



Bundeskartellamt

Sektoruntersuchung Messenger- und Video-Dienste

Zwischenbericht

„Branchenüberblick und Stimmungsbild Interoperabilität“

November 2021

Sektoruntersuchung Messenger- und Video-Dienste

(Zwischen-) Bericht gemäß § 32e GWB

Az. V-28/20

November 2021

Kontakt

Bundeskartellamt

Beschlussabteilung Wettbewerbs- und Verbraucherschutz

Kaiser-Friedrich-Straße 16

53113 Bonn

poststelle@bundeskartellamt.bund.de

www.bundeskartellamt.de

Vorbemerkung

Die Beschlussabteilung Wettbewerbs- und Verbraucherschutz des Bundeskartellamts hat im November 2020 eine verbraucherrechtliche Sektoruntersuchung nach § 32e Abs. 5 des Gesetzes gegen Wettbewerbsbeschränkungen¹ im Wirtschaftszweig Messenger- und Video-Dienste eingeleitet.² Sektoruntersuchungen richten sich nicht gegen bestimmte Unternehmen, sondern dienen der Untersuchung eines Wirtschaftszweigs im Hinblick auf mögliche verbraucherrechtliche Verstöße. Vorausgegangen war die erstmalige Übertragung von Kompetenzen im Bereich des Verbraucherschutzes auf das Bundeskartellamt mit der im Juni 2017 in Kraft getretenen 9. Novelle des Gesetzes gegen Wettbewerbsbeschränkungen (GWB).³

Auf die Regelung des § 32e Abs. 6 GWB über den ausgeschlossenen Aufwendungsersatz im Falle einer Abmahnung nach § 12 Abs. 1 Satz 2 des Gesetzes gegen den unlauteren Wettbewerb⁴ (UWG) wird hingewiesen.

¹ Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bek. v. 26.06.2013 (BGBl. I S. 1750, 3245), zuletzt geändert durch Gesetz vom 09.07.2021 (BGBl. I S. 2506) m. W. v. 15.07.2021 - GWB.

² S. Pressemitteilung vom 12.11.2020, abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2020/12_11_2020_SU_Messenger_Dienste.html?nn=3591568. Soweit nicht anders angegeben, ist Stand sämtlicher Internetquellen der 2. November 2021.

³ S. Pressemitteilung vom 12.06.2017, abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Pressemitteilungen/2017/12_06_2017_Abteilung%20V.pdf?__blob=publicationFile&v=2.

⁴ Gesetz gegen den unlauteren Wettbewerb in der Fassung der Bek. v. 03.03.2010 (BGBl. I S. 254), zuletzt geändert durch Gesetz vom 26.11.2020 (BGBl. I S. 2568) m. W. v. 02.12.2020 – UWG.

Inhaltsverzeichnis

Zusammenfassung	IV
A. Einleitung.....	1
B. Verfahrensgang	5
I. Verbraucherrechtliche Sektoruntersuchung.....	5
II. Zusammenarbeit mit dem BSI	5
C. Branchenüberblick Messenger- und Video-Dienste.....	7
I. Funktionsweise und Funktionen	8
II. Verhältnis zu anderen Kommunikationsmitteln	9
III. Kriterien für Datensicherheit und Datenschutz.....	12
1. Netzwerk, Protokolle und Server.....	13
2. Verschlüsselung	14
3. Identifier und Umgang mit Kontakten	16
4. Umgang mit Metadaten.....	17
IV. Verfahren der Standardisierung	18
V. Erste Ermittlungsergebnisse zur Branche.....	21
1. Branchenteilnehmer, Funktionen und Geschäftsmodelle im Überblick.....	22
2. Finanzierung und Umsätze	26
3. Nutzungszahlen	26
4. Wettbewerbssituation.....	28
D. Datenportabilität als Übergang zur Interoperabilität?.....	30
I. Einordnung und Anspruch der Vorschrift.....	30
II. Praktische Bedeutung	31
III. Ermittlungsergebnisse.....	33
E. Mehr Datenschutz durch Interoperabilität?	35
I. Umsetzung und Gestaltung	36
II. Interoperabilität im Wettbewerbs- und Sektorrecht	39
1. § 19a Gesetz gegen Wettbewerbsbeschränkungen (GWB)	40
2. Europäischer Kodex für elektronische Kommunikation (EKEK) / Telekommunikationsgesetz (TKG)	41
3. Digital Markets Act (DMA-Vorschlag).....	41
III. Beitrag wissenschaftlicher Erkenntnisse.....	42
1. Klasse statt Masse.....	42
2. Theorie der Netzwerke.....	43

3. Auswirkungen auf Wettbewerb und Innovation	45
4. Effekte einer Standardisierung	47
IV. Verbraucherverhalten	48
1. Interoperabilität oder Multi Homing?	49
2. Wunsch nach mehr Datenschutz?	51
V. Ermittlungsergebnisse	53
1. Interoperabilität	53
a) Interoperabilität im Spannungsfeld von Datensicherheit, Datenschutz und Investitionsbereitschaft	53
b) Bestehende oder geplante Interoperabilitätsregelungen	55
c) Umsetzung einer Interoperabilitätsverpflichtung, wie und für wen?	57
d) Auswirkungen von Interoperabilität	60
aa) Innovationsanreize und Differenzierungsmöglichkeiten	60
bb) Verbraucherinteressen (Nutzererlebnis und Multi Homing)	62
cc) Datensicherheit	63
dd) Datenschutz	65
ee) Nutzerzahlen und Umsätze	66
ff) Wettbewerbsintensität	67
2. Interoperabilität und Standardisierung im Lichte der Brancheninteressen	68
a) Der richtige Weg?	68
b) Herausforderungen und Risiken	69
c) Umsetzung	69
d) Eignung von Marktteilnehmern, Institutionen und Behörden, zu einem Standardisierungsprozess beizutragen	70
Anhang: Einbezogene Dienste und Glossar	X

Zusammenfassung

Das Bundeskartellamt befasst sich in der Sektoruntersuchung Messenger- und Video-Dienste insbesondere mit der Struktur der Branche, mit Fragen der Datensicherheit und des Datenschutzes sowie möglichen Verbraucherrechtsverstößen in diesem Zusammenhang, und nicht zuletzt mit dem Thema Interoperabilität. Es hat im Rahmen der Sektoruntersuchung über 40 verschiedene Dienste zu diesen Themen befragt und eine Reihe von Expertengesprächen geführt. Darüber hinaus wurde eine Vielzahl von Studien und Fachartikeln ausgewertet.

Im vorliegenden **Zwischenbericht** stellt das Bundeskartellamt die Ermittlungsergebnisse aus **zwei untersuchten Themenbereichen** dar: Zum einen wird ein Überblick über die Rahmenbedingungen der **Branche** sowie die verschiedenen Anbietergruppen, Funktionalitäten und Geschäftsmodelle gegeben. Zum anderen werden die Ergebnisse der Unternehmensbefragung zur **Interoperabilität** dargestellt und dazu eine erste rechtliche, technische und wissenschaftliche Einordnung vorgenommen. Interoperabilität meint in diesem Kontext die Möglichkeit, mit Nutzern anderer Dienste kommunizieren zu können, ohne die jeweilige App oder Software des anderen Dienstes installiert und sich dort registriert zu haben. Dabei geht es nicht nur darum, wie Interoperabilität technisch, organisatorisch und rechtlich zwischen verschiedenen Diensten hergestellt werden könnte. Vor allem ist zu berücksichtigen, inwieweit eine solche Interoperabilität die Datensicherheit und damit das Datenschutzniveau von Messenger- und Video-Diensten beeinflussen würde und in welchem Ausmaß mit Auswirkungen auf Innovationsanreize und die Wettbewerbsintensität in der Branche zu rechnen ist.

Branchenüberblick

Die Ermittlungen haben ein **vielgestaltiges Bild der Branche** gezeichnet, das weit über die bekannten und verbreiteten Messenger- und Video-Dienste hinausgeht. Zum besseren Verständnis wird zunächst auf die unterschiedliche Verwendung der **technischen Kriterien** wie Protokolle, Server, Verschlüsselung oder Identifier eingegangen, die für die Datensicherheit und den Datenschutz eines Messengers maßgeblich sind. Ebenso werden die offenen technischen Standardisierungsverfahren der Branche und die dahinterstehenden Prozesse und Institutionen überblicksartig dargestellt. Darüber hinaus unterscheiden sich die Dienste aber auch hinsichtlich ihrer **Funktionen, ihrer Geschäftsmodelle und ihrer wirtschaftlichen Bedeutung**. Hier reicht die Bandbreite vom internationalen, konzernbetriebenen Diensten mit vielen Millionen Nutzern und hohen Umsätzen bis hin zur kleinen freien Anwendung ohne Gewinnerzielungsabsicht.

- Aufgrund dieser Heterogenität der Branche können nach Auffassung des Bundeskartellamts politische Maßnahmen und rechtliche Vorgaben für die betroffenen Unternehmen und Anwendungen sehr unterschiedliche Auswirkungen haben. Auch verbraucherrechtliche Bewertungen oder Handlungsempfehlungen müssen diese Vielgestaltigkeit der Marktteilnehmer im Blick behalten.

Stimmungsbild Interoperabilität

Die Ermittlungsergebnisse zum Themenkomplex Interoperabilität von Messenger- und Video-Diensten bieten eine wichtige Sachverhaltsgrundlage für die Rechtspolitik. Denn neben den Behördenpublikationen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu kryptologischen Aspekten von Interoperabilität⁵ und der Bundesnetzagentur über die Verbraucherpräferenzen bei der Nutzung von Messenger-Diensten⁶ liegen mit dem Zwischenbericht zur Sektoruntersuchung nun auch behördliche Erkenntnisse über die **Möglichkeiten und Vorstellungen der betroffenen Unternehmen** vor. Die insofern zunächst deskriptiv dargestellten Ermittlungsergebnisse zum Thema Interoperabilität spiegeln die Komplexität des Themas, aber auch die Heterogenität der Branche wider, deren Marktteilnehmer teilweise unterschiedliche Sichtweisen vertreten.

Die Befragung der Unternehmen durch das Bundeskartellamt hatte dabei einen klaren Fokus. Es ging darum, den verschiedentlich geäußerten Erwartungen nachzugehen, dass durch Interoperabilität der Wechsel zu datenschutzfreundlichen Messenger-Diensten erleichtert und dadurch die **Datenschutzqualität** in diesem Bereich gefördert wird. Andere mit Interoperabilität verbundene Zielvorstellungen, wie etwa die Sicherstellung von Konnektivität im Bereich der interpersonellen Kommunikation oder ein Abbau von Marktmacht führender Messenger-Dienste, waren kein direkter Gegenstand der Untersuchung.

Als wesentliche **Einflussgrößen** für Datenschutzeffekte durch Interoperabilität können nach den Ermittlungsergebnissen die technischen Erfordernisse, die Datensicherheit, die Wechselwirkungen von Interoperabilität im Hinblick auf Innovationsanreize und die Wettbewerbsintensität sowie das Verbraucherverhalten gesehen werden. Das Bundeskartellamt hat in seiner Befragung der Branche alle drei Bereiche angesprochen. Der Schwerpunkt lag allerdings auf den zu erwartenden Wechselwirkungen von Interoperabilität, da diese vor allem von den direkt befragten Messenger- und Video-Diensten selbst beurteilt werden können.

Insgesamt hat die Befragung gezeigt, dass Interoperabilität von den betroffenen Unternehmen nicht rundheraus abgelehnt wird. Vielmehr wird in Teilbereichen Interoperabilität oder werden zumindest Formen des Austausches unterschiedlicher technischer Tiefe und Reichweite bereits

⁵ BSI, Moderne Messenger – heute verschlüsselt, morgen interoperabel?, November 2021, abrufbar unter: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html> .

⁶ BNetzA, Nutzung von OTT-Kommunikationsdiensten in Deutschland, Mai 2020, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Digitalisierung/OTT-KommunikationsdiensteKurz.pdf?__blob=publicationFile&v=4 .

praktiziert. In Standardisierungsgremien werden technische Grundlagen für Interoperabilität in globalem Kontext eruiert. Dies geht allerdings einher mit der klaren Haltung eines Großteils der Branche, dass eine gesetzliche Verpflichtung zur Interoperabilität mehr Schaden als Nutzen würde und insofern abzulehnen sei. Für den Fall einer erzwungenen Interoperabilität befürchten die Unternehmen mit einer ablehnenden Haltung insbesondere negative Effekte auf die Innovationstätigkeit und damit auch auf das Datensicherheits- und Datenschutzniveau beim Messaging und Videoconferencing. Im Einzelnen:

Knapp die Hälfte der befragten Unternehmen haben sich **offen gegenüber freiwilligen Interoperabilitätsvorhaben** gezeigt, wobei sich allerdings - asymmetrisch hierzu - nur weniger als die Hälfte daran beteiligen würde. Bei diesen Zahlen ist zu berücksichtigen, dass die Befragten ihre Einschätzung für oder gegen eine freiwillige Interoperabilität jeweils mit zahlreichen Anmerkungen, Voraussetzungen, Hinweisen und Einschränkungen versehen haben.

Des Weiteren brachten die Antworten zutage, dass eine **Erreichbarkeit über Dienst-Grenzen hinweg in gewissem Umfang bereits ermöglicht** wird. So sind die freien Messenger-Clients innerhalb ihres Systems untereinander vollständig interoperabel. Es existiert ferner ein weiterer Open Source-Bereich, der Interoperabilität quasi als Geschäftsmodell verfolgt. Bei einigen Video-Diensten wird zumindest eine Erreichbarkeit auch für dritte Nutzer ermöglicht, etwa indem Einladungslinks versendet werden können. Speziell für den Geschäftskundenbereich gibt es daneben bilaterale Regelungen oder Interoperabilitätsabkommen sowie Dienstleister, die eine gegenseitige Erreichbarkeit herstellen können. Eine sehr rudimentäre Form der Verbindung bieten schließlich Multi Messenger, mit deren Hilfe die Nutzer verschiedene Messenger-Dienste über eine Softwareoberfläche bedienen und Inhalte lesen können.

Eine Umsetzung von Interoperabilität sollte den Befragten zufolge nur auf Basis **globaler technischer Standards** erfolgen. Für die Branche wäre es andernfalls sehr aufwendig, weltweit unterschiedliche Anforderungen erfüllen und verschiedene Sets interoperabler Funktionen anbieten zu müssen. Für solch einen globalen Standardisierungsprozess bezeichnen gut 60 Prozent der Befragten die Internet Engineering Task Force (IETF) als bestgeeignet.

Hinsichtlich der **konkreten Auswirkungen von Interoperabilität auf die Datensicherheit und damit auf das Datenschutzniveau** ist die Bewertung durch die Unternehmen mehrschichtig: Einerseits wäre danach ein direkter (vorteilhafter) Effekt denkbar, wenn die Verbraucher bei einer Erreichbarkeit der Dienste untereinander zu datenschutzfreundlicheren Anbietern wechseln, Datenschutz somit als Wettbewerbsvorteil höhere Bedeutung erlangen und sich das Datenschutzniveau insgesamt erhöhen würde. Andererseits prognostizieren befragte Unternehmen auch indirekte (negative) Effekte auf Datensicherheit und Datenschutz. So könne sich eine mögliche Interoperabilitätsverpflichtung dämpfend auf die Innovationstätigkeit der Anbieter und in der Folge auch für das Datenschutzniveau auswirken, insbesondere wenn

weltweit einheitliche Standards oder Protokolle, die bei der Verschlüsselung hinter den bestehenden Standards zurückbleiben, sowie Identifier auf Basis des kleinsten gemeinsamen Nenners verwendet werden müssten. Die steigenden Anforderungen an die Datensicherheit könnten schließlich zu höheren Kosten führen, die insb. für kleinere Anbieter eine Hürde darstellen könnten.

Nach Meinung einer Mehrheit der befragten Unternehmen wären bei einer **gesetzlich vorgegebenen** Interoperabilität negative Konsequenzen für die Innovationstätigkeit und damit auch für die Datensicherheit zu erwarten. Allerdings gibt es auch Dienste, die sich laut Befragung neue Möglichkeiten davon versprechen, wenn Erreichbarkeit bzw. große Nutzerzahlen kein Differenzierungsmerkmal mehr darstellen. Dies könnte mit einer Belebung der Wettbewerbsintensität verbunden sein. Relativ einig sind sich die Befragten, dass eine per Gesetz verpflichtende Interoperabilität es komplizierter machen würde, die Sicherheit der Daten zu gewährleisten und damit auch die Datenschutzgesetze einzuhalten. Einige Stimmen der Branche halten dagegen, die Schwierigkeiten bei Datensicherheit und Datenschutz könnten auf technischer Ebene behoben werden, letztlich sei alles eine Frage der Investitionsbereitschaft.

Überwiegend erwarten die befragten Messenger- und Video-Dienste jedenfalls von einer erzwungenen Interoperabilität kein höheres Datenschutzniveau, sondern betonen, dass die **Untergrenze für das Datenschutzniveau** durch die geltenden Datenschutzgesetze wie etwa die Datenschutz-Grundverordnung (DSGVO) festgeschrieben wird. Diese müssten eingehalten werden, unabhängig davon, ob Interoperabilität zu anderen Messenger- und Video-Diensten bestehe oder nicht. In den Antworten wurde zudem darauf hingewiesen, dass bereits ein **gesetzlicher Rahmen für eine mögliche Interoperabilitätsverpflichtung** besteht. Dieser Rahmen wird gebildet durch § 21 Abs. 2 des ab Dezember 2021 geltenden Telekommunikationsgesetzes (TKG). Danach kann unter bestimmten Voraussetzungen und in einem bestimmten Verfahren Interoperabilität auferlegt werden, wenn die durchgehende Konnektivität zwischen Endnutzern gefährdet ist. Zu nennen ist hier ferner der im Januar 2021 in Kraft getretene neue § 19a Abs. 2 Nr. 5 Gesetz gegen Wettbewerbsbeschränkungen (GWB), wonach das Bundeskartellamt Normadressaten untersagen kann, die Interoperabilität von Produkten oder Leistungen oder die Portabilität von Daten zu verweigern oder zu erschweren und damit den Wettbewerb zu behindern.

- Die Erkenntnisse aus der Branchenbefragung zeigen aus Sicht des Bundeskartellamts insgesamt, dass die **Analyse der Wirkungszusammenhänge rund um das Thema Interoperabilität vielschichtig und komplex** ist. Eine eindimensionale Bewertung wäre nicht sachgerecht. Es sollten vielmehr nicht nur die notwendigen Investitionen in technische Veränderungen der Dienste oder die Entwicklung technischer Neuerungen für die Umsetzung berücksichtigt werden. Ebenso einzubeziehen wären mögliche positive oder

negative Wohlfahrtseffekte durch veränderte Innovationsanreize und Auswirkungen auf Geschäftsstrategien und Wettbewerbsintensität.

- Gleichzeitig hält des Bundeskartellamt das **Verhalten der Verbraucher** als wichtigen Einflussfaktor weiterhin für eine **schwer einschätzbare Größe**: Ob eine spürbar große Anzahl an Verbrauchern bei Interoperabilität tatsächlich, wie verschiedentlich erhofft, vermehrt zu datenschutzfreundlichen Anbietern wechseln würden, ist ausweislich aktueller Befragungen der Bundesnetzagentur⁷ und des Verbraucherzentrale Bundesverbands⁸ zu Nutzerinteressen und Wechselbereitschaft allenfalls als offen und eher als fraglich zu bezeichnen. Ebenso vorstellbar ist aus Sicht einiger befragter, eher verbraucherorientierter Dienste ein Szenario, in dem die Verbraucher aufgrund eines eingeschränkten Nutzererlebnisses dem Messaging den Rücken kehren. Eventuell gäbe es auch gar keine nennenswerten Reaktionen der Verbraucher auf eine Interoperabilität von Messenger- und Video-Diensten, da die Verbraucher mit ihren aktuellen Multi Homing - Lösungen zufrieden sind. Angesichts des derzeitigen Erkenntnisstands ist es nach Ansicht des Bundeskartellamts jedenfalls nicht geraten, zukünftigen Handlungsempfehlungen ein bestimmtes, einheitliches Verbraucherverhalten zugrunde zu legen.

Weiterer Gang der Sektoruntersuchung

Das Bundeskartellamt wird die **Auswertung der Ermittlungsergebnisse** nach Veröffentlichung des vorliegenden Zwischenberichts **fortsetzen**. Für jegliche Prognosen zukünftiger Entwicklungen ist zunächst eine grundlegende Kenntnis der Ausgangssituation erforderlich. Hier sind sowohl die Datensicherheit und die Kommunikation darüber gegenüber den Verbrauchern als auch die Datenverarbeitung gemäß DSGVO angesprochen. Das Bundeskartellamt wird auf Basis der Auswertungen zu diesen Fragen auch mögliche Verbraucherrechtsverstöße prüfen. Ein weiteres Thema werden alternative oder zusätzliche Maßnahmen zur Erhöhung des Datenschutzniveaus oder zur Herstellung einer besseren Erreichbarkeit sein, wozu sich die Messenger- und Video-Dienste im Rahmen der Befragung ebenfalls geäußert haben. Schließlich sind absehbare zukünftige Entwicklungen - nicht nur bei Standardisierungsvorhaben (z. B. MLS) sondern auch bei der Verbreitung technischer Neuerungen (z. B. „Augmented Reality“) - und von ihnen ausgehende Veränderungsprozesse zu beobachten und in die weitere Auswertung einzubeziehen.

⁷ BNetzA, Nutzung von OTT-Kommunikationsdiensten in Deutschland, Mai 2020, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/OTT.pdf?__blob=publicationFile .

⁸ VZBV, Interoperabilität bei Messengerdiensten, Mai 2021, abrufbar unter: <https://www.vzbv.de/pressemitteilungen/messenger-dienste-regulierung-mit-augenmass> .

- Das Bundeskartellamt wird die Sektoruntersuchung Messenger- und Video-Dienste **im Jahr 2022 mit einem Abschlussbericht beenden.**

A. Einleitung

Messenger- und Video-Dienste sind für viele Menschen inzwischen ein unverzichtbarer Teil der alltäglichen Kommunikation geworden. Die Verbraucher⁹ nutzen diese Dienste auf verschiedenen Endgeräten, um mit anderen Nutzern Text- und Sprachnachrichten sowie Dateien auszutauschen oder (per Video) zu telefonieren. Der Austausch kann dabei entweder bilateral (1:1) oder mit mehreren anderen Nutzern (Gruppe / Konferenz) erfolgen. Im Zuge dieser Entwicklung sind neue verbraucherrechtliche Fragestellungen aufgekommen.

Es gibt aus der Fachöffentlichkeit und von Seiten der Verbraucherverbände und -zentralen immer wieder Hinweise darauf, dass die Nutzer von Messenger- bzw. Video-Diensten verbraucherrechtlich zu wenig geschützt sind.¹⁰ So werden zum einen Sicherheitsmängel dieser Dienste thematisiert, etwa bei der Verschlüsselung. Wenn die Nutzer über sicherheitsrelevante Aspekte eines Messenger- oder Video-Dienstes nicht angemessen informiert werden, kann hier eine unzulässige Irreführung vorliegen. Zum anderen wird regelmäßig auf Datenschutzprobleme bei Messenger- oder Video-Diensten hingewiesen, z. B. was die Weitergabe von Kontaktdaten angeht. Hier können Verstöße gegen das Datenschutzrecht bestehen.

⁹ Ausschließlich zum Zweck der besseren Lesbarkeit wird im vorliegenden Bericht teilweise auf die geschlechtsspezifische Schreibweise verzichtet. Alle personenbezogenen Bezeichnungen sind geschlechtsneutral zu verstehen.

¹⁰ Vgl. *Verbraucherzentrale NRW*, WhatsApp-Alternativen: Messenger im Überblick, 15.07.2020, abrufbar unter: <https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-messenger-im-ueberblick-13055> sowie *Verbraucherzentrale NRW*, Soziale Medien: Verstöße gegen die DSGVO, 16.01.2019, abrufbar unter: <https://www.verbraucherzentrale.de/aktuelle-meldungen/digitale-welt/soziale-medien-verstoesse-gegen-die-dsgvo-30411>. Vgl. auch *Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*, Datenschutzwidrige Geschäftspraktiken und fairer Wettbewerb schließen sich aus, Pressemeldung vom 07.02.2019, abrufbar unter: <https://datenschutz-hamburg.de/pressemitteilungen/2019/02/2019-02-07-kartellamt-facebook>.

Aus politischen Kreisen wird zudem teilweise Kritik daran geäußert, dass die Verbraucher größtenteils nicht miteinander kommunizieren können, wenn sie verschiedene Dienste nutzen.¹¹ Mit dieser Kritik ist häufig die Annahme verbunden, dass eine diensteübergreifende Kommunikation zu einer verstärkten Nutzung von datenschutzfreundlichen Diensten führen würde. Viele der bekannten, bei Verbrauchern beliebten Messenger- und Video-Dienste sind aber technisch als geschlossenes System konzipiert. Sie sind nicht interoperabel. Interoperabilität meint in diesem Kontext die Möglichkeit, mit Nutzern anderer Dienste kommunizieren zu können, ohne die jeweilige App oder Software dieses anderen Dienstes installiert oder sich dort registriert zu haben.

Die in Deutschland aktiven Messenger- und Video-Dienste unterscheiden sich nicht nur nach ihrer Marktbedeutung, sondern auch nach ihren Funktionen, nach ihren Geschäftsmodellen oder Konzeptionen und nach ihren technischen Lösungen, insb. auch für bereits bestehende Interoperabilitätsregelungen. Im Rahmen dieser Sektoruntersuchung bezieht das Bundeskartellamt unabhängig von diesen Unterschieden Messenger- und Video-Dienste im weiteren Sinne in die Befragung ein, um den Wirtschaftssektor möglichst vollständig zu erfassen. Der Fragebogen des Bundeskartellamts¹² richtete sich folglich nicht nur an Dienste, bei denen Text-Messaging im Vordergrund steht, sondern auch an Videokonferenzanbieter, freie Messenger, Multi Messenger und sonstige Dienste, unabhängig davon, ob sie im privaten oder geschäftlichen Bereich ihren Schwerpunkt haben, sowie bestimmte Softwareanbieter.

Die Verfassung des wirtschaftlichen Umfelds, auf dem einige global agierende, diversifizierte und marktstarke Unternehmen vielen kleineren Anbietern und Anwendungen gegenüberstehen, macht die Analyse der Wirkungszusammenhänge zwischen Wettbewerb, Datenschutz und Innovation vielschichtig und komplex. Fraglich ist insbesondere, inwieweit mittels Interoperabilität das Ziel eines besseren Datenschutzes für die Verbraucher erreicht werden kann, ohne dies teuer mit schädlichen Auswirkungen auf Innovation und Wettbewerb zu erkaufen.

¹¹ Vgl. *Verbraucherschutzministerkonferenz*, Ergebnisprotokoll der 15. Verbraucherschutzministerkonferenz am 24. Mai 2019, TOP 12, Nr. 2, abrufbar unter: https://www.verbraucherschutzministerkonferenz.de/documents/ergebnisprotokoll-der-15-vsmk-am-24052019-in-mainz_rlp-extern_1559902425.pdf sowie Handelsblatt vom 15.09.2019, Interview mit Katarina Barley, Die Datenschutz-Grundverordnung ist ein scharfes Schwert, abrufbar unter: <https://www.handelsblatt.com/politik/international/europawahl/katarina-barley-im-interview-die-datenschutz-grundverordnung-ist-ein-scharfes-schwert/24339900.html> und Golem.de, Politiker fordern Interoperabilität, 2019, abrufbar unter: <https://www.golem.de/news/messenger-was-bringt-eine-fusion-von-facebook-whatsapp-und-instagram-1901-139014-2.html> .

¹² Der an die befragten Dienste versandte Fragebogen ist hier abrufbar: www.bundeskartellamt.de/messenger.html .

In dieser verbraucherrechtlichen Sektoruntersuchung möchte das Bundeskartellamt insbesondere die Struktur und die Rahmenbedingungen der Branche beleuchten, mögliche Verbraucherrechtsverstöße im Bereich von Datenschutz und Datensicherheit identifizieren und Erkenntnisse gewinnen, ob Interoperabilität positiven oder negativen Einfluss auf das Datenschutzniveau hätte. Aufgrund der Heterogenität der Branche, der zu erwartenden Wechselwirkungen zwischen Datenschutz und Wettbewerb und des in nicht wenigen Punkten unklaren Verbraucherverhaltens hielt es das Bundeskartellamt für angezeigt, Messenger- und Video-Dienste unmittelbar zu befragen. Sowohl die Zusammensetzung der Branche als auch die Position der zugehörigen Unternehmen und Anwendungen zu den genannten Aspekten waren außerhalb von interessierten Kreisen bisher weitgehend unbekannt.

In diesem Zwischenbericht stellt das Bundeskartellamt erste Erkenntnisse aus den Ermittlungen mit dem Schwerpunkt auf Branchenbild und einem möglichen Interoperabilitätsvorhaben dar. Dabei wird eine gewisse rechtliche, technische und wissenschaftliche Einordnung gegeben, ohne dass zu diesem Zeitpunkt schon eine eigene Bewertung und Positionierung damit verbunden wäre.

Im Anschluss an diese Einleitung wird zunächst kurz der Verfahrensgang der verbraucherrechtlichen Sektoruntersuchung erläutert (siehe hierzu Kapitel B.).

Danach geht es um eine kurze Beschreibung der Branche in ihrer Vielgestaltigkeit und mit ihren wesentlichen Kennzeichen (siehe hierzu Kapitel C.). In diesem Zusammenhang werden auch die Kriterien für Datensicherheit und Datenschutz skizziert. Danach werden Standardisierungsprozesse über offene Standards dargestellt. Im Anschluss werden erste Ermittlungsergebnisse zum konkreten wirtschaftlichen Umfeld der Messenger- und Video-Dienste, wie z. B. Geschäftsmodelle oder Nutzungszahlen, vorgestellt.

Es schließen sich Erörterungen zur Datenportabilität an, die in Art. 20 DSGVO eingeführt und ganz allgemein mit der Hoffnung verbunden wurde, Wechselvorhaben der Verbraucher zu erleichtern, und die so einen Übergang zur Interoperabilität darstellen könnte (Kapitel D.). Den theoretischen Erwägungen folgen auch hier Ermittlungsergebnisse, die als Indikator für das Wechselverhalten der Verbraucher interpretiert werden können.

Es folgt der zweite Schwerpunkt dieses Papiers, erste Ermittlungsergebnisse zur Interoperabilität (Kapitel E.). Vorausgeschickt werden auch hier zunächst einige Überlegungen zu wesentlichen Rahmenbedingungen und Erkenntnissen (zu beidem unter E.I.). Eine große Rolle spielen die technischen Weiterentwicklungen, da sie nicht nur die Umsetzungsmöglichkeiten bestimmen, sondern auch den damit verbundenen Aufwand festschreiben. Anders als in verbraucherrechtlichen Vorschriften können nach Wettbewerbs- und Telekommunikationsrecht - unter hohen Voraussetzungen und in einem festgelegten Verfahren - die Behörden eine Interoperabilitätsverpflichtung aussprechen (dazu unter E.II.). Die Komplexität dieser Aufgabe legen auch die zahlreichen wissenschaftlichen Untersuchungen nahe, zu denen ein kurzer

Überblick gegeben wird (dazu unter E.III.). Wesentlich für die Beurteilung möglicher Interoperabilitätsmaßnahmen ist das Verhalten des Verbrauchers (dazu E.IV.). Im Anschluss werden die Ermittlungsergebnisse zur Interoperabilität ausführlich vorgestellt (dazu E.V.). Neben bereits bestehenden Interoperabilitätslösungen in der Branche hat das Bundeskartellamt die Messenger- und Video-Dienste gebeten, ihre Haltung zu einer Interoperabilitätsverpflichtung und den damit verbundenen Auswirkungen im Detail darzulegen. Hier geht es insbesondere um die Diskussion, ob alles, was machbar wäre, auch sinnvoll ist. Ist alles nur eine Frage der Investitionsbereitschaft? Daraus ergab sich eine Diskussion um die Standardisierungsprozesse über offene Standards in der Branche.

Das Bundeskartellamt wird die Sektoruntersuchung fortführen und mit einem Abschlussbericht beenden, in den die weiteren Erkenntnisse, insb. zu Datensicherheit und technischen Umsetzungsmöglichkeiten von Interoperabilität sowie zur Datenverarbeitung einfließen.

B. Verfahrensgang

I. Verbraucherrechtliche Sektoruntersuchung

Die Beschlussabteilung hat im November 2020 eine verbraucherrechtliche Sektoruntersuchung „Messenger-Dienste“ nach § 32e Abs. 5 GWB eingeleitet.¹³

Im Vorfeld der Untersuchung und während des Untersuchungszeitraums hat das Bundeskartellamt Kontakt mit anderen Behörden und Institutionen aufgenommen und gehalten, die mit der Verbraucherschutzthematik Messenger- und Video-Dienste berührt oder selbst damit befasst sind. Dazu gehören das Bundesamt für Sicherheit in der Informationstechnik (BSI, siehe dazu im Einzelnen Kapitel II.), der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), die Bundesnetzagentur (BNetzA), die Stiftung Warentest sowie die Verbraucherzentrale Nordrhein-Westfalen (VZ NRW).

Ferner hat das Bundeskartellamt Gespräche mit Marktteilnehmern und Experten geführt, um die Untersuchungsthemen zu spezifizieren und die Befragung vorzubereiten.

Am 31. Mai 2021 hat das Bundeskartellamt die Fragebögen¹⁴ an 53 Adressaten im In- und Ausland versendet, von denen zwei nachträglich wieder von der Liste der Adressaten genommen wurden. Der Rücklauf der Antworten war bis zum 28. Juni 2021 vorgesehen. Es wurden verschiedene Fristverlängerungen bis 27. Juli 2021 gewährt. 44 Messenger- und Video-Dienste (86 Prozent der Befragten) haben den Fragebogen beantwortet.¹⁵ Die Angaben dieser Dienste bildeten die Basis der nachfolgend dargestellten Ermittlungsergebnisse.

Das Bundeskartellamt wird die Sektoruntersuchung nach der Publikation dieses Zwischenberichts fortsetzen und im Jahr 2022 mit einem Abschlussbericht beenden.

II. Zusammenarbeit mit dem BSI

Das Bundeskartellamt hat sich im Rahmen der Sektoruntersuchung Messenger- und Video-Dienste insbesondere mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ausgetauscht. Das BSI ist die Cyber-Sicherheitsbehörde des Bundes. Der Aufgabenbereich des

¹³ Vgl. Pressemitteilung des *Bundeskartellamtes* vom 12.11.2020, abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2020/12_11_2020_S_U_Messenger_Dienste.html?nn=3591568.

¹⁴ Der an die befragten Dienste versandte Fragebogen ist hier abrufbar: www.bundeskartellamt.de/messenger.html.

¹⁵ Siehe Liste der einbezogenen Dienste im Anhang.

BSI wird durch das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik¹⁶ festgelegt. Das BSI untersucht und bewertet bestehende Sicherheitsrisiken und schätzt die Auswirkungen neuer Entwicklungen ab.¹⁷

Am 22. Januar 2021 haben das Bundeskartellamt und das BSI eine Absichtserklärung unterzeichnet, mit dem Ziel, die jeweiligen Kompetenzen und Expertisen insbesondere im digitalen Verbraucherschutz zu bündeln.¹⁸ Im Zusammenhang mit der vorliegenden Sektoruntersuchung hat das BSI die geplanten Untersuchungsthemen aus technischer Sicht beleuchtet und dabei das Bundeskartellamt insbesondere im Rahmen der Fragebogenerstellung bei der Formulierung der Fragen zu technischen Aspekten der Datensicherheit beraten und ein Glossar der kryptographischen Fachbegriffe zugeliefert. Zeitgleich mit diesem Zwischenbericht hat das BSI eine eigene Publikation zu den Sicherheitsanforderungen und -eigenschaften von Messenger-Diensten aus Verbrauchersicht herausgegeben. Die BSI-Publikation beschreibt die grundlegenden Funktionsweisen von Messenger-Systemen und fokussiert dabei im Speziellen auf die Themen Verschlüsselung, Metadaten/Datenschutz und Interoperabilität.¹⁹

¹⁶ Gesetz über das Bundesamt für Sicherheit in der Informationstechnik v. 14.08.2009 (BGBl. I S. 2821), zuletzt geändert durch Art. 12 des G v. 23.06.2021 (BGBl. I S. 1982) – BSIG.

¹⁷ Das BSI hat u. a. ein umfangreiches Informationsangebot für Verbraucher und Unternehmen zu Fragen der digitalen Sicherheit entwickelt. Mit Fragen des Verbraucherschutzes im Digitalbereich ist das BSI ebenfalls befasst. Nach § 7 BSIG kann das BSI Warnungen aussprechen, falls Sicherheitslücken in informationstechnischen Produkten und Diensten bestehen. Nach § 7a BSIG können informationstechnische Produkte und Systeme durch das BSI untersucht werden, vgl. https://www.bsi.bund.de/DE/Das-BSI/Auftrag/auftrag_node.html, Stand: 1. September 2021.

¹⁸ Vgl. *Bundeskartellamt*, Pressemitteilung v. 22.01.2021, abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2021/22_01_2021_Zusammenarbeit_BSI_BKartA.html.

¹⁹ *BSI*, *Moderne Messenger – heute verschlüsselt, morgen interoperabel?*, November 2011, abrufbar unter: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html>.

C. Branchenüberblick Messenger- und Video-Dienste

Messenger- und Video-Dienste bieten eine Reihe von grundlegenden Kommunikationsdienstleistungen an. Die Verbraucher können nicht nur bilateral (1:1), sondern auch in Gruppen Textnachrichten austauschen, (per Video) telefonieren sowie Fotos, Videos, Sprachnachrichten und sonstige Dateien verschicken. Das Bundeskartellamt bezieht sich in dieser Sektoruntersuchung nicht nur auf den Austausch über Textnachrichten. Es hat sich zum Zwecke dieser Untersuchung für eine weite Definition von Messenger- und Video-Diensten entschieden. So wird der Begriff Messenger-Dienst als Sammelbegriff für offene und geschlossene Messaging-Systeme, Messenger-Clients und Multi Messenger verwendet, 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 welcher 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.

Die Gründe dafür liegen in der Entwicklung der Branche, wo viele individuelle Geschäftsmodelle und Anwendungen entstanden sind und ständig weiterentwickelt werden. Immer mehr Messenger- und Video-Dienste bieten ähnliche Funktionen an, wenn auch mit unterschiedlichen Schwerpunkten. Sogar die Grenzen zu Sozialen Netzwerken und Softwareanbietern erscheinen fließend. Schließlich können verbraucherrechtliche Versäumnisse alle Messenger- und Video-Dienste betreffen und sind nicht auf bestimmte Funktionen beschränkt.

Im Folgenden geht es zunächst darum, wie die Kommunikation über das Internet („Messaging“) funktioniert, was die Verbraucher dazu benötigen und welche Funktionen die Messenger- und Video-Dienste den Verbrauchern anbieten (hierzu unter I.). Anschließend wird kurz erläutert, in welchem Verhältnis Messenger- und Video-Dienste zu anderen Kommunikationsformen stehen (hierzu unter II.). Danach werden Kriterien für die Datensicherheit und den Datenschutz bei Messenger- und Video-Diensten beschrieben, die für die Verbraucher als Entscheidungshilfen bei der Auswahl eines Dienstes dienen können (siehe III.). Da die technische Entwicklung für die Untersuchungsthemen eine große Rolle spielt, wird auch dargelegt, wie offene Standards in der Branche entwickelt werden (hierzu unter IV.). Den Abschluss des Kapitels bilden erste Ermittlungsergebnisse zu den Branchenteilnehmern, zur Finanzierung, zu Nutzungszahlen und zur Wettbewerbssituation (hierzu unter V.).

I. Funktionsweise und Funktionen

Die Ursprünge des Messaging liegen im Chat, d. h. der elektronischen Kommunikation mittels geschriebenem Text in Echtzeit, meist über das Internet.²⁰ Das heutige Angebot der Messenger- und Video-Dienste geschieht auf Basis der gleichen Technik. Die Nutzer müssen zunächst eine Anwendersoftware (Client) auswählen und verwenden. Ein Client ist ein Programm oder eine Anwendung, welche(s) auf dem Endgerät eines Nutzers ausgeführt wird und über einen Server (Zentralrechner) kommuniziert. Viele Messenger-Apps können gleichermaßen auf mobilen und stationären Endgeräten, wie dem Smartphone oder dem Desktop-Computer, teils auch über den Internetbrowser verwendet werden.

In der Regel - falls ein Server verwendet wird - können Nachrichten auch abgeschickt werden, wenn der Gesprächspartner gerade nicht online ist; die Nachricht wird dann vom Server zwischengespeichert und später an den Empfänger ausgeliefert, wenn dieser wieder erreichbar ist.

Viele Messenger- und Video-Dienste unterstützen zusätzlich **Gruppenchats, Telefonie, Video-Telefonie und die Übertragung von Dateien sowie Audio- und Video-Streams**. Welche Funktionen im Einzelnen angeboten werden, kann je nach Messenger- und Video-Dienst variieren. Der Funktionsumfang wird maßgeblich beeinflusst von dem sog. Protokoll, das ein Messenger-Dienst verwendet. Das Protokoll kann auch als technische Sprache eines Messaging-Systems bezeichnet werden.

Unter den Messenger- und Video-Diensten sind die **Videokonferenzanbieter** diejenigen Dienste, die als Geschäftsschwerpunkt Videokonferenzen anbieten. Die Grenzen zu den verbraucherorientierten Diensten mit Schwerpunkt Messaging sind fließend. Meistens bieten Videokonferenzanbieter neben ihrem Kernangebot Videotelefonie/-konferenzen auch das Versenden von Textnachrichten an, wenn auch ggf. nur innerhalb bestimmter Apps für Geschäftskunden.²¹

Während der aktuellen **Covid-19 Pandemie** sind die Nutzerzahlen von Video-Diensten stark angestiegen. Dieser Effekt muss nicht kurzfristig sein. Im Zuge der Pandemie haben sich die Arbeitsorganisation und Trends in der Berufswelt, z. B. die verstärkte Einrichtung von Heimarbeitsplätzen, verändert. Die positiven Effekte haben nachhaltigen Eindruck hinterlassen. Auch daher dürfte zu erwarten sein, dass digitale Kommunikationsmethoden auch zukünftig von großem Interesse sein werden. Des Weiteren ist die teilweise fließende Abgrenzung zwischen

²⁰ Vgl. <https://de.wikipedia.org/wiki/Chat>, Stand: 11. September 2021.

²¹ Vgl. für weitere Messenger-Dienste mit dem Schwerpunkt auf Videokonferenzen z. B. *Gesellschaft für Datenschutz und Datensicherheit* (2020): GDD-Praxishilfe DS-GVO XVI – Videokonferenzen und Datenschutz, Anlage 1, abrufbar unter: <https://www.gdd.de/aktuelles/startseite/neue-praxishilfe-videokonferenzen-und-datenschutz-erschienen, Stand: 8. September 2020>.

vorwiegend privat oder geschäftlich genutzten Diensten bzw. Funktionalitäten für die Sektoruntersuchung nicht relevant. Datenschutzrechtliche Fragestellungen treten unabhängig davon auf. Das Bundeskartellamt hat gerade zu Beginn der Corona-Pandemie, als viele Verbraucher zunehmend über Videokonferenzen kommunizierten, von verschiedenen Seiten Anfragen erhalten, die Datenschutzprobleme bei Videokonferenzanbietern betreffen.

II. Verhältnis zu anderen Kommunikationsmitteln

Die hier betrachteten Kommunikationsmittel Messaging und Internettelefonie werden über das Internet, und damit „over-the-top“ (OTT), erbracht.²² OTT-Dienste können wiederum in unterschiedliche Kategorien unterteilt werden. Nach der Kategorisierung des Gremiums Europäischer Regulierungsstellen für elektronische Kommunikation (BEREC, Body of European Regulators for Electronic Communications) entsprechen Messenger-Dienste der Kategorie OTT-1-Dienste.²³ OTT-1-Dienste können zwar Sprachübertragungen über das Internet ermöglichen (Internettelefonie) und so in Konkurrenz zu klassischen Telefondiensten treten.²⁴ Sie sind aber unabhängig von Festnetz- oder Mobilfunkanschlüssen und erlauben daher keine Verbindung zu klassischen Telefondiensten mit sog. E.164-Rufnummern.

Auch wenn die Funktionen ähnlich sind, können Sprachtelefonie und SMS zumindest technisch von Messaging und Internettelefonie unterschieden werden. **Sprachtelefonie** bezeichnet die Sprachkommunikation über eine technische Vorrichtung. Die Übertragung geschieht entweder durch analoge oder digitale Telefondienste, wie ein Funknetz oder ein paketvermittelndes Datennetz.²⁵ **Short Message Service** (Kurznachrichtendienst, Abk. SMS) ist ein Telekommunikationsdienst, durch den Textnachrichten, die meist Kurzmitteilungen oder

²² Vgl. *Bundesnetzagentur* (2020), Nutzung von OTT-Kommunikationsdiensten in Deutschland, S. 5, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/OTT.pdf;jsessionid=227B4341DE126C64DDDBFEC85B4D5D62?_blob=publicationFile&v=5, S. 9 – 10, Stand: 24. August 2020.

²³ Vgl. *BEREC* (2016), Report on OTT Services, BoR (16), 35, S. 15 – 17. BEREC bildet drei Kategorien. Bei OTT-0 handelt es sich um Dienste, die Verbindungen zu klassischen Telefondiensten über mobile Rufnummern herstellen können. Messenger-Dienste zählen zu den sog. OTT 1-Diensten. Inhaltebasierte Anwendungen, die nicht hauptsächlich für die Kommunikation verwendet werden, werden als OTT-2-Dienste bezeichnet.

²⁴ *Body of European Regulators for Electronic Communications (BEREC)*, Report on OTT services, Januar 2016, S. 14 f., abrufbar unter: https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/5751-berec-report-on-ott-services_0.pdf.

²⁵ Vgl. <https://de.wikipedia.org/wiki/Telefonie>, Stand: 8. Oktober 2020.

ebenfalls SMS genannt werden, übertragen werden können.²⁶ SMS basiert auf der GSM²⁷-Technologie.

Anders als die rufnummernbasierten Sprachtelefonie und SMS sind Messenger-Dienste genauso wie **E-Mail** (Electronic Mail für „elektronische Post“) webbasiert und zählen zu den sog. OTT-1-Diensten. E-Mails sind briefähnliche Nachrichten, die über das Internet übertragen werden. Sowohl Textnachrichten als auch digitale Dokumente können in wenigen Sekunden an ihre Empfänger überall auf der Welt versendet werden. E-Mail ist ein offener Standard, den es seit 1968 gibt. Er basiert auf SMTP²⁸-, IMAP²⁹- und POP³⁰-Protokollen.³¹ Die verschiedenen E-Mail-Server sind über das E-Mail-Protokoll miteinander verknüpft, so dass Nachrichten zwischen verschiedenen Anbietern versendet werden können.³² Nutzer können bei beliebigen Anbietern ein Konto eröffnen. Datenschutzaspekte wurden und werden bis heute in Expertenkreisen hinsichtlich E-Mail in gleichem Ausmaß wie bei Messenger-Diensten thematisiert.

²⁶ SMS wurde zuerst für den GSM-Mobilfunk entwickelt und ist in verschiedenen Ländern auch im Festnetz als Festnetz-SMS verfügbar.

²⁷ GSM (Global System for Mobile Communications, Globales System für mobile Kommunikation) ist ein Mobilfunkstandard für volldigitale Mobilfunknetze, der hauptsächlich für Telefonie, aber auch für leitungsvermittelte und paketvermittelte Datenübertragung sowie Kurzmitteilungen (Short Messages) genutzt wird. Es ist der erste Standard der sog. zweiten Generation („2G“) als Nachfolger der analogen Systeme der ersten Generation, vgl. https://de.wikipedia.org/wiki/Global_System_for_Mobile_Communications, Stand: 8. September 2021.

²⁸ SMTP („Simple Mail Transfer Protocol“) ist ein Internetprotokoll, das zum Austausch von E-Mails in Computernetzen dient. Es wird dabei vorrangig zum Einspeisen und zum Weiterleiten von E-Mails verwendet, vgl. https://de.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol.

²⁹ IMAP („Internet Message Access Protocol“) ist ein Netzwerkprotokoll, das ein Netzwerkdateisystem für E-Mails bereitstellt. Über IMAP wird der komplette Inhalt des Email-Kontos eines Nutzers stets mit dem Mail-Programm auf dessen Computer oder Smartphone synchronisiert. Jegliche Ordner werden synchronisiert, so dass der Nutzer von allen Geräten den identischen Posteingang nutzen kann, vgl. https://de.wikipedia.org/wiki/Internet_Message_Access_Protocol.

³⁰ POP („Post Office Protocol“) ist ein Übertragungsprotokoll, über das ein Client E-Mails von einem E-Mail-Server abholen kann. Über die Version POP3 („Post Office Protocol Version 3“), werden lediglich die E-Mails aus dem Ordner des Posteingangs vom Server heruntergeladen. Das POP3-Verfahren dient nur zum simplen Download des Posteingangs. Eine Synchronisierung zwischen Endgerät und Email-Konto geschieht nicht, vgl. https://de.wikipedia.org/wiki/Post_Office_Protocol.

³¹ Vgl. *Wikipedia*, abrufbar unter: <https://de.wikipedia.org/wiki/E-Mail>, Stand: 8. Oktober 2020.

³² Vgl. *Kuketz*, Die verrückte Welt der Messenger – Teil 1, abrufbar unter: <https://www.kuketz-blog.de/die-verrueckte-welt-der-messenger-messenger-teil1/>, Stand: 7. Oktober 2020.

BEREC hat in die OTT-Kategorien auch **Soziale Netzwerke** eingeordnet. Soziale Netzwerke werden, genauso wie Streaming-Plattformen oder Suchmaschinen, als sog. OTT-2- oder „inhaltsbasierte“ OTT-Dienste kategorisiert.

In wettbewerbsrechtlichen Verfahren haben die Europäische Kommission und das Bundeskartellamt die Unterschiede zwischen Messenger-Diensten und Sozialen Netzwerken herausgearbeitet. Das Bundeskartellamt befand, dass bei Messenger-Diensten eine „[bilaterale] Kommunikation oder Gruppenkommunikation innerhalb kleinerer Gruppen“³³ stattfindet und die ausgetauschten Informationen typischerweise von begrenzter zeitlicher Relevanz seien. Die Definition der Europäischen Kommission umfasst mit dem Begriff „consumer communications app“ sehr ähnliche Anbieter, zieht aber zumindest eine Einbeziehung von E-Mail oder SMS in Betracht.³⁴ Es gebe jedoch sich deutlich unterscheidende Funktionalitäten zwischen sozialen Netzwerken und consumer communications apps.³⁵ In Kommunikationsnetzwerken kommunizieren typischerweise Nutzer miteinander, die sich bereits kennen, während in sozialen Netzwerken auch die mittelbare Kommunikation mit noch nicht bereits bekannten Personen möglich, bzw. vielmals sogar gewünscht, ist.³⁶

Für die Definition des betrachteten Wirtschaftszweigs in einer (verbraucherrechtlichen) Sektoruntersuchung ist eine Marktabgrenzung nach kartellrechtlichen Maßstäben nicht notwendig. Die Ermittlungsergebnisse vermitteln ohnehin den Eindruck, dass es gerade im US-amerikanischen Ausland und im asiatischen Raum Geschäftsmodelle gibt, in denen sich **inhaltsbasierte Dienstleistungen und Funktionen von typischen Messenger- und Video-Diensten mit Schwerpunkt Nachrichtenaustausch vermischen** und dass diese Entwicklung fortschreitet. Hier dürften im Zuge der weiteren Entwicklung ohnehin Veränderungen stattfinden.

³³ *Bundeskartellamt*, Beschluss vom 06.02.2019, B6-22/16, Rn. 290 – *Facebook*.

³⁴ *Europäische Kommission*, Entscheidung vom 03.10.2014, COMP/M 7217, Rn. 20 ff. – *Facebook/WhatsApp*.

³⁵ *Europäische Kommission*, Entscheidung vom 03.10.2014, COMP/M 7217, Rn. 61 – *Facebook/WhatsApp*.

³⁶ *Bundeskartellamt*, B6-113/15, Arbeitspapier – Marktmacht von Plattformen und Netzwerken, Juni 2016, S. 101.

Möglicherweise werden auch **Virtual Reality**³⁷ und **Augmented Reality**³⁸ in die Standardfunktionen von Messenger- und Video-Diensten sowie Sozialen Netzwerken aufrücken. Bei diesen neuen Funktionen kann sich der Nutzer mit Hilfsmitteln, wie z. B. den sog. VR-Brillen in Echtzeit - während er sich in seiner normalen Umgebung befindet - in künstlich erschaffene Welten begeben oder computergestützt relevante Zusatzinformationen abrufen. Im Unterschied zur Virtual Reality bleibt bei Augmented Reality das reale Umfeld erhalten und wird lediglich durch einzelne virtuelle Informationen ergänzt.

III. Kriterien für Datensicherheit und Datenschutz

Verbraucher, die sich für das Thema Datensicherheit bei Messenger- und Video-Diensten interessieren, können im Internet inzwischen auf zahlreiche Untersuchungen zu diesem Thema von Verbraucherverbänden, IT-Bloggern oder sonstigen informierten Kreisen zugreifen.³⁹ Die in diesen hilfreichen Untersuchungen präsentierten Ergebnisse sind größtenteils durch die Auswertung von Publikationen oder der Webseiten der einbezogenen Messenger- und Video-Dienste entstanden.

³⁷ „Virtuelle Realität“ (VR) bezeichnet ein digitales, am Computer geschaffenes Abbild der Realität. Eigene VR-Brillen lassen den Nutzer in eine neue, künstlich erschaffene Welt eintauchen, die täuschend echt wirkt. So kann er in Unterwasserwelten mit Walen schwimmen, ein Schiffswrack erkunden oder durch sein neues Haus laufen, bevor dieses gebaut wird, vgl. *Deutsche Telekom: Einfach erklärt – Augmented und virtuelle Realität*, abrufbar unter: <https://www.telekom.com/de/konzern/details/virtuelle-realitaet-486114> , Stand: 11. September 2021 oder Wikipedia, abrufbar unter: https://de.wikipedia.org/wiki/Virtuelle_Realit%C3%A4t , Stand: 23. Februar 2021.

³⁸ Unter der „Erweiterten Realität“ (AR) - im Englischen „Augmented Reality“ - wird hingegen das Zusammenspiel von digitalem und analogem Leben verstanden. Das kann über die Kamera des Smartphones oder wie meistens ebenfalls über eine Brille funktionieren. Wobei diese den Nutzer nicht komplett von seiner normalen Umgebung abschottet wie eine VR -Brille. Ihm werden vielmehr in die Brille zusätzliche Informationen über sein Umfeld eingeblendet. So kann beispielsweise einem Lagerarbeiter angezeigt werden, in welchem Regal das gesuchte Ersatzteil zu finden ist, oder dem Mechaniker nützliche Informationen über das technische Bauteil, das er reparieren soll, vgl. *Deutsche Telekom: Einfach erklärt – Augmented und virtuelle Realität*, abrufbar unter: <https://www.telekom.com/de/konzern/details/virtuelle-realitaet-486114> , Stand: 11. September 2021.

³⁹ Vgl. z. B. *Verbraucherzentrale NRW*, WhatsApp-Alternativen- Messenger im Vergleich, abrufbar unter: <https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-messenger-im-ueberblick-13055>, Stand: 28. Oktober 2021; *Mobilsicher*, Alles rund um Messenger, abrufbar unter: <https://mobilsicher.de/themenpakete/alles-rund-um-messenger>, Stand: 28. Oktober 2021; *Kuketz*, Messenger-Matrix, abrufbar unter: <https://www.kuketz-blog.de/messenger-matrix-uebersicht-vergleich-der-aktuellen-messenger/>, Stand: 28.10.2021; Initiative freie Messenger, Freie Messenger, abrufbar unter: <https://www.freie-messenger.de/>, Stand: 28. Oktober 2021.

Das Bundeskartellamt hat die Messenger- und Video-Dienste für diese Sektoruntersuchung direkt befragt. Den Themen Datensicherheit und Datenverarbeitung nach der EU-Datenschutzgrundverordnung (DSGVO)⁴⁰ hat es in seinem Fragebogen jeweils einen eigenen Abschnitt gewidmet. Beide Themen sind nicht nur für die Verbraucher wichtig, um selbständig einen sicheren Dienst auswählen zu können. Sie spielen auch für die rechtliche Analyse nach DSGVO und dem Gesetz gegen unlauteren Wettbewerb (UWG) eine Rolle. Die Ermittlungsergebnisse hierzu sind jedoch noch nicht Gegenstand dieses Zwischenberichts. Vielmehr wird sich das Bundeskartellamt im **Abschlussbericht** zu dieser Sektoruntersuchung zu den Themen Datensicherheit und Datenverarbeitung äußern. Nachfolgend werden lediglich einige zentrale Aspekte, die für das **Verständnis der Ermittlungsergebnisse** zur Interoperabilität wichtig sind, kurz vorgestellt. Für detailliertere Ausführungen sei auf die Publikation des BSI⁴¹ verwiesen, die zeitgleich zu diesem Zwischenpapier veröffentlicht worden ist.

1. Netzwerk, Protokolle und Server

Das Bundeskartellamt hat die Messenger- und Video-Dienste jeweils zu den Eigenschaften der von ihnen verwendeten Protokolle, insb. auch deren Überprüfbarkeit durch Dritte befragt. Protokolle können als die Sprache eines Messaging-Systems bezeichnet werden oder – technisch formuliert – als Regelsatz, nach welchem die Datenübertragung zwischen zwei oder mehreren Endpunkten der Kommunikation abläuft. Auswirkungen auf die Sicherheit der ausgetauschten Daten haben u.a. ferner die Struktur des Netzwerks der Messenger- und Video-Dienste und der Speicherort ihrer Daten.

Viele Messenger-Dienste benutzen eigene, proprietäre **Protokolle**, die von Dritten nicht oder nicht vollständig auf ihre jeweilige Funktionsweise getestet werden können. Diese sog. Proprietät ist nachteilig, wenn Nutzer nachvollziehen möchten, wie ihre Daten verarbeitet werden. Wenn Nutzer ihren Messenger nicht selber überprüfen können oder möchten, können **Zertifizierungen nach ISO** oder **Sicherheitsaudits** hilfreich sein, um die Datensicherheit zu belegen.

Den Einfluss des Diensteanbieters bestimmt auch nachhaltig die Netzwerkstruktur, d. h. ob ein Messenger-Dienst **zentral über einen bestimmten Server oder dezentral (föderal)** über ein

⁴⁰ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. EU L 119 v. 04.05.2016, S. 1 - DSGVO.

⁴¹ BSI, Moderne Messenger – heute verschlüsselt, morgen interoperabel?, November 2011, abrufbar unter: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html> .

Netzwerk unabhängiger Server organisiert ist. Bei zentraler Organisation gibt es einen Server, bei dem sich jeder Nutzer anmelden muss. Alle wesentlichen Entscheidungen liegen damit in der Hand des Diensteanbieters, wie es beispielsweise bei WhatsApp, Threema und Viber geschieht. Bei dezentraler Organisation, der sog. Föderation, werden die Server verschiedener Serverbetreiber miteinander verknüpft, ähnlich wie es bei E-Mail der Fall ist. Die Nutzer können miteinander kommunizieren, ohne von einem zentralen Anbieter abhängig zu sein. Föderation ermöglichen z. B. die beiden freien Protokolle XMPP und Matrix.⁴²

Ein weiterer Aspekt der Datensicherheit bei Messenger-Diensten ist der **Standort des Servers als Speicherort der Daten**, die bei Kommunikation anfallen. Die meisten Anbieter speichern diese auf eigenen Servern („hosted“). Andere Anbieter bieten sog. „on premises“-Versionen an, so dass Nutzer selbst einen Server betreiben können. Dabei verbleibt die gesamte Kommunikation auf dem Server des jeweiligen Nutzers (z. B. einer Organisation), ohne dass der Diensteanbieter die Daten verwaltet.

2. Verschlüsselung

Das Thema Verschlüsselung wird inzwischen in der allgemeinen Verbraucheröffentlichkeit intensiv diskutiert. Allerdings unterliegt die Verschlüsselung von Nachrichten bereits einem langen Entwicklungsprozess, der sich fortsetzt. In den 90er-Jahren wurden, z. B. beim Chat-Programm ICQ, Nachrichten noch unverschlüsselt versendet. Inzwischen wird bei der sog. **Transportverschlüsselung** die Nachricht zwar während ihres Transportweges verschlüsselt (verschlüsselter Kanal), liegt aber außerhalb des Übertragungsweges und an den Endpunkten unverschlüsselt vor, kann also sowohl vom Nutzer des Messenger-Dienstes selbst als auch vom Serverbetreiber eingesehen werden.

Anders als bei der Transportverschlüsselung wird bei der **Ende-zu-Ende-Verschlüsselung („E2E-Verschlüsselung“)** der Inhalt der Kommunikation über alle Übertragungsstationen hinweg verschlüsselt. Nur die Kommunikationspartner als Endpunkte der Kommunikation können die Daten entschlüsseln. Dabei wird die Public-Key-Verschlüsselung verwendet: Wenn z. B. Nutzer A die App seines Messenger-Dienstes startet, werden ein privater und ein öffentlicher Schlüssel generiert. Der private Schlüssel verbleibt auf dem Endgerät des Nutzers A. Der öffentliche Schlüssel wird auf dem Server hinterlegt für alle, die an A eine Nachricht verschicken wollen. Wenn Nutzer B an Nutzer A schreibt, wird seine Nachricht mit dem öffentlichen Schlüssel von A so verschlüsselt, dass nur A die Nachricht entschlüsseln und somit lesen kann. Das verschlüsselte Dokument wird über den Server zu A gesendet. A erhält das Dokument, welches

⁴² Vgl. *Kuketz*: Die verrückte Welt der Messenger – Teil 1, S. 5, abrufbar unter: <https://www.kuketz-blog.de/die-verrueckte-welt-der-messenger-messenger-teil1/>.

mit seinem privaten Schlüssel entschlüsselt wird. Der Inhalt der Nachricht kann somit nicht von Dritten, auch nicht von dem Messenger- und Video-Dienst selber gelesen werden.

Umgesetzt wird die Ende-zu-Ende-Verschlüsselung z. B. vom sog. **Double Ratchet Protokoll**⁴³ – häufig auch als Signal-Protokoll bezeichnet - welches von vielen Messenger-Diensten verwendet wird und als Stand der Technik gilt. Die Verschlüsselung von Nachrichten in Gruppen gilt allerdings noch als aufwendig und ist abhängig von der Gruppengröße komplex. Die Sicherheit der Kommunikation wird schließlich durch weitere **kryptographische Prinzipien und Eigenschaften** bestimmt, die auch das Double Ratchet Protokoll umsetzt. „Authentizität“ besagt, dass der Urheber von Daten oder der Absender einer Nachricht eindeutig identifizierbar und seine Urheberschaft nachprüfbar sein sollen. Zu nennen sind ferner z. B. die folgenden Eigenschaften kryptographischer Protokolle: „(Perfect) Forward Secrecy“ macht es unmöglich, durch die Kenntnis eines geheimen Haupt- oder Langzeitschlüssels einen Sitzungsschlüssel zu rekonstruieren. Eine aufgezeichnete verschlüsselte Kommunikation ist damit selbst bei der Kenntnis des Langzeitschlüssels nicht nachträglich zu entschlüsseln. „Backward Secrecy“ („Future Secrecy“, „Post-Compromise Security“) garantiert, dass verschlüsselte Nachrichten geheim bleiben, auch nachdem in der Vergangenheit ein Schlüssel kompromittiert wurde.⁴⁴ (Plausible) Deniability ermöglicht es, das Versenden einer Nachricht im Nachhinein glaubhaft abstreiten zu können.

Ein weiterer Sicherheitsaspekt in diesem Zusammenhang ist, ob eine Ablageverschlüsselung besteht. Ablageverschlüsselung (sog. Data at Rest) ist auf Daten gerichtet, die in irgendeiner Form im Speicher eines Computers/Endgeräts gespeichert sind. Der Nachrichtenverlauf auf dem Endgerät und ggf. bei Backups kann so vor unerwünschtem Zugriff geschützt werden.

Verschlüsselung allein reicht jedoch nicht aus, um die Kommunikation wirklich sicher zu machen. Die Echtheit des Kommunikationspartners bzw. seines Geräts und dessen Schlüssel kann durch ein **Verfahren der Authentifizierung** gesichert werden, was inzwischen als Stand der Technik gilt. Ein weiterer wichtiger Einflussfaktor einer sicheren Kommunikation ist die eindeutige Identifizierung des Nutzers gegenüber seinem Dienst, welche durch eine **Zwei-Faktor-Authentisierung** geschützt werden kann. Die Identität eines Nutzers wird so durch die

⁴³ Kryptographisches Protokoll für einen asynchronen (d.h. die Kommunikationspartner müssen nicht gleichzeitig online sein) Ende-zu-Ende-verschlüsselten Nachrichtenaustausch, siehe https://en.wikipedia.org/wiki/Double_Ratchet_Algorithm oder auch ausführlich *Signal: The Double Ratchet Algorithm*, abrufbar unter: <https://signal.org/docs/specifications/doubleratchet/>, beide Stand: 9. September 2021.

⁴⁴ Vgl. *Kuketz*, Die verrückte Welt der Messenger – Teil 1, S. 4, abrufbar unter: <https://www.kuketz-blog.de/die-verrueckte-welt-der-messenger-messenger-teil1/>, Stand: 7. Oktober 2020.

Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten, wie z. B. Passwort und Fingerabdruck, nachgewiesen.

Das Bundeskartellamt hat die Messenger- und Video-Diensten zu den genannten Aspekten befragt und wird im Abschlussbericht auf die diesbezüglichen Ermittlungsergebnisse eingehen.

3. Identifizierung und Umgang mit Kontakten

Messenger- und Video-Dienste verwenden verschiedene **Identifizierungsmerkmale**, anhand derer Nutzer eindeutig identifiziert und registriert werden können. Beispielsweise müssen Nutzer meistens die Telefonnummer oder die E-Mail-Adresse angeben, um den Dienst nutzen zu können. Nur bei wenigen Messenger- und Video-Diensten muss die Mobilfunknummer bisher nicht angegeben werden. In der Fachöffentlichkeit ist bekannt, dass zu diesen Diensten beispielsweise Threema, Wire, Conversations oder Element gehören. Threema vergibt an jeden Nutzer eine achtstellige ID. Wire kann mit Angabe einer E-Mail-Adresse genutzt werden. Conversations und Element, die auf Basis der Protokolle XMPP bzw. Matrix funktionieren, ordnen jedem Nutzer eine Chatadresse vergleichbar einer E-Mail-Adresse zu, über die kommuniziert werden kann.⁴⁵

Daran schließt sich die Frage an, wie mit den **Kontakten** der Nutzer umgegangen wird, d. h. ob auf das Kontaktverzeichnis bzw. Adressbuch des Nutzers zugegriffen wird. Der weit überwiegende Teil der Messenger-Dienste nutzt einen **Verzeichnisdienst**. Nicht nur die Telefonnummer des Nutzers selbst, auch die Telefonnummern aus seinem Adressbuch werden auf den Server hochgeladen und ggf. eingeblendet (Contact Discovery). So können auch Telefonnummern von Nutzern auf die Server der Anbieter gelangen, die bei dem jeweiligen Dienst nicht registriert sind und in die AGB nicht eingewilligt haben.

Nicht nur für die Verbraucher selbst, sondern auch für eine datenschutzrechtliche Bewertung von Messenger- und Video-Diensten ist die Frage, wie mit den Daten, insb. zur Identität der Nutzer und ihrer Kontaktpersonen umgegangen wird, besonders wichtig. Das Bundeskartellamt hat daher Auskünfte verlangt, welche Voraussetzungen die Nutzer erfüllen müssen, um den jeweiligen Dienst nutzen zu können und wird im Abschlussbericht auf die diesbezüglichen Ermittlungsergebnisse eingehen.

⁴⁵ Vgl. *Kuketz*, Die verrückte Welt der Messenger – Teil 1, S. 7, abrufbar unter: <https://www.kuketz-blog.de/die-verrueckte-welt-der-messenger-messenger-teil1/>, Stand: 7. Oktober 2020.

4. Umgang mit Metadaten

Ein wesentlicher Teil der Ermittlungen des Bundeskartellamts war auf die Datenverarbeitung der Messenger- und Video-Dienste gerichtet. Dabei geht es darum, wie und warum Daten erfasst, wo sie gespeichert, an wen sie weitergegeben, ob und wann sie gelöscht werden sowie ob die Praktiken der Dienste den rechtlichen Vorgaben – der europäischen DSGVO - entsprechen. Wie bereits erwähnt, wird das Bundeskartellamt im Abschlussbericht nähere Ausführungen dazu machen. Vorab soll kurz auf die sog. **Metadaten** hingewiesen werden, da diesen aus verbraucherrechtlicher Perspektive eine besondere Bedeutung zukommt.

Metadaten können von Messenger- und Video-Diensten genutzt werden, um die Funktionsweise des Dienstes zu verbessern. Sie können aber auch dazu dienen, Nutzerprofile anzulegen oder personalisierte Werbung zu platzieren. Es gibt Stimmen, wonach Messenger-Dienste wie WhatsApp und Telegram mehr Metadaten sammeln als für den eigentlichen Betrieb erforderlich sind.⁴⁶

Metadaten sind strukturierte Daten, die Informationen über Merkmale anderer Daten enthalten.⁴⁷ Sie umfassen beispielsweise Informationen darüber, wann jemand online ist und wie viele Geräte er verwendet, welche Kontakte bestehen und welche IP-Adressen diese haben.⁴⁸

Bei der Kommunikation über Messenger- und Video-Dienste fallen immer **Metadaten** an. Sollen diese vertraulich bleiben und nicht auf Servern gespeichert werden, müssten sich die Teilnehmer direkt miteinander verbinden und eben keinen Server nutzen (ein Beispiel dafür ist das System Briar⁴⁹). Wie das BSI ausführt, werden von datensparsamen Diensten so wenig Metadaten wie möglich erfasst und gespeichert. Allerdings dürfte es für den Großteil der Verbraucher nicht leicht sein, solche Dienste zu erkennen. Das BSI erläutert in seiner Publikation, inwieweit ein

⁴⁶ Vgl. z. B. *Kuketz*, Datenschutzfreundliche und sichere WhatsApp-Alternativen, abrufbar unter: <https://www.kuketz-blog.de/datenschutzfreundliche-und-sichere-whatsapp-alternativen/>, Stand: 14. September 2021 sowie <https://netzpolitik.org/2021/metadaten-wo-das-eigentliche-privacy-problem-von-whatsapp-liegt/>, Stand: 14. September 2021 oder <https://www.ionos.de/digitalguide/online-marketing/social-media/whatsapp-alternativen/>, Stand: 14. September 2021.

⁴⁷ Vgl. *Wikipedia*, abrufbar unter: <https://de.wikipedia.org/wiki/Metadaten>, Stand: 7. Oktober 2020.

⁴⁸ Vgl. z. B. *Initiative freie Messenger*, <https://www.freie-messenger.de/geheimnisse/privat/>, Stand: 14. September 2021.

⁴⁹ Vgl. <https://briarproject.org/>, Stand: 8. September 2021.

einsehbarer Source Code und Informationen über den Standort des Servers (insb. innerhalb oder außerhalb der EU) dabei hilfreich sein können.⁵⁰

Auch das **Löschen** der Daten wird in der Branche nicht einheitlich gehandhabt. Bei datenschutzorientierten Diensten geschieht dies den Ermittlungen zufolge sofort, bei anderen Diensten kann es mehrere Monate dauern. Ein wesentlicher Aspekt von sicheren Messenger-Diensten vor diesem Hintergrund ist nach Angaben des BSI, dass z. B. in der **Datenschutzerklärung** beschrieben wird, in welchem Umfang Metadaten erfasst und wann sie gelöscht werden. Datensparsame Messenger wären so konzipiert, dass so wenig Metadaten wie möglich anfallen und erfasst werden und diese auch zeitnah gelöscht werden. Auch wo die Daten in der Zwischenzeit gespeichert werden, kann einen Unterschied machen, da die Datenschutzgesetze weltweit unterschiedlich sind⁵¹ und die europäische DSGVO hier im Vergleich zu anderen Jurisdiktionen hohe Maßstäbe ansetzt.

Allerdings beeinflusst auch die **Einbindung in das Betriebssystem**, was mit den Metadaten geschieht. Selbst wenn Metadaten seitens des Dienstes zeitnah gelöscht werden, können diese gleichwohl durch das Betriebssystem des Endgeräts, bei Mobilgeräten und insb. Smartphones, also typischerweise iOS/iPadOS (Apple) bzw. Android (Google), gespeichert werden. Dies ist z. B. der Fall, wenn Push-Nachrichten, die den Eingang einer neuen Nachricht anzeigen, gesendet werden.

IV. Verfahren der Standardisierung

Messenger- und Video-Dienste funktionieren auf Basis von (Kommunikations-) Protokollen⁵² und weiterer technischer Komponenten. Entsprechend der Bedeutung technischer Funktionalitäten verfügt die Branche über eine gewisse technische Selbstorganisation durch **international anerkannte Standardisierungsorganisationen**. Dazu zählt an erster Stelle die **Internet Engineering Task Force (IETF)**, deren Schwerpunkt auf der Standardisierung der im Internet eingesetzten Kommunikationsprotokolle liegt. Standardisierungsprozesse erlangen auch dann

⁵⁰ Vgl. BSI, Moderne Messenger – heute verschlüsselt, morgen interoperabel?, November 2011, abrufbar unter: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html> .

⁵¹ Vgl. BSI, Moderne Messenger – heute verschlüsselt, morgen interoperabel?, November 2011, abrufbar unter: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html> .

⁵² Kommunikationsprotokolle definieren die Regeln für die Datenübertragung zwischen den Endpunkten der Kommunikation. Sie sind quasi die Sprache eines Messaging-Systems, mittels der die verschiedenen Einheiten des technischen Systems miteinander kommunizieren.

Bedeutung für die Branche der Messenger- und Video-Dienste, wenn Interoperabilität über Standards umgesetzt würde. Demzufolge hat das Bundeskartellamt die Branche zu Aspekten der Standardisierung befragt. Die befragten Unternehmen wiederum haben sich entsprechend häufig in ihren Antworten auf Standardisierungsverfahren mit ihren Vor- und Nachteilen bezogen.

Unter den internationalen Institutionen, die für die Branche bei Standardisierungsverfahren relevant sind, wurde die IETF in der Sektoruntersuchung am häufigsten erwähnt. Es handelt sich um eine offene, internationale Freiwilligenvereinigung von Netzwerktechnikern, Herstellern, Netzbetreibern, Forschern und Anwendern, die sich mit der technischen Weiterentwicklung des Internets befasst, um dessen Funktionsweise zu verbessern.⁵³

Auch auf das W3C wurde seitens der befragten Unternehmen mehrfach hingewiesen. Das **World Wide Web Consortium (W3C)** ist eine Mitgliedsorganisation zur Standardisierung der Techniken im World Wide Web.⁵⁴ Einige Befragte wiesen darauf hin, dass die W3C maßgeblich den **WebRTC-Standard** entwickelt habe. Dabei handelt es sich um einen offenen Standard, der eine Sammlung von Kommunikationsprotokollen und Programmierschnittstellen (API) definiert, die Echtzeitkommunikation über Rechner-Rechner-Verbindungen ermöglichen. Anwendungen wie Videokonferenzen, Dateitransfers bzw. Datenübertragungen, Chat und Screen Sharing können so funktionieren.⁵⁵

Daneben existieren weitere Standardisierungsgremien, wie z. B. die XSF (XMPP Standards Foundation) als gemeinnützige Stiftung, die das XMPP-Protokoll spezifiziert und weiterentwickelt.

Das **Verfahren bei der IETF** beginnt mit Vorschlägen aus der Industrie, die in einem ersten Treffen (sog. Birds of a Feather session, BoFs) während eines der drei jährlichen IETF-Meetings besprochen werden. Wird das Thema weiterverfolgt, wird eine Arbeitsgruppe („Working Group“) gebildet. Ist irgendwann ein Konsens über ein Entwurfspapier erreicht, nähert sich ein Entwurf langsam einem so genannten „Draft“. Dabei handelt es sich um eine frühe Fassung eines möglichen Standards, der nun auch außerhalb der eigentlichen Working Group diskutiert werden kann und soll. Das kann in Veranstaltungen im Rahmen von IETF-Treffen, anderen Branchentreffen oder über Veröffentlichungen für die Internet-Community geschehen.⁵⁶

⁵³ <https://www.ietf.org/about/>, Stand: 2. September 2021, vgl. https://de.wikipedia.org/wiki/Internet_Engineering_Task_Force, Stand: 2. September 2021.

⁵⁴ Vgl. <https://www.w3.org/>, Stand: 2. September 2021, vgl. https://de.wikipedia.org/wiki/World_Wide_Web_Consortium, Stand: 2. September 2021 und weitere öffentlich verfügbare Quellen.

⁵⁵ Vgl. <https://webrtc.org/>, Stand: 2. September 2021, <https://en.wikipedia.org/wiki/WebRTC>, Stand: 2. September 2021.

⁵⁶ Vgl. <https://www.netplanet.org/organisation/standardisierung.shtml>, Stand: 3. September 2021.

Drafts und später auch der fertige Standard werden als **RFC (Request for Comments)** veröffentlicht. Die RFC-Dokumente bilden eine anschauliche Grundlage für Standardisierungsvorgänge und die Entwicklung der Netzwerktechnologien im Internet. Verwaltet wird die Herausgabe von RFC durch den so genannten RFC Editor. Dies ist eine unabhängige Stelle, die von der Internet Society⁵⁷ finanziert wird.

In der Fachöffentlichkeit wird immer wieder diskutiert, inwieweit Arbeitsgruppen der IETF von Interessen großer Unternehmen geprägt sind. Geäußert wird einerseits, gerade die Offenheit der Standardisierungsarbeit könne zum Problem werden, wenn Großunternehmen zahlreiche angestellte Entwickler entsenden, um so die Entscheidungsfindung in einer Working Group zu beeinflussen.⁵⁸ Ziel könnte die Verbreitung eigener Software-Patente über den jeweiligen Standard (sog. **Standardessentielle Patente**, SEP, standard essential patents) sein.⁵⁹ Andererseits finden sich Berichte, z. B. über das Scheitern von China, in der IETF ein neues Internetprotokoll durchzusetzen, weil es an den „Grundprinzipien des Internets wie Anonymität und Gleichrangigkeit von Datenverkehren“⁶⁰ rüttelt.

Grundsätzlich verabschieden Standardisierungsorganisationen interne Regelwerke zum Umgang mit geschützten Technologien. Dies gilt auch für die IETF. Auch wenn diese Regelwerke unterschiedlich gestaltet sind, teilen sie meist zwei Elemente. Teilnehmer der Working Groups werden zum einen aufgefordert, standardessentielle Patente offenzulegen. Allerdings werden weder Mitglieder noch die Organisation selbst nach relevanten Patenten suchen oder bei

⁵⁷ Die Internet Society (ISOC; deutsch Internet-Verband) wurde 1992 auf der INET-Konferenz in Kōbe (Japan) gegründet und ist als Nichtregierungsorganisation für die Pflege und Weiterentwicklung der Internetinfrastruktur zuständig, abrufbar unter: https://de.wikipedia.org/wiki/Internet_Society, Stand: 10. September 2021.

⁵⁸ Vgl. in diesem Zusammenhang den Bericht über die Suche nach einheitlichen Spam-Maßnahmen, während der Microsoft seinen eigenen Standard als Grundlage des offenen Standards positionieren wollte, abrufbar unter: <https://www.netplanet.org/organisation/standardisierung.shtml>, Stand: 3. September 2021.

⁵⁹ Vgl. für eine detaillierte Erörterung des Themas z. B. *Max-Planck-Institut für Innovation und Wettbewerb* (2015): Standardessentielle Patente: Die Rolle von Standardisierungsorganisationen, Forschungsbericht 2015, abrufbar unter: https://www.mpg.de/9853703/jb_20151, Stand: 7. September 2021.

⁶⁰ *Wirtschaftswoche* vom 4. Mai 2020: Brummen fürs Internet, abrufbar unter: <https://www.wiwo.de/technologie/digitale-welt/web-standards-brummen-fuers-internet/25779644.html>, Stand: 3. September 2021.

offengelegten Patenten prüfen, inwieweit sie für den Standard wesentlich sind.⁶¹ Zum anderen wird die Deklaration von SEPs an die Selbstverpflichtung des Patentinhabers gekoppelt, Lizenzen zu fairen, zumutbaren und diskriminierungsfreien Bedingungen (sog. FRAND-Prinzip, fair, reasonable and non-discriminatory,) zu erteilen.⁶²

Dieses Verfahren der Entwicklung offener Standards über Standardisierungsorganisationen berührt auch die Fragestellungen der Sektoruntersuchung. Derzeit befindet sich ein Standard in Entwicklung, der eine umfassendere Verschlüsselung beim Austausch in Gruppen möglich machen soll. Im Einzelnen geht es um eine Sicherheitsschicht für die Ende-zu-Ende-Verschlüsselung von Nachrichten in kleinen und großen Gruppen (sog. **Messaging Layer Security**⁶³). Nach öffentlichen Angaben hat das BoFs im Februar 2018 in London stattgefunden. Die Gründungsmitglieder waren danach Mozilla, Facebook, Wire, Google, Twitter, University of Oxford und das französische Nationale Forschungsinstitut für Informatik und Automatisierung (INRIA).

V. Erste Ermittlungsergebnisse zur Branche

Die Branche der Messenger- und Video-Dienste ist vielfältig, so dass sich mögliche Maßnahmen und rechtliche Vorschriften auf die betroffenen Unternehmen unterschiedlich auswirken werden. Insofern sind Kenntnisse über die Anbieterseite unerlässlich, um die Ermittlungsergebnisse richtig interpretieren sowie später mögliche Verbraucherrechtsverstöße bewerten und zielgerichtete Handlungsempfehlungen formulieren zu können. Darüber hinaus ermöglicht eine breitere Darstellung der Branche den Verbrauchern eine gute Orientierung und Information über mögliche Alternativen jenseits der allgemein bekannten, großen Dienste.

⁶¹ Vgl. *Max-Planck-Institut für Innovation und Wettbewerb* (2015): Standardessentielle Patente: Die Rolle von Standardisierungsorganisationen, Forschungsbericht 2015, abrufbar unter: https://www.mpg.de/9853703/jb_20151, Stand: 7. September 2021.

⁶² Vgl. *Max-Planck-Institut für Innovation und Wettbewerb* (2015): Standardessentielle Patente: Die Rolle von Standardisierungsorganisationen, Forschungsbericht 2015, abrufbar unter: https://www.mpg.de/9853703/jb_20151, Stand: 7. September 2021 sowie *IETF* (2017): At Long Last, A Revised Patent Policy for IETF: What's Behind BCP79bis?, abrufbar unter: <https://www.ietf.org/blog/whats-behind-bcp79bis/> oder : <https://www.ietf.org/standards/ipr/>, Stand: 7. September 2021.

⁶³ Vgl. <https://datatracker.ietf.org/wg/mls/about/>, Stand: 2. September 2021, vgl. https://de.wikipedia.org/wiki/Messaging_Layer_Security, Stand: 2. September 2021.

1. Branchenteilnehmer, Funktionen und Geschäftsmodelle im Überblick

Aus den Vorgesprächen zur Sektoruntersuchung hatte das Bundeskartellamt bereits den Eindruck gewonnen, dass die Branche äußerst heterogen ist. Die Ermittlungen bestätigen dies und zeichnen ein deutliches Bild der Vielfalt der Marktteilnehmer. Hinter Messaging- und Video-Diensten steht eine große Industrie mit verschiedensten Geschäftsfeldern und ein weites Feld an nicht kommerziellen Anwendungen.

Was die **geographische Reichweite** angeht, könnte die Skala nicht größer sein. Zum einen finden sich weltweit tätige, diversifizierte Technologiekonzerne und global agierende Digitalkonzerne wie Cisco mit dem Videoconferencier Webex, Facebook mit WhatsApp und Facebook Messenger, Google mit Google Meet, Microsoft mit Microsoft Teams und Skype und auch Unternehmen wie die japanische Line Corporation, die zur südkoreanischen Naver Corporation gehört. Naver betreibt eine Suchmaschine, die in einigen Regionen stark nachgefragt wird, ein E-Mail-System und bietet digitale Auskünfte an. Es handelt sich bei diesen Diensten somit um ein Geschäft, das weltweit stattfindet. Zum anderen sind auch regional bzw. nationale Anbieter, Nischenanbieter, wie z. B. Univado (E-Learning) oder in der allgemeinen Öffentlichkeit weniger bekannte Messenger- und Video-Dienste wie Ginlo in dieser Branche aktiv.

Außerdem existiert ein weiterer **Open Source-Bereich**, zu dem Anbieter gehören, deren Geschäftsmodell Interoperabilität ist, sowie die große Welt der freien, d. h. von zentralen Providern unabhängigen Messaging-Systeme. Letztere umfasst das seit langer Zeit existierende Protokoll XMPP mit einer festen Community sowie Matrix und Systeme, die auf den für E-Mail genutzten Protokollen IMAP und SMTP basieren. Diese Dienste sind für die Verbraucher grundsätzlich unentgeltlich.

Die Heterogenität spiegelt sich auch in der technischen Struktur wider. Nach der **technischen Integration/Tiefe** ist zwischen Systemen und Clients zu unterscheiden. Ein Messaging- oder Video-**System** umfasst alle Elemente, die zum Messaging oder für Videokonferenzen benötigt werden. Es besteht aus dem Kommunikationsprotokoll, Serversoftware, Hardware und der Anwendersoftware (App, Client). Bei den sog. **Clients oder Apps** handelt es sich um ein Programm, welches auf dem Endgerät eines Netzwerks ausgeführt wird und mit einem Server (Zentralrechner) kommuniziert. Unter den Clients entsprechen die sog. **Multi (Protokoll-)Messenger** einer Software, die eine Vielzahl von Kommunikationsprotokollen beherrscht und Nutzern ermöglicht, verschiedene Messenger-Systeme über eine Softwareoberfläche zu bedienen. Ein systemübergreifender Nachrichtenaustausch ist aber nicht möglich. Auch unterstützen Multi Messenger die Funktionsmöglichkeiten, die das jeweilige Protokoll bietet, oft nicht vollständig.

Nach der **Unabhängigkeit von einem zentralen Diensteanbieter** können sog. geschlossene von freien Systemen unterschieden werden.

Bei **geschlossenen Systemen** werden alle Elemente und Eigenschaften des Systems, insb. der Client und die Server, über die Daten ausgetauscht und gespeichert geben, vom Anbieter vorgegeben.

Freie Messenger-Systeme funktionieren ähnlich wie E-Mail-Dienste. Sie fußen technisch auf einem Standardprotokoll (meist XMPP oder Matrix), so dass die Nutzer Nachrichten über verschiedene Messenger-Clients hinweg austauschen können. Gesprächspartner müssen also nicht die gleiche App installiert haben, um miteinander zu kommunizieren. Einen alles bestimmenden Diensteanbieter gibt es nicht. Es handelt sich um föderierte Systeme, die über dezentrale Serverstrukturen verfügen. Damit geht einher, dass es im Allgemeinen keine zentrale Datenspeicherung gibt. Nutzer entscheiden sich für einen Serverbetreiber, der ihre Präferenzen am besten umsetzt. Sie können ferner zwischen verschiedenen Clients für verschiedene Betriebssysteme wählen und sich für denjenigen entscheiden, der am besten Ihren Anforderungen entspricht.

Die bekanntesten und am weitesten verbreiteten, freien Messaging-Systeme sind Matrix, XMPP und Systeme, die die für E-Mail genutzten Protokolle verwenden.

XMPP (Jabber) ist ein föderales, dezentrales System. Um damit chatten zu können, muss ein Nutzerkonto bei einem beliebigen Server vorhanden oder angelegt sein. Nutzer können ihren eigenen Server betreiben. Hierfür sind jedoch ein gewisses technisches Verständnis und Engagement erforderlich. Deshalb gibt es sehr viele verschiedene öffentliche Anbieter, auf deren Server dann die Verwaltung von Konten, Adressbüchern und Chatverläufen der Nutzer für ggfs. mehrere Geräte erfolgen kann. Für XMPP existiert ein Standardisierungsgremium, die XMPP Standards Foundation (XSF). Bei XMPP gibt es viele versteckte Anwendergruppen mit geschätzt mehreren Millionen Nutzern. Dazu zählen z. B. Betreiber von Online-Spielen. Nach Angaben der Community wird XMPP von der NATO genutzt und auch bei der Bundespolizei getestet.⁶⁴ Auf Basis von XMPP hat auch WhatsApp ursprünglich sein geschlossenes Protokoll entwickelt.

Das Bundeskartellamt hat unter den XMPP-Clients Antworten von Conversations, Quicksy und Yaxim (alle für Android), für Apples iOS von Monal sowie für Linux von Gajim, Dino und Profanity erhalten.

Matrix wird seit 2014 entwickelt. Das System ist aktuell nicht als Internetstandard durch die IETF (Internet Engineering Task Force) definiert. Das Protokoll ist monolithisch („aus einem Guss“)

⁶⁴ Vgl. für eine ausführliche Darstellung *Initiative freie Messenger*, <https://www.freie-messenger.de/einfuehrung/>, Stand: 8. September 2021.

angelegt und besteht nicht aus unterschiedlichen oder erweiterbaren Modulen. Bei neuen oder veränderten Anforderungen wird es als Einheit geändert oder auch ergänzt. Für Matrix wurde der wohl bekannteste Client Element in die Untersuchung einbezogen. Matrix wird nach Angaben von Element an vielen deutschen Universitäten und der BWI⁶⁵ - dem IT-Systemhaus der Bundeswehr - eingesetzt.⁶⁶

E-Mail als Messaging-System zeichnet sich durch eine große Erreichbarkeit aus. Jeder Nutzer kann mit beliebiger E-Mail-Adresse kommunizieren, ohne dass der Empfänger das gleiche oder ein spezielles Messenger-Programm benötigt. Der Messenger-Client funktioniert hier wie ein klassischer Messenger, nutzt jedoch die bewährte E-Mail-Infrastruktur, u. a. mit den standardisierten und offenen Protokollen IMAP⁶⁷ und SMTP⁶⁸.⁶⁹ Das System E-Mail ist in der Sektoruntersuchung durch den Client „Delta Chat“ vertreten. Darüber hinaus gibt es weitere freie Messenger-Systeme wie Goldbug, Mattermost u. v. a. mehr.

Messenger- und Video-Dienste bieten jeweils ein weitgehend individuelles **Portfolio verschiedener Funktionen** an. Das Bundeskartellamt hat die Dienste im Rahmen der Sektoruntersuchung gefragt, welche wesentlichen Funktionen (hier: Versand von Textnachrichten, Telefonie, Videotelefonie und Versand von Dateien) die Verbraucher bei ihrem Dienst nutzen können und seit wann das Angebot besteht. Jeweils mehr als 30 der befragten Messenger- und Video-Dienste haben geantwortet, dass Nutzer über ihren Dienst Textnachrichten versenden, telefonieren, sich per Videotelefonie austauschen bzw. Dateien versenden können. Bei einzelnen Befragten aus dieser Gruppe können Verbraucher sich per Telefonie und Videotelefonie allerdings nur bilateral austauschen, nicht in Gruppen. Die Ermittlungsergebnisse zeigen ferner, dass die ersten Funktionen bereits ab dem Jahr 2000 angeboten wurden. Bis heute sind danach kontinuierlich immer mehr Dienste und immer mehr

⁶⁵ Die Abkürzung stand früher für Bundes-Wehr und Industrie, wird heute so aber nicht mehr verwendet, vgl. *BWI*, abrufbar unter: <https://www.bwi.de/das-macht-die-bwi>, Stand: 14. September 2021.

⁶⁶ Für weitere Einzelheiten siehe *Initiative freie Messenger*, https://www.freie-messenger.de/sys_matrix/, Stand: 17. August 2021.

⁶⁷ Das Internet Message Access Protocol (IMAP) ist ein Netzwerkprotokoll, das ein Netzwerkdateisystem für E-Mails bereitstellt, vgl. *Wikipedia*, https://de.wikipedia.org/wiki/Internet_Message_Access_Protocol, Stand: 8. September 2021.

⁶⁸ Das Simple Mail Transfer Protocol (SMTP) ist ein Protokoll der Internetprotokollfamilie, das zum Austausch von E-Mails in Computernetzen dient. Es wird dabei vorrangig zum Einspeisen und zum Weiterleiten von E-Mails verwendet, vgl. *Wikipedia*, https://de.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol, Stand: 8. September 2021.

⁶⁹ Vgl. für detaillierte Ausführungen *Initiative freie Messenger*, https://www.freie-messenger.de/sys_matrix/, Stand: 8. September 2021.

Funktionen hinzugekommen. Viele Dienste haben den Versand von Textnachrichten und Dateien einige Jahre früher angeboten als Telefonie und Videotelefonie. In einzelnen Fällen ist auch erkennbar, dass der Austausch in einer Gruppe erst später möglich war als die Kommunikation mit einem einzigen Gesprächspartner.

Die Mehrheit der Messenger- und Video-Dienste bietet somit alle wesentlichen **Funktionen** an, auch wenn teilweise Schwerpunkte auf einzelnen Leistungen liegen, wie z. B. Messaging bei WhatsApp oder Videoconferencing bei Webex, Zoom und Microsoft Teams. So ist die Messaging-Funktion bei vielen Anbietern von Videokonferenzen nur ein Teil der Videofunktion. Ein eigenständiger Chat-Dienst wird oft nicht betrieben. Einige Befragte haben auch darauf hingewiesen, dass ihnen nicht bekannt ist, ob die Nutzer den Dienst z. B. als Telefonkonferenz oder Videokonferenz nutzen, da Letzteres sich nur durch Einschaltung der Kamera unterscheidet.

Daraus ergeben sich unzählige **Geschäftsmodelle**. Neben den Schwerpunkten Messaging oder Videoconferencing verstehen sich Plattformen mit Messaging-Funktionen teils eher als Soziale Netzwerke bzw. Social Media- Plattformen (Facebook Messenger, Discord, We Chat) oder als Dienste für Kommunikation und Zusammenarbeit (z. B. Slack, Rocket.chat). Auch Software-Anbieter und Entwickler spezieller Software (z. B. Fastviewer), die Hilfe zur Selbsthilfe bieten, also Unternehmen beim Betrieb eines eigenen Kommunikations- bzw. Video-Systems unterstützen und z. B. auch Hosting-Dienstleistungen bieten, sind hier zu nennen. Auch diese über den Kern des Messaging und des Videoconferencing hinausgehenden Dienste wurden der Branche für die Zwecke der Sektoruntersuchung zugerechnet (ohne dass dies eine kartellrechtliche Marktabgrenzung ersetzen soll).

Unterschieden werden kann noch danach, ob ein Messenger- und Video-Dienst seinen Schwerpunkt auf **private oder geschäftliche Kunden** legt. Viele Video-Dienste beispielsweise haben gegenüber dem Bundeskartellamt deutlich gemacht, dass sie zwar auch ein begrenztes unentgeltliches Angebot bereitstellen, ihre Produkte aber hauptsächlich gegen Entgelt Geschäftskunden anbieten. Das Verhältnis von privat zu geschäftlich in der eigenen Nutzerbasis zu quantifizieren ist den meisten Branchenakteuren nach eigenen Angaben allerdings nicht genau möglich. So hat hierzu eine größere Zahl der Befragten erläutert, dass sie die Unterscheidung zwischen geschäftlicher bzw. privater Nutzung nicht erfassen (können), u. a. weil sie ein Tracking ihrer Nutzer grundsätzlich ablehnen oder weil diese Informationen ausschließlich dem jeweiligen Diensteanbieter bzw. Serverbetreiber bekannt sind.

Von den Diensten, die Angaben gemacht oder diese geschätzt haben, hat jeweils rd. ein Drittel angegeben, dass ihr Dienst ausschließlich oder nahezu ausschließlich geschäftlich, ausschließlich oder nahezu ausschließlich privat oder sowohl geschäftlich als auch privat genutzt wird.

Nicht alle Messenger- und Video-Dienste können mit jeder Art **Endgerät und Betriebssystem** verwendet werden. 38 Befragte haben angegeben, dass ihr Dienst mit Desktop/Notebook/Laptop bzw. mit Smartphone/Tablet genutzt werden kann. Über einen Webbrowser können nach eigenen Angaben nur 16 der befragten Dienste verwendet werden. Zu den nutzbaren Browsern gehören Safari, Firefox, Google Chrome, Internet Explorer, Microsoft Edge und Opera.

Jeweils mehr als 30 der befragten Messenger- und Video-Dienste haben erklärt, dass sie mit den Betriebssystemen Android, iOS/macOS (Apple) bzw. Windows anwendbar sind. Mehr als 20 Befragte haben angegeben, dass ihr Dienst mit Linux genutzt werden kann. Bei den Diensten, die nicht mit einem oder mehreren der großen Betriebssysteme anwendbar sind, handelt es sich im Wesentlichen um freie Messenger Clients. Diese basieren auf einem bestimmten Messaging System, wie z. B. XMPP oder Matrix. Verbraucher können hier aus einer großen Anzahl verfügbarer Clients eines Systems diejenige Anwendung auswählen, die ihren Bedürfnissen, z. B. ein bestimmtes Betriebssystem zu nutzen, am besten entspricht.

2. Finanzierung und Umsätze

Die Fragen zu Finanzierung und Umsätzen haben jeweils nur rund zwei Drittel der Dienste beantwortet. Darüber hinaus konnte im Rahmen der Sektoruntersuchung die Angaben zu Umsätzen und Finanzierungsquellen nicht überprüft werden.

Messenger- bzw. Video-Dienste finanzieren sich nach den Ermittlungen am häufigsten aus **Entgelten für Basisdienste** und Einnahmen aus **Entgelten für Zusatzdienste**. Bei den meisten Diensten machten diese Finanzierungsquellen jeweils 100 % der Einnahmen aus. Drei Dienste haben angegeben, sich vollständig bzw. überwiegend über Werbung zu finanzieren. Zwei andere Branchenteilnehmer erzielen ihre Einnahmen überwiegend über den Verkauf ihrer App. Zwei freie Messenger-Clients haben angegeben, sich überwiegend über Spenden zu finanzieren.

Auffällig ist, dass keiner der befragten Dienste Einnahmen aus Datennutzung/ -weitergabe für **personalisierte Werbung** als Einnahmequelle genannt hat, obwohl diese Antwortoption explizit vorgegeben war.

Bei den **Netto-Umsätzen im Jahr 2020** zeigte sich innerhalb der Branche erwartungsgemäß eine große Spanne zwischen Null Euro und zweistelligen Millionenbeträgen.

3. Nutzungszahlen

Das Bundeskartellamt hat die befragten Dienste außerdem gebeten, die Nutzungszahlen ihres Messenger- bzw. Video-Dienstes in Deutschland zu nennen – separat für Textnachrichten,

Telefonie und Videotelefonie oder insgesamt. Mehrere Dienste haben zu dieser Frage angegeben, dass sie die betreffenden Daten nicht erheben, u. a. weil es keine länderspezifische Erfassung gebe, weil die Nutzung über verschiedene Dienste erfolge oder weil eine Trennung von anderen Funktionen nicht möglich sei. Von den anderen Unternehmen wurden plausible Angaben insbesondere für die Zahl der registrierten Nutzer und die durchschnittliche Zahl der Nachrichten bzw. Minuten pro Tag im Jahr 2020 gemacht. Bei der nachfolgenden Übersicht erfolgt die Nennung der Dienste jeweils in alphabetischer Reihenfolge, so dass daraus keine Rückschlüsse über die (relative) Höhe der jeweiligen Nutzungszahlen gezogen werden können. Dienste, die in der Übersicht nicht erscheinen, fallen entweder nicht in die genannten Kategorien oder haben keine (plausiblen) Angaben gemacht.

Zahl der im Jahr 2020 registrierten Nutzer:	
50.000 bis 1 Mio.	Fastviewer, Ginlo, TeamViewer
1 Mio. bis 25 Mio.	Discord, GoToWebinar, Line, Skype, Slack, Threema, Viber, Webex, Zoom
Über 25 Mio.	Facebook Messenger, GoToMeeting, Snapchat, WhatsApp
Zahl der im Jahr 2020 durchschnittlich versendeten Textnachrichten pro Tag:	
50.000 bis 10 Mio.	Delta Chat, GoToWebinar, Skype
10 Mio. bis 100 Mio.	Discord, GoToMeeting, Microsoft Teams, Snapchat, Viber
Über 100 Mio.	Facebook Messenger, WhatsApp
Zahl der im Jahr 2020 durchschnittlich genutzten Telefonminuten pro Tag:	
50.000 bis 1 Mio.	GoToWebinar, Skype, Webex
1 Mio. bis 20 Mio.	Facebook Messenger, GoToMeeting, Snapchat, Viber
Über 20 Mio.	Discord, WhatsApp
Zahl der im Jahr 2020 durchschnittlich genutzten Videominuten pro Tag:	
50.000 bis 5 Mio.	GoToWebinar, Snapchat, Webex
5 Mio. bis 25 Mio.	Discord, Viber
Über 25 Mio.	Facebook Messenger, WhatsApp

4. Wettbewerbssituation

Um die Wettbewerbssituation näher zu beleuchten, hat das Bundeskartellamt die Messenger- und Video-Dienste nach ihrer eigenen Rolle im Markt und ihrer Einschätzung des Wettbewerbsumfelds gefragt.

Zu der Frage, aus welchen **Gründen** sich die Nutzer für ihren jeweiligen Messenger-/Video-Dienst entschieden haben, hat der überwiegende Teil der befragten Branchenakteure angegeben, dass hierfür u. a. das hohe Datenschutzniveau bzw. die hohe Datensicherheit ihres Dienstes maßgeblich ist. Mehr als die Hälfte der Dienste halten außerdem jeweils ihre nützlichen Funktionen, die Business-Funktionen und die kostenlose Verfügbarkeit des eigenen Dienstes für entscheidend für die Wahl der Nutzer. Nur knapp ein Drittel der Messenger- und Video-Dienste hat angegeben, dass sie ihre Nutzer auch aufgrund ihrer großen Nutzerbasis gewonnen haben.

Einzelne Dienste haben darauf hingewiesen, dass sie innerhalb einer festen Gruppe (z. B. einer Abteilung) funktionieren und deshalb sicherer sind oder dass für die Nutzung ihres Dienstes keine Registrierung erforderlich ist. Daher würden keine Netzwerk-Effekte entstehen. Nach Angaben der Befragten haben die Nutzer ihren Dienst darüber hinaus auch wegen der **einfachen Handhabung**, dem **Verzicht auf Werbung**, die **Integration mit anderen Systemen/Geräten**, die **Infrastruktur in Europa**, die Gestaltung als **Open Source-Dienst**, der **Nutzung eines internationalen Standards (XMPP)** oder aufgrund der **guten Qualität** des Dienstes gewählt.

Eine weitere Frage betraf die **wichtigsten Wettbewerber** des jeweiligen Dienstes einschließlich der entsprechenden Begründung. Wie zu erwarten war, wurden als wichtigste Wettbewerber insbesondere die großen bekannten Messenger- bzw. Video-Dienste wie Facebook Messenger, Google Meet, Microsoft Teams, Signal, Skype, Slack, Webex, WhatsApp und Zoom (alphabetische Reihenfolge) genannt, wobei jeweils nach Messengern und nach Video-Konferenz-Anbietern zu unterscheiden war. Ein führender Dienst hat darauf hingewiesen, dass grundsätzlich jeder Kommunikationsdienst als Wettbewerber angesehen werde und dass die exakte Benennung von Wettbewerbern ohne konkrete Abgrenzung des relevanten Marktes schwierig sei.

Als **wesentliche Wettbewerbsfaktoren** wurden insbesondere vergleichbare Funktionen und ähnliche Zielgruppen (Nutzer / Werbekunden) eines anderen Dienstes genannt sowie die kostenlose Nutzungsmöglichkeit und ein hoher Bekanntheitsgrad. Die große Nutzerzahl oder die große Marktmacht eines anderen Dienstes wurden hingegen seltener als Wettbewerbsfaktor angeführt.

Mehrere Befragte haben darauf hingewiesen, dass die Messenger- bzw. Video-Dienste von Microsoft (Microsoft Teams / Skype), Google (Google Meet) und Apple (iMessage/FaceTime) mit anderen marktstarken Anwendungen bzw. Geräten der betreffenden Unternehmen gekoppelt sind (Office365, Google Workspace, iPhone). Den Nutzern würden die Entscheidung und die Anwendung so erheblich „erleichtert“. Ein Open Source-Anbieter sieht sich in diesem Zusammenhang von Microsoft Teams behindert. Von den Marktteilnehmern wurde außerdem mehrfach darauf hingewiesen, dass dem ursprünglichen Protokoll von WhatsApp der XMPP-Standard zugrunde liege. Dessen Weiterentwicklung hätte WhatsApp aber nicht übernommen, sondern darauf aufbauend ein geschlossenes System konzipiert.

Auf die Frage nach den **strategischen Zielen** ihres Messenger- bzw. Video-Dienstes nannten einige Dienste die Erweiterung der Nutzerbasis, den Ausbau kostenpflichtiger Funktionen, die Erhöhung des Bekanntheitsgrades oder Verbesserungen bei Datenschutz, bei Datensicherheit und Qualität. Ausländische Dienste planen teilweise, sich stärker auf das lokale Angebot auszurichten. Kleine freie Messenger planen häufig keine wesentliche Ausweitung ihres Dienstes und haben teilweise angegeben, kein wirtschaftliches Interesse zu verfolgen. Ein Dienst hat erklärt, in stärkerem Maße mit kleineren Wettbewerbern kooperieren zu wollen.

Zur Wettbewerbssituation hat ein Dienst angemerkt, dass in der Politik nur solche Messenger eingesetzt werden, die IT-Standards einhalten (z. B. durch entsprechende Vorgaben in Ausschreibungen). Ein anderer Dienst hat darauf hingewiesen, dass es als starker Wettbewerbstreiber in der Branche wirke, wenn Nutzer parallel mehrere Dienste nutzen (sog. Multi Homing) und Netzwerkeffekte verhindert würden, wenn Nutzer ohne Registrierung andere Dienste (z. B. auf Einladung) nutzen können. Schließlich wurde von einem Unternehmen der intensive Wettbewerb und die hohe Wettbewerbsdynamik in dieser Branche betont.

D. Datenportabilität als Übergang zur Interoperabilität?

Mit Art. 20 Abs. 1 DSGVO hat der Gesetzgeber den Verbrauchern das Recht eröffnet, die sie betreffenden personenbezogenen Daten, die einem Verantwortlichen bereitgestellt wurden, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder dem neuen Verantwortlichen direkt übermitteln zu lassen. In der Fachöffentlichkeit werden Datenportabilität und Interoperabilität oftmals in einem Zusammenhang diskutiert.⁷⁰ Fraglich ist, ob die Konzeption der Norm grundsätzlich die Bedürfnisse der Nutzer von Messenger- und Video-Diensten einfangen kann (siehe dazu unter I.). Zweifel bestehen zudem an der praktischen Bedeutung der Vorschrift für die Nutzer, wenn sie ihren Messenger- und Video-Dienst wechseln wollen, und damit auch an dem rechtlichen Nutzen für mögliche darüberhinausgehende Interoperabilitätsmaßnahmen (siehe dazu unter II.). Im Rahmen der Ermittlungen hat das Bundeskartellamt die Messenger- und Video-Dienste schließlich nach den theoretischen Möglichkeiten und der tatsächlichen Nutzung der Übermittlung gespeicherter personenbezogener Daten gemäß Art. 20 DSGVO gefragt (dazu unter III.).

I. Einordnung und Anspruch der Vorschrift

Mit Art. 20 Abs. 1 DSGVO hat der Gesetzgeber den Verbrauchern das Recht eröffnet, die sie betreffenden personenbezogenen Daten, die einem Verantwortlichen bereitgestellt wurden, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder dem neuen Verantwortlichen direkt übermitteln zu lassen. Dem Verbraucher steht also die Möglichkeit zu, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln. Kern der Vorschrift ist somit neben der Verfügbarkeit auch die **Übertragbarkeit von personenbezogenen Daten**, welche auch als Datenportabilität bezeichnet wird.

Teils umstritten ist der Ursprung der Norm und damit auch ihre Zugehörigkeit zum Datenschutzrecht.⁷¹ So wird vereinzelt vorgebracht, es handele sich um eine Vorschrift mit rein verbraucherschutz- und wettbewerbsrechtlichen Zielen, anstelle von datenschutzrechtlichen

⁷⁰ Vgl. beispielsweise *OECD* (2020): Consumer data rights and competition- background note, abrufbar unter: [https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/WD\(2020\)59&docLanguage=En](https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/WD(2020)59&docLanguage=En), Stand: 14. September 2021; *Yoo* (2020): Unpacking data portability, CPI antitrust chronicle November 2020, abrufbar unter: <https://www.competitionpolicyinternational.com/unpacking-data-portability/>, Stand: 14. September 2021; *Kerber, Gil* (2020): Data portability rights: Limits, opportunities and the need for going beyond the portability of personal data, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3715357, Stand: 14. September 2021.

⁷¹ *Kühling/Buchner/Herbst*, DSGVO, Art. 20 Rn. 4.

Zielen.⁷² Nach überwiegender Auffassung stellt das Recht auf Datenportabilität jedoch genauso ein Gestaltungsrecht dar, wie andere Betroffenenrechte.⁷³ Entscheidend bei der systematischen Einordnung sei vielmehr, dass die Norm neben rein datenschutzrechtlichen Zielen eben auch andere, insbesondere wettbewerbs- und binnenmarktpolitischen Ziele verfolge. So stärke das Recht die Selbstbestimmung des Verbrauchers und fördere gleichzeitig den Wettbewerb zwischen den Anbietern sozialer Netze.⁷⁴

Die Vorschrift soll dem Verbraucher somit offenbar nicht nur ermöglichen, seine Daten zu erhalten. Sie soll ihn auch gleichzeitig dazu berechtigen, in gewisser Weise frei und selbstbestimmt über sie zu verfügen. Neben der Folge, dass dadurch sog. „Lock-in-Effekte“ verhindert werden können, erhofft sich der Gesetzgeber - wie bereits angedeutet - eine Steigerung des Wettbewerbs in Bezug auf neue Innovationsmöglichkeiten und den Austausch von personenbezogenen Daten.⁷⁵ Somit beruht der Ursprung der Vorschrift zwar weniger auf dem klassischen Datenschutzrecht i. S. d. Schutzes personenbezogener Daten, er trägt jedoch aufgrund der verbraucherschützenden und marktregulierenden Aspekte dennoch zum übergreifenden Schutzzweck des Datenschutzrechts bei.⁷⁶

II. Praktische Bedeutung

Das Recht auf Datenportabilität nach Art. 20 Abs. 1 DSGVO eröffnet dem Verbraucher zunächst weitreichende Dispositionsbefugnisse im Umgang mit seinen persönlichen Daten. Das Recht erhält seine Bedeutung nicht nur durch die generelle Möglichkeit, seine Daten anfordern zu können, sondern vor allem durch die in Art. 20 Abs. 2 DSGVO normierte Möglichkeit, seine Daten auch direkt an einen neuen Verantwortlichen übertragen zu lassen. Neben dem bloßen Erhalt der Daten könnte speziell bei der Untersuchung von Messenger-Diensten die direkte Übertragungsmöglichkeit womöglich Wechselvorhaben erleichtern.

⁷² *Dehmel/Hullen*, ZD 2013, 147, S. 153.

⁷³ *Kühling/Buchner/Herbst*, DSGVO, Art. 20 Rn. 4.

⁷⁴ *Ehmann/Selmayr/Kamann/Braun*, DS-GVO, Art. 20 Rn. 3.

⁷⁵ Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01 S. 6.

⁷⁶ *Kühling/Martin*, EuZW 2016, 448 S. 450. Konkret kann der datenschutzrechtliche Charakter darüber hinaus darin gesehen werden, dass die Norm eine Ausprägung der europäischen Grundrechte auf Privatleben und Schutz der personenbezogenen Daten darstellt, vgl. *Auernhammer/Schürmann* DS-GVO Art. 20 Rn. 3. Aufgrund des Erfordernisses einer immer weitergehenden Modernisierung des Rechts kann auch Art. 20 DS-GVO als ein Element der innovativen Grundrechte im digitalen Zeitalter gesehen und somit als ein Ausdruck der Fortentwicklung des Rechts gelten, vgl. *Ehmann/Selmayr/Kamann/Braun* DS-GVO Art. 20 Rn. 4; *Auernhammer/Schürmann* DS-GVO Art. 20 Rn. 3.

Allerdings kann das Konzept der Datenportabilität das Wesen des auf Echtzeit-Austausch ausgerichteten „Messaging“ oder „Chat“ nicht einfangen und bleibt daher schon im Ansatz hinter Interoperabilität zurück. Art. 12 Abs. 3 DSGVO sieht vor, dass das Bereitstellen der personenbezogenen Daten „unverzögerlich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags“ zu geschehen hat. Unter Umständen ist sogar eine Verlängerung um zwei weitere Monate möglich. Dies spricht dafür, dass **eine Übertragung „in Echtzeit“** auf Grundlage dieser Norm weder gewünscht noch möglich ist. Selbst wenn Datenportabilität ohne jegliche Verzögerung gewährleistet sein müsste und jeder Nutzer stets sofort und nach Belieben zwischen Diensten hin und her wechseln könnte, käme ein Austausch in Echtzeit, wie er beim Messaging üblich ist, nicht zustande.

Mit Blick auf den Tatbestand des Art. 20 DSGVO ist weiter festzustellen, dass die für eine funktionierende Interoperabilität erforderliche technische Kompatibilität nicht wechselseitig erzwungen werden kann. Übermittelt werden sollen Daten, die den Betroffenen selbst betreffen und von diesem auch bereitgestellt worden sind. Darüber hinaus muss die herkömmliche Datenverarbeitung automatisiert gem. Art. 20 Abs. 1 lit. b DSGVO stattfinden und auf einer der in Art. 20 Abs. 1 lit. a DSGVO genannten Rechtsgrundlagen beruhen. Gleichzeitig stellt die DSGVO aber nur begrenzte Anforderungen an das technische Format, in dem diese Daten bereitgestellt werden müssen. So ergibt sich aus Erwägungsgrund 68 der DSGVO, dass für den Verantwortlichen keine Pflicht besteht, „technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten“. Diese Einschränkung ist so zu verstehen, dass eine direkte Übermittlung der Daten durch den Verantwortlichen an einen anderen Verantwortlichen i. S. d. Art. 20 Abs. 2 DSGVO zwar erfolgen soll. Wenn dies aber technisch nicht umsetzbar ist, sich daraus keine Verpflichtung des Verantwortlichen ergibt, dies zu ermöglichen.⁷⁷ Hier verpflichtet also Art. 20 DSGVO Anbieter nicht, kompatible Datenverarbeitungssysteme zu schaffen, welche jedoch wohl Voraussetzung für Interoperabilität wären.

Die wohl bedeutendste Problematik aus datenschutzrechtlicher Perspektive dürfte hier die fehlende Möglichkeit sein, Daten generell zu trennen. Neben den sog. Stammdaten handelt es sich bei der Nutzung von OTT-Diensten wie Messenger- und Video-Diensten hauptsächlich um Daten, die auch einen Bezug zu anderen, dritten Personen aufweisen. Ein Ausschluss solcher **Daten Dritter** dürfte den Normzweck, weitreichende Wechselanreize zu schaffen, wohl hochgradig verfehlen. Inzwischen besteht Einigkeit, dass unter der Prämisse, die Rechte und Freiheiten jener Drittbetroffenen nicht zu verletzen, diese auch Teil des Übermittlungsanspruchs sein können. Folglich muss bei der Datenübertragung eine entsprechende Rechtsgrundlage vorliegen. Diese dürfte insbesondere im Falle der OTT-Dienst-Nutzung wohl mit dem berechtigten

⁷⁷ Siehe *Artikel 29-Datenschutzgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev. 01, April 2017, S. 19.

Interesse des Verantwortlichen nach Art. 6 Abs. 1 lit. f. DSGVO zu begründen sein. Daher dürften Registrierungsdaten, das Profilbild, auch wenn es eine weitere Person abbildet, sowie das Kontakteverzeichnis übertragen werden.

Eine letzte Schwierigkeit dürfte in der **praktischen Umsetzung** des Anspruchs auf Datenportabilität und damit auch einer Nutzbarmachung für Interoperabilitätsmaßnahmen liegen. Wesentlich für diese Einschätzung ist das Erfordernis des Bereitstellens. Hier kommt es darauf an, dass der Betroffene selbst wissentlich und aktiv über seine Daten verfügt hat. In der Praxis werden Nutzer bei einem Anbieterwechsel ihre vollständigen Daten, insb. Inhalte von Austausch über Textnachrichten - **Chat-Verläufe** - mitnehmen wollen. Gerade was die portablen Daten angeht, kann dies schwierig werden. So sind beispielsweise sog. beobachtete Daten, also jene, die durch passives Beobachten des Nutzerverhaltens gewonnen werden, nicht Teil des Anspruchs. Ausgeschlossen sind außerdem Informationen, die auf einer Auswertung von bereitgestellten Daten basieren. In dem Zusammenhang dürfte vor allem die Einordnung von Chatverläufen eine große Rolle spielen. Entscheidendes Problem ist, dass diese sich aus von verschiedensten Chatteilnehmern veröffentlichten Daten zusammensetzen. Sie sind nicht ausschließlich von dem Anspruchssteller bereitgestellt worden. Die einzelnen von diesen veröffentlichten Nachrichten müssten von den jeweiligen Antworten getrennt werden, was technisch zwar machbar sein, jedoch einen unverhältnismäßigen Aufwand darstellen dürfte.

Vor dem Hintergrund der beschriebenen Schwierigkeiten stand eine Überprüfung, ob die Verbraucher von dem Recht tatsächlich Gebrauch machen, bisher aus. Das Bundeskartellamt hat die Messenger- und Video-Dienste daher befragt, inwieweit die rechtlichen Ansprüche von den Verbrauchern wahrgenommen und von den Messenger-Diensten ausgeführt wurden. Die entsprechenden Informationen können auch für die Bewertung möglicher Interoperabilitätsvorhaben relevant sein. Sie könnten nicht nur Aufschluss über Präferenzen und das (Wechsel-)Verhalten der Verbraucher geben, sondern auch ein aktuelles Bild des Wettbewerbsgeschehens zeichnen (siehe dazu sogleich).

III. Ermittlungsergebnisse

Das Bundeskartellamt hat die Messenger- und Video-Dienste sowohl nach den theoretischen Möglichkeiten als auch nach der tatsächlichen Nutzung der Übermittlung gespeicherter personenbezogener Daten gemäß Art. 20 DSGVO gefragt.

Auf die Frage, in welcher **Form** Nutzer die Übermittlung der gespeicherten personenbezogenen Daten beim jeweiligen Dienst beantragen können, haben fast alle befragten Branchenteilnehmer Angaben gemacht. Einige Dienste haben hierzu eine E-Mail-Adresse genannt, einzelne auch einen Link zu einem Download- oder Web-Formular angegeben. Ob und in welchem Umfang

über diese Wege tatsächlich eine Datenübermittlung gemäß § 20 DSGVO beantragt werden kann, konnte im Rahmen der Sektoruntersuchung im Einzelfall allerdings nicht überprüft werden.

Darüber hinaus hat das Bundeskartellamt die Branche gefragt, welche personenbezogenen Daten Nutzer erhalten, wenn sie einen entsprechenden Antrag stellen. Von den Diensten, die Angaben zur Übermittlung von Daten gemacht haben, übermitteln alle persönliche Daten, wie z. B. Vor- und Nachname des Nutzers, Benutzername, Alter oder Geschlecht. Nur jeweils rund die Hälfte der Dienste übermittelt auch Daten zu Geräten/Konfiguration, Kontakten/Adressen, Gruppenmitgliedschaften oder App-Einstellungen. Als sonstige **übermittelte Daten** wurden von den Unternehmen und Anwendungen insbesondere Meeting-Daten, (offline) Nachrichten, Datenschutzeinstellungen, Chat-Historie, gespeicherte Dateien, Anmeldedaten, öffentliche Schlüssel, Nutzungsdaten, Ratings, Rankings, Stories, Friends, und Histories/Verläufe genannt. Einige freie Messenger-Dienste haben darauf hingewiesen, dass es vom jeweiligen Server abhängt, welche Daten übermittelt werden und wie diese ggfs. an einen anderen Dienst übertragen werden können. Aufgrund der Serverbezogenheit sei bei ihnen zudem eine Datenübertragung zwischen verschiedenen Clients i. d. R. nicht erforderlich.

Eine weitere Frage betraf den **Umfang der gestellten Anträge**, der Bearbeitung sowie der Übermittlung der Daten an einen neuen Anbieter. Zur Zahl der Anträge bzw. der bearbeiteten Anträge auf Datenübermittlung in den letzten drei Jahren haben nur sehr wenige Unternehmen Angaben gemacht. Die genannten Zahlen lagen zwischen 0 und rd. 300.000 Anträgen pro Jahr. Die Zahl der Anträge war dabei im Verhältnis zur Zahl der registrierten Nutzer beim jeweiligen Dienst verschwindend gering.

Keiner der befragten Dienste hat angegeben, dass Daten aufgrund eines Antrags unmittelbar an einen **neuen Anbieter übermittelt** wurden. Allerdings haben einige Dienste darauf hingewiesen, dass die Übermittlung der Daten an einen dritten Anbieter durch den Nutzer selbst erfolgt bzw. erfolgen kann, so dass hierzu keine näheren Informationen vorliegen. Hinsichtlich der **Dauer** der Bearbeitung eines Antrags auf Datenübermittlung wurden von den befragten Diensten sehr unterschiedliche Zeiträume genannt – zwischen wenigen Sekunden und weniger als 1 Monat.

Schließlich sollten die Dienste beschreiben, wo die Nutzer über ihre Rechte auf Datenportabilität nach Art. 20 DSGVO **informiert** werden. Der weit überwiegende Teil der befragten Dienste hat dazu entsprechende Angaben gemacht. In welcher Form und in welchem Umfang die erforderlichen Informationen unter den genannten Links tatsächlich verfügbar sind, konnte im Rahmen der Sektoruntersuchung jedoch nicht überprüft bzw. bewertet werden. Sechs der befragten Dienste haben angegeben, keine entsprechenden Informationen bereitzustellen.

Zusammenfassend ergibt sich aus den Antworten zu diesem Abschnitt, dass die befragten Dienste sich des Themas Datenportabilität und der diesbezüglichen Rechte der Nutzer durchaus

bewusst sind und entsprechende vorbereitende Maßnahmen getroffen haben. In der Praxis wurden bei den meisten Befragten offenbar gar keine oder nur sehr wenige Anträge auf Datenportabilität gestellt.

E. Mehr Datenschutz durch Interoperabilität?

Interoperabilität ist ein sich dynamisch entwickelnder Begriff, der vielfach an verschiedene Verwendungen angepasst wird und für den Wettbewerbs- und Verbraucherschutz noch nicht eindeutig definiert worden ist.⁷⁸ Als vorläufige Definition für die Zwecke dieser Sektoruntersuchung soll Interoperabilität als die **Fähigkeit unabhängiger, heterogener Systeme oder Produkte verstanden werden, in verschieden hohem Maße zusammenzuarbeiten**. Aus Sicht der Verbraucher bezeichnet Interoperabilität die Möglichkeit, sich mit Nutzern eines anderen als dem eigenen Messenger-Dienst auszutauschen zu können, ohne selber diesen anderen Dienst installiert oder sich dort registriert zu haben.⁷⁹

Das Bundeskartellamt greift mit der vorliegenden Sektoruntersuchung das Thema Interoperabilität nicht nur deshalb auf, weil es ein Einflussfaktor für das Umfeld der Messenger- und Video-Dienste ist. Es geht vor allem um die Frage, **ob durch Interoperabilität ein besseres Datenschutzniveau erreicht werden kann**. Leitfragen sind zum einen, ob es einen direkten Effekt gibt. Dahinter steht die häufig geäußerte Erwartung, dass, wenn Erreichbarkeit der Dienste untereinander gegeben wäre, die Verbraucher keine Scheu mehr haben, den Anbieter zu wechseln, da sie von den bisherigen Kontakten nicht mehr ausgeschlossen werden. Um die

⁷⁸ Vgl. z. B. die von der Internationalen Standardisierungsorganisation (ISO) verwendete Definition im Bereich des Cloud Computing, zitiert nach: *Brown*, Interoperability as a tool for competition regulation, Preprint, 30.07.2020, S. 32, abrufbar unter: <https://osf.io/preprints/lawarxiv/fbvxd/>, Stand November 2020, sowie *Kerber/Schweitzer*, Interoperability in the Digital Economy, JIPTEC, 2017, Vol. 8, S. 39-58, Rn. 5, oder *Palfrey/Gasser*, Interop, 2012, S. 5, so zitiert in: *Kerber/Schweitzer*, Interoperability in the Digital Economy, JIPTEC, 2017, Vol. 8, S. 39-58, Rn. 5.

⁷⁹ Eng verbunden mit Interoperabilität ist der Begriff der Kompatibilität. Das Verhältnis zur Interoperabilität wird jedoch nicht einheitlich beschrieben. Teilweise wird Kompatibilität als eine Vorstufe und notwendige Voraussetzung für Interoperabilität aufgefasst. Wenn Produkte kompatibel sind, können sie z. B. ohne Softwarekonflikte parallel auf einem Computer verwendet werden. Bei Interoperabilität müssen sie darüber hinaus zusammenarbeiten bzw. funktionieren können. Teilweise wird Interoperabilität als Unterkategorie von Kompatibilität angesehen, vgl. *Kerber/Schweitzer*, Interoperability in the Digital Economy, JIPTEC, 2017, Vol. 8, S. 39-58, Rn. 5. In der theoretischen ökonomischen Literatur wird in der Regel der Begriff der Kompatibilität verwendet, während sich in informationstechnologischen Schriften Interoperabilität als „Schlagwort“ etabliert hat, ohne dass dieser Unterscheidung modelltheoretische Unterschiede zugrunde liegen würden.

gewünschten positiven, direkten Effekte auf das Datenschutzniveau zu erreichen, müssten sich die Verbraucher allerdings datenschutzfreundlichen Anbietern zuwenden. Nach den Ergebnissen verschiedener Verbraucherbefragungen erscheinen Zweifel daran durchaus berechtigt (vgl. dazu IV). Aber auch indirekte Effekte auf das Datenschutzniveau durch Interoperabilität stehen im Raum. Die **negativen Auswirkungen von Interoperabilität auf Wettbewerb und Innovation** können über die Datensicherheit auch Folgen für datenschutzrechtliche Fragen haben.

Für eine bessere Einschätzung der Leitfragen, wird im Folgenden zunächst geklärt, wie Interoperabilität organisatorisch und technisch umgesetzt werden könnte. Welche Wege könnten beschritten werden, um Interoperabilität zu etablieren und was sind jeweils die Konsequenzen (dazu unter I.)? Von Interesse ist ferner, inwieweit Interoperabilität bereits Eingang in gesetzliche Vorschriften auf nationaler und europäischer Ebene gefunden hat und was die Gründe dafür sind (dazu unter II.). Anschließend ist zu prüfen, inwieweit bisherige wissenschaftliche Erkenntnisse die Zusammenhänge zwischen Interoperabilität, Innovation und Wettbewerb aufklären oder Hinweise zur Problemlösung und für Handlungsempfehlungen geben können (dazu unter III.). Sind sie überhaupt geeignet, die komplexen Wirkungszusammenhänge zu beleuchten? Abschließend geht es um die Verbraucher und ihr nur schwer zu prognostizierendes Verhalten. Werden sie die von Politik und Datenschützern in sie gesetzten Hoffnungen erfüllen oder haben sie selbst ganz andere Wünsche (dazu unter IV.)?

Vor diesem Hintergrund werden anschließend erste Ermittlungsergebnisse zu Fragen der Interoperabilität vorgestellt. Das Bundeskartellamt hat die Branche zu ihrer Einschätzung ausführlich befragt (dazu unter V.).

I. Umsetzung und Gestaltung

Am Anfang jedes Interoperabilitätsvorhabens steht die Frage, ob und inwieweit von hoheitlicher Seite Maßnahmen ergriffen werden sollen. Ist das gewünscht, geht es um eine **gesetzliche** Interoperabilitätsverpflichtung, die den betroffenen Unternehmen auferlegt wird. Die Alternative besteht in **freiwilligen** Interoperabilitätsvorhaben, die von Seiten des Staates, der Branche insgesamt oder Initiativen einzelner Marktteilnehmer initiiert oder gefördert werden können. In der Branche der Messenger- und Video-Dienste war es bisher dem Markt überlassen, Interoperabilitätsregelungen hervorzubringen.

In **organisatorischer Hinsicht** gibt es zwei Möglichkeiten, eine Interoperabilitätsregelung zu gestalten. Sie kann **symmetrisch** oder **asymmetrisch** umgesetzt werden. Während die

symmetrische Regelung alle Marktteilnehmer betrifft, sind bei letzterem Fall nur bestimmter Anbieter verpflichtet, ihre Dienste interoperabel zu gestalten.⁸⁰

Was die **technische Umsetzung** angeht, sollen an dieser Stelle nur grundlegende Überlegungen dargestellt werden, die für das Verständnis der Ausführungen der Branche notwendig sind. Grobe Kenntnisse der technischen Anforderungen und des damit verbundenen Aufwands sind ferner hilfreich, ein Bewusstsein für die damit verbundenen Anstrengungen und Kosten zu schaffen. Die Art der Umsetzung einer Interoperabilitätsregelung hat maßgeblichen Einfluss darauf, welche Kosten und welcher Aufwand entstehen, sowohl in technischer als auch in organisatorischer Hinsicht.

Die technische Umsetzung von Interoperabilität richtet sich im Wesentlichen danach, auf welcher **Verknüpfungsebene** Produkte oder Systeme zusammenarbeiten sollen. In der vorliegenden Untersuchung steht die substitutive technische Verknüpfung von Produkten bzw. Diensten im Mittelpunkt. Zu untersuchen ist, wie zwischen verschiedenen Anbietern derselben „Dienst Messenger- und Video-Dienst“, die im Wettbewerb zueinander stehen, Interoperabilität hergestellt werden kann. Es geht also vorrangig nicht darum, nach ihren Funktionen komplementäre Dienste zu verknüpfen. Aus der Verknüpfungsebene können sich wiederum verschiedene technische Möglichkeiten, die den **Grad der Interoperabilität** beschreiben, ergeben. Für eine Verknüpfung zweier substitutiver Dienste sei eine sogenannte „full protocol interoperability“ erforderlich, wie z. B. die Europäische Kommission ausführt. Diese biete im Gegensatz zur weniger stark integrierenden und deshalb hauptsächlich für Komplementärprodukte erforderlichen, reinen „protocol interoperability“ ein besonders hohes Maß an Interoperabilität. Darüber hinaus wird auch die „data interoperability“, auf Basis derer Daten z. B. über Programmierschnittstellen (APIs) in Echtzeit übertragen werden können, benannt.⁸¹

Nach vorläufigen Erkenntnissen des Bundeskartellamts kann Interoperabilität grundsätzlich über **drei verschiedene Wege** umgesetzt werden: Bridges und Converter u. ä., Client Interoperabilität, Serverschnittstellen.

Bridges bieten eine Art „Übersetzungsservice“ zwischen verschiedenen Protokollen. Sie ermöglichen Gateways und Übergänge zu anderen Diensten. Allerdings ist die Umsetzung nicht einfach, da sie in der Regel eine zentrale Registrierung beim Ziel-Messenger- und Video-Dienst

⁸⁰ Vgl. *Kerber/Schweitzer*, Interoperability in the Digital Economy, JIPTEC, 2017, Vol. 8, S. 39-58, Rn. 6; *Choi/Whinston*, Benefits and requirements for interoperability in the electronic marketplace, *Technology in Society*, 2000, 22, S. 33-44, 35 f.

⁸¹ Vgl. *European Commission*, Final Report 2019, Competition policy for the digital era, S. 83 ff

erfordern. Alle beteiligten Messenger- und Video-Dienste müssen also mit der Verwendung von Bridges einverstanden sein.

Durch **Client Interoperabilität** (Multiprotocol Clients) kann der Austausch zwischen Messenger-Diensten anwenderfreundlicher gestaltet werden. In Gestalt der **Multi Messenger-Dienste**, die bereits existieren, wird Client Interoperabilität schon in der Branche praktiziert. Multi Messenger bieten eine Benutzeroberfläche, über die die Verbraucher verschiedene Messenger-Systeme auslesen können. Der Nutzer muss dazu bei den jeweiligen Diensten registriert sein. Austausch ist allerdings immer nur innerhalb eines Systems möglich. Wer z. B. eine Antwort in ein anderes Messenger-System versenden will, muss dies über „copy and paste“ lösen.⁸²

Voraussetzung technischer Art ist grundsätzlich, dass alle partizipierenden Dienste eine öffentliche Schnittstelle implementieren und die eigene API oder das Protokoll offenlegen. Die Clients müssen die API jedes anderen teilnehmenden Dienstes (Messaging-Systems) implementieren.

Die weitgehendste Form der Interoperabilität kann über **standardisierte Serverschnittstellen** hergestellt werden. Generell können über Schnittstellen Verbindungen zu Servern aufgebaut werden. Für den bilateralen Austausch werden hier **APIs (Application Programming Interface)** eingesetzt. Die API - auch Programmierschnittstelle genannt - ermöglicht es Anwendungen miteinander zu kommunizieren. Die API ist nicht die Datenbank oder gar der Server, sondern der Code, der die Zugangspunkte für den Server regelt und die Kommunikation ermöglicht.⁸³ Für diese Umsetzungsvariante sind mehr technische Vorkehrungen zu treffen als für die Interoperabilität der Clients.

Sofern ein **marktweites Regime** angestrebt würde, wäre eine Übereinkunft in der Branche notwendig, ein standardisiertes frei zugängliches Messaging-System bzw. eine standardisierte

⁸² Vgl. *Open-Xchange* (2020): Whitepaper - A Technical and Policy Analysis of interoperable Internet Messaging, Version 1, September 2020.

⁸³ Eine API ist ein Satz von Befehlen, Funktionen, Protokollen und Objekten, die Programmierer verwenden können, um eine Software zu erstellen oder mit einem externen System zu interagieren. Sie stellt Entwicklern Standardbefehle für die Ausführung allgemeiner Operationen zur Verfügung, so dass Codes nicht von Grund auf neu geschrieben werden müssen. Vgl. <https://www.talend.com/de/resources/was-ist-eine-api/>, Stand: 25. August 2021. Z. B. auch vorgeschlagen von *Digitale Gesellschaft*, Stellungnahme der Digitalen Gesellschaft e. V. zur Konsultation des Bundesministeriums der Justiz und für Verbraucherschutz zu Interoperabilität und Datenportabilität bei sozialen Netzwerken, Mai 2019, S. 4, abrufbar unter: <https://digitalegesellschaft.de/2019/05/stellungnahme-der-digitalen-gesellschaft-e-v-zur-konsultation-des-bundesministeriums-der-justiz-und-fuer-verbraucherschutz-zu-interoperabilitaet-und-datenportabilitaet-bei-sozialen-netzwerken/>.

Server-API oder Protokoll zu implementieren und Sets interoperabler Funktionen zu definieren. Ferner müssten alle teilnehmenden Dienste nicht nur die Schnittstellen einrichten und ihre API oder das Protokoll offenlegen, sondern auch **zusätzliche Software** auf ihrem Server installieren oder die eigenen erweitern, um zwischen dem Standard-Protokoll und der eigenen Technik zu kommunizieren und um mit den Nutzern anderer Dienste umgehen zu können. Auch die diensteigenen Identifier müssten in die **einheitlichen Identifier** des interoperablen Systems überführt werden. Mit XMPP und Matrix gibt es bereits freie Messenger-Systeme mit offenen Standards. Die Clients hätten weniger Aufwand zu bestreiten. Sie müssten jedenfalls für die Kernfunktion Nachrichtenaustausch den Standard oder das standardisierte Protokoll übernehmen.⁸⁴ Weitere Standardisierungen wären z. B. bei inkompatiblen Verschlüsselungsstandards sowie bei weiteren Funktionen, wie z. B. dem Audio-/Video-Austausch, nötig, da hier in der Regel andere Protokolle verwendet werden als für den Nachrichtenaustausch.

Für die **Verbraucher** stehen allerdings nicht die technischen Voraussetzungen, sondern die Funktionen, die ermöglicht werden, im Vordergrund. Bei Messenger-Diensten könnte Interoperabilität auf **Basisfunktionen** beschränkt werden, d. h. auf das Senden von Textnachrichten sowie Gruppenchats, vielleicht auch das Übertragen von Fotos. Eine weitergehende Variante würde vorsehen, dass **alle Funktionen**, die ein Messenger-Dienst anbietet, auch von allen anderen Diensten angewendet werden können.

Interoperabilität ist schon lange nicht mehr nur von Interesse für Technikspezialisten und Internet-Experten. Interoperabilität hat inzwischen auch Eingang in Gesetze und Richtlinien in Deutschland und Europa gefunden. Bemerkenswert ist, dass sich der Gesetzgeber mit den weitreichenden Implikationen von Interoperabilität durchaus befasst hat.

II. Interoperabilität im Wettbewerbs- und Sektorrecht

Das Bundeskartellamt hat die verbraucherrechtliche Sektoruntersuchung Messenger- und Video-Dienste nach § 32e Abs. 5 GWB eingeleitet; sie richtet sich auf Messenger- und Video-Dienste als Wirtschaftszweig und ist deshalb nicht gegen einzelne Unternehmen gerichtet. Eine Verpflichtung zur Interoperabilität lässt sich nach Auffassung des Bundeskartellamts dem klassischen Verbraucherrecht bisher nicht entnehmen. Lediglich im Wirtschaftsrecht sind Bestimmungen enthalten, die eine behördlicherseits (unter hohen Voraussetzungen und in einem bestimmten Verfahren) auszusprechende Verpflichtung zur Interoperabilität zu konkurrierenden Diensten vorsehen, nämlich § 19a Abs. 2 Satz 1 Nr. 5 GWB sowie § 21 Abs. 2 des

⁸⁴ Vgl. *Open-Xchange* (2020): Whitepaper - A Technical and Policy Analysis of interoperable Internet Messaging, Version 1, September 2020, S. 12.

Telekommunikationsgesetzes.⁸⁵ Wegen der anhaltenden rechtspolitischen Diskussion über eine gesetzliche Verpflichtung von Messenger- und Video-Diensten zur horizontalen Interoperabilität hat das Bundeskartellamt in seiner Untersuchung den befragten Unternehmen auch zu diesem Themenkomplex Fragen gestellt. Einzelne Messenger- und Video-Dienste haben sich in ihren Antworten zum Fragebogen des Bundeskartellamts auf den geltenden Rechtsrahmen für eine mögliche verpflichtende Interoperabilitätsmaßnahme bezogen. Dies sind § 19a GWB (vgl. dazu unten 1.) und Art. 61 Abs. 2 Unterabs. 1 lit. c des Europäischen Kodex für elektronische Kommunikation⁸⁶ (siehe dazu unten 2.), der in § 21 Abs. 2 TKG Eingang gefunden hat. Daher sollen diese Vorschriften hier kurz erwähnt werden. Für eine ausführliche Diskussion sei auf die einschlägige Fachliteratur verwiesen. Der Vollständigkeit halber sei zudem auf die Vorbereitungen der Europäischen Kommission für den Digital Markets Act (DMA)⁸⁷ verwiesen (siehe dazu unten 3.).

1. § 19a Gesetz gegen Wettbewerbsbeschränkungen (GWB)

Sofern das Bundeskartellamt für Unternehmen eine überragende marktübergreifende Bedeutung für den Wettbewerb festgestellt hat (§ 19a Abs. 1 GWB), kann es dem betroffenen Unternehmen bestimmte Verhaltensweisen untersagen. So kann das Bundeskartellamt nach § 19a Abs. 2 Satz 1 Nr. 5 GWB untersagen, „die Interoperabilität von Produkten oder Leistungen oder die Portabilität von Daten zu verweigern oder zu erschweren und damit den Wettbewerb zu behindern“. In der Gesetzesbegründung wird dazu ausgeführt, dass gegen Interoperabilität gerichtete Maßnahmen starke Marktstellungen der Normadressaten des § 19a GWB absichern und weiter festigen können. Sie können Lock-In-Effekte begünstigen.

In der Gesetzesbegründung werden auch die möglichen ambivalenten Wirkungen der Interoperabilität und „andere mögliche Nachteile“ einer Interoperabilitätsverpflichtung genannt. Explizit erwähnt werden zu Gunsten von Wettbewerbern des Normadressaten wirkende Netzwerkeffekte, die geschwächt werden könnten sowie die Behinderung von Innovation und Produktgestaltungsmöglichkeiten als auch die Möglichkeit, dass der Normadressat Zugang zu (noch) mehr Daten erhalten könnte.

⁸⁵ Art. 1 des Gesetzes zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts (Telekommunikationsmodernisierungsgesetz) v. 23.06.2021, BGBl. I 1858 – TKG.

⁸⁶ Richtlinie des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation (EU) 2018/1972 v. 11.12.2018, Abl. L 321 v. 17.12.2018, S. 36 – EKEK.

⁸⁷ *Europäische Kommission*, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Digital Markets Act) v. 15.12.2020, COM (2020) 842 final, 2020/0374(COD) – DMA-Vorschlag.

2. Europäischer Kodex für elektronische Kommunikation (EKEK) / Telekommunikationsgesetz (TKG)

Der im Dezember 2018 in Kraft getretene EKEK erlaubt nationalen Regulierungsbehörden – in Deutschland also der **Bundesnetzagentur (BNetzA)** – Anbietern von „nummernunabhängigen interpersonellen Kommunikationsdiensten“ **Pflichten zur Interoperabilität aufzuerlegen** (Art. 61, Abs. 2 Unterabs. 1 lit. c. EKEK). Marktbeherrschung gem. Art. 68 Abs. 3 lit. a EKEK ist dazu keine notwendige Voraussetzung. Eine Interoperabilitätsverpflichtung kann aber nur unter den in Art. 61 Abs. 2 Unterabs. 2 EKEK genannten Bedingungen implementiert werden. Insbesondere darf Interoperabilität nur auferlegt werden, wenn die **durchgehende Konnektivität zwischen Endnutzern** gefährdet ist.

3. Digital Markets Act (DMA-Vorschlag)

Gemeinsam mit dem geplanten Gesetz über digitale Dienste⁸⁸ ist der DMA-Vorschlag eines der Kernelemente der EU-Digitalstrategie.⁸⁹ Im Herbst 2021 sollen die Verhandlungen zwischen EU-Parlament, EU-Kommission und den Mitgliedsländern über das umfangreiche Gesetzespaket, das aus Digital Services Act (das)-Vorschlag und DMA-Vorschlag besteht, aufgenommen werden. Die Europäische Union will mit den zwei zusammenhängenden Verordnungen die Internetregulierung neu aufstellen und dabei vor allem die Macht großer Online-Plattformen angehen. Der DMA-Vorschlag zielt hier primär auf Wettbewerbsfragen, der DSA-Vorschlag auf andere Bereiche der Plattformregulierung wie Online-Werbung, Haftungsfragen oder Inhaltsmoderation.⁹⁰

Im DMA-Vorschlag der EU-Kommission spielt Interoperabilität auch eine Rolle. Allerdings soll Interoperabilität hier - anders als in § 19a GWB - insbesondere im Vertikalverhältnis der Marktteilnehmer Berücksichtigung finden. Nach Art. 6 Abs. 1 (f) DMA-Vorschlag kann ein sog. Gatekeeper, also ein Unternehmen, das eine starke Vermittlerposition einnimmt, demnach verpflichtet werden, „gewerblichen Nutzern und Erbringern von Nebendienstleistungen den Zugang zu und die Interoperabilität mit denselben Betriebssystemen, Hardware- oder Software-

⁸⁸ *Europäische Kommission*, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Digital Services Act) und zur Änderung der Richtlinie 2000/31/EG v. 15.12.2020, COM (2020) 825 final, 2020/0361(COD) – DSA-Vorschlag.

⁸⁹ Vgl. *Europäische Kommission* (2021), Das Gesetz über digitale Märkte: für faire und offene digitale Märkte, abrufbar unter: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_de, Stand: 10. September 2021.

⁹⁰ Vgl. <https://netzpolitik.org/2021/plattformregulierung-europas-weg-in-die-digitale-zukunft/>, Stand: 2. September 2021.

Funktionen ermöglichen, die der Gatekeeper für die Erbringung von Nebendienstleistungen zur Verfügung hat oder verwendet“.

Festzuhalten ist, dass das Wettbewerbs- und Sektorrecht nicht Grundlage der vorliegenden verbraucherrechtlichen Sektoruntersuchung ist. Offenbar ordnet der Gesetzgeber dem Thema aber eine hohe Bedeutung zu, dessen Komplexität er aufgrund möglicher negativer Auswirkungen in den Rechtsvorschriften erwähnt. Dies stützt die Auffassung des Bundeskartellamts, dass eine Befragung der Branche ein fundierter Beitrag sein kann, um das Verhältnis der Effekte zueinander besser abschätzen zu können. Zunächst soll im folgenden Kapitel beschrieben werden, inwieweit bisherige wissenschaftliche Erkenntnisse die Zusammenhänge zwischen Interoperabilität, Innovation und Wettbewerb aufklären oder Hinweise zur Problemlösung und für Handlungsempfehlungen geben können.

III. Beitrag wissenschaftlicher Erkenntnisse

Das Bundeskartellamt untersucht, welche Effekte von einem möglichen Interoperabilitätsvorhaben auf das Datenschutzniveau bei Messenger- und Video-Diensten zu erwarten sind. Der Fokus des Bundeskartellamts liegt folglich auf einen speziellen Ausschnitt der Thematik - **Interoperabilität und Datenschutz** - bei welchem aber durchaus Wechselwirkungen zu Wettbewerb, Innovation und Datensicherheit bestehen. Zunächst soll die Komplexität der Fragestellung veranschaulicht werden (dazu unter 1.). Anschließend werden wesentliche Erkenntnisse zur Theorie der Netzwerke (dazu unter 2.) und mögliche Auswirkungen von Interoperabilität auf Wettbewerb und Innovation beschrieben (dazu unter 3.). Den Abschluss bildet eine kurze Zusammenfassung möglicher Effekte von Standardisierungsprozessen (dazu unter 4.).

1. Klasse statt Masse

Der Wirtschaftszweig der Messenger- und Video-Dienste, wie er für die Zwecke der Untersuchung definiert wurde, umfasst eine große Vielfalt an Unternehmen und Anwendungen: Die Konzentration auf nur eine Funktion existiert kaum noch. Stattdessen gibt es, wie gesehen, viele Geschäftsmodelle und Anwendungen, die sowohl Messaging, Videoconferencing, teilweise auch Social Media-Funktionen oder Features für Kommunikation und Zusammenarbeit verbinden. Manche Messenger-Dienste profitieren von einer großen Nutzerbasis über Netzwerkeffekte. Andere wiederum sind ohnehin interoperabel, so dass die Zahl der Nutzer des jeweiligen Dienstes für dessen Attraktivität für sich genommen von geringer Bedeutung ist. Unterschiedlich ist auch die Bepreisung der Leistungen. Manche Dienste werden unentgeltlich angeboten, andere finanzieren sich über Entgelte für Basis- oder Zusatzleistungen. Der Preis als wichtiger Parameter hängt somit von völlig unterschiedlichen Größen ab. Aus diesen Gründen sind nicht alle theoretischen wissenschaftlichen Beiträge für alle Branchenteilnehmer

gleichermaßen relevant. Übersetzt in ökonomische Modelle bedeutet dies, dass **keine einheitlichen branchenweiten Modellbedingungen** definiert werden können. Vielmehr sehen sich modellgestützte Analysen daher bereits verschiedenen **Diagnoseschwierigkeiten** ausgesetzt. Die Vielfalt der Abhängigkeiten und Variablen lässt sich nur begrenzt abbilden. Es können nur ausgewählte Parameter beobachtet werden, wozu bestimmte Marktbedingungen festgesetzt werden müssen. Doch wie sieht die Ausgangssituation aus? Bestehen bereits Beeinträchtigungen des Wettbewerbs? Diese Fragen sind ebenso komplex wie der Analysegegenstand selbst oder die Formulierung konkreter Handlungsempfehlungen.

Man kann es auch umgekehrt formulieren. Es kommt eine große Bandbreite wissenschaftlicher Erkenntnisse in Frage, die die Untersuchungsthemen in irgendeiner Weise berühren. Konkrete Hinweise für Lösungsansätze können aber nicht ohne Weiteres abgeleitet werden.

Gerade die **praktische Umsetzung** von Interoperabilität stand in Analysen ausländischer Wettbewerbsbehörden stärker im Vordergrund als in rein wissenschaftlichen Veröffentlichungen. In den Untersuchungen von CMA (Competition and Markets Authority) und ACCC (Australian Competition & Consumer Commission) wurde die Dominanz insbesondere von Facebook und Google im Detail herausgearbeitet. Allerdings beziehen sich die Vorschläge der CMA hauptsächlich auf soziale Netzwerke und weniger auf Messenger-Dienste. Die ACCC beschäftigt sich zwar mit Messenger-Diensten, berücksichtigt Fragen der Interoperabilität dabei aber nicht. Dementsprechend unterschiedlich sind die Schlussfolgerungen: Während die australische ACCC von Initiativen zugunsten von mehr Interoperabilität abrät, sieht die britische CMA dies deutlich positiver und macht für den Bereich der sozialen Netzwerke konkrete Vorschläge, wie eine Interoperabilitätsverpflichtung aussehen könnte.⁹¹

Im Folgenden soll ein Überblick **über diejenigen Erklärungsansätze** gegeben werden, die in vergleichsweise enger Form mit dem Untersuchungsthema oder den Branchenteilnehmern in Verbindung stehen.

2. Theorie der Netzwerke

Mit dem Siegeszug der (Sozialen) Netzwerke und Plattformen hat sich eine intensive Diskussion um die zugrundeliegenden wissenschaftlichen Erklärungsansätze - die ökonomische Theorie der

⁹¹ Vgl. *Competition and Markets Authority (2020)*, Online platforms and digital advertising – Market study final report, Juli 2020, S. 5, abrufbar unter: <https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study> sowie *Australian Competition & Consumer Commission: Digital Platform Services Inquiry – Interim Report*, September 2019, abrufbar unter: <https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-2025/final-report>, beide: Stand: 7. September 2021.

Netzwerke⁹² - herausgebildet. Diese findet inzwischen nicht mehr nur im wissenschaftlichen Umfeld und in der Fachöffentlichkeit statt. Das Thema ist auch in der allgemeinen Verbraucheröffentlichkeit angekommen, wie zuletzt der im Mai dieses Jahres veröffentlichte Bericht des Verbraucherzentrale Bundesverbands anschaulich belegt.⁹³

Nutzer von Messenger- und Video-Diensten schätzen diejenigen Netzwerke besonders, bei denen sie viele andere Nutzer erreichen können (sog. positiver direkter Netzwerkeffekt).⁹⁴ Aus positiven Netzwerkeffekten können Selbstverstärkungseffekte resultieren: Große Netzwerke werden immer attraktiver für die Nutzer. Netzwerkeffekte können je nach ihrer Stärke aber auch dazu beitragen, dass ein bisher wettbewerblicher Markt ab einer bestimmten Konzentration zu kippen droht und sich die gesamte Nachfrage nur noch auf einen Anbieter konzentriert, während die übrigen Wettbewerber nicht die erforderliche kritische Größe erreichen, sog. **Tipping**.⁹⁵ Selbst ein Markt, der noch nicht als „getippt“ zu beschreiben ist, aber auf dem dennoch ein Anbieter die mit Abstand höchsten Nutzerzahlen aufweist, birgt die Gefahr einer starken Bindung an ein Netzwerk und hoher Wechselkosten für die Nutzer (**Lock-In-Effekte**).⁹⁶ Für Soziale Netzwerke - die in der Sektoruntersuchung teils durch eigene Messaging-Funktionen vertreten sind - sind demzufolge bereits Vorschläge zu möglichen Interoperabilitätsverpflichtungen geäußert worden. So spricht sich die Competition and Markets Authority (CMA) in ihrer Market Study zu Internetplattformen und digitaler Werbung dafür aus – in einem begrenzten Rahmen – Facebook zu mehr Interoperabilität zu verpflichten.⁹⁷

⁹² Vgl. *Katz/Shapiro*, Network Externalities, Competition, and Compatibility, *The American Economic Review*, 1985, 75(3), S. 424-440; *Farrell/Saloner*, Standardization, Compatibility, and Innovation, *The RAND Journal of Economics*, 1985, 16(1), S. 70-83.

⁹³ *Verbraucherzentrale Bundesverband* (2021), Interoperabilität bei Messenger-Diensten, 17. Mai 2021, abrufbar unter: https://www.vzbv.de/sites/default/files/2021-05/21-05-18_vzbv_Diskussionspapier_Interoperabilit%C3%A4t_Messenger.pdf, Stand: 6. September 2021.

⁹⁴ Vgl. für eine Einordnung aus wettbewerbsrechtlicher Perspektive z. B. *Bundeskartellamt*, Marktmacht von Plattformen und Netzwerken, Arbeitspapier, Juni 2016, abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Think-Tank-Bericht.pdf?__blob=publicationFile&v=2, Stand: 27. Oktober 2021.

⁹⁵ Vgl. *Bundeskartellamt*, B6-113/15, Arbeitspapier – Marktmacht von Plattformen und Netzwerken, Juni 2016, S. 104 ff. m.w.N.

⁹⁶ Vgl. *Autorité de la concurrence/Competition and Markets Authority*, The economics of open and closed systems, 2014, Rn. 2.20.

⁹⁷ Vgl. *Competition and Markets Authority*, Online platforms and digital advertising, Market study, Final report, Juli 2020, Rn. 8.49 ff und Appendix W.

Diese Gefahren haben dazu geführt, dass eine wesentliche Eigenschaft solcher Märkte – fehlende Interoperabilität – vermehrt ins Blickfeld rückte. Mit Interoperabilität ist die Hoffnung verbunden, die Sogwirkung von Netzwerkeffekten aufzulösen oder zumindest abmildern zu können, um so die Marktstrukturen zu verbessern.

Im Folgenden sollen Erkenntnisse zum Verhältnis von Interoperabilität, Wettbewerb und Innovation skizziert werden.

3. Auswirkungen auf Wettbewerb und Innovation

Die Auswirkungen von Interoperabilität auf Wettbewerb⁹⁸ und Innovation können aufgrund der genannten Wechselwirkung nicht ganz außer Betracht gelassen werden, zumal zu diesem Thema bis heute intensiv geforscht wird. Die **wettbewerblichen Auswirkungen** von Interoperabilität werden in zahlreichen theoretischen bzw. modelltheoretischen Analysen untersucht. Ergebnis der Mehrheit der Untersuchungen ist erstens, dass Interoperabilität zu einer Verlagerung des Wettbewerbs „um den Markt“ zu einem Wettbewerb „auf dem Markt“ führt. Zweitens sind je nach Marktstruktur und Verbraucherverhalten unterschiedliche Auswirkungen auf die **Konsumentenwohlfahrt** zu erwarten.

Was Innovationsanreize angeht, werden mit Interoperabilität wiederum meistens positive Effekte verbunden. Dies gilt jedoch vor allem für Märkte mit homogenen oder standardisierten Produkten. Demgegenüber zeichnen sich **digitale Märkte** durch eine stetige Innovationsentwicklung aus, die keinen festen Regeln folgt.⁹⁹ Eine mögliche Interoperabilitätsverpflichtung dürfte somit innovative Märkte deutlich beeinflussen. Hier werden vermehrt negative Effekte angeführt.

Interoperabilität setzt voraus, dass die verschiedenen Messenger- und Video-Dienste gemeinsame Funktionen anbieten, damit sich die Nutzer über die verschiedenen Kommunikationswege (Textnachrichten, Telefonie, Videotelefonie usw.) jeweils miteinander austauschen können. Dies birgt die Gefahr, dass einmal geschaffene interoperable Funktionen

⁹⁸ Vgl. z. B. *Belleflamme/Peitz*, Platforms and Network Effects, in: Corchon/Marini (Hrsg.), Handbook of Game Theory and Industrial Organization, Vol. II, 2018, S. 286-317, Kap. 3.3 sowie *Crémer/Rey/Tirole*, Connectivity in the Commercial Internet, The Journal of Industrial Economics, 2000, 48(4), 433-472 als auch *Katz/Shapiro*, Network Externalities, Competition, and Compatibility, The American Economic Review, 1985, 75(3), S. 424-440 oder *Malueg/Schwartz*, Compatibility incentives of a large network facing multiple rivals, Journal of Industrial Economics, 2002, 54(4), S. 527-567 und *Shy*, A Short Survey of Network Economics. Review of Industrial Organization, 2011, 38, S. 119–149, Kap. 3.1.

⁹⁹ *Cremer/de Montjoye/Schweitzer*, Competition Policy for the digital era, Report for the EU Commission, 2019, S. 35, abrufbar unter: <https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf>.

nicht mehr ausreichend weiterentwickelt werden. Wettbewerb um neue innovative Geschäftsmodelle sowie vom Nutzer wertgeschätzte **Produktdifferenzierung** könnten zurückgehen.

Je nach genauer Ausgestaltung einer Interoperabilitätsverpflichtung wäre ausweislich von Studien sogar zu befürchten, dass Innovationen eines Unternehmens für alle Wettbewerber verfügbar gemacht werden müssten. Verwertbarkeit und entsprechende Anreize, neue Entwicklungen voranzutreiben, würden beeinträchtigt. Dem Konzept der Interoperabilität werden Abstufungen zuerkannt, die diese negativen Auswirkungen abmildern sollen, indem nur **Basisfunktionen** interoperabel gestaltet werden. Der theoretische Anspruch der Befürworter ist, auf diese Weise Differenzierungsmöglichkeiten und Innovationsanreize zu erhalten, zumindest bei den Funktionen, die nicht unter die Interoperabilitätsverpflichtung fallen.

Mit Interoperabilität können gleichwohl auch in digitalen Geschäftsfeldern **positive Effekte** auf die Innovationstätigkeit einhergehen. Dazu werden in der Wissenschaft **niedrigere Markteintrittshürden** und **verringerte Lock-in-Effekte** gezählt. Positive Effekte könnten demnach auch bei Innovationen in dem Bereich der komplementären Produkte zu erwarten sein. Anreize zu Innovationen und Differenzierungsmöglichkeiten würden sich erhöhen, wenn neue Produkte oder Services auf das interoperable Produkt aufbauen können.¹⁰⁰ Als Beispiel kann das Internet selbst gelten, welches für einen enormen Innovationsschub in wahrscheinlich fast jedem Wirtschaftszweig gesorgt hat. Dies sei nicht zuletzt dadurch gelungen, dass die Daten in verschiedensten Formaten über das Internet übertragen werden können.¹⁰¹

Eine verminderte Innovationstätigkeit mit den oben beschriebenen Effekten würde sich auch auf die Bereiche **Datensicherheit und Datenschutz** auswirken, die für Messenger- und Video-Dienste besonders relevant sind. Empirische Ergebnisse dazu gibt es nach derzeitiger Kenntnis des Bundeskartellamts nicht. Es existieren eine Reihe von theoretischen Aufsätzen zu den potenziellen Wettbewerbseffekten im Zuge der Einführung der DSGVO bzw. zu den Auswirkungen von Datenportabilität und Interoperabilität auf das Datenschutzniveau, die die OECD in ihrer Veröffentlichung „Consumer Data Rights and Competition – Background note“¹⁰²

¹⁰⁰ Kerber, Data Sharing in IOT Ecosystems and Competition Law: the Example of Connected Cars, *Journal of Competition Law & Economics*, 2019, 15(4), S. 381–426, Kap. II.B.

¹⁰¹ Gasser, Interoperability in the Digital Ecosystem, The Berkman Center for Internet and Society Research Publication No. 2015-13, 2015, Kap. 3.1.

¹⁰² Vgl. OECD (2020): Consumer Data Rights and Competition – Background note, DAF/COMP(2020)1, abrufbar unter: [https://one.oecd.org/document/DAF/COMP/WD\(2020\)40/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)40/en/pdf), Stand: 8. September 2021.

zusammengestellt hat. Wie zu erwarten war, weisen die Ergebnisse ebenso wie die Studien zu den Wechselwirkungen mit Wettbewerb und Innovation nicht in eine eindeutige Richtung.

Wissenschaftliche Erkenntnisse existieren auch zu den Effekten einer Standardisierung und verschiedenen Umsetzungsfragen und Details in diesem Zusammenhang. Aufgrund der Masse an Erkenntnissen, wird im folgenden Abschnitt nur für die Branche der Messenger- und Video-Dienste auf wesentliche Aspekte kurz hingewiesen.

4. Effekte einer Standardisierung

Wenn Interoperabilität technisch umgesetzt werden soll, müssen die teilnehmenden Systeme so gestaltet sein, dass sie bestimmten interoperablen Standards genügen. Standardisierungen für das Internet, insb. für die Protokolle, werden – wie oben bereits dargelegt – üblicherweise von einer Standardisierungsorganisation, der Internet Engineering Task Force (IETF), umgesetzt, die am Ende eines langen Diskussionsprozesses **offene Standards** veröffentlicht.¹⁰³ Offene Standards bedeutet, dass jeder Dienst entsprechend seiner unternehmerischen Strategie über die Implementierung eines Standards entscheiden wird, was vermutlich von Art und Umfang des Interoperabilitätsvorhabens abhängen wird.

Je nach konkreter Ausgestaltung ihrer Entwicklung und Umsetzung sowie den Merkmalen der betroffenen Märkte können Standards nach wirtschaftlicher Erfahrung vorteilhafte und nachteilige Auswirkungen nach sich ziehen. Standards können grundsätzlich **Transaktionskosten senken, den Marktzutritt neuer Wettbewerber erleichtern und zur Verbreitung neuer Technologien** beitragen. Ob und inwieweit sich ein offener Standard aber durchsetzt, hängt wesentlich von der Qualität der im Standard einbezogenen Technologien sowie den Anpassungskosten der Akteure ab, die ihn umsetzen. **Anpassungskosten** entstehen, wenn Marktteilnehmer einen verpflichtenden Standard erfüllen müssen, den sie bisher nicht verwenden oder den sie nur mit erheblichem Aufwand implementieren können.¹⁰⁴

Nachhaltige **Wohlfahrtsverluste** werden erwartet, wenn ein einmal geschaffener interoperabler Standard nur inkrementelle oder keine Innovationen mehr erlaubt. Gerade im Bereich der Informationstechnologie dürfte sowohl das Potential als auch die Notwendigkeit zu „radikalen Innovationen“ bestehen. Wenn Netzwerkeffekte zugunsten eines einmal festgelegten interoperablen Standards wirken, dürften es vollkommen neue Technologien schwer haben,

¹⁰³ Vgl. zu anderen Verfahren der Standardisierung *Farrell/Simcoe*, Four Paths to Compatibility, in: *Peitz/Waldfoegel* (Hrsg.), *The Oxford Handbook of the Digital Economy*, 2012, S. 34-58, Kap. 3.2.

¹⁰⁴ So z.B. *Graef*, Mandating portability and interoperability in online social networks: regulatory and competition law issues in the European Union, *Telecommunications Policy*, 2015, 39(6), S. 502-514, Kap. 4.2. in Bezug auf soziale Netzwerke.

diese Strukturen aufzubrechen.¹⁰⁵ Qualitätswettbewerb ist nur noch innerhalb der gesetzten Standards möglich.

Einheitliche Standards müssten **nicht unbedingt effizient oder wünschenswert** sein. In Märkten, in denen effektiver Wettbewerb herrscht, können sich verschiedene Dienste, Produkte und Dienstleistungen mit unterschiedlichen Graden an Interoperabilität am Markt etablieren.¹⁰⁶ Nichtsdestotrotz kann in vielen Fällen eine Standardisierung bestimmter Technologien oder Funktionen entweder aus Effizienzgründen oder aufgrund der individuellen Verdienstmöglichkeiten ein wichtiges Ziel der Marktteilnehmer sein.

Die Erkenntnisprozesse, die den beschriebenen wissenschaftlichen Beiträgen zugrunde liegen, sind anspruchsvoll und komplex. Die praktische Umsetzung ist es aber noch viel mehr. Denn ein wesentlicher Parameter, der ihren Erfolg oder Misserfolg bestimmt, ist das Verbraucherverhalten. Inwieweit hier im Hinblick auf Datenschutzziele weiterhin Skepsis angebracht ist oder ob Hoffnung geschöpft werden kann, dazu wird das folgende Kapitel Hinweise geben.

IV. Verbraucherverhalten

Mit den Verbrauchern sind in der Diskussion um Interoperabilität und Datenschutz große Hoffnungen und Erwartungen verbunden. Sie sollen zu datenschutzfreundlichen Messenger- und Video-Diensten wechseln, sobald Interoperabilität hergestellt ist und sie ihre bisherigen Kontakte auch dann erreichen können, wenn diese nicht beim gleichen Dienst registriert sind. Weniger häufig wird die Kehrseite dieser möglichen Entwicklung thematisiert, nämlich dass nicht auszuschließen ist, dass die erhofften Wechselanreize auch sinken. Falls Funktionen weitestgehend vereinheitlicht sind, keine spürbaren Innovationen erwartet werden und Netzwerkeffekte über Anbietergrenzen hinweg wirken, so erkennen die Verbraucher möglicherweise nicht, warum sie den Anbieter wechseln sollten. Wird weiterhin eine gewisse **Trägheit** im Wechselverhalten von Verbrauchern berücksichtigt, so könnte es theoretisch nicht auszuschließen sein, dass große Anbieter durch Interoperabilität zusätzliche Nutzer gewinnen.¹⁰⁷ Das Verbraucherverhalten ist somit wesentlich für die Wirksamkeit möglicher Maßnahmen mit dem Ziel der Verbesserung des Datenschutzniveaus. Ungeklärt ist aber nicht nur, ob und inwieweit Verbraucher im Sinne eines verbesserten Datenschutzes von Interoperabilität profitieren würden. Unklar ist bereits, ob sie Interoperabilität diesbezüglich überhaupt wünschen.

¹⁰⁵ Gasser, Interoperability in the Digital Ecosystem, The Berkman Center for Internet and Society Research Publication No. 2015-13, 2015, Kap. 3.1.

¹⁰⁶ Kerber/Schweitzer, Interoperability in the Digital Economy, JIPTEC, 2017, Vol. 8, S. 39-58, Rn. 13.

¹⁰⁷ Siehe auch *Bitkom*, Positionspapier, S. 5 f. für ein ähnliches Argument.

Verbraucherbefragungen explizit zu diesem datenschutzbezogenen Thema sind nicht bekannt (mehr dazu unter 1.). Losgelöst von jeglichen Fragen der Interoperabilität standen Aspekte des Datenschutzes zwar in den letzten Jahren häufiger im Mittelpunkt von Verbraucherbefragungen. Allerdings klafft zwischen den von den Verbrauchern geäußerten Meinungen und Haltungen und deren praktischer Umsetzung bisher eine Lücke (vgl. dazu unter 2.). Daher verwundert es nicht, dass bisher keine empirischen Erkenntnisse existieren, die Aufschluss darüber geben, wie sich die Verbraucher zu Interoperabilität und Datenschutz stellen.

1. Interoperabilität oder Multi Homing?

Die Bundesnetzagentur hat im Frühjahr 2020 eine Verbraucherbefragung zu Online-Kommunikationsdiensten durchgeführt, die die Vielfalt des Verbraucherverhaltens bei der Nutzung von OTT-Diensten¹⁰⁸ offenlegt.

Die Nutzer von Messenger-Diensten können mehrere Dienste ohne größeren Aufwand parallel nutzen (sog. **Multi Homing**¹⁰⁹). Nach den Ergebnissen der Bundesnetzagentur verwenden 65% der Nutzer mindestens zwei verschiedene Messenger-Dienste parallel. Damit betreiben nahezu zwei Drittel der Befragten bereits Multi Homing. Offenbar nutzen mehr jüngere als ältere Verbraucher Multi Homing. In der Altersgruppe der bis 40-Jährigen nutzen 82% der Nutzer mindestens zwei OTT-Kommunikationsdienste. In der Gruppe der über 40-Jährigen ist dieses Verhalten deutlich schwächer ausgeprägt. Hier verwendet fast die Hälfte der Nutzer (46%) ausschließlich einen Dienst.¹¹⁰

Ein Teil der Verbraucher trennt anscheinend bewusst verschiedene Messenger-Dienste derart voneinander, dass sie für bestimmte Personen nur über bestimmte Kanäle erreichbar sind.¹¹¹ So

¹⁰⁸ Vgl. *Bundesnetzagentur*, Nutzung von OTT-Kommunikationsdiensten in Deutschland, Bericht 2020. Die zugrundeliegende Verbraucherbefragung wurde in der Zwischenzeit aktualisiert, die Ergebnisse war zum Zeitpunkt des Erscheinens des Zwischenberichts noch nicht öffentlich verfügbar.

¹⁰⁹ Wie dieser Begriff genau zu fassen ist, wird in der wettbewerbsrechtlichen Praxis intensiv diskutiert und nicht einheitlich aufgefasst. Nach einem engen Verständnis kann nur dann von Multi Homing gesprochen werden, wenn eine parallele Nutzung desselben Bedarfs gegeben ist. Für eine tiefere Erörterung vgl. z. B. *Bundeskartellamt*, Arbeitspapier, Marktmacht von Plattformen und Netzwerken, abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Think-Tank-Bericht.pdf?__blob=publicationFile&v=2, Stand: 28. Oktober 2021.

¹¹⁰ Vgl. *Bundesnetzagentur*, Nutzung von OTT-Kommunikationsdiensten in Deutschland, Bericht 2020, S. 19f.

¹¹¹ Vgl. z. B. *Arnold/Schneider*, An App for Every Step: A psychological perspective on interoperability of Mobile Messenger Apps, 28th European Regional Conference of the International Telecommunications Society, 2017.

wird die Kommunikation mit z. B. guten Freunden auf anderen Messenger-Diensten geführt als der Austausch in größeren Gruppen wie Schulklassen oder Sportvereinen. Eine Verpflichtung zur Interoperabilität wäre demnach schon aus diesen dem Datenschutzaspekt vorgelagerten Verbraucherpräferenzen eventuell – abhängig von der konkreten Ausgestaltung – nicht im Interesse dieser Verbraucher.

Demgegenüber könnte sich ein gewisses Interesse an Interoperabilität daraus ergeben, dass ausweislich der Befragung der Bundesnetzagentur fast ein Drittel der OTT-Nutzer bereits eine Person kontaktieren wollte, diese aber nicht erreichen konnten, weil von dieser Person nicht derselbe Messenger-Dienst verwendet wurde. Dementsprechend scheinen insbesondere **positive direkte Netzwerkeffekte** bei der Nutzung von OTT-Kommunikationsdiensten wichtig zu sein. Je mehr Kontakte von Nutzer über einen bestimmten Dienst erreicht werden können, desto höher ist offenbar tendenziell das Interesse, genau diesen Dienst ebenfalls zu nutzen.

Direkt nach **Interoperabilität** gefragt, ergibt sich laut Bundesnetzagentur dann aber kein eindeutiges Meinungsbild. 49% der befragten OTT-Nutzer finden es (eher) wichtig, dass sich Nutzer verschiedener Dienste untereinander erreichen können, während 48% diese Aussage als nicht oder überhaupt nichtzutreffend beschreiben. Gleichzeitig sehen 53% keinen Bedarf darin, Nachrichten an Nutzer anderer OTT-Kommunikationsdienste versenden zu können. 45% wären hierzu jedoch gerne in der Lage.¹¹² Für den nahezu gleich hohen Anteil der Verbraucher, die kein Interesse an Interoperabilität haben, gibt es nach den Ergebnissen der Verbraucherbefragung zwei Gründe. Erstens kann Multi Homing dem Befragungsergebnis nach unkompliziert ausgeweitet werden. Insgesamt gaben 27% der befragten OTT-Nutzer an, dass sie grundsätzlich bereit wären, sich einen weiteren OTT-Dienst zu installieren, um einen bestimmten Nutzer eines anderen Dienstes erreichen zu können. Zweitens kann immer noch auf die **klassischen Telekommunikationsdienste** wie SMS oder Telefonie zurückgegriffen werden, wenn ein Kommunikationspartner nicht über Messenger-Dienste erreichbar ist. Dies geben 87% der befragten OTT-Nutzer an.¹¹³

Außerdem möchten 67% der Befragten nicht von Nutzern anderer Dienste kontaktiert werden können und für den Fall, dass eine solche Kontaktaufnahme dennoch möglich wäre, würden 86%

¹¹² Vgl. *Bundesnetzagentur*, Nutzung von OTT-Kommunikationsdiensten in Deutschland, Bericht 2020, S. 24.

¹¹³ Vgl. *Bundesnetzagentur*, Nutzung von OTT-Kommunikationsdiensten in Deutschland, Bericht 2020, S. 24.

der Befragten selber entscheiden wollen, ob sie den Kontakt ermöglichen.¹¹⁴ Die Entscheidungshoheit zu behalten, scheint für viele Verbraucher sehr wichtig zu sein.

In einer wissenschaftlichen Veröffentlichung in der Fachzeitschrift „Telecommunications Policy“ kommen die Autoren zum Ergebnis, dass eine **Interoperabilitätsverpflichtung nicht den Verbraucherinteressen** entspricht. Verbraucher würden es schätzen, für unterschiedliche Kontakte je nach der Tiefe der Beziehung jeweils ausgewählte Messenger-Dienste zu verwenden. Die psychologischen Erkenntnisse der Autoren erklärten, warum Verbraucher unabhängig von Netzwerkeffekten eine enge Bindung zu bestimmten Messenger-Diensten unterhalten. Die Untersuchung basiert auf einer Befragung von 2044 Verbrauchern in Deutschland, die Messenger-Dienste wie Facebook Messenger, Line, Skype, WeChat and WhatsApp aber auch E-Mail und traditionelle Kommunikationsmittel verwendeten.¹¹⁵

Sofern ein marktweites Interoperabilitätsvorhaben angestrebt würde, erscheint eine datenschutzkonforme Interoperabilität den Verbraucherwünschen zu entsprechen, die eine solche **aktive Einwilligung der Nutzer** zur Erreichbarkeit durch andere Dienste voraussetzt. Insbesondere, wenn für die Erreichbarkeit anderer Nutzer ein zentraler Verzeichnisdienst der Nutzer der verschiedenen Dienste geschaffen werden muss, wünschen die Verbraucher offenbar, nach ihrer Zustimmung befragt zu werden, bevor sei in ein solches Verzeichnis aufgenommen werden.

2. Wunsch nach mehr Datenschutz?

Verbraucher äußern in Umfragen regelmäßig ein starkes Bedürfnis nach Privatsphäre, gehen mit ihren privaten Daten in der Praxis aber vergleichsweise sorglos um. Dieser Widerspruch wird als

¹¹⁴ Vgl. *Bundesnetzagentur*, Nutzung von OTT-Kommunikationsdiensten in Deutschland, Bericht 2020, S. 23 f.

¹¹⁵ Vgl. *Arnold/Schneider/Lennartz*, Interoperability of interpersonal communications services – A consumer perspective, in: *Telecommunications Policy*, Vol. 44, Issue 3, April 2020, abrufbar unter: <https://www.sciencedirect.com/science/article/abs/pii/S0308596120300197>, Stand: 8. September 2021.

Privacy Paradox bezeichnet.¹¹⁶ Einer Studie des Sinus-Instituts zufolge ist 93% der Deutschen der Schutz ihrer persönlichen Daten wichtig. Nur 1 % der Befragten war es überhaupt nicht wichtig, was mit ihren persönlichen Daten geschieht.¹¹⁷ Gleichzeitig hat eine Studie der Bitkom aus dem Jahr 2018 ergeben, dass WhatsApp von 81% der Internetnutzer in Deutschland verwendet wird und damit der beliebteste Messenger-Dienst ist, während Dienste, denen in der öffentlichen Meinung eine größere Datenschutzfreundlichkeit zugesprochen wird, eine deutlich geringere Wertschätzung erfahren.¹¹⁸ Die dahinterstehenden Ursachen sind komplex und dürfen auch die eingeschränkte **Wahlfreiheit** der Verbraucher („widerwillig“¹¹⁹ – d. h. lediglich mit unerwünschter Datenpreisgabe oder überhaupt nicht¹²⁰) sowie das Ausbleiben alternativer Angebote aufgrund fehlenden Wettbewerbs nicht ausblenden. Es kann zudem ein **Marktversagen** vorliegen, soweit keine datenschutzfreundlichen Angebote am Markt verfügbar

¹¹⁶ Vgl. für den folgenden Abschnitt und detailliertere Ausführungen Bundeskartellamt, Sektoruntersuchung Smart-TVs, Bericht Juli 2020, abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_SmartTVs_Bericht.pdf?__blob=publicationFile&v=5, Stand: 20. Oktober 2020, und die dort angegebene Literatur, wie z. B. *Norberg/Horne/Horne*, The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors, *Journal of Consumer Affairs* 2007, 100 - 126, abrufbar unter <https://onlinelibrary.wiley.com/doi/full/10.1111/j.1745-6606.2006.00070.x>. Im aktuellen wissenschaftlichen Diskurs findet sich indessen eine Vielzahl von (verhaltens-)ökonomischen Theorien, die das Privacy Paradox erklären können. Ein Überblick findet sich bei *Barth/de Jong*, The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review, *Telematics and Informatics* 2017, 1038 - 1058, abrufbar unter: <https://doi.org/10.1016/j.tele.2017.04.013>. Das Privacy Paradox lässt sich schließlich auch mit dem Konzept des sog. begrenzt rationalen Verhaltens („bounded rationality“) erklären.

¹¹⁷ *Sinus Institut/YouGov*, Studie zu Datenschutz: Mehrheit der Deutschen zweifelt an Datensicherheit (2018), abrufbar unter: <https://www.sinus-institut.de/veroeffentlichungen/meldungen/detail/news/studie-zu-datenschutz-mehrheit-der-deutschen-zweifelt-an-datensicherheit/news-a/show/news-c/NewsItem/>.

¹¹⁸ *Bitkom*, Neun von zehn Internetnutzern verwenden Messenger (bitkom.org, 02.05.2018), abrufbar unter: <https://www.bitkom.org/Presse/Presseinformation/Neun-von-zehn-Internetnutzern-verwenden-Messenger.html>.

¹¹⁹ Siehe *Borgesius/Kruikemeier/Boerman/Helberger*, Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation, *EDPL* 2017, 1, abrufbar unter: https://www.ivir.nl/publicaties/download/EDPL_2017_03.pdf.

¹²⁰ Vgl. für diesen Abschnitt *Bundeskartellamt*, Sektoruntersuchung Smart-TVs, Bericht Juli 2020, abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_SmartTVs_Bericht.pdf?__blob=publicationFile&v=5, Stand: 20. Oktober 2020, und die dort angegebene Literatur.

sind oder der Nutzer das Datenschutzniveau einzelner konkurrierender Anbieter nicht oder jedenfalls nicht mit vertretbarem Aufwand in Erfahrung bringen kann.¹²¹

Diese theoretischen Überlegungen scheinen in Grundzügen Strukturen und Wirkungsmechanismen im Umfeld bestimmter Messenger-Dienste widerzuspiegeln. Doch es gibt auch **Hinweise**, dass die genannten Schwierigkeiten die Verbraucher in ihrer Handlungsfreiheit tatsächlich einschränken: Bei einer Allensbach-Studie aus dem Jahr 2019¹²² gaben Nutzer von WhatsApp – also Personen, die sich bereits entschieden haben, die App trotz eventuell bestehender Bedenken zu nutzen – an, dass sie mit einigen Klauseln der WhatsApp-Datenschutzbestimmungen nicht einverstanden sind und diese ablehnen würden, wenn sie die Möglichkeit dazu hätten. Dazu zählen z. B. die Weitergabe der Daten ins Ausland oder der Zugriff auf die Adressdaten der eigenen Kontakte.¹²³

V. Ermittlungsergebnisse

1. Interoperabilität

Mit den Ermittlungsfragen hat das Bundeskartellamt die aktuelle Situation und die Chancen und Risiken von Interoperabilität aus Sicht der befragten Messenger- und Video-Dienste adressiert.

a) Interoperabilität im Spannungsfeld von Datensicherheit, Datenschutz und Investitionsbereitschaft

Es wird in den Antworten betont, zwischen Interoperabilität und Datenschutz gebe es keine direkte Beziehung. Interoperabilität habe keine Auswirkungen darauf, wie Anbieter persönliche Daten nutzen. Eine Untergrenze für das Datenschutzniveau im Markt würde durch geltende Datenschutzgesetze bestimmt. Aber wenn über Interoperabilitätsziele gesprochen werde,

¹²¹ Vgl. *Botta/Wiedemann*, The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the *Facebook Odyssey*, *The Antitrust Bulletin* 2019, S. 428, 432 ff., abrufbar unter <https://journals.sagepub.com/doi/pdf/10.1177/0003603X19863590>.

¹²² *Institut für Demoskopie Allensbach*, Freiwillige und informierte Einwilligung? Die Nutzerperspektive – Untersuchung im Auftrag der *Focus Magazin Verlag GmbH*, September 2019; die Ergebnisse der Untersuchung wurden dem Bundeskartellamt für die Sektoruntersuchung Smart-TVs freundlicherweise von der *Focus Magazin Verlag GmbH* zur Verfügung gestellt.

¹²³ *Institut für Demoskopie Allensbach*, Freiwillige und informierte Einwilligung? Die Nutzerperspektive – Untersuchung im Auftrag der *Focus Magazin Verlag GmbH*, September 2019; die Ergebnisse der Untersuchung wurden dem Bundeskartellamt freundlicherweise für die Sektoruntersuchung Smart-TVs von der *Focus Magazin Verlag GmbH* zur Verfügung gestellt.

müssten die Anforderungen der Datenschutzgesetze berücksichtigt werden. Interoperabilität mache die Datensicherheit und damit auch die Einhaltung der Datenschutzregelungen komplizierter. Außerdem leide unter Interoperabilität die Innovationstätigkeit, insb. auch, was Innovationen in den Bereichen Datensicherheit und Datenschutz angehe.

Auf den MLS-Standard sind die Befragten in diesem Zusammenhang nicht eingegangen,

Der überwiegende Teil der Befragten erwartet von einer Interoperabilitätsverpflichtung nachteilige Auswirkungen insb. auf Innovation, Datensicherheit und Datenschutz. Interoperabilität laufe auch wider Verbraucherinteressen, indem das Nutzererlebnis beeinträchtigt und Multi Homing, also die Unterhaltung von Nutzerkonten bei mehreren Messenger-Diensten, verhindert werde. Ein verpflichtendes Interoperabilitätsvorhaben führe dazu, dass es in allen genannten Bereichen nur noch zum **kleinsten gemeinsamen Nenner** komme.

Einige Stimmen halten die Probleme, die mit Interoperabilität einhergehen, „grundsätzlich für nicht unüberwindbar“. Schwierigkeiten bei Datenschutz und Datensicherheit könnten auf technischer Ebene behoben werden. Ein Anbieter verweist auf sein eigenes Geschäftsmodell, dessen „Herz“ Interoperabilität sei. Auch auf das freie Messaging-System Matrix wird verwiesen. Dort habe man die meisten Herausforderungen bereits gemeistert. Für erfolgreiche Standardisierungsprozesse gebe es ebenfalls zahlreiche Beispiele. Letztendlich sei alles eine Frage der **Investitionsbereitschaft**, alle anderen Argumente zählten hingegen nicht, gerade wenn Unternehmen mit einer „Kragenweite“ wie Microsoft, Google und Facebook involviert wären. Ein global agierender Video-Dienst weist darauf hin, dass Messenger- und Videoplattformen nicht im Hinblick auf Interoperabilität entwickelt worden wären. Eine technische Umgestaltung der Dienste würde nun enormen Aufwand und eine erhebliche Investitionsbereitschaft erfordern. Einige Marktteilnehmer erläutern, dass - isoliert und losgelöst von den negativen Wechselwirkungen mit Innovation und Verbraucherinteressen betrachtet - **technisch tatsächlich vieles möglich** sei, gerade was die Datensicherheit angehe.

Einige Videokonferenzanbieter beziehen hier eindeutig Stellung: Eine Interoperabilitätsverpflichtung würde bei Video-Diensten keinen Mehrertrag bringen. Video-Dienste wären untereinander bereits auf adäquatem Wege erreichbar. Neben dem Zugang über einen zugesendeten Link über den Web-Browser gebe es viele frei erhältliche Apps, um Verbindungen zu bestimmten Video-Diensten herzustellen. Auch sei gegenseitiger Zugang über Schnittstellen möglich. Eine Verpflichtung sei unnötig. Einziges Ergebnis einer verpflichtenden Interoperabilität sei weniger Wettbewerb und eine schlechtere Qualität für die Nutzer.

Inwieweit Qualitätswettbewerb über die ggf. standardisierten Funktionen hinaus bei Interoperabilität noch stattfinden kann, wurde in den Antworten nicht erörtert.

b) Bestehende oder geplante Interoperabilitätsregelungen

Das Bundeskartellamt hat die Branche befragt, ob und inwieweit Interoperabilität bereits praktiziert wird und ob innerhalb der nächsten 18 Monate weitere Interoperabilitätsvorhaben umgesetzt werden sollen.

Dabei wurde deutlich, dass die Entwicklungen innerhalb der verschiedenen Anbietergruppen unterschiedlich sind. Bei der Interpretation der Ermittlungsergebnisse ist zu berücksichtigen, dass der Begriff Interoperabilität **Austauschregelungen mit unterschiedlicher technischer Tiefe** bezeichnen kann.

So bezeichnen sich einzelne **Multi Messenger** als interoperabel. Allerdings ermöglichen Multi Messenger nicht den Austausch über Messenger-Systeme hinweg. Vielmehr bieten sie eine Softwareoberfläche, anhand der auf verschiedene Messenger-Dienste zugegriffen und Inhalte gelesen werden können. Kommuniziert werden kann dabei aber immer noch nur innerhalb eines Dienstes. Ansonsten muss ein Nutzer über „kopieren und einfügen“ seine Nachrichten in einen anderen Dienst übertragen.

Bei den **freien Messenger-Systemen** XMPP und Matrix sowie den für E-Mail genutzten Protokollen oder Systemen besteht unter den jeweiligen Clients eines Systems Interoperabilität. Der Austausch bei XMPP basiert auf dem standardisierten XMPP-Protokoll und wird über föderierte Server umgesetzt. Für den Zugang zu bestimmten anderen Messenger- und Video-Diensten werden Bridges¹²⁴ oder Bots¹²⁵ angeboten, die allerdings keine vollständige Interoperabilität gewährleisten können. Der Matrix-Client Element betont, die Bridges für Matrix wären für jeden überall erhältlich, was auch andere Befragte erwähnen. Ein XMPP-Client führt aus, es gebe Interoperabilitätslösungen für den Einsatz in Unternehmen zwischen XMPP und Cisco. Ein in Sachen Interoperabilität aktiver Video-Dienst erläutert, es gebe eine von ihm betriebene Serviceeinheit, über die sich Dritte mit dem Unternehmen verbinden könnten. Alle technischen Spezifikationen und nähere Bestimmungen zu den Anschlüssen lägen bei den interessierten Dritten selbst.

¹²⁴ Eine Bridge kann zwei Computernetze verbinden. Siehe für die technischen Einzelheiten *IP Insider*, Was ist eine (Netzwerk)- Bridge?, abrufbar unter: <https://www.ip-insider.de/was-ist-eine-netzwerk-bridge-a-902076/>, Stand: 9. September 2021.

¹²⁵ Unter einem Bot (von englisch *robot* ‚Roboter‘) versteht man ein Computerprogramm, das weitgehend automatisch sich wiederholende Aufgaben abarbeitet, ohne dabei auf eine Interaktion mit einem menschlichen Benutzer angewiesen zu sein, vgl. <https://de.wikipedia.org/wiki/Bot>, Stand: 19. August 2021.

Schließlich ist zu unterscheiden, ob Messenger- und Video-Dienste alle Voraussetzungen bieten, Interoperabilität herzustellen oder ob diese tatsächlich bereits in bilateralen oder multilateralen Beziehungen praktiziert wird.

Viele Anbieter mit **Open Source-Philosophie** verfolgen Interoperabilität als Geschäftsstrategie oder Leitbild. So nutzen Anbieter wie BigBlueBotton oder Jitsi Meet, die sich als Open Source bezeichnen, offene Standards (z. B. WebRTC), die Interoperabilität sicherstellen und grundsätzlich gegenüber allen Messenger- und Video-Diensten ermöglichen sollen.

Einige Branchenteilnehmer bieten Dritten verschiedene Wege an, mit ihnen Interoperabilität herzustellen. Bei Plattformen wie Rocket.Chat geschieht dies nach eigenen Angaben z. B. über **Föderation**, wo - wie bei den freien Messaging-Systemen - jeder Server Teil des Netzwerks werden kann, so dass Nutzer aller verbundenen Server miteinander kommunizieren können. Außerdem wird u. a. eine sog. WebHooks-Schnittstelle¹²⁶ angeboten sowie **Bridges und Importer**¹²⁷. Bei führenden Video-Diensten können Verbraucher zunächst einmal den gegenseitigen Zugang über einen Link im Web-Browser nutzen, ohne die App des anderen Video-Dienstes installieren zu müssen. Dies sei lt. Aussage einiger Befragter durch den Standard **WebRTC** ermöglicht worden und werde zwischen vielen Video-Diensten so praktiziert. Einzelne Video-Dienste stellen auch **öffentliche APIs**¹²⁸ (Application Programming Interface, Programmierschnittstelle) zur Verfügung. Es werden auch kostenpflichtige Add-ins angeboten. Auf diese Weise könnten Nutzer von Microsoft Teams beispielsweise aus ihrer Benutzeroberfläche heraus einen Videoanruf zu Zoom starten.

¹²⁶ Mit WebHooks (zusammengesetzt aus „Web“ und „Hook“, zu deutsch etwa Web-Haken) wird ein nicht-standardisiertes Verfahren zur Kommunikation von Servern bezeichnet, das im Rahmen des verteilten Rechnens oder der Nachrichtenorientierten Middleware genutzt wird. WebHooks ermöglichen es, einer Server-Software mitzuteilen, dass ein bestimmtes Ereignis eingetreten ist und eine Reaktion auf das Ereignis auszulösen, vgl. <https://de.wikipedia.org/wiki/WebHooks>, Stand: 17. August 2021.

¹²⁷ Ein **Importer** ist eine [Softwareanwendung](#), die eine [Datendatei](#) oder [Metadateninformationen](#) in einem Format einliest und über spezielle [Algorithmen](#) in ein anderes Format konvertiert, vgl. [https://en.wikipedia.org/wiki/Importer_\(computing\)](https://en.wikipedia.org/wiki/Importer_(computing)), Stand: 25. August 2021.

¹²⁸ Eine API (Application Programming Interface, Programmierschnittstelle) ist ein Satz von Befehlen, Funktionen, Protokollen und Objekten, die Programmierer verwenden können, um eine Software zu erstellen oder mit einem externen System zu interagieren. Sie stellt Entwicklern Standardbefehle für die Ausführung allgemeiner Operationen zur Verfügung, so dass Codes nicht von Grund auf neu geschrieben werden müssen. Die API – auch Programmierstelle genannt- ermöglicht es demnach Anwendungen miteinander zu kommunizieren. Die API ist nicht die Datenbank oder gar der Server, sondern der Code, der die Zugangspunkte für den Server regelt und die Kommunikation ermöglicht. Somit wird der Datenaustausch zwischen verschiedenen Systemen um ein Vielfaches beschleunigt und vereinfacht, siehe <https://www.talend.com/de/resources/was-ist-eine-api/>, Stand: 25. August 2021.

Gerade was zweiseitige Regelungen oder auf bestimmte Anbieter ausgerichtete Interoperabilitätsabkommen betrifft, sind die Dienste, die sich insb. auf Geschäftskunden konzentrieren, besonders aktiv. Dies gehe lt. Aussage der Befragten auf die hohen Anforderungen an technische Möglichkeiten und die entsprechenden Verdienstmöglichkeiten zurück. Im Zuge dieser Interoperabilitätsabkommen werden in der Befragung vor allem die Video-Dienste Microsoft Teams, Webex und Zoom genannt. Für Geschäftskunden wird Interoperabilität auch über **proprietäre APIs** initialisiert.

Zusatzleistungen im Bereich der Interoperabilität sind häufig kostenpflichtig. Bei Geschäftskunden mit speziellen technischen Anforderungen sei für Videokonferenzen u. ä. mehr Aufwand erforderlich. Geschäftskunden hätten meist spezielle Anforderungen, wie z. B. Videoräume mit Kameras, Mikrofonen, Touchscreens oder Lautsprechern. Für den Betrieb dieser Hardware werde sehr spezielle Software verwendet, was den Zugang erschwere. Technisch spezialisierte Dienstleister könnten diesen aber über ausgesuchte „Middle-Layer Software“ herstellen. Als Beispiel werden Anbieter wie der norwegische Provider Pepix¹²⁹ angeführt. Wenn Interoperabilität über proprietäre APIs hergestellt werden soll, könnten ebenfalls Dienstleister wie Software as a Service (SaaS)¹³⁰ -Unternehmen zum Einsatz kommen, wie z. B. das Unternehmen m.io¹³¹, über das Verbindungen zu führenden Video-Diensten wie Microsoft Teams, Webex, Zoom oder auch Slack hergestellt werden können. Auch das Open Source-Projekt Matterbridge biete Bridges zwischen einer Reihe von Chat-Protokollen an. Unterstützte Protokolle sind z. B. XMPP, Slack, Discord, Telegram, Rocket.Chat oder Matrix.¹³²

c) Umsetzung einer Interoperabilitätsverpflichtung, wie und für wen?

Das Bundeskartellamt hat die Messenger- und Video-Dienste zudem gefragt, wie ein Interoperabilitätsvorhaben umgesetzt werden sollte. Zur Auswahl standen eine gesetzliche Interoperabilitätsverpflichtung, ggf. auch nur für bestimmte Anbieter, oder eine freiwillige Initiative.

¹²⁹ Vgl. <https://docs.pexip.com/admin/interoperability.htm>, Stand: 25. August 2021.

¹³⁰ Software as a Service (SaaS) ist ein Teilbereich des Cloud Computings. Das SaaS-Modell basiert auf dem Grundsatz, dass die Software und die IT-Infrastruktur bei einem externen IT-Dienstleister betrieben und vom Kunden als Dienstleistung genutzt werden. Für die Nutzung von Online-Diensten wird ein internetfähiger Computer sowie die Internetanbindung an den externen IT-Dienstleister benötigt. Der Zugriff auf die Software wird meist über einen Webbrowser realisiert. Für die Nutzung und den Betrieb zahlt der Servicenehmer ein Nutzungsentgelt, siehe https://de.wikipedia.org/wiki/Software_as_a_Service, Stand: 25. August 2021.

¹³¹ Vgl. <https://m.io/external>, Stand: 23. August 2021.

¹³² Vgl. <https://www.univention.de/produkte/univention-app-center/app-katalog/matterbridge/>, Stand: 18. August 2021.

Damit einher ging die Frage nach einer Beteiligung des eigenen Dienstes und den Gründen für die jeweilige Entscheidung.

Eine **gesetzliche Interoperabilitätsverpflichtung** für alle Messenger-Dienste halten nur drei Befragte (allesamt freie Messenger-Clients) für hilfreich. Es wird argumentiert, nur eine gesetzliche Verpflichtung könne die Nutzerinteressen wiederherstellen. Eine Öffnung gegenüber Wettbewerbern widerspreche den Geschäftszielen der großen Anbieter. Hilfsweise sei auch eine Verpflichtung von Anbietern ab einer gewissen Anzahl an Nutzern denkbar.

Eine gesetzliche **Verpflichtung für die größten Anbieter** kann sich weniger als ein Fünftel der Befragten vorstellen. Auch hierbei handelt es sich hauptsächlich um freie Messenger und einzelne Software-Anbieter. Am häufigsten als zu verpflichtende Dienste genannt werden die bekannten Messenger-Dienste Facebook Messenger, Signal, Telegram und auch Threema, WhatsApp oder Zoom (alphabetische Reihenfolge). Alternativ könnten nach Meinung der Befragten Dienste mit einer Nutzerbasis, die eine bestimmte Schwelle überschreitet, wie z. B. mehr als eine Mio. Nutzer weltweit oder die „TOP 10-Anbieter“ oder Dienste mit einer Marktkapitalisierung von mehr als 100 Millionen US-Dollar mit der Verpflichtung bedacht werden. Ein Befragter führt aus, die „Betreiber der führenden Betriebssysteme“ sollten mit einer Interoperabilitätsverpflichtung belegt werden. Ein weiterer Befragter wendet sich ebenfalls den marktstarken Akteuren zu. Diese sollten es wenigstens unterlassen, technische Vorkehrungen zu treffen, um Nutzer davon abzuhalten, Software der Wettbewerber zu verwenden oder zu diesen zu wechseln.

Knapp die Hälfte der Befragten kann sich ein auf **Freiwilligkeit** fußendes Interoperabilitätsvorhaben vorstellen. Weniger als die Hälfte der Befürworter würde sich aber nur beteiligen. Diese Aussagen müssen allerdings vorsichtig interpretiert werden, da sowohl Befragte, die sich beteiligen würden, als auch diejenigen, die sich nicht beteiligen würden, ihre Einschätzung mit zahlreichen Anmerkungen, Voraussetzungen, Hinweisen und Einschränkungen versehen haben. Dies erscheint nachvollziehbar, da das mögliche Interoperabilitätsabkommen vom Bundeskartellamt in seiner Frage nicht näher spezifiziert wurde, um Vorfestlegungen und entsprechende gesteuerte Meinungsäußerungen zu vermeiden. Beteiligung oder Nicht-Beteiligung erscheint somit ein graduelles Phänomen zu sein. Die Entscheidung hängt offenbar maßgeblich vom eigenen Hintergrund sowie von Erfahrungen und Prognosen ab und sicherlich von der Möglichkeit, selber Einfluss auf die Entwicklung nehmen zu können. Letztendlich weisen alle Beteiligten auch darauf hin, dass es bei der Bewertung jeglicher Interoperabilitätsregelungen auf viele Details ankomme. Beispielsweise sei maßgeblich, welche technische Tiefe oder Sicherheit angestrebt werde, ob es also z. B. um Ende-zu-Ende-verschlüsselte Nachrichten gehe oder eher um ein SMS-Format, welches deutlich unsicherer sei.

Diese Einschätzung spiegelt sich auch darin wider, dass ein Großteil der Gründe, die den Ausschlag für Zustimmung oder Ablehnung geben, identisch ist. **Negative Auswirkungen auf Innovation, Datenschutz und Datensicherheit** werden von einem Großteil der Befragten sowohl mit eher zustimmender als auch mit skeptischer Haltung angeführt. In beiden Gruppen wird ebenfalls - wenn auch deutlich weniger häufig - erwähnt, dass ein Interoperabilitätsvorhaben für kleinere Branchenbeteiligte schwerer umzusetzen sein könnte als für große Messenger- und Video-Dienste. Die Entfaltungsmöglichkeiten von Newcomern könnten danach erschwert werden.

Insgesamt betrachtet nehmen einige Messenger- und Video-Dienste, die sich selbst als Open Source-Anbieter bezeichnen, eine **relativ klare, befürwortende Haltung** ein, auch ohne nähere Bestimmung des Interoperabilitätsvorhabens. Sie erfüllen die Voraussetzungen für Interoperabilität, die auch Teil des Geschäftsmodells und der dahinterstehenden Überzeugung ist. Zum anderen äußern sich freie Messenger-Clients zustimmend, die in der breiten Öffentlichkeit unbekannter sind: Interoperabilität sei aus ihrem Blickwinkel wichtig, um den Netzwerkeffekt aufzubrechen und Nutzer in die Lage zu versetzen, selbständig und freiwillig anhand diverser Kriterien wie Features und Datenschutz Entscheidungen zu treffen.

Auch bekannte Video-Dienste lehnen Interoperabilität nicht grundsätzlich ab. Sie betreiben bereits gewisse Interoperabilitätsvereinbarungen unterschiedlicher technischer Tiefe und bieten die notwendigen Schnittstellen an. Gerade bei den führenden Video-Diensten spielen - den Antworten zufolge - die Erfahrungen auf globalen technischen Märkten und das Vertrauen, hier selbst Impulse zu setzen und auf die technische Entwicklung Einfluss nehmen zu können, eine Rolle für ihre Haltung.

Diejenigen Messenger- und Video-Dienste, die sich nicht beteiligen würden, nennen hierfür neben Problemen bei Datenschutz, Innovation und Datensicherheit weitere, ganz unterschiedliche Gründe. Ursächlich ist zum einen häufig die **eigene Geschäftsstrategie**, die Interoperabilität nicht vorsieht. Dies wird – z. B. von großen ausländischen Konzernen – aus **Kostengründen** angeführt. Die Entwicklungskosten wären nicht refinanzierbar. Von der breiten Öffentlichkeit wenig beachtete Clients äußern Bedenken wegen des enormen „**Bürokratie**“- und **Technikaufwands**, den jegliches Interoperabilitätsvorhaben auslöse, ohne dies näher zu erläutern. Auch auf **fehlende Marktkenntnis** in Deutschland wird verwiesen, die es nicht erlaube, derart weitreichende strategische Entscheidungen zu treffen. Kleinere Anbieter fokussieren sich auf **Nischenangebote**, wie z. B. E-Learning, oder geschäftliche Kundengruppen, die keine Interoperabilität wünschen und größten Wert auf **Vertraulichkeit und höchste Sicherheit** ihrer Daten legen.

Zwei populäre Messenger- und Video-Dienste verweisen auf die **rechtlichen Voraussetzungen** einer möglichen gesetzlichen Interoperabilitätsverpflichtung. Eine solche Verpflichtung dürfe nur

aufgelegt werden, wenn diese erfüllt seien. Die Abhilfemaßnahme müsse sich positiv für kleinere Wettbewerber auswirken und Markteintritte fördern. Eine Verpflichtung könne nur unter den in Art. 61 Abs. 2 Unterabs. 2 EKEK genannten Bedingungen auferlegt werden, nämlich dann, wenn die „durchgehende Konnektivität zwischen Endnutzern (...) bedroht“ sei. Dieses Risiko sei derzeit nicht erkennbar. Traditionelle Telefondienste wären überall verfügbar. Multi Homing und Anbieterwechsel sei den Verbrauchern jederzeit möglich.

d) Auswirkungen von Interoperabilität

Das Bundeskartellamt hat die Branche schließlich auch zu den allgemeinen Auswirkungen von Interoperabilität ausführlich befragt. Im Einzelnen wurden die Messenger- und Video-Dienste gebeten, ihre Einschätzung zu den Effekten auf Innovation, Datensicherheit und Datenschutz sowie Wettbewerbsintensität, Nutzerzahlen und Umsätze anzugeben.

aa) Innovationsanreize und Differenzierungsmöglichkeiten

Der weit überwiegende Teil der Befragten äußert, dass Interoperabilität und die damit einhergehende Standardisierung **Innovationsprozesse hemmen und Produktdifferenzierung schwächen** würde. Man müsse sich auf den kleinsten gemeinsamen Nenner einigen, was auch zu Fehlallokationen führe. Sowohl Dienste mit Schwerpunkt Messaging, die bei Verbrauchern besonders populär sind, als auch bekannte Video-Dienste argumentieren in dieser Frage einheitlich. Da die Angebote durch Interoperabilität einheitlicher würden, wären Kunden weniger geneigt, zwischen den Anbietern zu wechseln. Anbieter hätten dann wiederum weniger Anreize, neue innovative Funktionen zu entwickeln. „Perfekte Interoperabilität“ würde Technologien, die als Standard der Verpflichtung zu Grunde gelegt würden, „betonieren“.

Ein führender Videokonferenzanbieter verweist auf bereits bestehenden lebhaften Wettbewerb im Verbraucher- und im Geschäftskundensegment. Es gebe eine Reihe von Anbietern, die sowohl über den Preis als auch über die Entwicklung neuer Funktionen miteinander in intensivem Wettbewerb um Kunden - insb. auch Geschäftskunden - stünden. Wettbewerber erklären, Video-Dienste unterschieden sich voneinander durch unterschiedliche Funktionen, die sie **zusätzlich zu den Kernfunktionen** Audio- und Videoübertragung anbieten. Das gelte nicht nur für das Geschäftskundensegment, sondern auch für Verbraucherangebote. Dazu gehörten beispielsweise das Handheben, Emojis im Konferenzchat, Inhalte teilen, Einspielen visueller Hintergründe etc. Wenn das Teilen des Bildschirms oder Präsentationsmodi nicht länger während Videokonferenzen funktionierten, da einige der über ihre Nutzer beteiligten Dienste diese nicht unterstützen würden, wären Weiterentwicklungen in diesem Bereich nicht sinnvoll. So komme es immer nur zum kleinsten gemeinsamen Nenner. Die Branche könne sich nur so vorwärtsbewegen, wie der langsamste Teilnehmer mithalten könne.

Dies gelte umso mehr für komplexere Funktionen, auch im **geschäftlichen Bereich**. Bestimmte Video-Funktionen könnten in Datenverarbeitungs- oder Tabellenkalkulationsprogrammen oder Präsentationen eingebunden werden. Wenn dies unter einer verpflichtenden Interoperabilität nicht mehr allen Nutzern möglich sei, gehe dies wider ihre Interessen. Anbieter würden in solche Funktionen dann nicht mehr investieren.

Einige Anbieter nennen **Beispiele** für Bereiche, in denen die Innovationstätigkeit durch Interoperabilität in der Vergangenheit zum Erliegen kam. Ein Open Source-Anbieter zieht den Vergleich mit traditionellen Telefondiensten heran. Diese wären interoperabel, aber es gebe enge Grenzen, was jeder Anbieter umsetzen könne. Wenn andere Dienste z. B. „HD Audio“ nicht unterstützten, könne das eigene Angebot nicht verwirklicht werden. Diese Innovationslücke bei traditioneller Telefonie habe gerade die Messenger-Dienste hervorgebracht, die relativ schnell neue Funktionen und Fähigkeiten auf den Markt bringen können. Dies ginge wohl verloren, wenn die Dienste standardisiert würden und jegliche neuen Funktionen mit den vereinbarten Standards arbeiten müssten. Als Negativbeispiel wird auch auf die Entwicklung von E-Mail verwiesen, die technisch an einem gewissen Punkt stehen geblieben sei. Auch unter Datenschutzgesichtspunkten hätte es irgendwann keine Weiterentwicklung gegeben.

Einzelne Wettbewerber der führenden Dienste beklagen, dass auch die **Komplexität** steige, wenn Interoperabilität umgesetzt werden müsse. Kundendienst und Support für die Nutzer würden schwieriger und erforderten mehr Zeit und Aufwand. Entwicklerteams müssten dafür eingesetzt werden, statt sich der Entwicklung neuer und innovativer Funktionen zu widmen. Dieser Prozess fordere insbesondere kleinere Wettbewerber heraus und benachteilige sie. Wenn Interoperabilität forciert und Funktionen standardisiert würden, werde dies die großen Unternehmen begünstigen. Sie würden die Standards entsprechend ihrer Zwecke/Bedürfnisse und Ressourcen setzen. Kleinere Wettbewerber würden ihre Produkte daran anpassen müssen, was zulasten der Innovationen ginge, die sie ansonsten entwickelt hätten. Dies habe zwei Effekte: Zum einen würden Innovationstätigkeit und Produktvielfalt zu Lasten der Verbraucher zurückgehen. Zweitens werde die **Vormachtstellung der größten Akteure** zementiert. Abwanderungen bei kleinen Wettbewerbern wären absehbar, da sie ihrer Differenzierungsmöglichkeiten beraubt wären.

Auf mögliche Open Source-Implementierungen eines Standards, z. B. OpenMLS, wird in den Antworten nicht eingegangen.

Das „Internet der Verbraucher“ sei bisher so erfolgreich gewesen, da „Innovation ohne Erlaubnis“ möglich war. Zusammenstellungen (sog. „Sets“) an Funktionen waren nicht standardisiert, so dass kleinere, innovative Unternehmen neben den großen Wettbewerbern Geschäftsfelder erschließen konnten.

Es sind wiederum einige freie Messenger-Clients und einzelne andere Stimmen, die anders argumentieren: Bei Interoperabilität hätten viele unabhängige Dienste mit neuen Ideen eine Chance. Die großen kommerziellen Anbieter von Chat-Diensten würden in einem stärkeren Wettbewerb stehen, da Nutzer leichter wechseln könnten. Durch den erhöhten Wettbewerb und die Einhaltung eines gemeinsamen interoperablen Standards müssten sich die Anbieter von Clients oder auch Server-Diensten durch andere Alleinstellungsmerkmale, wie beispielsweise eine besonders gut zu bedienende Benutzeroberfläche, von anderen Anbietern absetzen. Das erhöhe die Innovationstätigkeit. Die etablierten Anbieter könnten sich nicht mehr auf ihrer großen Nutzerbasis ausruhen. Die Unternehmen könnten sich mehr auf die Entwicklung von Funktionen konzentrieren, und es wäre einfacher für neue Akteure, in den Markt einzutreten.

bb) Verbraucherinteressen (Nutzererlebnis und Multi Homing)

Nutzererlebnis

Mehrere Dienste nehmen die Perspektive der Verbraucher ein und sorgen sich um das Nutzererlebnis. Unterschiedliche Einschätzungen ergeben sich insb. auch daraus, dass die Anbieter unterschiedlich aufgestellt sind. So existieren z. B. Social Media-Plattformen, bei denen es um ein multifunktionales Nutzererlebnis geht, im Vergleich zu auf sicheres oder datenschutzfreundliches Messaging oder fortschrittliches Videoconferencing konzentrierten Diensten.

Verschiedene Betreiber von Social Media-Plattformen halten fest, selbst wenn alle erdenkliche Zeit und Ressourcen in einen interoperablen Messenger-Dienst investiert würden, wären die Funktionen nicht mit dem heutigen Angebot vergleichbar und für die Nutzer nicht mehr interessant. Das **Nutzererlebnis** sei dann minderwertig. Dies gelte auch, wenn es bei Interoperabilität nur zu einer Vereinbarung über Basis-Funktionen käme, und weitere **zusätzliche Funktionen** daneben betrieben werden könnten. Abgesehen davon, dass dies ebenfalls außerordentlich aufwendig sei, könne der Anspruch der heutigen Nutzer nicht erfüllt werden. Das Angebot von zusätzlichen Funktionen wie Umfragen, Sticker, Shops, Kataloge, Bezahlformen in Chat-Apps laufe auch über Server, was bei Interoperabilität wohl nicht beibehalten werden könne.

Ein weiterer Anbieter erläutert ebenfalls, Server wären so konfiguriert, dass es bestimmte Kanäle für bestimmte Themen gebe. Das könne so nicht mit anderen Diensten kompatibel gestaltet werden. Interoperabilität nur für die Messaging-Funktion wäre theoretisch denkbar. Aber dann würde das Nutzererlebnis, insb. für Sprach- und Videonachrichten, stark sinken. Man müsse sich am Anbieter mit der schlechtesten Performance orientieren.

Das interoperable Produkt ähnele wahrscheinlich der SMS, einem Produkt, das nicht mit Video- oder Audioelementen versehen sei, nicht verschlüsselt werde oder nur mit begrenzten Sicherheitsvorkehrungen versehen werden könne. Ein solch veraltetes Produkt könnte nicht angeboten werden. Es würde von Verbrauchern auch gar nicht gewünscht. Sie würden von ihrem

Dienst andere Nutzererlebnisse erwarten. Erfolgreiche Produkte gingen aus dynamischem Wettbewerb mit ständigen Weiterentwicklungen und Verbesserungen hervor. Dazu komme es unter Interoperabilität nicht.

Generell würde es bei Interoperabilität auch schwieriger, „Standards und Policy“ der Plattform umzusetzen und Missbrauch anzugehen.

Auch ein anderer Befragter weist darauf hin, dass es für die Verbraucher schwierig zu verstehen sein könnte, wenn sie bestimmte Funktionen, wie z. B. „Umfragen“ oder „selbstzerstörende Nachrichten“ unter Interoperabilität nicht mehr oder dann doch nur mit Nutzern desselben Dienstes verwenden können.

Multi Homing

Schließlich weisen mehrere vorrangig von Verbrauchern genutzte Messenger- und Video-Dienste darauf hin, dass die Verbraucher verschiedene Kommunikationskanäle für unterschiedliche Bedürfnisse nutzen (Multi Homing). Beispielsweise würde WhatsApp verwendet, um mit der Familie zu kommunizieren und andere Dienste für berufliche Zwecke. Eine verpflichtende Interoperabilität würde den Verbrauchern diese Flexibilität nehmen.

Es gebe keine Hinweise, dass Verbraucher Interoperabilität brauchten, „es sei denn, man füttere sie mit irreführenden Aussagen, z. B. dass Videotelefonie wie Sprachtelefonie funktionieren sollte.“

Multi Homing wäre weit verbreitet und werde von den Verbrauchern geschätzt. Die meisten Dienste könnten von verschiedenen Geräten ohne zusätzliche Kosten genutzt werden. Die Nutzer könnten sich so ihre Messenger-Welt zuschneiden und bestimmte Funktionen für bestimmte Aufgaben oder Nutzergruppen verwenden (z. B. ein Dienst für Familie und Freunde, einer für Geschäftliches usw.). Den Verbrauchern diese Möglichkeit zu nehmen, entspreche nicht den Grundsätzen der Wettbewerbspolitik.

cc) Datensicherheit

Nach Ansicht der Mehrheit der Branche würden die sinkenden Innovationsanreize unter Interoperabilität auch Entwicklungen für die Datensicherheit betreffen. Die so antwortenden Branchenteilnehmer prognostizieren, dass im Zuge von Interoperabilität eine Untergrenze - der kleinste gemeinsame Nenner – geschaffen werde. Insbesondere als datenschutzfreundlich bekannte Anbieter tragen diese Argumentation vor.

Einige Befragte erwähnen auch grundsätzliche Sicherheitsaspekte, wie z. B. dass die Öffnung des eigenen Ökosystems für andere Dienste die Möglichkeiten begrenze, Spam und Betrug zu verhindern. Ein anderer Dienst meint, durch Interoperabilität würden sichere Systeme für Anbieter geöffnet, die Datensicherheit nicht ernst nähmen. Die meisten Marktteilnehmer richten das Augenmerk aber auf die Verschlüsselung.

Verschlüsselung

Ein global agierender Dienst verweist hier auf die Entwicklung des **MLS-Standards**. Bei jeglichen Bemühungen um Interoperabilität müsse die Datensicherheit im Blick behalten werden. Eine Interoperabilitätsverpflichtung dürfe der Verabschiedung nicht zuvorkommen. Dies gehe dann auf Kosten der Datensicherheit in Form einer fortschrittlichen Ende-zu-Ende-Verschlüsselung.

Von vielen anderen Messenger- und Video-Diensten wird bezweifelt, dass bei Interoperabilität eine sichere Verschlüsselung umgesetzt werden kann. Da die Ende-zu-Ende-Verschlüsselung unter Interoperabilität ihrer Darstellung zufolge nicht funktionieren, müssten viele externe APIs bereitgestellt werden, die missbraucht werden könnten.

Die Messenger- und Video-Dienste, die im Zuge von Interoperabilität bei Fragen der Verschlüsselung nur den kleinsten gemeinsamen Nenner verwirklicht sehen, nennen als solchen die Transportverschlüsselung. Es sei nicht möglich, die Ende-zu-Ende-Verschlüsselung unter Interoperabilität beizubehalten. Dazu müssten alle Anbieter der interoperablen Funktionen das gleiche Protokoll verwenden. Andere Befragte halten fest, die Ende-zu-Ende-Verschlüsselung müsse bei Interoperabilität anbieter- und protokollübergreifend entwickelt werden. Technisch gehe es darum, sich auf einen Standard zu einigen, der Ende-zu-Ende-Verschlüsselung unter Interoperabilität ermögliche. Die Schwierigkeiten lägen bei der Videokommunikation und einer Mehrpunkt Ende-zu-Ende-Verschlüsselung mit dem Austausch von Schlüsseln zwischen unterschiedlichen Anbietern. Außerdem müssten die Geräte der Nutzer fähig sein, die anspruchsvolle Software zu betreiben. Ältere oder weniger gute Geräte wären hier im Nachteil, was Nutzer von den Diensten ausschließen könne. Eine Vielzahl an Dienstleistern sei wahrscheinlich notwendig, um die Server-Infrastruktur zu verwalten, was alles noch komplizierter mache. Eine Standardisierung erfordere, dass sich alle Beteiligten einigen, wie die technische Infrastruktur gestaltet werde, wer für Hosting und das Servermanagement verantwortlich sei. All dies würde signifikante Investitionen erfordern und wahrscheinlich Jahre dauern.

Einige freie Messenger-Clients schätzen die Auswirkungen von Interoperabilität positiver ein. Durch die Standardisierung von interoperablen Schnittstellen werde sich das Datensicherheitsniveau erhöhen. Verbraucher könnten zu sicheren Messenger- und Video-Diensten wechseln.

Einheitliche Identifier / Identitätsmanagement

Wenn Ende-zu-Ende-Verschlüsselung verwirklicht werden solle, sei lt. Aussage einiger Befragter ein **Identity Management**, das mit den vielen verschiedenen Diensten zusammenarbeiten könne, erforderlich. Führende Messenger- und Video-Dienste wie Facebook Messenger, Discord, iMessage/FaceTime, Microsoft Teams etc. verwendeten ihre eigenen Identifier. Ein entsprechendes Management sei eine technische Herausforderung, die auch hohe

Anforderungen an den Datenschutz stelle. Es müsse gegenseitiger Zugang zu allen Identitätsinformationen zwischen allen interoperablen Messaging- und Video-Systemen geben. Gleichzeitig müsse die Sicherheit von **Metadaten** garantiert werden. Eine technische Lösung dafür existiere noch nicht.

Ein Anbieter, der sich insb. an Nutzer wendet, die auf Datenschutz großen Wert legen, resümiert, all dies sei sicherlich nicht im Sinne der Verbraucher. Für die Nutzer werde die Sicherheit der Kommunikation intransparent und ungewiss. Der Anbieter führt auch an, die Nutzer wüssten nicht, welche App das Gegenüber verwendet.

dd) Datenschutz

Positive Auswirkungen von Interoperabilität auf den Datenschutz werden von einigen freien Messenger-Clients und einzelnen anderen Stimmen erwartet, während der Großteil der Befragten Bedenken äußert.

Nutzer könnten bei Interoperabilität einfacher zu datenschutzfreundlichen und sicheren Diensten wechseln. Anbieter, die im Vergleich zu einem dann unter Interoperabilität geltenden gemeinsamen Standard schlechteren Datenschutz böten, hätten einen Wettbewerbsnachteil, den sie beseitigen müssten.

Die Befragten, die Bedenken äußern, sprechen - wie auch bei der Datensicherheit - vom kleinsten gemeinsamen Nenner, der unter Interoperabilität beim Datenschutz nur noch praktiziert werde (Beispiel: Verwendung der Telefonnummer als Identifier). Schon heute wären die großen Plattformen datenschutzrechtlich nicht unter Kontrolle.

Die wichtigste Herausforderung sei dann, Dienste zu motivieren, mehr als die **Untergrenze** in Sachen Datenschutz zu erreichen. Anstelle verschiedener, von Diensten angebotener Datenschutzlevel (mit der Untergrenze DSGVO), wie es derzeit der Fall sei, würde der Markt unter einer Interoperabilitätsverpflichtung nur belohnen, wenn die Untergrenze erreicht werde, mehr nicht. Innovationen für den Datenschutz oder die Datensicherheit wären verloren.

Außerdem würden personenbezogene Daten auf mehrere Anbieter verteilt, an deren Seriosität ggf. Zweifel bestünden. Ein Video-Dienst teilt diese Sorge und verdeutlicht dies folgendermaßen: Bisher könne vor „Datenverlust“ geschützt werden, indem es z. B. bei Firmendaten nicht möglich sei, geschäftliche Informationen durch „ausschneiden und kopieren“ aus geschäftlichen Nachrichten herauszulösen und nach außen zu tragen. Aber wenn dies unter Interoperabilität nicht mehr vom Anbieter allein überwacht werden könne, gehe dieser Schutz verloren.

Weitere Probleme beim Datenschutz werden nach Angaben der Branche durch die **Internationalität** des zugrundeliegenden Geschäfts ausgelöst. Ein deutscher Anbieter bezweifelt, dass europäische und amerikanische Datenschutzbehörden übereinkommen werden. Ein anderer europäischer Dienst verweist auf mangelnden Datenschutz bei nicht europäischen

Anbietern. Einige Dienste äußern die Sorge, personenbezogenen Daten wären bei Interoperabilität dann für nicht vertrauenswürdige Dienste aus dem Ausland zugänglich. Es komme auf die Rechtsdurchsetzung und Überprüfung (Auditing) auch für Details an.

Auch während des Standardisierungsprozesses müssten Verbraucherrechte durchgesetzt und Verbraucherrechtsverstöße verfolgt werden, wenn große Marktteilnehmer sich nicht an die Regeln hielten.

Gegen internationale Datensammler helfe nur „Vollverschlüsselung“, bei Verfügbarkeit der Quellcodes zumindest der Client-Software, um zu verhindern, dass die App kopiert und anderweitig verwendet werde.

Als Risiko für den Datenschutz wird von einigen Befragten auch die **Zentralisierung** bei Interoperabilität genannt, insbesondere wenn es um **Metadaten** geht. Kommunikations-Metadaten wären für den Datenschutz höchst brisant. Je mehr unterschiedliche Anbieter in die Kommunikation eingebunden würden, desto mehr Angriffspunkte gebe es für die Ausspähung dieser Daten. Zentralisierung sei eine gefährliche Dynamik hierfür, da plötzlich all diese Daten an nur einem einzigen Punkt lägen, was die Angriffsfläche ebenso stark erhöhe. Dieses Dilemma sei nur in einem serverlosen, verteilten Kommunikationsnetzwerk lösbar. Ein anderer sinnvoller Umgang damit sei, verschiedene Werkzeuge anzubieten, und die Lösung ihrer Probleme den Nutzern selbst zu überlassen.

Daran schließt sich die Frage an, **wer die zentralisierten Daten überwacht** bzw. darüber verfügt und wie Verbraucher noch ihre Betroffenenrechte ausüben können. Die Anbieter selbst müssten ihre Daten mit anderen Messenger- und Video-Diensten teilen und würden die Kontrolle über die Daten ihrer Nutzer verlieren, wären aber weiterhin verantwortlich, alle Funktionen anzubieten.

ee) Nutzerzahlen und Umsätze

Mehrere führende Dienste aus dem Verbraucher- und auch aus dem Geschäftskundensegment erwarten, dass ihr Angebot weniger attraktiv wird und die Nutzerzahlen sinken, da Interoperabilität dazu zwingt, sich auf den kleinsten gemeinsamen Nenner zu einigen. Dadurch leide die „User Experience“ im Zuge schlechterer Servicequalität, was sich insbesondere bei Geschäftskunden negativ auswirken werde. Einzelne Wettbewerber der führenden Anbieter rechnen im Zuge von Interoperabilität ebenfalls mit **sinkenden Nutzerzahlen** für ihren Dienst. Wenn Differenzierungsmöglichkeiten verschwänden, fielen Netzwerkeffekte wieder verstärkt ins Gewicht und die die Marktführer würden wieder attraktiver.

In den Antworten wurde nicht thematisiert, ob und inwieweit von den Messenger- und Video-Diensten bei Interoperabilität zusätzlich zu den standardisierten interoperablen Funktionen noch individuelle Funktionen angeboten werden können.

Kleinere Video-Dienste hegen andere Erwartungen: Interoperabilität senke die Hürden, Video-Dienste zu nutzen. Es würden mehr Nischenangebote verfügbar werden, die den Bedürfnissen der Abnehmer besser entsprechen.

Ein Open Source-Anbieter erwartet keine besonderen Effekte. Das entsprechende Angebot sei schon weit verbreitet.

Viele freie Messenger-Clients rechnen mit steigenden Nutzerzahlen für ihre Anwendungen, wenn es zu marktweiter Interoperabilität käme. Nutzer würden sich auf die Dienste verteilen, wenn es keine geschlossenen Systeme mehr gebe. Es könnten mehr Nutzer erreicht werden, so dass auch nicht mehr so viele Messenger gleichzeitig betrieben werden müssten. Bessere Austauschmöglichkeiten würden die Nutzer auf bereits existierende Lösungen aufmerksam machen. Interoperabilität mit den bisher abgeschotteten großen Diensten steigern auch die **Attraktivität des offenen Netzwerks**.

Insgesamt scheint die Branche für die Entwicklung der **Umsätze** keine wesentlichen Veränderungen durch Interoperabilität zu erwarten. Vereinzelt überwiegen die negativen Erwartungen. Für die Dienste, die mit sinkender Nachfrage aufgrund schlechterer Qualität eines interoperablen Funktionen-Sets rechnen sowie Dienste, die Kundenabwanderungen befürchten, wird sich die Situation in den Umsätzen widerspiegeln. Ein datenschutzorientierter Anbieter resümiert mit „niemand bezahlt, wenn es das vorgeblich selbe gratis gibt“.

ff) Wettbewerbsintensität

Bei der Bewertung der Wettbewerbsintensität zeigt sich ein sehr uneinheitliches Bild.

Einige Videokonferenzanbieter bezeichnen ihr Wettbewerbsumfeld als hoch kompetitiv. Etablierte bekannte Namen stünden mit Newcomern und Nischenanbietern im Wettbewerb. Ein Anbieter gibt an, sich auch über ein großes Angebot an Interoperabilitätslösungen von seinen Wettbewerbern zu differenzieren. Auch ein freier Messenger-Client fürchtet den **Verlust seines Alleinstellungsmerkmals**, nämlich Interoperabilität. Aufgrund der geringeren Differenzierungsmöglichkeiten wird eine sinkende Wettbewerbsintensität unter Interoperabilität auch von anderen Video-Diensten befürchtet. Investitionen in Produktqualität und -sicherheit würden sich nicht mehr auszahlen.

Diese Argumentation wird auch im eher verbraucherorientierten Messaging-Bereich angeführt: Wenn kleine Dienste sich im Zuge einer Interoperabilitätsverpflichtung nicht mehr durch besondere Angebote auszeichnen könnten, würden die Nutzer zu den großen Plattformen abwandern. Die Position der **Marktführer werde zementiert** und der Wettbewerb erlahme. Ein Anbieter vermutet, dass der Wettbewerb sich dann hauptsächlich zwischen den großen amerikanischen Plattformen abspielen werde.

Einzelne Stimmen halten genau die umgekehrte Reaktion für wahrscheinlich: Interoperabilität würde dazu führen, dass kleinere Unternehmen mit Nischenangeboten für die Nutzer größerer Dienste attraktiver werden. Auch einige andere freie Messenger-Clients erwarten demgegenüber eine **erhöhte Wettbewerbsintensität**, wenn die Verbraucher im Zuge von verpflichtender Interoperabilität nicht mehr an die Inselsysteme gebunden wären und leichter wechseln könnten.

2. Interoperabilität und Standardisierung im Lichte der Brancheninteressen

a) Der richtige Weg?

Ein möglicher Standardisierungsprozess im Zuge eines insb. verpflichtenden Interoperabilitätsvorhabens wird von dem Großteil der Messenger- und Video-Dienste kritisch gesehen.

Diskutiert wird, inwieweit Interoperabilität für die betroffenen Märkte geeignet sei, um positive Effekte zu erzielen. Normalerweise würden mit Interoperabilität kompetitive und dynamische Märkte verbunden. Interoperabilität sei ein probates Mittel bei standardisierten, homogenen Dienstleistungen mit hoher Marktdurchdringung wie Telefonie oder Retail Banking. Allerdings wären gerade mit einer Interoperabilitätsverpflichtung aus Sicht der Branchenunternehmen auch große Risiken verbunden. Bei den hier in Rede stehenden Märkten würden Innovationen in allen wesentlichen Fragen verhindert. „Ohne Innovationen verbleibe wahrscheinlich nur die Facebook-Gruppe im Markt, neben der nur wenige andere weiter existieren könnten. Außerdem entstünde eine massive administrative und technologische Belastung“.

Ein international agierender Befragter betont, grundsätzlich gebe es mehrere Wege, über die Interoperabilität erreicht werden könne. Standardisierung sei nur einer davon. Das eigene Unternehmen biete vielfältige Interoperabilitätslösungen an. Das geschehe derart, dass die Innovationstätigkeit nicht darunter leide. Zu den angebotenen Lösungen gehöre auch eine Plattform auf Basis bekannter Standards, die Dritten erlaube, nicht nur mit dem eigenen Unternehmen, sondern auch mit bestimmten Dritten zu kommunizieren. Interoperabilität sei aber auch über proprietäre APIs, über die andere sich anbinden könnten (z. B. auch über Dienstleister), möglich.

Viele führende Unternehmen der Branche betonen, Interoperabilitätsvorhaben auf freiwilliger Basis unterstützen zu wollen, sofern die **Qualität und die Sicherheit der Produkte** gefördert würden. Einige betonen, durch die Beteiligung an der **Entwicklung des MLS-Standards** geschehe dies bereits. Auch für Interoperabilität gelte das Sprichwort “the perfect (interoperability) is the enemy of the good (user experience)”.

Generell lägen Hindernisse bereits auf **politischer Ebene**, nämlich in der Frage, ob große Anbieter sich beteiligen würden. Ohnehin würde die Implementierung eines interoperablen Standards nicht notwendigerweise in einem interoperablen System münden.

b) Herausforderungen und Risiken

Ein Befragter beschreibt ausführlich, Interoperabilität sei eine Herausforderung. Sie sei eigentlich unerschwinglich und könne nur in einem Standardisierungsprozess münden. Es sei aber der Wettbewerb, der Verbesserungen beim Datenschutz und Datensicherheit für die Verbraucher hervorbringe, nicht Standardisierung. Innovationsanreize blieben aus, wenn es einen Standard gebe, der auch ein festgelegtes Niveau für Datenschutz- und -sicherheit hervorbringe, das nicht weiter verbessert werde.

Ein umfassender Standard für alle Marktteilnehmer könne der **technischen Komplexität** und Dynamik des Marktes nicht gerecht werden. Da sich die verschiedenen Protokolle und Datenformate stark unterscheiden, dürfte es sehr schwierig und aufwendig werden, eine Standardisierung von Protokollen und Datenformaten zu erzwingen.

Große und kleine Marktakteure führen an, gerade **kleinere Marktteilnehmer** würden in einem solchen Prozess benachteiligt. Wenn die eigenen Angebote und Funktionen entsprechend den Vorgaben angepasst werden müssten, binde dies die Entwicklerressourcen über längere Zeit, was kleinere Unternehmen nicht verkraften könnten. Sie würden so im Wettbewerb zurückgeworfen.

Ein anderer Dienst weist darauf hin, dass es durch kleinere Inkompatibilitäten zu Fragmentierungen kommen könne, wie es z. B. bei XMPP der Fall sei. Einige Video-Dienste argumentieren ähnlich und verdeutlichen Probleme der Standardisierung anhand des WebRTC-Standards: Viele bestehende Messenger-/Video-Dienste wären mit dem WebRTC 1.0 Standard nicht kompatibel. Verschiedene Protokolle für „Signaling“ machten Interoperabilität kompliziert, auch wenn der WebRTC Standard benutzt werde. Selbst wenn alle Plattformen einen Standard für Video usw. wie WebRTC verwenden würden, gäbe es immer noch Unterschiede in der Netzwerkschicht und der „Signalisierung“ je nach Netzwerkinfrastruktur. Wenn jeder Dienst zur Interoperabilität gezwungen werde, müssten alle ihr eigenes sicheres Netzwerk verlassen. Dies wiederum würde Innovationen innerhalb der Sicherheitsentwicklung beeinträchtigen.

c) Umsetzung

Einzelne Befragte problematisieren ausführlich eine mögliche Umsetzung eines Standardisierungsvorhabens. Sofern Behörden Anforderungen an die Branche in Sachen Interoperabilität stellen wollten, müsste die Ansprüche, die Auswahl und die Definition der gewünschten interoperablen Funktionen auf einem **hohen technischen Niveau** spezifiziert werden. Entscheidend sei, was als Maßstab in einem sich schnell entwickelnden Umfeld angesehen werde. Vereinheitlichungen sowie fehlerhafte Anpassungen oder nicht marktgerechte Anpassungen könnten bei Fehlentscheidungen die Folge sein.

Außerdem komme es darauf an, wer die Festlegungen mache. Es müsse dann die **Branche** sein, die sowohl die Ziele identifiziert als auch die globalen Standards erarbeitet und immer wieder

weiterentwickelt, um die Anforderungen zu erfüllen. Nur so könne verhindert werden, dass veraltete Technologien festgeschrieben würden.

Bei jeglichen Bemühungen um Interoperabilität müssten die **Anforderungen der Datenschutzgesetze und die Datensicherheit** im Blick behalten werden. Derzeit sei der MLS-Standard in Entwicklung. Eine Interoperabilitätsverpflichtung dürfe der Verabschiedung nicht zuvorkommen. Dies gehe dann auf Kosten der Datensicherheit in Form einer fortschrittlichen Ende-zu-Ende-Verschlüsselung.

Schließlich sollte Interoperabilität nur auf Basis **globaler technischer Standards** umgesetzt werden. In einer globalen Welt dürften Interoperabilitätsanforderungen nicht auf Basis nationaler oder regionaler Standards formuliert werden. Für die Branche wäre es sehr aufwendig, weltweit unterschiedliche Anforderungen erfüllen und verschiedene Zusammenstellungen interoperabler Funktionen anbieten zu müssen. Ab einem gewissen Punkt sei dies nicht mehr haltbar. Globale technische Standards ließen globale Märkte entstehen. Wenn nationale oder regional zuständige Behörden Interoperabilitätsverpflichtungen erließen, entstünden kleinere Märkte innerhalb des weltweiten Aktionsraums. Entsprechend mehr müsse programmiert werden. Je länger die Programmcodes würden, desto mehr Fehler könnten sich einschleichen. Dies führe zu höheren Kosten und Zeitaufwand für Ausbesserungen.

d) Eignung von Marktteilnehmern, Institutionen und Behörden, zu einem Standardisierungsprozess beizutragen

Das Bundeskartellamt hat die Messenger- und Video-Dienste befragt, wen sie für geeignet halten, zu einem Standardisierungsprozess beizutragen. Die Antwort war jeweils zu begründen.

Für eine Umsetzung über Standardisierung bezeichnet gut 60 Prozent der Befragten die **IETF (Internet Engineering Task Force)** als am geeignetsten. In einer globalen Welt würden sich lokale Alleingänge nicht durchsetzen. Diese Meinung ist in allen Gruppen präsent, wird also sowohl von Open Source-Lösungen, freien Clients als auch führenden Anbietern vertreten. Nach Meinung der Befragten verfügt die IETF vor allem über die notwendige Erfahrung für diese Aufgabe. Die IETF habe bereits zahlreiche interoperable Standards, insb. auch die Protokollstandardisierung, für das Internet entwickelt und deren Durchsetzung gefördert. Als Beispiel werden XMPP, TLS¹³³, SIP¹³⁴ und WebRTC genannt. Die IETF verfüge auch über die

¹³³ Transport Layer Security, auch bekannt unter der Vorgängerbezeichnung Secure Sockets Layer, ist ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet, vgl. https://de.wikipedia.org/wiki/Transport_Layer_Security, Stand: 9. September 2021.

¹³⁴ Das Session Initiation Protocol (SIP) ist ein Netzprotokoll zum Aufbau, zur Steuerung und zum Abbau einer Kommunikationssitzung zwischen zwei und mehr Teilnehmern, siehe https://de.wikipedia.org/wiki/Session_Initiation_Protocol, Stand: 9. September 2021.

notwendige Unabhängigkeit. Es handele sich um eine unabhängige Task Force, die auf ein übergeordnetes Ziel hinarbeite und nicht vordergründig nationale Interessen bewerte. Ein Befragter stimmt grundsätzlich zu, merkt aber an, ihr Erfolg gründe sich bisher vorwiegend auf Bereiche wie „Infrastruktur/Transport/Access Layer“ mit standardisierten Leistungen und weniger auf Anwendungsfälle bei den hoch differenzierten Bereich „Service Layer“.

Etwas mehr als 25 Prozent der Messenger- und Video-Dienste sind der Auffassung, dass auch die **EU-Kommission** an einem Standardisierungsprozess beteiligt sein sollte. Ein führender Messenger-Dienst führt aus, die Europäische Kommission sei unter Art. 61 Abs. 2c EKEK verantwortlich für die Feststellung, ob die durchgehende Konnektivität zwischen Endnutzern bedroht ist. Konkret ist BEREC (Body of European Regulators for Electronic Communications) nach Art. 61 Abs. 2c EKEK“ zuständig, die Europäische Kommission zu informieren, ob durchgehende Konnektivität zwischen Endnutzern bedroht ist. Einige national und europaweit ausgerichtete Anbieter fordern eine europäische Kraft im Standardisierungsprozess. Nur europaweite Lösungen wären sinnvoll und die EU-Kommission könne entsprechenden Druck ausüben. Ein Adressat betont, auch andere öffentliche Institutionen könnten am technischen Standardisierungsprozess teilhaben, wobei der größte Teil des technischen Inputs von der Industrie kommen und die technische Diskussion vor allem zwischen den Marktteilnehmern stattfinden müsse. Einige wenige Messenger- und Videodienste erwähnen **nationale Behörden**, die die lokale Marktkenntnis innehaben und nationale Marktteilnehmer aufrufen können, sich an der Diskussion zu beteiligen.

Auf die Marktteilnehmer - also die **Branche** - als notwendige Teilnehmer am Standardisierungsprozess verweisen deutlich mehr Befragte, was letztendlich dem etablierten Verfahren entspricht. Die Branche sollte eine Arbeitsgruppe gründen - so ein bekannter Open Source-Anbieter - da es der Industrie überlassen werden sollte, einen Standard zu entwickeln. Die Marktteilnehmer wären diejenigen, die die Technologien entwickelten und einsetzten. Sie würden die Herausforderungen kennen und den Standard am Ende implementieren. Sie müssten allerdings mit einheitlicher Stimme sprechen und deutlich machen, was Sinn macht und was nicht. Der Wunsch nach Beteiligung der Marktteilnehmer spiegelt die Vielfalt der Branche wider. Die Marktteilnehmer sollten sicherstellen, dass alle Regionen sowie große und kleine Branchenbeteiligte vertreten wären. Ein Adressat betont, die Verhandlungen müssten allen Marktteilnehmern offenstehen.

Des Weiteren werden u.a. die XSF (XMPP Standards Foundation), welche die Protokollerweiterungen für XMPP begleitet und das W3C (World Wide Web Consortium), welches den WebRTC Standard entwickelt hat, genannt.

Anhang: Einbezogene Dienste und Glossar

Einbezogene Dienste

Adobe Connect / connect@reflect	All-in-One	BigBlueButton
Blabber.im	Conferencing & Collaboration (Telekom)	Conversations
Delta Chat	Dino	Discord
Element	Facebook Messenger	Fastviewer
Franz	Gajim	Ginlo
Google Meet	GoToMeeting	GoToWebinar
iMessage/FaceTime	Jabber	Jitsi Meet
Line	Loopup	Monal
Nextcloud Talk	Profanity	Quicksy
Rocket.Chat	Skype	Slack
Snapchat	Swyx	Microsoft Teams
TeamViewer	Threema	Tixeo
Trillian	Univado	Viber
Webex	WeChat	WhatsApp
Yaxim	Zoom	

Glossar

ACCC (Australian Competition and Consumer Commission): Australische Wettbewerbs- und Verbraucherschutzbehörde.

AES (Advanced Encryption Standard): Symmetrisches Verschlüsselungsverfahren, das im Jahr 2000 vom National Institute of Standards and Technology (NIST) standardisiert wurde und heutzutage eines der am meisten verwendeten symmetrischen Verfahren darstellt.

API (Application Programming Interface): Programmierschnittstelle; Programmteil, der von einem Softwaresystem anderen Programmen zur Anbindung an das System zur Verfügung gestellt wird.

App (von engl. Application): Anwendungssoftware (d.h. ein ausführbares Programm), welche eine nützliche Funktion erfüllt, aber i. d. R. nicht relevant für das Funktionieren eines Systems an sich ist.

Asymmetrisches Verfahren (Public-Key-Verfahren): Kryptographisches Verfahren, bei dem jeder Teilnehmer ein Schlüsselpaar erzeugt, das aus einem privaten Schlüssel, der zum Entschlüsseln oder Signieren von Daten verwendet wird, und einem öffentlichen Schlüssel, mit dem verschlüsselt oder Signaturen überprüft werden können, besteht. Der private Schlüssel muss geheim gehalten werden und es muss praktisch unmöglich sein, ihn aus dem öffentlichen Schlüssel zu berechnen.

Augmented Reality (erweiterte Realität, AR): Zusammenspiel von digitalem und analogem Leben über die Kamera des Smartphones oder über eine Brille, wobei diese den Nutzer nicht komplett von seiner normalen Umgebung abschottet wie eine VR -Brille. Ihm werden vielmehr in die Brille zusätzliche Informationen über sein Umfeld eingeblendet.

Authentizität: Eines der vier Sicherheitsziele der Kryptographie, welches besagt, dass der Urheber von Daten oder der Absender einer Nachricht eindeutig identifizierbar und seine Urheberschaft nachprüfbar sein sollen.

Backward Secrecy, Future Secrecy (Post-Compromise Security, „Selbstheilung“): Eigenschaft eines kryptographischen Protokolls, welches garantiert, dass verschlüsselte Nachrichten geheim bleiben, auch nachdem in der Vergangenheit ein Schlüssel kompromittiert wurde.

BEREC (Body of European Regulators for Electronic Communications): BEREC soll eine stärkere Koordinierung der jeweiligen nationalen Regulierungspraxis durch eine möglichst einheitliche Anwendung des europäischen Rechtsrahmens für elektronische Kommunikationsnetze und -dienste bewirken, um so die Weiterentwicklung des Binnenmarkts für diesen Bereich zu fördern.

BfDi (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit): Unabhängige eigenständige oberste Bundesbehörde für den Datenschutz und die Informationsfreiheit.

BNetzA (Bundesnetzagentur): Obere deutsche Bundesbehörde und Regulierungsbehörde mit der zentralen Aufgabe, den Wettbewerb in den Energie-, Telekommunikations-, Post- und

Eisenbahnmärkten zu fördern und die Leistungsfähigkeit der Infrastrukturen in diesen Bereichen sicherzustellen.

BSI (Bundesamt für Sicherheit in der Informationstechnik): Cyber-Sicherheitsbehörde des Bundes und als deutsche Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat zuständig für die Informationssicherheit bei Staat, Wirtschaft und Gesellschaft.

Client: Programm oder Anwendung, welche(s) auf dem Endgerät eines Netzwerks ausgeführt wird und mit einem Server (Zentralrechner) kommuniziert.

CMA (Competition and Markets Authority): Britische Wettbewerbs- und Marktaufsichtsbehörde.

Datenportabilität: Die Übertragbarkeit von personenbezogenen Daten.

Datenverarbeitung: Eine Vielzahl unterschiedlicher mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgänge im Zusammenhang mit personenbezogenen Daten (nach Art. 4 Abs. 2 DSGVO). Hier verwendet als Oberbegriff für Datenerfassung, Datennutzung, Datenweitergabe, Datenspeicherung, und Datenlöschung.

Deniable encryption: Verschlüsselungstechnik, bei der das Vorhandensein einer verschlüsselten Datei oder Nachricht in dem Sinne geleugnet werden kann, dass ein Gegenüber nicht beweisen kann, dass der Klartext existiert.

(Plausible) **Deniability** (Glaubhafte Abstreitbarkeit): Eigenschaft eines kryptographischen Protokolls, welche es ermöglicht, das Versenden einer Nachricht im Nachhinein glaubhaft abstreiten zu können.

DMA (Digital Markets Act, Verordnung über digitale Märkte): Teil des Verordnungsentwurfs der Europäischen Kommission zur Reform der Digital- und Wettbewerbsregeln.

Double Ratchet Protokoll: Kryptographisches Protokoll für einen asynchronen (d.h. die Kommunikationspartner müssen nicht gleichzeitig online sein) Ende-zu-Ende-verschlüsselten Nachrichtenaustausch.

DSA (Digital Services Act, Verordnung über digitale Dienste): Teil des Verordnungsentwurfs der Europäischen Kommission zur Reform der Digital- und Wettbewerbsregeln.

DSGVO (Datenschutzgrundverordnung): EU-Verordnung, die die Verarbeitung von personenbezogenen Daten natürlicher Personen durch natürliche Personen, Unternehmen oder Organisationen in der EU regelt.

DTLS (Datagram Transport Layer Security): Sicherheitsprotokoll, das auf der Funktionsweise von TLS (Transport Layer Security) basiert. Im Gegensatz zu TLS nutzt DTLS nicht das gesicherte, verbindungsorientierte Transportprotokoll TCP, sondern das ungesicherte UDP (User Datagram Protocol) zur verschlüsselten und geschützten Übertragung von Daten.

EKEK (Europäischer Kodex für elektronische Kommunikation): EU-Richtlinie, die elektronische Kommunikationsnetze und -dienste regelt.

Encryption at Rest: Ablageverschlüsselung; Verschlüsselung von Daten (sog. Data at Rest, im Gegensatz zu Data in Transit und Data in Use), die in irgendeiner Form im Speicher eines Computers/Endgeräts gespeichert sind.

Ende-zu-Ende-Verschlüsselung (End-to-End-Encryption): Die Verschlüsselung übertragener Daten über alle Übertragungsstationen hinweg. Nur die Kommunikationspartner als Endpunkte der Kommunikation können die Daten entschlüsseln.

(Perfect) **Forward Secrecy** (Folgenlosigkeit): Eigenschaft eines kryptographischen Protokolls, die es unmöglich macht, durch die Kenntnis eines geheimen Haupt- oder Langzeitschlüssels einen Sitzungsschlüssel zu rekonstruieren. Eine aufgezeichnete verschlüsselte Kommunikation ist damit selbst bei der Kenntnis des Langzeitschlüssels nicht nachträglich zu entschlüsseln.

GEREK (Gremium der europäischen Regulierungsbehörden): Siehe BEREK.

GSM (Global System for Mobile Communications): Mobilfunkstandard für volldigitale Mobilfunknetze, der hauptsächlich für Telefonie, aber auch für leitungsvermittelte und paketvermittelte Datenübertragung sowie Kurzmitteilungen (Short Messages) genutzt wird. Erster Standard der sogenannten zweiten Generation („2G“) als Nachfolger der analogen Systeme der ersten Generation (in Deutschland: A-Netz, B-Netz und C-Netz).

GWB (Gesetz gegen Wettbewerbsbeschränkungen): Grundgesetz der Marktwirtschaft und die zentrale gesetzliche Grundlage für die Arbeit des Bundeskartellamts. Schutzobjekt des GWB ist der Wettbewerb in der Bundesrepublik Deutschland, der vor jeder Beschränkung zu schützen ist, unabhängig davon, ob diese im Inland oder im Ausland verursacht wurde.

Identifizier (Client-) ID: Bezeichnet das Merkmal eines Messenger-Dienst-Nutzers, welches dessen eindeutige Identifizierung erlaubt.

IEEE (Institute of Electrical and Electronic Engineers): Weltweiter Berufsverband von Ingenieuren hauptsächlich aus den Bereichen Elektrotechnik und Informationstechnik, der u.a. Gremien für die Standardisierung von Techniken, Hardware und Software bildet.

IETF (Internet Engineering Task Force): Offene, internationale Freiwilligenvereinigung von Netzwerktechnikern, Herstellern, Netzbetreibern, Forschern und Anwendern, die sich mit der technischen Weiterentwicklung des Internets – insb. Standardisierung der im Internet eingesetzten Kommunikationsprotokolle – befasst, um dessen Funktionsweise zu verbessern.

IMAP (Internet Message Access Protocol): Netzwerkprotokoll, das ein Netzwerkdateisystem für E-Mails bereitstellt. Mit IMAP bleiben E-Mails am Server gespeichert und können somit von mehreren Geräten abgerufen werden.

Inhalte: Texte, Sprache, Video, Fotos, gespeicherte oder versendete Dateien.

Interoperabilität: Bezeichnet die Fähigkeit unabhängiger, heterogener Messaging-Systeme oder Messenger-Clients, in verschieden hohem Maße zusammenarbeiten zu können.

ISO (International Organization for Standardization): Die Internationale Organisation für Normung ist die internationale Vereinigung von Normungsorganisationen. Sie erarbeitet internationale Normen in allen Bereichen mit Ausnahme der Elektrik, Elektronik sowie der Telekommunikation. Sie ist Teil der WSC (World Standards Cooperation).

Messenger-Dienst: 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.

MLS (Messaging Layer Security): Messagingprotokoll, welches auf dem Double Ratchet Protokoll basiert und derzeit im Rahmen einer IETF-Arbeitsgruppe standardisiert wird. Der Standard strebt ein verbessertes Gruppenmanagement sowie die Interoperabilität verschiedener Messenger an.

Messaging-System: Sammelbegriff für das gesamte System, das zum Messaging benötigt wird, bestehend aus Kommunikationsprotokoll, Anwendersoftware (App, Client), Serversoftware und Hardware.

Multiprotocol Clients / Multi (Protokoll-)Messenger: Software, die eine Vielzahl von Kommunikationsprotokollen beherrscht und den Gebrauch verschiedener Kommunikationsdienste über eine Oberfläche ermöglicht.

Nutzer: Sammelbegriff für Organisatoren und Teilnehmer, die einen Messenger- oder Video-Dienst verwenden.

Open Source: Software, deren Quelltext öffentlich und von Dritten eingesehen, geändert und genutzt werden kann.

Organisator (Ersteller, Administrator, Host): Sammelbegriff für eine Person oder Institution, die aktiv einen Austausch über Textnachrichten, Telefonie oder Videotelefonie starten und andere Teilnehmer dazu einladen kann sowie ggfs. weitere Berechtigungen inne hat (z. B. Stummschalten von Teilnehmern, Löschen von Gruppen, Entfernen von Teilnehmern etc.).

OTR Protokoll (Off-the-Record Protokoll): Protokoll zur Nachrichtenverschlüsselung beim Instant Messaging (d.h. die Kommunikationspartner müssen gleichzeitig online sein), welches als Vorgänger des Double Ratchet Protokolls gilt.

OTT (Over the Top): Inhalte, die mittels einer Internetverbindung angeboten werden, ohne dass die Internetanbieter selbst Einfluss oder Kontrolle über den Inhalt hätten, so dass OTT-Dienste entkoppelt von den Infrastrukturanbietern sind.

Peer-to-Peer: Kommunikation unter Gleichen (bezogen auf ein Rechnernetz). Wird hier verwendet für die direkte Kommunikation zwischen zwei Nutzern.

Personenbezogene Daten: Nach Art. 4 Nr. 1 DSGVO sind dies alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

POP (Post Office Protocol): Übertragungsprotokoll, über das ein Client E-Mails von einem E-Mail-Server abholen kann. Mit POP3 werden die E-Mails vom Server abgeholt und sind dann nurmehr

lokal im E-Mail-Programm des Nutzers gespeichert. POP3 kann daher mit nur einem Gerät verwendet werden.

Proprietät: Soft- und Hardware, die auf herstellerspezifischen Standards basiert, sich von freier (Open Source) Soft- und Hardware abgrenzt und auch keinen äußeren, öffentlichen Eingriff zulässt.

(Kommunikations-) **Protokoll:** Regelsatz, nach der die Datenübertragung zwischen zwei oder mehreren Endpunkten abläuft.

RFC (Request for Comments): Sammlung durchnummerierter Dokumente, die von der IETF herausgegeben werden. RFCs behandeln Protokolle, Methoden, Programme und Konzepte, die für die Zusammenarbeit unterschiedlicher Systeme im Internet unentbehrlich sind.

RSA (Rivest–Shamir–Adleman): Asymmetrisches kryptographisches Verfahren, das sowohl zum Verschlüsseln als auch zum digitalen Signieren verwendet werden kann.

SEP (Standardessentielle Patente): Patente für Erfindungen, die essentieller Teil eines Standards sind.

SIP, Session Initiation Protocol (SIP): Netzprotokoll zum Aufbau, zur Steuerung und zum Abbau einer Kommunikationssitzung zwischen zwei und mehr Teilnehmern.

S/Mime (Secure/Multipurpose Internet Mail Extensions): Standard für die Verschlüsselung und das Signieren von MIME-Objekten durch ein hybrides Kryptosystem. S/MIME wird in sehr vielen Protokollen zur Absicherung in der Anwendungsschicht (Application Layer) eingesetzt, typischerweise bei E-Mail.

SMS (Short Message Service): Telekommunikationsdienst zur Übertragung von Textnachrichten, die meist Kurzmitteilungen oder ebenfalls SMS genannt werden.

SMTP (Simple Mail Transfer Protocol): Protokoll der Internetprotokollfamilie, das zum Austausch von E-Mails in Computernetzen dient. Es wird dabei vorrangig zum Einspeisen und zum Weiterleiten von E-Mails verwendet.

SSL (Secure Sockets Layer): Vorgängerbezeichnung von Transport Layer Security (TLS); Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.

Symmetrisches Verfahren (Kryptographie): Kryptographisches Verfahren, bei dem der Schlüssel zum Ver- und Entschlüsseln identisch ist und vorher zwischen den Kommunikationspartnern ausgetauscht werden muss.

Teilnehmer: Sammelbegriff für eine Person oder Institution, die lediglich auf „Einladung“ eines Organisators an einem Austausch über Textnachrichten, Telefonie oder Videotelefonie (einzeln oder in Gruppen) teilnehmen kann.

TLS (Transport Layer Security): Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet, Weiterentwicklung von Secure Sockets Layer (SSL).

Transportverschlüsselung (Punkt-zu-Punkt-Verschlüsselung): Bezeichnung für das Senden von unverschlüsselten Daten über einen verschlüsselten Kanal. Außerhalb des Übertragungsweges und an den Endpunkten liegen die Daten unverschlüsselt vor.

Video-Dienst: Sammelbegriff für 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).

Virtual Reality (virtuelle Realität, VR): Digitales, am Computer geschaffenes Abbild der Realität.

VZ NRW (Verbraucherzentrale NRW): Auf Landesebene organisierter Verein, der sich aufgrund eines staatlichen Auftrags dem Verbraucherschutz widmet und Beratungsleistungen erbringt.

WebRTC (Web Real-Time Communication): Offener Standard, der eine Sammlung von Kommunikationsprotokollen und Programmierschnittstellen (API) definiert, die Echtzeitkommunikation über Rechner-Rechner-Verbindungen ermöglichen.

W3C (World Wide Web Consortium): Gremium (Mitgliedsorganisation) zur Standardisierung der Techniken im World Wide Web.

XSF (XMPP Standards Foundation): Gemeinnützige Stiftung, die das XMPP-Protokoll spezifiziert und weiterentwickelt.

Zwei-Faktor-Authentisierung: Identitätsnachweis eines Nutzers mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren), wie z.B. Passwort und Fingerabdruck.