ausgestaltungsprobleme dokumentiert. Der Missbrauch der marktbeherrschenden Stellung durch Facebook wurde u. a. auch mit Netzwerk- und Lock-in-Effekten begründet, insbesondere den Registrierungspflichten und Anbindungsmöglichkeiten, mit denen Nutzer im Meta-Universum konfrontiert sind. Durch die massive Ansammlung von Daten aus verschiedenen Schnittstellen werde die Marktmacht weiter intensiviert. Umgekehrt dokumentiert die Entscheidung in Bezug auf die bestehenden Programmierschnittstellen, dass eine (Teil-)Interoperabilität auf vertikaler Ebene auch zu einem Ausbau der Marktmacht führen kann, wenn sie einseitig bestimmt und nutzbar gemacht wird.

In prozeduraler Hinsicht ist das Urteil vor allem für das Zusammenspiel von Wettbewerbsrecht und Datenschutzrecht sowie die damit in Verbindung stehende behördliche Zusammenarbeit interessant. Dieser Aspekt war auch der Schwerpunkt des Verfahrens vor dem EuGH. Das BKartA hatte den Missbrauch maßgeblich auf einen Verstoß gegen das Datenschutzrecht gestützt, der sich hier (zusätzlich) wettbewerbsschädigend auswirke. Der EuGH führte hierzu in seiner Grundsatzentscheidung vom 4. Juli 2023 aus, dass eine mitgliedstaatliche Wettbewerbsbehörde im Rahmen der Prüfung, ob ein Missbrauch einer beherrschenden Stellung durch ein Unternehmen im Sinne von Art. 102 AEUV vorliegt, auch datenschutzrechtliche Bestimmungen prüfen und zur Grundlage ihrer Entscheidung machen könne.

489 OLG Düsseldorf, 26.08.2019 – Kart 1/19; BGH, 23.06.2020 – KVR 69/19; OLG Düsseldorf, 30.11.2020 – Kart 13/20; BGH, 15.12.2020 – KVZ 90/20; BGH, 08.03.2021 – KVR 96/20; OLG Düsseldorf, 24.03.2021 – Kart 2/19.

Allerdings stehe dies unter dem Vorbehalt der Einhaltung ihrer Pflicht zur loyalen Zusammenarbeit mit den datenschutzrechtlichen Aufsichtsbehörden, die jedenfalls fordere, dass eine Wettbewerbsbehörde nicht von einer möglichen vorherigen Entscheidung der zuständigen nationalen Datenschutzbehörde oder der zuständigen federführenden Aufsichtsbehörde abweichen dürfe. Bei Zweifeln treffe sie insbesondere eine Konsultations- und Kooperationspflicht mit dieser Behörde.[490]

(e) Feststellung überragender marktübergreifender Bedeutung (§ 19a GWB)

Im Visier der Feststellung einer überragenden marktübergreifenden Bedeutung nach § 19a GWB finden sich vor allem die fünf großen amerikanischen Tech-Unternehmen Alphabet (Google), Meta, Microsoft, Amazon und Apple.[491]

In der konkreten Prüfung befindet sich das Verfahren gegen Microsoft, das am 28. März 2023 eingeleitet wurde.[492] Eine Prüfung konkreter Verhaltensweisen von Microsoft anhand der Kriterien des § 19a Abs. 2 GWB ist damit noch nicht verbunden.

Der erste Schritt der Prüfungsverfahren gegen Amazon und Apple wurde dagegen bereits mit entsprechenden Feststellungen überragender marktübergreifender Bedeutung am 5. Juli 2022 (Amazon)[493] bzw. am 3. April 2023 (Apple)[494] abgeschlossen. Sowohl Amazon[495] als auch Apple haben allerdings hiergegen Beschwerde beim BGH mit dem Antrag eingelegt, den Beschluss aufzuheben. In Bezug auf Apple ging das BKartA davon aus, dass das Unternehmen über marktbeherrschende, mindestens jedoch

490 C-252/21 – *Meta Platforms*, ECLI:EU:C:2023:537 –, Rn. 36 ff., 52 ff.

491 Vgl. zum Stand von Verfahren des BKartA gegen Digitalkonzerne die Übersicht (Stand Oktober 2023) unter https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Downloads/Liste_Verfahren_Digitalkonzerne.pdf?__blob=publicationFile&v=25.

492 Vgl. *BKartA*, Pressemitteilung vom 28.3.2023, https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2023/28_03_2023_Microsoft.html.

493 B2–55/21, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Missbrauchsaufsicht/2022/B2-55-21.pdf;jsessionid=781BD9A3A2D5C4E685F2D369C93368FD.1_cid509?__blob=publicationFile&v=2.

494 Vgl. die Pressemitteilung vom 5.4.2023, https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2023/05_04_2023_Apple_Abschluss.html?nn=3591568.

495 KVB 56/22; vgl. auch die Pressemitteilung des BGH, https://www.bundesgerichtshof.de/SharedDocs/Termine/DE/OhneTermin/KVB56-22.html.

marktstarke Stellungen auf allen vertikal verbundenen Stufen verfügt, ausgehend von Smartphones, Tablets und Smartwatches über die proprietären Betriebssysteme bis hin zum Apple App Store. Vor allem der App Store, der sowohl für App-Herausgeber als auch für Nutzer die einzig verfügbare digitale Vertriebsplattform im iOS-Universum ist, war im Fokus der Untersuchungen des BKartA.

In Bezug auf Amazon führte das BKartA die Schlüsselposition des Unternehmens im Bereich des E-Commerce an, die wesentlich auf der starken Wettbewerbsposition seiner jeweiligen länderspezifischen Handelsplattformen beruhe und dabei eine hybride Struktur aufweise, in der Amazon sowohl selbst Waren vertreibe (Retail) als auch Dritthändler sei. Für Kunden ergebe sich die hohe Attraktivität daher aus der enormen Angebotsbreite, die durch vielfältige Leistungen auf weiteren Märkten, z. B. in den Bereichen Videostreaming, Musikstreaming oder Internet of Things, ergänzt werde. Gefahren ergäben sich aber aus Sicht der Mitbewerber und auch der Händler inklusive der sonst Betroffenen innerhalb der vertikalen Strukturen. Im Fokus der Verfahren gegen Amazon stehen die Preiskontrolle (mögliche Einflussnahme auf Händlerpreise) und das sog. „Brandgating" (Benachteiligung von Marktplatzhändlern etwa durch Vereinbarung mit Markenhändlern zum Ausschluss von Dritthändlern).

Die rechtskräftige Feststellung einer überragenden marktübergreifenden Bedeutung von Meta hat das BKartA am 2. Mai 2022 getroffen. Begründet wurde sie maßgeblich mit dem starken, datengetriebenen Ökosystem, das Meta im gesamten Bereich der werbefinanzierten sozialen Medien betreibt. Dieses berge aufgrund hoher Bindungseffekte gegenüber privaten Nutzern und Geschäftskunden die Gefahr, dass andere Wettbewerber dauerhaft weitgehend auf einen Wettbewerb nur in Teilbereichen verwiesen würden und ihre Innovationskraft erheblich gefährdet werde. Die Verbundvorteile erleichterten darüber hinaus die beständige Erweiterung und Konsolidierung sowie die Finanzierung des Ökosystems. Interoperabilität spielte hier insofern eine Rolle, als sie von Meta vor allem durch zahlreiche Anbindungen innerhalb des eigenen Verbundsystems hergestellt wird, nicht aber nach außen für Dritte. Ein Beispiel war das in Bezug auf VR-Brillen (Oculus) eingeleitete Verfahren des BKartA, das die zwingende Kopplung der Nutzung der Brillen an ein Facebook-Konto betraf. Nachdem Meta diese Voraussetzung allerdings geändert hatte, bezieht sich dieses Verfahren

jetzt noch auf die Ausgestaltung von bestehenden Wahlmöglichkeiten einer Registrierung und die Zusammenführung von Daten.[496]

Google war das erste Unternehmen, über das eine Feststellung einer überragenden marktübergreifenden Bedeutung getroffen wurde. Am 30. Dezember 2021 fasste das BKartA einen entsprechenden Beschluss und hob darin hervor, dass Google eine breite Vielzahl von Diensten markt- und reichweitenstark anbiete.[497] Bei diesem Angebot und seiner Erweiterung bestehe die Möglichkeit, von Verbundvorteilen zu profitieren und marktübergreifend gegenüber anderen Unternehmen die Rolle eines Regelsetzers einzunehmen und dabei auch auf einen breiten sowie tiefen Datenzugang zurückzugreifen. Dadurch könne das Unternehmen seine Position ohne hinreichende wettbewerbliche Kontrolle weiter konsolidieren, ausweiten oder auf sonstige Weise zum eigenen Vorteil nutzen. Ein relevanter Aspekt war, dass Google insbesondere mit der Google-Suche, YouTube, Chrome, Android und dem Play Store über eine Vielzahl von zumindest marktstarken Diensten verfügt. Wie bei Meta spielte Interoperabilität lediglich im eigenen Verbundsystem (und damit negativ) eine Rolle, vor allem im Hinblick auf die Online-Werbedienste von Google.

(f) Google News Showcase

Basierend auf der zuvor genannten Feststellung einer überragenden marktübergreifenden Bedeutung von Google hat das BKartA bereits mehrere Verfahren auf dieser Basis gegen das Unternehmen eingeleitet. Die Interoperabilitätsbestimmung des § 19a Abs. 2 Nr. 5 GWB ist davon noch nicht betroffen. In einem medienrechtlichen Kontext, insbesondere vor dem Hintergrund der Vielfaltssicherung im Online-Bereich, ist aber der Fall des Google News Showcase interessant.

Im Sommer 2021 leitete das BKartA auf der Basis seiner neuen Befugnisse aus § 19a GWB ein Verfahren gegen Google ein, deren Anlass maßgeblich eine Beschwerde der Corint Media gegen das Angebot des Google News Showcase war. Bei diesem im Oktober 2020 von Google gestarteten Projekt,

496 Vgl. dazu die Pressemitteilungen vom 28.1.2021, https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2021/28_01_2021_Facebook_Oculus.html?nn=3591568, und vom 23.11.2022, https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2022/23_11_2022_Facebook.html.

497 B7–61/21, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Missbrauchsaufsicht/2021/B7-61-21.pdf?__blob=publicationFile&v=3.

das mit ausgewählten deutschen Verlagen im Frühjahr 2021 eröffnet worden war, handelt es sich im Wesentlichen um ein Nachrichtenangebot für Endnutzer. Partner-Verlagen in diesem Projekt wurde bei Teilnahme die Möglichkeit eröffnet, eine – auch im Vergleich zu anderen Inhalten – hervorgehobene und vertiefte Darstellung ihrer Verlagsinhalte auf Google zu erreichen. Hierfür zahlte Google im Gegenzug entsprechende Lizenzgebühren, erwarb teilweise auch ansonsten bei den Verlagen kostenpflichtige Inhalte und bot diese Google-Nutzern kostenlos an. Zentraler Gegenstand sind sog. „Story-Panels", die zunächst in der Google News App eingebunden wurden und seit Mitte 2021 auch in Google News auf dem Desktop-Browser zu finden waren. Hierbei handelt es sich um umrandete „Kacheln", in denen unter der prominent dargestellten Verlagsmarke Fotos, Überschriften und weitere Inhalte zusammengefasst werden. Bedenken hatte das BKartA (und auch die dagegen vorgehenden Verlage) vor allem dahingehend, dass durch die festgestellte überragende marktbeherrschende Stellung von Google eine Diskriminierung nicht angeschlossener Angebote stattfinden könnte und dass Google im Übrigen seine urheberrechtlichen Pflichten im Kontext des 2019 EU-weit eingeführten Leistungsschutzrechts für Presseverlage durch unangemessene Vertragsbedingungen vernachlässigen könnte. Verstärkt wurden diese Bedenken durch Googles Ankündigung, das Angebot zukünftig auch in die allgemeine Google-Suche einzubinden und ihm dadurch eine noch stärkere Relevanz zu geben.

Letztlich wurde das Verfahren am 21. Dezember 2022 seitens des BKartA eingestellt. Grund für die Einstellung war, dass Google wichtige Anpassungen in seinem Angebot infolge der Intervention der Wettbewerbsbehörde vorgenommen sowie weitere Verpflichtungszusagen zugunsten von Verlagen gemacht hatte.[498] Google hat seine Vertragspraxis so geändert, dass den Verlagen eine Geltendmachung ihres allgemeinen Presse-Leistungsschutzrechts nicht erschwert wird, die gänzlich unabhängig vom News Showcase erfolgen soll. Außerdem wurde zugesichert, dass künftig weitere Verlage an Google News Showcase teilnehmen können, also einer möglichen Benachteiligung von nicht integrierten Angeboten Rechnung getragen wird. Auch von der Integration des Angebots in die allgemeine Google-Suche wurde Abstand genommen, sodass die Teilnahme oder Nicht-Teilnahme eines Verlags am Showcase-Programm auch künftig nicht für das Ranking der Suchergebnisse relevant ist.

498 V-43/20, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Missbrauchsaufsicht/2022/V-43-20.pdf?__blob=publicationFile&v=2.

Dass das Verfahren ohne eine förmliche Verpflichtungszusagenentscheidung (§ 32b GWB) eingestellt wurde, lässt dabei die Möglichkeit offen, es bei künftigen Änderungen der Verhältnisse oder bei neuen Erkenntnissen wieder zu eröffnen. Das BKartA weist in seinen FAQ zum Verfahren auch auf ein derzeit davon unabhängiges, bei den deutschen Landesmedienanstalten laufendes Verfahren hin, das die Vorschriften des Medienstaatsvertrages zum Diskriminierungsverbot von Inhalten innerhalb von Intermediärsplattformen betrifft. Insoweit zeigt sich an dieser Stelle auch deutlich, dass ein Zusammenspiel und zugleich eine Abgrenzung zwischen den medienrechtlichen und den wettbewerbsrechtlichen Gesichtspunkten erforderlich ist. Das Verfahren des BKartA betraf die Ausnutzung der Stellung als Zugangstor aus der Perspektive der Wettbewerber. Die Regeln für Intermediäre im MStV betreffen dagegen Aspekte der Vielfaltssicherung und treten deshalb neben die Wettbewerbsregulierung und die Plattformregulierung bspw. nach dem DMA und DSA.

c. Die mögliche Rolle des Medienkonzentrationsrechts

Mit Ausnahme von Sonderregeln im GWB zur abgesenkten Interventionsschwelle bei der Fusionskontrolle für Presse und Rundfunk ist das Medienkonzentrationsrecht ein vom Wettbewerbsrecht zu unterscheidendes Rechtsgebiet, wenn es um Aspekte der Vielfaltssicherung geht. Neben aus den Grundrechten möglicherweise dazu abzuleitenden Geboten[499] findet es seine Verankerung auf einfachgesetzlicher Ebene in den Regeln des MStV, maßgeblich im Unterabschnitt zur Sicherung der Meinungsvielfalt. Neben mit engen Voraussetzungen versehenen Bestimmungen zur Begrenzung von Beteiligungsveränderungen bei der Gefahr für die Medienvielfalt gibt es ergänzende Vorschriften, die einen Beitrag zur Sicherstellung von Vielfalt leisten sollen, indirekt mit Interoperabilitätsüberlegungen verglichen werden können sowie einen Bezug zu wettbewerbsrechtlichen Ansätzen haben.

Den Regeln zur Einräumung von Drittsendezeiten und zu Fensterprogrammen in Programmen bestimmter Anbieter liegen dabei auch deutlich wettbewerbsrechtliche Gedanken, aber nicht zur Verhinderung von Marktmacht, sondern zur Sicherung von Vielfalt zugrunde. Reichweitenstarke Programme, die eine gewisse Menge an Zuschauern binden, werden verpflichtet, Programme von unabhängigen Dritten, die ansonsten wenig oder

499 Eingehend hierzu *Gounalakis/Zagouras*, Medienkonzentrationsrecht, S. 1 ff.

keine Reichweite hätten, zu übertragen und damit „im eigenen Dienst" zusätzliche Vielfalt herzustellen. Mit einem „Lock-in" ist die Reichweitenstärke nicht vergleichbar, sie bindet aber doch ein Publikum zu einer bestimmten Sendezeit und hindert es an der Inanspruchnahme anderer Programme. Die Einbindung der Drittprogramme hat dabei so zu erfolgen, dass z. B. technische Hindernisse vermieden werden. Bei einer Fortentwicklung des Medienkonzentrationsrechts über die aktuell noch geltende Fernsehzentriertheit hinaus könnte es ein Anknüpfungspunkt auch für Interoperabilitätserwägungen sein, wenn Verpflichtungen zur Übernahme von Inhalten auch andere Anbieter als Fernsehveranstalter treffen könnten. In ihrem 24. Jahresbericht stellt insoweit auch die KEK unter Bezugnahme auf den deutlichen Wandel im Mediennutzungsverhalten hin zu digitalen Angeboten fest, dass das gegenwärtige Medienkonzentrationsrecht hierauf praktisch keine Antworten gebe und dringend zu reformieren sei:

> *Nachdrücklich unterstützt die KEK daher die dringend gebotene und von Seiten des Gesetzgebers nun zeitnah in Aussicht gestellte Reformierung des bestehenden fernsehzentrierten Medienkonzentrationsrechts. Die Sicherung von Meinungsvielfalt bleibt weiterhin wichtig und ist nicht zuletzt auch verfassungsrechtlich geboten. Die KEK benötigt für diese Aufgabe einen zeitgemäßen Handlungsspielraum sowie die Befugnis zu wirksamen Sicherungsmaßnahmen, ähnlich den Befugnissen der Kartellbehörden.*[500]

III. Geltender Rechtsrahmen zur Interoperabilität: Telekommunikationsrecht

1. USA

a. Gesetzliche Regelungen

Im Mittelpunkt des US-amerikanischen Telekommunikationsrechts steht der Telecommunications Act of 1996.[501] Dieser zielt auf die Förderung des Wettbewerbs, um Verbrauchern einen fairen und bezahlbaren Zugang zu Telekommunikationsleistungen zu ermöglichen. Mit dem Telecommunications Act wird auch die Bereitstellung von Telekommunikationsdiensten über das Internet geregelt. Das Gesetz ist in sieben Kapitel gegliedert. Im

500 *KEK*, 24. Jahresbericht, S. 17.

501 Telecommunications Act of 1996, Pub. L. 104–104, 110 Stat. Der Telecommunications Act erweitert den Communications Act of 1934, Pub. L. 73–416, 48 Stat.

ersten Teil werden die Ziele bestimmt, also die Förderung des Wettbewerbs und die Bereitstellung von Telekommunikationsdiensten in den USA (Title I). Im zweiten und dritten Teil werden Rundfunk- und Kabelanbieter reguliert mit dem Ziel, ein vielfältiges Programmangebot zu schaffen und den Wettbewerb zu fördern (Title II und III). Hier werden Zulassung und Frequenzvergabe für Rundfunkanbieter geregelt, aber auch der Wettbewerb von Kabelanbietern wird geöffnet. Mit dem vierten Teil des Gesetzes sollte der regulatorische Rahmen für die Telekommunikation modernisiert werden, um Innovation und Effizienz zu fördern (Title IV). Im fünften Teil wird der Umgang mit anstößigen Inhalten und Gewalt im Rundfunk geregelt, vor allem zum Kinder- und Jugendschutz (Title V). Der sechste Teil berücksichtigt die Weitergeltung bisher ergangener wettbewerbsrechtlicher Entscheidungen zum Telekommunikationsmarkt sowie steuerliche Regelungen (Title VI). Im siebten und letzten Teil sind verschiedene Regelungen zusammengefasst, etwa zum Datenschutz von Bestands- bzw. Vertragsdaten (Title VII).

Interoperabilität ist ein konstitutives Merkmal für die Zusammenschaltung verschiedener Telekommunikationsnetze. Andernfalls könnte ein Kunde eines Telekommunikationsanbieters (z. B. AT&T) keine Verbindung zu einem Kunden eines anderen Telekommunikationsanbieters (z. B. Verizon) aufbauen. Vor diesem Hintergrund verpflichtet der Telecommunications Act Telekommunikationsanbieter umfassend zur Zusammenschaltung („interconnection") ihrer Telekommunikationsnetze:[502]

> *47 U.S. Code § 251 – Interconnection*
> *(a) General duty of telecommunications carriers*
> *Each telecommunications carrier has the duty—*
> *(1) to interconnect directly or indirectly with the facilities and equipment of other telecommunications carriers […].*

Telekommunikationsanbieter werden verpflichtet, direkte oder indirekte Verbindungen mit den Netzwerken und der Infrastruktur anderer Telekommunikationsanbieter und damit Interoperabilität zwischen Telekommunikationsnetzen herzustellen. Daneben ist gesetzlich das Recht zur Rufnummernmitnahme beim Wechsel eines Telekommunikationsanbieters, also auf eine spezifische Art der Datenportabilität, zugesichert:[503]

> *47 U.S. Code § 251 – Interconnection*

502 Telecommunications Act of 1996 § 101, 47 U.S. Code § 251(a).
503 Telecommunications Act of 1996 § 101, 47 U.S. Code §251(b)(2).

(b) Obligations of All Local Exchange Carriers
Each local exchange carrier has the following duties:
[…]
(2) Number Portability
The duty to provide, to the extent technically feasible, number portability in accordance with requirements prescribed by the Commission.

Gleichzeitig ist es Telekommunikationsanbietern untersagt, den barrierefreien Zugang zu Telekommunikationsnetzen zu erschweren (47 U.S. Code § 255) sowie Nutzer und Anbieter beim Zugang zu Telekommunikationsnetzen zu diskriminieren (47 U.S. Code § 256).

Durch die Verpflichtung zur Zusammenschaltung von Telekommunikationsnetzen werden sowohl die eigentliche Leistungserbringung als auch bspw. Rechte wie die Rufnummernmitnahme technisch erst ermöglicht. Verstöße gegen die Verpflichtung können mit Geldstrafen von bis zu USD 10.000 oder Freiheitsstrafen von bis zu einem Jahr Freiheitsstrafe sanktioniert werden.[504] Die Federal Communications Commission (FCC) ist als unabhängige Regierungsbehörde für Telekommunikationsdienste für die Durchsetzung zuständig (zur FCC näher unter b).

Neben der Interoperabilität für Kommunikationsnetze sind in den USA von der FCC auch Interoperabilitätsvorschriften für sog. *Telecommunications Relay Services* erlassen worden. Diese ermöglichen es Menschen mit Hör- oder Sprachbeeinträchtigungen, Sprach- und Videoanrufe zu tätigen und entgegenzunehmen. *Telecommunications Relay Services* stellen entsprechend ein funktionales Äquivalent zu audiobasierten Telekommunikationsdiensten dar. Hinsichtlich der Interoperabilität müssen bspw. Betreiber von Videodiensten zur Übertragung von Gebärdensprache (also *Video Relay Services (VRS)*) analog zum herkömmlichen Telekommunikationsnetz Interoperabilität für ihre Dienste gewährleisten:[505]

47 Code of Federal Regulations§ 64.621 – Interoperability and portability.
(a) General obligations of VRS providers.
[…]
(3) All VRS providers must ensure that their VRS access technologies and their video communication service platforms are interoperable with the

504 47 U.S. Code § 501.

505 47 CFR § 64.621. Im Unterschied zu vom US-Kongress erlassenen gesetzlichen Vorschriften des U.S. Code enthält der CFR von US-Bundesbehörden erlassene Regelungen und Verordnungen.

VRS Access Technology Reference Platform, including for point-to-point calls. […]

Die Plattform bzw. der Standard, mit dem Videodienste interoperabel sein müssen, wird von der FCC festgelegt.[506]

Neben den Regelungen für öffentliche Telekommunikationsnetze soll interoperable Kommunikation auch bei geschlossenen Netzen für die öffentliche und nationale Sicherheit geschaffen werden. Für die Notfallkommunikation etwa bei Naturkatastrophen oder der Terrorismusabwehr sollen unterschiedliche zuständige Behörden und Einsatzkräfte wie Polizei, Feuerwehr oder Rettungsdienste auf Bundes-, Stammes-, einzelstaatlicher und lokaler Ebene miteinander kommunizieren können, wofür interoperable Kommunikationsnetze für den Krisenfall erforderlich sind.[507] Zur Erforschung und Regulierung derartiger interoperabler Telekommunikationsnetze für den Krisenfall wurde das Office for Interoperability and Compatibility (OIC) beim US Department of Homeland Security (DHS), dem US-Bundesministerium für Innere Sicherheit, geschaffen.[508] Das OIC betreibt selbst kein Kommunikationsnetz, sondern koordiniert die Forschung, die Ermittlung von Anforderungen und die Entwicklung im Hinblick auf solche Netze für die Notfallkommunikation. Das OIC arbeitet zur Erreichung dieser Ziele mit dem US-Handelsministerium und der FCC zusammen.

b. Institutionelle Dimension

Die Federal Communications Commission (FCC) ist eine unabhängige US-Bundesbehörde. Sie ist zuständig für die Regulierung von Breitbanddiensten, dem Wettbewerb im Bereich der Telekommunikation, Funkfrequenzen und Medien sowie für die öffentliche Sicherheit im Bereich der Telekommunikation.[509] Errichtet wurde sie auf der Grundlage des Communication Act of 1934,[510] und sie zielt im Rahmen ihrer Zuständigkeit auch auf die Gewährleistung bezahlbarer Telekommunikationsdienste oder der Notfallkommunikation im Bereich der öffentlichen Sicherheit.[511] Die FCC

506 47 CFR §§ 64.601(a)(55), 64.619.
507 6 U.S. Code § 194.
508 6 U.S. Code § 195.
509 *FCC*, What We Do, https://www.fcc.gov/about-fcc/what-we-do.
510 Communications Act of 1934, Pub. L. 73–416, 48 Stat. 1064.
511 47 U.S. Code § 151.

wirkt primär auf die technische Interoperabilität von Telekommunikationsnetzwerken hin.

Als Bundesbehörde kann die FCC auf der Grundlage des Federal Advisory Committee Act[512] Beratungsgremien einsetzen, die Empfehlungen und Ratschläge erarbeiten. Daraus gingen bereits verschiedene solcher Beratungsgremien hervor,[513] etwa der Communications Equity and Diversity Council,[514] der Empfehlungen zur Förderung der Gerechtigkeit bei der Bereitstellung von und dem diskriminierungsfreien Zugang zu digitalen Kommunikationsdiensten und -produkten für alle Menschen in den USA erarbeitet. Auch wenn die Beratungsgremien Empfehlungen erarbeiten können, bleibt die Zuständigkeit für bindende Entscheidungen und die mögliche Umsetzung der Empfehlungen bei der FCC.[515] In Beratungsgremien sind in der Regel Bürger und Experten aus Unternehmen sowie anderen US-Behörden vertreten. Die „Advisory Committees" sollen hinsichtlich der darin vertretenen Standpunkte ausgewogen besetzt sein.[516]

Der Communications Security, Reliability, and Interoperability Council (CSRIC) berät die FCC in Angelegenheiten der Sicherheit, Zuverlässigkeit, Widerstandsfähigkeit und Interoperabilität von Telekommunikationssystemen.[517] Das Gremium wird alle zwei Jahre neu besetzt und tagt zwischen zwei und vier Mal im Jahr. Auf Behördenseite benennt die FCC eine für den CSRIC verantwortliche Person, die die Sitzungen einberuft, an ihnen teilnimmt und für die Tagesordnung zuständig ist.[518] Dem CSRIC gehören zwischen 20 und 40 Experten an, die überwiegend in Unternehmen, Verbänden und US-Behörden tätig sind.[519] Der CSRIC ist in mehrere Ar-

512 Federal Advisory Committee Act (FACA) of 1972, Pub. L. 92–463, 86 Stat. 770.

513 *FCC*, Advisory Committees of the FCC, https://www.fcc.gov/about-fcc/advisory-committees-fcc.

514 *FCC*, Communications Equity and Diversity Council, https://www.fcc.gov/communications-equity-and-diversity-council.

515 5 U.S. Code § 1008(b).

516 5 U.S. Code § 1004(b)(1).

517 *FCC*, Communications Security, Reliability, and Interoperability Council, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0.

518 5 U.S. Code § 1009(e) und (f).

519 *FCC*, Communications Security, Reliability, and Interoperability Council VIII, 2.9.2022, https://www.fcc.gov/file/23761/download. Der FCC wurde von der NGO Project on Government Oversight (POGO) vorgeworfen, das CSRIC überwiegend mit Industrievertretern zu besetzen; POGO Industry Influence on an FCC Advisory Panel, 10.6.2019, https://www.pogo.org/analysis/industry-influence-on-an-fcc-advisory-panel. Diese Vorwürfe wies die FCC zurück; FCC an die US-Senatorinnen

beitsgruppen organisiert, die sich bspw. mit Notrufen und der Sicherheit in Mobilfunknetzen beschäftigen[520] und regulatorische Handlungsempfehlungen sowie konkrete technische Beschreibungen für APIs für technische Interoperabilität erarbeiten. Ein Beispiel sind Empfehlungen zu „911 Service Over WI-FI", also Notrufe über WLAN, insbesondere dann, wenn kein Mobilfunknetz verfügbar ist.[521] Diese Empfehlungen bedingen eine technische Interoperabilität von Smartphones bzw. WLAN-Zugangspunkten, um die entsprechende Notruffunktionalität zu gewährleisten.

2. EU

a. Europäischer Kodex für die elektronische Kommunikation

(1) Vorbemerkung und Überblick

Mittelpunkt des EU-Telekommunikationsrechts ist seit 2018 die Richtlinie (EU) 2018/1972. Mit ihr wurde ein Europäischer Kodex für die elektronische Kommunikation (EKEK) eingeführt.[522] Dabei handelt es sich um ein komplexes Regelwerk neuer bzw. revidierter Vorschriften für den Telekommunikationssektor als Teil eines Pakets von Telekommunikationsgesetzen, einschließlich der Verordnung (EU) 2018/1971. Mit dem EKEK wurden die ehemaligen Richtlinien 2002/19/EG, 2002/20/EG und 2002/21/EG sowie Art. 5 des Beschlusses Nr. 243/2012/EU ersetzt und aufgehoben.[523] Gegenstand der Reform war aber nicht nur eine Zusammenfassung der bisheri-

Warren und Jayapal, 3.1.2020, https://docs.fcc.gov/public/attachments/DOC-361819A1.pdf.

520 *FCC*, Communications Security, Reliability, and Interoperability Council VIII Working Groups, September 2022, https://www.fcc.gov/file/23814/download.

521 *FCC*, Communications Security, Reliability, and Interoperability Council Report on 911 Service Over WI-FI, März 2023, https://www.fcc.gov/file/25057/download.

522 Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) EU ABl. L 321 vom 17.12.2018, S. 36–214.

523 Die Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation oder auch ePrivacy-Richtlinie) ist jedoch – im Gegensatz zum ursprünglichen Richtlinienpaket von 2002, bei dem die ePrivacy-Richtlinie zwar nicht unmittelbar im Paket mit den anderen telekommunikationsrechtlichen Richtlinien, aber nach kurzer Verzögerung zur Vervollständigung und damit als Teil des „Gesamtpakets" verabschiedet worden war – nicht Teil des EKEK, obwohl sie telekommunikationsrechtliche Bezüge hat. Ihre Reform erfolgt auf gesonderte Art und Weise und wird

gen Regelungswerke unter einem einheitlichen Dach, sondern auch die Erweiterung auf neue Ziele und Aufgaben. Dazu gehörten u. a. strengere Verbraucherschutzvorschriften, etwa um den Wechsel zwischen Dienstleistungsanbietern zu erleichtern und bei gebündelten Diensten einen besseren Schutz zu bieten, die Einführung öffentlicher SMS-Warnsysteme sowie die Erweiterung des Anwendungsbereichs auf solche Telekommunikationsdienste, die über das Internet angeboten werden und keine Rufnummern verwenden (bspw. Nachrichtenanwendungen und E-Mail). Die Richtlinie musste bis zum 21. Dezember 2020 in nationales Recht umgesetzt werden.

Im vorliegenden Kontext ist es wichtig, hervorzuheben, dass das EU-Telekommunikationsrecht (weiterhin) nicht die Inhalte von Diensten, die über elektronische Kommunikationsnetze und -dienste bereitgestellt werden, wie Rundfunkinhalte und bestimmte Dienste der Informationsgesellschaft, betrifft. Es geht also um die Regulierung der Infrastruktur und nicht der Inhalte. Deshalb lässt der EKEK auch alle Maßnahmen unberührt, die auf Unionsebene oder der Ebene der Mitgliedstaaten in Bezug auf diese Dienste getroffen werden, um die kulturelle und sprachliche Vielfalt zu fördern und die Wahrung des Pluralismus der Medien sicherzustellen.[524] Die Trennung der Regulierung von elektronischer Kommunikation und Inhalten soll aber nicht die Berücksichtigung von Verbindungen zwischen den beiden – insbesondere zur Gewährleistung des Pluralismus der Medien, der kulturellen Vielfalt und des Verbraucherschutzes – beeinträchtigen. Entsprechend – und obwohl der EKEK kein Instrument der Vielfaltssicherung ist – enthält Art. 3 Abs. 1 UAbs. 2 EKEK in der Umschreibung der Zielsetzungen den Hinweis, dass die nationalen Regulierungs- und anderen zuständigen Behörden im Rahmen ihrer Aufgaben dazu beitragen sollen, dass Maßnahmen umgesetzt werden, mit denen die Freiheit der Meinungsäußerung, die Informationsfreiheit, die kulturelle und sprachliche Vielfalt und der Medienpluralismus gefördert werden.

(2) Anwendungsbereich: elektronische Kommunikationsdienste

Im Rahmen des europäischen Telekommunikationsrechts war es lange Zeit umstritten, ob und inwieweit auch solche Dienste in den Anwendungsbe-

bezüglich eines Vorschlags für eine ePrivacy-Verordnung seit langem und immer noch diskutiert.

524 Erwgr. 7.

reich fallen oder zumindest in Zukunft aufgenommen werden sollten, die über das Internet übermittelt werden.

In einem Urteil vom Juli 2019 (und damit bereits nach der Veröffentlichung des EKEK im Amtsblatt der Union) stellte etwa der EuGH auf der Basis der Vorgängerregeln klar, dass keine Signalübertragung und damit kein elektronischer Kommunikationsdienst im Sinne der Richtlinie 2002/21/EG vorliege, wenn ein E-Mail-Dienst keinen Zugang zum Internet selbst vermittle, sondern lediglich internetbasiert eine Übertragung von Kommunikationsinhalten vornehme.[525] Das betraf damals Googles Dienst Gmail und stand im Widerspruch zu der Vorstellung des vorlegenden Verwaltungsgerichts Köln und der Bundesnetzagentur unter dem deutschen Telekommunikationsgesetz. Die Bereitstellung einer Software mit einer Stimmübertragungsfunktion über Internetprotokoll (Voice over Internet Protocol, VoIP), mit der Nutzer von einem Endgerät über das öffentliche Telefonnetz eines Mitgliedstaats eine Festnetz- oder Mobilfunknummer eines nationalen Rufnummernplans anrufen können, war jedoch nur acht Tage vor jenem Urteil vom EuGH als elektronischer Kommunikationsdienst eingestuft worden. Diese Einstufung gelte jedenfalls dann, wenn zum einen dem Herausgeber der Software für die Bereitstellung dieses Dienstes ein Entgelt gezahlt werde und die Bereitstellung zum anderen den Abschluss von Vereinbarungen des Herausgebers mit für die Übertragung und die Terminierung von Anrufen in das öffentliche Telefonnetz (Public Switched Telephone Network, PSTN) ordnungsgemäß zugelassenen Telekommunikationsdienstleistern beinhalte.[526] Im konkreten Fall ging es dabei um den Dienst Skype von Microsoft.

Mit dem EKEK wurde 2018 dieser technische Ansatz durch einen funktionaleren Ansatz abgelöst, wonach unter einem elektronischen Kommunikationsdienst nunmehr folgende Dienste zu verstehen sind (Art. 2 Nr. 4 EKEK):

> *gewöhnlich gegen Entgelt über elektronische Kommunikationsnetze erbrachte Dienste, die – mit der Ausnahme von Diensten, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben – folgende Dienste umfassen:*
> *a) „Internetzugangsdienste" im Sinne der Begriffsbestimmung des Artikels 2 Absatz 2 Nummer 2 der Verordnung (EU) 2015/2120,*

525 Rs. C-193/18 – *Google LLC / Bundesrepublik Deutschland*, ECLI:EU:C:2019:498.
526 C-142/18 – *Skype Communications Sàrl / Institut belge des services postaux et des télécommunications (IBPT)*, ECLI:EU:C:2019:460.

b) interpersonelle Kommunikationsdienste und
c) Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für die Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden […].

Das Merkmal „gegen Entgelt erbracht" ist dabei nicht im Sinne einer Zahlungsbedingung zu verstehen (etwa auch in einem Lizenzpaket), sondern erfasst auch solche Fälle, in denen der Endnutzer als Bedingung für den Zugang zu dem Dienst Werbung ausgesetzt ist oder der Dienst erhobene personenbezogene Daten monetarisiert.[527]

Neben den Klarstellungen in lit. a) und lit. c) der Regelung erfasst der EKEK mit der neuen Definition nunmehr auch ausdrücklich interpersonelle Kommunikationsdienste. Art. 2 Nr. 5 EKEK definiert diese als solche Dienste, die einen direkten interpersonellen und interaktiven Informationsaustausch zwischen einer endlichen Zahl von Personen ermöglichen, wobei die Empfänger von den Personen bestimmt werden, die die Kommunikation veranlassen oder daran beteiligt sind. Das sind also bspw. Sprachanrufe, alle Arten von E-Mails, Mitteilungsdienste oder Gruppenchats. Das vormals entscheidende Merkmal der Signalübertragung spielt daher nur noch eine untergeordnete Rolle innerhalb dieser Dienste, sofern sie eine Kommunikation ermöglichen. Grund für diese Erweiterung waren vor allem die Änderungen im Nutzerverhalten, innerhalb derer vermehrt die herkömmlichen Sprachtelefonie-, Textmitteilungs- und E-Mail-Übertragungsdienste durch Internet-Telefonie, -Mitteilungsdienste und Web-gestützte E-Mail-Dienste ersetzt werden.[528] Es muss für die Eröffnung des Anwendungsbereichs eine begrenzte bzw. endliche[529] Zahl an Empfängern geben (keine Massenverbreitung) und der Dienst muss diesen auch Antwortmöglichkeiten einräumen. Nicht darunter fallen daher der lineare Rundfunk, Videoabrufdienste, Webseiten, soziale Netzwerke[530], Blogs und der Infor-

527 Erwgr. 16 EKEK.
528 Erwgr. 15 EKEK.
529 Klassische Messenger-Dienste, die offensichtlich unter diese Definition fallen sollen, können Funktionen anbieten, die einer Massenverbreitung ähneln. So lässt sich bspw. bei Telegram über die dort anlegbaren „Channels" eine prinzipiell unendliche Zahl von nicht näher bestimmten Nutzern erreichen. Dabei handelt es sich aber nur um eine Funktion von vielen, was nichts an der Anwendbarkeit des EKEK ändern dürfte. Dazu auch *Becker/Holznagel/Müller*, Interoperability of Messenger Services, S. 119, 132.
530 Etwas anderes kann unter Umständen für Messenger-Funktionen gelten, die soziale Netzwerke anbieten (bei Facebook ist der Messenger mittlerweile ein in sich

mationsaustausch zwischen Maschinen. Im Unterschied zur Telefonie nutzen solche Dienste also nicht eigene Infrastrukturen, sondern beruhen für ihre Funktionsweise auf bestehenden Infrastrukturen des Internets. Nachrichten werden dabei über verschiedene offene Kommunikationsprotokolle (bspw. XMPP, IRC oder Echo) oder unternehmenseigene Protokolle (bspw. bei WhatsApp) übermittelt und sind dabei, anders als bei sozialen Netzwerken, an einen oder mehrere auszuwählende Empfänger gerichtet.[531]

Bedeutsam ist allerdings die ebenfalls in Nr. 5 vorgesehene Ausnahme: Der EKEK erfasst keine Dienste, die eine interpersonelle und interaktive Kommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen. Erwägungsgrund 17 schlüsselt das Merkmal des „Nebendienstes" näher auf. Demnach fallen darunter solche Dienste, die aus objektiven technischen Gründen nicht ohne den Hauptdienst genutzt werden können, sofern die Integration nicht nur zur Umgehung der Regeln des EKEK dient. Als Beispiel hierfür werden Kommunikationskanäle in Online-Spielen genannt. Im Übrigen bleibt das Merkmal aber auslegungsbedürftig und eine Einzelfallprüfung entlang des jeweiligen Dienstes ist notwendig. Unbedeutend in dem Sinne soll eine Kommunikationsfunktion nämlich dann und nur dann sein, wenn sie etwa lediglich einen sehr begrenzten objektiven Nutzen für die Endnutzer aufweist und in der Realität von ihnen kaum verwendet wird. Das dürfte so eindeutig für umfangreiche Chat-Funktionen – sofern diese nicht bereits als eigenständiger Dienst angeboten werden[532] – innerhalb sozialer Netzwerke jedenfalls nicht gelten. Auch diese könnten somit unter den Begriff der elektronischen Kommunikationsdienste und damit unter die entsprechenden Pflichten fallen.

Wichtig für die Anwendung der Bestimmungen des EKEK ist zudem die Unterscheidung zwischen „nummerngebundenen interpersonellen Kommunikationsdiensten" (also solchen, die entweder eine Verbindung zu öffentlich zugeteilten Nummerierungsressourcen, nämlich zu Nummern nationaler oder internationaler Nummerierungspläne, herstellen oder die eine Kommunikation mit Nummern nationaler oder internationaler Nummerierungspläne ermöglichen) und „nummernunabhängigen interperso-

geschlossener unabhängiger Dienst), wenn diese nicht eine unbedeutende Nebenfunktion sind; dazu im Folgenden.

531 *Becker/Holznagel/Müller*, Interoperability of Messenger Services, S. 119, 121.

532 Zum Beispiel der Facebook Messenger, der als eigenständige Anwendung genutzt werden kann und nicht mehr ausschließlich im sozialen Netzwerk integriert ist.

nellen Kommunikationsdiensten“ (also solchen, die weder eine Verbindung zu öffentlich zugeteilten Nummerierungsressourcen herstellen noch die Kommunikation mit Nummern nationaler oder internationaler Nummerierungspläne ermöglichen). Während nummernunabhängige interpersonelle Kommunikationsdienste nur dann Verpflichtungen unterliegen, wenn das öffentliche Interesse bestimmte Regeln für alle Arten von interpersonellen Kommunikationsdiensten erfordert,[533] treffen nummerngebundene interpersonelle Kommunikationsdienste stärkere Pflichten nach dem EKEK, da sie – wie die herkömmlichen Telefoniedienste – am öffentlich gesicherten interoperablen Ökosystem beteiligt sind und somit auch Nutzen daraus ziehen. Die bloße Nutzung einer Nummer als Kennung sollte, ausweislich Erwägungsgrund. 18 EKEK, nicht mit der Nutzung einer Nummer zur Herstellung einer Verbindung mit öffentlich zugeteilten Nummern gleichgesetzt und daher für sich allein nicht als ausreichend betrachtet werden, um als „nummerngebunden“ zu gelten. Während daher Dienste wie Skype unter diese stärker regulierte Kategorie fallen dürften, sind die in Deutschland wie der EU meistgenutzten Messenger-Dienste wie WhatsApp oder Telegram, wenngleich hier eine Mobilfunknummer als Kennung genutzt wird, als nummernunabhängige Dienste einzuordnen.[534]

(3) Interoperabilität im EKEK

(a) Überblick

Ein grundsätzliches Ziel des EKEK ist es, Interoperabilität der elektronischen Kommunikationsdienste zu fördern.[535] Den Begriff der Interoperabilität definiert der EKEK nicht. Vielmehr wird von einem entwicklungsoffenen Konzept ausgegangen, das sich auch mit den dynamischen Märkten weiterentwickelt.[536] Es geht um die Gewährleistung der durchgehenden Konnektivität zwischen Endnutzern, womit einerseits also Verbraucherinteressen angesprochen sind.[537] Andererseits bezweckt Interoperabilität

533 Diese unterliegen daher nach dem EKEK auch keiner Allgemeingenehmigungspflicht und im Vergleich zu anderen Diensten geringeren Anforderungen in Bezug auf das zu gewährleistende Sicherheitsniveau.
534 *Becker/Holznagel/Müller*, Interoperability of Messenger Services, S. 119, 134.
535 Art. 1 Abs. 2 lit. a, Art. 3 Abs. 2 lit. c EKEK, Erwgr. 148 f. EKEK.
536 Erwgr. 305 EKEK.
537 Erwgr. 148 S. 1 EKEK.

aber auch ausdrücklich (Erwägungsgrund 149 S. 3 EKEK) den Abbau von Marktzutrittsschranken sowie von Hindernissen für weitergehende Innovationen und dient damit originär auch wettbewerblichen Zielen.[538] Die Förderung eines nachhaltigen Wettbewerbs ist auch in den Zielsetzungen des EKEK (Art. 1 Abs. 2 lit. a EKEK) verankert. Erwägungsgrund 157 lässt sich dabei entnehmen, dass ein Gleichlauf im Sinne einer effektiven Ergänzung zwischen Verbraucher- und Wettbewerbsinteressen sowie entsprechend auch eine Kooperation zwischen verschiedenen zuständigen Behörden gewollt ist, bei der jedoch die Grenzen der jeweiligen Zuständigkeiten gewahrt werden.

Konkrete Bestimmungen für die Förderung von Interoperabilität finden sich maßgeblich an zwei Stellen: Art. 61 EKEK betrifft die Konnektivität von (bestimmten) elektronischen Kommunikationsdiensten sowie die Interoperabilität von interpersonellen Kommunikationsdiensten, während Art. 113 EKEK die Interoperabilität der Autoradio- und für Verbraucher bestimmten Radio- und Digitalfernsehgeräte betrifft. Ergänzend relevante Bestimmungen bestehen zu entsprechenden behördlichen Befugnissen und im Zusammenhang mit der Normung. Die Nummernportabilität hingegen, auf die hier ebenfalls kurz eingegangen werden soll, betrifft nicht die Interoperabilität von Diensten, sondern die Erleichterung des Anbieterwechsels. Einen Beitrag zur Vielfaltssicherung können daneben auch die Must-Carry-Pflichten zur Übertragung bestimmter Hörfunk- und Fernsehkanäle nach Art. 114 EKEK bzw. deren nationale Umsetzungen leisten,[539] die aber nachfolgend nicht Gegenstand der Betrachtung im Kontext von Interoperabilität sind.[540]

(b) Konnektivität und Interoperabilität (bestimmter) elektronischer Kommunikationsdienste (Art. 61 EKEK)

Art. 61 EKEK enthält keine unmittelbaren Interoperabilitätspflichten für bestimmte Anbieter, sondern legt vielmehr entsprechende Befugnisse und

538 *Monopolkommission*, Telekommunikation 2021, S. 203.

539 Vgl. dazu eingehend auch *Ukrow/Cole*, Aktive Sicherung lokaler und regionaler Medienvielfalt, S. 97 ff.

540 Solche Übertragungspflichten sind allerdings mit vertikalen Interoperabilitätsbestimmungen insoweit vergleichbar, als sie in gewisser Weise ebenfalls einen Zugang über eine bestimmte Schnittstelle zum Endnutzer ermöglichen.

Zuständigkeiten der nationalen Regulierungsbehörden für diesen Bereich fest. Abs. 1 enthält dabei zunächst eine generelle Förderungspflicht im Hinblick auf die Ziele des EKEK: Die nationalen Regulierungsbehörden fördern bei ihren Maßnahmen zur Verwirklichung der in Art. 3 EKEK festgelegten Ziele einen angemessenen Zugang und eine geeignete Zusammenschaltung sowie die Interoperabilität der Dienste und stellen diese sicher. Sie geben insbesondere Orientierungshilfe und machen die für den Zugang und die Zusammenschaltung geltenden Verfahren öffentlich zugänglich, damit kleine und mittlere Unternehmen und Betreiber mit begrenzter geografischer Reichweite von den auferlegten Verpflichtungen profitieren können. Insoweit ist für die Umsetzung dieser Regelung im nationalen Recht die Statuierung einer allgemeinen Ermächtigung zur Verwirklichung des EKEK erforderlich.[541]

Abs. 2 enthält demgegenüber konkretere Befugnisse. Denjenigen Unternehmen, die einer Allgemeingenehmigung unterliegen und die den Zugang zu Endnutzern kontrollieren, können die Regulierungsbehörden die Verpflichtung auferlegen, ihre Netze zusammenzuschalten oder ihre Dienste interoperabel zu machen (Art. 61 Abs. 2 lit. a) und b) EKEK). Während die Zusammenschaltung von Netzen bereits Gegenstand der Vorgängerregelung in Art. 5 Abs. 1 lit. a) der Zugangsrichtlinie[542] war, ist die ausdrückliche Verankerung von Interoperabilitätspflichten abseits der allgemeinen Förderpflicht aus Abs. 1 erst durch den EKEK erfolgt. Die Möglichkeit ist begrenzt auf den erforderlichen Umfang, unterliegt also einer Beurteilungspflicht der Behörden. Einer Allgemeingenehmigung ist die Bereitstellung von elektronischen Kommunikationsnetzen oder -diensten unterworfen, für die der EKEK umfangreiche Rahmenbedingungen enthält (Art. 12 ff. EKEK) und insbesondere regelt, an welche Bedingungen eine solche Genehmigung geknüpft werden kann. Auf diese soll hier aber nicht näher eingegangen werden.[543] Hervorzuheben ist jedoch, dass nummernunabhängige interpersonelle Kommunikationsdienste, also insbesondere der Großteil

541 Dazu bereits im Blick auf die frühere Regelung EuGH Rs. C-227/07 – *Kommission / Polen*, ECLI:EU:C:2008:620 – Rn. 64 f.

542 Richtlinie 2002/19/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung (Zugangsrichtlinie), EU ABl. L 108, 24.4.2002, S. 7–20.

543 Zur Diskussion der etwas missverständlichen Formulierung zur Allgemeingenehmigung und zu den Folgen für nummernunabhängige Kommunikationsdienste vgl. auch *Becker/Holznagel/Müller*, Interoperability of Messenger Services, S. 119, 134 f.

der am häufigsten genutzten Messenger-Dienste (mit Ausnahme von Skype, das auch nummernbasiert genutzt werden kann), nach dem in den Erwägungsgründen dokumentierten Willen der EU-Gesetzgeber nicht unter die Allgemeingenehmigung fällt und daher auch nicht den Regelungen in Art. 61 Abs. 2 lit. a) und b) EKEK unterliegt.[544]

Jene Dienste wie WhatsApp oder Threema fallen „nur" unter die Regelung des Art. 61 Abs. 2 lit. c) EKEK, wonach in begründeten Fällen, in denen die „durchgehende Konnektivität zwischen Endnutzern wegen mangelnder Interoperabilität" bedroht ist, die nationalen Regulierungsbehörden auch nummernunabhängige interpersonelle Kommunikationsdienste verpflichten können, ihre Dienste interoperabel zu machen. Diese Vorschrift wurde erst mit der Reform im EKEK eingeführt. Wann von einer solchen Gefährdungslage für die Konnektivität im Binnenmarkt auszugehen ist, erläutert der EKEK nicht weiter. Als einen (aber nicht zwingenden) Faktor nennen die Erwägungsgründe eine Situation, in der nummerngebundene Dienste, also etwa die klassische Telefonie, nicht oder kaum mehr genutzt werden. Die Bestimmung gilt zudem nur für solche Dienste, die eine „nennenswerte Abdeckung und Nutzerbasis" aufweisen. Der Begriff „nennenswert" sollte so verstanden werden, dass die geografische Abdeckung und die Zahl der Endnutzer des betreffenden Anbieters eine kritische Masse im Hinblick auf das Ziel einer durchgehenden Konnektivität zwischen Endnutzern erreicht. Anbietern mit einer begrenzten Anzahl von Endnutzern oder begrenzter geografischer Abdeckung, die nur einen geringfügigen Beitrag zur Erreichung dieses Ziels leisten würden, sollten solche Interoperabilitätsverpflichtungen in der Regel nicht auferlegt werden können.[545]

Insoweit scheint zwar zunächst ein Beurteilungsspielraum für die nationalen Behörden zu verbleiben. Eine Gesamtschau der – im Vergleich zu den Regeln für elektronische Kommunikationsdienste strengeren, insbesondere von einem höheren Gefährdungsgrad für die Ziele des EKEK abhängigen – Regeln sowie der begleitenden Erwägungsgründe macht aber deutlich, dass die Auferlegung einer Interoperabilitätspflicht Ausnahme bleiben soll. Entsprechend knüpft UAbs. 2 die Möglichkeit noch an weitere Bedingungen. Eine Interoperabilitätspflicht für nummernunabhängige interpersonelle Kommunikationsdienste soll danach nämlich den zur Sicherstellung von Interoperabilität notwendigen Umfang nicht überschreiten und darf nur auferlegt werden, wenn die Kommission nach Konsultation

544 Erwgr. 44 EKEK.
545 Erwgr. 151 EKEK.

des Gremiums europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) festgestellt hat, dass die durchgehende Konnektivität zwischen Endnutzern in der gesamten Union oder in mindestens drei Mitgliedstaaten in nennenswertem Ausmaß bedroht ist, und wenn sie Durchführungsmaßnahmen erlassen hat, in denen Art und Umfang der auferlegbaren Verpflichtungen festgelegt werden. Insoweit ist also das Tätigwerden auf nationaler Ebene von der Initiative der Kommission abhängig – nationale Stellungnahmen können dabei über das GEREK erfolgen (dazu unten C.III.2.b). Daher werden auch die auslegungsbedürftigen Rechtsbegriffe der „Bedrohung der Konnektivität" und der „nennenswerten Nutzerbasis" auf der Ebene des Durchführungsrechtsakts zwar nicht konkretisierend geklärt, aber für die Umsetzungsebene im Einzelfall verbindlich festgelegt.

Hintergrund dieser Ultima-Ratio-Regel für die nummernunabhängigen Dienste war, dass derzeit die durchgehende Konnektivität und der Zugang zu Notdiensten zwar noch davon abhängen, dass die Endnutzer nummerngebundene interpersonelle Kommunikationsdienste nutzen. Künftige technische Entwicklungen bzw. eine verstärkte Nutzung nummernunabhängiger interpersoneller Kommunikationsdienste könnten allerdings eine unzureichende Interoperabilität zwischen den Kommunikationsdiensten mit nachteiligen Folgen, was etwa die Notfallkommunikation betrifft, mit sich bringen. Dies, so Erwägungsgrund 149 EKEK, könnte zu erheblichen Marktzutrittsschranken und Hindernissen für weitergehende Innovationen führen und die tatsächliche durchgehende Konnektivität zwischen Endnutzern merklich gefährden. Das wiederum spiegelt erneut die Doppelzielsetzung des EKEK zwischen Verbraucherschutz und Schutz des Wettbewerbs. Dabei ist davon auszugehen, dass der Europäischen Kommission im Rahmen ihres Durchführungsrechtsakts auch ein gewisser Beurteilungsspielraum zusteht, worauf die genannten Erwägungsgründe hindeuten.[546] In dem Rahmen wäre es daher denkbar, dass es künftig für eine durchgehende Konnektivität auch als erforderlich angesehen wird, dass stärkere Multimedia- und Gruppen-Funktionen in Diensten möglich sein müssen, die regelmäßig nur von nummernunabhängigen interpersonellen Kommunikationsdiensten umgesetzt werden können, typischerweise aber nicht im Rahmen der klassischen Telefonie.[547]

546 So auch *Monopolkommission*, Telekommunikation 2021, S. 100.
547 *Monopolkommission*, Telekommunikation 2021, S. 100.

Medienrechtlich relevant ist zudem Art. 61 Abs. 1 UAbs. 1 lit. d) EKEK. In dem Umfang, der zur Gewährleistung des Zugangs der Endnutzer zu vom Mitgliedstaat festgelegten digitalen Hörfunk- und Fernsehdiensten und damit verbundenen ergänzenden Diensten erforderlich ist, können nationale Regulierungsbehörden die Betreiber auch dazu verpflichten, zu fairen, ausgewogenen und nichtdiskriminierenden Bedingungen den Zugang zu Anwendungsprogramm-Schnittstellen (API) und zu elektronischen Programmführern (EPG) zu gewähren. Diese Regelung wurde aus Art. 5 Abs. 1 lit. b) der Zugangsrichtlinie nahezu wortgleich fortgeführt.[548] Die Regulierung von EPGs ist in den Mitgliedstaaten sehr unterschiedlich und vor allem unterschiedlich stark ausgeprägt.[549]

Im Ergebnis ist festzuhalten, dass Art. 61 EKEK eine Reihe von Interoperabilitätspflichten enthält, diese aber lediglich als Ermächtigungsnormen für potenzielle Regelungen zu solchen Pflichten gestaltet sind. Ob Interoperabilität für ausgewählte elektronische Kommunikationsdienste verbindlich gemacht wird, hängt also davon ab, ob die nationalen Regulierungsbehörden bzw. bezüglich nummernunabhängiger interpersoneller Kommunikationsdienste zudem die Kommission tätig werden. Insbesondere ist dies wiederum von einer Beurteilung der Situation im Einzelfall abhängig – nur dort, wo Konnektivität tatsächlich negativ beeinträchtigt ist, wo der Zugang zu Endnutzern kontrolliert wird oder – bei lit. c) – sich eine Bedrohungslage eingestellt hat, ist ein Einschreiten möglich, dann aber auch vor dem Hintergrund der Zielsetzung des EKEK geboten. Die Befugnisse sollen generell zurückhaltend in Anspruch genommen werden, was sich nicht nur aus der Konzeption der Regelung selbst ergibt, sondern wie erwähnt auch in den Erwägungsgründen zum Ausdruck kommt. Daher soll grundsätzlich der Verhandlungsweg mit den relevanten Akteuren zur Auflösung etwaiger Problemlagen der einseitigen Verpflichtung Vorrang haben (Erwägungsgrund 144 EKEK).

Wichtig zu betonen ist, dass die Befugnisse aus Art. 61 EKEK unabhängig von den Möglichkeiten gelten, Unternehmen mit beträchtlicher Marktmacht nach Art. 68 ff. EKEK besondere Verpflichtungen aufzuerlegen, darunter auch Nichtdiskriminierungsverpflichtungen (Art. 70 EKEK). Im Ergebnis geht Art. 61 EKEK daher im Unterschied zu den asymmetrischen

548 Dazu eingehend, insbesondere auch zu Aspekten der Verhinderung von Bottleneck-Effekten, *EAI*, IRIS Special: Regulating Access to Digital Television.

549 Dazu etwa *van der Sloot*, Due Prominence in Electronic Programme Guides, S. 33 ff.; *ders.*, in: JIPITEC, 3, 138, 2012, Rn. 1 ff.

Bestimmungen der Art. 68 ff. EKEK vom Ansatz einer symmetrischen Interoperabilitätspflicht aus.[550] Während die Feststellung einer besonderen Marktmacht im Rahmen von Art. 61 EKEK zwar nicht erforderlich ist, enthalten die Kriterien der Vorschrift aber dennoch wie gezeigt ähnliche wettbewerbliche Bezüge. Insoweit wird Art. 61 Abs. 2 lit. c EKEK auch von der GEREK als asymmetrische Regelung in einem ansonsten symmetrischen Kontext von Art. 61 aufgefasst.[551]

Nicht vergleichbar – obwohl es hier sicherlich Schnittmengen mit den Adressaten geben kann – ist die Regelung jedoch mit der Interoperabilitätspflicht für Messenger-Dienste von Gatekeepern nach Art. 7 DMA. Es bleibt daher abzuwarten, ob Art. 61 EKEK auch nach Inkrafttreten des DMA eine Praxisrelevanz behalten wird. Hypothetisch ist das denkbar, da zwar Gatekeeper-Dienste (DMA) regelmäßig die Hürde einer nennenswerten Abdeckung und Nutzerbasis (EKEK) erreichen, umgekehrt Dienste mit nennenswerter Abdeckung und Nutzerbasis aber nicht unbedingt die Schwellenwerte des DMA erreichen müssen. Es wird auch von der Initiative der Kommission abhängen, ob sie neben der Durchsetzung des DMA gegenüber Gatekeepern zudem Feststellungen der Bedrohung der Konnektivität in der Union trifft und damit den Weg für ein Tätigwerden der nationalen Regulierungsbehörden für den Telekommunikationssektor eröffnet.

(c) Interoperabilität von Autoradio-, Radio- und Digitalfernsehgeräten

Art. 113 EKEK enthält Bestimmungen zur Interoperabilität der Autoradio- und für Verbraucher bestimmten Radio- und Digitalfernsehgeräte. Unter der Rahmenrichtlinie[552] betraf dies noch die Interoperabilität „digitaler interaktiver Fernsehdienste" und stand ausdrücklich unter der Zielsetzung, „den freien Informationsfluss, die Medienpluralität und die kulturelle Vielfalt zu fördern". Diese Formulierung ist mit dem EKEK entfallen und die Vorschrift hat insgesamt eine wesentliche Umstrukturierung erfahren.

550 So auch *Becker/Holznagel/Müller*, Interoperability of Messenger Services, S. 119, 139.
551 *GEREK*, BoR (21) 85, S. 14 f.
552 Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie), EU ABl. L 108, 24.4.2002, S. 33–50.

Gemäß Abs. 1 stellen die Mitgliedstaaten die Interoperabilität der Autoradio- und für Verbraucher bestimmten Digitalfernsehgeräte gemäß Anhang XI sicher. Das betrifft einen einheitlichen Verschlüsselungsalgorithmus und unverschlüsselten Empfang für alle Verbrauchergeräte, die für den Empfang von Digitalfernsehen vorgesehen sind, offene Schnittstellenbuchsen für alle Digitalfernsehgeräte mit einer Diagonale von mehr als 30 cm und Empfänger in Autoradios, die für den Empfang von digitalem[553] terrestrischen Rundfunk geeignet sind. Die Regelung bezieht sich also auf Geräteinteroperabilität und steht vorrangig in einem (auch)[554] verbraucherschutzrechtlichen Kontext: Endnutzer sollten die Garantie der Interoperabilität aller Geräte haben, die innerhalb der Union für den Rundfunkempfang in neuen Fahrzeugen der Klasse M und den Digitalfernsehempfang verkauft werden.[555] Sie ist als verbindlicher Auftrag an die Mitgliedstaaten formuliert, beschränkt sich dabei aber auf die erwähnten Bereiche.

Abs. 2 hingegen sieht vor, dass die Mitgliedstaaten auch Maßnahmen erlassen können, die die Interoperabilität anderer für Verbraucher bestimmter Radiogeräte gewährleisten. Ergreifen die Mitgliedstaaten diese Möglichkeit, so haben sie sicherzustellen, dass sich die Auswirkungen auf den Markt für Radiogeräte von geringem Wert begrenzen und weder auf Erzeugnisse angewandt werden, bei denen der Funkempfänger nur eine reine Nebenfunktion (bspw. bei Smartphones) hat, noch auf Anlagen, die von Funkamateuren verwendet werden. Es handelt sich demnach um eine Kann-Vorschrift, deren Ergreifen dem Ermessen der Mitgliedstaaten obliegt. Ihre Einführung in den EKEK ist dennoch auch in Bezug auf Harmonisierungswirkungen bedeutsam, weil zum einen Grenzen gesetzt werden und zum anderen eine Zusammenarbeit innerhalb der verschiedenen Kooperationsmechanismen sowie ggf. im Bereich der Normung des EKEK stattfinden kann, was gerade im Kontext von Interoperabilität von Diensten relevant ist, bei der nationale Insellösungen kaum sinnvoll sind.

Abs. 3 wiederum betrifft, in Ergänzung zu Art. 113 Abs. 1 EKEK, auch Digitalfernsehgeräte, adressiert aber andere Anbieter. Mitgliedstaaten sollen die Anbieter digitaler Fernsehdienste dazu anhalten, ggf. sicherzustellen,

553 Das verhindert aber nicht, dass Autofunkempfänger in neuen Fahrzeugen auch analogen terrestrischen Rundfunk empfangen können, und hindert auch nicht die Mitgliedstaaten, entsprechende Pflichten vorzusehen. Vgl. Erwgr. 306.

554 Erwgr. 304 nennt darüber hinaus auch Interessen der öffentlichen Sicherheit, da durch Interoperabilität auch der Empfang von Notfallinformationen verbessert wird.

555 Erwgr. 303.

dass die Digitalfernsehgeräte, die sie ihren Endnutzern zur Verfügung stellen, interoperabel sind, sodass diese Digitalfernsehgeräte, soweit technisch machbar, bei einem Wechsel zu einem anderen Anbieter digitaler Fernsehdienste weiter verwendet werden können. Die hier angesprochene Interoperabilität geht über diejenige für Empfangsgeräte hinaus, da nicht allein das Vorhandensein eines gemeinsamen Verschlüsselungsalgorithmus und einer Schnittstellenbuchse gefordert wird, sondern die Interoperabilität mit Diensten, die über diese Schnittstellen bereitgestellt werden. Bereits die zurückhaltenden Formulierungen („halten an", „gegebenenfalls", „soweit technisch machbar") verdeutlichen, dass es sich hierbei weder um einen unmittelbaren Umsetzungsauftrag im Sinne einer Interoperabilitätspflicht handelt noch um eine Regelung, die für alle digitalen Fernsehdienste gleichermaßen greifen kann. Vielmehr ist Ziel der Vorschrift, die Hardware-Interoperabilität und Wechselmöglichkeiten der Verbraucher weiter zu fördern, soweit dem nicht begründete Argumente entgegenstehen.

UAbs. 2 von Art. 113 Abs. 3 EKEK formuliert hingegen einen Umsetzungsauftrag: Die Mitgliedstaaten sollen sicherstellen, dass Endnutzer bei Ablauf ihres Vertrags das Digitalfernsehgerät kostenlos und einfach zurückgeben können, es sei denn, der Anbieter weist nach, dass es mit den Digitalfernsehdiensten anderer Anbieter — einschließlich desjenigen, zu dem der Endnutzer gewechselt hat — vollständig interoperabel ist. Für eine solche Interoperabilität besteht eine gesetzliche Vermutung, wenn das Gerät harmonisierten Normen oder Teilen davon entspricht, deren Fundstellen im Amtsblatt der Europäischen Union veröffentlicht worden sind. In der Praxis werden gegenwärtig vor allem an Fernsehgeräte anschließbare digitale Decoder (sog. „Set-Top-Boxen") bereitgestellt. Insoweit, und auch wenn UAbs. 1 nur im Sinne einer Förderungspflicht zu verstehen ist, wirkt es sich nachteilig für Gerätehersteller aus, wenn sie der Interoperabilitätsobliegenheit nicht nachkommen, da sie dann mit Nachteilen bei Geräterückgaben durch Verbraucher rechnen müssen.

Insgesamt soll die vorgeschriebene Interoperabilität im Rahmen von Art. 113 EKEK eine hohe Kompatibilität von Endgeräten schaffen und in deren Folge die Möglichkeit, dass die Konvergenzentwicklung zwischen Telekommunikation, Medien und Informationstechnologien voranschreitet und damit zur Verwirklichung des Binnenmarktes beiträgt.[556] Verbraucher sollen also ermächtigt werden, unabhängig vom Übertragungsweg

556 *Janik*, in: Geppert/Schütz, § 75 TKG Rn. 2.

möglichst viele audiovisuelle Inhalte und Dienste auf möglichst vielen unterschiedlichen Endgeräten zu empfangen bzw. empfangen zu können. Während inhaltliche Ziele wie freie Meinungsäußerung, Pluralismus der Medien und kulturelle und sprachliche Vielfalt Gegenstand der audiovisuellen Politik sind,[557] dient das Telekommunikationsrecht an dieser Stelle zur Schaffung der technischen Rahmenbedingungen bzw. zur Beseitigung technischer Hürden. In diesem Zusammenhang ist die Regelung des Art. 113 EKEK auch als Entsprechung zur Zugangsregulierung im TK-Recht zu sehen: Zugangsrechte verhindern, dass technische Zugangsinformationen (bspw. die Schnittstelle von Decodern) Marktteilnehmern vorenthalten werden, obwohl sie sich als wichtige „bottlenecks" darstellen,[558] zugleich ebnet die Interoperabilitätsbestimmung den Weg dafür, dass dies auch technisch möglich und insbesondere nicht durch die Berufung auf gewerbliche Schutzrechte verhindert werden kann.

(d) Anbieterwechsel und Nummernportabilität

Art. 106 EKEK enthält umfassende Garantien, dass eine Portierung von Rufnummern im Falle eines Anbieterwechsels auf entsprechenden Verbraucherwunsch sicherzustellen ist und einfach, schnell und kostenangemessen erfolgen kann. Rufnummern werden grundsätzlich zunächst den Telekommunikationsunternehmen zugewiesen, die diese Nummern wiederum ihren Kunden zuweisen. Im Fall des Anbieterwechsels bedeutet dies, dass die Rufnummer quasi mit dem Kunden an einen anderen Dienst übertragen werden muss. Das ist dem Grunde nach vergleichbar mit der Datenportabilität (dazu unten, C.IV) von einem Verarbeiter zu einem anderen, ist aber weniger komplex – erfasst ist nur die öffentlich zugewiesene Rufnummer – und betrifft eher organisatorische sowie Kostenfragen.

Die Einführung der Nummernübertragbarkeit im Telekommunikationssektor hat den Wettbewerb verbessert, die Wechselkosten reduziert[559] und damit einer Negativentwicklung, namentlich Lock-in-Effekten wegen der Bindung an eine Rufnummer, entgegengewirkt, wie dies auch im Kontext von Interoperabilitätserwägungen eine Rolle spielt. Dieses Ziel konnte

557 Erwgr. 7 EKEK.
558 *Janik*, in: Geppert/Schütz, § 75 TKG Rn. 3.
559 Vgl. dazu eingehend *Cho/Ferreira/Telang*, The Impact of Mobile Number Portability on Price, Competition and Consumer Welfare.

allerdings vergleichsweise einfach gewährleistet werden, da mit der Standardisierung von Rufnummern und wesentlich ähnlichen Prozessen bei allen Anbietern im Telekommunikationssektor bereits ein „interoperabler" Grundbaustein vorhanden war, auf dem die Nummernportabilität aufbauen konnte. Die Übertragung dieser Regeln und der damit verbundenen positiven Folgen auf andere Sektoren oder Dienste wäre deutlich komplexer. Bereits bei den nummernunabhängigen Messenger-Diensten, die im Ergebnis ähnliche Funktionen bieten wie die Telekommunikation, bestehen solche einheitlichen Standards nicht, insbesondere keine einheitlichen Rufnummern aus öffentlichen Nummernregistern. Vielmehr arbeiten diese Dienste regelmäßig auf der Basis unterschiedlicher Technologien und weisen ihren Nutzern selbst bestimmte Nummern oder „IDs" zu, über die sie von anderen Nutzern erreicht werden können. Noch komplexer wäre eine solche Nummernübertragbarkeit, die man bspw. mit einer „Profilübertragbarkeit" bei sozialen Netzwerken oder in Mediatheken vergleichen könnte, im Mediensektor. Hier würde es eher um Datenportabilität gehen, die in der Praxis vor anderen Herausforderungen steht.[560]

(e) Normung und Spezifizierung

Der EKEK ist auf der Prämisse aufgebaut, dass die Normung ein wichtiges Element für ein harmonisiertes und kompatibles Telekommunikationsrecht auf Unionsebene ist. Die Normung sollte dabei in erster Linie ein marktorientierter Vorgang sein. Diese Ausrichtung wird aber an bestimmten Stellen durchbrochen und die Einhaltung bestimmter Normen auf Unionsebene gefordert. Das ist insbesondere dann der Fall, wenn es um die Verbesserung der Interoperabilität, der Wahlfreiheit der Nutzer und der Interkonnektivität im Binnenmarkt geht.

Gemäß Art. 39 Abs. 1 EKEK erstellt die Europäische Kommission ein Verzeichnis von nicht zwingenden Normen oder Spezifikationen als Grundlage für die Förderung einer einheitlichen Bereitstellung elektronischer Kommunikationsnetze und -dienste, wobei sie bei Bedarf die europäischen Normungsorganisationen (Europäisches Komitee für Normung (CEN), Europäisches Komitee für elektronische Normung (Cenelec) und Europäisches Institut für Telekommunikationsnormen (ETSI)) einbezie-

560 Eingehend für das Recht nach Art. 20 DS-GVO unten C.IV.2.a

hen kann. Dieses Verzeichnis wurde zuletzt 2008 aktualisiert.[561] Es enthält bspw. auch verschiedene Normungen und Spezifizierungen für Rundfunkdienste, was etwa technische Schnittstellen oder Dienstmerkmale betrifft.[562] Die Mitgliedstaaten sollen die Anwendung dieser Normen insbesondere dann fördern, wenn sie unbedingt notwendig ist, um die Interoperabilität zu gewährleisten (Abs. 2). Gibt es keine von der Kommission veröffentlichten Normen, gilt diese Förderpflicht in Bezug auf die Anwendung der Normen der CEN, Cenelec und ETSI und, wenn auch solche nicht existieren, in Bezug auf Normen oder Empfehlungen internationaler Einrichtungen.

Werden diese Normen nicht ordnungsgemäß angewandt und führt dies dazu, dass die Interoperabilität der Dienste in einem oder mehreren Mitgliedstaaten nicht gewährleistet ist, so hat die Kommission unter den Voraussetzungen der Art. 39 Abs. 4 i. V. m. Art. 118 Abs. 4 EKEK i. V. m. Art. 5 der Verordnung 182/2011/EU[563] die Möglichkeit, sie verbindlich festzuschreiben.[564] Das erfolgt im Komitologieverfahren, d. h. unter Beteiligung der Mitgliedstaaten im Ausschussverfahren. Aufgrund dieser Möglichkeit ist die Normung nicht nur für die Umsetzung von möglicherweise durch nationale Regulierungsbehörden auferlegten Interoperabilitätspflichten relevant, sondern kann generell als eine Art Vorstufe zur Auferlegung von Interoperabilitätspflichten angesehen werden. Die freiwillige Orientierung von Anbietern an solchen Normen, auch wenn sie (noch) keiner Interoperabilitätspflicht unterliegen, und die technische Hilfestellung dadurch könnten so auch Anreize aus der Industrie heraus schaffen.[565]

---

561 Entscheidung der Kommission vom 11. Dezember 2006 über das Verzeichnis der Normen und Spezifikationen für elektronische Kommunikationsnetze und -dienste sowie zugehörige Einrichtungen und Dienste, ersetzt alle vorherigen Fassungen, EU ABl. L 086, 27.3.2007, S. 11, zuletzt geändert durch Entscheidung der Kommission vom 17. März 2008 (EU ABl. L 93, 4.4.2008, S. 24), konsolidierte Fassung abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1704812837371&uri=CELEX%3A02007D0176-20080404.

562 Bspw. die ETSI TS 101 993 für Digital Audio Broadcasting (DAB) in Bezug auf Java-Spezifikationen.

563 Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren, EU ABl. L 55 vom 28.2.2011, S. 13–18.

564 Im aktuellen Verzeichnis sind keine verbindlichen Normen festgehalten.

565 Vgl. dazu aber auch *Monopolkommission*, Telekommunikation 2021, S. 105, die darauf hinweist, dass die Existenz von Normen im Bereich der nummernunabhängigen ITD (z. B. XMPP) bislang jedoch nicht dazu geführt habe, dass sich Unternehmen auf einen einheitlichen Branchenstandard geeinigt hätten.

Sowohl Art. 61 EKEK als auch Art. 113 EKEK knüpfen unmittelbar an die Normung an. Nach Art. 61 Abs. 2 UAbs. 2 ii) EKEK können etwa die Maßnahmen der nationalen Regulierungsbehörden gegenüber nummernunabhängigen interpersonellen Kommunikationsdiensten auch verhältnismäßige Verpflichtungen einschließen, Normen oder Spezifikationen gemäß Art. 39 Abs. 1 EKEK oder andere einschlägige europäische oder internationale Normen anzuwenden oder umzusetzen. Erwägungsgrund 303 weist in Bezug auf Art. 113 EKEK weiter darauf hin, dass die Mitgliedstaaten in der Lage sein sollten, ein Mindestmaß an harmonisierten Normen für solche Geräte vorzuschreiben. Diese Normen könnten von Zeit zu Zeit entsprechend der Weiterentwicklung der Technik und des Markts angepasst werden. Erwägungsgrund 305 geht noch einen Schritt weiter und stellt fest, dass auch die Normungsorganisationen sich dafür einsetzen sollten, eine Weiterentwicklung geeigneter Normen parallel zu den betreffenden Technologien zu gewährleisten. Für die Darstellung und Präsentation vernetzter Fernsehdienste sei die Herausbildung einer gemeinsamen Norm durch die Marktteilnehmer für die Verbraucher von Vorteil. Im Rahmen der Verträge sollten die Mitgliedstaaten und die Kommission politische Initiativen zur Förderung dieser Entwicklung ergreifen können.

b. Institutionelle Dimension

(1) Nationale Regulierungsbehörden

Im Rahmen des EKEK haben die Mitgliedstaaten sicherzustellen, dass jede der im EKEK festgelegten Aufgaben von einer zuständigen Behörde wahrgenommen wird.[566] Hierzu werden auch Regeln zur Unabhängigkeit der nationalen Regulierungsbehörden und anderer zuständiger Behörden (Art. 6 EKEK), zur Ernennung und Entlassung von Mitgliedern (Art. 7 EKEK), zur politischen Unabhängigkeit (Art. 8 EKEK), zu einer Rechenschaftspflicht und zur Mittelausstattung der nationalen Regulierungsbehörden (Art. 9 EKEK) festgelegt. Dabei haben die nationalen Regulierungsbehörden, wie Art. 3 Abs. 1 UAbs. 2 EKEK ausdrücklich statuiert, im Rahmen ihrer Zuständigkeiten dazu beizutragen, die Umsetzung von Maßnahmen zur Förderung der Meinungs- und Informationsfreiheit, der kulturellen

566 Dazu und zum Folgenden auch *Cole/Etteldorf*, Future Regulation of Cross-border Audiovisual Content Dissemination, S. 183 ff.

und sprachlichen Vielfalt sowie des Medienpluralismus zu gewährleisten. Die Verbindung zum Mediensektor wird hier also anerkannt, aber als getrennt von Infrastrukturregulierung zu betrachtende Inhalteregulierung gesehen, wobei ein harmonisches Zusammenspiel angestrebt wird.[567]

Auch zum Wettbewerbsrecht bestehen Schnittmengen, insbesondere was die Regeln über die Auferlegung von besonderen Pflichten an marktmächtige Unternehmen betrifft. Angesichts möglicher sektorübergreifender Strukturen auf nationaler Ebene können die Mitgliedstaaten daher auch den nationalen Regulierungsbehörden weitere im EKEK und im sonstigen Unionsrecht vorgesehene Aufgaben übertragen, insbesondere solche, die den Wettbewerb oder den Marktzutritt betreffen. Werden diese Aufgaben im Zusammenhang mit dem Wettbewerb oder dem Marktzugang anderen zuständigen Behörden zugewiesen, so bemühen sich diese, die nationale Regulierungsbehörde zu konsultieren, bevor sie eine Entscheidung treffen.

Der EKEK weist den Behörden eine Bandbreite an Aufgaben und Befugnissen zu, die die Mitgliedstaaten zu gewährleisten haben. Daneben enthält er in spezifischen Vorschriften weitere Sonderbefugnisse. Im Rahmen von Art. 61 EKEK sind es insbesondere die nationalen Behörden, die berechtigt sind, Interoperabilitätspflichten aufzuerlegen. Das erfasst auch konkrete Bedingungen, wie Interoperabilität herzustellen ist, sodass insoweit die nationalen Regulierungsbehörden die Umsetzung auch durch Leitvorgaben steuern können.[568] Hierbei sind sie an die Kriterien der Objektivität, Transparenz, Verhältnismäßigkeit und Diskriminierungsfreiheit gebunden. Sie haben spezielle im EKEK vorgesehene verfahrensrechtliche Bestimmungen einzuhalten wie etwa Konsultations- und Transparenzpflichten (Art. 23 EKEK).

In Bezug auf den Erlass von Verpflichtungen im Rahmen von Art. 61 EKEK haben die zuständigen nationalen Behörden zunächst gemäß Art. 32 Abs. 3 EKEK einen Maßnahmenentwurf an die Kommission, das GEREK und die nationalen Regulierungsbehörden der anderen Mitgliedstaaten unter Angabe der Gründe für die Maßnahme zu übermitteln, die dann innerhalb eines Monats Stellung nehmen können.[569] Diesen Stellungnahmen hat die nationale Regulierungsbehörde beim finalen Erlass von Maßnahmen „weitestmöglich" Rechnung zu tragen (Art. 32 Abs. 8 EKEK). Ist die Kom-

567 Erwgr. 7 EKEK.

568 Dazu auch *Becker/Holznagel/Müller*, Interoperability of Messenger Services, S. 119, 140.

569 Ausnahmen sind für ein Dringlichkeitsverfahren nach Art. 32 Abs. 8 EKEK vorgesehen.

mission allerdings der Ansicht, dass die Maßnahme ein Hemmnis für den Binnenmarkt begründen würde oder unvereinbar mit dem Unionsrecht sei, kann sie sie einfrieren (Art. 33 Abs. 1 EKEK). In dem Fall kommt es innerhalb von drei Monaten zu einem Verfahren, in dem GEREK, nationale Behörde und Kommission unter Berücksichtigung der Ansichten von Marktteilnehmern eng zusammenarbeiten, um eine geeignete(re) Lösung zu finden. Das GEREK hat in dem Rahmen auch eine Stellungnahme abzugeben. Die Kommission kann binnen eines Monats nach Ablauf des Dreimonatszeitraums und unter weitestmöglicher Berücksichtigung der Stellungnahme des GEREK entweder

- eine Empfehlung abgeben, in der die betreffende nationale Regulierungsbehörde aufgefordert wird, den Maßnahmenentwurf zu ändern oder zurückzuziehen, wobei die Kommission auch entsprechende konkrete Vorschläge macht und die Gründe für diese Empfehlung nennt, insbesondere wenn das GEREK die ernsten Bedenken der Kommission nicht teilt; oder
- beschließen, ihre Vorbehalte zurückzuziehen; oder
- für Maßnahmenentwürfe nach Art. 61 Abs. 3 EKEK einen Beschluss erlassen, in dem sie die nationale Regulierungsbehörde auffordert, den Maßnahmenentwurf zurückzuziehen, wenn das GEREK die ernsten Bedenken der Kommission teilt.

Eine rechtliche Verbindlichkeit dieser Maßnahmen der Kommission legt der EKEK zwar nicht fest. Die nationale Regulierungsbehörde trifft jedoch eine Begründungspflicht, wenn sie davon abweicht.

(2) Zusammenarbeit im GEREK und Rolle der Kommission

Das supranationale Kooperationsgremium für nationale Aufsichtsbehörden im Bereich der elektronischen Kommunikation ist das GEREK.[570] Dieses Gremium existierte bereits zuvor,[571] wurde aber durch die Verordnung

570 Dazu und zum Folgenden auch *Cole/Etteldorf*, Future Regulation of Cross-border Audiovisual Content Dissemination, S. 186 ff.

571 Vgl. Verordnung (EG) Nr. 1211/2009 des Europäischen Parlaments und des Rates vom 25. November 2009 zur Einrichtung des Gremiums Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) und des Büros, EU ABl. L 337 vom 18.12.2009, S. 1–10.

(EU) 2018/1971[572] förmlich eingerichtet. Das GEREK besteht aus einem Board der Regulierungsbehörden und verschiedenen Arbeitsgruppen. Das Board setzt sich aus einem Mitglied aus jedem Mitgliedstaat zusammen, das von der nationalen Regulierungsbehörde ernannt wird, die die Hauptverantwortung für die Beaufsichtigung unter dem EKEK trägt. In Bezug auf andere Behörden, die im Rahmen des EKEK mit bestimmten Aufgaben betraut sind, sieht Art. 5 Abs. 1 UAbs. 2 EKEK vor, dass die nationalen Regulierungsbehörden berechtigt sind, die erforderlichen Daten und sonstigen Informationen von den Marktteilnehmern einzuholen, um einen Beitrag zur Erfüllung der Aufgaben des GEREK zu leisten.

Die Kommission nimmt an allen Beratungen des Boards teil, hat jedoch kein Stimmrecht. Art. 8 der Verordnung (EU) 2018/1971 enthält eine Bestimmung zur Unabhängigkeit: Bei der Wahrnehmung der ihm übertragenen Aufgaben und unbeschadet der Tatsache, dass seine Mitglieder im Namen ihrer jeweiligen nationalen Regulierungsbehörden handeln, handelt das Board unabhängig und objektiv im Interesse der Union, ungeachtet etwaiger nationaler oder persönlicher Einzelinteressen, und die Mitglieder des Regulierungsrats und ihre Stellvertreter dürfen Weisungen von Regierungen, Organen, Personen oder Stellen (unbeschadet der Koordinierung) weder anfordern noch entgegennehmen.

Art. 10 EKEK verknüpft den gesamten EKEK eng mit dem GEREK. Insbesondere sollen die Mitgliedstaaten dafür sorgen, dass die nationalen Regulierungsbehörden die Leitlinien, Stellungnahmen, Empfehlungen, gemeinsamen Standpunkte, bewährten Verfahren und Methoden des GEREK bei der Annahme ihrer eigenen Entscheidungen für ihre nationalen Märkte weitestgehend berücksichtigen. Auch die einzelnen Bestimmungen des EKEK sehen wiederholt eine zentrale Rolle für das GEREK in den Verfahren vor, insbesondere bei den verschiedenen Kooperationsmechanismen und der Entwicklung von Leitlinien für die einheitliche Anwendung des EKEK. Daraus ergeben sich jedoch in der Regel keine verbindlichen Befugnisse des GEREK – weder gegenüber den nationalen Regulierungsbehörden noch gegenüber der Kommission.

572 Verordnung (EU) 2018/1971 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 zur Einrichtung des Gremiums europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) und der Agentur zur Unterstützung des GEREK (GEREK-Büro), zur Änderung der Verordnung (EU) 2015/2120 und zur Aufhebung der Verordnung (EG) Nr. 1211/2009, EU ABl. L 321 vom 17.12.2018, S. 1–35.

Auch im Rahmen der Interoperabilitätsbestimmungen, insbesondere der Bestimmungen zu nummernunabhängigen interpersonellen Kommunikationsdiensten, spielt das GEREK eine Rolle neben der Europäischen Kommission. Wie oben angesprochen, können diesen Diensten Interoperabilitätspflichten nur dann auferlegt werden, wenn die Kommission nach Konsultation des GEREK und unter weitestmöglicher Berücksichtigung seiner Stellungnahme festgestellt hat, dass die durchgehende Konnektivität zwischen Endnutzern in der gesamten Union oder in mindestens drei Mitgliedstaaten in nennenswertem Ausmaß bedroht ist. Wenn solche Interoperabilitätsprobleme auftreten, kann die Kommission beim GEREK einen Bericht anfordern, in dem die Sachlage auf dem betreffenden Markt auf Unions- und auf mitgliedstaatlicher Ebene bewertet wird. Erst auf dieser Basis entscheidet sie, ob ein regulierendes Eingreifen der nationalen Regulierungsbehörden erforderlich ist. In dem Fall erlässt sie Durchführungsmaßnahmen, in denen Art und Umfang etwaiger Regulierungsmaßnahmen der nationalen Regulierungsbehörden festgelegt werden, wozu auch Verpflichtungen zur Veröffentlichung und Genehmigung der Nutzung, Änderung und Weiterverbreitung relevanter Informationen durch die Behörden und andere Anbieter sowie Maßnahmen zählen, die alle oder bestimmte Betreiber zur Anwendung von Normen oder Spezifikationen verpflichten.

c. Verhältnis zum DMA

Obwohl sowohl DMA als auch EKEK Interoperabilitätspflichten für elektronische Kommunikationsdienste enthalten (können), weisen sie doch Unterschiede auf.[573]

Zunächst können elektronische Kommunikationsdienste in Form von nummernunabhängigen interpersonellen Kommunikationsdiensten unter beide Regime fallen. Nach Art. 1 Abs. 3 DMA fallen zwar Märkte im Zusammenhang mit elektronischen Kommunikationsdiensten nach Art. 2 Nr. 4 EKEK nicht in den Anwendungsbereich des DMA, ausgenommen davon sind aber ausdrücklich nummernunabhängige interpersonelle Kommunikationsdienste. Der DMA gilt insbesondere also dann, wenn diese Dienste Teil eines Plattformökosystems sind, das der DMA vorrangig im Blick hat.[574] Beim DMA ist das abhängig von einer Benennung als Gate-

573 Vgl. hierzu und zum Folgenden auch eingehend *GEREK*, BoR (21) 85.
574 Erwgr. 64 DMA.

keeper, die an die oben dargestellten (asymmetrischen) Bedingungen von Art. 3 DMA geknüpft ist, während der EKEK zunächst (symmetrisch) alle elektronischen Kommunikationsdienste erfasst. Auch in Bezug auf die Interoperabilitätspflichten bestehen Unterschiede: Während der DMA ex ante generell Gatekeepern solche Pflichten ohne einen weiteren notwendigen regulatorischen Schritt auferlegt, ist deren Ergreifen in Art. 61 EKEK von einer Entscheidung der nationalen Regulierungsbehörden abhängig; während der DMA Bedingungen zur Ausgestaltung schon bereithält und Interoperabilität von einem Antrag von Nicht-Gatekeeper-Diensten abhängig macht, wäre die Ausgestaltung unter dem EKEK Vorgaben von Regulierungsbehörden überlassen.

Schnittmengen liegen dabei auf der Hand. Das gilt insbesondere für die beiden ähnlichen, asymmetrischen[575] Instrumente in Art. 61 Abs. 2 lit. c) EKEK und Art. 7 DMA bezüglich der Interoperabilität von nummernunabhängigen interpersonellen Kommunikationsdiensten von Gatekeepern wie den bereits benannten Diensten WhatsApp und Messenger (beides Meta). Diese fallen unter die Pflichten nach Art. 7 DMA, könnten aber auch von Maßnahmen zur Herstellung von Interoperabilität nach Art. 61 Abs. 2 lit. c) EKEK erfasst werden. Während die Kommission die Dienste bereits unter dem DMA benannt und damit auch festgestellt hat, dass sie essenzielles Zugangstor im Binnenmarkt sind, hat sie eine Gefährdung der Interkonnektivität im Binnenmarkt durch diese Dienste, wie sie für Interoperabilitätspflichten nach dem EKEK erforderlich wäre, aber noch nicht angenommen. Gerade für diese Dienste läge das aber nahe, wie sich aus den Ausführungen in den Benennungsentscheidungen ergibt, obwohl diese Benennungen an anderen Kriterien gemessen werden. Es bleibt daher abzuwarten, ob die Kommission erst die Effektivität der neuen Regeln des DMA abwartet oder zusätzlich auch den Weg des EKEK in Bezug auf Interoperabilität beschreitet, der auch andere Angebote treffen könnte (Bedrohung der Interkonnektivität „nur" in drei Mitgliedstaaten). Möglich wäre es, da der DMA dem jedenfalls nicht entgegensteht: Nach Art. 1 Abs. 4 DMA berührt Art. 7 DMA nämlich nicht die Befugnisse und Zuständigkeiten, die den nationalen Regulierungsbehörden und anderen zuständigen Behörden nach Art. 61 EKEK übertragen werden. Auch Erwägungsgrund 64 spricht davon, dass die Interoperabilitätspflichten nach dem DMA „unbeschadet" der Möglichkeiten aus dem EKEK gelten.

575 Zur Einordnung von Art. 61 EKEK in dieser Hinsicht vgl. bereits oben, C.III.2.a(3)(b).

Solche „unbeschadet"-Formulierungen stoßen aber dort an ihre Grenzen, wo sich konkrete Pflichten aus Art. 7 DMA und Maßnahmen nach Art. 61 EKEK nicht mehr decken und ggf. Letztere über Erstere hinausgehen. Insoweit hat sich das GEREK auch ausdrücklich für eine eingehende Analyse der Beziehung der beiden Rechtsinstrumente ausgesprochen sowie für die Aufnahme von engen Kooperationsregeln zwischen Kommission und GEREK, wenn es um das Ergreifen von Maßnahmen gegen elektronische Kommunikationsdienste geht.[576] Dem wurde zumindest begrenzt im DMA Rechnung getragen: Das GEREK ist einerseits Teil der Hochrangigen Expertengruppe, die die Kommission berät, andererseits sollte die Kommission „gegebenenfalls" das GEREK konsultieren „können", um festzustellen, ob die in dem Referenzangebot, das der Torwächter innerhalb von Art. 7 DMA verwenden möchte oder verwendet hat, veröffentlichten technischen Einzelheiten und allgemeinen Bedingungen die Einhaltung der Interoperabilitätspflicht gewährleisten (Erwägungsgrund 64 DMA). Da beide Instrumente noch nicht umfassend in der Praxis Anwendung gefunden haben, lässt sich zum derzeitigen Zeitpunkt noch keine Einschätzung treffen, ob und inwieweit sich DMA und EKEK in der Hinsicht wie beabsichtigt ergänzen oder praktisch eventuell behindern. Die restriktiven Regelungen des Art. 61 Abs. 2 lit. c) EKEK, die ein Eingreifen nur unter strengen Voraussetzungen vorsehen, stehen zu den Ex-ante-Regelungen des DMA aber zumindest in einem Spannungsverhältnis.[577]

3. Deutschland

a. Telekommunikationsgesetz

(1) Überblick

Wichtigste Rechtsgrundlage des deutschen Telekommunikationsrechts ist das Telekommunikationsgesetz (TKG).[578] Interoperabilität wird darin an mehreren Stellen aufgegriffen. TK-Regulierung soll zunächst nach § 2 Abs. 2 Nr. 4 TKG als generelle Zielsetzung u.a. die Interoperabilität europaweiter Dienste und die durchgehende Konnektivität fördern. Auch im Rahmen

576 *GEREK*, BoR (21) 85, S. 19 f.
577 *WIK-Consult*, Interoperabilitätsvorschriften für digitale Dienste, S. 38.
578 Telekommunikationsgesetz vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch Art. 5 des Gesetzes vom 14. März 2023 (BGBl. 2023 I Nr. 71) geändert worden ist.

der besonderen Ziele der Frequenzregulierung (§ 86 Abs. 1 Nr. 4 TKG) wird auf Interoperabilität Bezug genommen: Ziel ist hier (auch) die Förderung der Harmonisierung der Frequenznutzung für Telekommunikationsnetze und -dienste in der EU, um deren effizienten und störungsfreien Einsatz zu gewährleisten und um Vorteile für die Verbraucher, etwa durch Wettbewerb, größenbedingte Kostenvorteile und Interoperabilität der Dienste und Netze, zu erzielen.

Darüber hinaus finden sich insbesondere die folgenden Anknüpfungspunkte für Interoperabilität im TKG. Das betrifft die Hardware-Interoperabilität in Bezug auf Fernseh- und Radiogeräte (§ 75 TKG) und Regeln für Telekommunikationsdienste, wozu eine Regelung zu Verhandlungen der Anbieter über Zugang und Zusammenschaltung (§ 20 TKKG) auf der einen Seite und auf der anderen Seite die Befugnisse der Bundesnetzagentur (BNetzA) gehören, Interoperabilitätspflichten anzuordnen. Die BNetzA kann entweder im Wege der „klassischen Marktregulierung" nach § 26 TKG gegen Unternehmen beträchtlicher Marktmacht Anordnungen treffen, wenn eine solche Marktposition in einem förmlichen Verfahren festgestellt worden ist, oder nach § 21 TKG gegen Unternehmen vorgehen, die den Zugang zu Endnutzern kontrollieren, was auch auf marktmachtrelevante Faktoren Bezug nimmt, aber nicht identisch mit dem Begriff der Marktmacht ist und keine entsprechende Feststellung in einem förmlichen Verfahren voraussetzt.[579]

Mit dem Telekommunikationsmodernisierungsgesetz vom 23. Juni 2021 (TK-ModG),[580] das am 1. Dezember 2021 in Kraft getreten ist, wurde der EKEK in nationales Recht umgesetzt. Ein Element dieser umfassenden Modernisierung (im Fokus standen Genehmigungsverfahren, Frequenzpolitik und Verbraucherschutz) war auch die rechtssichere Einbindung nummernunabhängiger interpersoneller Telekommunikationsdienste in den Anwendungsbereich des TKG. Zuvor war umstritten, ob und welche internetbasierten und nummernunabhängigen Dienste als „Telekommunikationsdienst" im Sinne des TKG und welche als Telemediendienste im Sinne des TMG einzuordnen sind.[581] Diese Unklarheit hatte letztlich zur bereits

579 Dazu und zum Folgenden auch *Monopolkommission*, Telekommunikation 2021, S. 98 ff.

580 Gesetz zur Umsetzung der Richtlinie (EU) 2018/1972 des europäischen Parlaments und des Rates vom 11. Dezember 201 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts vom 23. Juni 2021, BGBl. 2021 I Nr. 35.

581 Dazu *BT-WD*, Regulierung von Messengerdiensten, S. 8 m. w. N.

erwähnten Klärung durch den EuGH in Bezug auf den Dienst Gmail geführt.[582] Mit dem TK-ModG übernimmt das deutsche Recht nun die Formulierung aus dem EKEK, mit Ausnahme der unterschiedlichen Begrifflichkeiten des „Telekommunikationsdienstes" statt des „elektronischen Kommunikationsdienstes".

Entsprechend den europäischen Vorgaben ist aber auch der deutsche Gesetzgeber in Bezug auf die Regulierung solcher Telekommunikationsdienste zurückhaltend. Diese sollen insgesamt nur dann Verpflichtungen unterliegen, wenn die Anwendung spezifischer regulatorischer Verpflichtungen auf alle Arten von interpersonellen Telekommunikationsdiensten im öffentlichen Interesse liegt, unabhängig davon, ob sie bei der Bereitstellung ihres Dienstes Nummern nutzen. Demgemäß finden – neben Vorgaben zur Interoperabilität – vornehmlich Regelungen aus dem Teil Kundenschutz und dem Abschnitt Öffentliche Sicherheit Anwendung auch auf nummernunabhängige interpersonelle Telekommunikationsdienste.[583] Da die Regeln des TKG insgesamt vornehmlich eine Umsetzung des EKEK darstellen, der oben bereits eingehend dargestellt wurde, soll nachfolgend nur auf Besonderheiten in der deutschen Regelung eingegangen werden.

(2) Zugang und Zusammenschaltung (§ 20 TKG)

Nach § 20 Abs. 1 TKG sind Betreiber öffentlicher Telekommunikationsnetze berechtigt und auf Verlangen anderer Unternehmen verpflichtet, mit diesen über ein Angebot auf Zugang und Zusammenschaltung zu verhandeln, um die Kommunikation der Nutzer, die Bereitstellung von Telekommunikationsdiensten sowie deren Interoperabilität im gesamten Gebiet der EU zu gewährleisten.

Die Regelung statuiert damit lediglich ein Verhandlungsrecht bzw. eine Verhandlungspflicht, nicht aber etwa ein Einigungsgebot.[584] Die BNetzA als zuständige Regulierungsbehörde kann auf Antrag Beteiligter als neutraler Vermittler in den Verhandlungen eingesetzt werden, sofern die Wettbewerbslage dies erfordert. Ein (bestimmtes) Verhandlungsergebnis im Sinne der verbindlichen Zugangseröffnung oder Zusammenschaltung kann nach dieser Vorschrift aber auch durch die BNetzA nicht erzwungen werden.

582 Rs. C-193/18 – *Google LLC / Bundesrepublik Deutschland*, ECLI:EU:C:2019:498.
583 Vgl. hierzu die Gesetzesbegründung BT-Drs. 19/26108, S. 234.
584 Vgl. zur Klarstellung dieser Bedeutung im TKModG auch die Gesetzesbegründung BT-Drs. 19/26108, S. 257.

Hierfür sind vielmehr die weiteren regulatorischen Befugnisse heranzuziehen.

(3) Zugangsverpflichtung und Zusammenschaltung bei Kontrolle über Zugang zu Endnutzern (§ 21 TKG)

§ 21 TKG setzt die Regeln des § 61 EKEK um, ist in seiner Untergliederung aber übersichtlicher als das EU-Vorbild. Nach § 21 Abs. 1 TKG kann die BNetzA Unternehmen, die den Zugang zu Endnutzern kontrollieren, (1.) verpflichten, ihre Telekommunikationsnetze mit denen anderer Unternehmen zusammenzuschalten, soweit dies erforderlich ist, um die durchgehende Konnektivität und die Bereitstellung von Diensten sowie deren Interoperabilität zu gewährleisten, oder ihnen (2.) weitere Verpflichtungen auferlegen, soweit dies zur Gewährleistung der durchgehenden Konnektivität oder zur Gewährleistung der Interoperabilität erforderlich ist. Damit werden Art. 61 Abs. 2 lit. a) und b) EKEK umgesetzt, wobei die Formulierung im TKG weniger „auffordernd" ist als im EKEK (dort: „ihre Dienste interoperabel zu machen"), sich aber in der Befugnis inhaltlich deckt. Mit dem TK-ModG wurde aus dieser Bestimmung (ehemals § 18 TKG a. F.) der Zusatz „auf entsprechende Nachfrage" gestrichen, sodass deutlich wird, dass die BNetzA auch von Amts wegen tätig werden kann, wie es Art. 61 Abs. 6 EKEK vorsieht. In Bezug auf die Bedingung des Kontrollierens eines Zugangs für Endnutzer wurde die Formulierung des EKEK übernommen, sodass die obigen Ausführungen entsprechend gelten. Die Gesetzesbegründung weist darauf hin, dass die Feststellung einer beträchtlichen Marktmacht keine Voraussetzung hierfür bildet.[585]

§ 21 Abs. 2 TKG enthält die Umsetzung von Art. 61 Abs. 2 lit. c) EKEK in Bezug auf die Interoperabilität nummernunabhängiger interpersoneller (Tele-)Kommunikationsdienste. Die BNetzA kann die Anbieter solcher Dienste, darunter auch Messenger-Dienste, verpflichten, ihre Dienste interoperabel zu machen, wenn (1.) der Dienst eine nennenswerte Abdeckung und Nutzerbasis aufweist, (2.) die durchgehende Konnektivität zwischen Endnutzern wegen mangelnder Interoperabilität zwischen interpersonellen Telekommunikationsdiensten bedroht ist, (3.) eine Verpflichtung zur Gewährleistung der durchgehenden Konnektivität zwischen Endnutzern

585 Gesetzesbegründung BT-Drs. 19/26108, S. 257.

erforderlich[586] ist und (4.) die Kommission Durchführungsmaßnahmen nach dem EKEK erlassen hat. Die Regelung belässt der BNetzA („kann") einen Beurteilungsspielraum, was angesichts des sich wandelnden Stands der Technik und der ökonomischen Realisierbarkeit, die eine Einzelfallabwägung darüber verlangen, welches Maß an Interoperabilität von den Anbietern gefordert werden kann, sinnvoll ist.[587]

Nach dem bisherigen Stand geht die BNetzA in der Anwendung des TKG, wie der EKEK selbst, (noch) davon aus, dass gegenwärtig die durchgehende Konnektivität (noch) nicht bedroht, sondern dadurch gewährleistet ist, dass Endnutzer nummerngebundene interpersonelle Telekommunikationsdienste, d. h. klassische Telekommunikationsdienste, nutzen.[588] Allerdings erkennt sie, wie der EKEK, durchaus an, dass künftige technische Entwicklungen und auch das Verhalten der Endnutzer zu einer unzureichenden Interoperabilität zwischen interpersonellen Telekommunikationsdiensten führen könnten.[589] Ist das der Fall, sind unter § 21 Abs. 2 TKG sowohl Verpflichtungen denkbar, die eine Kommunikation von Privatpersonen ermöglichen, als auch solche, die standardisierte Schnittstellen für die Kommunikation von Unternehmen anordnen können, damit mehr interpersonelle Telekommunikationsdienste derartige Funktionen gegenüber Unternehmen anbieten können.[590] Eine nennenswerte Nutzerbasis, zumindest in Deutschland, dürften aber zahlenmäßig nur wenige Messenger-Dienste erreichen und damit als mögliche Adressaten einer Verpflichtung in Betracht kommen.[591]

---

586 Der EKEK enthält die Formulierung „soweit sie den zur Sicherstellung der Interoperabilität von interpersonellen Kommunikationsdiensten notwendigen Umfang nicht überschreiten" und verweist in dem Zusammenhang auch auf mögliche andere verhältnismäßige Pflichten, die auferlegt werden können.

587 *Janik*, in Geppert/Schütz, § 75 TKG, Rn. 6.

588 *BNetzA*, Nutzung von Online-Kommunikationsdiensten in Deutschland. Vgl. für den Vergleich zu herkömmlicher Telefonie die Pressemitteilung der BNetzA vom 10.11.2023, https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2023/20231110_VerbraucherOnlineKomm.html.

589 *BNetzA*, Interoperabilität zwischen Messenger-Diensten, S. 23.

590 *Monopolkommission*, Telekommunikation 2021, S. 99 ff.

591 Die in Deutschland am stärksten verbreiteten Online-Kommunikationsdienste erreichten 2023 folgende Nutzungsanteile: 92 % WhatsApp (2021: 93 %), 36 % Facebook Messenger (2021: 39 %), 27 % Instagram Direct Messages (2021: 25 %), 20 % Microsoft Teams (2021: 14 %) und 19 % Zoom (2021: 18 %); vgl. *BNetzA*, Nutzung von Online-Kommunikationsdiensten in Deutschland.

In Umsetzung von Art. 61 Abs. 1 UAbs. 1 lit. d) EKEK legt § 21 Abs. 3 TKG schließlich fest, dass die BNetzA Betreiber verpflichten kann, zu fairen, ausgewogenen und nichtdiskriminierenden Bedingungen Zugang zu APIs und elektronischen Programmführern (EPGs) zu gewähren, soweit dies zur Gewährleistung des Zugangs der Endnutzer zu digitalen Hörfunk- und Fernsehdiensten sowie damit verbundenen ergänzenden Diensten erforderlich ist. Solche ergänzenden Dienste sollen auch programmbezogene Dienste sein, die speziell konzipiert sind, um die Barrierefreiheit für Endnutzer mit Behinderungen zu verbessern, sowie programmbezogene Dienste des vernetzten Fernsehens.[592]

Insgesamt stehen die Befugnisse des § 21 TKG unter der Bedingung, dass Maßnahmen der BNetzA fair, objektiv, transparent, verhältnismäßig und nichtdiskriminierend sein müssen. Im Falle der Möglichkeiten insbesondere nach Abs. 2, die bereits hohe Hürden für ein Einschreiten setzen, kommt hier demzufolge eine weitere Ebene der Prüfung hinzu. Insgesamt stellt sich die Anordnung einer Interoperabilitätspflicht, nach derzeitigem Stand, als Ultima Ratio dar, für die offenbar noch keine entsprechenden Bedürfnisse bei der Behörde gesehen werden.

(4) Zugangsverpflichtungen bei beträchtlicher Marktmacht (§ 26 TKG)

Selbst wenn aber ein Ergreifen von Maßnahmen derzeit noch nicht in Betracht kommt – insbesondere in Bezug auf Messenger-Dienste hat die Europäische Kommission diesen Weg noch nicht eröffnet –, bleibt weiterhin auch eine allgemeine Marktregulierung nach §§ 10 ff. TKG durch die BNetzA möglich. Aufbauend auf einer Marktanalyse (§ 11 TKG) und dem Durchlaufen eines Konsolidierungsverfahrens (§ 12 TKG) kann die BNetzA Unternehmen, die über eine beträchtliche Marktmacht verfügen, bestimmte Verpflichtungen auferlegen, wenn damit ein Marktversagen behoben werden kann.

Hierzu gehören nach § 26 TKG auch Zugangsverpflichtungen, darunter die Verpflichtung, bestimmte notwendige Voraussetzungen für die Interoperabilität durchgehender Nutzerdienste zu schaffen (§ 26 Abs. 3 Nr. 4 TKG) und offenen Zugang zu technischen Schnittstellen, Protokollen oder anderen Schlüsseltechnologien, die für die Interoperabilität von Diensten oder für Dienste für virtuelle Telekommunikationsnetze unentbehrlich

592 Gesetzesbegründung BT-Drs. 19/26108, S. 258; vgl. auch Erwgr. 153 EKEK.

sind, zu gewähren (§ 26 Abs. 3 Nr. 8 TKG). Neben der Feststellung beträchtlicher Marktmacht und eines entsprechenden Marktversagens steht dies allerdings unter der zusätzlichen Bedingung, dass ohne entsprechende Verpflichtungen die Entwicklung eines nachhaltig wettbewerbsorientierten Endkundenmarktes behindert würde und die Interessen der Endnutzer beeinträchtigt würden (§ 26 Abs. 1 TKG). Das unterliegt wiederum einem umfassenden Prüferfordernis durch die BNetzA, § 26 Abs. 2 TKG. Sie muss berücksichtigen, ob die Auferlegung von Pflichten in einem angemessenen Verhältnis zu den Zielen des TKG (wozu auch Interoperabilität gehört) steht, und hat dabei die technische Machbarkeit, wirtschaftliche Faktoren und mögliche Beeinträchtigungen gewerblicher Schutzrechte und Rechte am geistigen Eigentum zu beachten. Entgegenstehen können der Verpflichtung insbesondere Gefahren für die Netzintegrität oder die Sicherheit des Netzbetriebs (§ 26 Abs. 4 TKG) sowie technische Gründe (§ 21 Abs. 6 TKG).

Sind die Voraussetzungen erfüllt und ist die Marktmacht durch die BNetzA förmlich festgestellt, wären asymmetrische Interoperabilitätsvorgaben für das marktmächtige Unternehmen auf einem bestimmten Markt, auf dem es dominant ist, möglich. Die Marktabgrenzung bestimmt aber hier zugleich die potenzielle Reichweite solcher Pflichten. Während ein gesonderter Markt für Messenger-Dienste sicherlich existiert, wäre ein einheitlicher Telekommunikationsmarkt schwieriger zu begründen, da die jeweiligen Dienste aus Verbrauchersicht (derzeit zumindest noch) nicht austauschbar sind. Einer solchen Annahme bedürfte es aber, um etwa Interoperabilität auch zwischen nummerngebundenen und nummernunabhängigen Diensten anzuordnen, also zwischen Messaging und Telefonie.[593]

(5) Interoperabilität von Fernseh- und Radiogeräten (§ 75 TKG)

§ 75 TKG dient der Umsetzung von Art. 113 EKEK in Verbindung mit Anhang XI des EKEK und setzt mit Änderungen die Vorgängervorschrift des bisherigen § 48 TKG fort. Die durch den EKEK vorgegebene Ausweitung, neben Fernsehgeräten auch Radiogeräte zu erfassen, wurde bereits mit

593 Die *Monopolkommission*, Telekommunikation 2021, S. 101, weist in dem Zusammenhang darauf hin, dass dies auch gegen den EKEK verstoßen würde, der von einer strikten Unterscheidung dieser beiden Kommunikationsformen ausgeht.

dem Sechsten Gesetz zur Änderung des Telekommunikationsgesetzes vom 6. Februar 2020[594] in nationales Recht überführt.

Die Abs. 1 und 2 beziehen sich auf digitale Fernsehempfangsgeräte, die zum Verkauf, zur Miete oder anderweitig angeboten werden. Solche Geräte müssen, soweit sie einen integrierten Bildschirm enthalten, dessen sichtbare Diagonale 30 Zentimeter überschreitet, mit mindestens einer Schnittstellenbuchse ausgestattet sein, die von einer anerkannten europäischen Normenorganisation angenommen wurde oder einer gemeinsamen, branchenweiten, offenen Spezifikation entspricht und den Anschluss von Peripheriegeräten sowie die Möglichkeit einer Zugangsberechtigung erlaubt (§ 75 Abs. 1 TKG). Um die Nutzung von unterschiedlichen verschlüsselten Diensten mit unterschiedlichen Zugangsberechtigungs- und Rechtemanagementsystemen zu ermöglichen, muss die Entschlüsselung über ein an einer Schnittstelle anschließbares Gerät gewährleistet werden, soweit diese Funktionalitäten nicht bereits im digitalen Fernsehgerät selbst softwarebasiert austauschbar integriert sind. Dies kann beispielsweise über eine CI/CI+-Schnittstelle erfolgen. So lässt sich erreichen, dass Entwicklungen auf dem Pay-TV-Markt geräteunabhängig erfolgen können.[595] Nach Abs. 2 müssen solche digitalen Fernsehempfangsgeräte daher auch die Fähigkeit haben, Signale zu entschlüsseln, die einem einheitlichen europäischen Verschlüsselungsalgorithmus entsprechen, wie er von einer anerkannten europäischen Normenorganisation verwaltet wird, und Signale anzuzeigen, die unverschlüsselt übertragen wurden.

§ 21 Abs. 3 TKG betrifft demgegenüber in einer separaten Vorschrift Autoradiogeräte. Jedes Autoradiogerät, das in ein neu in Verkehr gebrachtes, für die Personenbeförderung ausgelegtes und gebautes Kraftfahrzeug eingebaut wird, muss einen Empfänger nach dem jeweiligen Stand der Technik enthalten, der zumindest den Empfang und die Wiedergabe von Hörfunkdiensten unmittelbar ermöglicht, die über digitalen terrestrischen Rundfunk ausgestrahlt werden. Bei Empfängern, die den harmonisierten Normen oder Teilen davon entsprechen, wird die Konformität mit der Anforderung in Satz 1, die mit den betreffenden Normen oder Teilen davon übereinstimmt, angenommen.

Von der Möglichkeit nach Art. 113 Abs. 2 EKEK, auch andere für Verbraucher bestimmte Radiogeräte Interoperabilitätspflichten zu unterwer-

594 BGBl. I 2020, S. 146.
595 Gesetzesbegründung BT-Drs. 19/26108, S. 301.

fen, hat der deutsche Gesetzgeber in § 21 Abs. 4 TKG Gebrauch gemacht. Jedes für Verbraucher bestimmte, erstmalig zum Verkauf, zur Miete oder anderweitig auf dem Markt bereitgestellte, überwiegend für den Empfang von Ton-Rundfunk bestimmte Radiogerät, das den Programmnamen anzeigen kann und nicht Abs. 3 unterfällt, muss einen Empfänger enthalten, der zumindest den Empfang und die Wiedergabe digitaler Hörfunkdienste ermöglicht. Davon ausgenommen sind allerdings Bausätze für Funkanlagen, Geräte, die Teil einer Funkanlage des Amateurfunkdienstes sind, und Geräte, bei denen der Hörfunkempfänger eine reine Nebenfunktion hat. Im Unterschied zu § 21 Abs. 3 TKG besteht die Ausrüstungspflicht hier also in einem Empfänger, der zumindest den Empfang und die Wiedergabe digitaler Hörfunkdienste ermöglicht. Anders als dort werden auch die möglichen Empfangswege nicht vorgeschrieben. Neben Signalen, die über den digitalen terrestrischen Rundfunk ausgestrahlt werden, sind auch andere Verbreitungswege zulässig, womit die Regelung auf beliebige Verbreitungswege von Internetradio ausgedehnt wird.[596]

§ 21 Abs. 5 TKG schließlich dient der Umsetzung von Art. 113 Abs. 3 UAbs. 2 und 3 EKEK und richtet sich an Anbieter digitaler Fernsehdienste. Diese haben digitale Fernsehempfangsgeräte, die sie ihren Endnutzern im Zusammenhang mit der Nutzung der digitalen Fernsehdienste zur Verfügung stellen,[597] kostenfrei und einfach von ihren Endnutzern zurückzunehmen, außer sie sind mit dem Dienst, zu dem der Endnutzer gewechselt ist, vollständig interoperabel. Ob das der Fall ist, hängt nach der Gesetzesbegründung wesentlich von den Dienstmerkmalen ab, die als Teil des Fernsehdienstes angesehen werden. Auf jeden Fall sollen hiervon Video- und Audioinhalte umfasst sein, aber auch Zusatzdienste, die nach Verkehrsauffassung wesentlich sind, sollen in Betracht kommen. Die Vermutungsregel bei Normung, wie sie sich aus dem EKEK ergibt, wird wiederum aufgegriffen. Die harmonisierten Normungen enthalten damit nur eine Vorgabe hinsichtlich der für die Interoperabilität zu betrachtenden Dienstmerkmale. Die Interoperabilität kann vom Anbieter digitaler Fernsehdienste auch auf anderen Wegen als über die Anwendung harmonisierter Normen erreicht werden. Er trägt hierfür allerdings die Beweislast.

596 Gesetzesbegründung BT-Drs. 19/26108, S. 302.

597 Nicht von der Verpflichtung erfasst sind Hersteller digitaler Fernsehgeräte, die zwar digitale Fernsehdienste für die Nutzer ihrer Geräte in geringem Umfang bereitstellen, hierüber aber keine gesonderten Verträge abschließen oder wenn dies nicht die Hauptleistungspflicht des Vertrages über den Erwerb eines digitalen Fernsehgeräts ist.

Die in Art. 113 Abs. 3 UAbs. 1 EKEK vorgesehene, breit formulierte Möglichkeit, dass die Mitgliedstaaten Anbieter auch (darüber hinaus) „anhalten", ihre Dienste interoperabel zu machen, wurde nicht gesondert im TKG aufgegriffen. Bemerkenswert ist dabei aber der Hinweis in der Gesetzbegründung zum TK-ModG:

> *Im Zusammenhang mit neuen Formen der Übertragung digitaler Fernsehsignale, insbesondere im Wege von interaktiven Diensten und unterstützenden Anwendungen („Apps"), können sich neue Interoperabilitätsprobleme ergeben, die zu einer Verkürzung der Nutzungsdauer von Geräten oder einer Bindung an den diese bereitstellenden Anbieter digitaler Fernsehdienste führen. Gegenwärtig wird jedoch noch keine Notwendigkeit gesehen, über die zwingend in der Richtlinie (EU) 2018/1972 vorgesehenen Regelungen und die mögliche Mitwirkung der Bundesnetzagentur an interoperabilitätsfördernden Normungs- und Standardisierungsvorhaben hinaus weitere Verpflichtungen festzulegen. Dies kann sich jedoch zukünftig ändern.*[598]

b. Institutionelle Dimension

Zentrale Regulierungsbehörde ist für das Telekommunikationsrecht die Bundesnetzagentur. Seit der Novellierung des TKG ist sie auch zuständige Behörde für nummernunabhängige interpersonelle Telekommunikationsdienste – die Entscheidung, ob diese als Telemedien unter das Medienrecht fallen oder als Telekommunikationsdienste unter das TKG, wurde also zugunsten von Letzterem auf Bundesebene gelöst.[599]

Die BNetzA ist nach § 191 TKG und aus den einzelnen Zuständigkeiten im TKG mit verschiedenen Aufgaben und Befugnissen ausgestattet. Ergänzend gelten auch die Regelungen des Gesetzes über die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen,[600] nach dessen § 5 u. a. auch die Einrichtung eines Beirats vorgesehen ist. Dieser

598 Gesetzesbegründung BT-Drs. 19/26108, S. 302.

599 Das bedarf aber einer Prüfung im Einzelfall, die bspw. nicht für jede Art von Messenger-Dienst inklusive neuartiger Dienstentwicklungen pauschal getroffen werden kann.

600 Gesetz über die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen vom 7. Juli 2005 (BGBl. I S. 1970, 2009), das zuletzt durch Art. 3 des Gesetzes vom 16. Juli 2021 (BGBl. I S. 3026) geändert worden ist.

besteht aus jeweils 16 Mitgliedern des Deutschen Bundestages und 16 Vertretern oder Vertreterinnen des Bundesrates. Wie im GWB ist auch in § 195 Abs. 2 TKG die Monopolkommission als ein unabhängiges Beratungsgremium mit Befugnissen ausgestattet. Sie erstellt alle zwei Jahre ein Sektorgutachten, in dem sie den Stand und die absehbare Entwicklung des Wettbewerbs und die Frage, ob nachhaltig wettbewerbsorientierte Telekommunikationsmärkte in der Bundesrepublik Deutschland bestehen, beurteilt, die Anwendung der Vorschriften dieses Gesetzes über die Regulierung und Wettbewerbsaufsicht würdigt und zu sonstigen aktuellen wettbewerbspolitischen Fragen Stellung nimmt. Im Kontext von Interoperabilität spielen insbesondere die Ausführungen im Gutachten der Monopolkommission von 2021 eine Rolle.[601]

Insbesondere im Rahmen der Interoperabilitätsbestimmungen in § 21 TKG nimmt die BNetzA eine entscheidende Rolle ein, da es sich um „Kann-Vorschriften" handelt, die (auch) eine Beurteilung des Marktes und der Nutzungsverhältnisse erfordern. Hinsichtlich der Interoperabilität von Messenger-Diensten, die im vorliegenden Kontext besondere Relevanz hat, obliegt es der BNetzA, zu beurteilen, ob einer Bedrohung der Konnektivität auf dem deutschen Markt mit Interoperabilitätspflichten begegnet werden muss. In diesem Rahmen gilt das bereits oben (C.III.2.a(3)(b)) dargestellte zweistufige Verfahren aus dem EKEK. Zunächst muss die Kommission bestimmen, welche Gefahren für die Konnektivität im Binnenmarkt bestehen und welche Mittel dagegen ergriffen werden können. Erst auf der Basis eines solchen Durchführungsakts kann in einem zweiten Schritt die BNetzA entscheiden, ob es aus Perspektive (auch) des nationalen Marktes erforderlich ist, die von der Kommission dargelegten Maßnahmen zu ergreifen, und in welchem Umfang dies zu geschehen hat.[602]

Eine solche Feststellung ist aber seitens der Kommission noch nicht erfolgt. Vielmehr geht sie in ihrer aktuell gültigen Empfehlung vom 18. Dezember 2020 über relevante Produkt- und Dienstmärkte des elektronischen Kommunikationssektors[603] davon aus, dass nur zwei Märkte, nämlich

601 *Monopolkommission*, Telekommunikation 2021. Vgl. dazu auch eingehend unten C.VI.3.b

602 Dazu auch *Becker/Holznagel/Müller*, Interoperability of Messenger Services, S. 119, 136.

603 Empfehlung (EU) 2020/2245 der Kommission vom 18. Dezember 2020 über relevante Produkt- und Dienstmärkte des elektronischen Kommunikationssektors, die gemäß der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation für eine Vorab-

der Vorleistungsmarkt für den an festen Standorten lokal bereitgestellten Zugang und der Vorleistungsmarkt für dedizierte Kapazitäten, für eine Vorabregulierung in Betracht kommen. Das dürfte jedenfalls ein Indiz dafür sein, dass, wie auch der EKEK bereits in seinen Erwägungsgründen beschreibt, derzeit noch kein Marktregulierungsbedarf angesichts von Bedrohungslagen für die Konnektivität bei Messenger-Diensten gesehen wird. Das verwundert auch insoweit nicht, als sich die Kommission beim DMA bis zuletzt deutlich gegen die Einführung einer Interoperabilitätspflicht für Messenger-Dienste ausgesprochen hatte.[604] Daher wäre es auch ohne Belang, würde sich eine entsprechende Bedrohungslage für die Interkonnektivität in Deutschland auf der Basis der Untersuchungen der Bundesnetzagentur[605] bereits abzeichnen, wofür aber die BNetzA wie auch die Monopolkommission[606] offenbar selbst noch keine Anhaltspunkte sehen. Insoweit sind signifikante Hürden zu überwinden, bevor die Regelung überhaupt praktisch zur Anwendung kommen kann.

c. Verhältnis zum Wettbewerbsrecht

Zu der Frage, in welchem Verhältnis das deutsche Telekommunikationsrecht zur asymmetrischen Regulierung im DMA steht, kann auf die Ausführungen oben verwiesen werden, da insoweit im TKG lediglich die Regeln des EKEK entsprechend umgesetzt werden.

Auf nationaler Ebene stellt sich aber darüber hinaus auch die Frage, in welchem Verhältnis die Regelungen des § 21 TKG und des § 19a Abs. 2 S. 1 Nr. 5 GWB zueinander stehen. Beide lassen die Auferlegung von Interoperabilitätspflichten zu. Während das TKG dies von einer Bedrohung der Konnektivität abhängig macht, bedarf es im GWB der Feststellung einer überragenden marktübergreifenden Bedeutung. Problematisch stellt sich das insbesondere in Bezug auf nummernunabhängige interpersonelle Kommunikationsdienste dar, da die Regeln des EKEK und des TKG das Instrument nur als Ultima Ratio vorsehen. Solche hohen Voraussetzungen

---

regulierung in Betracht kommen (Bekannt gegeben unter Aktenzeichen C(2020) 8750), C/2020/8750, EU ABl. L 439, 29.12.2020, S. 23–31.

604 Non-paper from the Commission services on interoperability for messenger services and online social networks in the DMA, https://www.lobbycontrol.de/wp-content/uploads/non_paper_interoperability_dma.pdf.

605 *BNetzA*, Interoperabilität in Messenger-Diensten; vgl. eingehend unten C.VI.3.c.

606 *Monopolkommission*, Telekommunikation 2021; vgl. eingehend unten C.VI.3.b.

sind in § 19a GWB nicht statuiert, und auch das TKG-Instrument ist nicht mit der allgemeinen Marktregulierung des GWB (wie im TKG die §§ 10 ff. i. V. m. § 26) vergleichbar. Dennoch ist die Anwendbarkeit auf ein und denselben Dienst in der Praxis denkbar („überragende marktübergreifende Bedeutung" im GWB im Vergleich zu „nennenswerte Abdeckung und Nutzerbasis" im TKG). Vertreten wird daher, dass § 21 Abs. 2 TKG Lex specialis zum GWB sei, wenn und weil hiervon ohnehin nur ganz bestimmte Dienste erfasst seien – anders als im GWB, das nicht auf bestimmte Dienste oder Dienstekategorien abstellt – und weil die Bestimmungen eine sehr ähnliche Schutzrichtung (Netzwerkeffekte auf mehrseitigen Märkten bekämpfen und Marktzutrittsschranken sowie Hindernisse für Innovationen wirksam begegnen) aufwiesen, die für ein Spezialverhältnis sprächen.[607] Wäre ein Vorgehen gegen solche Dienste im Rahmen des GWB möglich, selbst wenn keine Bedrohung der Ende-zu-Ende-Konnektivität vorliegt, könnte das der Zielsetzung und dem ausdifferenzierten Regulierungssystem im Telekommunikationsrecht zuwiderlaufen sowie die Verfahrenserfordernisse auf EU-Ebene, insbesondere die Durchführungsrechtsakte der Kommission, „umgehen". Auch entspräche es nicht der vom EKEK vorgesehenen unionsweit koordinierten Vorgehensweise, wenn in dem Fall ein Mitgliedstaat auf der Basis des Wettbewerbsrechts einen Sonderweg gehen könnte.

Auf der anderen Seite lässt sich ebenso vorbringen, dass ein Vorgehen unter der allgemeinen Marktregulierung nach dem TKG weiterhin möglich bleibt und auch danach insbesondere Interoperabilität gegen Anbieter mit Marktmacht angeordnet werden kann, wie die Gesetzesbegründung des TKG hervorhebt. Auch nach der allgemeinen Wettbewerbsregulierung unter dem GWB dürften entsprechend diese Möglichkeiten weiterhin bestehen und nicht wegen der Existenz von Art. 61 EKEK gesperrt sein. Mit den Regeln wird im Übrigen auch bei Ergreifen der Möglichkeit durch das BKartA oder die BNetzA etwas anderes erreicht. Nach § 19a GWB kann das BKartA punktuell auf ein durch einen bestimmten Anbieter verursachtes Markthindernis eingehen, die Maßnahmen sind jedoch nicht auf eine dauerhafte Anwendung als Ersatz für eine gesetzliche Regelung angelegt. Das TKG wirkt in seiner Regulierung finaler, obwohl auch solche Maßnahmen der BNetzA der fortwährenden Untersuchung und Überprüfung unterliegen. Es spricht daher mehr dafür, kein Ausschließlichkeitsverhältnis anzunehmen und stattdessen im Rahmen einer Kooperation und Koordinierung zwischen den beiden Behörden einen abgestimmten Weg

607 *Monopolkommission*, Telekommunikation 2021, S. 102 f.

zu suchen. Für die allgemeine Marktregulierung sind in solchen Fällen mit § 197 TKG bereits umfassende Regeln vorgesehen, die sogar teilweise eine einvernehmliche Entscheidung vorsehen. Sie gelten allerdings nicht speziell in Bezug auf § 21 TKG oder § 19a GWB. Allgemein sollen aber „[beide] Behörden auf eine einheitliche und den Zusammenhang mit dem Gesetz gegen Wettbewerbsbeschränkungen wahrende Auslegung dieses Gesetzes [hinwirken]" (§ 197 Abs. 4 TKG).

IV. Geltender Rechtsrahmen zur Interoperabilität: Datenschutzrecht unter dem Aspekt der Datenportabilität

Das Datenschutzrecht kann, wie oben erläutert, deshalb ebenfalls als Teil des Rahmens zur Interoperabilität verstanden werden, weil es Bestimmungen zur Datenportabilität enthält. Dabei geht Interoperabilität zwar über die punktuelle und regelmäßig einseitige Datenportabilität hinaus und unterscheidet sich von dieser durch einen kontinuierlichen, meist wechselseitigen Datenaustausch.[608] Allerdings ist Datenportabilität zum einen eine wichtige Voraussetzung und Teil der Schaffung von Interoperabilität, die ohne einen gewissen Austausch von Daten nicht realisierbar ist, wobei dies im Umfang von der Art und Weise der interoperierenden Dienste abhängt. Zum anderen weisen Portabilität und Interoperabilität sowohl technisch als auch in Bezug auf die (rechtlichen) Rahmenbedingungen eine Reihe von Gemeinsamkeiten auf.[609]

1. USA

In den USA ist das Recht auf Datenportabilität im Datenschutzrecht von 13 der 50 Bundesstaaten normiert (a), während eine vergleichbare Regelung auf Bundesebene fehlt.[610] Daneben ist ein auf Gesundheitsdaten beschränktes spezifisches Recht auf Datenübertragbarkeit vorgesehen (b).

608 *WIK-Consult*, Interoperabilitätsvorschriften für digitale Dienste, S. III.

609 So auch *Digital Competition Expert Panel*, Unlocking digital competition, S. 72; *Ofcom*, Mandated interoperability in digital markets, S. 5.

610 Detaillierter Einblick in die US-amerikanischen Ansätze zum Datenschutz bspw. bei *Bincoletto*, Data Protection by Design in the E-Health Care Sector, S. 294 ff.

a. Einzelstaatliches Datenschutzrecht

Etwa ein Viertel der US-Bundesstaaten haben Datenschutzgesetze für den nicht-öffentlichen Bereich erlassen, in denen sowohl Verpflichtungen für datenverarbeitende Unternehmen als auch Betroffenenrechte vorgesehen sind. Zu den Verpflichtungen zählen die Einhaltung von Grundsätzen wie Zweckbindung und Transparenz, aber auch die Durchführung von Risikoabschätzungen für bestimmte Datenverarbeitungsvorgänge. Betroffenen werden verschiedene Rechte im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten eingeräumt, darunter das Recht auf Auskunft, Berichtigung, Löschung, Widerspruch oder das Recht, nicht ausschließlich einer automatisierten Entscheidungsfindung unterworfen zu werden.[611]

In 13 Bundesstaaten ist dabei ein Recht auf Datenportabilität normiert: in Colorado, Connecticut, Delaware, Florida, Iowa, Kalifornien, Montana, Oregon, Tennessee, Texas, Utah und Virginia.[612] Dort ist die Datenportabilität teilweise als eigenes Recht (vergleichbar mit Art. 20 DS-GVO) und teilweise als Konkretisierung des Auskunftsrechts (vergleichbar mit Art. 15 DS-GVO) vorgesehen.[613] Die übrigen Bundestaaten sehen (noch) kein Recht auf Datenportabilität vor.

Kalifornien hatte 2018 das erste einzelstaatliche Datenschutzrecht in den USA erlassen, in dem das Recht auf Datenportabilität wie folgt ausgestaltet worden war:[614]

California Civil Code § 1798.130(3)(B)(iii)
[A business shall] Provide the specific pieces of personal information obtained from the consumer in a format that is easily understandable to the

611 Übersicht bei International Association of Privacy Professionals, US State Privacy Legislation Tracker 2024, Stand 22.4.2024, https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf.

612 California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020; Colorado Privacy Act; Connecticut Act Concerning Personal Data Privacy and Online Monitoring; Delaware Personal Data Privacy Act; Florida Digital Bill of Rights; Indiana Consumer Data Protection Act; Iowa Act Relating to Consumer Data Protection of 2023; Montana Consumer Data Privacy Act; Oregon Consumer Privacy Act; Tennessee Information Protection Act; Texas Data Privacy and Security Act; Utah Consumer Privacy Act of 2022; Virginia Consumer Data Protection Act. Weitere Staaten bereiten entsprechende Datenschutzgesetze vor bzw. haben Gesetze verabschiedet, die noch nicht in Kraft getreten sind; siehe https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

613 Teilweise steht die Anwendbarkeit noch aus: ab 2024 in Florida, Montana, Oregon und Texas, ab 2025 in Delaware und Iowa sowie ab 2026 in Indiana.

614 California Civil Code § 1798.130(3)(B)(iii).

average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance. "Specific pieces of information" do not include data generated to help ensure security and integrity or as prescribed by regulation. Personal information is not considered to have been disclosed by a business when a consumer instructs a business to transfer the consumer's personal information from one business to another in the context of switching services.

Die Regelungen zur Datenportabilität in den unterschiedlichen Bundesstaaten ähneln sich stark und sind mit der kalifornischen Regelung vergleichbar. Grundsätzlich gelten die Datenschutzgesetze nur für Verbraucher („consumer"), sodass nur diesen das Recht auf Datenübertragbarkeit zusteht. Während davon in Kalifornien bspw. alle im Bundesstaat lebenden Personen erfasst sind,[615] steht die Datenportabilität in Texas nur den dort registrierten Bewohnern zu und auch nur, soweit diese im privaten Rahmen handeln. Im Arbeitsumfeld (also bspw. für Arbeitnehmer) findet in Texas das Recht auf Datenportabilität bspw. keine Anwendung.[616] In allen Bundestaaten wird der Anwendungsbereich der Datenschutzgesetzgebung beschränkt, indem nicht alle Datenverarbeiter davon betroffen sind. So können Verbraucher ihr Recht teils nur bei Unternehmen geltend machen, die bestimmte Umsatzschwellen überschreiten (im kalifornischen Recht z. B. mehr als USD 25 Mio.[617]), eine hohe Anzahl an Daten von Verbrauchern verarbeiten (z. B. von mehr als 100.000 Verbrauchern in Kalifornien,[618] Colorado[619] und Utah[620]), oder 50 % ihres Umsatzes mit dem Handel personenbezogener Daten von Verbrauchern erzielen (z. B. in Kalifornien[621]).

Beim Recht auf Datenportabilität sollen die Daten in einem übertragbaren und, soweit technisch machbar, einfach nutzbaren Format zur Verfügung gestellt werden. Lediglich in Kalifornien sollen vergleichbar mit Art. 20 Abs. 1 DS-GVO die Daten, soweit technisch machbar, in einem strukturierten, gängigen und maschinenlesbaren Format bereitgestellt werden. Kein Bundesstaat präzisiert in den Gesetzen Anforderungen an das

615 California Civil Code § 1798.140(i).
616 Texas Business and Commerce Code, § 541.001(7).
617 California Civil Code § 1798.140(d)(1)(A).
618 California Civil Code § 1798.140(d)(1)(B).
619 Colorado Revised Statutes, Part 13, § 6–1–1304(1)(b)(I).
620 Utah Code Annotated 1953, § 13–61–102(1)(c).
621 California Civil Code § 1798.140(d)(1)(C).

Format oder konkrete Elemente der Interoperabilität. In Kalifornien formuliert das Gesetz, dass personenbezogene Daten auf Wunsch des Verbrauchers von einem Verantwortlichen zu einem anderen übermittelt werden können müssen. Für die Anwendbarkeit des Rechts auf Datenportabilität wird in fast allen Bundesstaaten vorausgesetzt, dass personenbezogene Daten entweder digital vorliegen oder automatisiert verarbeitet werden. In Indiana, Tennessee, Texas und Utah müssen wie bei Art. 20 Abs. 1 DS-GVO nur diejenigen Daten zur Verfügung gestellt werden, die Verbraucher zuvor dem Verantwortlichen bereitgestellt haben.[622] Darüber hinaus kann in Indiana der Verantwortliche entscheiden, ob er alle vom Verbraucher bereitgestellten Daten oder eine Zusammenfassung derselben übermittelt.[623] Die übrigen Bundesstaaten sehen diese Einschränkung in den Gesetzen nicht vor. Sichergestellt wird auch, dass der im Rahmen der Datenportabilität Verantwortliche keine Geschäftsgeheimnisse bei diesem Vorgang offenlegen muss.[624]

b. Sektorspezifische datenbezogene Interoperabilitätsanforderungen

Neben der im allgemeinen Datenschutzrecht geregelten Datenportabilität, soweit darin niedergelegt, gibt es weitere spezifische Datenportabilitäts- und Interoperabilitätsanforderungen insbesondere im Gesundheitswesen der USA. Relevant sind im vorliegenden Kontext zwei umfassende Gesetze aus dem Gesundheitsbereich, die den Schutz von Patientenrechten und den Umgang mit deren Daten vorsehen. Entsprechende Regelungen finden sich im Health Insurance Portability and Accountability Act (HIPAA) (1), der u. a. auf den Schutz von Gesundheitsdaten von Patienten gegen unberechtigte Zugriffe abzielt, sowie im 21st Century Cures Act (2), der zur Verbesserung von Forschung und Wettbewerb den Austausch von und Zugang zu Gesundheitsdaten ermöglichen soll.[625]

---

622 Indiana Code § 24–15–3–1(b) (2023); Tennessee Code Annotated, § 47–18–3203(a)(2)(D); Texas Business and Commerce Code, § 541.051(b)(4); Utah Code Annotated 1953, § 13–61–201(3).

623 Indiana Code § 24–15–3–1(b) (2023).

624 Siehe z. B. Montana: "A consumer must have the right to: […] obtain a copy of the consumer's personal data […], provided the controller is not required to reveal any trade secret"; Montana Consumer Data Privacy Act, § 5(1)(d).

625 Überblick zu den datenschutzbezogenen Vorschriften im US-Gesundheitsrecht *Bincoletto*, Data Protection by Design in the E-Health Care Sector, S. 313 ff. Zu Über-

(1) Datenportabilität auf der Grundlage des Health Insurance Portability and Accountability Act (HIPAA)

Auf Bundesebene sieht der auf den Schutz von Gesundheitsdaten beschränkte Health Insurance Portability and Accountability Act of 1996 (HIPAA) ein Recht auf Datenportabilität vor. Ziel des HIPAA ist die Schaffung von Standards für die Verwaltung sowie für den Schutz und Austausch von Gesundheits- und Patientendaten vor allem für Unternehmen und Einrichtungen des Gesundheitswesens. Dazu zählen bspw. Ärzte, Krankenhäuser oder Versicherungsgesellschaften.

HIPAA ist in fünf Teile gegliedert. Teil I regelt den Krankenversicherungsschutz für Arbeitnehmer und deren Familien bei einem Wechsel oder Verlust des Arbeitsplatzes. Teil II dient der Vorbeugung von Betrug und Missbrauch im Gesundheitssektor. In diesem Teil sind die Regelungen zum Austausch von Gesundheitsdaten (z. B. zwischen Ärzten, Krankenhäusern und Versicherungen), aber auch zu Datensicherheit und Datenschutz enthalten. Dieser Teil ist durch verschiedene Verordnungen ergänzt worden, darunter die HIPAA Security Rule,[626] die Sicherheitsstandards für den Umgang mit Patientendaten festlegt, und die HIPAA Privacy Rule,[627] die Datenschutzregeln für Patientendaten einschließlich der Datenportabilität vorgibt.[628] Die weiteren Teile sind im vorliegenden Zusammenhang nicht von Relevanz.

Mit Blick auf Datenschutz und Datensicherheit werden in Teil II US-Gesundheitseinrichtungen verpflichtet, Patienteninformationen vor unbefugter Offenlegung zu schützen. Dies bedeutet im Grundsatz, dass neben den Patienten selbst, den von diesen bestimmten Dritten (z. B. Rechtsanwalt oder Betreuungsperson) und den an einer Gesundheitsleistung Beteiligten niemand Einsicht in die Patientendaten nehmen darf. Im Zuge dessen ist auch die Weitergabe von Patienteninformationen geregelt. Vor diesem Hin-

---

schneidungen der beiden unabhängig voneinander bestehenden Rechtsakte im Hinblick auf Patientendaten vgl. auch die Zusammenfassung bei *Morgan/Moriarty*, 21st Century Cures Act & The HIPAA Access Right.

626 45 CFR Part 160, Subparts A and C of Part 164. Siehe auch HIPAA Security Rule, https://www.hhs.gov/hipaa/for-professionals/security/index.html.

627 45 CFR Part 160 and Subparts A and E of Part 164. Siehe auch https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

628 Zu beiden Konkretisierungen *Bincoletto*, Data Protection by Design in the E-Health Care Sector, S. 335 ff. bzw. 341 ff. und 354 ff.

tergrund ist als Teil der HIPAA Privacy Rule das Recht auf Datenauskunft geregelt:[629]

> *45 CFR § 164.524(c)*
> *(a)(1) Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set […].*
> *(c)(2) The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual. […]*

Patienten können verlangen, dass ihnen ihre eigenen Gesundheitsinformationen bereitgestellt werden, sofern es sich um Daten in Patientenakten, Abrechnungsinformationen oder sonstige Daten handelt, die medizinischen Entscheidungen über Patienten zugrunde gelegt werden.[630] Die Daten müssen, soweit möglich, in der vom Patienten gewünschten Form, dem gewünschten Format und der gewünschten Art und Weise bereitgestellt werden. Dabei hängt die Entsprechung mit der gewünschten Form und dem Format davon ab, ob die Daten ohne weiteres so bereitgestellt werden können. Weitere Spezifikationen oder Interoperabilitätsanforderungen sind im HIPAA nicht vorgesehen. In der Praxis setzen Gesundheitseinrichtungen zum Teil Plattformen ein, die vollständig integrierte Lösungen für die Verwaltung von Arztpraxen und Krankenhäusern einschließlich von Patientenakten anbieten.[631] Als Teil dessen können Patienten ihre Daten in einem Portal oder einer mobilen App online einsehen und übertagen.[632]

---

629 Health Insurance Portability and Accountability Act of 1996 Security and Privacy Rules, 45 CFR § 164.524(c).

630 45 CFR § 164.501.

631 Siehe etwa https://www.mychart.org/ von Epic Systems; der Hersteller Epic Systems ist nicht mit dem Videospielanbieter Epic Games zu verwechseln.

632 Siehe etwa am Johns Hopkins Hospital in Baltimore, Maryland: https://www.hopkinsmedicine.org/patient-care/patients-visitors/medical-records#copy.

(2) Datenzugang auf Grundlage des 21st Century Cures Act

Im Jahr 2016 ist der 21st Century Cures Act[633] zur Verbesserung der Forschungsbedingungen im Gesundheitssektor durch Beschleunigung der Entwicklung und Zulassung von Arzneimitteln und Medizinprodukten in Kraft getreten. Das Gesetz ist in drei Kapitel gegliedert. Im ersten Kapitel (Division A) werden unterschiedliche Maßnahmen zusammengefasst, zu denen auch Bestimmungen zur Verbesserung von im Gesundheitswesen eingesetzter IT-Technologie gehören, die auch Anforderungen an die Interoperabilität von IT-Systemen stellen (Title IV).

Im Zuge der Förderung der medizinischen Forschung und Entwicklung sieht das Gesetz Regelungen zur Interoperabilität von IT-Systemen vor, die Gesundheitsdaten verarbeiten.[634] Dadurch soll der Austausch von Gesundheitsdaten zur Erleichterung von Forschung und Wettbewerb gefördert werden,[635] während die Patientendatenschutzrechte aus dem HIPAA davon unberührt bleiben. Als Folge des 21st Century Cures Act darf der Zugang zu sowie der Austausch von Gesundheitsdaten nicht beeinträchtigt werden (*information blocking*), wobei Verstöße gegen dieses Gebot mit Geldbußen von bis zu USD 1 Mio. pro Verstoß geahndet werden können.[636] *Information blocking* bezieht sich also auf die Behinderung des Zugangs, Austauschs oder der Nutzung elektronischer Gesundheitsinformationen, die nachteilige Auswirkungen bei der Verbesserung der Patientenversorgung zur Folge haben könnte.

Der 21st Century Cures Act wird durch zwei für die Gesundheitsbranche bindende Verordnungen konkretisiert. Zum einen wird in der Interoperability and Patient Access Final Rule der Zugang zur Patientenakte sowie deren Interoperabilität im Gesundheitsbereich festgelegt (unten (a)).[637] Diese Verordnung wurde von der US-Bundesbehörde Centers for Medicare & Medicaid Services (CMS) erlassen, die für die staatlichen Krankenversicherungen zuständig ist. Zum anderen konkretisiert die 21st Century Cures Act Final Rule Anforderungen an die Zertifizierung von im Gesundheitsbereich

633 21st Century Cures Act of 2015, Pub. L. 114–255, 130 Stat 1033.
634 21st Century Cures Act of 2015, § 4003, 42 U.S. Code § 300jj-11 ff.
635 Office of the National Coordinator for Health Information Technology (ONC), ONC's Cures Act Final Rule, https://www.healthit.gov/topic/oncs-cures-act-final-rule.
636 21st Century Cures Act of 2015, § 4004, 42 U.S. Code § 300jj-52(b)(2)(A).
637 Interoperability and Patient Access Final Rule, 85 FR 25510–25640, erlassen vom US Center for Medicare & Medicaid Services (CMS).

eingesetzter IT und spezifiziert Kriterien zur Prüfung des Vorliegens von *information blocking*, das eine Beschränkung von Interoperabilität bedeutet (unten (b)).[638] Diese Verordnung wurde vom US Office of the National Coordinator for Health Information Technology (ONC) erlassen, das u. a. für die bundesweite Koordinierung des Austauschs von Gesundheitsdaten verantwortlich ist.

(a) CMS Interoperability and Patient Access Final Rule

Die im Jahr 2020 veröffentlichte Interoperability and Patient Access Final Rule soll den Datenaustausch zwischen den an der Gesundheitsversorgung Beteiligten, also zwischen Patienten, Ärzten und Krankenhäusern sowie Kostenträgern im Bereich der staatlichen Krankenversicherung ermöglichen.[639] Durch die Herstellung von Interoperabilität sollen Daten ausgetauscht werden können und Patienten Zugriff auf ihre Gesundheitsinformationen erhalten. Darüber hinaus soll Patienten der Zugriff auf die eigene Patientenakte auch über mobile Apps ermöglicht werden. Die so erlangte Transparenz soll Patienten in die Lage versetzen, die Kosten und die Wirkung ihrer Behandlungen und der ihnen gemachten Gesundheitsangebote abzuschätzen.

Zur Förderung der Interoperabilität müssen von Gesundheitsanbietern verschiedene APIs bereitgestellt werden. Dies betrifft die Bereithaltung einer API, über die Patienten ihre eigenen Patientendaten einschließlich der Kosten für ihre Gesundheitsversorgung abrufen können. Ferner müssen Schnittstellen bereitgestellt werden, über die Informationen zu Anbietern von Gesundheitsleistungen abgerufen werden können. Das soll es Patienten ermöglichen, schnell unterschiedliche Gesundheitsanbieter zu identifizieren. Daneben sollen Patienten beim Wechsel ihres Kostenträgers, also etwa der Krankenversicherung, klinische Patientendaten zum neuen Kostenträger übermitteln können, um eine vollständige Übersicht von Patientendaten auch beim neuen Kostenträger zu ermöglichen.

638 21st Century Cures Act Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule, 85 FR 25642–25961, erlassen vom US Office of the National Coordinator for Health Information Technology (ONC).

639 CMS Interoperability and Patient Access Fact Sheet, 9.3.2020, https://www.cms.gov/newsroom/fact-sheets/interoperability-and-patient-access-fact-sheet.

Darüber hinaus wird vonseiten der Behörde CMS öffentlich darüber berichtet, welche Anbieter von Gesundheitsleistungen Interoperabilität durch *information blocking* behindern. CMS erhält dazu Informationen über die Umsetzung von Interoperabilität direkt von den Anbietern von Gesundheitsleistungen.[640] Durch diese Berichtspflicht sollen Qualität und Kosten von Gesundheitsleistungen verbessert werden. Anbieter müssen bspw. zur Qualität und zu den Kosten ihrer Versorgungstätigkeit berichten. Mit Blick auf die Interoperabilität betrifft das etwa den Einsatz zertifizierter Gesundheits-IT, die Ausstellung elektronischer Rezepte, aber auch den Austausch von Daten mit anderen Anbietern sowie die Bereitstellung von Informationen an Patienten.[641] Da der Grad an Kostenerstattung durch die staatliche Krankenversicherung für Anbieter von Gesundheitsleistungen von den bereitgestellten Informationen und dem Grad der erreichten Qualität bei den erbrachten Diensten abhängt, besteht ein Anreiz, die Informationen entsprechend mitzuteilen und Interoperabilität als einen Teilaspekt der Leistungserbringung in der Praxis tatsächlich umzusetzen.

(b) ONC Cures Act Final Rule

Die Interoperabilitätsanforderungen des 21st Century Cures Act werden ferner durch die im Jahr 2020 verabschiedete Cures Act Final Rule konkretisiert.[642] Diese Verordnung regelt die Förderung der Interoperabilität von elektronischen Gesundheitsdaten, die dafür benötigte Datensicherheit, den Umgang mit *information blocking* sowie die Zertifizierung von Gesundheits-IT. Anders als die CMS Interoperability and Patient Access Final Rule findet die Cures Act Final Rule auf alle Anbieter von Gesundheitsleistungen Anwendung.

Im Speziellen wird die Nutzung eines technischen Standards für die einheitliche Beschreibung von Gesundheitsdaten vorgeschrieben, dem United

640 CMS Quality Payment Program, https://www.cms.gov/medicare/quality/value-based-programs/quality-payment-program.

641 Medicare and Medicaid Promoting Interoperability Program Basics, https://www.cms.gov/medicare/regulations-guidance/promoting-interoperability-programs/medicare-medicaid-basics.

642 21st Century Cures Act Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule, 85 FR 25642–25961, erlassen vom US Office of the National Coordinator for Health Information Technology (ONC).

States Core Data for Interoperability (USCDI).[643] Hiervon erfasst sind etwa klinische Aufzeichnungen, Testergebnisse und Informationen zu Medikationen. Systeme müssen im Hinblick auf diese Daten interoperabel ausgestaltet sein. Neben der Beschreibung des Datenformats werden auch Kompatibilitätsanforderungen für APIs gestellt. Konkret müssen Schnittstellen den technischen Standard HL7 Fast Healthcare Interoperability Resources (FHIR)[644] befolgen. Der Standard wird von Health Level Seven International (HL7) entwickelt, einer gemeinnützen Organisation, die sich für die weltweite Interoperabilität von Gesundheitsdaten einsetzt.[645] Bei der Entwicklung der Standards sind Unternehmens- und Regierungsvertreter beteiligt. Durch die Definition eines Daten- und eines Austauschstandards können verschiedene IT-Anbieter miteinander in den Wettbewerb treten, wodurch Anbieter von Gesundheitsleistungen zwischen verschiedenen, aber interoperablen Angeboten wählen können. Dies soll den Wettbewerb fördern.

Darüber hinaus sollen so die technischen Grundlagen und Bedingungen dafür geschaffen werden, dass Patienten wie oben beschrieben auf die eigene Patientenakte zugreifen können, darin eingeschlossen über mobile Apps. Hinsichtlich des *information blocking* ist es nach dieser Verordnung untersagt, für die Bereitstellung von Gesundheitsdaten an Patienten eine Gebühr zu erheben oder Gesundheitsdaten nur zeitverzögert bereitzustellen. Allerdings sind Ausnahmen zum Verbot von *information blocking* vorgesehen, etwa zur Gewährleistung von Datenschutz- und Datensicherheit oder wenn Gesundheits-IT zeitweise aus Wartungs- oder Performancegründen nicht erreichbar ist.[646]

Zusammenfassend zielt die Cures Act Final Rule mit diesen Klarstellungen auf die Vereinfachung des kostenfreien Zugangs von Patienten zu ihren Gesundheitsdaten und die Portabilitätsmöglichkeit sowie die Schaffung eines Wettbewerbs für Gesundheits-IT, die gleichzeitig den Austausch und die Interoperabilität in der Gesundheitsbranche sicherstellt.

643 United States Core Data for Interoperability, https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi.

644 Fast Healthcare Interoperability Resources (FHIR), https://hl7.org/fhir/.

645 About HL7, https://www.hl7.org/about/index.cfm.

646 The Office of the National Coordinator for Health Information Technology (ONC), Information Blocking, https://www.healthit.gov/topic/information-blocking.

2. EU

Innerhalb der EU ist das Recht auf Datenportabilität zentral in Art. 20 der Datenschutz-Grundverordnung (DS-GVO)[647] geregelt. Die Bestimmung hat einen breiten Anwendungsbereich und erfasst grundsätzlich alle automatisierten Verarbeitungsprozesse personenbezogener Daten unabhängig vom Sektor, in dem sie stattfinden. Daneben bestehen auch sektorspezifische Datenportabilitätsbestimmungen, z. B. in der Digitale-Inhalte-Richtlinie[648] oder auch im Finanz-, Automobil- und Energiesektor, wobei Letztere im vorliegenden Kontext von geringer Relevanz für eine vergleichende Betrachtung sind.[649]

a. Recht auf Datenportabilität aus Art. 20 DS-GVO

(1) Inhalt und Ziel der Bestimmung

Art. 20 Abs. 1 DS-GVO bestimmt, dass Betroffene das Recht haben, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Weiter haben sie das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch ersteren Verantwortlichen zu übermitteln, sofern die Verarbeitung auf einer Einwilligung oder einer vertragsbedingten Verarbeitung beruht und sie mithilfe automatisierter Verfahren erfolgt.

Ziel der Vorschrift ist es, Betroffenen auf ihren Wunsch hin die Kontrolle über „ihre" personenbezogenen Daten zurückzugeben.[650] Betroffene sollen nach Erwägungsgrund 68 S. 1 eine bessere Kontrolle über die eigenen Daten haben. Im Fokus der damaligen Einführung des Rechts auf Datenübertragbarkeit in die DS-GVO stand vor allem eine bessere Kontrolle über Daten, die von Diensten der Informationsgesellschaft und sozialen

---

647 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) EU ABl. L 119 vom 4.5.2016, S. 1–88.

648 Vgl. dazu unten C.V.4.

649 Dazu *Krämer/Senellart/de Streel*, Making Data Portability More Effective for the Digital Economy, S. 31 ff.

650 Erwgr. 68 DS-GVO.

Netzwerken gesammelt werden.[651] Die Vorschrift erstreckt sich jedoch wie erwähnt auf alle Verarbeiter (nicht aber: Auftragsverarbeiter). Wie sich auch aus wettbewerbsrechtlichen Bezügen der Vorschrift ablesen lässt,[652] beschränkt sich Art. 20 DS-GVO nicht auf die Kontrolle im Machtbereich des Betroffenen, sondern will darüber hinaus eine weitere Verwendung der Daten erleichtern. Das ergibt sich bereits daraus, dass es einen Unterschied zwischen dem Recht auf Datenportabilität und dem Recht auf Kopie nach Art. 15 Abs. 3 DS-GVO geben muss, wobei dieses nur den Kontrollbereich des Betroffenen betrifft.[653]

Das Recht auf Datenportabilität weist insoweit Ähnlichkeiten zum Recht auf Nummernportabilität aus dem Telekommunikationsrecht auf. Allerdings ist der Rahmen in der DS-GVO, wie die Portabilität auszugestalten ist, ausgeprägter.[654] Zudem liegen beiden Instrumenten unterschiedliche Zielsetzungen zugrunde: Während es bei der Nummernübertragbarkeit um die Sicherung der Wahlmöglichkeiten für Verbraucher und eines wirksamen Wettbewerbs geht,[655] soll das Recht auf Datenübertragbarkeit eine bessere Kontrolle von Betroffenen über ihre personenbezogenen Daten gewährleisten[656] und ist damit Ausformung grundrechtlich geschützter Individualinteressen. Dennoch könnten sich die mit einer Rufnummernportierung nach Telekommunikationsrecht (§ 46 Abs. 3 TKG) verbundenen Daten für die Portabilität für natürliche Personen auch auf Art. 20 DS-GVO stützen, so wie es z. B. auch bei der Übertragung von Kontoinformationen von einer Bank an ein FinTech denkbar wäre.[657]

---

651 Dazu *Piltz*, in: Gola/Heckmann, Art. 20 Rn. 7; *Paal*, in: Paal/Pauly, Art. 20 Rn. 6, jeweils m. w. N.

652 Dazu unten C.IV.2.a(4).

653 Vgl. zur Unterscheidung etwa die umfangreiche Entscheidung der schwedischen Aufsichtsbehörde gegen Spotify (Final decision under the General Data Protection Regulation — Spotify AB, No. DI-2019–6696, https://edpb.europa.eu/system/files/2023-07/se_2023-06_decisionpublic.pdf. Die Behörde betont hier etwa (S. 19), bei Art. 15 Abs. 3 DS-GVO gehe es darum, dass die Daten für den Betroffenen verständlich und daher lesbar sein müssten, während Art. 20 DS-GVO eine Maschinenlesbarkeit fordere.

654 Dazu unten C.IV.2.a(3).

655 Vgl. Erwägungsgrund 40 der Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (Universaldienstrichtlinie), EU ABl. L 108 vom 24.4.2002, S. 51–77.

656 Vgl. Erwgr. 68 DS-GVO.

657 So *Brüggemann*, in: DSRITB, 2017, S. 1, 3.

Das Recht nach Art. 20 DS-GVO ist begrenzt auf personenbezogene Daten, also auf Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DS-GVO). Anspruchsteller kann demnach auch nur eine natürliche Person sein,[658] während der Begriff des Endnutzers im DMA auch juristische Personen beinhaltet. Erfasst sein können offensichtlich personenbezogene Daten wie Namen oder Anschriften, aber im digitalen Bereich auch solche, die eine Rückverfolgung auf eine natürliche Person ermöglichen, wie z. B. Mail-Adressen oder IP-Adressen. Daten Dritter (nicht aber: Daten mit Drittbezug) dürfen nicht mit übertragen werden.[659] Der Personenbezug erstreckt sich zunächst auch auf alle Daten, die mit dieser identifizierbaren Person verbunden sind, mithin also auf sämtliche Profilinformationen.

Eine Einschränkung kann sich aber aus dem Erfordernis der „Bereitstellung" durch den Betroffenen ergeben. Die DS-GVO formuliert insoweit anders als Art. 6 Abs. 9 DMA („bereitgestellt *oder von ihnen generiert*"). Näher definiert ist dieser Vorgang des Bereitstellens in der DS-GVO nicht, Erwägungsgrund 68 verwendet ebenfalls lediglich die ähnliche Formulierung „zur Verfügung stellen" von Daten. Entsprechend uneinheitlich wird das Merkmal beurteilt.[660] Restriktive Ansichten fordern zur Erfüllung dieses Merkmals eine aktive und wissentliche Handlung des Betroffenen und stützen sich dabei auf den Wortlaut sowie einen systematischen Vergleich mit den weiteren Betroffenenrechten, insbesondere dem Auskunftsrecht, das weiter formuliert ist und ansonsten neben dem Recht auf Datenübertragung keine praktische Relevanz hätte.[661] Angeführt wird auch, dass die Konstellation von Art. 20 DS-GVO insgesamt auf einer vertraglichen Grundlage oder einer Einwilligung beruht, weshalb auch die Bereitstellung auf dieser Grundlage erfolgen müsse, um das Recht auszulösen.[662] Erfasst wären danach etwa solche Daten, mit denen Betroffene einen Dienst aktiv befüllen, wie z. B. Registrierungsdaten, Profilinformationen, Kontakte, aber auch Bilder und Texte, inklusive Kommentare und Nachrichten bspw. auf sozialen Netzwerken. Nicht erfasst wären Daten, die anbieterseitig einem Betroffenen zugeordnet werden, oder solche, die von Dritten kommen

658 Vgl. *Brüggemann*, in: DSRITB, 2017, S. 1, 2.
659 Vgl. dazu auch unten C.IV.2.a(2) zur Rechteverletzung Dritter.
660 Für eine Übersicht zum Meinungsstand vgl. *Westphal/Wichtermann*, in: ZD, 2019, S. 191, 191 ff.; *Paal/Götz*, in: ZD, 2023, S. 67, 68; *Wrobel*, in: DSRITB, 2018, S. 247, 249 f.
661 So *Piltz*, in: Gola/Heckmann, Art. 20 Rn. 17.
662 Dies anführend, im Ergebnis aber wohl a. A. *Wrobel*, in: DSRITB, 2018, S. 247, 249.

(bspw. über Social-Media-Plugins). Andere Ansichten sehen dagegen auch solche Daten erfasst, die aus der Beobachtung der Tätigkeiten eines Nutzers resultieren („observed data")[663], also etwa aus dem Tracking des Nutzers generierte, die bspw. die Grundlage von Empfehlungs- oder Werbealgorithmen sind. Beispiele hierfür wären Suchhistorie oder -verhalten, Playlists, Standortdaten oder Fitnessdaten. Diese Ansichten argumentieren mit dem Sinn und Zweck von Art. 20 DS-GVO, der mehr Betroffenenkontrolle ermöglichen will, was auch (und insbesondere) bei solchen Daten gewollt sei.[664] Würde man diese Daten nicht unter Art. 20 DS-GVO fassen und damit als Daten, die Betroffene nicht ohne Hilfe des Verantwortlichen selbst übertragen können, hätte die Regel nichts am damaligen Status quo verändert.[665] Grenze sind nach dieser Ansicht nur Daten, die auf einer Schlussfolgerung oder Ableitung („inferred and derived data") des Verantwortlichen beruhen, wie bspw. Bonitäts-Scores und andere Profiling-Ergebnisse.[666]

Vermittelnde Ansichten befürworten eine servicespezifische Auslegung, die eine Interessenabwägung aus Betroffenen- und Anbietersicht erfordert und das Merkmal des Bereitstellens im Sinne einer aktiven Bereitstellung nur einer Infrastruktur (für weitere Verarbeitungstätigkeiten des Verantwortlichen) begreift.[667] Abgeleitete personenbezogene Daten würden danach (und nur dann) dem Anwendungsbereich unterfallen, wenn sie nötig wären, um einen vergleichbaren Service anbieten zu können, weil nur diese für die vertragsgemäße Nutzung des Dienstes erforderlich und damit von Art. 20 DS-GVO erfasst sein sollten.[668] Dieses Verständnis ist wohl die im Ergebnis für beide beteiligten Seiten sinnvollste Lösung, aber angesichts von Rechtssicherheitsinteressen und praktischer Umsetzbarkeit problematisch.[669] Andere vermittelnde Ansichten wollen bei den beobachteten Daten differenzieren und sehen nur solche als erfasst an, die einerseits der Betrof-

663 So die *Artikel-29-Arbeitsgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, S. 11; auch *Nebel*, in: ZD-Aktuell, 2019, 04380, mit Verweis auf weitere eher extensive Ansichten.

664 Es kommt demgegenüber aber auch in Betracht, dass der Betroffene solche Daten eben gerade nicht portiert haben will, da er oder sie sich explizit von ihm zugewiesenen (nicht eigenen) Daten in einem Zieldienst lösen will. Dazu eingehend *Westphal/Wichtermann*, in: ZD, 2019, S. 191, 192.

665 *Wrobel*, in: DSRITB, 2018, S. 247, 250.

666 *Nebel*, in: ZD-Aktuell, 2019, 04380.

667 *Strubel*, in: ZD, 2017, S. 355, 357 ff.; *Paal/Götz*, ZD, 2023, S. 67, 68.

668 So neben *Strubel* auch *Brüggemann*, in: DSRITB, 2017, S. 1, 6.

669 *Westphal/Wichtermann*, in: ZD, 2019, S. 191, 192.

fene nicht selbst ohne Hilfe des Verantwortlichen übertragen kann und die andererseits für den Wechsel zwischen Verarbeitern erforderlich sind, da nur in solchen Fällen mit der Portabilität Lock-in-Effekte überwunden werden könnten, worauf Art. 20 DS-GVO abziele.[670] Als Grenze – und damit von Art. 20 DS-GVO nicht mehr erfasst – müssten aber solche Daten gelten, die erst das Ergebnis einer Auswertung durch den Verantwortlichen sind oder von Dritten bereitgestellt wurden.[671]

Beschränkt ist das Datenportabilitätsrecht zudem auf solche Verarbeitungen, die auf einer Einwilligung basieren oder zur Erfüllung eines Vertrags erforderlich sind. Dies korrespondiert mit den Rechtfertigungstatbeständen der Art. 6 Abs. 1 lit a) und b) DS-GVO. Das ist problematisch, weil Verarbeiter (insbesondere: Dienste der Informationsgesellschaft) zu einem bestimmten Grad entscheiden können, auf welche Rechtsgrundlage sie ihre Verarbeitung stützen, wenn es mehrere einschlägige Möglichkeiten gibt. Neben den beiden genannten Rechtfertigungstatbeständen wird dazu in der Online-Umgebung häufig die Berufung auf berechtigte Interessen (Art. 6 Abs. 1 lit. f) DS-GVO) herangezogen. Das gilt etwa für die Anzeige von personalisierten Inhalten auf sozialen Netzwerken, Video-Sharing-Plattformen oder Vide-on-Demand-Diensten, ob sie nun auf Steuerung des Nutzers basiert (bspw. „Gefällt mir"-Angaben) oder anbieterseitig auf der Grundlage von Tracking erfolgt. Unabhängig davon, ob eine Verarbeitung auf dieser Grundlage tatsächlich rechtmäßig ist,[672] schließt sie jedenfalls das Recht auf Datenportabilität nach dem Wortlaut der Bestimmung aus. Der Betroffene hat also keinen Anspruch darauf, diese ggf. rechtswidrig erhobenen Daten im Rahmen des Datenportabilitätsrechts zu erhalten.[673] Einige wollen daher dann eine Ausnahme machen, wenn die Daten zumindest „auch" auf der Basis von Einwilligung oder Vertrag verarbeitet werden,[674] wobei dies bei einer Verarbeitung rein auf der Basis berechtigter Interessen ebenfalls nicht vorliegen würde.

Schließlich erstreckt sich das Recht nur auf Daten aus automatisierten Verarbeitungsvorgängen. Erforderlich ist daher eine Verarbeitung im We-

670 *Wrobel*, in: DSRITB, 2018, S. 247, 251.
671 *Paal*, in Paal/Pauly, Art. 20 Rn. 17.
672 Zur Rechtfertigungsgrundlage der Datenverarbeitung etwa bei sozialen Netzwerken (hier konkret Facebook) vgl. z. B. eingehend das Urteil des EuGH in Sachen *Meta Platforms*, C-252/21 – ECLI:EU:C:2023:537.
673 So auch *Nebel*, in: ZD-Aktuell, 04380.
674 *Paal/Götz*, in: ZD, 2023, S. 67, 68.

sentlichen durch Computersysteme, wobei damit auch jene auf Online-Plattformen erfasst sind.

Keiner ausdrücklichen Regelung zugeführt ist die Dauer des Rechts aus Art. 20 DS-GVO. Solange der mit der Verarbeitung verbundene Dienst oder das Vertragsverhältnis noch existieren und vom Betroffenen genutzt werden, ist die Frage unproblematisch. Welche Folgen es aber für das Recht auf Datenportabilität hat, wenn entweder der Dienst selbst eingestellt oder einseitig vom Betroffenen gekündigt wird, ergibt sich aus dem Gesetz nicht. Problematisch ist hierbei, dass die Datenverarbeitung, wenn sie noch erfolgt, nicht mehr auf der Grundlage von Einwilligung oder Vertrag erfolgen kann und Art. 20 DS-GVO seinem Wortlaut nach nicht mehr einschlägig ist. In einer solchen Situation den Betroffenen ihre Rechte zu entziehen, selbst wenn Daten weiterhin, eventuell rechtswidrig, verarbeitet werden, ist mit dem Telos der Bestimmung nicht vereinbar.[675]

(2) Ausnahmen

Ausnahmen vom Recht auf Datenportabilität finden sich in Abs. 3 und 4. Es gilt zum einen nicht für solche Verarbeitungen, die für die Wahrnehmung einer Aufgabe erforderlich sind, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt. Das schließt insbesondere Verarbeitungsvorgänge durch Behörden aus dem Anwendungsbereich von Art. 20 DS-GVO aus.[676] Gleiches gilt für private Einrichtungen, die mit einer Aufgabe im öffentlichen Interesse betraut sind. Dieser Anwendungsfall sollte – spiegelbildlich zu Art. 6 Abs. 1 lit. e) DS-GVO – auf öffentlich-rechtliche Betrauungsakte an Private verstanden werden, nicht also im Sinne des „Dienens" öffentlicher Interessen. Die Vorschrift ist in diesen Zusammenhängen begrenzt worden, weil solche Verarbeitungstätigkeiten regelmäßig auf der Basis öffentlich-rechtlicher Aufgabenwahrnehmung und nicht auf der Basis von Einwilligung oder Vertragserfüllung erfolgen.

Wichtiger ist die Ausnahme nach Art. 20 Abs. 4 DS-GVO, wonach das Recht auf Datenübertragbarkeit nicht die Rechte und Freiheiten anderer Personen beeinträchtigen darf. Die Regelung ist weit zu verstehen und betrifft einerseits das Recht auf Schutz personenbezogener Daten Dritter,

675 Dazu eingehend und im Ergebnis ebenso *Westphal/Wichtermann*, in: ZD, 2019, S. 191, 192 ff.

676 *Piltz*, in: Gola/Heckmann, Art. 20 Rn. 6.

wie es bei der Übertragung von Kontaktlisten beeinträchtigt sein könnte. Während das bei der Übertragung von Kontakten, die ein Betroffener selbst angelegt hat (bspw. in E-Mail-Programmen), weniger problematisch ist,[677] gilt es auch für von Dritten angelegte Profile oder Kontakte in sozialen Netzwerken, also etwa eine Portierung der Freundesliste. Insofern wäre aber ggf. eine Übertragung des Kontakts, also des vollständigen „Profils" in ein anderes Netzwerk, von der Einwilligung des Dritten abhängig, der vielleicht nicht in dem Zielnetzwerk erscheinen möchte. Weiter können sich „Mischdaten" ergeben, wenn z. B. Bilder oder Inhalte von einem Nutzer in einem Netzwerk geteilt, also offenkundig bereitgestellt werden, diese aber bspw. durch „Likes" oder Kommentare von anderen Nutzern auch einen Drittbezug erhalten.[678] Diese Nutzer haben zwar im Rahmen ihrer Registrierung der Verarbeitung ihrer Daten innerhalb des Dienstes zugestimmt, nicht aber einer Übermittlung derselben an andere Dienste.

Die Ausnahme kann sich andererseits auch auf andere „Rechte und Freiheiten" erstrecken, wie z. B. urheberrechtlich geschützte Lizenzen (bspw. Übertragung von Fotos / medialen Inhalten von einem Dienst / einer Mediathek in eine andere) oder Geschäftsgeheimnisse auf Anbieterseite, die bei einer Übertragung offenbart würden.[679] Übertragungsformate von Daten zwischen verschiedenen Anwendungen könnten etwa aufgrund ihres Informationsgehalts über das entsprechende System und wegen ihrer Komplexität der eigenen Datenstruktur selbst als Geschäftsgeheimnisse deklariert werden, womit ihre Übertragbarkeit vom Verarbeiter ausgeschlossen wird.[680] Dies würde dann auch für die „beobachteten" Daten, z. B. Tracking-Daten, gelten.

Insgesamt ist im Rahmen von Abs. 4 daher eine umfassende Abwägung der Grundrechte und Interessen des Betroffenen mit den entsprechenden Interessen und Rechtspositionen der „auch betroffenen" Person(en) vorzunehmen, wobei möglicherweise der Umfang der Datensätze zu beschränken ist. Diese Beschränkung wiederum kann die Relevanz des Rechts auf Datenportabilität für den Betroffenen in Frage stellen, wenn (für ihn oder sie) wesentliche Daten (bspw. Kontaktlisten oder Kundenrezensionen)

677 So etwa *Brüggemann*, in: DSRITB, 2017, S. 1, 9, mit Hinweis darauf, dass das regelmäßig bereits nicht unter die DS-GVO fällt, weil (und wenn) das Adressbuch ausschließlich privat genutzt wird.

678 *Uphues*, in: Hoeren/Sieber/Holznagel, Teil 15.3 Rn. 26.

679 *Wrobel*, in: DSRBITB, 2018, S. 247, 251.

680 So *Piltz*, in: Gola/Heckmann, Art. 20 Rn. 38.

nicht im portierten Datensatz enthalten sind.[681] Insoweit zeigt sich im Rahmen der DS-GVO, dass die oben (unter C.I.2.c) angeführten rechtlichen Grenzen und Voraussetzungen Eingang in das Recht auf Datenportabilität gefunden haben, weil sie von diesem unberührt bleiben.

(3) Umsetzung von Datenportabilität

Art. 20 DS-GVO unterscheidet drei verschiedene Arten der Portabilität. Abs. 1 S. 1 statuiert eine Art Herausgabeanspruch des Betroffenen gegenüber dem Verantwortlichen.[682] Der Betroffene muss die Daten „erhalten", was nicht gleichgesetzt werden kann mit einem „Zugang zu" Daten etwa in einer dafür vorgesehenen Benutzeroberfläche. Das bedeutet, es muss eine Form von Zusendungs- oder Downloadmöglichkeit bestehen. Abs. 1 S. 2 erweitert diesen Anspruch auf die Übermittlung der so erhaltenen Daten an einen anderen Verantwortlichen, statuiert also eine Art Erlaubnistatbestand für den vom Betroffenen in Anspruch genommenen Dienst zur Datenweitergabe. Jedoch erfolgt die Übermittlung durch den Betroffenen selbst. Art. 20 Abs. 2 DS-GVO wiederum ermöglicht die Übertragung unmittelbar von dem verarbeitenden Verantwortlichen an einen anderen Verantwortlichen, ersetzt also die Übermittlung durch den Betroffenen selbst. Allerdings ist diese Möglichkeit an die nicht näher definierte „technische Machbarkeit" auf Seiten des Verantwortlichen geknüpft. Zu beachten ist, dass Art. 20 DS-GVO den Verantwortlichen nicht von seinen sonstigen Pflichten aus der DS-GVO entbindet. Dementsprechend bedarf nicht nur die Übertragung der Daten einer Rechtfertigungsgrundlage (insb. bezüglich Drittdaten), sondern es muss auch die Sicherheit der Daten während des Übertragungsvorgangs durch geeignete technische und organisatorische Sicherheitsmaßnahmen gewährleistet werden.[683]

In Bezug auf das „Wie" der Datenübertragbarkeit stellt Art. 20 DS-GVO drei Kriterien bzw. Anforderungen an die Ausgabe der Daten auf, fordert ein strukturiertes, gängiges und maschinenlesbares Format. Die Maschinenlesbarkeit und Strukturiertheit sind technische Anforderungen, das Merkmal der Gängigkeit eine faktische Bedingung.[684] Das Merkmal der Maschinenlesbarkeit zeigt, dass es in Art. 20 DS-GVO vorrangig nicht um

681 *Paal*, in: Paal/Pauly, Art. 20 Rn. 27.
682 *Piltz*, in: Gola/Heckmann, Art. 20 Rn. 9 f.
683 *Wrobel*, in: DSRITB, 2018, S. 247, 252.
684 *Piltz*, in: Gola/Heckmann, Art. 20 Rn. 24.

die Transparenz gegenüber dem Betroffenen geht (anders als in Art. 15 Abs. 3 DS-GVO), wenn dieser für eigene Zwecke der Information und Dokumentation seine Daten sichern will. Vielmehr geht es um die weitere Verwendung dieser Daten in anderen Diensten. In Erwägungsgrund 68 findet sich eine weitere Bedingung, die entweder innerhalb der ausdrücklich im Gesetzestext genannten Anforderungen oder als eigenständiges Kriterium einzuhalten ist und wonach das Format interoperabel sein soll.

Eine nähere Beschreibung dieser Merkmale ist der DS-GVO nicht zu entnehmen. Das ist auch der Tatsache geschuldet, dass der Anwendungsbereich sich auf alle Verantwortlichen erstreckt, die Daten automatisiert verarbeiten, womit eine Vielzahl möglicher Daten und Anwendungsbereiche betroffen sein kann, von Beschäftigtenakten über Musik-Playlists bis hin zu Profilen in sozialen Netzwerken oder auf Online-Marktplätzen. Einheitliche Formate für alle diese Bereiche existieren nicht, und diese sind wohl auch keiner Vereinheitlichung zugänglich.[685] Daher sind aus Art. 20 DS-GVO nur Mindestanforderungen abzuleiten, die, orientiert am Ziel der Bestimmung, einer Auslegung zugeführt werden müssen, was sowohl Verarbeiter als auch Regulierungsbehörden und Gerichte (dazu sogleich unter C.IV.2.b) vor Herausforderungen stellen kann. Die „Gängigkeit" erfordert jedenfalls, dass es sich um ein auf dem Markt bekanntes Format wie z. B. TXT-, RTF-, XML-, JSON- oder CSV-Dateien handeln muss, die Maschinenlesbarkeit, dass eine Kompatibilität mit gängigen Betriebssystemen besteht. Die Strukturiertheit bezieht sich auf die Anordnungen der Informationen.[686]

Die Schaffung bestimmter Standards gibt die DS-GVO nicht vor. Der ursprüngliche Kommissionsvorschlag, der im Hinblick auf das Recht anders aufgebaut war,[687] enthielt eine solche Regelung, indem die Kommission die

685 So auch *Deusch/Eggendorfer*, in: DSRITB, 2019, S. 861, 866.

686 Zu technischen Umsetzungsmöglichkeiten eingehend *Deusch/Eggendorfer*, in: DSRITB, 2019, S. 861, 861 ff.

687 Art. 18 in dieser Fassung war noch unterteilt in das Recht auf Kopie in einem elektronischen Format und das Recht auf Übertragbarkeit. Abs. 2 des Entwurfs lautete: „Hat die betroffene Person die personenbezogenen Daten zur Verfügung gestellt und basiert die Verarbeitung auf einer Einwilligung oder einem Vertrag, hat die betroffene Person das Recht, diese personenbezogenen Daten sowie etwaige sonstige von ihr zur Verfügung gestellte Informationen, die in einem automatisierten Verarbeitungssystem gespeichert sind, in einem gängigen elektronischen Format in ein anderes System zu überführen, ohne dabei von dem für die Verarbeitung Verantwortlichen, dem die personenbezogenen Daten entzogen werden, behindert zu werden."

technischen „Standards, Modalitäten und Verfahren für die Überführung der personenbezogenen Daten" über Durchführungsrechtsakte hätte festlegen müssen.[688] Diese Formulierung der Bestimmung setzte sich aber wegen Bedenken zu Flexibilität und Reichweite der Norm in der finalen Fassung nicht durch.

Nach der finalen Fassung der DS-GVO besteht jedenfalls keine Pflicht zur Übernahme oder Beibehaltung technisch kompatibler Datenverarbeitungssysteme durch die Verarbeiter (Erwgr. 68). Das wäre auch nur dann sinnvoll, wenn die Empfängerseite an bestimmte Standards gebunden wäre (bspw. beim Wechsel zwischen sozialen Netzwerken sowohl Ausgangsanbieter als auch Zielanbieter die gleichen Formate nutzen und auslesen können müssten). Hierzu trifft aber Art. 20 DS-GVO keine Aussage, da nur der „Ausgangsverarbeiter" und nicht der „Zielverarbeiter" gebunden wird, wenngleich Letzterer auch selbst „Ausgangsverarbeiter" für andere Betroffene sein kann.

Das Recht auf Datenportabilität enthält zwar keine Zumutbarkeitsbedingung – auch die in Art. 20 Abs. 2 DS-GVO erwähnte „technische Machbarkeit" ist insbesondere nicht an wirtschaftliche, sondern an rein technische Umsetzungsmöglichkeiten geknüpft –, sodass sich Verarbeiter nicht unter Berufung auf eine (wirtschaftliche) Unmöglichkeit dem Recht entziehen können. Denkbar wäre in solchen Fällen aber eine Berufung auf Abs. 4, wonach die Übertragung nicht Rechte und Freiheiten beeinträchtigen soll, was bei weiter Auslegung auch als eine Art Angemessenheitsklausel zugunsten des „Ausgangsverarbeiters" dienen kann.[689] Zudem kann das Recht gem. Art. 12 Abs. 5 DS-GVO bei offenkundig unbegründeten oder exzessiven Anträgen verweigert werden. In der Praxis wird daher eine Betrachtung dessen, was Verarbeitern zumutbar ist, erfolgen müssen, was wiederum den Umfang der Portabilität bestimmt, für die es wie bei der Interoperabilität unterschiedliche technische Umsetzungsmöglichkeiten gibt.[690] Zudem ermöglicht die fehlende Spezifizierung und das Fehlen von Standards in der DS-GVO dem Verantwortlichen, unter Umständen durch ein potenziell weniger operables Format starke Lock-in-Effekte zu erzeugen.[691] Erwägungs-

688 COM/2012/011 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2012%3A0011%3AFIN.

689 So wohl *Wrobel*, in: DSRITB 2018, 247, 250.

690 Zu technischen Umsetzungsmöglichkeiten vgl. *Krämer/Senellart/de Streel*, Making Data Portability More Effective for the Digital Economy, S. 37 ff.

691 So auch *Paal*, in: Paal/Pauly, Art. 20 Rn. 20.

grund 68 enthält nur einen Appell, interoperable Formate zu entwickeln, aber keine Rechtspflicht dazu.[692] Weil nur auf den Betroffenen bezogene Daten übertragen werden dürfen, könnten technische Hürden zur Separierung von Drittdaten dazu führen, dass auf Seiten der Verantwortlichen eine Neigung besteht, nur (eindeutig dem Betroffenen zuzuordnende) Bestandsdaten zu übermitteln.[693]

Aufgrund dieser technischen Schwierigkeiten hat das Recht aus Art. 20 DS-GVO im Vergleich zum Auskunftsrecht in der Praxis bislang eine eher untergeordnete Rolle gespielt. Während vor allem größere Anbieter wie Meta oder Google entsprechende Funktionen zum Download der Daten zwar regelmäßig bereitstellen, ist die Übertragung an dritte Plattformen oder die unmittelbare Übertragung zwischen Diensten ohne aktive Maßnahme des Betroffenen in der Praxis zurückhaltend implementiert.[694] Bereits in ihrem ersten Evaluierungsbericht zur DS-GVO stellte die Kommission fest, dass Art. 20 DS-GVO in vielen Sektoren nicht vollständig beachtet wird.[695] Hinzu kommt, dass sich Betroffene im Vergleich zu anderen Rechten der DS-GVO über die Existenz ihres Rechts auf Datenportabilität weniger bewusst sind.[696]

Mit dem flexiblen Ansatz der DS-GVO hatten die Gesetzgeber gehofft, dass die Nachfrage der Nutzer nach solchen Möglichkeiten zu einem Wettbewerb der Anbieter um interoperable Angebote führen würde[697] und sich entsprechend nutzbare Formate aus der Industrie heraus entwickeln würden. Erwähnenswert ist in diesem Zusammenhang neben mehreren kleineren Projekten ein Projekt der vor allem marktdominierenden Akteu-

692 *Paal/Götz*, in: ZD, 2023, S. 67, 68.

693 *Jülicher/Röttgen/v. Schönfeld*, in: ZD, 2016, S. 358, 360 f.

694 Dazu auch *Nebel*, in: ZD-Aktuell, 2019, 04380; *Kuebler-Wachendorff et al.*, in: Informatik Spektrum, 4/2021, S. 264, 267 f.

695 Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation, COM/2020/264 final, Rn. 8.

696 So gaben in der Eurobarometerumfrage 487a der Europäischen Kommission 2019 (https://europa.eu/eurobarometer/surveys/detail/2222) 45 % der Befragten an, noch nie von dem Recht auf Datenübertragbarkeit gehört zu haben, 5 % antworteten mit „ich weiß nicht", 37 %, dass sie davon gehört hätten, aber es noch nicht in Anspruch genommen hätten. Nur 13 % hatten dieses Recht bereits geltend gemacht. Für neuere, aber im Ergebnis ähnliche Daten vgl. *Kuebler-Wachendorff et al.*, in: Informatik Spektrum, 4/2021, S. 264, 266.

697 *Paal*, in Paal/Pauly, Art. 20 Rn. 20.

re: Google hat 2018 eine Open-Source-Initiative gestartet, um den Datenaustausch zwischen verschiedenen Plattformen zu ermöglichen. An diesem Data Transfer Project beteiligen sich auch Facebook, Microsoft, X (ehemals Twitter) und Apple.[698] Ziel ist es, eine Open-Source-Plattform für die Datenportabilität von Dienst zu Dienst zu schaffen, damit alle Nutzer ihre Daten jederzeit problemlos zwischen Online-Dienstanbietern verschieben können. Kern ist eine Open-Source-Bibliothek, die jedem Dienst zur Verfügung steht, um direkte Übertragungen im Namen der Benutzer auszuführen und zu verwalten. Das öffnet dann auch Schnittstellen für kleinere Anbieter. Konkret baut das auf drei Komponenten auf: (1.) einer Reihe gemeinsamer Datenmodelle zur Einbeziehung jeder Art von Diensten (z. B. Fotos, Kontakte, Wiedergabelisten), (2.) Adaptern, die die Authentifizierung eines Benutzers bei einem Dienst und die Transformation von Daten zu und von den gemeinsam genutzten Datenmodellen übernehmen, und (3.) einem Aufgabenverwaltungsrahmen, der alle Teile zusammenfügt und abwickelt.

Aufgrund dreier Aspekte ist die Umsetzung des Datenportabilitätsrechts in der Praxis und dessen Inanspruchnahme durch Betroffene herausfordernd: aufgrund des unklaren bzw. auslegungsbedürftigen Anwendungsbereichs von Art. 20 DS-GVO, des Mangels an Klarheit in Bezug auf die Bedingungen der portablen Formate und der technischen Fragestellungen der Umsetzung.[699] Auch die Überwachung und Durchsetzung der Gewährleistung des Rechts findet vor diesem Hintergrund bislang nur zurückhaltend, in bestimmten Sektoren sogar „verschwindend gering“[700] statt.[701]

698 Vgl. dazu und weiterführend den Blog-Beitrag von Microsoft, abrufbar unter https://blogs.microsoft.com/eupolicy/2018/07/20/microsoft-facebook-google-and-twitter-introduce-the-data-transfer-project-an-open-source-initiative-for-consumer-data-portability/.

699 Eingehend *Kuebler-Wachendorff et al.*, in: Informatik Spektrum, 4/2021, S. 264, 265 f.

700 So *BKartA*, Abschlussbericht Sektoruntersuchung Messenger- und Video-Dienste, S. 130, in Bezug auf Messenger- und Videodienste. Den Angaben zufolge gab es hier zwischen null und 300.000 Anträge auf Datenportierung pro Jahr, also einen „verschwindend geringen“ Anteil im Vergleich zu den Nutzerzahlen der befragten Dienste.

701 *Krämer/Senellart/de Streel*, Making Data Portability More Effective for the Digital Economy, S. 10 f.; speziell zu Messenger-Diensten vgl. *BKartA*, Abschlussbericht Sektoruntersuchung Messenger- und Video-Dienste, S. 130, das darauf hinweist, dass die Handhabung seitens der Dienste (insb. in der Frage, welche Daten übermittelt werden) sehr unterschiedlich ist.

(4) Relevanz für Interoperabilität und Wettbewerb

Obwohl die DS-GVO grundsätzlich (auch) den freien Verkehr personenbezogener Daten in der Union schützt (Art. 1 Abs. 3 DS-GVO), ist Art. 20 DS-GVO eher auf den Schutz von Grundrechten und Grundfreiheiten von Betroffenen (Art. 1 Abs. 2 DS-GVO) ausgerichtet. Dies ändert aber nichts daran, dass sich die Portabilität von Daten bzw. deren Ermöglichung durch die Verarbeiter auch mittelbar für andere Binnenmarktziele förderlich auswirken kann.[702] So senkt die einfache und zugängliche Übertragbarkeit von Daten (bspw. Profilinformationen in sozialen Netzwerken,[703] E-Mails von Webmail-Diensten[704] etc.) auch die Hürden für den Wechsel zwischen Diensten, wirkt damit Lock-in-Effekten entgegen und stimuliert den Wettbewerb.[705]

Es überrascht daher nicht, dass im Rahmen des Legislativverfahrens zur DS-GVO diskutiert wurde, ob es sich bei dem Recht auf Datenportabilität nicht eher um ein Tool zur Förderung des Wettbewerbs handle und es daher nicht eher von einer datenschutzrechtlichen Regulierung auszuklammern und einer wettbewerbsrechtlichen zuzuführen sei.[706] Auch wurde vorgebracht, dass ein solches Recht im Datenschutz eher systemfremd sei und es stattdessen im allgemeinen Verbraucherschutzrecht verankert werden sollte.[707] Die wettbewerbsrechtliche Relevanz hängt aber auch davon ab, wie weit man den Anwendungsbereich von Art. 20 DS-GVO fasst, insbesondere welche Daten als bereitgestellt gelten und welche Qualität letztlich die Daten und Ausgabeformate haben.[708] Insoweit ist zwar anzuer-

702 Eingehend auch *Krämer/Senellart/de Streel*, Making Data Portability More Effective for the Digital Economy, S. 50 ff.

703 Dazu *Graef*, in: Telecommunications Policy, 39, 6, 2015, S. 502, 509.

704 Dazu etwa die Entscheidung der finnischen Datenschutzbehörde vom 22.3.2023 (Nr. 10048/182/20); vgl. *Etteldorf*, in: ZD-Aktuell, 2023, 01313.

705 In Bezug auf den Wechsel zwischen Diensten auch *Paal*, in Paal/Pauly, Art. 20 Rn. 4 f.; *Brüggemann*, in: DSRITB, 2017, S. 1, 5; *Wrobel*, in: DSRITB, 2018, S. 247, 247 f.

706 Council of the European Union, Interinstitutional File: 2012/0011 (COD), 10614/14, 6.6.2014, S. 3.

707 Vgl. zur Diskussion m. w. N. *Piltz*, in Gola/Heckmann, Art. 20 Rn. 1; *Paal*, in Paal/Pauly, Art. 20 Rn. 2.

708 *Krämer/Senellart/de Streel*, Making Data Portability More Effective for the Digital Economy, S. 50, heben insbesondere die wettbewerbsrechtliche Relevanz von abgeleiteten Daten (inferred data) hervor, die aber, wie oben unter C.IV.2.a(1) dargestellt, selbst bei extensiver Auslegung nicht unter Art. 20 DS-GVO fällt.

kennen, dass die Datenportabilität auch zumindest mittelbar wettbewerbsfördernd wirken kann, indem insbesondere das Multi-Homing erleichtert wird. Wie sich aber innerhalb des multidimensionalen Ansatzes verschiedener Gesichtspunkte des DMA ebenfalls zeigt, ist sie nicht alleiniger oder jedenfalls nur ein untergeordneter Faktor wettbewerbsrechtlicher Problematiken in der Digitallandschaft. In der bereits erwähnten Fusionskontrollentscheidung der Kommission zu *Facebook/WhatsApp* stellte die Kommission (jedoch vor Geltung der DS-GVO) sogar fest, dass Datenportabilität zumindest im Zusammenhang mit Kommunikations-Apps kein wettbewerbsrechtlich entscheidender Faktor sei, etwa indem der Wechsel zwischen Anwendungen durch fehlende Portabilität erschwert werde.[709] Das begründete sie damit, dass Chatverläufe weiterhin auf dem Endgerät abrufbar seien und auch Kontakte portierbar seien, wenngleich dies von entsprechenden Handlungen des Nutzers abhänge. Schwerpunkt der Datenportabilität des Art. 20 DS-GVO und damit auch die Rechtfertigung ihrer Verortung im Datenschutzrecht ist im Gegensatz zu solchen Erwägungen weitergehend die Emanzipation des Nutzers, der nach seinem Willen („auf Anfrage hin") ungehindert über die Verarbeitung seiner Daten (ggf. bei einem anderen Dienst) entscheiden können soll und damit mehr Kontrolle über die Daten erhält.

Vor diesem Hintergrund ist der Konnex zwischen Interoperabilität und Portabilität zu betrachten. Portabilität bzw. die Bereitstellung von gängigen Datenformaten kann zunächst Grundvoraussetzung von Interoperabilität sein, wenn die konkrete technische Umsetzung dies erfordert (bspw. bei Bridge-Lösungen, die eine Übersetzung von einem Format in ein anderes ermöglichen). Problematisch ist aber insoweit, dass Art. 20 DS-GVO keine dauerhafte Datenübertragung im Sinne einer aufrechtzuerhaltenden Programmierschnittstelle gewährleistet, sondern es sich jeweils um einen Einzelvorgang handelt. Weder ist daher eine solche Schnittstelle verpflichtend einzurichten noch haben Betroffene einen Anspruch auf dauerhafte Übertragungsströme. Vielmehr muss im Einzelfall geprüft werden, ob die Übertragung, wie oben dargestellt, aus Zumutbarkeitsgesichtspunkten (Art. 12 DS-GVO) und angesichts der technischen Machbarkeit mittels einer Schnittstelle erfolgen kann.[710] Eine nahtlose Anknüpfung von Interoperabilitätsbestimmungen an die Struktur von Art. 20 DS-GVO ist daher

709 COMP/M.7217 (Fn. 332) Rn. 113.
710 *Paal/Götz*, ZD, 2023, S. 67, 68.

nur bedingt effektiv.[711] Eine Erweiterung von Datenportabilitätsvorschriften hin zu einem näher an die Interoperabilität reichenden Umfang wäre aber grundsätzlich denkbar. Diese müsste dann insbesondere genauere Implikationen für die technische Umsetzung der Portabilität enthalten und entsprechende Bedingungen an die zeitkritische Umsetzung (bspw. Echtzeitübertragung von Daten an Drittunternehmen) stellen. Aus Verhältnismäßigkeitsgesichtspunkten wäre das aber nicht innerhalb des alle Verantwortlichen treffenden Anwendungsbereichs von Art. 20 DS-GVO möglich. Eine Beschränkung auf elektronische Kommunikationsdienste scheint aber denkbar, sodass entsprechende Ansätze in den Revisionsprozess der ePrivacy-Richtlinie durch einen Vorschlag für eine ePrivacy-Verordnung[712] eingebracht werden könnten.[713]

Ein großer Unterschied liegt auch in der Art und Weise, wie Portabilität und Interoperabilität Netzwerk- bzw. Lock-in-Effekten entgegenwirken sollen: Datenportabilität fördert zumindest mittelbar den Systemwechsel, ermöglicht also aktiv ein Multi-Homing und gestattet dem Nutzer eine freie Auswahl, aber keine Interaktion zwischen Systemen. Insbesondere wird der „Zielempfänger" von portablen Daten in Art. 20 DS-GVO nicht angesprochen, kann also deren Annahme verweigern, auch wenn dies den Sinn und Zweck des Rechts auf Datenübertragbarkeit insgesamt konterkariert. Praktisch gesprochen bedeutet dies bspw., dass auch in einer Situation, in der das soziale Netzwerk A seinen Nutzern den Download ihrer Daten in einem gängigen Paket ermöglicht, dieses Recht nicht weiterhilft, wenn das soziale Netzwerk B mit dem Paket nichts anfangen kann oder will (obwohl es in deren Geschäftsinteresse liegen dürfte, neuen Nutzern den Einstieg zu erleichtern). Datenportabilität schafft zudem allein keinen Anreiz für das Multi-Homing, sie erleichtert es nur. Um beim Beispiel der sozialen Netzwerke zu bleiben: Selbst wenn eine Portierung der Kontakte in ein

711 So im Ergebnis auch *BKartA*, Abschlussbericht Sektoruntersuchung Messenger- und Video-Dienste, S. 131, wo darauf hingewiesen wird, dass zwar eine unmittelbare Übertragung von Daten durch Art. 20 DS-GVO möglich sei, die z. B. auch für die Übertragung von Nachrichten gelten könnte, aber die fehlende Verankerung von zeitlichen Vorgaben das Gleichsetzen mit Interoperabilität hindere; vgl. auch *Monopolkommission*, Telekommunikation 2021, S. 88.

712 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final – 2017/03 (COD).

713 Ähnliches ansprechend (aber Interoperabilitätspflichten im Ergebnis ablehnend) *Monopolkommission*, Telekommunikation 2021, S. 106.

neues Netzwerk möglich ist, hilft das nicht darüber hinweg, dass mit dem Systemwechsel die Kommunikationsmöglichkeit mit den „alten" Kontakten entfällt oder zumindest davon abhängt, dass diese Kontakte auch im Zielnetzwerk aktiv sind. Interoperabilität hingegen will genau eine solche Interaktion ermöglichen und die Nutzerautonomie unabhängig vom Verhalten Dritter erhöhen. Allerdings stellt sich dies für Multi-Homing anders dar, da ein solches zwar möglich bleibt, aber Nutzer nicht unbedingt einen Anreiz dazu haben, wenn ihr gewähltes Stammsystem ohnehin mit allen anderen interoperabel ist.

Auch im Übrigen erfasst Datenportabilität nur einen Teilausschnitt von Interoperabilität, was der begrenzte Anwendungsbereich von Art. 20 DS-GVO (ebenso wie bei Art. 6 Abs. 9 DMA) veranschaulicht. Erfasst ist nur der einseitige Austausch von vom Betroffenen (oder im DMA: Endnutzer) bereitgestellten (oder im DMA: generierten) Daten mit Personenbezug (oder im DMA: auch ohne Personenbezug). Das ist nur ein Teil dessen, was durch mehrseitige Interaktion im Rahmen von Interoperabilität ermöglicht wird. Die Wahlfreiheit oder Autonomie bei der Datenportabilität erstreckt sich lediglich auf einen neuen oder weiteren Dienst, muss also mit einer weiteren aktiven Handlung verbunden werden. Bei Interoperabilität erstreckt sie sich auf die gesamte Kommunikation und Interaktion mit anderen Diensten oder bestimmten Funktionen.

Grenzen und (technische) Herausforderungen, die sich bei der Datenportabilität ergeben, sind aber zumindest in begrenzter Weise auf mögliche Interoperabilitätsbestimmungen übertragbar. Zum einen demonstrieren die Ausnahmen von Art. 20 Abs. 3 und 4 DS-GVO sowie insgesamt der begrenzte Anwendungsbereich des Datenübertragungsrechts, dass sich auch Interoperabilitätsbestimmungen in den geltenden gesetzlichen Rahmenbedingungen bewegen müssen. Insbesondere wären auch hier das Eigentumsrecht, vor allem das geistige Eigentum sowie Geschäftsgeheimnisse, und Rechte Dritter aus dem Privatsphärenschutz zu wahren. Das kann zu deutlichen Verkürzungen bei der Effektivität von Interoperabilität bzw. dem Ziel einer nahtlosen Interaktion führen. Die möglichen Vorteile von verbindlichen Interoperabilitätsvorschriften sind insoweit bereits abhängig von (sektor-)spezifischen rechtlichen Bestimmungen und dem Willen Dritter (bspw. dem Willen der Urheber, die Inhalte systemübergreifend zu lizenzieren, oder der Kontakte, in die Kommunikation über andere Plattformen einzuwilligen, etc.).

Zum anderen zeigt das Fehlen einheitlicher technischer Standards zur (effektiven) Umsetzung der Portabilität in der Praxis, dass das Bestehen einer entsprechenden Verpflichtung allein noch nicht zu Veränderungen im entsprechenden Marktsegment führt. Ohne die Förderung auch des technischen Fortschritts steht zu erwarten, dass das „Recht" auch weiterhin ein weitgehend ungenutztes bleibt. Der flexible Ansatz der DS-GVO ohne fest vorgeschriebene Standards ist zwar einerseits sinnvoll für den weiten Anwendungsbereich von Art. 20 DS-GVO, der den automatisiert verarbeitenden Handwerksbetrieb genauso erfasst wie die sehr große Online-Plattform.[714] Auch wird damit verhindert, dass ein dominanter Anbieter den Standard für alle anderen diktiert, da die Empfangsseite von den Regeln grundsätzlich nicht betroffen ist. Allerdings verursacht er andererseits Umsetzungsprobleme, wie auch die im Folgenden dargestellten Beispielverfahren zeigen.

b. Institutionelle Dimension

Die DS-GVO baut auf einem umfangreichen und komplexen Aufsichtssystem auf, das den zuständigen nationalen Aufsichtsbehörden weitreichende Untersuchungs- und Rechtsdurchsetzungsbefugnisse einräumt. Dabei bestehen ausdifferenzierte Mechanismen für die Zusammenarbeit, inklusive einer Kooperation der Behörden im Europäischen Datenschutzausschuss (EDSA) sowie dort stattfindender Kohärenzverfahren. Diese Mechanismen sind von besonderer Bedeutung für die grenzüberschreitende Rechtsdurchsetzung und Schaffung von unionsweiter Konsistenz der Anwendung der DS-GVO. Zu den Aufgaben des EDSA gehört zu diesem Zweck insbesondere die Erarbeitung von Leitlinien, die dazu dienen sollen, Klärung und Vereinheitlichung bei der Rechtsanwendung sicherzustellen. Gerade für den Bereich der Datenportabilität, die häufig aufgrund ihres Fokus auf den Online-Bereich grenzüberschreitende Bezüge hat, ist eine eingehende Betrachtung von Kohärenzbestrebungen sinnvoll.

714 Insoweit stellt sich aber eher der weite Anwendungsbereich von Art. 20-DS-GVO, der in seiner Schaffung eher u. a. auf soziale Netzwerke ausgerichtet war, als problematisch dar. Vgl. dazu auch *Dehmer*, in: ZD, 2020, S. 62, 63.

(1) Leitlinien zur Datenportabilität

Der EDSA bestätigte die mit der Datenschutz-Grundverordnung zusammenhängenden Leitlinien der (unter der Datenschutz-Richtlinie operativen) Artikel-29-Datenschutzgruppe bei seiner ersten Plenarsitzung.[715] Sie sind nicht unmittelbar verbindlich, dienen aber als Orientierungshilfe für die Auslegung und Umsetzung von Art. 20 DS-GVO.

Zu diesem Zweck wird in den Leitlinien zum Recht auf Datenübertragbarkeit der Artikel-29-Arbeitsgruppe, die bereits zur Bestimmung Stellung genommen hatte, zunächst der Anwendungsbereich erörtert. Mit Blick auf den Personenbezug von Daten heben die Leitlinien den weiten Anwendungsbereich mit Beispielen hervor. Art. 20 DS-GVO könnte etwa die aktuelle Wiedergabe- oder Einkaufsliste bei einem Musik-Streaming-Dienst, Kontakte aus Webmail-Anwendungen oder Informationen über Einkäufe mit verschiedenen Kundenkarten betreffen. Auch die Zielsetzung des Rechts auf Datenübertragbarkeit umschreiben die Leitlinien mit einem weiten Verständnis. Abgesehen davon, dass durch die Verhinderung des „Lock-in-Effekts" die Selbstbestimmung der Verbraucher gestärkt werde, bestehe auch die Erwartung, dass durch das Recht auf Datenübertragbarkeit Innovationsmöglichkeiten und ein sicherer Austausch personenbezogener Daten zwischen Verantwortlichen unter der Kontrolle der betroffenen Person gefördert würden. Die Datenübertragbarkeit könne den kontrollierten und begrenzten Austausch personenbezogener Daten zwischen Nutzern personenbezogener Daten in Organisationen begünstigen und so das Dienstleistungsangebot und die Kundenerfahrung bereichern.[716] Insoweit sieht auch die Artikel-29-Arbeitsgruppe, bestätigt durch den EDSA, wettbewerbsrechtliche und verbraucherschutzrechtliche Aspekte in Art. 20 DS-GVO aufgegriffen.

Konkretisierungen enthalten die Leitlinien auch zum Umfang der Verpflichtungen des Verantwortlichen: Es gibt keine spezifische Pflicht zur Überprüfung der Datenqualität vor der Datenübermittlung sowie keine über den üblichen Umfang hinausgehenden Speicher- und Aufbewahrungspflichten. Mit Letzterem beantwortet der EDSA auch inzident die Frage nach der Weitergeltung des Portabilitätsrechts nach Beendigung des Dienstes. Die Leitlinien bestätigen weiter, dass sich aus Art. 20 DS-GVO

715 Vgl. die Meldung vom 25. Mai 2018, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/right-data-portability_de.

716 *Artikel-29-Arbeitsgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, S. 6.

keine Pflichten für die Empfänger von Daten im Zusammenhang mit einer Portabilitätsanfrage ergeben und diese insbesondere nicht verpflichtet sind, Daten entgegenzunehmen oder weiterzuverarbeiten. Vielmehr wird sogar betont, dass der Empfänger wiederum selbst seinen üblichen Pflichten nach der DS-GVO unterliegt, d. h. insbesondere eine eigenständige Rechtsgrundlage für die Verarbeitung braucht und daher ggf. prüfen muss, ob das ihm übermittelte Datenpaket nicht über die Begrenzungen der DS-GVO hinausgeht. Genannt wird dabei das Beispiel von Datenübertragungen von einem Webmail-Dienst, bei dem nicht unbedingt auch Kontaktdaten der Adressaten von Mails gespeichert werden müssten.

In Bezug auf die Reichweite der Bestimmung gehen die Leitlinien von einer weiten Bedeutung der „bereitgestellten Daten" aus, die auch solche Daten erfasst, die aus einer Beobachtung des Betroffenen resultieren. Beispielhaft werden Rohdaten genannt, die in einem intelligenten Messgerät oder von anderen miteinander vernetzten Geräten in Tätigkeitsprotokollen oder in Webseiten- bzw. Suchverläufen verarbeitet werden.[717] Nicht darunter fallen sollen aber aus Rückschlüssen erzeugte und abgeleitete Daten. Beispiele hierfür wären ein Nutzerprofil auf der Basis einer Analyse von mithilfe eines intelligenten Zählers erfassten Rohdaten, die Ergebnisse einer Bewertung des Gesundheitszustands oder ein Risikoprofil, das im Zusammenhang mit dem Risikomanagement und Finanzvorschriften erstellt wurde. Insgesamt schließt dieses Verständnis algorithmische Ergebnisse aus, betrifft also auch die in einem medialen Kontext besonders relevanten Empfehlungsalgorithmen für Werbung oder Inhalte.

Im Kontext der Ausnahme vom Portabilitätsrecht bei Verletzung von Rechten Dritter gehen die Leitlinien vor allem auf Datenschutzinteressen Dritter ein. So wird betont, dass der Betroffene, der die Portabilität (auch) von Daten Dritter begehrt, selbst eine Rechtfertigungsgrundlage braucht, um diese dann in einem anderen Dienst zu nutzen. Das könnte sich insbesondere auf berechtigte Interessen stützen und dürfte bei der Übertragung von Webmail-Dienst- oder Konto-Daten (in beiden Fällen enthalten Datensätze auch Informationen über die Empfänger von Kommunikation oder Transaktion) einschlägig sein. Problematisch scheint aber, dass der EDSA die Verantwortung für ein Verhindern von Rechtsverletzungen teilweise auf den Betroffenen verlagert. So soll es unter die Ausnahme fallen (und damit kein Portabilitätsrecht bestehen), wenn der Empfänger der Daten (bspw. ein neuer Webmail-Dienst oder ein neues soziales Netzwerk) die in

717 *Artikel-29-Arbeitsgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, S. 11.

dem Datensatz enthaltenen Daten bspw. für Marketingzwecke verwenden würde (bspw. das Versenden elektronischer Werbung durch einen Webmail-Dienst oder ein soziales Netzwerk, das mit den Daten die Profile für Online-Werbung speist). Insofern müsste der Betroffene bei Drittpersonenbezug erst eine umfassende Prüfung der Datenschutzbedingungen des Ziels der Datenübertragung vornehmen, um zu beurteilen, ob die Übertragung für ihn sinnvoll und rechtmäßig möglich ist. Auch das schränkt eine Nutzung des Rechts aus Art. 20 DS-GVO mit Blick auf das Ziel von Multi-Homing signifikant ein.

Erwähnenswert sind weiter die Erläuterungen in den Richtlinien, unter welchen Umständen eine Anfrage zur Datenübertragung abgelehnt oder ein Entgelt berechnet werden kann. Die Leitlinien verweisen dazu auf den einzigen möglichen Fall der Ablehnung von Portabilitätsbegehren nach Art. 12 Abs. 5 DS-GVO bei exzessiven Anfragen. Es dürfte danach kaum Fälle geben, bei denen diese Verweigerungsmöglichkeit einschlägig sei, insbesondere beziehe sie sich nicht auf wirtschaftliche Argumente. Es bestehe jedoch die Möglichkeit, ein Entgelt für Portabilitätsanfragen zu berechnen (ebenfalls unter den Bedingungen des Art. 12 DS-GVO), allerdings könnten dabei dem Einzelnen die Implementierungskosten solcher Mechanismen nicht im Ganzen oder anteilig berechnet werden.

Schließlich enthalten die Leitlinien Erläuterungen zu der Frage, wie die Daten bereitgestellt werden müssen. Als geeignete Verfahren sieht der EDSA insbesondere zwei Methoden: direkte Übermittlung des vollständigen Datensatzes (oder mehrerer Auszüge von Teilen des Datensatzes) oder Einsatz eines automatisierten Werkzeugs, das die Extrahierung der relevanten Daten ermöglicht. Eine Bereitstellung könne z. B. über sichere E-Mails, SFTP-Server, sichere Web-Schnittstellen oder Web-Portale erfolgen. Betroffenen Personen sollte der Rückgriff auf einen persönlichen Datenspeicher, ein persönliches Informationsmanagementsystem oder andere vertrauenswürdige Dritte ermöglicht werden, damit sie die personenbezogenen Daten vorhalten und speichern und ggf. Verantwortlichen die Erlaubnis erteilen können, auf die personenbezogenen Daten zuzugreifen und sie zu verarbeiten.[718] Für die Maschinelesbarkeit wird auf Erwägungsgrund 21 der Richtlinie 2013/37/EU abgestellt:

> *[…] wenn [das Dokument] in einem Dateiformat vorliegt, das so strukturiert ist, dass Softwareanwendungen die konkreten Daten, einschließlich*

718 *Artikel-29-Arbeitsgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, S. 19.

einzelner Sachverhaltsdarstellungen und deren interner Struktur, einfach identifizieren, erkennen und extrahieren können. In Dateien verschlüsselte Daten, die in maschinenlesbarem Format strukturiert sind, sind maschinenlesbare Daten. Maschinenlesbare Formate können offen oder geschützt sein; sie können einem formellen Standard entsprechen oder nicht. Dokumente, die in einem Dateiformat verschlüsselt sind, das eine automatische Verarbeitung einschränkt, weil die Daten nicht oder nicht ohne Weiteres aus ihnen extrahiert werden können, sollten nicht als maschinenlesbar gelten. Dokumente, die in einem Dateiformat verschlüsselt sind, das eine automatische Verarbeitung einschränkt, weil die Daten nicht oder nicht ohne Weiteres aus ihnen extrahiert werden können, sollten nicht als maschinenlesbar gelten.

Im Übrigen zielen die Leitlinien aber nicht auf eine Entscheidung über ein Standardformat. Das am besten geeignete Format werde je nach Sektor unterschiedlich sein, und geeignete Formate existierten bereits, sollten jedoch stets so gewählt werden, dass sie die Voraussetzung der Lesbarkeit erfüllten und eine weitreichende Portabilität der Daten ermöglichten. Gibt es für eine Branche oder für einen Kontext keine gängigen Formate, sollten die Verantwortlichen personenbezogene Daten in gemeinhin verwendeten offenen Formaten (wie XML, JSON oder CSV) zusammen mit sachdienlichen Metadaten in der bestmöglichen Granularitätsstufe bereitstellen, dabei aber ein hohes Abstraktionsniveau beibehalten.

Hervorzuheben ist im vorliegenden Kontext aber insbesondere eine Aussage des EDSA: „Ziel der Übertragbarkeit ist es daher, nicht kompatible, sondern interoperable Systeme zu schaffen“[719]. Dabei nimmt der Ausschuss Bezug auf die eingangs genannte ISO-Definition zur Interoperabilität. Im Folgenden setzen die Leitlinien dieses Verständnis mit einer „Wiederverwendbarkeit“ der Datensätze zusammen, um die es im Kern gehen solle. Dem entspreche beispielsweise ein PDF, das den Posteingang eines Webmail-Dienstes darstelle, nicht. In dem Kontext empfiehlt der Ausschuss „nachdrücklich, dass Interessenvertreter der Branche und Fachverbände auf der Grundlage gemeinsamer interoperabler Standards und Formate zusammenarbeiten sollten, um die Anforderungen des Rechts auf Datenübertragbarkeit zu erfüllen“, und verweist auf bestehende Bestrebungen innerhalb des Europäischen Interoperabilitätsrahmens, der vor allem den Bereich e-Governance betrifft (dazu unten C.V.2).

719 *Artikel-29-Arbeitsgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, S. 21.

(2) Überwachung und Rechtsdurchsetzung

Die DS-GVO enthält ein umfangsreiches Rechtsdurchsetzungssystem, das sich auch auf die Durchsetzung von Betroffenenrechten bezieht. Die zuständigen nationalen Behörden können demnach etwa Warnungen beim Verstoß gegen Betroffenenrechte aussprechen, Verantwortliche zu rechtstreuem Verhalten anweisen (also hier: Portabilitätsanfragen zu entsprechen) oder auch Bußgelder verhängen.[720] Auch Verstöße gegen Art. 20 DS-GVO können nach Art. 83 Abs. 5 lit. b DS-GVO mit Geldbußen von bis zu 20 Mio. EUR oder im Fall eines Unternehmens von bis 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres geahndet werden. Das erstreckt sich aber nur auf den adressierten Verantwortlichen, der die Bereitstellung oder Übertragung vorzunehmen hat, nicht auf denjenigen, der die Annahme der bereitgestellten Daten verweigert.[721]

Für die Zuständigkeit einer Behörde ist in grenzüberschreitenden Zusammenhängen die Verteilung nach dem Prinzip der Federführung zu beachten (Art. 56 DS-GVO). Danach bleiben zwar alle nationalen Behörden zuständig für die Überwachung und Durchsetzung der DS-GVO auf ihrem Hoheitsgebiet, allerdings ist bei grenzüberschreitenden Datenverarbeitungsvorgängen nur die federführende Behörde der Hauptniederlassung für den Erlass von Maßnahmen zuständig. Bei Streitigkeiten kann ein Kohärenzverfahren unter Beteiligung des EDSA zum Einsatz kommen, das die federführende Behörde zu bestimmten Maßnahmen im Ergebnis verbindlich anweisen kann. Wegen des EU-Sitzes vieler größerer und vor allem der amerikanischen Anbieter im Online-Bereich in Dublin ist regelmäßig eine Zuständigkeit der irischen Data Protection Commission gegeben.

Nicht einheitlich beurteilt wird bislang die Frage, inwieweit den Aufsichtsbehörden ein Initiativ- und Durchsetzungsrecht bei Verstößen gegen Betroffenenrechte zukommt, wenn keine entsprechende Beschwerde eines Individuums vorliegt. Das hat bislang eine eher untergeordnete Rolle gespielt, weil die Betroffenenrechte, auch Art. 20 DS-GVO, an ein Antragserfordernis gebunden sind und ein Verstoß daher regelmäßig erst dann festgestellt wird, wenn ein solcher Antrag von einem Betroffenen gestellt

720 Vgl. für eine komplette Auflistung Art. 58 DS-GVO.

721 *Brüggemann*, in: DSRITB, 2017, S. 1, 11, mit Verweis aber auch auf a. A. von *Schürmann*, in: Eßer/Krämer/v. Lewinski, Art. 20 Rn. 38, der mit Sinn und Zweck von Art. 20 argumentiert.

und nicht ordnungsgemäß erfüllt wurde, sich der Betroffene daher mit einer Beschwerde an die Behörden gewandt hat.

In Bezug auf Art. 20 DS-GVO ist das aber besonders relevant, weil zwar auch hier ein Antragserfordernis besteht, aber Verantwortliche auf praktischer Ebene bereits entsprechende Mechanismen zur Datenportabilität vorhalten müssen, damit Nutzer sie ggf. in Anspruch nehmen können. Gerade im Bereich von Online-Plattformen dürfte es wenig wirtschaftlich sein, lediglich ad hoc auf Individualanfragen zu reagieren, sondern es werden im Nutzerbereich regelmäßig entsprechende Download-Bereiche bereitgestellt werden müssen. Insofern betrifft das die Frage, ob Datenschutzbehörden initiativ und flächendeckend überprüfen können, ob Datenportabilitätsmechanismen bereitgestellt werden, und ob sie ggf. entsprechende Abhilfemaßnahmen gegen Verantwortliche ergreifen. Wäre das nicht der Fall, ergäbe sich hier ein wesentlicher Unterschied zum Wettbewerbsrecht. Während das Datenschutzrecht (nur) das Recht zugunsten von Individuen beträfe, wären wettbewerbsrechtliche Maßnahmen wegen fehlender Portabilität im Sinne einer Pflicht zugunsten eines funktionierenden Binnenmarktes zu verstehen.[722] Es spricht viel dafür, die Möglichkeit der Datenschutzbehörden zu einer initiativen Kontrolle unter die allgemeine Befugniswahrnehmung zu subsumieren. Nach Art. 57 Abs. 1 lit a) DS-GVO hat jede Aufsichtsbehörde in ihrem Hoheitsgebiet die Anwendung der DS-GVO zu überwachen und durchsetzen, ohne dass dies auf bestimmte Bereiche beschränkt wäre.[723]

(3) Ausgewählte Entscheidungen zu Art. 20 DS-GVO

Eine Rechtsprechung des EuGH existiert, soweit ersichtlich, zum Recht auf Datenübertragung bislang nicht. Entscheidungen von Datenschutzbehörden und nationalen Gerichten sind, zumindest soweit veröffentlicht, ebenfalls eher selten.[724] Die wenigen ergangenen Entscheidungen zeigen

722 In diese Richtung wohl *Graef*, in: Telecommunications Policy, 39, 6, 2015, S. 502, 514.

723 Im Ergebnis, ohne die Frage direkt zu adressieren, auch *Krämer/Senellart/de Streel*, Making Data Portability More Effective for the Digital Economy, die für eine stärkere Überwachung der Umsetzung plädieren.

724 Vgl. dazu den Überblick in der Datenbank von GDPR.hub, die nationale Entscheidungen umfänglich dokumentieren, https://gdprhub.eu/index.php?title=Category:Article_20_GDPR.

aber die Vielschichtigkeit möglicher Fallgestaltungen und dass in deren Zentrum regelmäßig eine Berufung auf die oben dargestellten Leitlinien des EDSA steht. Ausgewählte Entscheidungen mit medien- und kommunikationsrechtlicher Relevanz[725] sollen daher nachfolgendend dargestellt werden.

(a) Finnland: Datenportabilität bei E-Mail-Diensten und Art der Bereitstellung

Mit Entscheidung vom 22. März 2023 äußerte sich die finnische Datenschutzbehörde zum Recht auf Datenportabilität im Zusammenhang mit Webmail-Diensten.[726] Sie stellte fest, dass dieses Recht auch auf E-Mails anwendbar ist, die innerhalb eines Mailing-Diensts verarbeitet werden, und dass es dabei nicht einem „gängigen und strukturierten Format" entspricht, wenn der Verantwortliche den Betroffenen lediglich auf die Möglichkeit verweist, seine E-Mails selbst und jeweils einzeln zu exportieren. Auch entspreche es nicht dem Grundsatz der Unentgeltlichkeit (Art. 12 Abs. 5 DS-GVO), wenn (nur) zahlenden Kunden ein Tool zum Gesamtexport aller Mails zur Verfügung gestellt werde.[727]

Im zugrunde liegenden Fall hatte ein registrierter Nutzer eines verschlüsselten E-Mail-Diensts 2020 im Rahmen eines geplanten Anbieterwechsels gegenüber seinem bisherigen Anbieter eine Übertragung seiner E-Mails verlangt. Der Diensteanbieter verweigerte jedoch eine Übertragung mit dem Hinweis darauf, dass er einerseits die Anwendbarkeit von Art. 20 DS-GVO auf E-Mails bereits für fragwürdig halte und andererseits der Betroffene jedenfalls die Möglichkeit habe, seine E-Mails jeweils einzeln in einem „.eml"-Format selbst zu exportieren. Für zahlende Nutzer des

725 Das Recht auf Datenportabilität spielt aber häufig auch in freiberuflichen Arbeitsverhältnissen oder in Bezug auf Gesundheitsdaten eine Rolle. Vgl. hierzu etwa die Entscheidungen aus den Niederlanden zu der Uber- und Ola-Driver-App (Rb. Amsterdam – C/13/689705/HA RK 20–258, https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBAMS:2021:1019&showbutton=true&keyword=AVG, Rb. Amsterdam – C/13/687315 / HA RK 20–207, https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBAMS:2021:1020) oder die Entscheidung aus Belgien über die Portabilität von Daten beim Wechsel zu einer neuen Krankenversicherung (Gegevensbeschermingsautoriteit, No. DOS-2023–00609, https://www.gegevensbeschermingsautoriteit.be/publications/zonder-gevolg-nr.-45-2023.pdf).

726 Tietosuojavaltuutetun toimisto, No. 0048/182/20, https://finlex.fi/fi/viranomaiset/tsv/2023/20231883.

727 Vgl. *Etteldorf*, in: ZD-Aktuell, 2023, 01315.

E-Mail-Dienstes, zu denen der Betroffene jedoch nicht gehörte, stand indessen ein Tool zur Verfügung, mit dessen Hilfe alle E-Mails in einer Gesamtdatei exportiert werden konnten. Dieses sollte zu gegebener Zeit auch für nicht zahlende Nutzer zur Verfügung stehen; Verzögerungen begründete der Anbieter dabei mit der aufwändigen technischen Umsetzung, die auf die Verschlüsselung der E-Mails zurückzuführen sei.

Die finnische Datenschutzbehörde sah in diesem Verhalten einen Verstoß gegen Art. 12 Abs. 5 DS-GVO und Art. 20 DS-GVO. Zunächst stellte sie dabei fest, dass Art. 20 DS-GVO auch auf E-Mails anwendbar sei. Dieses Recht umfasse personenbezogene Daten, die die betroffene Person bewusst und aktiv bereitstelle, sowie Daten, die durch ihre Aktivitäten erzeugt würden, wozu auch E-Mails gehörten. Es entspreche aber nicht dem Recht auf Datenübertragbarkeit bzw. der korrespondierenden Pflicht des Verantwortlichen, wenn er Betroffene auf ein einzelnes und manuelles Abspeichern von Mails verweist, da es sich hierbei nicht um ein „strukturiertes und gängiges" Format handle. Die Behörde begründet das mit dem erheblichen Aufwand, den der Betroffene sonst betreiben müsste, denn Nutzer der kostenlosen Version des E-Mail-Dienstes könnten 150 E-Mails pro Tag versenden, was sich bereits nach einem Monat auf über 4.000 E-Mail-Nachrichten summieren könne, wobei eingehende Mails noch hinzukämen. Das manuelle Exportieren von Nachrichten im Einzelnen sei langsam und die Gewährleistung des Rechts nach Art. 20 DS-GVO daher für Betroffene sehr zeitaufwändig, was laut Behörde im vorliegenden Fall dazu führe, dass der Verantwortliche dieses Recht praktisch erschwere und seine Geltendmachung gleichsam verhindert habe.

Auch die in Art. 12 Abs. 5 DS-GVO verankerte grundsätzliche Unentgeltlichkeit der Rechteausübung sei durch das Vorgehen nicht gewahrt, da der Verantwortliche, indem er ein (die Grundsätze von Art. 20 DS-GVO wahrendes) Tool nur zahlenden Kunden anbiete, die vollständige Ausübung des Rechts praktisch unter den Vorbehalt der Entgeltlichkeit stelle. Zwar sehe Art. 12 Abs. 5 DS-GVO die Möglichkeit vor, bei offensichtlich unbegründeten oder unangemessenen Anträgen ein Entgelt zu verlangen. Das habe der Verantwortliche aber vorliegend weder bewiesen noch vorgebracht, sondern sich nur generell auf einen zeit- und finanzaufwändigen Entwicklungsprozess des Tools berufen. Ein Bußgeld verhängte die Behörde neben der Feststellung des Verstoßes nicht.

Aus der Entscheidung aus Finnland geht vor allem eine verbraucherschutzrechtliche Perspektive des Rechts auf Datenportabilität hervor. Die Portabilität soll nicht nur gewährleistet, sondern auch erleichtert werden.

(b) Österreich: Datenportabilität bei eingestellten Apps und gängige Dateiformate

Das Österreichische Bundesverwaltungsgericht entschied mit Urteil vom 7. September 2023, dass gegenüber App-Betreibern eingestellter Apps kein Anspruch auf Datenportabilität besteht, wenn personenbezogene Daten nur lokal auf dem Endgerät von Nutzern verarbeitet wurden und der App-Betreiber keinen Zugang zu diesen Daten hat. Ferner könnten, soweit eine Verpflichtung zur Bereitstellung von Daten besteht, personenbezogene Daten zulässigerweise in den Dateiformaten JSON und GPX übertragen werden, die das Erfordernis eines strukturierten, gängigen, maschinenlesbaren und interoperablen Formats erfüllen.[728]

Im zugrunde liegenden Fall hatte die Nutzerin einer Lauf-App Beschwerde bei der österreichischen Datenschutzbehörde gegen den Betreiber der App erhoben, weil dieser sich geweigert hatte, Trainingsdaten zu aufgezeichneten Sportaktivitäten (bspw. Laufstrecke, Distanz, Zeit) an die Nutzerin zu übertragen. Bis Dezember 2020 waren über die App aufgezeichnete Trainingsdaten dieser Nutzerin an den Betreiber der App übermittelt worden. Anschließend wurde die Lauf-App durch eine neue App desselben Betreibers ersetzt. Nach Abschaltung der „alten" App konnten weiterhin lokal auf dem Gerät der Nutzerin Trainingsdaten erhoben und gespeichert werden, diese wurden jedoch nicht mehr an den App-Betreiber übermittelt. Die bis Dezember 2020 an den App-Betreiber übermittelten Daten konnte die Nutzerin in den Dateiformaten JSON (textbasiertes Datenformat zum Speichern und Übertragen von Daten) und GPX (Datenformat zum Austausch von Geodaten) mit einem Tool auf der Webseite des App-Betreibers exportieren. Die Nutzerin beschwerte sich darüber, dass es sich bei JSON und GPX um keine gängigen maschinenlesbaren und interoperablen Dateiformate handle, die daher für die Durchschnittsanwenderin unbrauchbar seien, weil sie etwa eine grafische Darstellung der Trainingsdaten wie in der Ansicht in der App nicht ermöglichten.

Die Datenschutzbehörde wies 2022 die Beschwerde der Nutzerin ab, da der App-Betreiber ab Dezember 2020 keine Verarbeitung personenbezogener Daten im Sinne der DS-GVO mehr vorgenommen habe und es sich bei JSON und GPX um strukturierte, gängige, maschinenlesbare und interoperable Dateiformate handle. In Rahmen der hiergegen erhobenen Klage schloss sich letztinstanzlich auch das Österreichische Bundesverwaltungs-

728 Vgl. *Braun*, in: ZD-Aktuell, 2023, 01440.

gericht dieser Argumentation an. Da es infolge der Abschaltung der App ab Dezember 2020 zu keiner Übermittlung von Trainingsdaten oder anderer personenbezogener Daten an den App-Betreiber kam, wurden die Daten ausschließlich durch die Nutzerin selbst, nicht aber durch den App-Betreiber verarbeitet. Die Voraussetzungen für die Verpflichtung zur Datenübertragbarkeit nach Art. 20 DS-GVO seien daher ab dem Zeitpunkt nicht mehr gegeben. Für Daten vor Dezember 2020 bestehe jedoch ein Anspruch auf Datenübertragbarkeit, den der App-Betreiber erfüllt habe. Der Anspruch erfasst laut Gericht lediglich die durch die betroffene Person selbst aktiv bereitgestellten Daten sowie Trainingsdaten, die durch die Nutzung der App oder durch Beobachtung angefallen sind. Nicht mehr als „bereitgestellt" i. S. d. Art. 20 Abs. 1 DS-GVO würden jedoch solche Daten gelten, die aus Ableitungen oder Rückschlüssen von diesen Kategorien von Daten erzeugt worden seien. Im Rahmen des Rechts auf Datenübertragbarkeit bestehe daher kein Anspruch auf eine entsprechend grafisch attraktive Darstellung. Auch stellten die Datenformate JSON und GPX weit verbreitete, gängige, strukturierte und interoperable Datenformate dar, da sowohl JSON als auch GPX ohne (anbieter-)spezifische Programme geöffnet und weiterverwendet werden könnten.

Die Entscheidung aus Österreich hebt hervor, dass es (unabhängig von der Art der Bereitstellung, auf der bei der finnischen Entscheidung der Fokus lag) bei dem Format nicht um eine Information des Nutzers, mithin um eine nutzerfreundliche Darstellungsweise geht. Vielmehr stehen die Übertragbarkeit und Nutzbarkeit der Formate innerhalb eines anderen Dienstes im Vordergrund. Bemerkenswert ist dabei, dass sich das Österreichische Bundesverwaltungsgericht auf Formulierungen stützt, wie sie sich aus der Auslegung durch die Leitlinien des EDSA ergeben.

(c) Belgien: Übertragung einer Facebook-Fanpage

Am 12. Januar 2021 entschied die belgische Aufsichtsbehörde in einem Rechtsstreit über eine Facebook-Fanpage.[729]

In der zugrunde liegenden Rechtssache hatte eine Musikerin zunächst die Verwaltung ihrer Facebook-Fanpage, die ihren Namen und Vornamen trug, an einen Musikverlag übertragen. Nachdem die vertraglichen Bezie-

729 Gegevensbeschermingsautoriteit, No. DOS-2020–01192, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-02-2021.pdf.

hungen mit dem Produzenten allerdings endeten, machte sie eine Rückübertragung der Rechte an dieser Fanpage geltend und stützte sich dabei gegenüber dem Musikverlag (aber nicht gegenüber Meta) auch auf Art. 20 DS-GVO. Der Verlag brachte demgegenüber vor, dass auf der Fanpage auch urheberrechtlich geschützte Materialien des Verlages gepostet würden (Fotos und Videos) und diese sich allein beruflichen Zwecken widmeten, nicht aber in Beziehung zu der Musikerin als Privatperson stünden. In Bezug auf Art. 20 DS-GVO müsse dies bedeuten, dass hier keinerlei Daten von einer natürlichen Person bereitgestellt seien, der Anspruch also nicht bestehe. Selbst wenn das der Fall wäre, würde die Übertragung aber zumindest die Urheberrechte des Verlags verletzen, der Investitionen in die Fanpage getätigt habe, wäre also aufgrund einer Verletzung von Rechten Dritter vom Anwendungsbereich des Art. 20 DS-GVO ausgenommen. Auf eine Übertragung von „Verwaltungsrechten" an einer Fanpage sei die Regel im Übrigen nicht anwendbar, da hier kein Datenschutzrecht, sondern Urheberrecht betroffen sei.[730]

Da der Verlag im Ergebnis eine Übertragung verweigerte, wandte sich die Betroffene an die belgische Datenschutzbehörde, u. a. mit dem Begehren, dass die Behörde den Verlag zur Übertragung anweise. Diese gab der Musikerin recht.

Zunächst stellte die Behörde dabei fest, dass es für die Anwendbarkeit des Datenschutzrechts (und damit die Zuständigkeit der Behörde) keinen Unterschied mache, ob Daten in einem beruflichen oder privaten Kontext erhoben würden. Im Übrigen sei es dafür auch irrelevant, dass die Fanpage nur in Teilen aus personenbezogenen Daten bestehe, da sie durch die deutliche Benennung des Profils jedenfalls mit personenbezogenen Daten verbunden sei. In Bezug auf das Recht auf Datenportabilität subsumierte die Behörde den Sachverhalt eindeutig unter Art. 20 DS-GVO: Im Rahmen eines Vertragsverhältnisses habe die Musikerin dem Verlag personenbezogene Daten wie ihren Namen und ihr Bild zur Verfügung gestellt. Der Verlag habe diese – u. a. – zur Erstellung und Verwaltung einer Fanpage auf Facebook genutzt, was aufgrund des zugrunde liegenden Vertragsverhältnisses gemäß Art. 6 Abs. 1 lit. b DS-GVO zulässig gewesen sei. Damit bestehe der Anspruch. Mit Art. 20 DS-GVO, so die Behörde in ihrer Entscheidung, habe der EU-Gesetzgeber die Kontrolle über die eigenen Daten für die

730 An der Stelle sei angemerkt, dass ähnliche Fälle bereits unter Art. VI 104 des belgischen Wirtschaftsgesetzbuches entschieden wurden. Dabei wurde in dem Betrieb einer Fanpage für einen anderen ein unlauteres Marktverhalten gesehen.

Betroffenen stärken wollen, und das insbesondere in einem digitalen Online-Umfeld, in dem soziale Medien ein großes Publikum erreichten. Ein Übertragungsrecht sah die Behörde zwar nicht im Verhältnis der Musikerin und dem Verlag, wohl aber zwischen dem Verlag und Facebook. Gemäß Art. 20 Abs. 2 DS-GVO könne von einem für die Verarbeitung Verantwortlichen (dem Verlag) erwartet werden, dass er die personenbezogenen Daten direkt an einen anderen für die Verarbeitung Verantwortlichen (Facebook) übermittle, damit dieser die (Verwaltungsrechte für die) Fanpage dem Betroffenen (der Musikerin) zur Verfügung stellen könne.

Das Argument der Verletzung von Urheberrechten und kommerziellen Interessen ließ die Behörde zwar gelten, kam aber bei der erforderlichen Abwägung zu dem Ergebnis, dass die Fanpage so eng mit der Identität der Musikerin verbunden sei, dass ihre Interessen überwiegen müssten. Wenn die Übermittlung überhaupt in die Rechte und Freiheiten des Verlags eingreife, so sei dies eine Folge eines (früheren) Vertragsverhältnisses. Dies rechtfertige jedoch in keiner Weise das „Hijacking" der personenbezogenen Daten einer betroffenen Person und den diesbezüglichen Rechtsschutz, insbesondere dann nicht, wenn die betroffene Person zuvor zu erkennen gegeben habe, dass sie die Verwaltung der Fanpage selbst übernehmen wolle.

Im Ergebnis sprach die Behörde ein Bußgeld in Höhe von 10.000 EUR aus, wobei dieses sich auch auf andere Verletzungen des Rechts auf Schutz personenbezogener Daten bezog. Eine Anweisung zur Vornahme der Datenübertragung sprach die Behörde nicht aus, allerdings aus formalen Gründen, da die Musikerin nicht nachweisen konnte, dass sie einen solchen Antrag gegenüber dem Verlag gestellt hatte, und eine Zwischenentscheidung der Datenschutzbehörde, die eine entsprechende Anweisung enthalten hatte, war ebenso aus formalen Gründen aufgehoben worden. Es bestand also zum Entscheidungszeitpunkt keine entsprechende Verpflichtung zur Bereitstellung der Daten. Im Übrigen hatte sich der Übertragungsanspruch während der Untersuchung erledigt, weil Meta als Betreiber des sozialen Netzwerks eingeschritten war und die Verwaltung der Fanpage wie beantragt an die Musikerin zurückübertragen hatte.[731] Dennoch wies die Behörde angesichts der im Verfahren offenkundig werdenden Weigerung

731 Am 26. Mai 2021 entschied im Übrigen das Beschwerdegericht in Brüssel (Hof van Beroep) ebenfalls in dieser Sache (Beschwerdegericht, No. 2021/AR/205, https://www.gegevensbeschermingsautoriteit.be/publications/arrest-van-26-mei-2021-van-het-marktenhof-ar-205.pdf). Der Aspekt der Datenübertragbarkeit spielte aber aus den genannten Gründen auch hier keine Rolle mehr.

des Musikverlags in ihrer Entscheidung allgemein darauf hin, dass der Musikverlag die erforderlichen Maßnahmen ergreifen müsse, um den Rechten betroffener Personen, insbesondere dem Recht auf Übertragbarkeit, rechtlich korrekt entsprechen zu können, wenn die betroffenen Personen einen entsprechenden Antrag stellten.

Die Entscheidung aus Belgien zeigt, dass das Recht nach Art. 20 DS-GVO auch in eher atypischen Konstellationen Anwendung finden kann und sich Formate nicht unbedingt auf Datenpakete beschränken müssen.

3. Deutschland

a. Umsetzung der EU-Vorgaben aus Art. 20 DS-GVO

Anders als in Bezug auf andere Betroffenenrechte (Information, Auskunft, Widerspruch und Löschung) hat der deutsche Gesetzgeber in Bezug auf das Recht auf Datenportabilität keine zusätzlichen Bestimmungen neben der DS-GVO in §§ 32 ff. des Bundesdatenschutzgesetzes vorgesehen. Insoweit bestand allerdings bei Art. 20 DS-GVO auch ein geringerer Ausgestaltungsspielraum. Daher ergeben sich auf materiell-rechtlicher Ebene keine Besonderheiten, die von der vorherigen Darstellung der EU-Ebene abweichen.

b. Institutionelle Dimension

(1) Aufsichtssystem

Das institutionelle System der Datenschutzaufsicht in Deutschland ist komplex und tritt zu dem bereits komplexen System nach der DS-GVO hinzu.

Der Bundesbeauftragte für den Datenschutz (BfDI) ist zum einen für die Datenschutzaufsicht bei öffentlichen Stellen des Bundes zuständig. Das betrifft also etwa Bundesbehörden, bundesunmittelbare Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie öffentlich-rechtliche Unternehmen des Bundes. Zum anderen beaufsichtigt der BfDI die Einhaltung des Datenschutzes bei Unternehmen, die Telekommunikations- oder Postdienstleistungen erbringen oder unter das Sicherheitsüberprüfungsgesetz fallen. Für Anbieter von Telekommunikations- oder Postdienstleistungen gilt das nur, soweit sie personenbezogene Daten zur Erbringung dieser

Dienste verarbeiten, also nicht etwa auch für ihre Teilnahme am Adresshandel oder im Bereich des Beschäftigtendatenschutzes.

Für den Bereich des Datenschutzes bei wirtschaftlichen Unternehmen sind dagegen die Datenschutzbehörden der Länder zuständig, bestimmt nach dem Sitz des Verantwortlichen. Zur besseren Koordinierung länderübergreifend relevanter Fragen haben sich diese Behörden und der BfDI in der unabhängigen Datenschutzkonferenz (DSK) des Bundes und der Länder zusammengeschlossen. Aufgabe dieses Gremiums ist es, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten.[732] Hierzu erlässt die DSK (unverbindliche) Entschließungen, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen. Eingerichtet sind auch Arbeitskreise zu verschiedenen Themen wie etwa „Datenschutz-/Medienkompetenz" und „Medien".

Für die Datenverarbeitung zu journalistischen Zwecken gelten wiederum andere Regeln, die auf der Basis des Medienprivilegs in Art. 85 DS-GVO eingeführt worden sind. Das bedeutet, dass für diesen Bereich, nicht aber auch für die Wirtschaftstätigkeit von Presse, Rundfunk und journalistisch-redaktionellen Telemedien andere Aufsichtssysteme gelten.[733] Im Bereich des öffentlich-rechtlichen Rundfunks sind Rundfunkdatenschutzbeauftragte in den Anstalten selbst eingerichtet, die die Aufsicht führen. Für den privaten Rundfunk gelten in den Bundesländern unterschiedliche Regeln, die entweder eine Aufsicht der Landesmedienanstalten oder der Datenschutzbehörden oder Mischformen vorsehen. Für die Presse und journalistisch-redaktionelle Telemedien kann dagegen eine Aufsicht durch den Deutschen Presserat einschlägig sein, wenn sie dem Pressekodex angeschlossen sind.

Im Übrigen ist aber zu beachten, dass sich das System der Federführung aus der DS-GVO in Deutschland fortsetzt. So ist nur dann die Zuständigkeit Deutschlands und hier wiederum föderal untergliedert der Datenschutzbehörde eines Landes gegeben, wenn die Hauptniederlassung eines Anbieters in Deutschland bzw. der Sitz in dem entsprechenden Land liegt. Global agierende Player, die im medienrechtlichen Kontext relevant sind, haben ihre Hauptniederlassung regelmäßig nicht in Deutschland. Wie das Dringlichkeitsverfahren des Hamburgischen Datenschutzbeauftragten

732 Vgl. dazu die Geschäftsordnung der DSK, https://www.datenschutzkonferenz-online.de/media/dsk/Geschaeftsordnung_DSK_Stand_November-2023.pdf.

733 Für eine synoptische Übersicht des komplexen Systems sowie der jeweiligen gesetzlichen Regeln auf Landesebene *Etteldorf*, in UFITA, 1/2018, 170 ff.

zur Datenzusammenführung von WhatsApp- und Facebook-Daten gezeigt hat, das letztlich vor dem EDSA verhandelt wurde, bestehen aber auch Einwirkungsmöglichkeiten auf globale Player.[734]

(2) Datenschutzkonferenz

Speziell zum Recht nach Art. 20 DS-GVO hat sich die DSK noch nicht mit Entschließungen, Beschlüssen, Orientierungshilfen, Standardisierungen oder Stellungnahmen positioniert. Insoweit verweist sie auf die einschlägigen Leitlinien auf EU-Ebene. Im Vorfeld der Einführung des Rechts hatte sich die DSK ausdrücklich für die Schaffung eines solchen Rechts vor dem Hintergrund der Begrenzung von Marktmacht und Schutz der informellen Selbstbestimmung ausgesprochen.[735] Insbesondere das Recht auf Datenportabilität könne sowohl die Souveränität des einzelnen Nutzers stärken als auch die auf der Sammlung personenbezogener Daten beruhende Machtposition einzelner Marktteilnehmer begrenzen.

In diesem Zusammenhang wurde auch für eine Stärkung der Zusammenarbeit zwischen Wettbewerbs- und Datenschutzbehörden plädiert. Im Übrigen können aber, wie bereits oben innerhalb der Beschreibung von Grenzen des Portabilitätsrechts erwähnt, Positionierungen der Datenschutzkonferenz zu anderen Themen, etwa zu den Voraussetzungen der Einwilligung, auch für die Beurteilung von neuen oder bestehenden Interoperabilitätsvorschriften relevant sein.

(3) Ausgewählte Entscheidungen

Das Recht aus Art. 20 DS-GVO hat bislang in Entscheidungen aus Deutschland, soweit ersichtlich, kaum eine Rolle gespielt. Dabei ist aber

734 Vgl. Urgent Binding Decision 01/2021 on the request under Article 66(2) GDPR from the Hamburg (German) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited, https://edpb.europa.eu/our-work-tools/our-documents/urgent-binding-decision-board-art-66/urgent-binding-decision-012021_en.

735 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. und 9. Oktober 2014 in Hamburg, https://www.datenschutzkonferenz-online.de/media/en/20141008_en_Marktmacht_und_informationelle_Selbstbestimmung.pdf.

anzumerken, dass die Landesdatenschutzbehörden ihre Entscheidungen regelmäßig nicht veröffentlichen und nur selten Pressmitteilungen zu besonders relevanten Fällen herausgeben. Insoweit werden Entscheidungen häufig erst dann sichtbar, wenn sie den Weg zu den Gerichten finden. Aber auch hier spielte, soweit ersichtlich, Art. 20 DS-GVO höchstens eine Nebenrolle,[736] während das Recht auf Kopie nach Art. 15 Abs. 3 DS-GVO (auch in Abgrenzung zu Art. 20 DS-GVO)[737] das weitaus häufiger geltend gemachte Betroffenenrecht ist.

Eine – ebenfalls nicht offiziell veröffentlichte – Entscheidung des BfDI vom 27. Januar 2022 dürfte zwar kommunikationsrechtliche Relevanz haben, ist aber in Bezug auf Art. 20 DS-GVO wenig ergiebig, obwohl sie die enge Reichweite der Vorschrift nochmals hervorhebt.[738] Darin ging es um eine Auskunfts- und eine Übertragungsanfrage (Art. 15 und 20 DS-GVO) eines Kunden gegenüber der Deutschen Telekom. Diese wurden zwar erfüllt, aber nach Ansicht des Kunden nicht vollständig. Insbesondere beschwerte sich der Kunde, dass Informationen über seine Verkehrsdaten, seine Verträge mit dem für die Verarbeitung Verantwortlichen und seine Anfragen an den Kundendienst fehlten. Außerdem seien nicht alle Empfänger in den ihm übermittelten Unterlagen, sondern nur die „wichtigsten" aufgeführt und es würden Daten zur Internetnutzung sowie zur Nutzung von MagentaTV fehlen. Er reichte daher eine Beschwerde beim BfDI ein, der ihr stattgab.

Bezüglich Art. 20 DS-GVO hob der BfDI aber hervor, dass diese Vorschrift nur eine Teilmenge der Daten betreffe, für die nach Art. 15 DS-GVO ein Auskunftsrecht bestehe. Die vom Kunden begehrten Serviceanfragen, IP-Adressen und Internetverbindungen (Dokumentation besuchter Webseiten) seien hiervon nicht erfasst. So würden Serviceanfragen regelmäßig nicht automatisiert verarbeitet, sondern schriftlich, IP-Adressen würden zugewiesen und nicht vom Kunden übermittelt, und Internetverbindungen

736 Etwa bei LSG Nordrhein-Westfalen, Beschluss vom 17.06.2021 – L 15 U 144/21 B ER in Bezug auf die Herausgabe einer Verwaltungsakte auf CD-ROM, wo aber letztlich ein Anspruch wegen des mangelnden Personenbezugs nicht in Betracht kam, wie auch bei VG Weimar, Beschluss vom 02.03.2021 – 3 E 209/21 in Bezug auf die Kopie einer Approbationsurkunde

737 Vgl. dazu etwa OVG Nordrhein-Westfalen, Urteil vom 08.06.2021 – 16 A 1582/20, wo es um die Herausgabe einer schriftlichen Kopie eines Examens ging. Hier ging das Gericht insbesondere auf die Abgrenzung zu Art. 20 DS-GVO ein.

738 Für eine Zusammenfassung sowie eine englische Fassung der Entscheidung Hanusch, BfDI (Germany) – 24–191 II, https://gdprhub.eu/index.php?title=BfDI_(Germany)_-_24-191_II.

würden vom Telekommunikationsanbieter nicht erfasst. Im Übrigen sah der BfDI die Kritik an dem von der Telekom bereitgestellten Format als unbegründet.

V. Geltender Rechtsrahmen zur Interoperabilität: weitere relevante Rechtsgebiete

1. Interoperabilitätsrelevante Aspekte im Medienrecht

Weder das US-amerikanische[739] noch das ursprüngliche Medienrecht auf nationaler oder EU-Ebene greifen Interoperabilität als solche explizit auf. Daher gibt es auch keine darauf unmittelbar folgenden Interoperabilitätspflichten. Dennoch kennt das Medienrecht relevante Anknüpfungspunkte, auf die im vorliegenden Zusammenhang der Vollständigkeit halber eingegangen wird. Neben Zugangs- oder sog. „Must Carry"-Pflichten können Regelungen zur (fairen, diskriminierungsfreien, transparenten) Ausgestaltung eines bestehenden Zugangs als mit Interoperabilität im weiteren Sinne verbunden gesehen werden.

Must-Carry-Regeln haben bei der Verbreitung von Rundfunk sowohl auf nationaler Ebene in Deutschland als auch auf EU-Ebene schon bei der analogen Signalverbreitung eine Verankerung gefunden.[740] Auf EU-Ebene war die Normierung in Art. 31 der sog. Universaldienstrichtlinie aus 2002[741] ein wichtiger Schritt. Diese Regelung, heute Art. 114 EKEK, erlaubt es den Mitgliedstaaten, zur Übertragung bestimmter Hör- und Fernsehkanäle und -dienste den unter ihre Gerichtsbarkeit fallenden Unternehmen, die für die öffentliche Verbreitung von solchen Diensten genutzte elektronische

739 Neben Regelungen der einzelnen Bundesstaaten ist das US-amerikanische „Medienrecht" im Communications Act 1934 (47 U.S.C. § 151 et seq.) enthalten, der von der FCC überwacht wird. Enthalten sind Regeln für die Telefon-, Telegrafen-, Fernseh- und Radiokommunikation inklusive solchen für die Zuweisung von Frequenzen, Tarifen und Gebühren, Bedingungen für den Abonnentenzugang sowie Regeln für Werbung, Rundfunk im öffentlichen Interesse und zur staatlichen Nutzung von Kommunikationssystemen.

740 Eingehend *Assion*, Must Carry: Übertragungspflichten auf digitalen Rundfunkplattformen, S. 3 ff.

741 Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (Universaldienstrichtlinie, UDRL), EU ABl. L 108, 24.4.2002, S. 51–77.

Kommunikationsnetze betreiben, zumutbare Übertragungspflichten aufzuerlegen, wenn eine erhebliche Zahl von Endnutzern diese Netze als Hauptmittel zum Empfang von Hörfunk- und Fernsehsendungen nutzt. Solche Verpflichtungen dürfen jedoch nur auferlegt werden, soweit sie zur Erreichung klar umrissener Ziele von allgemeinem Interesse erforderlich, verhältnismäßig und transparent sind.[742] Die Auferlegung eines angemessenen Entgelts ist möglich.[743] Erwägungsgrund 115 EKEK erläutert das hinter der Norm stehende Ziel. Bei der ursprünglichen Einführung der Vorschrift auf EU-Ebene gab es in den Mitgliedstaaten bereits entsprechende Pflichten, und es sollte (zugunsten der Netzbetreiber, die vor einer übermäßigen Inanspruchnahme geschützt werden sollten) sichergestellt werden, dass diese nur in angemessener Weise, aufgrund legitimer öffentlicher Interessen und im Einklang mit dem Unionsrecht bestehen bleiben.

In Deutschland finden sich entsprechende Pflichten in Bezug auf Medienplattformen[744] (§§ 81 ff. MStV). Konkretisierende Vorgaben finden sich in der Satzung zur Konkretisierung der Bestimmungen des Medienstaatsvertrags über Medienplattformen und Benutzeroberflächen der Landesmedienanstalten (MB-Satzung).[745] § 81 MStV betrifft die Belegung von (infrastrukturgebundenen) Medienplattformen und enthält Must-Carry-Pflichten, die sich vornehmlich auf die Programme des öffentlich-rechtlichen Rundfunks und der reichweitenstärksten privaten Sender sowie auf regionale und lokale Programme beziehen.[746] Auch im nicht durch die Vorgaben belegten Bereich soll der Betreiber einer Medienplattform in Bezug auf verbleibende Kapazitäten sicherstellen, dass ein vielfältiges Angebot gewährleistet wird. Eine ähnliche Regelung gilt für den Hörfunk. Die Tatsache, dass solche Regeln Eingang in das Medienrecht und nicht in

742 Dazu hinsichtlich der Belegungsregeln im analogen Kabelnetz EuGH, Urteil 22.12.2008, Rs. C-336/07 – *Kabel Deutschland Vertrieb und Service*, ECLI:EU:C:2008:765.

743 Eingehend dazu auch *Ukrow/Cole*, Sicherung lokaler und regionaler Medienvielfalt, S. 97 ff.

744 Nach § 2 Abs. 2 Nr. 14 MStV umfasst das jedes Telemedium, soweit es Rundfunk, rundfunkähnliche Telemedien oder Telemedien nach § 19 Abs. 1 MStV zu einem vom Anbieter bestimmten Gesamtangebot zusammenfasst. Das erfasst auch die Zusammenfassung von softwarebasierten Anwendungen, die im Wesentlichen der unmittelbaren Ansteuerung solcher Angebote dienen.

745 Siehe https://www.die-medienanstalten.de/fileadmin/user_upload/Rechtsgrundlagen/Satzungen_Geschaefts_Verfahrensordnungen/Medienplattformen_Benutzeroberflaechen_Satzung.pdf.

746 Vgl. im Detail *Oster*, in: HK-MStV, § 82 MStV.

das Telekommunikationsrecht gefunden haben, zeigt ihren Schwerpunkt im medialen Kontext zur Sicherung eines vielfältigen und relevanten Medien- und Informationsangebots zugunsten der Rezipienten. Eine Regelung der „Interoperabilität" findet dabei zwar nicht statt – das Vorhandensein einer entsprechenden Möglichkeit wird bereits durch die Definition von Medienplattformen (Telemedien, die Rundfunk, rundfunkähnliche oder presseähnliche Telemedien zusammenfassen) vorausgesetzt, d. h., ein Angebot, das nicht bereits mit entsprechenden Programmen „interoperabel" ist, kann nicht von der Regelung erfasst sein. Die Regelung ist aber mit (vertikaler) Interoperabilität vergleichbar, weil die Darstellung unterschiedlicher Angebote in einer für den Nutzer einheitlichen Oberfläche bzw. einem einheitlichen Dienst angestrebt ist. Der gemeinsame Standard bzw. die gemeinsame Schnittstelle besteht im gewählten Übertragungsweg. Damit ergeben sich in diesem Zusammenhang aber auch nicht die gleichen Gefährdungspotenziale und rechtlichen sowie technischen Herausforderungen wie bei der Umsetzung von Interoperabilität.

In Ergänzung zu dieser „Belegungsregelung" enthält § 82 MStV – als Regelung zum „Zugang zu Medienplattformen" betitelt – Regelungen zur Ausgestaltung der Belegung, also auch zur Sicherstellung, dass der Zugang der erfassten Angebote zu den Medienplattformen unabhängig von den Must-Carry-Regeln nach bestimmten Vorgaben ermöglicht wird.[747] Nach Abs. 1 haben Anbieter von Medienplattformen zu gewährleisten, dass die von ihnen eingesetzte Technik ein vielfältiges Angebot auf der Plattform ermöglicht. In Abs. 2 werden die allgemeinen Grundsätze der Diskriminierungsfreiheit und Chancengleichheit statuiert. Danach dürfen zur Sicherung der Meinungs- und Angebotsvielfalt Rundfunk, rundfunkähnliche Telemedien und Telemedien nach § 19 Abs. 1 MStV beim Zugang zu Medienplattformen nicht unmittelbar oder mittelbar unbillig behindert und gegenüber gleichartigen Angeboten nicht ohne sachlich gerechtfertigten Grund unterschiedlich behandelt werden. Dies gilt insbesondere in Bezug auf Zugangsberechtigungssysteme und APIs inkl. verbundener technischer Vorgaben sowie für die Ausgestaltung von Zugangsbedingungen, insbesondere für Entgelte und Tarife. Zur Bestimmung der Gleichartigkeit ist dabei auf Art, Inhalt und Gestaltung des Angebots abzustellen, nicht aber darauf, wer der Anbieter des Inhalts ist.[748]

747 Vgl. im Detail *Oster*, in: HK-MStV, §82 MStV Rn. 45 ff.

748 Begründung zum Staatsvertrag zur Modernisierung der Medienordnung in Deutschland, S. 44.

Obwohl in der Vorschrift APIs angesprochen werden, die auch im Zusammenhang mit Interoperabilität bedeutsam sind, ist damit nicht die Anordnung einer Schnittstellenoffenheit verbunden, wobei Medienplattformen prinzipiell für die auf ihnen verbreiteten Dienste interoperabel sind. Eine der Interoperabilität vergleichbare Wirkung hat § 82 Abs. 2 MStV dennoch: § 5 Abs. 3 der MB-Satzung konkretisiert, dass eine unbillige Behinderung insbesondere dann vorliegt, wenn Medienplattformen im Rahmen des „technisch Möglichen und wirtschaftlich Zumutbaren keine realistische Chance auf Zugang eröffnen". Das ist also dann relevant, wenn ein eine Medienplattform zwar prinzipiell gerade auf die Zusammenfassung von Rundfunk und bestimmten Telemedien ausgerichtet ist, aber für bestimmte solche Angebote die Aufnahme in der Medienplattform aus unterschiedlichen Gründen verunmöglicht. Daher kann zumindest unter Verweis auf die Diskriminierungsfreiheit eine „Interoperabilität" im Sinne einer gleichberechtigten Zugangseröffnung von den Medienanstalten angeordnet werden. Abs. 1 verknüpft das auch mit dem Kontext von Vielfaltssicherung. Regeln zur technischen Ausgestaltung dieser „Vorstufe" von Interoperabilität fehlen, da §§ 81 und 82 MStV erkennbar nicht auf die Schaffung von interoperablen Systemen, sondern den Must-Carry-Bereich und die allgemeine Belegung ausgerichtet sind.

Für den Bereich der Vielfaltssicherung waren und sind im Lichte der eingangs dargestellten Gefahrenlagen im digitalen Bereich diese Regelungen von Bedeutung. Oben wurde herausgearbeitet, dass gerade in vertikalen Strukturen und Märkten häufig nicht der Zugang oder die fehlende Interoperabilität an sich das Problem ist, sondern deren (faire) Ausgestaltung. Aus dem Blickwinkel der Sicherung von medialer und Meinungsvielfalt geht es mehr noch als bei wettbewerbsrechtlicher Betrachtung vorwiegend um eine gleichberechtigte Zugänglichkeit und die anschließende Sichtbarkeit und Auffindbarkeit eines Angebots auf einer Plattform. Entsprechend sind auch weitere Regeln des MStV mittelbar in diesem Zusammenhang relevant, die zu einer solchen Distributionskette zum Endverbraucher beitragen: So werden nach § 84 MStV Vorgaben bezüglich der Auffindbarkeit von Public-Value-Inhalten in Benutzeroberflächen gemacht. Für Medienintermediäre statuiert § 94 MStV zur Sicherung der Meinungsvielfalt ein Diskriminierungsverbot mit Blick auf journalistisch-redaktionell gestaltete Angebote, soweit der Intermediär auf deren Wahrnehmbarkeit einen besonders hohen Einfluss hat.

2. Interoperabilität im e-Government

Auf der Ebene der EU gehen Bestrebungen zu einer besseren Vernetzung bei der Einführung von e-Government-Lösungen bereits auf die 1980er Jahre zurück, die seither schrittweise in unterschiedlichen Bereichen ausgebaut und formalisiert wurden.[749] Im Zusammenhang mit e-Government spielt die Interoperabilität der dabei verwendeten Dienste und technischen Lösungen eine zentrale Rolle.[750]

Zunächst wurden verschiedene Programme aufgelegt, die eine Interoperabilität in Bezug auf eine Zusammenarbeit in bestimmten Sektoren herstellen sollten, so z. B. das „Cooperation in the Automation of Data and Documentation for Imports-Exports and Agriculture (CADDIA)"-Programm, das „Communications network Community programme on trade electronic data interchange systems (TEDIS)" oder das „Interchange of Data between Administrations (IDA)"-Programm. Ein wichtiger Bestandteil ist auch die Pflicht zur Notifizierung bei der Kommission für mitgliedstaatliche Normen und technische Vorschriften, die in der zwischenzeitlich kodifizierten Richtlinie über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften von 1998[751] niedergelegt wurde. Die beiden ISA-Programme[752] begründeten im Zeitraum zwischen 2010 und 2022 wesentliche sektorübergreifende Initiativen für Interoperabilitätslösungen für europäische öffentliche Verwaltungen. Maßgeblich wurde die Entwicklung digitaler Lösungen unterstützt, die es öffentlichen Verwaltungen, aber auch

749 Zum Folgenden und zur historischen Entwicklung des Interoperabilitätsrahmens in der EU s. *Pflücke*, Interoperability in the EU, S. 1, 5 ff.

750 Im Folgenden wird nicht auf die in der EU in den letzten Jahren intensiv vorangetriebene gesonderte Interoperabilität von Datenbanken eingegangen, die im Zusammenhang mit der Prävention und Verfolgung von Straftaten verwendet werden. Vgl. zu dieser Problematik nur *Quintel*, Data Protection, Migration and Border Control – The GDPR, the Law Enforcement Directive and Beyond, v. a. S. 44 f.

751 Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften, EU ABl. L 204 vom 21.07.1998, S. 37–48. Diese wurde kodifiziert in der Richtlinie (EU) 2015/1535 (EU ABl. L 241 vom 17.9.2015, S. 1–15).

752 Beschluss Nr. 922/2009/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über Interoperabilitätslösungen für europäische öffentliche Verwaltungen (ISA), EU ABl. L 260 vom 3.10.2009, S. 20–27; Beschluss (EU) 2015/2240 des Europäischen Parlaments und des Rates vom 25. November 2015 zur Einrichtung eines Programms über Interoperabilitätslösungen und gemeinsame Rahmen für europäische öffentliche Verwaltungen, Unternehmen und Bürger (Programm ISA2) als Mittel zur Modernisierung des öffentlichen Sektors, EU ABl. L 318 vom 4.12.2015, S. 1–16.

Unternehmen und Bürgern ermöglichen sollten, von interoperablen grenz- und sektorübergreifenden öffentlichen Dienstleistungen zu profitieren.

Weitere Strategien, Empfehlungen und Programme formulierte im Jahr 2010 eine Mitteilung mit dem Titel „Interoperabilisierung europäischer öffentlicher Dienste“[753], die im Anhang die „Europäische Interoperabilitätsstrategie“ (EIS)[754] und den „Europäischen Interoperabilitätsrahmen“ (European Interoperability Framework, EIF)[755] enthielt. 2017 wurde der EIF reformiert bzw. erweitert und bleibt auch als rechtlich unverbindliches Instrument für die grenzüberschreitende Kooperation im e-Government in der EU relevant.[756]

Obwohl sich der EIF auf den Bereich des e-Government bezieht und damit nicht im Zusammenhang mit dem Mediensektor steht, lassen sich aus seinem Aufbau und den berücksichtigten Prinzipien sowie technischen Modalitäten Erkenntnisse ableiten, die für die allgemeine Diskussion zu Interoperabilitätslösungen interessant sind. So sind die Prinzipien, die öffentlichen Diensten und damit auch dem EIF als Strukturvoraussetzungen für die herzustellende Interoperabilität zugrunde liegen, zu einem Großteil aus dem Unions-Primärrecht abgeleitet und daher sektorübergreifend von Bedeutung. Sie sind als Empfehlungen an die Mitgliedstaaten formuliert, wie diese den jeweiligen nationalen Interoperabilitätsrahmen ausgestalten sollen, um ein (auch grenzüberschreitendes) Funktionieren und damit eine (auch grenzüberschreitende) Zusammenarbeit zu ermöglichen:

- Subsidiarität und Verhältnismäßigkeit: Der EIF ist als gemeinsame Orientierung gedacht, die Mitgliedstaaten sollen ihn heranziehen und dann an nationale Bedürfnisse anpassen.
- Offenheit: Mitgliedstaaten werden zur Nutzung eines Open-Data- und Open-Source-Ansatzes ermutigt.

753 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Interoperabilisierung europäischer öffentlicher Dienste“ vom 16.12.2010, COM(2010) 744 final.

754 COM(2010) 744 final (ibid.), Anhang 1.

755 COM(2010) 744 final (ibid.), Anhang 2.

756 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Europäischer Interoperabilitätsrahmen – Umsetzungsstrategie, COM(2017) 134 final. Eine erläuternde Broschüre zum neuen Interoperabilitätsrahmen ist abrufbar unter https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf.

- Transparenz: Mitgliedstaaten sollen unter Berücksichtigung des Datenschutzrechts interne administrative Prozesse transparent machen und Benutzeroberflächen in dieser Hinsicht ausgestalten.
- Wiederverwertbarkeit: Mitgliedstaaten sollen sicherstellen, dass IT-Lösungen, Informationen und Daten unter Berücksichtigung der Regeln von Privatsphäre und dem Geheimnisschutz geteilt und in Kooperationsprozesse eingebracht werden können.
- Technologieneutralität und Datenportabilität: Mitgliedstaaten sollen Bürgern, Unternehmen und Verwaltungseinheiten keine oder zumindest nicht solche technologiespezifischen Lösungen auferlegen, die nicht deren tatsächlichen Bedürfnissen entsprechen; Datenportabilität soll, soweit möglich und rechtlich zulässig, sichergestellt werden.
- Nutzerzentriertheit: Mitgliedstaaten sollen Systeme nutzerzentriert ausgestalten, damit Nutzer (andere Behörden, Verbraucher, Unternehmen) über mehrere Kanäle mit der Verwaltung interagieren können („multichannel approach"); es soll eine zentrale Kontaktstelle geben („single point of contact"), deren Feedback berücksichtigt und die nach Möglichkeit nur einmalig und nur im Rahmen des Notwendigen nach Daten und Informationen gefragt werden soll.
- Inklusion und Zugänglichkeit: Mitgliedstaaten sollen sicherstellen, dass ihre Systeme allen Bürgern, inklusive solcher mit Behinderungen, zugänglich sind.
- Sicherheit und Privatsphäre: Mitgliedstaaten sollen einen Rahmen für Sicherheits- und Privatsphärenanforderungen sicherstellen, insbesondere für den Austausch von Daten.
- Mehrsprachigkeit: Mitgliedstaaten sollen sicherstellen, dass Systeme auch sprachlich auf die Bedürfnisse ihrer erwarteten Nutzer (andere Behörden, Verbraucher, Unternehmen) abgestimmt sind.
- Administrative Vereinfachung: Mitgliedstaaten sollen Verwaltungsverfahren vereinfachen und, soweit möglich, auf digitale Lösungen setzen.
- Aufbewahrung: Mitgliedstaaten sollen eine langfristige Aufbewahrungslösung für Informationen im Zusammenhang mit europäischen öffentlichen Diensten und insbesondere für Informationen, die grenzüberschreitend ausgetauscht werden, formulieren.
- Bewertung der Wirksamkeit und Effizienz: Mitgliedstaaten sollen eine wiederkehrende Bewertung der Wirksamkeit und Effizienz verschiedener Interoperabilitätslösungen und technologischen Optionen unter Berücksichtigung des Nutzerbedarfs, der Verhältnismäßigkeit und der Ausgewogenheit zwischen Kosten und Nutzen vornehmen.

Darüber hinaus beschreibt der EIF auch ein Interoperabilitätsmodell, das auf alle digitalen öffentlichen Dienste anwendbar ist und damit ebenso allgemeingültige Grundstrukturen festlegt. Es besteht im Wesentlichen aus vier Schichten, in denen Arten von Interoperabilität näher ausdifferenziert werden, die bereits oben (vgl. A.III.3) angesprochen wurden: rechtliche Interoperabilität, organisatorische Interoperabilität, semantische Interoperabilität und technische Interoperabilität. Über diesen steht im Modell eine Interoperabilitätspolitik, die über den Rahmen, institutionelle Vereinbarungen, organisatorische Strukturen und andere Aspekte wie etwa Durchsetzung und Implementierung entscheidet. Zu diesen Entscheidungen kann auch die Definition und Auswahl von Standards gehören.

Schließlich empfiehlt der EIF Konzeptionsmodelle für integrierte öffentliche Dienste bzw. deren Regulierung. Die Struktur des Modells umfasst eine „integrierte Dienstleistungserbringung" auf der Grundlage einer „Koordinierungsfunktion", um die Komplexität für den Endnutzer zu verringern. Angestrebt soll eine „No wrong door"-Dienstleistungspolitik werden, um alternative Optionen und Kanäle für die Dienstleistungserbringung zu bieten und gleichzeitig die Verfügbarkeit digitaler Kanäle sicherzustellen (digital-by-default). Zentrales Element ist dabei wiederum die Wiederverwendung von Daten und Diensten, um die Kosten zu senken und die Qualität und Interoperabilität der Dienste zu verbessern. Ferner sollen Kataloge, die wiederverwendbare Dienste und andere Ressourcen beschreiben, zur besseren Auffindbarkeit und Nutzung beitragen. Schließlich enthält das Modell auch Empfehlungen zur Sicherheit und zum Datenschutz (bspw. privacy-by-design, Risikomanagement, Zugriffsautorisierung, Verschlüsselung, Zeitstempel etc.).

Interoperabilität bildet auch weiterhin eine wesentliche Bestrebung der Europäischen Kommission für das e-Government. Ende 2020 hat die Kommission eine Initiative zur Bewertung des EIF und der weiteren strategischen Ausrichtung gestartet. In deren Kontext wurden Studien[757] und eine öffentliche Konsultation[758] durchgeführt, die die bisherigen Rahmenbedin-

757 *Europäische Kommission*, Study supporting the final evaluation of the programme on interoperability solutions for European public administrations, businesses and citizens (ISA²); *dies.*, Study supporting the evaluation of the implementation of the EIF; *dies.*, Study supporting the impact assessment for a future interoperability strategy.

758 Interoperable digitale öffentliche Dienste – Bewertung des Europäischen Interoperabilitätsrahmens und strategische Ausrichtung, Ref. Ares(2020)5562536, 15.10.2022, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12579-Int

gungen zwar als positiv bewerteten, aber – der Freiwilligkeit und Ausgestaltungsbedürftigkeit des EIF geschuldet – die fehlende oder nur teilweise Umsetzung als Hindernis hervorhoben, das zu Interoperabilitätshemmnissen führt. Aufbauend darauf setzt die Initiative „Interoperable Europe"[759] das ISA2-Programm seit 2022 fort und soll die Bestrebungen unter Beachtung festgestellter Hindernisse im bisherigen Rahmen weiterentwickeln.[760]

Kernelement dieser Initiative ist der Vorschlag eines Gesetzes für ein interoperables Europa[761], den die Kommission im November 2022 veröffentlicht hat. Am 13. November 2023 haben sich Rat und Parlament auf einen Kompromiss geeinigt und das Gesetz wurde erst kürzlich im Amtsblatt der Union veröffentlicht.[762] Die Verordnung soll mit verbindlichen Regeln grenzüberschreitende Interoperabilität und Zusammenarbeit im öffentlichen Sektor in der gesamten EU vorantreiben.[763] Im Vordergrund steht eine strukturierte EU-weite Zusammenarbeit, bei der sich öffentliche Verwaltungen, die von öffentlichen und privaten Akteuren unterstützt werden, im Rahmen von Projekten zusammenschließen, die von den Mitgliedstaaten sowie von Regionen und Städten gemeinsam getragen werden. Verpflichtet werden die Mitgliedstaaten bzw. deren öffentliche Stellen oder sonstige Einrichtungen auch zu Interoperabilitätsbewertungen (Art. 3 der Verordnung für ein interoperables Europa) bei der Einführung neuer oder der Veränderung bestehender Netz- und Informationssysteme, sofern diese in einem grenzüberschreitenden Kontext verwendet werden. Die Weiterga-

---

eroperable-digital-public-services-European-Interoperability-Framework-evaluation-strategy_de.

759 Vgl. https://joinup.ec.europa.eu/interoperable-europe/policy.

760 Vgl. dazu die Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über eine gestärkte EU-Interoperabilitätspolitik im öffentlichen Sektor, Verknüpfung öffentlicher Dienste, Unterstützung der öffentlichen Politik und Schaffung öffentlichen Nutzens – Auf dem Weg zu einem „interoperablen Europa", COM(2022) 710 final, https://eur-lex.europa.eu/legal-content/de/TXT/?uri=COM%3A2022%3A710%3AFIN.

761 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes Maß an Interoperabilität des öffentlichen Sektors in der Union (Gesetz für ein interoperables Europa), COM(2022) 720 final, https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A52022PC0720.

762 Verordnung (EU) 2024/903 des Europäischen Parlaments und des Rates vom 13. März 2024 über Maßnahmen für ein hohes Maß an Interoperabilität des öffentlichen Sektors in der Union (Verordnung für ein interoperables Europa), EU ABl. L, 2024/903, 22.3.2024, http://data.europa.eu/eli/reg/2024/903/oj.

763 Für einen detaillierteren Überblick vgl. *Pflücke*, Interoperability in the EU, S. 1, 8 ff.

be von quelloffenen Lösungen soll in Zukunft über ein „Portal für ein interoperables Europa" laufen, das eine zentrale Anlaufstelle für Lösungen und die gemeinschaftliche Zusammenarbeit werden soll. Schließlich sind auch verschiedene Innovations- und Unterstützungsmaßnahmen vorgesehen; dazu zählen Reallabore für politische Experimente, GovTech-Projekte zur Entwicklung und Ausweitung von Lösungen für die Weiterverwendung sowie die Unterstützung von Schulungen etc. Eingerichtet wird zudem ein Beirat für ein interoperables Europa mit je einem Vertreter jedes Mitgliedstaats sowie insgesamt drei jeweils von der Kommission, dem Ausschuss der Regionen und dem Europäischen Wirtschafts- und Sozialausschuss benannten Vertretern. Ihm werden verschiedene Aufgaben im Zusammenhang mit der Verordnung zugewiesen, u. a. auch jene, einen neuen EIF zu entwickeln.

In den Mitgliedstaaten hat dieser von der EU initiierte Rahmen in unterschiedlichem Maß Umsetzung gefunden.[764] Auch in den USA gibt es vergleichbare Bestrebungen, die durch den im Jahr 2002 in Kraft getretenen E-Government Act veranlasst wurden.[765] Ziel des Vorhabens war es, e-Government in den USA zu verstärken, wobei festgelegt wurde, dass US-Bundesbehörden e-Government-Anwendungen interoperabel ausgestalten müssen.

3. Interoperabilität im Cloud-Computing

Wenngleich die Interoperabilitätsfragen im Zusammenhang mit Cloud-Computing, also der dezentralen Speicherung von Daten auf Servern oder der Nutzung von nicht lokal installierten Systemen wie Softwarelösungen, eng mit dem Datenschutzrecht verbunden sind, wird hier kurz gesondert darauf eingegangen, weil sich spezifische Rechtsakte und Policy-Dokumente für solche Lösungen sowohl in den USA als auch in der EU finden.

Während in den USA im Sommer 2023 der Multi-Cloud Innovation and Advancement Act of 2023 in den US-Kongress eingebracht wurde, dessen Ziel es ist, eine sichere Nutzung verschiedener Cloud-Anbieter durch die US-Bundesregierung zu bewerten (vgl. dazu unten C.VI.1.h), befassen sich auf EU-Ebene bereits mehrere Rechtsakte mit der Interoperabilität im

764 Zur Umsetzung in Deutschland vgl. etwa *Deutscher Bundestag*, Zehnter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft", S. 24 ff.

765 E-Government Act of 2002, Pub. L. 107–347, 116 Stat. 2899.

Cloud-Computing.[766] Daneben finden die Portabilitätsregel der DS-GVO und die Regeln des DMA (soweit sie von Gatekeepern angeboten werden) auf solche Dienste Anwendung (bzw. können auf sie Anwendung finden), was auch für die Bestimmungen des Data Act gilt (eingehend unten C.V.6).

Es gehört zur Daten- und Digitalstrategie der Kommission, europäischen Unternehmen und Behörden Zugang zu sicheren, nachhaltigen und interoperablen Cloud-Infrastrukturen und -Diensten zu bieten.[767] Sie plant insbesondere, ein Regelwerk in Form eines EU-Cloud-Rechtsakts und eines Leitfadens für die Vergabe öffentlicher Aufträge für Datenverarbeitungsdienste zusammenzustellen. Mit dem „EU Data Protection Code of Conduct for Cloud Service Providers"[768], eines Verhaltenskodexes, der die einheitliche Durchsetzung der europäischen Datenschutzstandards im Cloud-Computing-Umfeld gemäß der DS-GVO sicherstellen soll, wurden bereits erste Schritte gegangen. Die Interoperabilität und Datenportabilität bei Cloud-Diensten kann sich als wichtige Grundbedingung auch für solche Aspekte innerhalb anderer Dienste darstellen, soweit diese Dienste (etwa auch Medien oder Intermediäre) mit Cloud-Systemen arbeiten, da Datentransfers von portablen Formaten abhängig sind.

4. Interoperabilität und Verbraucherschutz

Auch aus der Perspektive des Verbraucherschutzes spielt Interoperabilität eine immer größere Rolle, insbesondere im Hinblick auf digitale Inhalte, was auch in der Digitale-Inhalte-Richtlinie[769] der EU von 2019 zum Ausdruck kommt. Diese definiert in Art. 2 Nr. 12 Interoperabilität als die Fähigkeit digitaler Inhalte oder digitaler Dienstleistungen, mit anderer Hardware oder Software als derjenigen, mit der digitale Inhalte oder digitale Dienstleistungen derselben Art in der Regel genutzt werden, zu funktionieren. Interoperabilitätspflichten sieht die Richtlinie allerdings nicht vor. Vielmehr

766 Dazu auch *Godlovitch/Kron*, Interoperability, switchability and portability – Implications for the Cloud.

767 Vgl. hierzu *Europäische Kommission*, Cloud-Computing, https://digital-strategy.ec.europa.eu/de/policies/cloud-computing, m. w. N.

768 Vgl. https://eucoc.cloud/en/home.

769 Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, EU ABl. L 136, 22.5.2019, S. 1–27.

wird Interoperabilität (neben Funktionalität[770] und Kompatibilität[771]) als wesentliches Merkmal von digitalen Inhalten oder Dienstleistungen qualifiziert, indem Art. 7 der Digitale-Inhalte-Richtlinie bestimmt, dass diese Inhalte oder Dienstleistungen nur dann als vertragsgemäß anzuerkennen sind, wenn u. a. die Interoperabilität so gewährleistet ist, wie sie im Vertrag beschrieben ist. Das bezieht sich auch auf vorvertragliche Informationen,[772] also ggf. auch auf Versprechen, die in Bezug auf die Interoperabilität eines Produkts oder Dienstes gemacht wurden. Damit stellt sich die Frage nach der verschuldensunabhängigen Haftung nach dem Gewährleistungsrecht. Umgesetzt sind die Regeln in § 327e Abs. 2 BGB[773].

Auch die EU-Verbraucherrechte-Richtlinie[774], die ebenfalls 2019 durch die sog. Omnibus-Richtlinie[775] umfassend geändert wurde, enthält Anknüpfungspunkte an die Interoperabilität. Mit einem Verweis auf Art. 2 Nr. 12 der Digitale-Inhalte-Richtlinie wird nicht nur die gleiche Definition für Interoperabilität aufgestellt. Vielmehr werden Informationspflichten eingeführt, die sich auch auf die Interoperabilität erstrecken. Nach Art. 5 Abs. 1 der geänderten Verbraucherrechte-Richtlinie haben Unternehmen Verbraucher vor dem Abschluss von Fernabsatzverträgen oder von Verträgen, die außerhalb von Geschäftsräumen geschlossen werden, in klarer und

770 Funktionalität ist die Fähigkeit digitaler Inhalte oder digitaler Dienstleistungen, ihre Funktionen ihrem Zweck entsprechend zu erfüllen; Art. 2 Nr. 11 Digitale-Inhalte-Richtlinie.

771 Kompatibilität ist die Fähigkeit digitaler Inhalte oder digitaler Dienstleistungen, mit Hardware oder Software zu funktionieren, mit der digitale Inhalte oder digitale Dienstleistungen derselben Art in der Regel genutzt werden, ohne dass die digitalen Inhalte oder digitalen Dienstleistungen konvertiert werden müssen; Art. 2 Nr. 10 Digital-Inhalte-Richtlinie.

772 Erwgr. 42 Digitale-Inhalte-Richtlinie.

773 Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das zuletzt durch Art. 34 Abs. 3 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 411) geändert worden ist.

774 Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates, EU ABl. L 304, 22.11.2011, S. 64–88.

775 Richtlinie (EU) 2019/2161 des Europäischen Parlaments und des Rates vom 27. November 2019 zur Änderung der Richtlinie 93/13/EWG des Rates und der Richtlinien 98/6/EG, 2005/29/EG und 2011/83/EU des Europäischen Parlaments und des Rates zur besseren Durchsetzung und Modernisierung der Verbraucherschutzvorschriften der Union, EU ABl. L 328, 18.12.2019, S. 7–28.

verständlicher Weise über die Kompatibilität und Interoperabilität von Waren mit digitalen Elementen, digitalen Inhalten und digitalen Dienstleistungen zu informieren. Das gilt allerdings unter zwei Einschränkungen: Zum einen gilt die Informationspflicht nur „gegebenenfalls – soweit wesentlich –", also nur, soweit die Information über Interoperabilität eine wesentliche Information für den Verbraucher darstellt, und zum anderen, wenn diese Informationen dem Unternehmer bekannt sind oder vernünftigerweise bekannt sein müssen. Diese Vorgaben finden ihre nationale Umsetzung in Art. 246 Abs. 1 Nr. 8 und Art. 246a § 1 Nr. 18 des Einführungsgesetzes zum Bürgerlichen Gesetzbuch[776].

Für den vorliegenden Kontext sind diese Regeln insoweit relevant, als sie für digitale Inhalte[777] und digitale Dienstleistungen[778] gelten, sich also potenziell auf eine Vielzahl von Anwendungen im digitalen Raum wie bspw. Messenger-Dienste oder soziale Netzwerke erstrecken.[779] Anders als in Bezug auf Kompatibilität wird Interoperabilität jedoch nicht als objektive Qualitätsanforderung etabliert, sondern als subjektives Kriterium, das erst dann relevant wird, wenn es als Merkmal von den Vertragsparteien vereinbart wurde. Deshalb kann aus dem Verbraucherschutzrecht an dieser Stelle auch weder eine Pflicht noch ein Anreiz abgeleitet werden, Interoperabilität herzustellen. Vielmehr ist, umgekehrt, Interoperabilität mit bestimmten Schutzpflichten verbunden, wenn sie auf Betreiben des Unternehmens für digitale Inhalte eingerichtet wird. Die Verletzung solcher Pflichten, bspw. das Werben mit einer Interoperabilität, die aber nur teilweise oder für ganz bestimmte Hard- und Software gewährleistet wird, ohne dass über diese Einschränkung informiert wird, kann nicht nur zu einem Verstoß gegen diese Regeln führen, sondern möglicherweise auch mittels des Gesetzes

776 Einführungsgesetz zum Bürgerlichen Gesetzbuche in der Fassung der Bekanntmachung vom 21. September 1994 (BGBl. I S. 2494; 1997 I S. 1061), das zuletzt durch Art. 3 des Gesetzes vom 11. Dezember 2023 (BGBl. 2023 I Nr. 354) geändert worden ist.

777 Digitale Inhalte sind Daten, die in digitaler Form erstellt und bereitgestellt werden; Art. 2 Nr. 1 Digitale-Inhalte-Richtlinie.

778 Digitale Dienstleistungen sind Dienstleistungen, die dem Verbraucher die Erstellung, Verarbeitung oder Speicherung von Daten in digitaler Form oder den Zugang zu solchen Daten ermöglichen, oder Dienstleistungen, die die gemeinsame Nutzung der vom Verbraucher oder von anderen Nutzern der entsprechenden Dienstleistung in digitaler Form hochgeladenen oder erstellten Daten oder sonstige Interaktionen mit diesen Daten ermöglichen; Art. 2 Nr. 2 Digitale-Inhalte-Richtlinie.

779 Dazu auch *WIK-Consult*, Interoperabilitätsvorschriften für digitale Dienste, S. 26 ff.

gegen unlauteren Wettbewerb (UWG)[780], insbesondere die Verbrauchergeneralklausel des § 3 Abs. 2 UWG, sanktioniert werden.

Im Kontext von Verbraucherschutz und digitalen Inhalten – oder eher: digitalen Diensten – ist ein weiteres Rechtsinstrument von Bedeutung, das eine noch größere Nähe zum Medienrecht aufweist. Mit dem DSA – der „Schwester-Verordnung" zum DMA aus dem Digitale-Dienste-Paket[781] – haben die EU-Gesetzgeber eine umfassende „Digitale Grundordnung" geschaffen, die in der gesamten EU unmittelbar anwendbar ist. Spätestens seit dem 17. Februar 2024 gelten die Regelungen auch für alle vom DSA erfassten Dienste, also vor allem Vermittlungsdienste.[782] Der DSA hat im Gegensatz zum DMA eher verbraucherzentrierte Schutzziele, indem es vor allem um den wirksamen Schutz der in der Charta verankerten Grundrechte geht – zu denen auch der Grundsatz eines hohen Verbraucherschutzes zählt –, was wiederum einen Beitrag zum reibungslosen Funktionieren des Binnenmarkts für Vermittlungsdienste leisten soll (Art. 1 Abs. 1 DSA).

Obwohl der DSA keine unmittelbaren Interoperabilitätspflichten zwischen Vermittlungsdiensten zugunsten von Verbrauchern festlegt, ist bemerkenswert, dass Erwägungsgrund 4 die Interoperabilität als Förderungsziel statuiert. Ihm zufolge ist die Angleichung der nationalen Regulierungsmaßnahmen hinsichtlich der Anforderungen an Anbieter von Vermittlungsdiensten auf Unionsebene erforderlich, um eine Fragmentierung des Binnenmarkts zu verhindern und zu beenden, für Rechtssicherheit zu sorgen und somit die Unsicherheit für Entwickler zu verringern und die Interoperabilität zu fördern. Gleichzeitig soll durch die technologieneutrale Gestaltung der Anforderungen die Innovation nicht gehemmt, sondern vielmehr gefördert werden. Interoperabilität selbst adressiert der DSA dagegen innerhalb seiner technischen Vorschriften und dort vor allem im Kontext der Normung und Standardisierung.

Das betrifft zum einen die zusätzliche Transparenz der Online-Werbung, zu der sehr große Online-Plattformen und sehr große Online-Suchmaschinen über die sonstigen Transparenzauflagen hinaus verpflichtet sind. Art. 39 DSA sieht vor, dass sie eine entsprechende API „Werbearchive" vorhalten müssen, die bestimmte gesetzlich näher definierte Informationen zu

780 Gesetz gegen den unlauteren Wettbewerb in der Fassung der Bekanntmachung vom 3. März 2010 (BGBl. I S. 254), das zuletzt durch Art. 13 des Gesetzes vom 8. Oktober 2023 (BGBl. 2023 I Nr. 272) geändert worden ist.

781 Vgl. Europäische Kommission, Das Digitale Services Act Paket, https://digital-strategy.ec.europa.eu/de/policies/digital-services-act-package.

782 *Cole*, in: mediendiskurs, 27, 104, 2/2023, S. 92–95.

Werbung enthalten müssen, die über ihre Angebote angezeigt wird. In diesem Kontext weist Art. 44 Abs. 1 lit. f) DSA darauf hin, dass die Kommission in Konsultation mit dem Gremium die Entwicklung und Umsetzung freiwilliger Normen durch europäische und internationale Normungsgremien fördern und unterstützen soll, was zumindest (auch) die Interoperabilität von Werbearchiven nach Art. 39 DSA betrifft. Diese Archive dienen nicht primär dem Informationszugriff der Verbraucher – der DSA enthält Kennzeichnungspflichten, die für Verbraucher deutlich unmittelbarer und informativer nutzbar sind –, sondern der Bewertung durch Forschung und Aufsichtsbehörden. Wie die Informationspflicht über „die Gesamtzahl der erreichten Nutzer und gegebenenfalls aggregierte Zahlen aufgeschlüsselt nach Mitgliedstaat für die Gruppe oder Gruppen von Nutzern, an die die Werbung gezielt gerichtet war", zeigt, soll damit bewertet werden können, ob und wie Werbung von wem auf die Informations- und Meinungsbildung Auswirkungen hat. Die Interoperabilität solcher Werbearchive – die Kommission hat im Übrigen hier auch eine Konkretisierungsbefugnis für Struktur, Organisation und Funktionsweise solcher Datenbanken – erweitert den Rahmen für eine solche Bewertung.

In einem ähnlichen regulatorischen Kontext steht auch die zweite Regelung des DSA, die Interoperabilität aufgreift. Nach Art. 85 DSA soll das Informationsaustauschsystem, das die Kommission für die Kommunikation zwischen den Koordinatoren für digitale Dienste, der Kommission und dem Gremium errichtet und pflegt, nach Möglichkeit interoperabel sein. Nach Abs. 2 erlässt die Kommission Durchführungsrechtsakte zur Festlegung der praktischen und operativen Modalitäten für die Funktionsweise des Informationsaustauschsystems und seiner Interoperabilität mit „anderen einschlägigen Systemen". Unter solche fallen sicherlich bestehende Systeme wie das IMI.[783] Denkbar, wenngleich nicht primär im Fokus dieses Austausches auf der Ebene der Regulierungsbehörden, wäre auch eine Anbindung an anbietereigene Systeme wie bspw. Meldesysteme, die Transparenzdatenbank nach Art. 24 Abs. 5 DSA oder Werbearchive.[784]

Im Übrigen kann der DSA, obwohl er gleichzeitig rechtliche Grenzen und Herausforderungen für die Interoperabilität aufstellt,[785] für deren Umsetzung förderlich sein. Da es sich um eine Verordnung handelt, die auf

783 Dazu auch *Cole/Etteldorf/Ullrich*, Updating the Rules for Online Content Dissemination, S. 136 f.

784 Dazu auch *Etteldorf*, in: Cappello (Hrsg.), Algorithmische Transparenz und Rechenschaftspflicht bei digitalen Diensten, S. 36 f.

785 Vgl. dazu oben C.I.2.g.

dem Marktortprinzip basiert und mit einem ausdifferenzierten Aufsichtssystem verbunden ist, erfolgt hier nicht nur eine Strukturierung des digitalen Binnenmarkts, sondern auch eine Harmonisierung im Sinne einer Festlegung von rechtlichen Standards, an die sich alle Akteure einer bestimmten Kategorie von Diensten halten müssen. Diese rechtliche Angleichung der Rahmenbedingungen führt dazu, dass auch innerhalb potenzieller (horizontal) interoperabler Systeme mindestens gleiche Grundbedingungen herrschen, soweit potenzielle Unternehmen nicht von den Pflichten ausgenommen sind, wie es für Kleinst- und Kleinunternehmen der Fall ist.

5. Interoperabilität und Barrierefreiheit

Am 28. Juni 2019 trat die Richtlinie (EU) 2019/882 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen[786] in Kraft. Dieser sog. „European Accessibility Act (EAA)" soll durch Barrierefreiheitsanforderungen für bestimmte Produkte und Dienstleistungen einen Beitrag zum reibungslosen Funktionieren des Binnenmarkts leisten. Dazu zählt die barrierefreie Gestaltung des Online-Handels für Verbraucher, bestimmter Hardware-Systeme (u. a. Computer und Smartphones, Telefone, Modems und Router etc.) und der elektronischen Kommunikation, Letzteres insbesondere in Bezug auf Notrufe. Im vorliegenden Kontext sind aber die Bestimmungen zu einem barrierefreien Zugang zu audiovisuellen Medien von besonderer Relevanz. Zweck der Regeln ist es, dass der Zugang zu audiovisuellen Inhalten barrierefrei gewährleistet wird und Mechanismen vorhanden sind, die es Nutzern mit Behinderungen ermöglichen, ihre assistiven Technologien zu nutzen.

Hierzu legt Abschnitt IV des Anhangs zum EAA Barrierefreiheitsanforderungen fest, die von Diensten, die den Zugang zu audiovisuellen Mediendiensten ermöglichen,[787] zu erfüllen sind. Erfasst werden davon

786 Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates vom 17. April 2019 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen, EU ABl. L 151 vom 7.6.2019, S. 70–115.

787 Das sind nach Art. 3 Nr. 6 EAA über elektronische Kommunikationsnetze übermittelte Dienste, die genutzt werden, um audiovisuelle Mediendienste zu ermitteln, auszuwählen, Informationen darüber zu erhalten und diese Dienste anzusehen, sowie alle bereitgestellten Funktionen – wie beispielsweise Untertitel für Gehörlose und Schwerhörige, Audiodeskription, gesprochene Untertitel und das Dolmetschen in Gebärdensprache –, die auf die Umsetzung von Maßnahmen zurückgehen, die

insbesondere Webseiten, Online-Anwendungen, auf Set-top-Boxen basierende Anwendungen, herunterladbare Anwendungen, auf Mobilgeräten angebotene Dienstleistungen einschließlich mobiler Anwendungen und entsprechende Media-Player sowie auf einer Internetverbindung basierende Fernsehdienste.[788] Diese haben zum einen elektronische Programmführer bereitzustellen, die wahrnehmbar, bedienbar, verständlich und robust sind, und Informationen über die Verfügbarkeit von Barrierefreiheit zu geben. Zum anderen müssen sie gewährleisten, dass die Barrierefreiheitskomponenten (Zugangsdienste) der audiovisuellen Mediendienste wie Untertitel für Gehörlose und Schwerhörige, Audiodeskription, gesprochene Untertitel und das Dolmetschen in Gebärdensprache vollständig, in für eine korrekte Anzeige angemessener Qualität sowie audio- und videosynchronisiert gesendet werden und es dem Nutzer ermöglichen, deren Anzeige und Verwendung selbst einzustellen. Diese Regeln betreffen demnach allein den Zugang zu audiovisuellen Mediendiensten. Die Barrierefreiheit audiovisueller Mediendienste selbst wird hingegen in der AVMD-Richtlinie adressiert. Nach Art. 7 Abs. 2 AVMD-Richtlinie sollen die Mitgliedstaaten Mediendiensteanbieter ermutigen, Aktionspläne für Barrierefreiheit zu erarbeiten, die auf eine stetige und schrittweise Verbesserung des Zugangs zu ihren Diensten für Menschen mit Behinderungen ausgerichtet sind.

Der EAA wurde in Deutschland im Barrierefreiheitsstärkungsgesetz[789] sowie durch den zweiten Medienänderungsstaatsvertrag im MStV umgesetzt. Neben Definitionen für barrierefreie Angebote und Dienste, die den Zugang zu audiovisuellen Mediendiensten ermöglichen (§ 2 Abs. 2 Nr. 30 und 31 MStV), sowie der Ergänzung der Allgemeinen Programmgrundsätze um die Berücksichtigung der Belange von Menschen mit Behinderungen wurden bestehende Regelungen zur Barrierefreiheit im Rundfunk (§ 7 MStV) und in rundfunkähnlichen Telemedien (§ 76 MStV) angepasst sowie ein neuer Unterabschnitt 5 im Abschnitt V des MStV eingeführt. §§ 99a bis 99e enthalten seitdem Anforderungen und Pflichten im Zusammenhang mit Barrierefreiheit für Dienste, die den Zugang zu audiovisuellen Mediendiensten ermöglichen.[790] Das bereits seit 2012 regelmäßig stattfindende Monitoring Barrierefreiheit der Medienanstalten beobachtet die Entwicklung

getroffen werden, um diese Dienste gemäß Art. 7 der Richtlinie 2010/13/EU zugänglich zu machen; das umfasst auch elektronische Programmführer (EPG).

788 Erwgr. 31 EAA.

789 Barrierefreiheitsstärkungsgesetz vom 22. Juli 2021, BGBl. I 2970.

790 Vgl. dazu ausf. *Ukrow*, in: HK-MStV, §§99a ff.

barrierefreier Angebote im privaten Fernsehen und, seit 2021, in ausgewählten Streamingdiensten.[791]

Barrierefreiheit spielt für den Zugang zu medialen Inhalten eine entscheidende Rolle, da nur dadurch ermöglicht werden kann, dass auch Menschen mit Einschränkungen an ihnen und damit am öffentlichen Diskurs in gleicher Weise teilhaben können. Sie hat daher auch große Bedeutung für die Vielfaltssicherung. Bei der Herstellung von Barrierefreiheit spielt Interoperabilität eine wichtige Rolle. Maßgeblich geht es dabei um die Interoperabilität von Dienstleistungen und Produkten, inklusive Hardware und Software, mit assistiven Technologien.[792] Der Begriff assistive (assistierende) Technologie steht für mögliche Hilfsmittel, die benötigt werden, um Informationen trotz Einschränkungen zugänglich, wahrnehmbar und verarbeitbar zu machen.[793] Darunter fallen insbesondere Screenreader (Bildschirmvorlese-Software), Braillezeilen, Bildschirmvergrößerungen, Sprachsteuerung, Spezialmäuse und -tastaturen oder Augen- und Mundsteuerung. Der EAA greift an mehreren Stellen auch die notwendige Interoperabilität innerhalb der Barrierefreiheitsanforderungen auf.[794]

Produkte, die unter Art. 2 Abs. 1 EAA fallen (u. a. Hardwaresysteme und für diese bestimmte Betriebssysteme für Universalrechner für Verbraucher; Verbraucherendgeräte mit interaktivem Leistungsumfang, die für den Zugang zu audiovisuellen Mediendiensten verwendet werden; und E-Book-Lesegeräte), haben bspw. Anleitungen für die Nutzung bereitzustellen, die auch über die Interoperabilität mit assistiven Lösungen informieren. Bei der Gestaltung von Benutzerschnittstellen ist die Interoperabilität mit Programmen und Hilfsmitteln zur Navigation zu beachten. Auch für Dienstleistungen, die unter Art. 2 Abs. 2 EAA fallen (u. a. elektronische Kommunikationsdienste und Dienste, die den Zugang zu audiovisuellen Mediendiensten ermöglichen), gilt eine Informationspflicht über die Interoperabilität mit Hilfsmitteln und -einrichtungen. Für e-Books ist sogar die Ermöglichung alternativer Wiedergabearten für den Inhalt und die Interoperabilität des Inhalts mit vielfältigen assistiven Technologien in wahr-

791 Vgl. dazu https://www.die-medienanstalten.de/themen/barrierefreiheit.

792 Dazu auch eingehend *Krueger/Stineman*, in: Journal of Virtual Worlds Research, 4, 3, 2011.

793 Lexikon Barrierefreiheit des BBfI, https://www.barrierefreiheit-dienstekonsolidierung.bund.de/Webs/PB/DE/service/lexikon/functions/bmi-lexikon.html?cms_lv3=18654654&cms_lv2=18267320.

794 Bspw. Erwgr. 41 in Bezug auf e-Books, Erwgr. 45 in Bezug auf elektronische Kommunikationsdienste.

nehmbarer, verständlicher, bedienbarer und robuster Weise vorgeschrieben. Im Sinne dieser Vorschriften wird Interoperabilität daher eher im Sinne von Kompatibilität verstanden.

6. Datenportabilität und Interoperabilität im Data Act

Während das Datenschutzrecht einerseits der Interoperabilität Grenzen setzt und andererseits in Form des Rechts auf Datenportabilität wichtige Voraussetzungen für die Interoperabilität statuiert, stehen demgegenüber auch Bestrebungen, den Verkehr von Daten und deren Nutzbarmachung für Innovationen zu erleichtern. Mit der Europäischen Datenstrategie[795] hat die Kommission festgestellt, dass eine Regulierung von Datenportabilität und Interoperabilität im Wettbewerbsrecht allein nicht ausreicht und die Umsetzung und Überwachung das Wettbewerbsrecht auch überlastet. Ergebnis dieser neuen Strategie ist daher neben der Verordnung Data Governance Act[796] und der Open Data-Richtlinie[797] vor allem der Data Act[798], auf den sich Europäisches Parlament und Rat am 28. Juni 2023 geeinigt haben. Im Unterschied zum Data Governance Act, der entsprechende Strukturen und Prozesse für den Verkehr von Daten schafft, geht es im Data Act im Wesentlichen darum, Regeln dafür festzulegen, wer aus welchen (personenbezogenen und nicht personenbezogenen) Daten unter welchen Bedingungen einen Mehrwert ziehen darf.[799]

795 COM(2020)66 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

796 Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt), EU ABl. L 152 vom 3.6.2022, S. 1–44.

797 Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors, EU ABl. L 172, 26.6.2019, S. 56–83.

798 Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung), EU ABl. L, 2023/2854, 22.12.2023.

799 Eingehend zum Vorschlag für einen Data Act *Hennemann* u. a., The Data Act Proposal.

Insbesondere vier Maßnahmen und Zielsetzungen des Data Act sind im Zusammenhang mit Interoperabilitätsfragen[800] relevant:

- solche, die es Nutzern von verbundenen Diensten (oder: vernetzten Geräten) ermöglichen, auf die von ihnen auf ihren Geräten generierten Daten und auf mit diesen Geräten verbundene Dienste zuzugreifen (Datenportabilität);
- solche zum Schutz vor missbräuchlichen Vertragsbedingungen, die einseitig (und regelmäßig zu Lasten von kleineren Unternehmen) auferlegt werden;
- solche, die Nutzern die Freiheit geben, zwischen verschiedenen Cloud-Datenverarbeitungsdienstleistern zu wechseln (Datenportabilität);
- solche zur Förderung der Entwicklung von Interoperabilitätsstandards für den Datenaustausch und die Datenverarbeitung im Einklang mit der EU-Standardisierungsstrategie.

Zentrale Begriffe des Data Act sind das vernetzte Produkt und der verbundene Dienst, die den Rechtsakt auch für den Mediensektor relevant machen. Ein „vernetztes Produkt" ist ein Gegenstand, der Daten über seine Nutzung oder seine Umgebung erhält, erzeugt oder sammelt und der in der Lage ist, Produktdaten über einen elektronischen Kommunikationsdienst, eine physische Verbindung oder einen geräteinternen Zugang zu übermitteln, und dessen Hauptfunktion nicht in der Speicherung, Verarbeitung oder Übermittlung von Daten im Auftrag Dritter, mit Ausnahme des Nutzers, besteht. Diese Daten haben potenziellen Wert sowohl für Nutzer als auch für die Verbesserung der Leistung der vernetzten Produkte und werden daher von den Regeln des Data Act zum Datenzugang erfasst. Allerdings ist es wichtig, wie Erwägungsgrund 15 klarstellt, zwischen den Märkten für die Bereitstellung solcher Produkte und damit verbundener Dienstleistungen und den Märkten für nicht damit verbundene Software und Inhalte wie Text-, Audio- oder audiovisuelle Inhalte, die häufig durch Rechte des geistigen Eigentums geschützt sind, zu unterscheiden. Folglich sollten Daten, die solche Produkte erzeugen, wenn der Nutzer Inhalte aufnimmt, überträgt, anzeigt oder abspielt, sowie die Inhalte selbst (eben auch Medieninhalte) nicht unter den Data Act fallen. Obwohl auch Smart-TVs oder Sprachassistenten daher grundsätzlich solche Produkte sein könnten,

800 Dazu auch *Schnurr*, Switching and Interoperability Between Data Processing Services in the Proposed Data Act, S. 11 ff.

zeigt spätestens die Klarstellung in Erwägungsgrund 15,[801] dass es dem Data Act nicht um die Portabilität von Inhalten oder die Interoperabilität von Medien- oder Kommunikationsdiensten geht.

Eine ähnliche Ausklammerung der im Fokus medienrechtlicher Erwägungen stehenden Aspekte enthält auch die Definition des verbundenen Dienstes. Das ist ein digitaler Dienst, der kein elektronischer Kommunikationsdienst ist, einschließlich Software, der zum Zeitpunkt des Kaufs so mit dem Produkt verbunden ist, dass sein Fehlen das Produkt daran hindern würde, eine oder mehrere seiner Funktionen auszuführen, oder der später vom Hersteller oder einem Dritten mit dem Produkt verbunden wird, um die Funktionen des Produkts zu ergänzen, zu aktualisieren oder anzupassen. Ausdrücklich fallen darunter zwar auch virtuelle Assistenten (Art. 2 Abs. 2a Data Act). Allerdings stellt auch insoweit Erwägungsgrund 22 klar, dass nur diejenigen Daten in den Anwendungsbereich fallen, die sich aus der Interaktion zwischen dem Nutzer und einem verbundenen Produkt oder einem damit verbundenen Dienst über den virtuellen Assistenten ergeben. Vom virtuellen Assistenten erzeugte Daten, die in keinem Zusammenhang mit der Nutzung eines verbundenen Produkts oder einer damit verbundenen Dienstleistung stehen, sind nicht erfasst.

Insoweit ist die Relevanz für den Datenverkehr im Binnenmarkt zwar insgesamt groß, für den Mediensektor aber im Licht der Adressaten eher gering. Dies gilt auch für die Regeln zu Interoperabilität und Datenportabilität. Interoperabilität definiert Art. 2 Nr. 40 Data Act als die Fähigkeit von zwei oder mehr Datenräumen oder Kommunikationsnetzen, Systemen, vernetzten Produkten, Anwendungen, Datenverarbeitungsdiensten oder Komponenten, Daten auszutauschen und zu nutzen, um ihre Funktionen auszuführen. Sowohl diese Definition als auch die materiellen Bestimmungen mit den Verpflichtungen zeigen, dass es mehr um interoperable Datenformate als um interoperable Dienste geht, wobei die Verordnung die Begriffe der Datenportabilität und Interoperabilität an vielen Stellen nicht klar voneinander abgrenzt oder sogar vermengt.[802] So enthält etwa Kapitel VIII, das insgesamt mit „Interoperabilität" überschrieben ist, Regeln zu wesentlichen Anforderungen an die Interoperabilität von Daten (Art. 33

801 Der Rat hatte in seiner Allgemeinen Ausrichtung in Erwgr. 15 sogar explizit „smart TV" und „smart speaker" vom Anwendungsbereich ausgeschlossen; vgl. Third Presidency compromise text, No. 15035/22, https://data.consilium.europa.eu/doc/document/ST-15035-2022-INIT/en/pdf.

802 Kritisch hierzu *Schnurr*, Switching and Interoperability Between Data Processing Services in the Proposed Data Act, S. 11 ff.

Data Act) sowie an die Interoperabilität von Datenverarbeitungsdiensten (Art. 34 und 35 Data Act).

Nutzbar auch im medienrechtlichen Kontext kann der Data Act aber sein, sollten sich aus ihm Interoperabilitätsspezifikationen und harmonisierte Interoperabilitätsnormen ergeben. Kapitel VI enthält zudem Bestimmungen zum Wechsel zwischen Datenverarbeitungsdiensten (= digitale Dienstleistungen, die einem Kunden bereitgestellt werden und einen flächendeckenden und auf Abruf verfügbaren Netzzugang zu einem gemeinsam genutzten Pool konfigurierbarer, skalierbarer und elastischer Rechenressourcen zentralisierter, verteilter oder hochgradig verteilter Art ermöglichen, die mit minimalem Verwaltungsaufwand oder minimaler Interaktion des Diensteanbieters rasch bereitgestellt und freigegeben werden können), also insbesondere auch Cloud- und Edge-Dienste. Diese sollen verschiedene, in den Art. 25 ff. Data Act näher beschriebene Maßnahmen treffen, um es Kunden zu ermöglichen, zu einem Datenverarbeitungsdienst, der die gleiche Dienstart abdeckt, oder zu Informations- und Kommunikationstechnik-Infrastrukturen in eigenen Räumlichkeiten zu wechseln oder ggf. mehrere Anbieter von Datenverarbeitungsdiensten gleichzeitig in Anspruch zu nehmen.

VI. Weitere aktuelle Ansätze

1. USA

Das US-Repräsentantenhaus hatte 2020 eine Untersuchung zum Wettbewerb in digitalen Märkten vorgelegt, der die Besonderheiten digitaler Märkte und daraus ableitbarem Regulierungsbedarf aufzeigte.[803] Interoperabilität und Datenportabilität sind dort als zwei Bausteine für die Wiederherstellung des Wettbewerbs digitaler Plattformen genannt. Nicht nur vor diesem Hintergrund können in den USA im Wettbewerbsrecht neue

803 US House of Representatives, Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, Investigation of Competition in Digital Markets, 2020, https://democrats-judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf. Daneben gibt es einen weiteren, hauptsächlich von Mitgliedern der Republikanischen Partei verfassten Bericht, der in Teilen als eine Art Sondervotum gegen den genannten Bericht gelesen werden kann (*Bueren/Crowder*, in: ZHR, 186, 2022, S. 788, 804; US House of Representatives, Rep. Ken Buck, The Third Way, 2020, https://buck.house.gov/sites/evo-subsites/buck-evo.house.gov/files/wysiwyg_uploaded/Buck%20Report.pdf).

regulatorische Vorschläge zur Regulierung von Big Tech gefunden werden, die in Teilen auf Interoperabilität eingehen.

Die unterschiedlichen Vorschläge zu einer Erweiterung des Wettbewerbsrechts adressieren fünf Kernanliegen: (1) Ex-ante-Verhaltensregeln, wozu u. a. das Verbot von *self preferencing* fällt, (2) strukturelle Trennung und Beschränkung von Geschäftsbereichen von Big Tech zur Verhinderung von Interessenkonflikten, (3) besondere Regelungen für Zusammenschlüsse in diesem Bereich, (4) grundsätzliche Veränderungen im US-Wettbewerbsrecht sowie (5) Interoperabilität und Datenportabilität.[804] Mit Blick auf Interoperabilität und Datenportabilität werden im Folgenden die Entwürfe des ACCESS Act (a), des Open App Markets Act (b), des American Innovation and Choice Online Act (c), des Digital Platform Commission Act (d), des Digital Platform Commission Act (e), des Journalism Competition and Preservation Act (f), der Personal Financial Data Rights (g) sowie des Multi-Cloud Innovation and Advancement Act (h) vorgestellt.

a. ACCESS Act

Jüngst wurde in den US-Kongress ein Gesetzesentwurf für den Augmenting Compatibility and Competition by Enabling Services Switching Act (ACCESS Act of 2023) zur Schaffung von Interoperabilität für soziale Netzwerke eingebracht.[805] Ziel des im Wettbewerbsrecht verorteten und weitreichenden Gesetzesvorschlags ist die Schaffung von Rahmenbedingungen, die den Wettbewerb zwischen großen Online-Kommunikationsplattformen wie Facebook, YouTube, WhatsApp oder TikTok erhöhen. Sollte der Entwurf des ACCESS Act in dieser Form verabschiedet werden, hätten Nutzer das Recht, große soziale Netzwerke zu verlassen, ohne gleichzeitig ihre Kontakte zu verlieren. Dies soll durch eine gesetzliche Verpflichtung zur Datenportabilität und Interoperabilität von Nutzerdaten zwischen Plattformen erreicht werden. Große Online-Kommunikationsplattformen sind dabei als Produkte oder Dienstleistungen zu definiert, bei denen direkt oder

804 US Congressional Research Service, Antitrust Reform and Big Tech Firms, R46875, 13.11.2023, zuletzt aktualisiert am 21.11.2023, https://crsreports.congress.gov/product/pdf/R/R46875, S. 57.

805 ACCESS Act of 2023, S.2521 (118th Congress). Bereits 2019 und 2021 wurden zwei erfolglose, im Folgenden nicht näher betrachtete Versuche der Verabschiedung eines ACCESS Act unternommen; siehe ACCESS Act of 2021, H.R.3849 (117th Congress) sowie ACCESS Act of 2019, S.2658 (116th Congress).

indirekt Geld mit der Erhebung, Verarbeitung, dem Verkauf oder dem Teilen von Nutzerdaten verdient wird und die mehr als 100 Millionen monatlich aktive Nutzer in den USA aufweisen.[806] Der Gesetzesentwurf besteht aus sieben Teilen: Dem Titel des Gesetzes (Section 1), Definitionen (Section 2), Regelungen zur Datenportabilität (Section 3), Regelungen zur Interoperabilität (Section 4), Regelungen für Datentreuhänder im Auftrag von Nutzern (Section 5), Umsetzungs- und Durchsetzungsfragen etwa zum Zeitpunkt der Anwendbarkeit, zur Aufsicht und zu Sanktionen (Section 6) sowie das Verhältnis zu anderen Rechtsakten (Section 7).

Die Verpflichtung zur Datenportabilität (Section 3) soll die Übertragbarkeit von Nutzerdaten gewährleisten. Plattformen sollen entsprechende transparente, von Dritten erreichbare Schnittstellen bereithalten, über die ein Plattformnutzer Daten von Nutzer zu Nutzer oder von Plattform zu Plattform übermitteln können soll. Die Daten sollen in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden:[807]

> *SEC. 3. PORTABILITY.*
> *(a) General Duty Of Large Communications Platform Providers.—A large communications platform provider shall, for each large communications platform it operates, maintain a set of transparent, third party-accessible interfaces (including application programming interfaces) to initiate the secure transfer of user data to a user, or to a competing communications provider acting at the direction of a user, in a structured, commonly used, and machine-readable format.*

Wettbewerber sollen auf diesem Weg empfangene Daten auf sichere Weise verarbeiten.[808] Ausnahmen von der Verpflichtung zur Datenportabilität sind nur vorgesehen, wenn ein Plattformbetreiber mit einem Produkt oder Dienst keinen Umsatz durch die Verarbeitung der Nutzerdaten erzielt.[809]

Zusätzlich zu diesem geplanten bereichspezifischen Recht auf Datenportabilität sollen Plattformanbieter Interoperabilität schaffen (Section 4). Interoperabilität wird im vorliegenden Entwurf nicht legaldefiniert. Plattformen sollen aber transparente, von Dritten erreichbare Schnittstellen

806 ACCESS Act of 2023, § 2(7).
807 ACCESS Act of 2023, § 3(a).
808 ACCESS Act of 2023, § 3(b).
809 ACCESS Act of 2023, § 3(b).

bereithalten, um „technisch kompatible, interoperable Kommunikation mit einem Nutzer" der Plattform eines Wettbewerbers zu ermöglichen:[810]

> *SEC. 4. INTEROPERABILITY.*
> *(a) General Duty Of Large Communications Platform Providers.—A large communications platform provider shall, for each large communications platform it operates, maintain a set of transparent, third-party-accessible interfaces (including application programming interfaces) to facilitate and maintain technically compatible, interoperable communications with a user of a competing communications provider.*

Wie im Falle der Datenportabilität sollen Plattformen von Wettbewerbern, die Daten über Interoperabilitätsschnittstellen abrufen, die erhaltenen Daten sicher weiterverarbeiten.[811] Plattformanbieter sollen die Ausgestaltung der Interoperabilitätsschnittstelle selbst bestimmen können. Im derzeitigen Entwurf ist nicht geplant, technische Anforderungen und Standards an Interoperabilitätsschnittstellen gesetzlich oder behördlich vorzugeben.[812] Gleichwohl soll das National Institute of Standards and Technology (NIST) modellhafte technische Standards – insbesondere für beliebte Plattformarten wie soziale Netzwerke – entwickeln und veröffentlichen, nach denen Plattformanbieter ihre Interoperabilitätsschnittstellen gestalten könnten.[813] Die Schnittstellen sollen von Plattformen auf der Grundlage „fairer, angemessener und nicht-diskriminierender Bedingungen" bereitgestellt werden.[814] Dazu gehört, dass die Bereitstellung und Nutzung von Interoperabilitätsschnittstellen grundsätzlich kostenfrei zu erfolgen habe. Plattformbetreibern soll zugestanden werden, vernünftige Schwellenwerte im Hinblick auf die Häufigkeit, die Art und den Umfang der Nutzung von Schnittstellen durch Wettbewerber festzulegen. Würden diese Schwellen überschritten, könnten auch angemessene Gebühren (*reasonable fee*) von Wettbewerbern erhoben werden.[815] Plattformanbieter sollen darüber hinaus eigene faire, angemessene und nicht-diskriminierende Erwartungen an die Nutzung von Interoperabilitätsschnittstellen festlegen können (*usage expectations*). Würden Wettbewerber diese Bedingungen verletzen, könnten Plattformanbieter

810 ACCESS Act of 2023, § 4(a).
811 ACCESS Act of 2023, § 4(b).
812 ACCESS Act of 2023, §§ 4(c)(2)(A), 6(g).
813 ACCESS Act of 2023, § 6(c).
814 ACCESS Act of 2023, § 4(c)(2)(A).
815 ACCESS Act of 2023, § 4(c)(2)(B)(i).

entsprechende Nutzungsgebühren verlangen oder Strafen[816] gegen Wettbewerber verhängen.[817] Die Nutzungsgebühren hätten jedoch im Verhältnis zu Kosten, Komplexität und Risiko des Plattformbetreibers zu stehen, der die Schnittstelle betreibt.[818]

Damit Wettbewerber Kenntnis von diesen Bedingungen erlangen könnten, wären entsprechende Nutzungsbedingungen, Gebühren und mögliche Strafen im Vorfeld zu veröffentlichen.[819] Kurzfristigen Änderungen durch Plattformbetreiber soll durch eine Verpflichtung zur Vorankündigung aller Änderungen innerhalb einer angemessenen Frist vorgebeugt werden.[820] Um Sicherheit und Datenschutz für Nutzerdaten bei der Bereitstellung der Interoperabilitätsschnittstelle zu gewährleisten, sollen Plattformanbieter entsprechende Schutzstandards für den Zugang zu ihrer Schnittstelle vorsehen. Auch hier müssen die Datenschutz- und Sicherheitsanforderungen im Verhältnis zur Bedrohung der Nutzerdaten stehen, sollen also nicht als Zugangshürde missbraucht werden können. Mutmaßliche Verstöße von Wettbewerbern gegen Datenschutz- und Sicherheitsstandards wären an die zuständige Aufsichtsbehörde FCC (siehe oben C.II.1.b) zu melden.[821] Änderungen an Interoperabilitätsschnittstellen oder der Nutzungsbedingungen, die bezwecken oder zur Folge haben, dass die Interoperabilität für Wettbewerber in unzumutbarer Weise beeinträchtigt oder gar unterlaufen wird, sollen als Verstoß gegen die Verpflichtung zur Schaffung und Aufrechterhaltung von Interoperabilität auf der Grundlage fairer, angemessener und nicht-diskriminierender Bedingungen verstanden werden.[822]

Betreibt ein Plattformanbieter darüber hinaus mehrere eigene Produkte oder Dienstleistungen, die untereinander interoperabel sind (bspw. Metas Facebook und Instagram[823] oder Googles YouTube und Bard[824]), so soll

816 Vorstellbar wären etwa temporäre Nutzungseinschränkungen, z. B. eine temporäre starke Begrenzung der Anzahl möglicher Anfragen an die Schnittstelle.
817 ACCESS Act of 2023, § 4(c)(2)(B)(ii).
818 ACCESS Act of 2023, § 4(c)(2)(B)(iii).
819 ACCESS Act of 2023, §§ 4(c)(2)(B)(iv), 4(3).
820 ACCESS Act of 2023, § 4(c)(2)(B)(iv).
821 ACCESS Act of 2023, § 4(c)(2)(B)(v).
822 ACCESS Act of 2023, § 4(c)(2)(C).
823 *Instagram*, Dein Instagram- und Facebook-Konto zur selben Kontenübersicht hinzufügen, https://help.instagram.com/176235449218188/.
824 *Google*, Bard can now connect to your Google apps and services, https://blog.google/products/bard/google-bard-new-features-update-sept-2023/.

anderen Online-Kommunikationsplattformen eine funktionell äquivalente Version dieser internen Schnittstelle angeboten werden müssen:[825]

> *SEC. 4. INTEROPERABILITY.*
> *(c) Interoperability Obligations For Large Communications Platform Providers.—(3) Functional Equivalence.—A large communications platform provider that maintains interoperability between its own large communications platform and other products, services, or affiliated offerings of such provider shall offer a functionally equivalent version of that interface to competing communications services.*

Damit Wettbewerber auf Interoperabilitätsschnittstellen zugreifen können, sollen Plattformbetreiber verpflichtet werden, eine präzise und vollständige technische Dokumentation der Schnittstelle bereitzustellen.[826] Änderungen an der Schnittstelle, die Auswirkungen auf die Interoperabilität haben, wären rechtzeitig öffentlich bekannt zu machen.[827] Um eine Kommerzialisierung von Daten zu vermeiden, sollen die über eine Interoperabilitätsschnittstelle erlangten Daten lediglich dazu verwendet werden können, die Interoperabilität zwischen Diensten sowie die Einhaltung der Vorgaben des Datenschutzes und der Datensicherheit zu gewährleisten.[828] Wie bei der Datenportabilität wären Ausnahmen von der Verpflichtung zur Interoperabilität nur vorgesehen, wenn Plattformbetreiber mit einem Produkt oder Dienst keinen Umsatz durch die Verarbeitung der Nutzerdaten erzielen.[829]

Interoperabilität soll aber nicht nur zwischen großen Online-Kommunikationsplattformen hergestellt werden müssen. Auch Treuhänder (sog. *custodial third-party agents*[830]) im Auftrag eines Nutzers sollen Zugang zu Interoperabilitätsschnittstellen erhalten:[831]

> *SEC. 5. DELEGATABILITY.*
> *(a) General Duty Of Large Communications Platform Providers.—A large communications platform provider shall maintain a set of transparent third-party-accessible interfaces by which a user may delegate a custodial third-party agent to manage the user's online interactions, content, and*

825 ACCESS Act of 2023, § 4(c)(3).
826 ACCESS Act of 2023, § 4(c)(4).
827 ACCESS Act of 2023, § 4(c)(5).
828 ACCESS Act of 2023, §§ 4(c)(6), 4(d).
829 ACCESS Act of 2023, § 4(e).
830 ACCESS Act of 2023, § 2(5).
831 ACCESS Act of 2023, § 5(a).

account settings on a large communications platform on the same terms as a user.

Ein Treuhänder könnte von einem Nutzer beauftragt werden, Nutzerinteraktionen, Inhalte und Kontoeinstellungen vorzunehmen. Treuhänder könnten damit Konten eines Nutzers auf mehreren Plattformen verwalten und entsprechend Nachrichten und Inhalte für Nutzer aggregieren.[832] Das Konzept des *custodial third-party agent* erinnert deshalb an Personal Information Management Platforms (PIMS), mit denen Nutzer ihre Daten zentral verwalten können.[833] Treuhändern wäre unter dem ACCESS Act allerdings lediglich derselbe Zugang zu Interoperabilitätsschnittstellen zu gewähren wie dem Nutzer selbst, er soll im Umfang also nicht über die dem Nutzer eingeräumten Rechte hinausgehen.[834] Um Zugang zu den Schnittstellen der Plattformanbieter zu erlangen, müssten sich Treuhänder zunächst bei der FTC (dazu oben C.II.1.b(1)) registrieren.[835] Würde die FTC jedoch feststellen, dass ein Treuhänder gegen gesetzliche Bestimmungen aus Section 5 ACCESS Act verstoßen hat, soll die Behörde die Zulassung wieder entziehen können.[836]

Die Verpflichtungen eines Treuhänders bestünden (1) in der Gewährleistung von Datenschutz und Datensicherheit für Nutzerdaten sowie (2) in dem Verbot der Verarbeitung von Nutzerdaten zum Nachteil der Nutzer und dem Verbot der Verarbeitung von Nutzerdaten, wenn dies zu einem vernünftigerweise vorhersehbaren Schaden für den Nutzer führen würde und die entsprechende Verarbeitung nicht den Wünschen oder Erwartungen des Nutzers entspräche. Außerdem (3) dürfte der Treuhänder Nutzerdaten nicht zum eigenen wirtschaftlichen Vorteil verarbeiten.[837] Für ihre Dienste dürften Treuhänder Nutzungsgebühren verlangen.[838] Plattformanbieter dürften Treuhändern Zugang zur Schnittstelle verwehren, wenn diese entweder nicht von der FTC zugelassen wären oder wiederholt betrügerische oder bösartige Aktivitäten mit Nutzerdaten ermöglicht hätten.[839]

832 *Hartmann*, in: Bayer/Holznagel/Korpisaari/Woods, Perspectives on Platform Regulation, S. 112.
833 *European Data Protection Supervisor*, TechDispatch #3/2020 – Personal Information Management Systems, https://data.europa.eu/doi/10.2804/096824.
834 ACCESS Act of 2023, § 5(h).
835 ACCESS Act of 2023, §§ 5(b), 5(c).
836 ACCESS Act of 2023, § 5(d).
837 ACCESS Act of 2023, § 5(f).
838 ACCESS Act of 2023, § 5(g).
839 ACCESS Act of 2023, § 5(e).

Im Hinblick auf die Umsetzung des ACCESS Act (Section 6) soll nach dem Vorschlag die FTC Verfahren für die Zulassung von Treuhändern veröffentlichen. Ferner soll die FTC Regeln und Verfahren erlassen, auf deren Grundlage es Plattformanbietern erleichtert wird, die Echtheit von Anfragen eines Treuhänders im Namen eines Nutzers zu bestimmen.[840] Dasselbe gilt für Verfahren zur Authentisierung und Validierung von Anfragen von Nutzern, um Missbrauch zu verhindern. Die Verfahren zur Bestimmung der Echtheit von Anfragen von Nutzern müssten von der FTC zusammen mit Branchenvertretern erarbeitet werden.[841] Außerdem ist geplant, dass die FTC Beschwerdewege für Nutzer, Plattformbetreiber, Wettbewerber und Treuhänder schafft, damit diese Verletzungen des ACCESS Act melden könnten.[842]

Auch wenn gesetzlich oder behördlich keine technischen Vorgaben für Interoperabilitätsschnittstellen gemacht werden, soll das National Institute of Standards and Technology (NIST) modellhafte technische Standards für Interoperabilitätsschnittstellen beliebter Online-Kommunikationsplattformen wie soziale Netzwerke, Messenger und Medienaustauschplattformen (*multimedia sharing services*) entwickeln und veröffentlichen.[843] Ein Anreiz für Plattformbetreiber zur Implementierung der NIST-Standards für Interoperabilitätsschnittstellen wird dadurch geschaffen, dass bei deren Beachtung die widerlegbare Vermutung gelten soll, dass der Zugang zur Schnittstelle zu fairen, angemessenen und nicht-diskriminierenden Bedingungen gewährt worden ist.[844]

Die FTC wäre für die regelmäßige Überprüfung der Einhaltung des Gesetzes durch große Online-Kommunikationsplattformen zuständig.[845] Jeder Verstoß gegen den ACCESS Act soll von der FTC im Rahmen ihrer Kompetenzen (dazu oben C.II.1.b) geahndet werden können.[846] Entsprechend gelten dieselben wettbewerbsrechtlichen Voraussetzungen an eine Verletzung, aber auch dieselben Geldbußen von bis zu USD 10,000 pro Verletzungshandlung.[847] Bei der Ermittlung der Höhe von Geldbußen wäre die

840 ACCESS Act of 2023, § 6(a).
841 ACCESS Act of 2023, § 6(b).
842 ACCESS Act of 2023, § 6(d).
843 ACCESS Act of 2023, § 6(c).
844 ACCESS Act of 2023, § 6(g).
845 ACCESS Act of 2023, § 6(e).
846 ACCESS Act of 2023, § 6(f).
847 ACCESS Act of 2023, § 6(f)(2); 15 U.S. Code § 45.

Beeinträchtigung eines betroffenen Nutzers jeweils als eigene Verletzungshandlung zu sehen.[848]

US-Bundesstaaten würden auch bei Inkrafttreten des ACCESS Act eigene wettbewerbsrechtliche Regelungen zur Interoperabilität von sozialen Netzwerken erlassen können. Der ACCESS Act soll als Bundesrecht nur dann Vorrang vor einzelstaatlichem Recht haben, wenn dieses mit den Bestimmungen des ACCESS Act nicht vereinbar wäre.[849] Im abschließenden siebten Teil des Reformvorschlags wird das Verhältnis zu bestehender Gesetzgebung im Bereich Datenschutz und Sicherheit geregelt. Diese soll durch den ACCESS Act unberührt bleiben.[850]

b. Open App Markets Act

Während der Entwurf des ACCESS Act auf die Interoperabilität großer sozialer Netzwerke zielt, bezweckt der 2021 eingebrachte Entwurf für einen Open App Markets Act (OAMA) den Schutz des Wettbewerbs in App-Marktplätzen.[851] Betroffen wären vor allem der Apple App Store und der Google Play Store. Auch wenn der Gesetzesentwurf nach den letzten Kongressneuwahlen bisher noch nicht wieder in die aktuelle Legislaturperiode 2023–2025 des US-Kongresses eingebracht wurde, enthält er mit der Verpflichtung zur Herstellung von Interoperabilität einen nennenswerten Entwurf für einen Mechanismus, um den Wettbewerb in App-Stores zu gewährleisten. Der Gesetzesvorschlag ist in acht Teile gegliedert: Titel und Definitionen (Section 1 und 2), Regelungen zum Schutz eines wettbewerbsorientierten App-Marktes (Section 3), Datenschutz und Sicherheit (Section 4), Durchsetzung (Section 5), Berichtspflichten durchsetzender Behörden (Section 6), Auslegungshinweise (Section 7), Anwendbarkeit des Gesetzes bei möglicher Verfassungswidrigkeit von Teilen des Gesetzes (Section 8) sowie Inkrafttreten (Section 9).

Das Gesetz soll Anwendung finden auf Betreiber von App-Marktplätzen mit mehr als 50 Millionen US-Nutzern.[852] Zunächst sollen App-Anbieter im

848 ACCESS Act of 2023, § 6(f)(2)(D).
849 ACCESS Act of 2023, § 6(h).
850 ACCESS Act of 2023, § 7
851 Open App Markets Act (OAMA), S.2710 (117th Congress), eingebracht am 11.8.2021, in der Fassung vom 17.2.2022.
852 OAMA, § 2(3).

jeweiligen App-Marktplatz nicht mehr zur Nutzung des marktplatzeigenen In-App-Zahlungssystems verpflichtet werden und, anders als heute, ihre Apps in anderen App-Stores günstiger anbieten dürfen.[853] Darüber hinaus sollen App-Marktplatzanbieter in ihren Bedingungen für App-Anbieter keine Klauseln vorsehen dürfen, die verbieten, dass App-Anbieter ihre Nutzer insbesondere zu Angeboten und Preisen kontaktieren dürfen. Auch sollen Marktplatzanbieter keine nicht-öffentlichen Informationen, bspw. zur Nutzung von Apps, verwenden dürfen, um eigene Produkte zu gestalten, die mit Apps von Drittanbietern im Wettbewerb stünden.[854]

Hinsichtlich der Interoperabilität sollen App-Marktplatzanbieter – die wie Apple und Google auch ein Betriebssystem kontrollieren – es Nutzern ermöglichen, Apps und App-Marktplätze von Drittanbietern zu wählen und als Standardeinstellung zu speichern, Apps von Drittanbietern auf anderem Wege als über App-Stores zu installieren sowie vorinstallierte Apps und App-Stores zu deinstallieren:[855]

> *SEC. 3. PROTECTING A COMPETITIVE APP MARKET.*
> *(d) Interoperability.—A covered company that controls the operating system or operating system configuration on which its app store operates shall allow and provide readily accessible means for users of that operating system to—*
>
> (1) *choose third-party apps or app stores as defaults for categories appropriate to the app or app store;*
> (2) *install third-party apps or app stores through means other than its app store; and*
> (3) *hide or delete apps or app stores provided or preinstalled by the app store owner or any of its business partners.*

Die im Entwurf aufgenommene Regelung zur Interoperabilität zielt darauf ab, die Bevorzugung eigener Apps von Marktplatz-Anbietern (*self-preferencing*) zu verbieten (auch in der Suchfunktion des Marktplatzes[856]) und letztlich die Nutzung von Drittanbieter-Apps und -Marktplätzen zu erlauben bzw. zu fördern. Hierfür ist, anders als bei sozialen Netzwerken, keine Interoperabilität von Schnittstellen für Nutzerdaten erforderlich. Vielmehr sollen App-Marktplatzanbieter, die gleichzeitig mobile Plattformen bereit-

853 OAMA, § 3(a).
854 OAMA, §§ 3(b), 3(c).
855 OAMA, § 3(d).
856 OAMA, § 3(e).

stellen, neben der erzwungenen Öffnung Drittentwicklern Zugang zu Informationen über Betriebssysteme, Hardware und Softwarefeatures gewähren, sodass diese befähigt werden, mit den von den Plattformanbietern bereitgestellten Apps funktional vergleichbare Apps zu entwickeln:[857]

SEC. 3. PROTECTING A COMPETITIVE APP MARKET.

(f) Open App Development.—A covered company shall provide access to operating system interfaces, development information, and hardware and software features to developers on a timely basis and on terms that are equivalent or functionally equivalent to the terms for access by similar apps or functions provided by the covered company or to its business partners.

App-Marktplatzanbieter sollen jedoch angemessene Maßnahmen ergreifen dürfen, um für Datenschutz und Sicherheit zu sorgen oder die Einhaltung weiterer gesetzlicher Verpflichtungen zu gewährleisten. Dazu gehört auch die Information für Nutzer, dass Apps von Drittanbietern Risiken bergen können, ebenso wie die Entfernung betrügerischer Apps von Endgeräten.[858]

Der OAMA soll durch die FTC, den Generalstaatsanwalt für Wettbewerbsrecht beim US DOJ und Staatsanwälte der Bundesstaaten durchgesetzt werden. Sie werden dabei mit denselben Befugnissen ausgestattet wie im Federal Trade Commission Act, dem Sherman Antitrust Act und dem Clayton Act (dazu oben C.II.1).[859] Daneben sollen im Wege der Zivilgerichtsbarkeit durch betroffene App-Entwickler Ansprüche aus dem OAMA durchgesetzt werden können.[860] Die FTC, das DOJ und der US-Rechnungshof sollen spätestens drei Jahre nach Inkrafttreten des OAMA jeweils ein Bericht zu den Auswirkungen des OAMA auf den Wettbewerb, Markteintrittsbarrieren und die Konzentration von Marktmacht bzw. Marktanteile verfassen.[861]

Es bleibt abzuwarten, ob der Open App Markets Act nochmals als Gesetzesvorschlag in den US-Kongress eingebracht wird oder ob die im Entwurf geregelten Fragen letztlich gerichtlich entschieden werden. So strengte der Spielehersteller Epic Games – der Hersteller des beliebten Online-Spiels Fortnite – auf der Grundlage des Sherman Antitrust Act (dazu oben C.II.1.a) zwei Verfahren gegen Apple und Google in Bezug

857 OAMA, § 3(f).
858 OAMA, § 4.
859 OAMA, § 5(a)(1).
860 OAMA, § 5(b).
861 OAMA, § 6.

auf ihre mobilen App-Marktplätze an. Beide Unternehmen verpflichten App-Anbieter, den jeweils eigenen In-App-Zahlungsanbieter zu verwenden, bei der beide Unternehmen derzeit bis zu 30 % Umsatzbeteiligung pro In-App-Transaktion verlangen. Dabei forderte Epic Games insbesondere im Verfahren gegen Apple die Öffnung von Apples mobilem Betriebssystem iOS für App-Marktplätze von Drittanbietern.[862] Epic konnte vor dem Berufungsgericht einen Teilerfolg erzielen, wonach App-Entwickler künftig Zahlungsmöglichkeiten außerhalb des Apple-App-Marktplatzes bewerben dürfen, was bisher aufgrund der Verpflichtung zur Nutzung des Apple-Zahlungsdienstes untersagt war.[863] Jedoch setzte Apple diese Verpflichtung bisher noch nicht in die Praxis um. Vielmehr fochten sowohl Apple als auch Epic das Urteil vor dem Obersten Gerichtshof der Vereinigten Staaten an, der das Verfahren im Januar 2023 jedoch nicht zur Entscheidung annahm.[864] Es bleibt abzuwarten, welche Änderungen Apple tatsächlich vornehmen wird.

Im Verfahren gegen Google, das ebenfalls gegen die verpflichtende Nutzung des Google-Zahlungsanbieters für In-App-Käufe und die entsprechende Umsatzbeteiligung gerichtet war, wurde im Dezember 2023 in einem Geschworenenverfahren entschieden, dass Google mit dem Google Play Store ein wettbewerbswidriges Monopol für den Absatz von Android-Apps und für entsprechende In-App-Transaktionen erlangt habe.[865] Die Folgen aus der Entscheidung sind für Google noch unklar. Im nächsten Schritt muss das Gericht nun die von Google zu erfüllenden Auflagen festlegen. Hierzu sollten im Januar 2024 Anhörungen stattfinden. Google kündigte bereits an, Berufung gegen die Entscheidung der Geschworenen einlegen zu wollen. Die Verfahren gegen Apple und Google zeigen, dass die vom Open-App-Markets-Act-Vorschlag intendierten Ziele eventuell auch im Wege wettbewerbsrechtlicher Rechtsprechung erreicht und Interoperabilität für App-Marktplätze mit fairen Konditionen hergestellt werden könnte.

c. *American Innovation and Choice Online Act*

Der erstmals im Jahr 2021 eingebrachte Entwurf für einen American Innovation and Choice Online Act (AICOA) zielte primär auf die Regulierung des *self-preferencing*, also die Untersagung der Bevorzugung eigener

862 Epic Games, Inc. v. Apple Inc., 4:20-cv-05640, (N.D. Cal.), 10.9.2021.
863 Epic Games Inc. v. Apple Inc, 9th U.S. Circuit Court of Appeals, No. 21–16506.
864 US Supreme Court, Docket No. 23–344, Vide 23–337, 16.1.2024.
865 Epic v. Google, Case 3:20-cv-05671-JD (N.D. Cal.), 11.12.2023.

Produkte und Dienstleistungen durch große Online-Plattformen.[866] Der Entwurf ist in sieben Teile gegliedert: Titel des Gesetzes (Section 1), Definitionen (Section 2), Regelung rechtswidrigen Verhaltens (Section 3), die Rechtsdurchsetzung durch FTC und US DOJ sowie Schlussbestimmungen (Sections 5 bis 7).

Der AICOA zielt auf die Regulierung von Online-Plattformen mit mehr als 50 Millionen monatlich aktiven US-Nutzern, 100.000 monatlich aktiven gewerblichen US-Nutzern oder weltweit mindestens 1 Milliarde aktiven Plattformnutzern. Ferner muss das plattformbetreibende Unternehmen einen Marktwert von über USD 550 Milliarden aufweisen sowie in der Lage sein, den Zugang gewerblicher Plattformnutzer zu ihren Kunden oder zu essenziellen Werkzeugen oder Leistungen einzuschränken, die sie benötigen, um ihre Kunden zu erreichen.[867] Zusätzlich müssen vom AICOA erfasste Plattformen gemeinsam von der FTC und dem US DOJ als solche benannt werden, wenn sie die zuvor genannten Voraussetzungen erfüllen.[868] Dieses Vorgehen ist mit der Benennung von Gatekeepern durch die Europäische Kommission nach Art. 3 DMA vergleichbar (dazu oben C.II.2.c(1)). Der AICOA wäre, anders als der Open App Markets Act, nicht auf App-Marktplätze beschränkt. Primär zielt der Entwurf des AICOA auf das Verbot der Bevorzugung eigener Produkte oder Dienstleistungen durch Plattformbetreiber auf der eigenen Plattform, wenn dies den Wettbewerb erheblich gefährden würde.[869] Hinsichtlich der Interoperabilität wäre es Plattformbetreibern untersagt, gewerblichen Nutzern den Zugang zu oder die Interoperabilität mit der Plattform, Betriebssystemen sowie Hard- oder Softwarefunktionen erheblich zu behindern, wenn dieser Zugang oder diese Interoperabilität den eigenen Produkten oder Dienstleistungen des Plattformbetreibers zur Verfügung steht:[870]

SEC. 3. UNLAWFUL CONDUCT.
(a) In General.—It shall be unlawful for a person operating a covered platform in or affecting commerce to—

866 American Innovation and Choice Online Act of 2023 (AIOCA), S.2033 (118th Congress). Der erste Entwurf wurde als American Innovation and Choice Online Act of 2021, H.R.3816 (117th Congress) eingebracht.
867 American Innovation and Choice Online Act of 2023, § 2(a)(5).
868 American Innovation and Choice Online Act of 2023, § 3(d).
869 American Innovation and Choice Online Act of 2023, § 3(a).
870 American Innovation and Choice Online Act of 2023, § 3(a)(4).

(4) *materially restrict, impede, or unreasonably delay the capacity of a business user to access or interoperate with the same platform, operating system, or hardware or software features that are available to the products, services, or lines of business of the covered platform operator that compete or would compete with products or services offered by business users on the covered platform, except where such access would lead to a significant cybersecurity risk […].*

Darüber hinaus ist es Plattformen untersagt, vertragliche oder technische Beschränkungen vorzunehmen, die gewerbliche Plattformnutzer daran hindern, relevante Daten in andere Systeme oder Anwendungen zu exportieren:[871]

SEC. 3. UNLAWFUL CONDUCT.
(a) In General.—It shall be unlawful for a person operating a covered platform in or affecting commerce to—

(7) *materially restrict or impede a business user from accessing data generated on the covered platform by the activities of the business user, or through an interaction of a covered platform user with the products or services of the business user, such as by establishing contractual or technical restrictions that prevent the portability by the business user to other systems or applications of the data of the business user […].*

Ausnahmen hiervon sind zum Erhalt der Sicherheit und des Datenschutzes oder zum Funktionserhalt betroffener Plattformen vorgesehen.[872] Darüber hinaus kann ein Plattformbetreiber darlegen, dass ein bestimmtes Verhalten keine erhebliche Beeinträchtigung des Wettbewerbs nach sich gezogen hat oder ziehen würde.[873] Interoperabilität wird im Entwurf nicht legaldefiniert, was Plattformen die einseitige Möglichkeit zur Ausgestaltung der Interoperabilitäts- und Zugangsbedingungen einräumt. Darüber hinaus ist der Anwendungsbereich für Interoperabilität in der Weise beschränkt, dass sie nur bei einer erheblichen Wettbewerbsbeeinträchtigung, die zu befürchten oder bereits eingetreten ist, geschaffen werden muss.

Das Gesetz soll von der FTC und dem US DOJ sowie durch einzelstaatliche Generalanwälte durchgesetzt werden.[874] Ein Verstoß soll mit bis zu

871 American Innovation and Choice Online Act of 2023, § 3(a)(7).
872 American Innovation and Choice Online Act of 2023, § 3(b).
873 American Innovation and Choice Online Act of 2023, § 3(b)(2).
874 American Innovation and Choice Online Act of 2023, § 3(c).

10 % des gesamten US-Umsatzes eines Plattformbetreibers im Zeitraum des Verstoßes geahndet werden können.[875] Daneben sollen die US-Wettbewerbshüter zeitlich begrenzte Verfügungen aussprechen können, etwa um eine Handlung zu unternehmen oder zu unterlassen.[876] Bei wiederholten Verletzungen gegen den AICOA sollen der CEO oder andere leitende Angestellte der betroffenen Plattform ein Jahresgehalt als Strafe an das US Finanzministerium zahlen müssen.[877] Die Aufsichtsbehörden sollen Leitlinien zur Durchsetzung des Gesetzes veröffentlichen, insbesondere zur Klarstellung, was eine erhebliche Wettbewerbsbeeinträchtigung darstellt. Ziel dieser Leitlinien ist es, Transparenz herzustellen, Verstöße abzuschrecken sowie Innovation und wettbewerbsförderndes Verhalten zu fördern. Vor einer Verabschiedung sollen die Leitlinien von anderen Behörden und der Öffentlichkeit kommentiert werden können.[878]

d. Digital Platform Commission Act

Derzeit gibt es keine eigens für die Aufsicht und Regulierung von Big-Tech-Unternehmen eingerichtete US-Bundesbehörde, auch wenn dies in der öffentlichen Diskussion in bewusster Ergänzung zur FTC mitunter gefordert wird.[879] Der Entwurf für einen Digital Platform Commission Act sieht die Errichtung einer solchen US-Bundesbehörde, die Federal Digital Platform Commission, vor. Sie soll für die Aufsicht und Regulierung digitaler Plattformen zuständig sein.[880] Die Behörde soll u. a. den Zugang zu digitalen Plattformen und den Wettbewerb fördern sowie eine schädliche Machtkonzentration von Plattformen verhindern (Section 4).[881] Sie soll digitale Plattformen als systemrelevant bestimmen können (Section 10),[882] denen dann gesonderte Verpflichtungen auferlegt werden können (Section 5(b)).

875 American Innovation and Choice Online Act of 2023, § 3(c)(6)(B).
876 American Innovation and Choice Online Act of 2023, § 3(c)(6)(C).
877 American Innovation and Choice Online Act of 2023, § 3(c)(6)(D).
878 American Innovation and Choice Online Act of 2023, § 4.
879 *Wheeler/Verveer/Kimmelmann*, New Digital Realities; New Oversight Solutions in the US, 2020; *Feld*, The Case for the Digital Platform Act, 2019.
880 Digital Platform Commission Act of 2023, S.1671 (118th Congress). Der erste Entwurf wurde 2022 als Digital Platform Commission Act of 2022, S.4201 (117th Congress) eingebracht.
881 Digital Platform Commission Act of 2023, § 4(b).
882 Digital Platform Commission Act of 2023, §§ 3(7), 10.

Als Kriterien zur Ermittlung der Systemrelevanz vorgesehen sind (1) die Erreichbarkeit für die Öffentlichkeit, (2) ein erhebliches Engagement von Nutzern, etwa durch das Teilen von Beiträgen, (3) die Tätigkeit in mehreren US-Bundestaaten oder international, (4) erhebliche landesweite wirtschaftliche, soziale oder politische Auswirkungen der Plattform. Zu letzterem Kriterium gehören (a) die Möglichkeit zur maßgeblichen Beeinflussung der nationalen Verbreitung von Nachrichten, (b) die Möglichkeit der wirtschaftlichen, sozialen oder politischen Schädigung einer Person, wenn sie von der Nutzung der Plattform ausgeschlossen wird, (c) die Marktmacht, (d) die Nutzeranzahl und (e) die Abhängigkeit von Unternehmen von der Plattform, um Kunden zu erreichen.[883] Für systemrelevante Plattformen soll die Behörde zusammen mit einem Expertengremium (*Code Council*, dazu unten) kommerzielle und technische Standards für die Datenportabilität und Interoperabilität – verstanden als die Fähigkeit technischer Systeme, Daten auszutauschen und Informationen zu teilen – formulieren:[884]

> *SEC. 5. JURISDICTION*
> *(b) Provisions Relative To Systemically Important Digital Platforms.—Not later than 180 days after the earliest date as of which not fewer than 3 Commissioners have been confirmed, the Commission shall determine whether to promulgate rules, with input from the Code Council as appropriate, to establish for systemically important digital platforms—*
>
> (1) *commercial and technical standards for—*
> (A) *data portability; and*
> (B) *interoperability, which shall be defined as the functionality of information systems to—*
> (i) *exchange data; and*
> (ii) *enable sharing of information […].*

Daneben sollen Anforderungen an die algorithmische Transparenz,[885] die Transparenz von Nutzungsbedingungen[886] und die Risikoabschätzungen für die Verbreitung schädlicher Inhalte[887] sowie Transparenzverpflichtungen gegenüber der Behörde und die Verpflichtung zu unabhängigen Au-

883 Digital Platform Commission Act of 2023, § 10(b).
884 Digital Platform Commission Act of 2023, § 5(b)(1).
885 Digital Platform Commission Act of 2023, § 5(b)(2).
886 Digital Platform Commission Act of 2023, § 5(b)(3).
887 Digital Platform Commission Act of 2023, § 5(b)(4).

dits[888] sowie zur Barrierefreiheit[889] enthalten sein. Zahlreiche verwaltungsspezifische Regelungen zur Errichtung der Behörde (Section 6 und 7)[890] werden im Gesetzesentwurf durch die Verpflichtung zur Errichtung eines *Code Council* ergänzt (Section 8), der freiwillige oder verpflichtende Verhaltensregelungen, technische Standards oder sonstige Regelungen entwickeln soll. Der Council soll zu je gleichen Teilen mit Vertretern digitaler Plattformen, Nicht-Regierungsorganisationen oder Wissenschaftlern und technischen Experten besetzt werden.[891]

Zu den weiteren Verpflichtungen der geplanten Federal Digital Platform Commission zählen die Unterstützung anderer Bundesbehörden (Section 11), die Behandlung von Ausnahmen zu erlassenen Regelungen (Section 12) und die Durchführung eigener Forschung (Section 13). Die Behörde soll mit Ermittlungsbefugnissen gegenüber Plattformen ausgestattet werden (Section 14). Darüber hinaus soll der wettbewerbsrechtliche Clayton Antitrust Act um besondere *Pre-merger-notification*-Verpflichtungen für systemrelevante digitale Plattformen erweitert werden (Section 15). Privatpersonen und Wettbewerber sollen sich bei der Federal Digital Platform Commission über digitale Plattformen beschweren können, wenn sie einen Verstoß derselben gegen die auf sie anwendbaren Regeln nach dem Digital Platform Commission Act vermuten. Gleichzeitig sollen sie, wie im übrigen US-Wettbewerbsrecht, ein zivilrechtliches Klagerecht erhalten. Dieses soll sich auch auf die Generalstaatsanwälte der Bundesstaaten erstrecken (Section 16). Die Behörde selbst soll mit Abhilfebefugnissen wie der Möglichkeit, Verwarnungen auszusprechen, aber auch Betroffenen Schadensersatz zusprechen und Bußgelder von bis zu 15 % des weltweiten Jahresumsatzes des Vorjahres zu verhängen (Section 17), ausgestattet sein. Betroffene Unternehmen sollen Rechtsmittel gegen Entscheidungen und Anordnungen der Behörde einlegen können (Section 18). Die Arbeit der geplanten Federal Digital Platform Commission soll nach fünf Jahren evaluiert werden.

Die geplante Behörde würde digitale Plattformen und algorithmische Transparenz – und damit auch die damit verbundene Künstliche Intelligenz – regulieren. Die bereichsübergreifende Behörde wäre mit einem erheblichen Aufgabenportfolio und entsprechenden Befugnissen ausgestattet, dar-

888 Digital Platform Commission Act of 2023, § 5(b)(5).
889 Digital Platform Commission Act of 2023, § 5(b)(6).
890 Digital Platform Commission Act of 2023, §§ 6, 7.
891 Digital Platform Commission Act of 2023, § 8.

unter auch die Festlegung von Datenportabilitäts- und Interoperabilitätsregelungen für systemrelevante digitale Plattformen. Dass diese nicht gesetzlich vorgegeben, sondern von der Behörde und Experten aus Industrie, Zivilgesellschaft und Wissenschaft in Form der Co-Regulierung erarbeitet werden sollen, ermöglicht eine inhaltliche Flexibilität für die konkrete Ausgestaltung von Interoperabilität. Ob die Behörde jedoch so errichtet wird wie geplant oder nicht doch wesentliche Kompetenzen auf bestehende Behörden wie die FCC oder die FTC verteilt würden, bleibt im weiteren politischen Prozess abzuwarten, soweit der Gesetzesvorschlag überhaupt Aussicht auf eine Mehrheit hat.

e. Digital Consumer Protection Commission Act

In den US-Kongress wurde mit dem Digital Consumer Protection Commission Act (DCPCA) of 2023[892] ein weiterer Vorschlag zur Schaffung einer US-Bundesbehörde zur Regulierung großer Online-Plattformen eingebracht. Die Kompetenzen der geplanten Digital Consumer Protection Commission sollen im Bereich des Wettbewerbs, der Transparenz, des Datenschutzes und der nationalen Sicherheit liegen. Der weitreichende Gesetzesentwurf besteht aus acht Teilen: Errichtung der Behörde (Title I), Anforderungen an Transparenz (Title II), Reform des Wettbewerbsrechts mit Regelungen zur Datenportabilität und Interoperabilität (Title III), Regelungen zum Datenschutz auf Bundesebene (Title IV), nationale Sicherheit (Title V), Zulassung dominanter Online-Plattformen (Title VI), Durchsetzung des Gesetzes, u. a. durch weitere US-Behörden wie der FTC (Title VII), sowie Schlussbestimmungen (Title VIII).

Die Digital Consumer Protection Commission soll branchenweite Verordnungen (*rules*, dazu auch oben C.IV.1.b(1)) erlassen können und mit weitreichenden Untersuchungs- und Abhilfebefugnissen ausgestattet werden.[893] Im Gesetzesentwurf wird zwischen Plattformen und sog. dominanten Plattformen unterschieden, wobei letztere stärker reguliert werden sollen. Eine dominante Plattform ist ein Unternehmen, das im Falle einer Börsennotierung mindestens 50 Millionen monatlich aktive US-Nutzer (25 Millionen bei nicht börslich gelisteten Unternehmen) oder 100.000 monatliche aktive US-Geschäftskunden (75.000 bei nicht börslich gelisteten

892 Digital Consumer Protection Commission Act of 2023, S.2597 (118th Congress).
893 Digital Consumer Protection Commission Act of 2023, § 2115.

Unternehmen) hat und einen Börsenwert von über USD 550 Milliarden (bzw. ein EBITDA[894] von USD 30 Milliarden) aufweist.[895] Neben diesen wirtschaftlichen sind im Entwurf keine weiteren Kriterien zur Ermittlung einer dominanten Plattform vorgesehen, sollen aber von der Digital Consumer Protection Commission festgelegt werden können.[896]

Dominante Plattformen sollen von der geplanten Digital Consumer Protection Commission zugelassen werden müssen.[897] Ohne gültige Zulassung soll der Plattformbetreiber nicht mehr gewerblich tätig sein dürfen:

> *SEC. 2602. REQUIREMENT FOR OPERATORS OF DOMINANT PLATFORMS TO OBTAIN LICENSES.*
> *(b) Consequences Of Failure To Obtain License.—An operator of a dominant platform may not operate as a corporation, body corporate, body politic, joint-stock company, or limited liability company, as applicable, for the purposes of Federal law if the operator of the dominant platform does not have a license granted by the Commission under subsection (a).*

Eine vormals erteilte Zulassung soll wieder entzogen werden können, wenn ein Unternehmen wiederholt „ungeheuerliches" (*egregious*) und unrechtmäßiges Fehlverhalten an den Tag gelegt hat, das zu einem erheblichen Schaden für Plattformnutzer, Beschäftigte, Anteilseigner oder Geschäftspartner der dominanten Plattform geführt hat, ohne dass dieses Fehlverhalten vom Plattformbetreiber geahndet wurde.[898] Bedingungen zur Lizenzvergabe sind gesetzlich nicht festgelegt, könnten aber von der Digital Consumer Protection Commission vorgegeben werden.[899] Darüber hinaus müssen Plattformbetreiber, namentlich die leitenden Unternehmensangestellten, gegenüber der Digital Consumer Protection Commission die Einhaltung des DCPCA bestätigen. Bewusste Falschangaben könnten mit Geldstrafen von bis zu USD 10 Millionen pro Person und/oder Freiheitsstrafen von bis zu fünf Jahren sanktioniert werden.[900]

---

894 Earnings Before Interest, Taxes, Depreciation and Amortization, dt. Gewinn vor Zinsen, Steuern, Abschreibungen auf Sachanlagen und Abschreibungen auf immaterielle Vermögensgegenstände.
895 Digital Consumer Protection Commission Act of 2023, § 2121(a)(2).
896 Digital Consumer Protection Commission Act of 2023, § 2121(c)(3)(B).
897 Digital Consumer Protection Commission Act of 2023, § 2602.
898 Digital Consumer Protection Commission Act of 2023, § 2603(c)(2).
899 Digital Consumer Protection Commission Act of 2023, § 2603(f).
900 Digital Consumer Protection Commission Act of 2023, § 2604.

Zu den Verpflichtungen für dominante Plattformen gehört nach dem Vorschlag die Veröffentlichung der Nutzungsbedingungen und Kriterien für die Inhaltemoderation. Ferner sollen Plattformen ein Beschwerdeverfahren in Bezug auf Entscheidungen über die Moderation von Nutzerinhalten einrichten.[901] Hinsichtlich des Schutzes des freien Wettbewerbs sollen dominante Plattformen eine marktbeherrschende Stellung nicht missbrauchen dürfen. Dies schließt bspw. das *self-preferencing*, also die Bevorzugung eigener Dienste und Produkte, aber auch das *tying*, also die Kopplung von Leistungen, ein.[902] Darüber hinaus sieht der Entwurf des DCPCA vor, dass Zusammenschlüsse im Vorfeld und nachträglich überprüft werden können. Dabei soll es möglich sein, Unternehmenstransaktionen zu untersagen bzw. rückabzuwickeln, Unternehmen also zu entflechten.[903]

Zum wettbewerbsrechtlichen Teil zählen auch Regelungen zur Datenportabilität und Interoperabilität, die nur auf dominante Plattformen Anwendung finden sollen. Mit Blick auf die Datenportabilität sollen Plattformbetreiber verpflichtet werden, entsprechende Schnittstellen (einschließlich APIs) zur Verfügung zu stellen, über die ein privater oder gewerblicher Nutzer kostenfrei bereitgestellte oder bei der Nutzung der Plattform angefallene Daten abrufen können soll:[904]

> *SEC. 2321. DATA PORTABILITY AND INTEROPERABILITY.*
> *(a) Data Portability.—An operator of a dominant platform, with respect to the dominant platform, shall maintain a set of interfaces that are transparent and accessible to third parties (including application programming interfaces) to provide a user (or a third party authorized by a user), upon the request of the user (or such a third party) and free of charge, with effective portability of data provided by the user or generated through the activity of the user in the context of the use of the relevant core platform service of the dominant platform, including by providing free of charge tools to facilitate the effective exercise of that data portability.*

Ein Nutzer soll somit Daten selbst abrufen oder durch einen Dritten abrufen lassen können, aber nicht direkt an andere Plattformen übermitteln können. Der Begriff der Datenportabilität wird nicht legaldefiniert, sodass auch keine Regelungen hinsichtlich des Datenformats vorgesehen sind.

901 Digital Consumer Protection Commission Act of 2023, §§ 2201, 2202.
902 Digital Consumer Protection Commission Act of 2023, § 2311.
903 Digital Consumer Protection Commission Act of 2023, §§ 2313–2315.
904 Digital Consumer Protection Commission Act of 2023, § 2321(a).

Während Datenportabilität allen, also privaten und gewerblichen Nutzern dominanter Plattformen eingeräumt werden soll, ist Interoperabilität mit dominanten Plattformen nur für gewerbliche Nutzer und Wettbewerber vorgesehen:[905]

> *SEC. 2321. DATA PORTABILITY AND INTEROPERABILITY.*
> *(b) Interoperability.—An operator of a dominant platform, with respect to the dominant platform, shall, free of charge—*
>
> (1) *allow a business user, provider of services, provider of ancillary services, or provider of hardware access to and interoperability with the same hardware features and software features accessed or controlled via an operating system that are available to services on the dominant platform or hardware provided by the operator;*
> (2) *provide a business user (or a third party authorized by a business user), upon the request of the business user (or such a third party), with continuous and real-time access and use of aggregated and non-aggregated data, that is provided for or generated in the context of the use of the relevant core platform services of the dominant platform or ancillary services offered by the dominant platform to the business user and each end user engaging with a product or service provided by the business user; and*
> (3) *provide, at the request of a business user, the possibility and necessary tools to access and analyze data on the dominant platform without a transfer from the dominant platform.*

Erstens sollen Betreiber dominanter Plattformen gewerblichen Nutzern der Plattform sowie Dienste- und Hardwareanbietern kostenfrei Zugang zu und Interoperabilität mit der Hard- und Software des Plattformanbieters einräumen, und zwar im selben Maße, wie diese Interoperabilität Diensten des Plattformbetreibers zusteht.[906] Die Formulierung schließt damit nicht nur die Interoperabilität mit Softwarefeatures in (Betriebs-)Systemen von Plattformanbietern, sondern bspw. auch den Zugang zu Sensoren in technischen Geräten wie Smartphones oder Virtual-Reality-Headsets ein. Zweitens soll gewerblichen Nutzern einer Plattform ein dauerhafter Echtzeitzugang zu Inhalts- und Nutzungsdaten der Plattform gewährt werden.[907] Drittens sol-

905 Digital Consumer Protection Commission Act of 2023, § 2321(b).
906 Digital Consumer Protection Commission Act of 2023, § 2321(b)(1).
907 Digital Consumer Protection Commission Act of 2023, § 2321(b)(2).

len Betreiber dominanter Plattformen gewerblichen Nutzern auf Verlangen die Möglichkeit und die erforderlichen Werkzeuge zum Zugang und zur Analyse von Daten unmittelbar auf der Plattform einräumen, ohne dass hierfür Daten von der Plattform exportiert werden müssen.[908] Auch hierbei wird dominanten Plattformen eingeräumt, Maßnahmen für die Sicherheit oder den Schutz von Daten ergreifen zu dürfen.[909]

Mit diesen drei Regelungen geht das im Entwurf des DCPCA vorgesehene Recht auf Interoperabilität in Teilen erheblich weiter als bspw. der Entwurf des ACCESS Act. Insbesondere das nicht weiter differenzierte Recht zum kostenfreien Zugang zu und zur Analyse von Daten auf einer dominanten Plattform scheint, anders als im ACCESS Act, Interessen von Plattformbetreibern an der angemessenen Nutzung von Interoperabilitätsschnittstellen nur bedingt zu berücksichtigen. Auch werden technische Standards und regulatorische Kriterien für Interoperabilität nicht im Entwurf des DCPCA festgelegt. Eine ausdrückliche Aufforderung zum Erarbeiten branchenweiter Standards (*rulemaking*), wie dies bspw. bei Wettbewerbsverletzungen im Bereich des *self-preferencing* oder *tying* der Fall ist,[910] ist ebenfalls nicht vorgesehen. Die praktische Ausgestaltung und Umsetzung der Interoperabilität wäre damit den dominanten Plattformen selbst überlassen, was wiederum zu einer fragmentierten Interoperabilitätslandschaft selbst im Anwendungsbereich der dominanten Plattformen führen könnte.

Neben dem wettbewerbsrechtlich ausgestalteten Recht auf Datenportabilität und Interoperabilität bei dominanten Plattformen sieht der Entwurf des DCPCA im Rahmen von Datenschutzrechten ein Recht auf Datenportabilität bei den übrigen Plattformen des nicht-öffentlichen Bereichs vor:[911]

> *SEC. 2416. RIGHTS OF DATA SUBJECTS TO ACCESS, CORRECTION, PORTABILITY, AND DELETION.*
> *(a) Access To And Portability Of Personal Data.—A person shall have the right to—[…]*
>
> (3) *obtain any personal data of the person that has been processed by a covered entity in a structured, readily usable, portable, and machine-readable format;*

908 Digital Consumer Protection Commission Act of 2023, § 2321(b)(3).
909 Digital Consumer Protection Commission Act of 2023, § 2321(c).
910 Digital Consumer Protection Commission Act of 2023, § 2311(e).
911 Digital Consumer Protection Commission Act of 2023, §§ 2002(8), 2416.

(4) *with respect to personal data of the person that is stored by a covered entity, transmit or cause the covered entity to transmit the personal data to another covered entity, where technically feasible […].*

Diese Ausgestaltung des Rechts auf Datenportabilität ähnelt Art. 20 DS-GVO, da Daten in einem strukturierten, gängigen, portablen und maschinenlesbaren Format bereitgestellt und entweder an den Nutzer oder an eine andere Plattform übermittelt werden müssten. Darüber hinaus sehen die Datenschutzregeln im Gesetzesentwurf ein Verbot insbesondere der Verarbeitung von Nutzerdaten vor, wenn die Verarbeitung nicht im Interesse des Nutzers liegt oder Nutzern schaden würde.[912] Darüber hinaus würde nutzerbasierte Werbung in der Form eingeschränkt, dass dominante Plattformen hierfür lediglich eigene Daten verwenden dürften, aber keine Daten von Dritten heranziehen könnten.[913] Zum Schutz personenbezogener Daten ist die Verpflichtung zur Umsetzung technischer und organisatorischer Maßnahmen sowie zur Meldung von Datenschutzvorfällen an die Digital Consumer Protection Commission vorgesehen.[914]

Der Digital Consumer Protection Commission Act soll nicht nur von der geplanten Digital Consumer Protection Commission durchgesetzt werden können, sondern auch von einzelstaatlichen Generalstaatsanwälten,[915] betroffenen Plattformnutzern und Wettbewerbern[916] sowie hinsichtlich des Wettbewerbsrechts auch durch die FTC und das US DOJ.[917] Bei Verstößen gegen das Gesetz könnten gegen Plattformbetreiber Bußgelder von bis zu 15 % des weltweiten Jahresumsatzes des Vorjahrs verhängt werden.[918] Verstöße könnten auch strafrechtlich mit Freiheitsstrafen von bis zu einem Jahr verfolgt werden.[919]

912 Digital Consumer Protection Commission Act of 2023, §§ 2411–2414.
913 Digital Consumer Protection Commission Act of 2023, § 2415.
914 Digital Consumer Protection Commission Act of 2023, §§ 2421, 2422.
915 Digital Consumer Protection Commission Act of 2023, § 2701(a).
916 Digital Consumer Protection Commission Act of 2023, § 2701(b).
917 Digital Consumer Protection Commission Act of 2023, § 2701(c).
918 Digital Consumer Protection Commission Act of 2023, § 2115(c)(2).
919 Digital Consumer Protection Commission Act of 2023, § 2115(a)(3)(D).

f. Journalism Competition and Preservation Act

Auf großen Online-Plattformen werden Nachrichten veröffentlicht und geteilt unabhängig davon, ob sie ursprünglich aus dem Bereich Print, Online oder Rundfunk stammen. Entsprechende Einnahmen, etwa aus Werbung, fließen jedoch größtenteils Online-Plattformen und nicht dem Journalismus, also denjenigen, die Nachrichten produzieren oder veröffentlichen, zu. US-Zeitungsverlage haben deshalb angeregt,[920] im Kartellrecht eine Ausnahme vorzusehen, die es Verlagen kollektiv erlaubt, Inhalte vor Online-Plattformen zurückzuhalten und Lizenzbedingungen für die Veröffentlichung von Nachrichten zu verhandeln, ohne dafür kartellrechtlich belangt werden zu können.

Ein entsprechender Entwurf für einen Journalism Competition and Preservation Act wurde im Jahr 2018 in den US-Kongress eingebracht.[921] Der Ansatz kann als US-amerikanische Entsprechung zum europäischen Leistungsschutzrecht für Presseverlage verstanden werden, das mit der DSM-Richtlinie in Europa normiert wurde. Verleger erhofften sich durch eine derartige Regelung eine gestärkte kollektive Verhandlungsposition gegenüber Online-Plattformen, die journalistische Inhalte von Dritten veröffentlichen und weltweit mindestens 1 Milliarde monatlich aktive Nutzer aufweisen.[922] Die kartellrechtliche Ausnahme sollte jedoch nur dann gelten, wenn die Verhandlungen sich nicht nur auf den Preis beschränken, andere Nachrichtenersteller nicht benachteiligen und sich unmittelbar auf die Qualität, Richtigkeit, Namensnennung oder das Branding sowie die Interoperabilität von Nachrichten beziehen:[923]

> *SEC. 3. SAFE HARBOR FOR CERTAIN COLLECTIVE NEGOTIATIONS.*
> *(b) Limitation of Liability.—A news content creator shall not be held liable under the antitrust laws for engaging in negotiations with other news content creators during the negotiation period to collectively withhold content from, or negotiate with, an Online Content Distributor regarding the terms on which the news content creators' news content may be distributed by the Online Content Distributor, if—*

920 *Shafer*, Newspapers' Embarrassing Lobbying Campaign, Politico, 10.6.2019, https://www.politico.com/magazine/story/2019/06/10/newspapers-embarrassing-lobbying-campaign-227100/.
921 Journalism Competition and Preservation Act of 2018, H.R. 5190 (115th Congress).
922 Journalism Competition and Preservation Act of 2018, § 3(a)(2).
923 Journalism Competition and Preservation Act of 2018, § 3(b).

(1) *the negotiations with the Online Content Distributor—*

(A) *are not limited to price and are nondiscriminatory as to similarly situated news content creators, and directly relate to the quality, accuracy, attribution or branding, and interoperability of news; and*

(B) *pertain to terms that would be available to all news content creators;*

(2) the coordination among the news content creators is directly related to and *reasonably necessary for negotiations with an Online Content Distributor that are otherwise consistent with this Act; and*

(3) *the negotiations do not involve any person that is not a news content creator or an Online Content Distributor.*

Im Gesetzesentwurf wird die Interoperabilität von Nachrichten nicht definiert. Es ist daher zu vermuten, dass Nachrichten auf verschiedenen Plattformen veröffentlicht werden können sollen. Der Journalism Competition and Preservation Act konnte im 115. US-Kongress (2017–2019) nicht verabschiedet werden. Der Gesetzesentwurf wurde im Hinblick auf die Haftungsfreistellung unverändert erneut in den 116. US-Kongress (2019–2021)[924] und den 117. US-Kongress (2021–2023)[925] eingebracht, fand aber bislang ebenfalls keine Mehrheit in diesen Legislaturperioden. Ohnehin wird vermutet, dass der Entwurf kaum die erhoffte gestärkte Verhandlungsposition für Verleger bringen würde, weil Nachrichten nur einen kleinen Teil von Online-Plattformen ausmachen würden. Darüber hinaus würden große weltweite Verleger nicht gehindert, individuelle Lizenzvereinbarungen mit Anbietern wie Meta oder Google zu schließen. Die Position kleiner Verleger würde dadurch trotz des Journalism Competition and Preservation Act nur unwesentlich gestärkt.[926]

Gleichwohl wurde der Entwurf auch in der laufenden Legislaturperiode, dem 118. Kongress, eingebracht und erfuhr dabei durch den Senat erhebliche Änderungen und Konkretisierungen.[927] Zum einen sollen anders als zuvor Online-Plattformen erfasst werden, die mindestens 50 Millionen monatliche aktive US-Nutzer haben und entweder mindestens 1 Milliarde monatlich aktive Nutzer weltweit oder einen Börsenwert von über USD 550 Milliarden aufweisen.[928] Darüber hinaus sind detaillierte Anforderun-

924 Journalism Competition and Preservation Act of 2019, H.R. 2054 (116th Congress).
925 Journalism Competition and Preservation Act of 2021, H.R. 1753 (117th Congress).
926 *Netanel*, in: Harvard Journal of Law & Technology 34, 2, 2021, S. 473, 509.
927 Journalism Competition and Preservation Act of 2023, S.1094 (118th Congress).
928 Journalism Competition and Preservation Act of 2023, § 2(3).

gen an Verleger und Rundfunkanbieter geplant, um von der kartellrechtlichen Ausnahme Gebrauch machen zu können. So sollen die betreffenden Medien primär eine US-Zielgruppe haben und mindestens 25 % an Inhalten von lokalem, nationalem oder internationalem Interesse enthalten oder nicht mehr als 1.500 Vollzeitangestellte beschäftigen.[929] Darüber hinaus sollen Zusammenschlüsse der betroffenen Plattform, also etwa Google, wie auch der FTC und dem US DOJ angezeigt werden müssen.[930] Darüber hinaus soll nur über „pricing, terms, and conditions" verhandelt werden dürfen. Der Begriff erfährt eine negative Abgrenzung zur Wahrung der Rechte der Plattformen:[931]

> *SEC. 2. DEFINITIONS.*
> *(10) PRICING, TERMS, AND CONDITIONS.—The term "pricing, terms, and conditions" does not include any term or condition which relates to the use, display, promotion, ranking, distribution, curation, suppression, throttling, filtering, or labeling of the content or viewpoint of any person.*

Verhandelnde Verleger sollen also nicht über die Nutzung, Anzeige, Bewerbung, das Ranking, das Kuratieren, die Verbreitung, Unterdrückung, Drosselung, Filterung oder Kennzeichnung ihrer Inhalte auf einer Online-Plattform verhandeln können. Interoperabilität von Nachrichten findet im jüngsten Entwurf auch keine ausdrückliche Erwähnung mehr. Dafür soll der US-Rechnungshof einen Bericht über abgeschlossene Verhandlungen und Vereinbarungen zwischen Plattformen und Verlegern veröffentlichen und insbesondere die Auswirkungen auf lokale und regionale Nachrichten sowie ein freies, offenes und interoperables Internet, einschließlich der Möglichkeit für die Öffentlichkeit, Nachrichten abzurufen und zu teilen, berücksichtigen:[932]

> *SEC. 8. REPORT*
> *(a) Study.—The Comptroller General shall study the impact of the joint negotiations authorized under this Act, including a summary of the deals negotiated, the impact of such deals on local and regional news, the effect on the free, open, and interoperable Internet including the ability of the public to share and access information, and the effect this Act has had on employment for journalists.*

929 Journalism Competition and Preservation Act of 2023, § 2(11).
930 Journalism Competition and Preservation Act of 2023, § 3(a)(2)(A) und (D).
931 Journalism Competition and Preservation Act of 2023, § 2(10).
932 Journalism Competition and Preservation Act of 2023, § 8.

Es bleibt abzuwarten, ob, wann und in welcher Form der Journalism Competition and Preservation Act weiter diskutiert wird.

g. Personal Financial Data Rights

In den USA sind im Finanzwesen noch keine Datenportabilitäts- bzw. Interoperabilitätsanforderungen normiert. Allerdings erließ Präsident Biden im Jahr 2021 eine Executive Order zur Stärkung der US-amerikanischen Wirtschaft, in der Interoperabilität am Finanzmarkt angedacht wird. Eine Executive Order ist eine bindende Anordnung des US-Präsidenten für die Bundesregierung. Das Consumer Financial Protection Bureau (CFPB) wird darin aufgefordert, eine Verordnung zu erlassen, auf deren Grundlage Verbraucher Daten über ihre finanziellen Transaktionen erhalten und nutzen können, um auf einfachem Weg ihre Finanzinstitution wechseln oder innovative Finanzprodukte in Anspruch nehmen zu können:[933]

> *The Director of the Consumer Financial Protection Bureau […] is encouraged to consider commencing or continuing a rulemaking […] to facilitate the portability of consumer financial transaction data so consumers can more easily switch financial institutions and use new, innovative financial products.*

Das CFPB ist eine Regulierungsbehörde für Verbraucherschutz im Finanzwesen, die mit Aufsichts- und Durchgriffsrechten auf US-Finanzinstitute ausgestattet ist. Es hatte bereits 2016 die Arbeit an einer entsprechenden Verordnung aufgenommen.[934] Erst im Jahr 2023 wurde der Entwurf für eine entsprechende Verordnung zu Personal Financial Data Rights veröffentlicht.[935] Kommentare und Anmerkungen dazu konnten eingereicht werden, und auf der Grundlage der Eingaben wird das CFPB den Entwurf vor einer endgültigen Verabschiedung überarbeiten. Der Entwurf ist in vier Abschnitte unterteilt: (A) Allgemeine Regelungen, etwa zum Anwendungsbereich, (B) Verpflichtung zur Bereitstellung von Daten, (C) technische

933 Executive Order on Promoting Competition in the American Economy, Exec. Order No. 14036, 86 FR 36987 (9.7.2021).

934 CFPB, Required Rulemaking on Personal Financial Data Rights, https://www.consumerfinance.gov/personal-financial-data-rights/.

935 CFPB, Notice of Proposed Rulemaking for the Required Rulemaking on Personal Financial Data Rights 31.10.2023, 88 FR 74796, https://files.consumerfinance.gov/f/documents/cfpb-1033-nprm-fr-notice_2023-10.pdf.

Anforderungen an Schnittstellen sowie (D) Übermittlung von Daten an berechtigte Dritte. Die Verordnung soll vor allem auf Banken und Kartengesellschaften, etwa Kreditkartengesellschaften, Anwendung finden.

Die technischen Standards für die Interoperabilität sollen von Experten in einem offenen Gremium erarbeitet werden, das von der CFPB anerkannt wird. Die Verpflichtung zur Bereitstellung von Daten soll u. a. Transaktionsdaten, Kontostände, Produktbedingungen (bspw. Kontoführungskosten, Zinsen, eingeräumte Überziehungskredite) sowie Stammdaten des Verbrauchers umfassen. Daten sollen auch an Drittanbieter übermittelt werden können, wobei diese Anbieter auf der Grundlage der erhaltenen Daten keine zielgerichtete Werbung betreiben und die Daten nicht verkaufen dürfen. Mit der durch die Verordnung vorgesehenen Interoperabilität sollen Verbraucher elektronisch Zugang zu ihren Finanzdaten erhalten und sie etwa im Rahmen eines Kontowechsels oder bei der Inanspruchnahme digitaler Finanzdienstleistungen mit Dritten teilen können.

h. Multi-Cloud Innovation and Advancement Act

Im Sommer 2023 wurde der Multi-Cloud Innovation and Advancement Act of 2023 in den US-Kongress eingebracht.[936] Ziel des knappen Gesetzesvorhabens ist es, eine sichere Nutzung verschiedener Cloud-Anbieter durch die US-Bundesregierung zu eruieren. Verschiedene Behörden, darunter NIST, sollen einen Leitfaden entwickeln, der aufzeigt, wie US-Bundesbehörden Anwendungen und Daten portabel und interoperabel zwischen öffentlichen und privaten Cloud-Umgebungen entwickeln und einsetzen können:

> *SEC. 3. IMPLEMENTATION OF MULTI-CLOUD SOFTWARE TECHNOLOGY.*
> *(a) In General.—Not later than 1 year after the date of the enactment of this Act, the Director, in consultation with the Administrator of General Services, the Director of the National Institute of Standards and Technology, the Director of the Cybersecurity and Infrastructure Security Agency, and the Administrator of the United States Digital Service, is directed to carry out the following:*

936 Multi-Cloud Innovation and Advancement Act of 2023, H.R.4891 (118th Congress).

(1) *Examine how executive agencies can implement multi-cloud computing software technology architecture to allow for portability and interoperability across multiple cloud computing software vendors.*
(2) *Develop written guidance for all executive agencies based on the results of the examination described in paragraph (1) that—*
   (A) *describes how executive agencies should use multi-cloud software technology to allow for applications, data, and programs to be portable and interoperable between public, private, and edge cloud environments […].*

Der Gesetzesentwurf versteht „multi-cloud software technology" als Software, die Portabilität und Interoperabilität für Daten, Anwendungen und Programme zwischen verschiedenen Cloudanbietern ermöglicht:

> *SEC. 3. IMPLEMENTATION OF MULTI-CLOUD SOFTWARE TECHNOLOGY.*
> *(e) Definitions.—In this section:*
> *(6) Multi-Cloud Software Technology.—The term "multi-cloud software technology" means software technology that allows for data, application, and program portability and interoperability between multiple cloud computing software vendors and between public, private, and edge cloud environments in a manner that securely delivers operational and management consistency, comprehensive visibility, and resiliency.*

Mit dem Vorhaben soll Behörden oftmals fehlende fachliche Expertise zur Verfügung gestellt und der Betrieb von Cloud-Umgebungen durch US-Behörden effizienter und sicherer gestaltet werden.

2. Weitere Entwicklungen im internationalen Überblick

a. Vereinigtes Königreich

Auch im Vereinigten Königreich sind Entwicklungen im Zusammenhang mit Interoperabilität und entsprechende Initiativen auch für eine Gesetzgebung im Bereich des Wettbewerbsrechts verortet.

(1) Furman-Report

Beachtung verdient dabei zunächst der Abschlussbericht des Expertengremiums für digitalen Wettbewerb (Digital Competition Expert Panel), der auch als Furman-Report, benannt nach dem Vorsitzenden des Gremiums Jason Furman, bezeichnet wird.[937] Dieser Bericht gab 2019 Empfehlungen für Änderungen des britischen Wettbewerbsrechts, die erforderlich seien, um den wirtschaftlichen Herausforderungen der digitalen Märkte im Vereinigten Königreich und auf internationaler Ebene zu begegnen. Kernvorschläge waren eine Aktualisierung des Kartell- und Fusionsrechts und das Ergreifen einer Reihe wettbewerbsfördernder Maßnahmen zur Öffnung digitaler Märkte. Letzteres umfasste sowohl Grundprinzipien für Verhaltenskodizes zwischen Plattformen als auch eine Stärkung der Befugnisse der Wettbewerbsbehörde.

Unter anderem stellte der Bericht fest, dass Interoperabilität zwischen Online-Plattformen für einen belebten Wettbewerb essenziell sei. Hindernisse ergäben sich derzeit nicht nur aus technischen Umsetzungsproblemen und fehlender Koordinierung zwischen den Anbietern, sondern vor allem aus mangelnden Anreizen und Vorteilen, eine solche Interoperabilität sicherzustellen. Zwar gebe es Positivbeispiele, bei denen sich Interoperabilität durch die Koordinierung von Anbietern selbst eingestellt habe (bspw. E-Mails), im Digitalsektor bedürfe es aber eher regulatorischer Anreize oder einer verpflichtenden Gesetzgebung, wie es vormals bei der Telefonnummernportabilität der Fall gewesen sei. Der Bericht schlug daher vor, die Einheit für Digitale Märkte (Digital Markets Unit, DMU), die bei der britischen Wettbewerbsbehörde (Competition and Markets Authority (CMA)) eingerichtet ist, mit erweiterten Befugnissen auszustatten. Insbesondere sollte es Aufgabe der DMU sein, mehr Datenmobilität für Verbraucher und Systeme mit offenen Standards zu fördern. Zu diesem Zweck schlug der Furman-Report auch die Aktualisierung der Fusionskontrollrichtlinien dahingehend vor, dass eine intensivere Berücksichtigung mehrseitiger Plattformen bzw. Plattformmärkte erfolgen sollte, die auch die Bedeutung der Interoperabilität zwischen den Systemen und die Fähigkeit und Bereitschaft der Nutzer zum Wechsel zwischen Diensten einbezieht. Schließlich sollten Herausforderungen im Zusammenhang mit (fehlender) Interoperabilität durch die Verankerung allgemeiner Prinzipien in Verhaltenskodizes aufgegriffen werden. Zu diesen Prinzipien zählte der Bericht einen fairen, kon-

937 Digital Competition Expert Panel, Unlocking digital competition.

sistenten und transparenten Zugang zu Plattformen inklusive entsprechender Bedingungen für die Hervorhebung, das Ranking und die Bewertung von Inhalten sowie den Verzicht auf unfaire Beschränkungen oder „Strafen" für Nutzer, die Alternativen wählen.

(2) Untersuchungen der CMA

Die CMA hat 2019, teils aufbauend und bezugnehmend auf den Furman-Report, eine umfassende Untersuchung von Online-Plattformen und dem digitalen Werbemarkt eingeleitet. Die Ergebnisse der Untersuchung hat sie 2020 in einem umfassenden Bericht veröffentlicht.[938] Darin kam sie zu dem Ergebnis, dass die Dominanz einiger weniger großer Unternehmen – hier beim Fokus auf den digitalen Werbemarkt vor allem Google und Facebook (nunmehr Meta) – zu zahlreichen wettbewerbsrechtlich problematischen Entwicklungen führt. Genannt wurden Netzwerkeffekte und Größenvorteile, eine beeinträchtigte Entscheidungsfindung der Verbraucher durch Voreinstellungen, ein ungleicher Zugang zu Nutzerdaten, der Mangel an Transparenz, in sich geschlossene Ökosysteme (walled gardens) und die vertikale Integration sowie daraus resultierende Interessenkonflikte.

Die Empfehlung der CMA, um diesen Problemen im Vereinigten Königreich zu begegnen, lautete daher, ähnlich wie die Ergebnisse des Furman-Reports, dass die Regierung ein proaktives wettbewerbsförderndes Regulierungssystem für Online-Plattformen einführen solle. Eine Vergleichbarkeit besteht insoweit zu den Entwicklungen in Deutschland mit der GWB-Novelle sowie mit dem DMA auf EU-Ebene. Die DMU sollte befugt sein, einen Verhaltenskodex durchzusetzen, der das Verhalten von Plattformen mit Marktmacht regelt und sicherstellt, dass Bedenken schnell geklärt werden können, bevor unwiderruflicher Schaden für den Wettbewerb entsteht. Die DMU sollte ferner über Kompetenzen verfügen, um Ursachen der Marktmacht zu bekämpfen und den Wettbewerb zu stärken, einschließlich der Möglichkeit, die Interoperabilität zu verbessern und den Zugang zu Daten zu ermöglichen, die Auswahl für die Verbraucher zu vergrößern und ggf. die Auflösung von Plattformen anzuordnen.

938 *CMA*, Online platforms and digital advertising, Bericht samt Annexen abrufbar unter https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study.

Die Notwendigkeit der Herstellung von Interoperabilität sah die Untersuchung insbesondere[939] bei sozialen Netzwerken. Die Marktmacht von Facebook beruhe zum großen Teil auf starken Netzwerkeffekten, die sich aus seinem großen Netz verbundener Nutzer und der begrenzten Interoperabilität mit anderen sozialen Medienplattformen ergäben. Im Rahmen des avisierten Verhaltenskodex solle die DMU deshalb auch intervenieren können, wenn Facebook Einschränkungen der Interoperabilität vornehme, die die Fähigkeit der Konkurrenten einschränkten, direkt mit Facebook zu konkurrieren. Zudem solle sie auch die Herstellung der Interoperabilität anweisen können, wobei dies nur unter Berücksichtigung einer umfassenden Abwägung der Belange (tatsächliche Netzwerkeffekte, Datenschutz der Nutzer, Kosten, Folgen einer Homogenisierung) und ggf. beschränkt auf bestimmte Funktionen sozialer Netzwerke erfolgen solle.

Die Notwendigkeit von Interoperabilität ist aber laut CMA beschränkt: Zum einen geht die Behörde davon aus, dass aufgrund der aktuellen Marktlage zunächst[940] nur Facebook (nunmehr Meta in Bezug auf alle seine sozialen Netzwerke) verpflichtet sein sollte. Zum anderen sollte sich Interoperabilität nur auf bestimmte Funktionen beschränken, die sozialen Netzwerken gemein sind. Konkret nennt die CMA die Kontaktsuche und Cross-Posting-Funktionen, die interoperabel gestalten werden könnten. Für „ehrgeizigere" Interoperabilitätsbestrebungen, insbesondere eine vollständige Interoperabilität von Inhalten, sieht die CMA aber keine Veranlassung. Das betrifft also im Wesentlichen eine umfassende horizontale Interoperabilität zwischen sozialen Netzwerken. In Bezug auf die vertikale Interoperabilität merkt die CMA an, dass bei Facebook entsprechende Schnittstellen bereits in vielfältiger Hinsicht bestünden, z. B. zur Integration von Apps wie Spielen oder Plugins für Webseiten. Hier gehe es daher eher um die faire Ausgestaltung dieser Schnittstellen, die Gegenstand wettbewerbsrechtlicher Intervention sein könne.

Bemerkenswert ist dabei vor allem die Begründung der Wettbewerbsbehörde für solche Maßnahmen, die einen starken medienrechtlichen Einschlag aufweist: Die Beherrschung der digitalen Werbeeinnahmen durch solche Plattformen könne zu einem größeren sozialen, politischen und kulturellen Schaden durch den Rückgang maßgeblicher und zuverlässiger

939 In Bezug auf Suchmaschinen wurde Ähnliches für eine horizontale Interoperabilität zwischen Google und dritten Suchmaschinen wie Bing festgestellt.

940 Die CMA weist aber darauf hin, dass sich dieses Gleichgewicht auch schnell ändern könne.

Nachrichtenmedien und, daraus resultierend, zur Verbreitung von Desinformation und zum Niedergang der lokalen Presse führen. Ein florierender und wettbewerbsfähiger Markt für unabhängige Nachrichten und unabhängigen Journalismus sei daher für eine wirksame Demokratie von wesentlicher Bedeutung: Wenn die Nachhaltigkeit des maßgeblichen Journalismus untergraben werde, werde dies wahrscheinlich die Bedenken im Hinblick auf Desinformation und irreführende Informationen verstärken.

2022 folgte eine Untersuchung des mobilen Ökosystems.[941] Betrachtet wurde dabei vor allem die Interoperabilität der mobilen Betriebssysteme, App-Stores und Webbrowser von Google und Apple als den beiden dominanten Akteuren in diesen Bereichen. Auch hier wurde ein Mangel an Interoperabilität und Schnittstellenoffenheit festgestellt, der sich wettbewerbsgefährdend auswirke. Im Hinblick auf die Interoperabilität zwischen mobilen Betriebssystemen wurde sogar eine regulatorische Intervention als sinnvoll vorgeschlagen (vor allem bezüglich der Interoperabilität von iOS zu Android). Zugleich sah die CMA eine solche Intervention in Bezug auf Messenger-Dienste als (noch) nicht notwendig an.

(3) Entwurf eines Gesetzes für digitale Märkte, Wettbewerb und Verbraucher

Das Gesetz für digitale Märkte, Wettbewerb und Verbraucher (Digital Markets, Competition and Consumers Bill) wurde, aufbauend auf und unter Berücksichtigung der Empfehlungen aus den beiden oben genannten Berichten, im April 2023 vorgeschlagen und in das Gesetzgebungsverfahren eingebracht.[942] Seinen Weg durch das House of Commons, also das britische Unterhaus, hat der Entwurf bereits durchschritten. Die erste Lesung im House of Lords fand am 22. November 2023 statt. Es handelt sich um einen umfassenden Vorschlag bestehend aus sechs Teilen, die sich mit verschiedenen Aspekten von Wettbewerb und Verbraucherschutz befassen. Wesentlich sind dabei vier Säulen:[943]

- eine signifikante Erweiterung der Befugnisse der CMA zur Durchsetzung von Verbraucherschutzrecht, die unmittelbar in einem verwaltungs-

941 *CMA*, Mobile ecosystems, market study final report.
942 Vgl. https://bills.parliament.uk/bills/3453.
943 Vgl. dazu *Freshfields Bruckhaus Deringer*, The wait is over: UK Digital Markets, Competition and Consumers Bill introduced to Parliament.

rechtlichen Modell prüfen kann, ob Verbraucherschutzvorschriften verletzt wurden, und ggf. Strafen verhängen kann;
- Schaffung eines Ex-ante-Regulierungsrahmens, der von der DMU durchgesetzt werden kann;
- Einführung neuer Schwellenwerte für die Kontrolle von Unternehmenszusammenschlüssen;
- Erweiterung der Untersuchungs- und Rechtsdurchsetzungsbefugnisse der CMA im Wettbewerbsrecht, inklusive eines umsatzbasierten Bußgeldrahmens.

Der Ex-ante-Regulierungsrahmen sieht dabei vor, dass die DMU als Untergliederung der CMA Unternehmen einen strategischen Marktstatus (Strategic Market Status, SMS) zuweisen kann, wenn sie bestimmte Voraussetzungen erfüllen. Solche SMS-Unternehmen müssen den Verhaltensnormen entsprechen, die das Gesetz für diese besondere Kategorie aufstellt, und können Adressaten proaktiver wettbewerbsfördernder Maßnahmen der DMU (sog. Pro-Competitive Interventions) sein. Sie unterliegen einer Meldepflicht für Fusionen unterhalb der Fusionskontrollschwellenwerte, die eine aufschiebende Wirkung hinsichtlich der Durchführung der Fusion entfaltet. Mit Ausnahme der Regelung zur Zusammenschlusskontrolle bestehen sehr viele Parallelen zum DMA.[944] Der britische Gesetzesentwurf ist aber deutlich umfangreicher und teils konkreter in seinen Regeln.

Um in Bezug auf eine digitale Tätigkeit als SMS-Unternehmen eingestuft zu werden, muss ein Unternehmen über eine „beträchtliche und gefestigte" („substantial and entrenched") Marktmacht verfügen, eine strategisch wichtige Position innehaben und entweder einen weltweiten Umsatz von 25 Milliarden Pfund oder einen Umsatz von 1 Milliarde Pfund im Vereinigten Königreich erzielen. Dem Gesetzesentwurf zufolge muss eine „beträchtliche und gefestigte" Marktmacht durch eine „vorausschauende Bewertung über einen Zeitraum von mindestens 5 Jahren" ermittelt werden. Innerhalb des Gesetzesentwurfs gilt, wie im DMA, das Marktortprinzip. Verlangt wird eine wesentliche Verbindung der Tätigkeit des fraglichen Unternehmens zum Hoheitsgebiet des Vereinigten Königreichs. Ein wichtiger Unterschied zum DMA besteht darin, dass der britische Entwurf sich nicht auf bestimmte zentrale Plattformdienste beschränkt und auch nicht bestimmte Pflichten an bestimmte Dienste richtet. Vielmehr sind allgemeiner „digitale

944 Eingehend dazu *Andriychuk*, Analysing UK Digital Markets, Competition and Consumers Bill through The Prism of EU Digital Markets Act.

Aktivitäten" erfasst, was der CMA bzw. DMU wesentlich flexiblere Ansätze und praktische Bewertungen ermöglicht.

Die DMU kann SMS-Unternehmen Verhaltensweisen auferlegen, soweit diese erforderlich sind, um die im Gesetzesentwurf festgelegten Ziele zu erreichen: faire Behandlung von Nutzern, freie Wahlmöglichkeiten von Nutzern sowie Vertrauen und Transparenz gegenüber Nutzern. Solche Verhaltensaufforderungen können Änderungen der Geschäftsbedingungen, die Einführung von Beschwerdemechanismen, Informationspflichten sowie das Verbot von Selbstpräferenzierung, Diskriminierung, Angebotsbündelung, missbräuchlicher Datennutzung oder Nutzungsbeschränkungen bedeuten. Zu den Fällen, in denen die DMU Verhaltensaufforderungen gegenüber SMS-Unternehmen beschließen kann, gehört es explizit, wenn ein SMS-Unternehmen „die Interoperabilität zwischen dem relevanten Dienst oder digitalen Inhalten and Produkten einschränkt, die von anderen Unternehmen angeboten werden" (Kapitel 3, Sektion 20 Abs. 3 lit. (e) des Entwurfs). Überdies besteht eine Befugnis des Secretary of State als zuständigem Minister, die in diesem Abschnitt aufgelisteten verbotenen Verhaltensweisen, die mit Verhaltensaufforderungen der DMU adressiert werden können, im Verordnungswege zu erweitern. Daneben kann die DMU auch proaktiv wettbewerbsfördernde Maßnahmen ergreifen, um wettbewerbsschädigenden Entwicklungen entgegenzuwirken. Bemerkenswert ist, dass die Behörde dabei auch in einem relativ breiten Umfang bestimmen kann, wie das SMS-Unternehmen die Umsetzung von Anordnungen konkret auszugestalten hat.

Spezifische Aspekte der Medienvielfaltssicherung werden zwar im Entwurf nicht aufgegriffen. Erwähnenswert sind allerdings die geplanten Änderungen der Fusionskontrolle, die in diesem Zusammenhang relevant werden dürften. Zum einen wird festgelegt, dass die Notifizierungspflicht von Zusammenschlüssen unabhängig von den eigentlichen Schwellenwerten dann greift, wenn ein Unternehmen des Zusammenschlusses ein Medien- oder Presseunternehmen ist. Zum anderen werden auch die Interventionsmöglichkeiten des Secretary of State in sog. „public interest cases" erweitert und teilweise auch auf das wettbewerbsrechtliche Rechtsdurchsetzungssystem ausgedehnt (Erweiterung von Fristen und einstweilige Maßnahmen in solchen Fällen).

(4) Ofcom-Diskussionspapier zur Interoperabilität in digitalen Märkten

Während die zuvor dargestellten Entwicklungen sich maßgeblich auf wettbewerbsrechtliche und verbraucherschutzrechtliche Ziele beziehen, hat auch die Ofcom – die britische Medien- und Kommunikationsregulierungsbehörde – jüngst zu dieser Diskussion beigetragen. In ihrem Diskussionspapier „Mandated interoperability in digital markets" untersucht sie -u. a. mit Blick auf den soeben dargestellten Gesetzesentwurf – Konzepte und Komplexitäten, die sich bei der Anwendung von verpflichtender Interoperabilität als wettbewerbsfördernder Maßnahme ergeben könnten.

Solche Maßnahmen sieht die Ofcom als sinnvoll an, wenn sie die Marktmacht der etablierten Unternehmen oder der Torwächter verringern können und dadurch mehr Wettbewerb und Innovation durch kleinere Unternehmen und potenzielle Neueinsteiger ermöglicht wird oder wenn sie einen Mehrwert für die Nutzer durch größere Vielfalt, höhere Qualität und/oder niedrigere Preise mit sich bringen. Die genannte „Vielfalt" ist in einem verbraucherschutzrechtlichen Sinne gemeint („variety") und nicht im Sinne speziell der Medienvielfalt („plurality" oder „pluralism"). Solche Erwägungen finden sich auch im Ofcom-Diskussionspapier trotz ihrer Eigenschaft auch als Medienregulierungsbehörde nicht. Insgesamt liest sich das Diskussionspapier im Hinblick auf die Vorteile von Interoperabilität deutlich zurückhaltender und mahnt zur Vorsicht und zur besonderen Berücksichtigung der folgenden Bereiche bei wettbewerbsfördernden Maßnahmen zur Interoperabilität:

- Unternehmen, die von den Interoperabilitätsverpflichtungen betroffen sein sollten
- Funktionalitäten oder Daten, die interoperabel gemacht werden sollen
- erforderliches Maß an Offenheit und der damit verbundene technische Ansatz
- Relevanz von Standardsetzungsverfahren
- Bedingungen, unter denen die Interoperabilität Dritten zur Verfügung gestellt werden sollte
- alle mit der Umsetzung verbundenen Governance- und Überwachungsregelungen
- mögliche Auswirkungen der vorgeschriebenen Interoperabilität in Bereichen wie Datenschutz und Sicherheit

b. Frankreich

Während auch in anderen Mitgliedstaaten ähnliche Initiativen zu beobachten sind, wird nachfolgend am französischen Beispiel kurz dargestellt, wie auf nationaler Ebene von EU-Mitgliedstaaten die Reaktionsmöglichkeiten auf die Schieflagen im digitalen Ökosystem ermittelt werden, wobei Interoperabilität ein möglicher Lösungsansatz ist. Die Initiativen bewegen sich in Frankreich, wie in anderen Staaten und den oben genannten Beispielen ebenfalls, auf wettbewerbsrechtlicher Ebene bzw. basieren auf wettbewerbsrechtlichen Anknüpfungspunkten.

Im November 2019 wurde in Frankreich die Informationsmission zu digitalen Plattformen ins Leben gerufen, in deren Rahmen auch eine Sonderkommission zu Untersuchungszwecken eingesetzt wurde. Diese sollte sich maßgeblich mit den Fragen befassen, ob das bestehende Wettbewerbsrecht die notwendigen Mittel bietet, um große digitale Plattformen wirksam zu regulieren, oder ob andere Instrumente eingeführt werden sollten, um aktuellen Gefährdungen zu begegnen. Ins Auge gefasst wurde dabei ein mögliches Gesetz zur Strukturierung digitaler Plattformen („droit de la régulation des plateformes numériques structurantes"). Am 24. Juni 2020 stellte die Kommission ihren Bericht in der Nationalversammlung vor.[945]

Einer der 21 von der Kommission erarbeiteten Vorschläge (Nr. 12) lautete dabei „Förderung der Umsetzung der Datenportabilität und Interoperabilität von Diensten durch proaktive Maßnahmen der Regulierungsbehörde und die Annahme relevanter technischer Standards mit dem Ziel, die mit der Plattformstrukturierung verbundenen Sperrmechanismen einzuschränken". Festgestellt wurde, dass das Datenportabilitätsrecht aus der DS-GVO noch nicht zur Geltung gekommen, seine Praxiseffektivität äußerst gering und Interoperabilität (auch deshalb) im digitalen Ökosystem nur sehr begrenzt vorhanden sei. Eine solche Interoperabilität würde aber Nutzern die Möglichkeit geben, selbst zu bestimmen, welche Dienste sie nutzen möchten, ohne Gefahr zu laufen, aus den Communitys, mit denen sie kommunizieren möchten, ausgeschlossen zu werden, oder ohne gezwungen zu sein, einem (sozialen) Netzwerk beizutreten, um mit anderen kommunizieren zu können. Positive Effekte hinsichtlich bestehender Netzwerkeffekte sowie eine Förderung des Wettbewerbs könnten sich dann auch positiv

945 Commission des affaires économiques sur les plateformes numérique, 24.6.2020, N°3127, https://www.assemblee-nationale.fr/dyn/15/rapports/cion-eco/l15b3127_rapport-information#_Toc256000002.

auf die Innovation zum Nutzen der Verbraucher auswirken. Vorgeschlagen wurde daher, der für die Aufsicht über die Strukturierung von Plattformen zuständigen Regulierungsbehörde insbesondere die Aufgabe zu erteilen, die Datenportabilität und die Interoperabilität von Plattformen zu fördern, indem sie ggf. Verpflichtungen zur Strukturierung digitaler Plattformen in diesem Bereich festlege.

Nur knapp einen Monat später veröffentlichte der französische Digitalrat (Conseil national du numérique, CNN) eine Fallstudie zur Interoperabilität sozialer Netzwerke, die sich ausschließlich und daher tiefgreifend mit diesem Untersuchungsgegenstand befasst.[946] Der CNN ist eine unabhängige französische Beratungskommission, die Stellungnahmen und Empfehlungen zu allen Fragen abgeben kann, die die Auswirkungen digitaler Technologien auf Wirtschaft und Gesellschaft betreffen. Nach einer umfassenden Untersuchung der Vorteile und Risiken, insbesondere auch rechtlicher Rahmenbedingungen, kommt die Fallstudie zu dem Ergebnis, dass die Einführung von Interoperabilitätspflichten sozialer Netzwerke grundsätzlich zu befürworten sei. Allerdings fordert der CNN eine dem vorangehende umfassende Untersuchung der Auswirkungen der Umsetzung des Rechts auf Datenübertragbarkeit. Derzeit laufende Projekte[947] könnten sich bereits als wirksam erweisen, um jene Ziele zu erreichen, die auch mit Interoperabilität angestrebt werden, und insbesondere direkte Netzwerkeffekte teilweise zu beheben.

Dabei sei eine Abstimmung mit der Industrie unerlässlich. Auch solle eine Interoperabilitätsvorschrift nicht eine Einzelbestimmung, sondern Teil einer umfassenderen Reform der Regulierung digitaler Plattformen sein und lediglich ein mögliches Instrument darstellen, das bspw. nationalen Regulierungsbehörden zur Verfügung stehe. Im Hinblick auf die Ausgestaltung spricht sich der CNN für eine Ex-ante- und asymmetrische Regulierung von systemrelevanten Plattformen aus, die dabei nicht nur wirtschaftliche und wettbewerbsrechtliche Kriterien berücksichtige, sondern auch gesellschaftliche und verbraucherschutzrechtliche Aspekte sowie qualitative Aspekte wie den Besitz wesentlicher Daten oder die Auswirkungen auf das kognitive System der Nutzer und die daraus resultierende Abhängigkeit oder gar Sucht einbeziehe. In technischer Hinsicht wird in der Studie ein Protokoll mit Standards oder APIs vorgeschlagen, das von designierten Re-

946 *CNN*, Concurrence et régulation des plateformes.

947 Damit bezieht sich der CNN auf das von Google angestoßene Data Transfer Project, das bereits oben (C.IV.2.a(3)) erläutert wurde.

gulierungsbehörden[948] ausgearbeitet und vorgeschrieben werden soll. Diese Behörden wären auch für die Überwachung der Umsetzung durch die großen Plattformen zuständig. Angestrebt werden soll keine vollständige, sondern nur eine partielle Interoperabilität, die stufenweise umzusetzen sei (und sich auf Kontakte, Direktnachrichten, Teilen von Inhalten in dieser Reihenfolge erstrecken soll). Als sinnvolle Ebene zur Umsetzung von Interoperabilitätsvorschriften kommt laut CNN nur die EU oder sogar eine internationale Vereinbarung im Rahmen der OECD in Betracht.

c. Australien

Die australische Wettbewerbs- und Verbraucherschutzbehörde Australian Competition & Consumer Commission (ACCC) führt bereits seit 2017 Untersuchungen zu digitalen Plattformen durch.[949] Bis zur Fertigstellung des Abschlussberichts für die derzeit laufenden Untersuchungen von 2020 bis 2025 veröffentlicht die ACCC alle sechs Monate Zwischenberichte, die sich bisher mit (1) Messenger-Diensten, (2) App-Marktplätzen, (3) Browser und Suchmaschinen, (4) dem Online-Versandhandel, (5) der Erforderlichkeit neuer Verbraucherschutz- und Wettbewerbsgesetze für digitale Plattformen, (6) sozialen Netzwerken und (7) Wettbewerbsfragen digitaler Ökosysteme beschäftigt haben.[950] Den Berichten liegen Analysen europäischer und US-amerikanischer Gesetzgebung, aber auch Ergebnisse aus Beteiligungsverfahren zugrunde, in denen Plattformanbieter sowie Vertreter aus Wissenschaft und Zivilgesellschaft jeweils themenbezogene Stellungnahmen abgeben konnten. Darauf aufbauend unterbreitet die australische Wettbewerbsbehörde in ihren Berichten Handlungs- und Regulierungsempfehlungen zum Umgang mit digitalen Plattformen in Australien.

948 In Betracht kommen nach dem CNN nicht nur die Wettbewerbsbehörden, sondern auch die Telekommunikations-, Datenschutz-, Verbraucherschutz- und audiovisuellen Regulierungsbehörden, die aber in jedem Fall eng zusammenarbeiten sollten.

949 Australian Competition & Consumer Commission Digital platform services inquiry 2020–25, Project Overview, https://www.accc.gov.au/inquiries-and-consultations/digital-platform-services-inquiry-2020-25. Bereits 2017–2019 wurde eine entsprechende Untersuchung durchgeführt, siehe Australian Competition & Consumer Commission, Digital platforms inquiry 2017–19, Project Overview, https://www.accc.gov.au/inquiries-and-consultations/finalised-inquiries/digital-platforms-inquiry-2017-19.

950 Die Berichte sind abrufbar unter ACCC Digital platform services inquiry 2020–25, Project Overview, https://www.accc.gov.au/inquiries-and-consultations/digital-platform-services-inquiry-2020-25.

Im sechsten Zwischenbericht zur Erforderlichkeit neuer Verbraucherschutz- und Wettbewerbsgesetze setzt sich die ACCC mit der Möglichkeit zur Meldung von Betrug, gefälschten Bewertungen (bspw. für mobile Apps) sowie wettbewerbsschädlichem Verhalten wie der Bevorzugung eigener Dienste und Produkte und in diesem Zuge auch mit Transparenz, Interoperabilität und Datenportabilität auseinander.[951] Im Ergebnis unterbreitet die ACCC einen Regulierungsvorschlag aus einer Kombination von Gesetzgebung und verpflichtenden Verhaltensregeln[952] (*codes of conduct*) für digitale Plattformen. Die Gesetzgebung soll dabei grundlegende Prinzipien festlegen, die bei der Erarbeitung von Verhaltensregeln zu berücksichtigen seien. Die Prinzipien seien noch zu erarbeiten, sollten aber den Wettbewerb nach dem Leistungsprinzip, informierte und effektive Wahlmöglichkeiten für Verbraucher sowie den fairen Handel und Transparenz für Plattformnutzer berücksichtigen.[953]

Die hiervon abgeleiteten Verhaltensregeln sollen zielgerichtet bei den relevanten Plattformen Anwendung finden. Die Anwendbarkeit dieser Regeln sei deshalb von der Bedeutung einer Plattform für australische Verbraucher und Märkte sowie dem Gefährdungspotenzial der betreffenden Plattformen für einen freien Wettbewerb abhängig zu machen.[954] Die ACCC schlägt einen „*service-by-service approach*" vor, um auf die Besonderheiten verschiedener Plattformtypen wie Suchmaschinen, sozialer Netzwerke, Videoplattformen oder des Online-Werbemarkts eingehen zu können.[955] Auf der Grundlage qualitativer (z. B. Marktmacht oder Betrieb mehrerer digitaler Plattformen) und quantitativer (z. B. Anzahl monatlich aktiver australischer Nutzer) Kriterien könnten digitale Plattformen bestimmt werden, die von den Verpflichtungen erfasst sein sollten.[956] Dieser Ansatz bietet aus regulatorischer Hinsicht Flexibilität und die Möglichkeit, schnell auf Marktveränderungen zu reagieren. Gleichzeitig sollten die einzelnen Verhaltensregeln aufeinander abgestimmt werden, um eine Mehrfachregulierung einzelner Dienste, die mehrere Plattformtypen vereinen, zu vermeiden.

951 Australian Competition & Consumer Commission (ACCC), Digital platform services inquiry, Interim report No. 5 – Regulatory reform, September 2022.

952 Zu Verhaltensregeln (*code of conduct*) im australischen Recht siehe Australian Government, Codes of Conduct, 1.12.2022, https://business.gov.au/legal/fair-trading/codes-of-conduct (29.12.2022).

953 ACCC, Digital platform services inquiry, Interim report No. 5, S. 112 f.

954 ACCC, Digital platform services inquiry, Interim report No. 5, S. 111 ff.

955 ACCC, Digital platform services inquiry, Interim report No. 5, S. 112.

956 ACCC, Digital platform services inquiry, Interim report No. 5, S. 114 ff.

Die ACCC benennt hinsichtlich der zu regulierenden Aspekte folgende Bereiche: die wettbewerbsgefährdende Bevorzugung eigener Produkte (*self-preferencing*), das Koppeln von Produkten und Diensten (*tying*), die Vorinstallation von Produkten, das Behindern des Wechsels von Plattformen und von Interoperabilität, datenbezogene Hürden, eine mangelnde Transparenz und die Benachteiligung von gewerblichen Plattformnutzern.[957] Mit Blick auf Interoperabilität befürchtet die ACCC, dass marktmächtige Plattformen die Interoperabilität mit Produkten und Diensten von Drittanbietern beschränken könnten. Die Behörde sieht im Vorschreiben der Nutzung von Software (etwa der Browser-Engine WebKit von Apple, die auf dem mobilen Betriebssystem iOS von allen Wettbewerbern verpflichtend genutzt werden muss) Risiken für die Interoperabilität und damit den Wettbewerb. Wettbewerbsrechtliche Verhaltensregeln könnten entsprechend von Betreibern mobiler Plattformen (wie Apple und Google) fordern, App-Marktplätze und Apps von Drittanbietern zwingend zu berücksichtigen. So könnten etwa Browser-Engines von Drittanbietern zugelassen werden, oder der Zugang zu Schnittstellen für Hard- und Software wäre zu gewähren, um Drittanbietern die Möglichkeit zur Interoperabilität mit mobilen Plattformen zu ermöglichen. Dabei sollten jedoch die Integrität und Sicherheit einer Plattform sowie der Datenschutz sichergestellt bleiben.[958]

Neben der Interoperabilität wird die Datenportabilität als Reaktion auf einen fehlenden Zugang zu Daten als Hindernis für den Markteintritt und Expansionsmöglichkeiten betrachtet. Wenn Plattformen keinen Zugang zu (Nutzer-)Daten haben, kann dies einen Wettbewerbsnachteil zur Folge haben – entweder als Markteintritts- oder als Wachstumsbarriere. Daher schlägt die ACCC vor, dass Wettbewerber Zugang zu Daten großer Plattformen erhalten sollen (vergleichbar mit Art. 6 Abs. 11 DMA für den Zugang zu Daten großer Suchmaschinen). Die Datenportabilität könne so aussehen, dass Nutzer ihre Daten an sich selbst oder einen Dritten in einem strukturierten, gängigen und maschinenlesbaren Format einmalig oder dauerhaft übermitteln können. Derzeit ist in Australien das Recht auf Datenportabilität auf die Finanzdienstleistungsbranche beschränkt,[959] soll aber sukzessive über die Finanzbranche hinaus ausgeweitet werden.[960]

957 ACCC, Digital platform services inquiry, Interim report No. 5, S. 123.
958 ACCC, Digital platform services inquiry, Interim report No. 5, S. 156 ff.
959 Vgl. *Jevglevskaja/Buckley*, in: EDPL, 2024, S. 74–82.
960 ACCC, Digital platform services inquiry, Interim report No. 5, S. 165 ff.

Die australische Regierung unterstützt prinzipiell die Empfehlungen der ACCC über die Einführung abgestufter Regelungen für digitale Plattformen zum Schutz und zur Förderung des Wettbewerbs.[961] Deshalb wurde im Dezember 2023 das Finanzministerium (Department of Treasury), in dessen Zuständigkeit die Wettbewerbsaufsicht fällt, von der Regierung beauftragt, einen entsprechenden konkreten Vorschlag zu erarbeiten. Dabei sollen sowohl internationale Entwicklungen und Erfahrungen als auch Positionen digitaler Plattformen berücksichtigt werden. Digitalen Plattformen könnten gezielte und dienstespezifische Verpflichtungen und Verbote im Hinblick auf wettbewerbswidriges Verhalten auferlegt werden. Um eine effektive Durchsetzung der geplanten Regulierung zu gewährleisten, soll geprüft werden, ob die Wettbewerbs- und Verbraucherschutzbehörde ACCC gestärkt werden müsse. Dies könnte bspw. durch die Einräumung von Untersuchungsrechten der Behörde gegenüber digitalen Plattformen erreicht werden. Das Finanzministerium plant im Jahr 2024 die Durchführung eines Beteiligungsverfahrens zur Gestaltung eines möglichen Ex-ante-Regulierungsrahmens für den digitalen Wettbewerb.[962]

Interessant sind insbesondere die in Australien im Vergleich zu anderen Staaten sehr umfassenden Regeln zur Datenportabilität, die sich derzeit in der Weiterentwicklung befinden.[963] Das sog. Consumer Data Rights Framework (CDR), das 2019 eingeführt wurde, zielt darauf ab, Verbrauchern eine größere Kontrolle über ihre Daten und auch eine wirtschaftlich sinnvolle Nutzung derselben zu ermöglichen. Sie sollen Unternehmen instruieren können, Daten an andere Unternehmen zu übertragen. Momentan gilt das CDR-Framework nur in den ausgewählten Sektoren Banken und Energie, es soll aber schrittweise erweitert werden und sich konkret zunächst auf den Sektor Telekommunikation und letztlich auf alle Wirtschaftsbereiche erstrecken. Ausgangspunkt ist der Treasury Laws (Consumer Data Right) Act 2019[964], der zu zahlreichen Änderungen in anderen Gesetzen, insbesondere dem Competition and Consumer Act 2010[965], geführt hat. Dieser legt

961 Australian Government, Government's response to the ACCC Digital Platform Service's Inquiry, 8.12.2023, https://treasury.gov.au/publication/p2023-474029.

962 Assistant Treasurer Stephen Jones, Government's response to the ACCC's major competition and consumer recommendations for digital platforms, Pressemitteilung v. 8.12.2023, https://ministers.treasury.gov.au/ministers/stephen-jones-2022/media-releases/governments-response-acccs-major-competition-and.

963 Vgl. hierzu und zum folgenden eingehend *Jevglevskaja/Buckley*, in: EDPL, 2024.

964 Act No. 63, 2019, https://www.legislation.gov.au/C2019A00063/latest/text.

965 Act No. 51, 1974, https://www.legislation.gov.au/C2004A00109/2022-07-01/text.

Ziele und Grundsätze der Regelung, Prinzipien zum Schutz der Privatsphäre sowie Ausnahmen vom allgemeinen Datenschutzrecht fest. Zudem wird darin die Aufgabe der mit der Durchsetzung betrauten Regulierungsbehörden (neben der Wettbewerbsbehörde auch weitere Einrichtungen wie etwa die Datenschutzbehörde und eine zentrale unabhängige Beratungseinrichtung der Regierung) festgelegt.

Zu den von der Regelung erfassten Akteuren in Zusammenhang mit den relevanten Daten gehören „Dateninhaber" (Unternehmen, die über die in einem Benennungsinstrument spezifizierten Daten verfügen), „akkreditierte Personen" (von der Wettbewerbsbehörde zum Empfang von CDR-Daten ermächtigte Stellen) und „akkreditierte Datenempfänger" (Unternehmen, die CDR-Daten empfangen können). Die Regelung schützt „CDR-Verbraucher", bei denen es sich um natürliche und juristische Personen (einschließlich kleiner, mittlerer und großer Unternehmen) handeln kann und die sich aus den sektoralen Umständen ergeben. Im Bankensektor gehören bspw. zu den CDR-Dateninhabern zugelassene Banken, und die „CDR-Daten" umfassen verschiedene Arten von Verbraucherdaten, Kontodaten und Transaktionsdaten zu verschiedenen „Produkten" (von Debit- und Kreditkartenkonten über Hypotheken- und Privatkreditkonten bis hin zu Geschäftsfinanzierungskonten einschließlich der damit zusammenhängenden Überziehungskredite und Kreditlinien).

Bemerkenswert sind die technischen und organisatorischen Grundlagen für die Datenportabilität, die das CDR-Framework sehr differenziert und damit anders als Art. 20 DS-GVO festlegt. Standardisierungen, Akkreditierungsverfahren und die Einholung von Einwilligungen sind einbezogen, die einerseits zur Datenschutzkonformität und andererseits zur Gewährleistung der Sicherheit der Datentransfers beitragen. Die Entwicklung und Einhaltung von Standards ist für die Verarbeitung von CDR-Daten und deren Formate, für Übertragungsformate, Sicherheitskonzepte, die Einholung von Einwilligungen und deren Widerruf vorgesehen. Standards werden dabei in Kooperation von einer hierfür eingerichteten Institution (dem Data Standards Chair) und der Wettbewerbsbehörde unter Beteiligung der Industrie entwickelt und verbindlich vorgegeben.

Das Akkreditierungsverfahren, das ebenfalls von der Wettbewerbsbehörde durchgeführt wird, stellt sicher, dass Unternehmen, die Daten von Dateninhabern auf Veranlassung von Verbrauchern empfangen dürfen, bestimmte Vorgaben einhalten. Diese Vorgaben beziehen sich auf Sicherheitskonzepte und spezielle Regeln zur (Weiter-)Verarbeitung von Daten. Einwilligungen, zu deren Einholung die beteiligten Dateninhaber und

-empfänger verpflichtet sind, sind schließlich die Voraussetzung dafür, dass Daten unter dem CDR-Framework weitergeleitet werden dürfen. Dieser organisatorische Rahmen macht die Regeln zur Datenportabilität in der Praxis deutlich erfolgversprechender als das Gegenstück in der DS-GVO, ist aber demgegenüber auch mit einem deutlich höheren Aufwand für beteiligte Unternehmen verbunden.

d. China

(1) Interoperabilität

Im Jahr 2019 unternahm der Staatsrat der Volksrepublik China erste Schritte hin zu einer Interoperabilität für digitale Plattformen und gab sog. „Guiding Opinions on Promoting the Regulated and Healthy Development of the Platform Economy" heraus. In diesen wies er chinesische Behörden an, das Recht der Verbraucher auf Wahlfreiheit und Interoperabilität zu respektieren.[966] Seitdem werden digitale Plattformen in China intensiver reguliert. So wurde im Jahr 2022 eine Änderung des Antimonopolgesetzes beschlossen.[967] Das Monopolgesetz ist in acht Teile gegliedert: Ziele des Gesetzes und grundsätzliche Regelungen (Kapitel I), Regelungen zu Monopolvereinbarungen (Kapitel II), Regelungen zum Missbrauch einer marktbeherrschenden Stellung (Kapitel III), Regelungen zu Zusammenschlüssen (Kapitel IV), Regelungen zum Missbrauch von Machtpositionen zur Ausschaltung oder Einschränkung des Wettbewerbs (Kapitel V), Ermittlungsbefugnisse bei Verdacht auf ein Monopol (Kapitel VI), Strafen (Kapitel VII) und Schlussbestimmungen (Kapitel VIII). Mit der Änderung im Jahr 2022 ist es Betreibern digitaler Plattformen verboten, Algorithmen, Technologien oder auch Plattformregeln anzuwenden, die nach dem Antimonopolgesetz verbotene Handlungen darstellen:[968]

966 *Fei*, CLSR, 48, 2023, S. 6; Staatsrat der Volksrepublik China, Guiding Opinions on Promoting the Regulated and Healthy Development of the Platform Economy v. 8.1.2019, mit inoffizieller englischer Übersetzung, https://lawinfochina.com/display.aspx?id=30987&lib=law.

967 Anti Monopoly Law of China, zuletzt geändert am 22.6.2022, mit inoffizieller englischer Übersetzung, https://www.chinalawtranslate.com/en/anti-monopoly-law-2022/.

968 Art. 9 Antimonopolgesetz.

Artikel 9[969]
Unternehmen dürfen keine Daten oder Algorithmen, Technologien, Kapitalvorteile oder Plattformregeln usw. verwenden, um nach diesem Gesetz verbotene monopolistische Praktiken auszuüben.

Zu den verbotenen Handlungen gehören das wettbewerbsgefährdende Ausnutzen von Marktmacht, das Festsetzen von Preisen oder das Aufteilen von Märkten (Art. 7, 17, 18 Antimonopolgesetz). Verstöße können zu Strafen von mindestens 1 % und maximal 10 % des Vorjahresumsatzes führen (Art. 56 ff. Antimonopolgesetz). Die chinesische Wettbewerbsbehörde State Administration for Market Regulation (SAMR) veröffentlichte darüber hinaus bereits 2021 einen Entwurf zur Klassifizierung digitaler Plattformen mit dem Ziel, den Wettbewerb und die Verbraucherinteressen zu schützen und gleichzeitig Innovationen zu fördern.[970] In dem Entwurf werden sog. „super platforms" definiert als Plattformen, die mehr als 500 Millionen aktive chinesische Nutzer im Vorjahr aufwiesen, mehrere Plattformen betreiben, eine hohe Marktkapitalisierung aufweisen und die Möglichkeit haben, Beziehungen von Händlern mit Verbrauchern zu beschränken.[971] Nach einem weiteren Entwurf der SAMR zu Verpflichtungen digitaler Plattformen sollen diese „super platforms" Interoperabilität mit anderen Plattformbetreibern gewährleisten, soweit Sicherheit, Rechte und Interessen der Nutzer gewahrt werden.[972] Abgesehen von der Herstellung von Interoperabilität in Wettbewerbsverfahren oder auf Anweisung von sektorspezifischen Regulierungsbehörden gibt es für digitale Plattformen in China keine rechtliche Verpflichtung zur Herstellung von Interoperabilität.[973]

Die Regulierung in China ist eine Antwort auf Praktiken großer in China aktiver Plattformen. Zum einen hatten diese über einen längeren Zeitraum ein sog. *link blocking* betrieben, wonach Nutzer einer Plattform keine Links dieser Plattform zu einer anderen Plattform posten konnten

969 Eigene Übersetzung d. Verf. auf der Grundlage der nicht amtlichen englischen Übersetzung, https://lawinfochina.com/display.aspx?id=30987&lib=law.
970 *Chinese State Administration for Market Regulation (SAMR)*, Guidelines for Internet Platform Categorization and Grading (Draft for Comment) v. 29.10.2021, mit nicht amtlicher englischer Übersetzung v. 28.2.2022, https://digichina.stanford.edu/work/translation-guidelines-for-internet-platform-categorization-and-grading-draft-for-comment-oct-2021/.
971 Art. 3.2 SAMR Guidelines for Internet Platform Categorization and Grading (Draft for Comment).
972 *Fei*, CLSR, 48, 2023, S. 6.
973 *Fei*, CLSR, 48, 2023, S. 6.

bzw. diese Links nicht angezeigt wurden. Ein Beispiel für diese Praktik war die Unmöglichkeit für Verbraucher, Videos der Plattform Douyin, die von ByteDance betrieben wird,[974] auf der Plattform WeChat von Tencent zu teilen und umgekehrt.[975] Darüber hinaus konnte auf Plattformen von Alibaba nicht mit Tencent's WeChat Pay gezahlt werden, sondern nur mit dem eigenen Zahlungsdienst Alipay.[976] Im Jahr 2021 entschied das chinesische Ministerium für Industrie und Informationstechnik in einem informellen Verfahren mit den größten Plattformanbietern[977] Tencent, Alibaba und ByteDance, dass diese untereinander und mit Dritten Interoperabilität in Form eines technischen Zugangs zu ihren Plattformen herstellen müssen.[978] Darüber hinaus wurden die Plattformen verpflichtet, neben dem eigenen auch Zahlungsdienstleister von Dritten durch die Möglichkeit zur Zahlung mit QR-Codes zu akzeptieren.[979]

Details zu diesem hinter verschlossenen Türen geführten Verfahren sind nicht bekannt. Dieses intransparente Verfahren ist unabhängig von kurzfristigen Effekten und rechtsstaatlichen Erwägungen problematisch, da es das Risiko der selektiven und möglicherweise nur zeitlich begrenzten Durchsetzung mit sich bringt.[980] Darüber hinaus wird insbesondere der Mehrwert des Verbots des *link blocking* für Nutzer hinterfragt, da Nutzer zum Öffnen von Links ohne weiteres verschiedene Apps installieren und nutzen konnten.[981] Zwar überzeugt dieses Argument mit Blick auf das Gegenrechnen von Opportunitätskosten für Nutzer und Umsetzungskosten für Plattformen, allerdings verkennt diese Sicht, dass *link blocking* möglicherweise ein Symptom des selektiven Abschottens von Plattformschnittstellen gegenüber einzelnen Wettbewerbern darstellt und damit den Wettbewerb als solches gefährden könnte.[982] Mit Blick auf die exklusive Nutzung und Bevorzugung des plattformeigenen Zahlungsdienstes überzeugt auch das Argument nicht, dass geschlossene Zahlungssysteme die Profitabilität und damit die Innovationsfähigkeit digitaler Plattformen för-

974 Außerhalb Chinas wird die Plattform Douyin unter dem Namen TikTok betrieben.
975 *Fei*, CLSR, 48, 2023, S. 5.
976 *Fei*, CLSR, 48, 2023, S. 5.
977 *Huaxia*, in: Xinhuanet v. 26.7.2021.
978 *Riordan/Olcott/McMorrow*, in: Financial Times v. 13.9.2021.
979 *Fei*, in: CLSR, 48, 2023, S. 7 f.
980 *Yan/Feng*, in: CLSR, 50, 2023, S. 14.
981 *Fei*, in: CLSR, 48, 2023, S. 9.
982 *Yan/Feng*, in: CLSR, 50, 2023, S. 14.

dern.[983] Hinsichtlich der Interoperabilität von Zahlungssystemen zeigt der Blick nach China auch, dass die Verpflichtung zu technischen Standards wie der Zahlung mit QR-Codes eine kleinere Herausforderung darstellt, als kommerzielle Interessen verschiedener Plattformanbieter in Einklang zu bringen.[984] Dabei muss jedoch einschränkend berücksichtigt werden, dass Zahlungsstandards in einem bereits stark regulierten Bankenbereich möglicherweise einfacher durchsetzbar sind als in bisher weniger intensiv regulierten Bereichen wie sozialen Netzwerken.

So viele Vorteile und Komfort solche Super-Apps[985] auch für Nutzer bieten, insbesondere indem sie ihnen eine zentralisierte Verwaltung ihres gesamten „digitalen Lebens" gestatten, so lösen sie doch umgekehrt starke Bedenken aus.[986] Das gilt zum einen für die Abhängigkeitsverhältnisse der Nutzer und, damit verbunden, auch für die Einwirkungsmöglichkeiten der Plattformbetreiber auf und ihre Einsicht in deren „digitales Leben". Zum anderen betrifft es den Wettbewerb, indem Mitbewerbern der Marktzutritt erheblich erschwert, wenn nicht sogar unmöglich gemacht wird und geschäftliche Nutzer (insbesondere Anbieter von Drittanwendungen) vom Zugang zu einer Super-App und von deren Bedingungen abhängig sind. Die Situation in China ist nicht unmittelbar auf die EU übertragbar, da sich dort Marktgegebenheiten auch in ein völlig anderes Regulierungs- und Marktumfeld einbetten, in dem es nur wenige alternative Plattformen gibt.[987] Bedenken zu entsprechenden Entwicklungen existieren allerdings auch für westliche Staaten.[988] Die Rolle von Interoperabilität in diesem Kontext ist ebenfalls noch nicht eindeutig bestimmt: Teilweise wird sie als Ursache bzw. begünstigende Bedingung für das Entstehen von Super-Apps bewertet, teilweise aber auch als Lösung für genau jene Probleme gesehen, die aus Super-Apps resultieren.[989]

983 *Fei*, in: CLSR, 48, 2023, S. 9.
984 *Fei*, in: CLSR, 48, 2023, S. 10.
985 Zur Begriffserklärung und zu den Strategien solcher Anwendungen etwa *Hasselwander*, in: Heliyon, 2024, e25856.
986 Vgl. dazu und zum Folgenden *Yang*, in: MIT Technology Review v. 18.10.2022; *Ofcom*, What super-apps could mean for the communications sector, m. w. N.
987 Messenger-Dienste wie WhatsApp oder Telegram sind genau wie ausländische soziale Netzwerke in China geblockt, E-Mail- und SMS-Kommunikation wird kaum verwendet.
988 Zu entsprechenden Bedenken etwa in Bezug auf X (ehemals Twitter) wegen Aussagen von Elon Musk vgl. Schumpeter, in: The Economist v. 8.12.202.
989 Zur Diskussion etwa Ofcom, Mandated interoperability in digital markets, vgl. dazu C.VI.2.a(4).

(2) Datenportabilität

Chinas Gesetz zum Schutz persönlicher Daten (auch Personal Information Protection Law, PIPL)[990] enthält im Rahmen der Gewährleistung von Betroffenenrechten ein eingeschränktes Recht auf Datenübermittlung (Art. 45 PIPL), das als ein Recht auf Datenportabilität verstanden werden kann:

> *Artikel 45*[991]
> *[…] Beantragt eine Person die Übermittlung ihrer personenbezogenen Daten an einen designierten Datenverarbeiter, der die Anforderungen der nationalen Cyberspace-Behörde für die Übermittlung personenbezogener Daten erfüllt, so stellt dieser Datenverarbeiter die Mittel für die Übermittlung bereit.*

Personen können einen Verantwortlichen anweisen, ihre personenbezogenen Daten an einen anderen Verantwortlichen zu übermitteln. Die betroffenen Daten oder das Format der Datenübermittlung werden nicht näher spezifiziert.

Daneben hat die chinesische Wettbewerbsbehörde SAMR nicht bindende Richtlinien zum Umgang mit personenbezogenen Daten erlassen, die ein Recht auf Datenportabilität enthalten.[992] Die Behörde empfiehlt, dass Betroffenen die Möglichkeit zum Abruf personenbezogener Daten zur Verfügung gestellt werden soll bzw., soweit technisch möglich, personenbezogene Daten an einen von der betroffenen Person bestimmten Dritten zu übermitteln sind:[993]

> *8.6 Erlangung einer Kopie von persönlichen Informationen (PI)*[994]
> *Auf Anfrage einer betroffenen Person soll der Verantwortliche der Person eine Möglichkeit zur Verfügung stellen, um eine Kopie der folgenden PI zu*

990 Personal Information Protection Law of the People's Republic of China v. 20.8.2021 mit offizieller englischer Übersetzung v. 29.12.2021, http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm.

991 Eigene Übersetzung d. Verf. auf der Grundlage der offiziellen englischen Übersetzung v. 29.12.2021, http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm.

992 *SAMR*, Information security technology- Personal information (PI) security specification, GB/T 35273—2020 v. 6.3.2020, mit offizieller englischer Übersetzung, https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf.

993 *SAMR*, Information security technology – Personal information (PI) security specification, S. 14.

994 Eigene Übersetzung d. Verf. auf der Grundlage der offiziellen englischen Übersetzung v. 6.3.2020, https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf.

erhalten, oder, sofern technisch machbar, eine Kopie der folgenden PI an einen von der betroffenen Person benannten Dritten übermitteln:

a) *grundlegende PI und Identitätsinformationen;*
b) *persönliche gesundheitliche und physiologische Informationen sowie Informationen über Ausbildung und Beruf.*

Die Daten sind dabei auf sog. grundlegende personenbezogene Daten (darunter werden Name, Geburtsdatum, Geschlecht, ethnische Gruppe, familiäre Beziehungen, Anschrift und Kontaktdaten verstanden) sowie Gesundheitsdaten, Angaben zur Bildung und zum Lebenslauf beschränkt.[995] Die Inanspruchnahme des Rechts soll für Betroffene kostenfrei sein. Gleichwohl sind zahlreiche Ausnahmen von der Datenportabilität vorgesehen, etwa für Daten, die für die Erfüllung gesetzlicher Verpflichtungen oder zu Zwecken der nationalen Sicherheit verarbeitet werden.[996]

3. Diskussionen und Initiativen in Deutschland

Nach dem Blick auf Initiativen und regulatorische Lösungen in ausgewählten Staaten werden in diesem Kapitel abschließend wichtige Diskussionsbeiträge und Untersuchungen relevanter Behörden in Deutschland dargestellt. Insbesondere für Messenger-Dienste sind verschiedene Untersuchungen veranlasst worden.

a. Bundeskartellamt: Sektoruntersuchung Messenger- und Video-Dienste

Die im vorliegenden Zusammenhang besonders relevante Initiative kommt aus dem BKartA, das im November 2020 eine umfassende Sektoruntersuchung nach § 32e Abs. 5 GWB im Wirtschaftszweig Messenger- und Video-Dienste mit einer verbraucherrechtlichen Perspektive einleitete.[997] In der Untersuchung befasst sich das BKartA mit der Struktur der Branche,

995 *SAMR*, Information security technology – Personal information (PI) security specification, S. 25 f.
996 *SAMR*, Information security technology – Personal information (PI) security specification, S. 14 f.
997 Vgl. die Pressemitteilung des *BKartA* vom 12.11.2020, https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2020/12_11_2020_SU_Messenger_Dienste.html?nn=3591568.

mit Fragen der Datensicherheit und des Datenschutzes sowie möglichen Verbraucherrechtsverstößen in diesem Zusammenhang, aber auch mit dem Thema Interoperabilität. 44 verschiedene Dienste wurden zu diesen Themen befragt und eine Reihe von Expertengesprächen wurde geführt. Eine Zusammenarbeit fand außerdem sektorübergreifend mit verschiedenen Einrichtungen statt, darunter das Bundesamt für Sicherheit in der Informationstechnik, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, die Bundesnetzagentur, die Stiftung Warentest sowie die Verbraucherzentrale Nordrhein-Westfalen.

In einem Zwischenbericht von 2021 stellte das BKartA die vorläufigen Ergebnisse vor, enthalten war darin ein „Branchenüberblick und Stimmungsbild Interoperabilität".[998] Im Mai 2023 wurde sodann der deutlich umfangreichere Abschlussbericht veröffentlicht, der auf den Ergebnissen des Zwischenberichts aufbaut.[999] Neben der Interoperabilität war Leitthema, wie der Datenschutz als Wettbewerbsparameter innerhalb und außerhalb interoperabler Dienste vorangebracht werden kann. Vor der Darstellung der Ergebnisse ist anzumerken, dass mit der vor dem Hintergrund von Verbraucherinteressen sicherlich sinnvollen Erstreckung der Untersuchung auf Messenger- und Video-Dienste[1000] zwei in Technik und Nutzungsart unterschiedliche Systeme untersucht wurden. Die für Messenger-Systeme verwendete Technologie ist insbesondere deutlich älter und homogener als bspw. jene für Videokonferenzsysteme. Das führt dazu, dass die Ergebnisse und Stellungnahmen differenziert je nach Marktsegment betrachtet werden sollten.[1001]

In seinem Abschlussbericht kommt das BKartA in Bezug auf den Markt für Messenger- und Videodienste (im Folgenden: MVD) zunächst zu dem

998 *BKartA*, Zwischenbericht Sektoruntersuchung Messenger- und Video-Dienste.

999 *BKartA*, Abschlussbericht Sektoruntersuchung Messenger- und Video-Dienste.

1000 Die Begriffe wurden innerhalb der Untersuchung weit verstanden und beschränkten sich insbesondere nicht nur auf Textangebote. Der Begriff „Messenger-Dienst" ist danach ein Sammelbegriff für offene und geschlossene Messaging-Systeme, Messenger-Clients und Multi-Messenger, die Messaging-Funktionen und/oder Videotelefonie (einzeln und/oder in Gruppen, wie z. B. bei Videokonferenzen, Online-Meetings, Webinaren u. Ä.) anbieten. Gleiches gilt für die Bezeichnung Video-Dienst, unter der alle Systeme und Anwendungen von Videotelefonie (einzeln und/oder Gruppen, wie z. B. bei Videokonferenzen, Online-Meetings, Webinaren u. Ä.) und ggf. Messaging-Funktionen (einzeln und/oder in Gruppen) erfasst werden. Siehe *BKartA*, Zwischenbericht Sektoruntersuchung Messenger- und Video-Dienste, S. 7.

1001 *Brown*, Private Messaging Interoperability in the EU DMA, S. 25, hebt sogar hervor, dass dadurch der Wert der Ergebnisse geschmälert ist.

Ergebnis, dass dieser vielfältig in Bezug auf Akteure und Geschäftsmodelle sei. Es handle sich um eine weltweit agierende Branche, die nicht nur auf Seiten der größeren Teilnehmenden technologische und digitale Entwicklungen und Innovationen hervorbringe. Vielmehr zeichneten sich auch konkurrierende Dienste durch innovative Geschäftsmodelle und Spezialisierungen auf der Basis besonderer Services und Funktionen aus. Es gebe viele Geschäftsmodelle und Anwendungen, die sowohl Messaging, Videoconferencing, teilweise auch Social-Media-Funktionen oder Features für die Kommunikation und Zusammenarbeit verbinden. Manche Messenger-Dienste profitierten dabei von einer großen Nutzerbasis über Netzwerkeffekte, andere wiederum seien ohnehin interoperabel, sodass die Zahl der Nutzer des jeweiligen Dienstes für dessen Attraktivität für sich genommen von geringerer Bedeutung sei. Unterschiedlich sei auch die Bepreisung der Leistungen, von unentgeltlichen Diensten über solche, die sich über Entgelte für Basis- oder Zusatzleistungen oder Werbesysteme finanzieren, bis hin zu kostenpflichten Diensten bspw. mit Abo-Modellen.

Mit dem Thema Interoperabilität befasst sich der Bericht bei der Frage, ob Interoperabilität (und Datenportabilität) zu mehr Datenschutz innerhalb von MVD führt. Ein wesentlicher Punkt der Untersuchung sind daher Ansätze für mehr Datenschutz in einem wettbewerblichen Kontext. Zur Interoperabilität stellt der Bericht bestehende Rechtsgrundlagen aus dem europäischen und nationalen Wettbewerbs- und Telekommunikationsrecht dar. Im Anschluss werden neue Möglichkeiten untersucht, die teilweise noch während der Untersuchung durch den DMA bereits Rechtswirklichkeit geworden sind. Interessant ist insbesondere die ausführliche Befragung der Branche zu den Vor- und Nachteilen von Interoperabilität,[1002] die zu dem Ergebnis kommt, dass die Auferlegung eines möglichen vollständigen Standardisierungsprozesses im Zuge eines verpflichtenden Interoperabilitätsvorhabens vom Großteil der Messenger- und Video-Dienste kritisch gesehen wird. Mögliche positive Effekte würden nach dem Großteil der geäußerten Ansichten von negativen Effekten überlagert. Aufschlussreich ist, wen die befragten Branchenmitglieder für geeignet halten, zu einem möglichen Standardisierungsprozess beizutragen: Die meisten Antworten (60 %) votierten für die Internet Engineering Task Force, also eine global agierende, unabhängige, offene und freie Vereinigung, die über entsprechende Erfahrungen verfügt. Dies wurde damit begründet, dass sich regionale Alleingänge nicht würden durchsetzen können. Als andere Möglichkeiten

1002 Dazu ausführlich unten D.V.2.

wurden die Europäische Kommission und eine Selbstregulierung durch die Branche genannt.

Der Bericht endet mit Empfehlungen zur Stärkung der Durchsetzung von Verbraucherrechten, für eine kontinuierliche Aufklärung der Verbraucher und zu besseren Bedingungen für datenschutzfreundliche Dienste. Im Hinblick auf Interoperabilität spricht sich die Untersuchung für innovationsfreundliche und verbraucherorientierte Lösungen aus. Dabei seien bei jeglichen Vorhaben zur Umsetzung und Gestaltung von Interoperabilität die Auswirkungen auf Innovation und Wettbewerb zu beachten, beispielsweise wenn dazu notwendige Standardisierungen auf unterschiedliche technische Gestaltungen der Dienste treffen. Das betont das BKartA im Übrigen auch im Kontext der anstehenden Implementierung der Vorschriften des DMA. Insoweit wird auch die Umsetzung einer über die Basisinteroperabilität (wie im DMA) hinausgehenden Interoperabilität als schwierig betrachtet, weil die Dienste in Bezug auf Zusatzfunktionen sehr asymmetrisch ausgestaltet sind. Vereinheitlichungen und Anpassungen könnten auch die Innovationskräfte der Dienste unterschiedlich beeinträchtigen.

Aus Perspektive der Verbraucher warnt das BKartA zudem vor einer Verkomplizierung des Informationsflusses vor allem durch den Datenschutz, wenn Interoperabilität hergestellt wird. Hierzu heißt es: „Der mit Interoperabilität verbundene Wunsch, Netzwerkeffekte zu entkräften und datenschutzfreundlichen Diensten bessere Chancen im Wettbewerb zu ermöglichen, indem die Verbraucherinnen und Verbraucher wechseln, könnte so konterkariert werden". Im Übrigen sei dabei auch bei jeglichen Vorhaben zur Umsetzung und Gestaltung von Interoperabilität die Sicherheit und der Schutz der personenbezogenen Daten im Blick zu behalten. Dazu gehöre, dass ein entsprechendes Regelungswerk vorsehe, bereits aktivierte Sicherheitskriterien beim Messenger-übergreifenden Austausch zu erhalten und Daten nur sparsam zu nutzen. Das BKartA hebt in diesem Zusammenhang die Frage des Serverstandorts (wegen möglicher Datenübertragungen in Staaten außerhalb der EU), die Art des Geschäftsmodells (Datenweitergabe innerhalb von Konzernen und die Erkennbarkeit dieser Transfers für die Nutzer) und den Umgang mit Kontakten (Nutzer tragen Verantwortung auch für die Daten von Dritten) hervor.

Aufgrund der vielgestaltigen Herausforderungen im Bereich der Messenger- und Video-Dienste – informationstechnologisch, verbraucher- und datenschutzrechtlich sowie ökonomisch – sei eine Zusammenarbeit verschiedener Wissensträger bei solchen Interoperabilitätsvorhaben sinnvoll, insbesondere sei auch die Branche einzubeziehen. Da die Branche in tech-

nischer und kommerzieller Hinsicht vielfältig aufgestellt sei, sollten zudem Regeln zur technischen Umsetzung diskriminierungsfrei sein, solange der Stand der Technik von den die Vorgabe Umsetzenden gewährleistet werde.

b. Gutachten der Monopolkommission

Die Monopolkommission ist ein unabhängiges Beratungsgremium, das die Bundesregierung und die gesetzgebenden Körperschaften auf den Gebieten der Wettbewerbspolitik, des Wettbewerbsrechts und der Regulierung berät. Nach § 195 Abs. 2 und 3 TKG erstellt sie alle zwei Jahre ein Gutachten zum Stand und zur absehbaren Entwicklung des Wettbewerbs auf den Telekommunikationsmärkten in Deutschland. Darin evaluiert sie auch die Nachhaltigkeit wettbewerbsorientierter Telekommunikationsmärkte, würdigt die Anwendung der Vorschriften des TKG über die Regulierung und die Wettbewerbsaufsicht und nimmt zu sonstigen aktuellen wettbewerbspolitischen Fragen Stellung.

Das Gutachten von 2021 befasste sich auch mit der Interoperabilität von nummernunabhängigen interpersonellen Kommunikationsdiensten wie WhatsApp, Threema, Signal, Wire und Co.[1003] Darin werden die aktuellen rechtlichen Rahmenbedingungen sowie die Marktlage im Telekommunikationssektor unter Berücksichtigung von Verbraucher- und Unternehmensinteressen untersucht. Das Gutachten kommt zu dem recht klar formulierten Ergebnis, dass Interoperabilitätsverpflichtungen, die eine diensteübergreifende Kommunikation ermöglichen würden, für Messenger-Dienste zum Zeitpunkt der Untersuchung abzulehnen seien, weil sie nach Ansicht der Monopolkommission derzeit mehr Nach- als Vorteile für den Wettbewerb verursachen würden. Das Umfeld von nummernunabhängigen interpersonellen Telekommunikationsdiensten sei, wie auch das BKartA in der zuvor genannten Untersuchung hervorhebt, als sehr dynamisch, innovativ und bei den Geschäftsmodellen als ausdifferenziert anzusehen. Nutzer würden Multi-Homing nach ihren Präferenzen betreiben. Bedenken äußert die Monopolkommission dahingehend, ob solche Interoperabilitätspflichten überhaupt technisch (die Dienste nutzen verschiedene Standards, basieren auf verschiedenen Adressierungsschemata etc.) und datenschutzkonform umgesetzt werden können.

1003 *Monopolkommission*, Telekommunikation 2021.

Die ablehnende Haltung der Monopolkommission gilt jedenfalls für symmetrische Interoperabilitätspflichten für alle Anbieter, da sie dort unverhältnismäßig und wettbewerbsschädlich seien, indem sie Anbietern weitgehend die Möglichkeit entzögen, sich gegenüber großen Anbietern durch bessere Funktionen oder höhere Datenschutzstandards abzugrenzen. Im Hinblick auf asymmetrische Interoperabilitätspflichten für marktdominante Akteure ist das Sektorgutachten jedoch im Ergebnis differenzierter: Zwar werden sie zum derzeitigen Zeitpunkt ebenfalls als nicht nötig angesehen, weil keine Situation bestehe, in denen Netzwerkeffekte aufgrund ihrer Intensität ein Einschreiten geböten. Allerdings enthält das Sektorgutachten – sicherlich aufgrund des parallel zur Abfassung des Gutachtens bereits vorangeschrittenen Gesetzgebungsprozesses zum DMA – Ausführungen zu den rechtlichen Grenzen solcher Pflichten, sollte eine entsprechende Situation mit der Notwendigkeit eines Einschreitens eintreten. Neben Zweifeln daran, ob eine Interoperabilität überhaupt zwischen nummernunabhängigen und nummerngebundenen Diensten mit Blick auf die Vorgaben des EKEK angeordnet werden könnte,[1004] sei auch bei der Interoperabilität zwischen Messenger-Diensten eine eingehende rechtliche Bewertung erforderlich, da eine solche Auflage erheblich in Grundrechte und Grundfreiheiten eingreife. Insbesondere wäre darauf zu achten, dass umfassende Nichtdiskriminierungsbedingungen enthalten seien und nicht bestimmte (proprietäre) Standards oder Schnittstellen dazu führten, dass die Stellung eines Dienstes oder einer Gruppe von Diensten gegenüber Dritten begünstigt werde. Konkret sollten also Nichtdiskriminierungsregelungen für APIs bzw. Clearingstellen bestehen. Auch wäre eine Interoperabilität von Grundfunktionen (wie die „Basisfunktionen" im DMA) denkbar, aber eine solche könne nicht auf Zusatzfunktionen ausgedehnt werden, da dann die Möglichkeit von Wettbewerbern für eine Differenzierung und damit die Konkurrenz zwischen den Messenger-Diensten eingeschränkt würden.

Die Monopolkommission empfiehlt, dass die Bundesnetzagentur die weitere Entwicklung nummernunabhängiger ITD – insbesondere hinsichtlich sog. „Super-Apps" – im Auge behält und die bereits begonnenen

1004 Dagegen spricht laut Monopolkommission, dass viele der im EKEK vorgesehenen Verpflichtungen interpersonellen Telekommunikationsdiensten nur deshalb auferlegt werden, da sie am öffentlich gesicherten interoperablen Ökosystem beteiligt sind und somit auch Nutzen daraus ziehen. Das sei aber bei nummernunabhängigen Diensten nicht ohne weiteres der Fall, und eine gleiche Behandlung dieser Dienste sei mit dem Wortlaut des EKEK unvereinbar.

Untersuchungen fortsetzt. Allerdings steht sie auch der Einleitung eines förmlichen Marktregulierungsverfahrens nach den §§ 10 ff. TKG kritisch gegenüber, das alternativ zu den Maßnahmen in § 21 TKG im Wege der allgemeinen Marktregulierung ergriffen und auch mit Interoperabilitätspflichten nach § 26 TKG verbunden werden könnte. Nach Ansicht der Kommission käme ein solches Verfahren verfrüht, da die Auferlegung von Interoperabilitätsverpflichtungen derzeit nicht angezeigt sei. Für die Zukunft könnte die Einleitung eines derartigen Verfahrens jedoch die Möglichkeit bieten, eine Diskussion im EU-Regulierungsverbund über die Auferlegung von Interoperabilitätsverpflichtungen anzustoßen.

c. Bundesnetzagentur: Interoperabilität zwischen Messenger-Diensten

In einer Untersuchung von 2021 unter dem Titel „Interoperabilität zwischen Messenger-Diensten – Überblick der Potenziale und Herausforderungen“[1005] untersuchte auch die BNetzA das Thema Interoperabilität in Bezug auf Messenger-Dienste. Dabei standen drei Leitfragen zum Bedarf nach Interoperabilität, zu den Auswirkungen auf den Wettbewerb sowie zu Datenschutz- bzw. Datensicherheitsaspekten im Vordergrund. Gestützt auf eigene und von Dritten durchgeführte Erhebungen betont die BNetzA in ihrem Bericht, dass der Wunsch der Verbraucher zur Umsetzung von Interoperabilitätsvorschriften im Bereich der Messenger-Dienste wegen vorhandener Möglichkeiten des Multi-Homings überwiegend verhalten ausgeprägt sei. Auch seien entsprechende Forderungen von Seiten kleinerer Konkurrenten bislang nicht bekannt. Was die Auswirkungen auf den Wettbewerb betrifft, hebt auch die BNetzA die Komplexität der Thematik und die damit verbundenen Unsicherheiten in der Prognose von möglichen Folgen einer Interoperabilität hervor. Gerade die Tatsache, dass bei Nutzern tatsächlich ein Multi-Homing stattfinde, deute darauf hin, dass möglicherweise eine Interoperabilität von eher geringer Bedeutung für den Wettbewerb sei.

Im Ergebnis identifizierte die BNetzA zwei wesentliche Herausforderungen bzw. potenzielle Zielkonflikte. So könnten Interoperabilitätsmaßnahmen zwar theoretisch den Wettbewerb intensivieren und die Etablierung alternativer Anbieter fördern, was jedoch einen Konsens über das Funktionieren der Messenger-Dienste (Standardisierung bzgl. der Funktionen, Öffnung von Schnittstellen) erfordere, weshalb mögliche negative Wechsel-

1005 *BNetzA*, Interoperabilität zwischen Messenger-Diensten.

wirkungen auf die Innovationsoffenheit (z. B. dynamische Anpassungen) zu berücksichtigen seien. Ferner könne es vor dem Hintergrund von Datenschutz und Datensicherheit einen Zielkonflikt zwischen der Offenheit eines föderierten Kommunikationsnetzwerks mit möglichst vielen Anbietern und der Gewährleistung eines möglichst hohen Schutzes von (personenbezogenen) Daten geben.

Aus diesem Grund, so die BNetzA in ihrer damaligen Schlussfolgerung, müsse vor einer etwaigen Auferlegung von Interoperabilitätsverpflichtungen in einem ersten Schritt geprüft werden, ob ein relevantes Marktversagen im Bereich der Messenger-Dienste vorliege und ob entsprechende Verpflichtungen als Abhilfemaßnahme grundsätzlich geeignet seien. In jedem Fall sei bei einer etwaigen Umsetzung eine umfassende regulatorische Begleitung unabdingbar, die insbesondere auch die Festlegung von Adressaten und interoperabel auszugestaltenden Funktionen, die technische Definition relevanter Schnittstellen bzw. Standards, Regelungen hinsichtlich des Datenschutzes und der Datensicherheit sowie ergänzende Regelungen zu dynamischen Anpassungen in den Blick nehmen müsse.

d. Zehnter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft"

Mit Beschluss des Deutschen Bundestages vom 4. März 2010 wurde die Enquete-Kommission „Internet und digitale Gesellschaft" eingerichtet, die – neben weiteren Aufgaben – auch für den Bereich Bildung und Forschung die „Weiterentwicklung und Definition offener Standards und Normen [... sowie die] Bedeutung von Open Source, freier Software und Interoperabilität" untersuchen sollte.[1006] Anfang Juni 2012 konstituierte sich die Projektgruppe „Interoperabilität, Standards, Freie Software", die im Zehnten Zwischenbericht zu diesen Themen Stellung nahm.[1007] Dabei wurde nicht ein spezifischer Bereich analysiert, sondern es wurden allgemeine Feststellungen in Bezug auf verschiedene Bereiche der Online-Umgebung getroffen. Spezifisch behandelte Bereiche waren dagegen Fernsehen über das Internet (Internet Protocol Television, IPTV) und e-Government.

1006 *Deutschen Bundestag*, Beschluss vom 4. März 2010, BT-Drs. 17/950.

1007 *Deutscher Bundestag*, Zehnter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft".

Auf der Basis der Untersuchung von Vor- und Nachteilen, Voraussetzungen, möglichen Problemen und Verfahren zur Umsetzung von Interoperabilität sprach die Enquete-Kommission Handlungsempfehlungen aus. Neben allgemeinen Empfehlungen zur Förderung des Themas Interoperabilität und freier Software, insbesondere im Bereich der Verwaltung, wurde in Bezug auf IPTV hervorgehoben, dass ein einheitlicher Standard für Set-Top-Boxen sicherstellen könnte, dass Kunden schneller zwischen den Anbietern wechseln und auch einzelne Prepaid-Angebote verschiedener Anbieter gleichzeitig nutzen könnten. Ein solcher Standardisierungsprozess könne über Normierungsgremien oder die Industrie vorangetrieben werden. Wünschenswert wäre es, wenn ausgehend von der Industrie allgemeinverbindliche Standards geschaffen würden. Zum Teil wurde bemängelt, dass gerade dieser Selbstorganisierungsprozess der Industrie zu ineffizienten Verfahren und technisch suboptimalen Standards führen könne.[1008]

Im Ergebnis lautete die Empfehlung in Bezug auf IPTV daher, zunächst die Schaffung von allgemeinen Standards durch Marktteilnehmer (Anbieter, Nutzer und Netzwerkbetreiber) abzuwarten. Erst bei einem Fehlgehen dieser Bemühungen solle eine freiwillige Vereinbarung der Marktteilnehmer unter Beteiligung der BNetzA in Betracht gezogen werden und nur als letzter Schritt ein regulierendes Einschreiten durch den Gesetzgeber erfolgen.[1009]

e. Fachgespräch „Plattformen: Interoperabilität und Neutralität" – Ausschuss Digitale Agenda

Das Thema Interoperabilität wurde auch bei einem öffentlichen Fachgespräch zum Thema „Plattformen: Interoperabilität und Neutralität" in der 78. Sitzung des Deutschen Bundestags (Ausschuss Digitale Agenda) am 14. Dezember 2016 diskutiert.[1010] Übergeordnet ging es um die Frage, welche Bedeutung Interoperabilität und Neutralität im digitalen Zeitalter

1008 *Deutscher Bundestag*, Zehnter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft", S. 22.

1009 *Deutscher Bundestag*, Zehnter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft", S. 50 f.; hierzu gab es allerdings innerhalb der Kommission auch Sondervoten.

1010 Vgl. Kurzprotokoll der 78. Sitzung, Protokoll-Nr. 18/78, abrufbar unter https://www.bundestag.de/resource/blob/526220/8b8bf1ea65625ef28a331469886d1071/Protokoll-data.pdf.

insgesamt und im Speziellen mit Bezug auf Plattformen zukommt. Das Fachgespräch stand im Kontext der anstehenden GWB-Novelle. Eine der Fragen, die an die Sachverständigen gerichtet wurde und tatsächliche Strukturen der Plattformökonomie sowie deren regulatorischen Rahmen betrafen, lautete: „Wie stehen Sie zu Vorschlägen einer möglichen Regulierung solcher Plattformen, die inzwischen erheblichen Einfluss auf die Meinungsbildung haben? Inwieweit bedarf es hier Vorgaben zur Absicherung von Meinungsfreiheit und -vielfalt?".[1011]

Die Antworten der Sachverständigen hierauf waren unterschiedlich.[1012] Teilweise wurde, insbesondere mit Verweis auf Newsaggregatoren und soziale Netzwerke, die Bedeutung (der Sicherstellung) von Transparenz für die Nutzer hervorgehoben, eine inhaltsbezogene Medienregulierung im Bereich der digitalen Ökonomie hingegen abgelehnt, da gegenwärtig keine hinreichenden Anhaltspunkte für eine Erforderlichkeit zum Schutz der Meinungsfreiheit bestünden.[1013] Noch abweisender vertrat ein Sachverständiger, dass eine Regulierung von öffentlichkeitsrelevanten Plattformen hinsichtlich ihrer Neutralität weder zielführend noch wünschenswert sei und vielmehr ein negativ zu bewertender Eingriff in die Meinungsfreiheit sei.[1014] Umgekehrt gab es aber auch die Einschätzung, dass Plattformen Orte des politischen Diskurses und deshalb Voraussetzung für die Teilhabe am öffentlichen und politischen Leben seien und deshalb ein Regulierungsbedarf zur Sicherstellung gleichberechtigter Teilhabe bestehe.[1015] Teilweise wurden populistische Tendenzen und Algorithmus-basierte Filterblasen als Kernprobleme auch für die Vielfalt gesehen, die sich in Zukunft wohl noch verfestigen würden, weshalb Normen zur Sicherung des Wettbewerbs und der Datenportabilität zumindest teilweise Lösungen liefern könnten.[1016]

1011 *Deutscher Bundestag, Ausschuss Digitale Agenda*, Ausschussdrucksache 18(24)SB37, https://www.bundestag.de/resource/blob/484000/29c58cb642d302d886420e5c9b91fcec/Fragenkatalog-data.pdf, Nr. 7.

1012 Als Sachverständige äußerten *Jürgen Kühling* (Monopolkommission), *Clark Parsons* (Internet Economy Foundation), *Michael Seemann* (Kulturwissenschaftler) und *Mirko Boehm* (Free Software Foundation Europe). Die schriftlichen Stellungnahmen sind abrufbar unter https://www.bundestag.de/webarchiv/Ausschuesse/ausschuesse18/a23/anhoerungen/fachgespraech-483996.

1013 So *Kühling*, S. 7.

1014 So *Seemann*, S. 11.

1015 So *Boehm*, S. 4.

1016 So *Parsons*, S. 13.

f. Ansätze im Medien- und Kommunikationsbericht der Bundesregierung

Die Bundesregierung legt dem Bundestag alle zwei Jahre einen Bericht zur Entwicklung der Medien- und Kommunikationsordnung vor.[1017] Ein für den Medien- und Kommunikationsbericht 2021[1018] in Auftrag gegebenes wissenschaftliches Gutachten untersuchte, welche Vor- und Nachteile im Aufbau kooperativer Medienplattformen liegen.[1019] Solche Medienplattformen sind nicht gleichbedeutend mit Interoperabilität. Die Diskussion um deren Aufbau verfolgt aber häufig ähnliche Ziele wie Interoperabilitätspflichten bzw. -bestrebungen: Es geht um die Bündelung von Angeboten oder Funktionen innerhalb einer Benutzeroberfläche oder in einem Dienst, was sowohl Vorteile für Nutzer als auch teilnehmende Unternehmen in wettbewerblicher Hinsicht (insb. Reichweite, Konkurrenzfähigkeit gebündelter Angebote gegenüber großen Plattformen) bietet. Im Unterschied zur Interoperabilität, insbesondere zur vertikalen oder asymmetrischen Interoperabilität, geht es dabei nicht um die Öffnung von Schnittstellen durch vor allem marktdominante Anbieter, sondern um die (häufig gleichberechtigte) Kooperation zwischen Anbietern.

Das Gutachten arbeitet zunächst den Diskurs über kooperative Medienplattformen auf, um anschließend den Themenkomplex aus institutionentheoretischer, kommunikationswissenschaftlicher, medienökonomischer und juristischer Perspektive zu beleuchten. Es kommt zu dem Schluss, dass der Aufbau einer europäischen „Super-Plattform" als Gegenwicht vor allem zu US-amerikanischen Plattformen wie Netflix oder Facebook nicht zielführend sei. Vielmehr stellten anbieteroffene, kooperative Medienplattformen eine Möglichkeit dar, „um die für die liberale Demokratie essenziellen publizistischen Leistungen unter digitalen Bedingungen ökonomisch erbringen und dauerhaft sicherstellen zu können."[1020] Hierfür solle der rechtliche Rahmen im Mehrebenensystem, insbesondere im Kartellrecht, entsprechend weiterentwickelt und eine staatliche Förderung etabliert werden. Wegen der fundamentalen gesellschaftlichen Bedeutung von

1017 Beschlussempfehlung und Bericht des Ausschusses für Kultur und Medien, BT-Drs. 19/14402, S. 9.

1018 Medien- und Kommunikationsbericht der Bundesregierung 2021, BT-Drs. 19/31165.

1019 *Gostomzyk et al.*, Kooperative Medienplattformen in einer künftigen Medienordnung, 2021, S. 6.

1020 *Gostomzyk et al.*, Kooperative Medienplattformen in einer künftigen Medienordnung, 2021, S. 156.

Medien könnte ein entsprechendes Vorhaben unter Schirmherrschaft des Bundespräsidenten oder durch eine gemeinsame Digital-Agentur von Bund und Ländern adressiert werden.[1021]

Das Gutachten unterscheidet drei verschiedene Arten kooperativer Medienplattformen: Erstens hätten sich audiovisuelle Plattformen in Form von Mediatheken gebildet, die teils auch von eigentlich konkurrierenden Anbietern betrieben würden (bspw. das Streaming-Angebot Joyn, das ehemals von ProSiebenSat.1 und Discovery getragen wurde). Zweitens lasse sich eine Standardisierung und Öffnung von Schnittstellen zur Vernetzung existierender Angebote beobachten. Praktisch handle es sich in der Regel um vereinheitlichte Login-Verfahren für Nutzer, die einen Zugang für mehrere journalistische Angebote bereitstellten (bspw. NetID von RTL, ProSiebenSat.1 und United Internet). Drittens hätten sich relativ offene Plattformen als Ausspielfläche für journalistische Inhalte etabliert (bspw. radioplayer.de als Plattform für verschiedene Radiosender).[1022] Interoperabilität kommt dabei nicht ausdrücklich zur Sprache, ist aber insbesondere für die Standardisierung und die Öffnung von Schnittstellen sowie für offene Plattformen eine Voraussetzung, um Kooperation überhaupt zu ermöglichen.

Damit publizistische Leistungen auch in Zukunft über Medienplattformen bereitgestellt und vermittelt werden können, schlägt das Gutachten offene kooperative Plattformen vor, die sich gegenüber nicht-publizistischen Angeboten abgrenzen sollen. Zu Letzteren wird auch die Vernetzung bestehender Plattformen, wie die Verknüpfung von Mediatheken oder vereinheitlichte Login-Verfahren, gezählt. Eine kooperative Medienplattform entstünde, wenn verschiedene Anbieter sich für den Aufbau, Betrieb und die Fortentwicklung einer Plattform zusammenschlössen, ohne dabei den publizistischen Wettbewerb zu gefährden. Interoperabilität wird auch hier nicht explizit benannt, gleichwohl wird die Bedeutung von Standardisierung und die Öffnung von Schnittstellen zur Vernetzung existierender Angebote als zentrales Element gesehen.[1023]

Obwohl öffentlich-rechtliche Rundfunkanstalten aus § 26 Abs. 5 MStV den Auftrag zur Kooperation hätten, sei der Aufbau einer gemeinsamen

1021 *Gostomzyk et al.*, Kooperative Medienplattformen in einer künftigen Medienordnung, 2021, S. 163 ff.

1022 *Gostomzyk et al.*, Kooperative Medienplattformen in einer künftigen Medienordnung, 2021, S. 26 ff.

1023 *Gostomzyk et al.*, Kooperative Medienplattformen in einer künftigen Medienordnung, 2021, S. 157.

öffentlich-rechtlichen Medienplattform hiervon gerade nicht erfasst.[1024] Für gemeinsame Plattformen des öffentlich-rechtlichen Rundfunks wäre aus damaliger Sicht eine Klarstellung des Auftrags wie auch der Kooperationsvorschriften im MStV erforderlich. In der Folge wäre eine kartellrechtliche Bereichsausnahme zu treffen, die eine wirtschaftliche Zusammenarbeit ermögliche, ohne in den publizistischen Wettbewerb einzugreifen.[1025] Im privaten Bereich könnten Presseverlage kooperative Medienplattformen schaffen. Aufgrund der Marktsituation mit einer fortgeschrittenen Konzentration im Bereich des privaten Rundfunks sei dies dort ohne wettbewerbsrechtliche Ausnahme nicht möglich. Zudem könnten Kooperationen hier nachteilige Auswirkungen für Wettbewerber haben. Gleichwohl seien offene Plattformlösungen denkbar, wenn eine Beteiligung aller Anbieter publizistischer Leistungen gewährleistet wäre.[1026] Für medienübergreifende Kooperationen, also zwischen Presse und Rundfunk, bedürfe es jedoch einer Anpassung des Kartellrechts. Insbesondere sollte eine Kooperation auf den Aufbau, die Entwicklung und den Betrieb von Plattformen begrenzt und die redaktionelle Zusammenarbeit ausgeschlossen werden, um die Medienvielfalt nicht zu gefährden.[1027] Auch eine Kooperation von öffentlich-rechtlichen und privaten Medien wäre aus Sicht des Gutachtens rechtlich möglich, etwa in Form einer gemeinsamen Stiftung oder einer Genossenschaft. Möglich wären zudem gemeinsame Such- und Empfehlungssysteme, die auf bestehende publizistische Angebote des öffentlich-rechtlichen Rundfunks und privater Anbieter verlinken würden.[1028]

Abschließend unterstreicht das Gutachten, dass kooperative Medienplattformen eines von mehreren Elementen eines digitalen Medien-Ökosystems sein könnten. Anstelle einer großen Plattform müsste es sich vielmehr um diverse, prinzipiell offene Plattformen handeln. Diese könnten zur Qualitätsdifferenzierung auch grundsätzlich Zutrittsbarrieren etablieren, sofern sich die an den Plattformen beteiligten Medien auf gemeinsame

1024 *Gostomzyk et al.*, Kooperative Medienplattformen in einer künftigen Medienordnung, 2021, S. 146.
1025 *Gostomzyk et al.*, Kooperative Medienplattformen in einer künftigen Medienordnung, 2021, S. 161.
1026 *Gostomzyk et al.*, Kooperative Medienplattformen in einer künftigen Medienordnung, 2021, S. 149.
1027 *Gostomzyk et al.*, Kooperative Medienplattformen in einer künftigen Medienordnung, 2021, S. 149 f.
1028 *Gostomzyk et al.*, Kooperative Medienplattformen in einer künftigen Medienordnung, 2021, S. 152.

Standards einigten.[1029] Auch hier kommt Interoperabilität nicht ausdrücklich zur Sprache, diese stellt jedoch eine notwendige Voraussetzung für solche kooperativen Medienplattformen dar. Im März 2022 wurde der Medien- und Kommunikationsbericht 2021 an den Ausschuss für Kultur und Medien (federführend), den Rechtsausschuss und den Ausschuss für Digitales überwiesen. Darauf aufbauende gesetzgeberische Aktivitäten auf Bundesebene sind nicht ersichtlich.

1029 *Gostomzyk et al.*, Kooperative Medienplattformen in einer künftigen Medienordnung, 2021, S. 164.