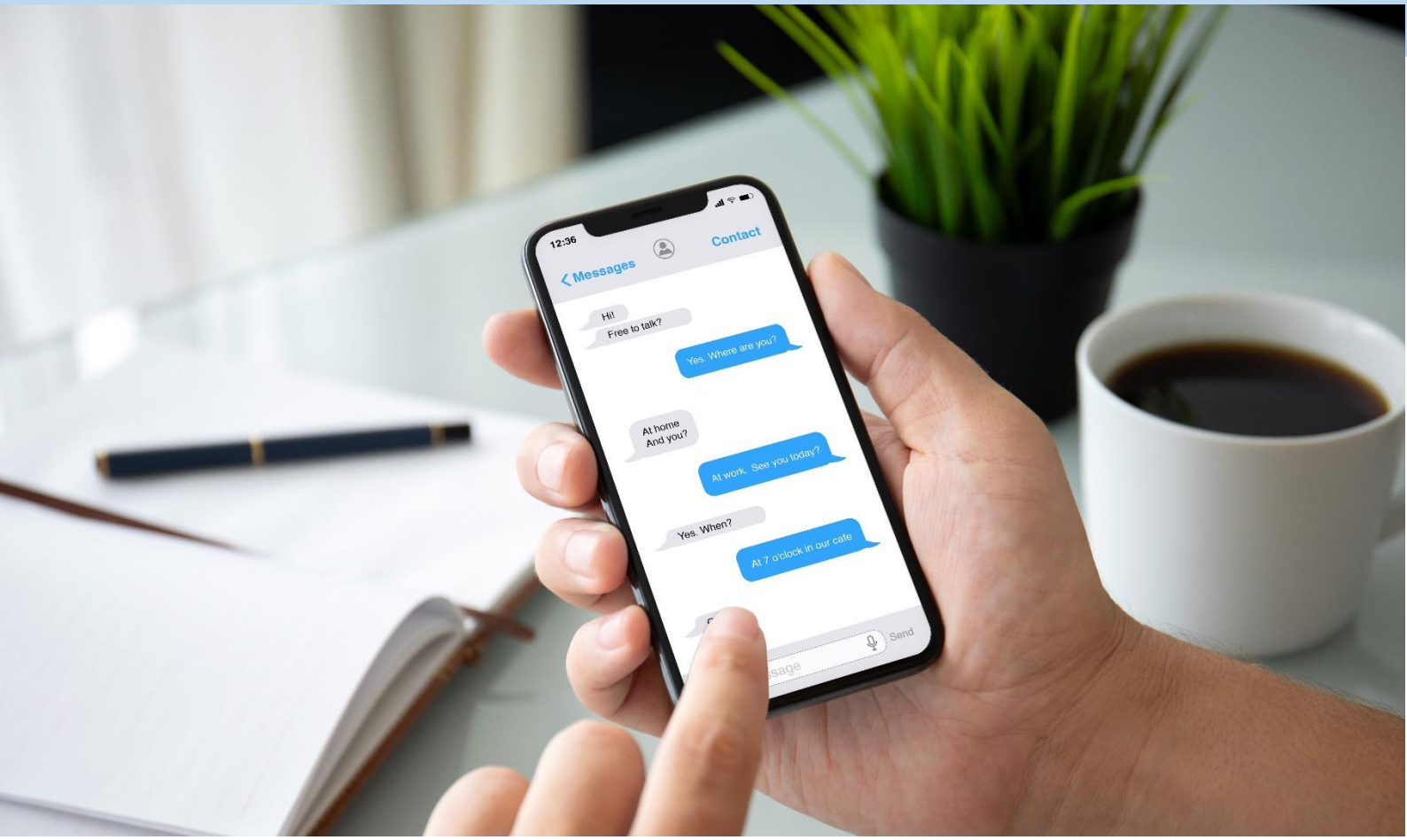
Bundeskartellamt

Offene Märkte | Fairer Wettbewerb

Sektoruntersuchung

Messenger- und Video-Dienste

Abschlussbericht



Sektoruntersuchung Messenger- und Video-Dienste
Bericht gemäß § 32e GWB
Az. V-28/20
Mai 2023

Kontakt
Bundeskartellamt
Beschlussabteilung Wettbewerbs- und Verbraucherschutz
Kaiser-Friedrich-Straße 16
53113 Bonn
www.bundeskartellamt.de

Bildnachweis:
AdobeStock/DenPhoto

Vorbemerkung

Die Beschlussabteilung Wettbewerbs- und Verbraucherschutz des Bundeskartellamts hat im November 2020 eine verbraucherrechtliche Sektoruntersuchung nach § 32e Abs. 5 des Gesetzes gegen Wettbewerbsbeschränkungen[1] im Wirtschaftszweig Messenger- und Video-Dienste eingeleitet.[2] Im November 2021 wurde hierzu der Zwischenbericht „Branchenüberblick und Stimmungsbild Interoperabilität“ veröffentlicht, dessen Ergebnisse auch Teil des vorliegenden Abschlussberichts sind.[3] 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).[4]
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 Wettbewerb[5] (UWG) wird hingewiesen.

---

1 Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bek. vom 26.06.2013 (BGBl. I S. 1750, 3245), zuletzt geändert durch Art. 2 Gesetz vom 19.07.2022 (BGBl. I S. 1214) - GWB.

2 Siehe *Bundeskartellamt*, 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.

3 Siehe *Bundeskartellamt*, Pressemitteilung vom 04.11.2021, abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Pressemitteilungen/2021/04_11_2021_SU_Messenger-Dienste_Zwischenbericht.pdf?__blob=publicationFile&v=2.

4 Siehe *Bundeskartellamt*, 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 .

5 Gesetz gegen den unlauteren Wettbewerb in der Fassung der Bek. vom 03.03.2010 (BGBl. I S. 254), zuletzt geändert durch Art. 20 Gesetz vom 24.06.2022 (BGBl. I S. 959) – UWG.

Inhaltsverzeichnis

Abbildungsverzeichnis

Zusammenfassung

Leitfrage der Untersuchung

Messenger- und Video-Dienste sind für viele Menschen inzwischen ein unverzichtbarer Teil der alltäglichen Kommunikation geworden. Die Verbraucherinnen und Verbraucher können auf verschiedenen Endgeräten Text- und Sprachnachrichten sowie Dateien austauschen und (per Video) telefonieren und alle diese Funktionen individuell einsetzen und kombinieren. Lange bewährte Kommunikationsarten erscheinen somit in einem modernen Gewand. Der **Wunsch nach Individualität oder einer maßgeschneiderten Lösung** für die eigenen Bedürfnisse schlägt sich bei Messenger- und Video-Diensten in einer großen **Vielfalt an Geschäftsmodellen und Anwendungen** nieder. Wie das Bundeskartellamt im Zwischenbericht zu dieser Sektoruntersuchung bereits ausgeführt hat, sind die Funktionen, die Angebote und die wirtschaftliche Bedeutung der Messenger- und Video-Dienste sehr verschieden. Neben den in der Öffentlichkeit besonders bekannten Diensten besteht eine große Bandbreite an Branchenteilnehmenden, welche von internationalen, konzernbetriebenen Diensten mit vielen Millionen Nutzerinnen und Nutzern, hohen Umsätzen und eigenen digitalen Ökosystemen[6] mit starken Positionen auf benachbarten Märkten über nationale oder auf deutschsprachige Regionen konzentrierte Dienste oder Dienste mit besonderen Geschäftsschwerpunkten bis hin zu Open Source-Diensten und freien Anwendungen ohne Gewinnerzielungsabsicht reicht. Es handelt sich um eine weltweit agierende Branche, die nicht nur auf Seiten der größeren Teilnehmenden technologische und digitale Entwicklungen und Innovationen hervorbringt. Konkurrierende Dienste zeichnen sich durch

---

6 Mit dem Begriff "digitales Ökosystem" wird ein Bündel einer Vielzahl an Diensten eines Konzerns mit Wechselwirkungen untereinander bezeichnet, vgl. *Bundeskartellamt*, Stellungnahme zur öffentlichen Anhörung des Wirtschaftsausschusses zum Digital Markets Act, 25. April 2022, abrufbar unter: https://www.bundestag.de/resource/blob/891308/f13edcf322cc218da602e6dc4b58391b/ADrs-20-9-59_Stellungnahme-Mundt-data.pdf sowie *Bundeskartellamt*, The Evolving Concept of Market Power in the Digital Economy – Note by Germany, abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/OECD_2022_Competition_Committee_Concept_Market_Power_Digital_Economy.pdf?__blob=publicationFile&v=2. Siehe z. B. auch *Fletcher,* Digital competition policy: Are ecosystems different?, Note for the OECD Hearing on Competition Economics of Digital Ecosystems, abrufbar unter: https://one.oecd.org/document/DAF/COMP/WD(2020)96/en/pdf. In der Informationstechnik wird mit dem Begriff Ökosystem eine Soft- und Hardware-Architektur bezeichnet, welche auf jeweils ganz eigenen Geräten, Systemen und Zugangsvoraussetzungen beruht und damit entsprechendes Zubehör voraussetzt und hervorbringt, vgl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/%C3%96kosystem.

innovative Geschäftsmodelle und Spezialisierungen auf Basis besonderer Services und Funktionen aus. Nicht nur auf Seiten der freien Systeme und Anwendungen gibt es viel Expertise und Engagement in Sachen Unabhängigkeit und Schutz der persönlichen Daten der Nutzerinnen und Nutzer. Allerdings legt die Marktverfassung den Schluss nahe, dass dieses Potential bisher nicht ausgeschöpft, nicht flächendeckend verteilt und nicht so zugunsten eines hohen Datenschutzniveaus eingesetzt wird, wie es möglich wäre. Damit sind neue **verbraucherrechtliche Fragestellungen** aufgekommen. Die Verbraucherinnen und Verbraucher selbst scheinen diese verbraucherrechtlichen Aspekte gegenüber anderen Kriterien bei der Auswahl ihres Messenger- und Video-Dienstes jedoch bisher hintenanzustellen. Daher steht im Zentrum dieses Abschlussberichts zur Sektoruntersuchung Messenger- und Video-Dienste die Leitfrage, wie **Datenschutz als Wettbewerbsparameter** vorangebracht werden kann, um marktweit bei Messenger- und Video-Diensten ein höheres Datenschutzniveau zu erreichen. Welche Anreize und Maßnahmen sind notwendig, damit die Verbraucherinnen und Verbraucher ihren Messenger- und Video-Dienst auch nach der Datenschutzfreundlichkeit auswählen? Und wie können die anbietenden Messenger- und Video-Dienste bewegt werden, Datenschutzfreundlichkeit vermehrt als Differenzierungsmerkmal einzusetzen und die Verbraucherinnen und Verbraucher besser darüber zu informieren?

Das Bundeskartellamt hat zunächst die Ausgangssituation bei Datensicherheit und Datenschutz und das wettbewerbliche Umfeld der Branche untersucht. Ein Schwerpunkt lag auf den technischen Grundlagen und Methoden des Messaging und des Audio-/Video-Austauschs. Die technischen Gegebenheiten und Praktiken bei den einzelnen Diensten beeinflussen nicht nur die **Datensicherheit und die (rechtskonforme) Umsetzung Datenschutzmaßnahmen**. Die technische Infrastruktur kann sich auch auf Wettbewerbsprozesse auswirken. Sie ist somit auch maßgeblich für das Ziel des Bundeskartellamts, Datenschutz als Wettbewerbsparameter zu fördern.

Von ihr hängt beispielsweise ab, ob und inwieweit der Zugang und der Anschluss an andere Messenger- und Video-Systeme oder die Integration technischer Innovationen in ein System möglich ist. Die Komplexität der technischen Infrastruktur und Verfahren dürften auch die Initiative der Verbraucherinnen und Verbraucher beeinträchtigen. Ihre Bereitschaft, Datenschutz wie oben beschrieben als Auswahlkriterium zu nutzen, setzt zunächst ein grundlegendes Verständnis der anspruchsvollen technischen Zusammenhänge voraus. Die **Perspektive der Verbraucherinnen und Verbraucher** ist entscheidend für jegliche Handlungsempfehlungen. Es sind Rahmenbedingungen zu schaffen und Anreize zu setzen, um sie und die anbietenden Dienste zu motivieren, dem Datenschutz im Wettbewerb eine höhere Priorität einzuräumen.

Das Bundeskartellamt hat über 40 verschiedene Dienste zu diesen Themen befragt und eine Reihe von Expertengesprächen geführt. Darüber hinaus wurde eine Vielzahl von Studien und Fachartikeln ausgewertet.

Verlauf und weitere Themen

Im **Zwischenbericht,** der im November 2021 veröffentlicht wurde, hat das Bundeskartellamt die Ermittlungsergebnisse aus zwei untersuchten Themenbereichen dargelegt: Zum einen wurde ein Überblick über die Rahmenbedingungen der **Branche** sowie die verschiedenen Anbietergruppen, Funktionalitäten und Geschäftsmodelle gegeben. Zum anderen wurden die ersten Ergebnisse der Unternehmensbefragung zur **Interoperabilität** dargestellt. Es wurde hinterfragt, 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.
In diesem **Abschlussbericht** hat das Bundeskartellamt die vorgenannten Ausführungen um die Erkenntnisse zum Thema Datenschutz bei Messenger- und Video-Diensten, insb. um **Kriterien der Datensicherheit und der Datenverarbeitung** erweitert. Die Ermittlungsergebnisse werden dargelegt, eingeordnet und rechtlich überprüft. Des Weiteren werden die bis hierher noch ausstehenden Ermittlungsergebnisse zur **Interoperabilität**, die sich insb. auf die technische Umsetzung und Gestaltung richten, dargestellt und mit den entsprechenden Regelungen des **Digital Markets Act (DMA)**, der zwischenzeitlich am 1. November 2022 in Kraft getreten ist, in Beziehung gesetzt. Vor diesem Hintergrund werden **Ansätze für mehr wettbewerblichen Datenschutz** entwickelt, die sich sowohl auf die Verbraucherinnen und Verbraucher als auch auf die Dienste richten. Darauf aufbauend schließt der Bericht mit **Empfehlungen** zur Verbesserung des Datenschutzniveaus bei Messenger- und Video-Diensten in Deutschland. Hier werden nicht nur die rechtlichen Bedingungen, Ausschreibungs- und Förderungspraktiken und die Situation des öffentlichen Bereichs angesprochen. Es wird angeregt, die **Rahmenbedingungen für wettbewerblichen Datenschutz** zu verbessern und eine transparente Bewertung der Datenschutzqualität einzuführen.

Kriterien der Datensicherheit und Datenverarbeitung bei Messenger- und Video-Diensten

Das Bundeskartellamt hat sich für diese Sektoruntersuchung ausführlich mit den technischen Grundlagen des Messaging und des Audio-/Video-Austauschs beschäftigt. Es hat eine **Checkliste** mit den wesentlichen Kriterien für Datensicherheit und Datenschutz erstellt. Diese umfasst zunächst das **Protokoll** einschließlich der Ende-zu-Ende-Verschlüsselung auf dem Stand der Technik. Das Protokoll kann als Sprache eines Messaging- und Video-Systems verstanden werden, dass die Regeln für den Austausch und den Anschluss an das System umfasst. Die **Ende-zu-Ende-Verschlüsselung** sorgt dafür, dass der Datenaustausch vom Sender bis zum Empfänger von niemand anderem gelesen werden kann als von den Kommunizierenden selbst. Verschlüsselung macht nur Sinn, wenn auch die Identität der Nutzerinnen und Nutzer, die die verschlüsselten Daten austauschen, eindeutig ist. Mit der **Zwei-Faktor-Authentisierung** können die Verbraucherinnen und Verbraucher die eigene Identität gegenüber ihrem

Messenger- und Video-Dienst sowie gegenüber ihren Kommunikationspartnerinnen und -partnern absichern.

Verwenden Dienste generell **internationale technische Standards** geht damit ein gewisses überprüftes Qualitätsniveau einher. Zudem kann Interoperabilität einfacher hergestellt werden, wenn sich die Kommunikation auf identischen technischen Prinzipien gründet. Wenn der **Quellcode eines Messenger- und Video-Dienstes einsehbar** ist, können kompetente Dritte die Datensicherheit des Systems überprüfen. Ist dies nicht der Fall, sollte es die Möglichkeit geben, dass zumindest Sicherheitsaudits durch unabhängige renommierte Prüfinstitutionen durchgeführt und veröffentlicht werden. Sofern die Datenschutzerklärung nicht gelesen wird, kann die Art des Geschäftsmodells ein Indiz dafür sein, ob Daten eine ungewisse Weiterverwendung finden oder nicht. Hier ist auf **Datensparsamkeit** zu achten. Wenn Nutzerinnen und Nutzer **Konten** anlegen müssen, wie es bei Diensten großer Konzerne, die ein digitales Ökosystem betreiben, der Fall ist, werden viele Daten bereits dadurch erfasst.

Messenger- und Video-Dienste sollten die Daten von EU-Bürgerinnen und -Bürgern **im Geltungsbereich der DSGVO speichern** und nicht in andere Jurisdiktionen transferieren, um die Datensicherheit rechtskonform zu bewahren. Dies betrifft insbesondere den Vergleich mit den USA, wo die Geheimdienste auf dort gespeicherte Daten der Verbraucherinnen und Verbraucher zugreifen können.

Verbraucherinnen und Verbraucher können ihre Daten und diejenigen ihrer Kontaktpersonen schützen, wenn sie auf die Synchronisation des **Kontaktverzeichnisses verzichten**, bzw. ihren Dienst dementsprechend auswählen oder anweisen.

Die Ermittlungsergebnisse waren nach mehreren Maßstäben zu bewerten. Zunächst war zu überprüfen, ob die Kriterien der Datensicherheit und des Datenschutzes entsprechend dem **Stand der Technik** umgesetzt werden und zukunftsfähig sind. Diese Frage gewann vor dem Hintergrund einer möglichen Interoperabilität von Messenger- und Video-Diensten und ihrer Auswirkungen auf Datenschutz und Datensicherheit an Bedeutung. Kurz vor Abschluss der Sektoruntersuchung – im November 2022 – ist der DMA mit einem **Interoperabilitätsregime** für Gatekeeper in Kraft getreten, womit sich das rechtliche Umfeld in dieser Frage konkretisiert hat. Schließlich war die **Wahrnehmung der Verbraucherinnen und Verbraucher** einzubeziehen. Verschiedene Verbraucherbefragungen und wissenschaftliche Untersuchungen lassen keine eindeutigen Rückschlüsse zu, inwieweit die Verbrauchenden in der Lage und willens sind, sich komplexe technische Hintergründe zu erarbeiten und in datenschutzfreundliche Auswahlstrategien umzusetzen. Auch ob und inwieweit die **Information und Präsentation datenschutzrelevanter Fakten** durch die Dienste geeignet ist, die Verbrauchenden „einzufangen“, ist fraglich. Zweifel scheinen hier angesichts der gegenwärtigen Marktverfassung und der fortbestehenden starken Position bekannter Dienste angebracht.

Nach dem Ergebnis der Ermittlungen existiert in der Branche der Messenger- und Video-Dienste viel **Innovationskraft und Expertise** in Sachen Unabhängigkeit und Schutz der persönlichen Daten der

Nutzerinnen und Nutzer. Allerdings sind in der Branche gleichzeitig **verschiedene Praktiken zu bemängeln**. Die Ergebnisse der Sektoruntersuchung legen den Schluss nahe, dass verschiedene Dienste Engagement vermissen lassen und die Expertise und Möglichkeiten nicht so umsetzen, wie es aus Sicht der Nutzerinnen und Nutzer wünschenswert und möglich wäre. Dies lässt sich aber nur schwer an einzelnen Gruppen von Diensten festmachen. So schneiden nach den Ermittlungsergebnissen zwar freie Messaging-Systeme und Open Source-Dienste bei einer Vielzahl der Kriterien gut ab. Allerdings ist die Frage, wie Datensicherheit im Detail gestaltet wird, hier letztendlich vom ausgewählten (Server-) Betreiber abhängig. Generell eröffnen sich den Nutzerinnen und Nutzern bei den meisten Diensten **viele Wahlmöglichkeiten**, die teilweise ein gewisses Bewusstsein für sicherheitsrelevantes Handeln erfordern, wie z. B. - wie eben erwähnt - die **Auswahl des Serverbetreibers** oder generell auch die **Aktivierung der Ende-zu-Ende-Verschlüsselung**. Umgekehrt können Verbraucherinnen und Verbraucher, wenn sie bereit sind, sich zu informieren, ein **weites Feld an Möglichkeiten** vorfinden, um ihren Messenger so zu gestalten bzw. den Client zu finden, der ihre Anforderungen am besten erfüllt und aufgrund von Datensparsamkeit und der Verwendung internationaler Standards auch im Hinblick auf Interoperabilität zukunftsfähig ist.

Auch einige Videokonferenzdienste bieten ihren Nutzerinnen und Nutzern viele Optionen. In weiten Teilen ist das der Ausrichtung auf die Wünsche von Geschäftskundinnen und Geschäftskunden geschuldet. Ein hohes Sicherheitsniveau kann umgesetzt werden. Letztendlich liegt sicherheitsbewusstes Handeln aber häufig in der **Verantwortung des jeweiligen Host** oder der Administratorin oder des Administrators, unabhängig davon, ob diese Rolle geschäftlich oder privat ausgeführt wird.

Was die zu bemängelnden Praktiken oder das fehlende Engagement angeht, so betrifft dies zum einen die **Verschlüsselung**. Einzelne bekannte Messenger- und Video-Dienste überraschen damit, dass sie Sicherheit **nicht auf dem Stand der Technik** umsetzen und es zum Beispiel bei einer Transportverschlüsselung belassen oder die Ende-zu-Ende-Verschlüsselung nur bei bestimmten Funktionen einsetzen, was nicht mit technischen Restriktionen begründet werden kann. Ferner wäre es wünschenswert, dass branchenweit weitere Sicherheitsverfahren, wie die Verschlüsselung der Daten auf dem Endgerät, die Ablageverschlüsselung, die Zwei-Faktor-Authentisierung sowie Backups in der Branche einen höheren Verbreitungsgrad hätten. Des Weiteren sei auf die rechtliche Analyse verwiesen. Einige Dienste **speichern Daten europäischer Nutzerinnen und Nutzer außerhalb des Geltungsbereichs der DSGVO**, was rechtlich nicht zulässig ist**,** oder der genaue Speicherort bleibt unklar. Auch die **Synchronisation des Kontaktverzeichnisses** in Folge derer Daten Dritter verarbeitet werden, wird von verschiedenen Diensten betrieben und kann unzulässig sein.

Rechtliche Einordnung

Das Bundeskartellamt hat von den Messenger- und Video-Diensten zunächst sowohl zur Datenspeicherung und zum Datentransfer als auch zur Synchronisation des Kontaktverzeichnisses Auskünfte verlangt und die Ergebnisse einer rechtlichen Analyse unterzogen. Nach den Ermittlungsergebnissen liegen **Verstöße einiger Messenger- und Video-Dienste** gegen die Vorschriften der DSGVO nahe.

Die **Synchronisation des Kontaktverzeichnisses** führt dazu, dass auch die Kontaktdaten von Nicht-Nutzerinnen und Nicht-Nutzern erfasst werden. Nach derzeitiger Auffassung des Bundeskartellamts entspricht diese gängige Praxis vieler bekannter Messenger- und Video-Dienste nicht den Anforderungen von Art. 6 Abs. 1 Unterabs. 1 Buchst. a) DSGVO, sofern sie dauerhaft erfolgt. Der Personenbezug der Daten besteht fort, auch wenn die Telefonnummer durch einen kryptographischen Hashwert ersetzt wird, der mit der Nutzerin oder dem Nutzer verknüpft ist, aus deren Kontaktverzeichnis die Telefonnummer stammt. Aus der Wahrung berechtigter Interessen ergibt sich keine weitere Legitimation des Verantwortlichen, da der Vernetzungsvorteil zu gering erscheint.

Die Ermittlungsergebnisse zum Prozess der Datenverarbeitung legen nahe, dass sich einige Messenger- und Video-Dienste beim **Datentransfer in Drittländer und beim Speichern auf Servern in Drittländern** (Art. 45 DSGVO) nicht rechtskonform verhalten. Dies betrifft vor allem diejenigen Dienste, die Daten deutscher Nutzerinnen und Nutzer in den USA speichern. In Länder außerhalb der EU und des Europäischen Wirtschaftsraums dürfen Daten nur übermittelt werden, wenn ein angemessenes Datenschutzniveau in dem jeweiligen Drittland (Art. 45 DSGVO) sichergestellt ist. Allerdings ist der frühere Datenschutzschild (EU-US Privacy Shield), den die EU mit den USA verhandelt hatte, nach dem „*Schrems II*“ - Urteil des EuGH aus dem Sommer 2020 ungültig.

Neben möglichen Verstößen gegen die DSGVO war ein weiteres rechtliches Untersuchungsfeld eine mögliche Irreführung der Verbraucherinnen und Verbraucher durch **Informationsmängel (**§ 5a Abs. 1 UWG) **bei der Ende-zu-Ende-Verschlüsselung**. Hier dürfte sich nach Auffassung des Bundeskartellamts ein Transparenzverstoß durch Informationsmängel in Bezug auf die Verschlüsselungsart nicht leicht begründen lassen. Für einen möglichen Verstoß gegen das Transparenzgebot des UWG müsste die „geschäftliche Relevanz“ von Sicherheitseigenschaften wie der Ende-zu-Ende-Verschlüsselung begründet werden. Allerdings ist die Marktentwicklung seit der Konzipierung der Sektoruntersuchung vorangeschritten. Die Ende-zu-Ende-Verschlüsselung hat sich als Branchenstandard etabliert, so dass es hinsichtlich dieser Sicherheitseigenschaft keinen Unterschied machen dürfte, wo Nutzerinnen und Nutzer sich registrieren. Vor diesem Hintergrund war überraschend, dass einige wenige bekannte Dienste die Ende-zu-Ende-Verschlüsselung nicht oder nur eingeschränkt umsetzen. Eine bessere Einschätzung der Sichtweise der Verbraucherinnen und Verbraucher hätte weiteren

Ermittlungsaufwand wie etwa eine Verbraucherbefragung erfordert, mit welchem aufgrund der Komplexität der Begrifflichkeiten aber nur ungewisse Aufklärungschancen verbunden gewesen wären. Auch die Einordnung des Verhaltens der Verbrauchenden aus Unternehmenssicht blieb uneindeutig, da es viele kostenfreie Angebote der Messenger- und Video-Dienste gibt. Letztendlich musste eine abschließende Bewertung jeweils der **Klärung im Einzelfall** vorbehalten bleiben.

Interoperabilität

Mit Inkrafttreten des Digital Markets Act im November 2022 hat sich das rechtliche Umfeld der Messenger- und Video-Dienste in Sachen Interoperabilität geklärt. Wegen der anhaltenden rechtspolitischen Diskussion über eine gesetzliche Verpflichtung von Messenger- und Video-Diensten zur Interoperabilität hatte das Bundeskartellamt in seiner Untersuchung den befragten Unternehmen **bereits vor der Einigung im Trilog zum DMA im März 2022** auch zu diesem Themenkomplex Fragen gestellt. Wie im Zwischenbericht bereits ausführlich dargelegt, hatte die Befragung der Unternehmen durch das Bundeskartellamt 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 konnten nach den im Zwischenbericht dargelegten Ermittlungsergebnissen die technischen Erfordernisse, die Ausgestaltung der Datensicherheit, die Wechselwirkungen von Interoperabilität im Hinblick auf Innovationsanreize und die Wettbewerbsintensität sowie das Verbraucherverhalten gesehen werden. Insgesamt hatte die Befragung gezeigt, dass Interoperabilität von den betroffenen Unternehmen nicht rundheraus abgelehnt wird. Vielmehr werden in Teilbereichen Interoperabilität oder zumindest Formen des Austausches in unterschiedlicher technischer Tiefe und Reichweite bereits praktiziert. In Standardisierungsgremien werden technische Grundlagen für Interoperabilität in globalem Kontext erarbeitet. Dies ging allerdings einher mit der klaren Haltung eines Großteils der Branche, dass eine gesetzliche Verpflichtung zur branchenweiten Interoperabilität mehr schaden als nützen 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.
Das Bundeskartellamt hatte herausgestellt, dass die Erkenntnisse aus der Branchenbefragung belegen, wie vielschichtig und komplex die **Analyse der Wirkungszusammenhänge rund um das Thema Interoperabilität** ist. Bei der Umsetzung sollten nicht nur die notwendigen Investitionen in technische

Veränderungen der Dienste oder die Entwicklung technischer Neuerungen berücksichtigt werden. Ebenso einzubeziehen wären mögliche positive oder negative Wohlfahrtseffekte durch veränderte Innovationsanreize und Auswirkungen auf Geschäftsstrategien und Wettbewerbsintensität.
Nach **dem in Art. 7 DMA normierten Konzept einer Interoperabilitätsverpflichtung** sind lediglich designierte Gatekeeper unter den Messenger-Diensten Adressat der Verpflichtung. Des Weiteren lebt die Verpflichtung erst auf, sobald sich ein anderer Dienst mit einem entsprechenden Petitum (freiwillig) an den Gatekeeper wendet. Schließlich sind lediglich die Basisfunktionen von der Verpflichtung umfasst. Nichtsdestotrotz dürften die damit einhergehenden praktischen Herausforderungen erheblich sein. Die Datensicherheit muss technisch auch unter Interoperabilität gewährleistet werden. Aufgrund der vielfältigen individuellen Lösungen der Dienste und technischer Herausforderungen bleibt eine **marktweit interoperable Ende-zu-Ende-Verschlüsselung** bisher eine Herausforderung. Zusätzlich sind zahlreiche datenbezogene Schwierigkeiten zu überwinden. Dies betrifft z. B. die **Datenüberwachung und -verantwortung**, wenn diese durch mehr Hände gereicht werden. Bei unterschiedlichem Umgang mit Kontaktverzeichnis und Datenspeicherung unter den Diensten muss **jederzeit rechtskonformes Verhalten** sichergestellt werden. Ob und inwieweit **Innovationschancen** erhalten werden können, ist eine komplexe Frage, die nicht theoretisch gelöst werden kann. Nach den Erkenntnissen aus den Ermittlungen sind hier durchaus Zweifel angebracht. Zwar ist das DMA-Interoperabilitätsregime auf Basisfunktionen beschränkt. Allerdings sind die Architektur der Dienste und die technische Verortung der einzelnen Funktionen auf dieser sehr individuell, so dass Interoperabilität hier Vereinheitlichungen und Anpassungen in unterschiedlichem Ausmaß erfordern würde, was auch die Innovationskräfte unterschiedlich beeinträchtigen könnte.
Die Bewertung ist letztendlich abhängig vom unterstellten Entwicklungsszenario. Wenn es nur zu einzelnen oder wenigen **bilateralen Vereinbarungen** zwischen Gatekeepern und Petenten käme, erscheinen die Herausforderungen lösbar, zumal die Erschwernisse auf Seiten der Petenten freiwillig in Kauf genommen werden. Eine Vielzahl von individuellen Referenzangeboten erscheint dagegen aus gesamtwirtschaftlicher Perspektive nachteilig, so dass dann über entsprechende marktweite Standardisierungen beraten werden müsste. Letzteres erscheint nach den Ermittlungsergebnissen des Bundeskartellamts zum jetzigen Zeitpunkt wenig wahrscheinlich. Nicht auszuschließen ist, dass die Interoperabilitätsverpflichtung für Gatekeeper **Neueinsteigern Chancen bietet**, die auf den Anschluss an die großen Netzwerke führender Dienste angewiesen sind.

Ansätze für mehr wettbewerblichen Datenschutz

Die Datenschutzqualität scheint insb. auf Seiten der Verbraucherinnen und Verbraucher als Nachfragende und auch bei einigen Diensten nicht die notwendige Beachtung innerhalb wettbewerblicher Auswahlprozesse zu finden. Es dürfte somit nicht davon auszugehen sein, dass sich

das Datenschutzniveau unter den gegebenen Rahmenbedingungen marktgetrieben verbessern wird. Vielmehr sind zum einen datenschutzfreundliche Dienste im Wettbewerb zu stärken. Zu hinterfragen ist zum anderen, welche Anreize notwendig sind, damit die Verbraucherinnen und Verbraucher die Datenschutzqualität als wesentliche Produkteigenschaft erkennen und zu datenschutzfreundlichen Diensten wechseln.

Wettbewerber etablierter Dienste haben auf **diskriminierende Ausschreibungsbedingungen** für Messaging und Video-Dienstleistungen mit sachlich unnötigen Hürden verwiesen. Hier wäre zu überprüfen, welche Bedingungen für die gewünschte Funktionserfüllung tatsächlich erforderlich sind. Eine weniger restriktive Handhabung darüberhinausgehender Anforderungen, z. B. an Größe und Umsatz, könnte ggf. datenschutzfreundlichen Diensten den Weg ebnen.

Viele der befragten Dienste versprechen sich auch von einer Überprüfung der aktuellen **Förderungspraxis von Open Source und Standardisierung** positive Effekte auf das Datenschutzniveau. Zugunsten der Sicherheit der Daten der Nutzerinnen und Nutzer könnte der gesamte Lebenszyklus einer Software einbezogen werden. Nicht nur die neu entwickelte Anwendung oder Technik als Innovation, sondern auch die kontinuierliche Wartung und Pflege der auf dieser Basis am Markt etablierten und von den Verbraucherinnen und Verbrauchern genutzten Produkte erscheint im Sinne der Datensicherheit förderungswürdig.
Wenn der öffentliche Bereich darüber hinaus ausschließlich datenschutzfreundliche Dienste einsetzen würde, wäre dies nach Ansicht vieler Befragter ein positives Signal für den Datenschutz. Allerdings legen die Erkenntnisse des Bundeskartellamts nahe, dass hier noch Verbesserungsmöglichkeiten bestehen könnten. Datenschutzfreundliche Messenger- und Video-Dienste haben sich bisher offenbar – sowohl, was ihre Auswahl als auch ihren bezahlten Einsatz im öffentlichen Bereich betrifft - nicht gegenüber weit verbreiteten Diensten durchsetzen können. Branchenvertretende haben zahlreiche Beispiele vorgelegt, wieviel Einsatz und Überzeugungskraft notwendig ist, damit datenschutzfreundliche Messenger- und Video-Dienste, die weniger bekannt sind als die etablierten Dienste, in Erwägung gezogen werden. Dies betrifft vor allem Bereiche, wo viele Verbraucherinnen und Verbraucher erreicht werden sollen, wie z. B. im öffentlichen Rundfunk, aber auch bei Städten und Gemeinden, Bundesministerien oder Verwaltungseinheiten sowie im Bildungsbereich.

Was **Datenschutz als Qualitätseigenschaft** angeht, ist bisher nicht ersichtlich, dass viele Verbraucherinnen und Verbraucher die Auswahl ihres Messenger- und Video-Dienstes nach dessen Datenschutzfreundlichkeit richten. Wenn sie es doch versuchen, müssen sie mit sehr ungleich verteilten Informationen - zugunsten der Dienste, zu ihren Lasten - zurechtkommen. Die Verbraucherinnen und Verbraucher müssten zunächst herausfinden, welche Informationen überhaupt relevant sind, dann diese suchen, sich ein grundlegendes Verständnis erarbeiten und abschließend aus mehreren Kriterien

noch ein Gesamturteil bilden und vergleichen. In einer **technisch basierten Branche** scheinen sich unüberwindbare Hürden zu stellen: Die technischen Kriterien, Verfahren und Praktiken, die die Datenschutzqualität eines Messenger- und Video-Dienstes bestimmen, sind für Laien komplex und schwer nachzuvollziehen. Die Messenger- und Video-Dienste verspüren dadurch - jedenfalls abseits des Geschäftskundensegments - wenig Druck, den Verbraucherinnen und Verbrauchern eine informierte Entscheidung in Sachen Datenschutz zu ermöglichen.

Im Zuge aktueller Entwicklungen treten weitere Herausforderungen hinzu: Die Interoperabilitätsregeln im DMA werden die Datensicherheit und damit den Datenschutz vor weitere Herausforderungen stellen. Die Dienste sind technisch unterschiedlich aufgestellt. Viele bekannte Dienste sind als geschlossenes System gestaltet worden. Die Daten der Nutzerinnen und Nutzer können somit neuen Risiken ausgesetzt sein. Dieser Umstand erfordert hohe Aufmerksamkeit, wenn Interoperabilität praktiziert wird. Allerdings kann die Informationslage für die Verbraucherinnen und Verbraucher gleichzeitig noch undurchschaubarer werden.

*Die **Komplexität der notwendigen Informationen kann am Beispiel der Verschlüsselung** veranschaulicht werden, auch wenn vereinfachend von tieferen technischen Details und Benennungen abgesehen wird. So sind zunächst verschiedene **Varianten** der Verschlüsselung zu unterscheiden. Bei der Transportverschlüsselung wird der Transportkanal einer Nachricht verschlüsselt. Sie kann aber sowohl von Nutzerinnen und Nutzern des Messenger- und Video-Dienstes selbst, als auch vom Serverbetreiber eingesehen werden. Anders als bei der Transportverschlüsselung wird bei der Ende-zu-Ende-Verschlüsselung („E2E-Verschlüsselung") die Nachricht verschlüsselt über alle Übertragungsstationen hinweg versendet. Nur die Kommunikationspartner als Endpunkte der Kommunikation können die Daten entschlüsseln. Beide Varianten können jeweils einzeln oder kombiniert eingesetzt werden. Letzteres bietet das höchste Sicherheitsniveau. Zur Verschlüsselung kommen **verschiedene kryptographische Verfahren** wie die symmetrische oder die asymmetrische Verschlüsselung mit öffentlichen und privaten Schlüsseln zum Einsatz. Die Ende-zu-Ende-Verschlüsselung wird in der Praxis über unterschiedliche technische Standards umgesetzt, je nachdem, welche Kommunikationsform - Textnachricht, Audio-/Video-Austausch - verwendet wird und welches Messaging- und Video-System genutzt wird. Darüber hinaus bestehen bisher **zahlreiche technische Einschränkungen**, die auch einer möglichen Interoperabilität im Wege stehen würden. Dies betrifft zum einen die Verschlüsselung von **Textnachrichten in Gruppen (Gruppenchat)**, die mit ansteigender Gruppengröße immer aufwendiger wird. Die Lösung in Form des neuen Standards Messaging Layer Security (MLS) wird vereinzelt erprobt. Außerdem wurde eine neue Arbeitsgruppe bei der IETF eingesetzt, die Lösungen für interoperables Messaging entwickeln soll und dazu auch den MLS-Standard verwenden wird. Ob und inwieweit sowie wann es zu einer flächendeckenden Umsetzung in der Branche kommt, ist abzuwarten.*

*Auch bei **Videokonferenzen und Webinaren** unterliegt die Ende-zu-Ende-Verschlüsselung zurzeit technischen Einschränkungen. Generell erfordert die Ende-zu-Ende-Verschlüsselung, dass die Teilnehmenden technisch in der Lage sind, die notwendigen Verschlüsselungsfunktionen bereitzustellen und anzuwenden. Alle Teilnehmenden müssen sich auf dem gleichen Sicherheitsniveau bewegen. Im Umkehrschluss kann eine E2E-Verschlüsselung nicht erreicht werden, sobald eine Teilnehmerin oder ein Teilnehmer das geforderte Sicherheitsniveau unterschreiten.*

*Dieser Fall tritt z. B. dann ein, wenn Teilnehmende einen sogenannten **WebRTC-Client** einsetzen. WebRTC ist ein direkt im Browser verankertes Protokoll, welches nur zwischen zwei Endpunkten Ende-zu-Ende verschlüsseln kann. Bei mehr als zwei Teilnehmenden einer Videokonferenz sind dies jeweils das Endgerät der Nutzerin oder des Nutzers mit dem Server des Dienstes, was den Anforderungen der Ende-zu-Ende-Verschlüsselung nicht mehr entspricht.*

*Auch mit bestimmten **Funktionen**, die Nutzerinnen und Nutzer in Videokonferenzen gerne verwenden, kann die Ende-zu-Ende-Verschlüsselung derzeit technisch nicht verbunden werden: Zu diesen Funktionen gehören z. B. die **Einwahl aus dem öffentlichen Telefonnetz** oder die **Aufzeichnung von Meetings** durch den anbietenden Dienst. Dies ist nur möglich, wenn der Dienstbetreiber auf den Datenstrom zugreifen kann, um den Audioanruf einzubinden bzw. die Daten aufzuzeichnen. Auch die **Anbindung bestimmter externer Geräte** (z. B. Raumkonferenzsystem-Geräte, die auf dem SIP-Protokoll basieren) ist unter Ende-zu-Ende-Verschlüsselung nicht möglich, da dazu die verschiedenen Protokolle synchronisiert werden müssten. Führende Dienste haben auf eben solche und weitere Einschränkungen, wie beispielsweise die **Verwendung von „Assistenten“** ausdrücklich hingewiesen.*

*Große Videokonferenzen für **Webinare mit mehreren Hundert Teilnehmenden** können zurzeit technisch nicht durch Ende-zu-Ende-Verschlüsselung gesichert werden. In diesem Anwendungsfall ist es notwendig zu prüfen, ob der anbietende Dienst einen Video-Dienst-Standort in Deutschland betreibt und dieser sicherheitstechnisch geprüft wurde (beispielsweise durch ein BSI C5 Testat). Transportverschlüsselung und der sichere Betrieb des Video-Dienstes in Deutschland sollten hierfür das Kriterium sein. Ferner ist darauf zu achten, dass die Identität der Teilnehmenden zweifelsfrei festgestellt werden kann („Authentisierung“). Ende-zu-Ende-Verschlüsselung stellt die Integrität der übermittelten Daten sicher. Ohne eine vorherige zweifelsfreie Authentisierung sorgt sie zwar für den Schutz der übermittelten Daten, stellt aber nicht sicher, wer diese Daten empfangen kann.*

In der Checkliste des Bundeskartellamts, die einer Einschätzung der Datenschutzqualität von Messenger- und Video-Diensten zugrunde gelegt werden könnte, ist die **Verschlüsselung nur eines von mehreren Kriterien,** die sich die Verbraucherinnen und Verbraucher erschließen müssten. Vor diesem Hintergrund erscheint es nicht zumutbar und zielführend, die Verantwortung für mehr wettbewerblichen Datenschutz allein den Verbraucherinnen und Verbrauchern zuzuordnen, auch dann nicht, wenn die Informationen für die Verbrauchenden extrem komprimiert und vereinfacht würden. Maßnahmen zugunsten der Datenschutzqualität müssen auch die Dienste einbeziehen. An die Seite einer effektiven Durchsetzung des geltenden Rechts sollten daher Maßnahmen gestellt werden, die den Datenschutz als Wettbewerbsparameter stärken können.

Datenschutzqualität vergleichend und transparent bewerten

Nach derzeitiger Auffassung des Bundeskartellamts könnten rein marktbezogene Maßnahmen nicht ausreichend sein, um Datenschutz aus seinem Schattendasein unter den Wettbewerbsparametern herauszuhelfen und die notwendige Aufmerksamkeit zu verschaffen. Eine transparente und vergleichende Bewertung der Datenschutzqualität von Messenger -und Video-Diensten, z. B mit Hilfe

eines Rating-Verfahrens anhand ausgewählter Kriterien des Datenschutzes und der Datensicherheit, könnte hilfreich sein.

Ein solches Verfahren könnte beide Marktseiten in Sachen Datenschutz aktivieren. Die größte Resonanz dürfte es zunächst auf der Seite der anbietenden Messenger- und Video-Dienste auslösen. Es darf vermutet werden, dass viele Messenger- und Video-Dienste ein **öffentlich negatives Zeugnis oder ein schlechteres Ranking als der wichtigste Wettbewerber** vermeiden möchten. Datenschutz ist nicht nur „Gesetz" - in Deutschland und Europa in Gestalt der DSGVO - sondern inzwischen auch zu einem sensiblen Thema geworden, das von der (Fach-) Öffentlichkeit aufmerksam verfolgt wird und auch im politischen Umfeld Beachtung findet. Dazu hat auch die ständige Auseinandersetzung mit den Praktiken einiger führender Branchenvertreter und öffentliches Nachdenken über staatliche Initiative wegen unerwünschter Praktiken und Entwicklungen beigetragen. Möglicherweise möchten aber auch die Verbraucherinnen und Verbraucher nicht bei einem Messenger- und Video-Dienst registriert sein, der **im Ranking den letzten Platz** einnimmt. Vielleicht möchte auch eine ihrer Kontaktpersonen lieber einen Messenger- und Video-Dienst nutzen, der ein niedrigeres Datenschutzrisiko aufweist als der bisher gewählte Dienst. Dies gilt auch, wenn stellvertretend für die Verbrauchenden agiert wird: Ein veröffentlichtes Rating-Urteil einer vertrauenswürdigen Instanz kann die **glaubwürdige Information sein, die berufliche „Entscheider" oder Ansprechpartner** für die Öffentlichkeit bei Behörden und Unternehmen benötigen, um über die DSGVO-Konformität eines Messenger- und Video-Dienstes und damit dessen Einsatzmöglichkeiten in der eigenen Institution zu entscheiden.

Das Bundeskartellamt empfiehlt in Anknüpfung an den vorliegenden Bericht:

- Die **Durchsetzung des Verbraucherrechts sollte gestärkt** werden. Die digitale Wirtschaft stellt die Verbraucherinnen und Verbraucher insb. aufgrund ihrer technischen Basis ständig vor neue Herausforderungen, die trotz des Engagements aller Akteure immer schwerer einzufangen sind. Die Kompetenzen und Erfahrungen des Bundeskartellamts bei der Rechtsdurchsetzung können hier einen sinnvollen Beitrag zur Bewältigung und Gestaltung leisten.
- Die Bemühungen um die Aufklärung der Verbraucherinnen und Verbraucher, insb. zugunsten der Entwicklung von Medienkompetenz, sind zu intensivieren. Alle Bevölkerungsgruppen sollten in eine **Kommunikationsstrategie für den Datenschutz** integriert werden. Eine entsprechende bundesweite Kampagne sollte daher sowohl die internetbasierten digitalen Medien als auch herkömmliche Medien, wie Fernsehen, nutzen.
- Ein denkbares Signal wäre, wenn der **öffentliche Bereich** datenschutzfreundliche Messenger- und Video-Dienste stärker einsetzen würde. Ansprechpersonen und Entscheiderinnen und Entscheider brauchen verlässliche Informationen **zur DSGVO-Konformität von Messenger- und Video-Diensten** – gerade auch derjenigen Dienste, die nicht im Fokus des öffentlichen Interesses stehen. Daher könnten Institutionen, Organisationen und Unternehmen den

Mitarbeitenden entsprechende **schriftliche Informationsbriefe, -broschüren und Handreichungen** zur Verfügung stellen.

- **Interoperabilität** sollte nicht nur **innovationsfreundlich**, sondern auch **verbraucherorientiert** umgesetzt werden. Die ohnehin komplexen technischen und rechtlichen Zusammenhänge von Datensicherheit und Datenschutz dürften unter Interoperabilität noch weniger zu überblicken sein. Bei jeglichen Vorhaben und Bemühungen zur Gestaltung von Interoperabilität einschließlich ihrer technischen Herausforderungen dürfen die Verantwortlichen stellvertretend für die Nutzerinnen und Nutzer die **Anforderungen eines sicheren Verbraucherprodukts** nicht aus dem Blick verlieren.

A. Einleitung

Seit jeher war es der Wille des Menschen, sich mit anderen Menschen auszutauschen, in Verbindung zu treten und Gedanken und Ideen festzuhalten. Ein solcher Prozess der Verständigung[7] wird auch Kommunikation genannt. Dazu muss ein Absender Zeichen welcher Art auch immer an einen Empfänger übermitteln. Diese Beschreibung der Kommunikation kommt der Definition des modernen Messaging sehr nah. Überhaupt scheint es, als ließe der von den Verbraucherinnen und Verbrauchern so intensiv praktizierte Austausch über Textnachrichten, Telefonie- und Videotelefonie, einschließlich des Versendens von Fotos und Emojis, alle Entwicklungsstufen der Kommunikationsgeschichte wiederaufleben, wenn auch in einer modernen Gestalt.

So kommunizierten die Menschen zunächst über Bilder, die auf Felswände oder auf Steine gemalt oder geritzt wurden.[8] Kommunikation über Bildzeichen liegt auch heute wieder im Trend. Mit dem Messaging haben z. B. die Emojis Einzug in die Kommunikation gehalten. Im Unterschied zu früher setzen viele Verbraucherinnen und Verbraucher Bildsymbole heute allerdings ein, um Gefühlen Ausdruck zu geben. Später traten als weitere Kommunikationsarten zunächst die eigentliche Schrift und schließlich noch die Fotographie hinzu. Für Verbraucherinnen und Verbraucher scheint es inzwischen unverzichtbar zu sein, mit ihren Smartphones zu fotografieren und die Fotos über ihren Messenger- und Video-Dienst direkt an ihre Kontakte zu versenden.

Heutzutage hüllt das Messaging diese lange bewährten Kommunikationsarten in ein modernes Gewand. Anders als früher können die Verbraucherinnen und Verbraucher heute die verschiedenen Funktionen, die Messenger- und Video-Dienste ermöglichen, **individuell einsetzen und kombinieren**. Ferner stehen bisher etablierte Kommunikationsformen wie E-Mail, Briefpost oder SMS als weitere Kommunikationswege bereit.

---

[7] Vgl. *Der Oberbürgermeister der Bundesstadt Bonn*, „Was willst Du mir damit sagen?“ Die Geschichte der Kommunikation, abrufbar unter: https://www.bonn.de/medien-global/amt-41/stadtarchiv/Ausstellung_Geschichte_der_Kommunikation.pdf.

[8] Die Bilderschrift geht vor allem auf die Sumerer im Gebiet des heutigen Irak und die Ägypter zurück, die ca. 3000 v. Chr. mit den Hieroglyphen eine komplexe Bilderschrift entwickelten. Siehe z. B. *Planet Wissen*, abrufbar unter: https://www.planet-wissen.de/gesellschaft/lernen/erfindung_der_schrift/index.html# Hieroglyphe, siehe *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Geschichte_der_Schrift, siehe *ARD alpha*, abrubar unter: https://www.br.de/wissen/schrift-ursprung-keilschrift-mesopotamien-100.html, siehe Viaprinto, abrufbar unter: https://www.viaprinto.de/blog/2016/06/die-geschichte-der-schrift/.

Der **Wunsch nach Individualität oder einer maßgeschneiderten Lösung** für die eigenen Bedürfnisse schlägt sich bei Messenger- und Video-Diensten in einer großen **Vielfalt an Geschäftsmodellen und Anwendungen** nieder. Wie das Bundeskartellamt im Zwischenbericht zu dieser Sektoruntersuchung bereits ausgeführt hat, sind die Funktionen, die Geschäftsmodelle und die wirtschaftliche Bedeutung der Messenger- und Video-Dienste sehr verschieden. Neben den bei Verbraucherinnen und Verbrauchern beliebten führenden Diensten besteht eine große Bandbreite an Branchenteilnehmenden, welche von internationalen, konzernbetriebenen Diensten mit vielen Millionen Nutzerinnen und Nutzern, hohen Umsätzen und eigenen digitalen Ökosystemen[9] mit starken Positionen auf benachbarten Märkten über nationale oder auf deutschsprachige Regionen konzentrierte Dienste oder Dienste mit besonderen Geschäftsschwerpunkten bis hin zu Open Source-Diensten und freien Anwendungen ohne Gewinnerzielungsabsicht reicht.

Ein Anliegen dieser Sektoruntersuchung war zunächst, diese Vielfalt offen zu legen. Dies hat mehrere Gründe.

Die Aufmerksamkeit der Aufsichtsbehörden und Datenschützerinnen und Datenschützer ruht häufig auf einem bestimmten Geschäftsmodell führender Messenger-Dienste, im Rahmen dessen über ein kostenloses Angebot Daten der Verbraucherinnen und Verbraucher gesammelt und verwertet werden. Allerdings hat sich daneben - abseits dieser populären Dienste - eine differenzierte Branche mit erheblichen Umsatz- und Nutzerzahlen entwickelt, deren Zusammensetzung weiten Teilen der Öffentlichkeit nach wie vor unbekannt ist. Fraglich war, ob und inwieweit mögliche, mit dem führenden

---

[9] Mit dem Begriff “digitales Ökosystem” wird ein Bündel einer Vielzahl an Diensten eines Konzerns mit Wechselwirkungen untereinander bezeichnet, vgl. *Bundeskartellamt*, Stellungnahme zur öffentlichen Anhörung des Wirtschaftsausschusses zum Digital Markets Act, 25. April 2022, abrufbar unter: https://www.bundestag.de/resource/blob/891308/f13edcf322cc218da602e6dc4b58391b/ADrs-20-9-59_Stellungnahme-Mundt-data.pdf sowie *Bundeskartellamt*, The Evolving Concept of Market Power in the Digital Economy – Note by Germany, abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/OECD_2022_Competition_Committee_Concept_Market_Power_Digital_Economy.pdf?__blob=publicationFile&v=2. Siehe z. B. auch *Fletcher,* Digital competition policy: Are ecosystems different?, Note for the OECD Hearing on Competition Economics of Digital Ecosystems, abrufbar unter: https://one.oecd.org/document/DAF/COMP/WD(2020)96/en/pdf. In der Informationstechnik wird mit dem Begriff Ökosystem eine Soft- und Hardware-Architektur bezeichnet, welche auf jeweils ganz eigenen Geräten, Systemen und Zugangsvoraussetzungen beruht und damit entsprechendes Zubehör voraussetzt und hervorbringt, vgl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/%C3%96kosystem.

Geschäftsmodell verbundene **Rechtsverstöße und auch weitere verbraucherrechtliche Versäumnisse** in der Branche Verbreitung gefunden haben. Dies betrifft zum Beispiel die Weitergabe von Kontaktdaten, die den führenden Diensten als Verstoß gegen das Datenschutzrecht vorgehalten wird. Es geht außerdem um Sicherheitsmängel, etwa bei der Verschlüsselung. Wenn die Nutzerinnen und Nutzer über sicherheitsrelevante Aspekte eines Messenger- oder Video-Dienstes nicht angemessen informiert werden, könnten sie unzulässig in die Irre geführt werden. Sektoruntersuchungen sind hier das geeignete Instrument. Sie richten sich nicht auf bestimmte Unternehmen, sondern nehmen eine Branche als Ganzes in den Blick.

Des Weiteren waren im politischen Raum immer wieder Forderungen nach Interoperabilität aufgekommen.[10] Inzwischen haben sich diese **politischen Forderungen** nicht nur im Koalitionsvertrag, sondern auch im Interoperabilitätsregime des Gesetzes über digitale Märkte, dem Digital Markets Act[11] niedergeschlagen. Im Zwischenbericht hat das Bundeskartellamt bereits erläutert und mit den Ermittlungsergebnissen belegt, dass die Analyse der Wirkungszusammenhänge zwischen Wettbewerb, Datenschutz und Innovation vielschichtig und komplex ist. In diesem Abschlussbericht steht nun die **konkrete Umsetzung** eines Interoperabilitätsvorhabens im Vordergrund, bei dem kaum abgeschätzt werden kann, wie es tatsächlich in Anspruch genommen werden wird. Eine Herausforderung sind nicht nur die Vielfalt der technischen Architektur der Messenger- und Video-Dienste und die individuellen Anpassungen internationaler Standards. Insbesondere wenn die persönlichen Daten der Nutzerinnen und Nutzer in einem internationalen Geschäft durch weitere Hände gereicht werden, müssen neue Lösungen gesucht werden, ohne die gesamtwirtschaftliche Kosten aus dem Blickfeld zu verlieren.

---

[10] 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.

[11] Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates v. 14.09.2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828, ABl. L 265/1 v. 12.10.2022 (Gesetz über digitale Märkte) – DMA, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R1925&from=EN .

Schließlich ist die Heterogenität der Branche auch ein Spiegel der Verbraucherwünsche, die eben durchaus vielfältig und unterschiedlich sind. Gleiches gilt für die Voraussetzungen, unter denen Verbraucherinnen und Verbraucher Entscheidungen treffen. Dies betrifft nicht nur eine Unterscheidung zwischen geschäftlichen und privaten Vorhaben, auf welche das Bundeskartellamt in den Ermittlungsergebnissen Bezug nimmt, wenn es geboten ist. Vielmehr ist zuletzt in der Fachöffentlichkeit ein eher **differenziertes Verbraucherleitbild** diskutiert worden, welches die Verbraucherinnen und Verbraucher als verantwortungsvoll, verletzlich oder vertrauend[219] beschreibt.[220] Es scheint insofern inzwischen weitgehend Einigkeit zu bestehen, dass Unterschiede zwischen den Verbraucherinnen und Verbrauchern, was ihre Wahrnehmung, Emotion und Motivation angehen, zu berücksichtigen sind.[221] Dies gilt nicht nur dann, wenn es um ihre Schutzbedürftigkeit geht, die im Mittelpunkt der Handlungsempfehlungen in diesem Sektoruntersuchungsbericht steht. Ein realistisches Verbraucherleitbild ist auch wichtig, damit entsprechend angepasste Maßnahmen ergriffen werden, die Verbraucherinnen und Verbraucher motivieren, Datenschutz als Wettbewerbsparameter voranzubringen und ihre Daten besser zu schützen.

Der Anspruch an die Handlungsempfehlungen ist somit hoch. Nicht nur die Vielfalt der Branche, auch die politischen Festlegungen zur Interoperabilität sowie die Wünsche und Verhaltensweisen der Verbraucherinnen und Verbraucher sind zu berücksichtigen und bestmöglich zu integrieren, wenn Handlungsempfehlungen für ein höheres Datenschutzniveau formuliert werden. Notwendig wären somit Maßnahmen, die **beide Marktseiten motivieren**, im wettbewerblichen Geschehen dem Datenschutz mehr Priorität einzuräumen. Dies bezieht sich nicht nur auf das Abstellen der verbraucherrechtlichen Verstöße, die in diesem Bericht geprüft werden. Es geht insbesondere um eine bessere Information der Nachfragerinnen und Nachfrager und im Zuge dessen um die engagiertere praktische Umsetzung von wettbewerblichem Datenschutz. In Frage steht auch, wie der öffentliche Bereich sich auch außerhalb von rechtlichen Verfahren, die die zuständigen Behörden führen, für ein höheres Datenschutzniveau einsetzt. Auch bei Interoperabilitätsvorhaben und dem damit verbundenen Wunsch nach vermehrten Wechselaktivitäten der Verbrauchenden ist zu berücksichtigen, dass es aus deren Sicht an Transparenz und Vergleichbarkeit zur Datenschutzqualität bereits beim bilateralen Austausch über Messenger- und Video-Dienste mangeln dürfte.

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

Danach wird die **Branche** in ihrer Vielgestaltigkeit und mit ihren wesentlichen Kennzeichen (siehe hierzu Kapitel C.) sowie das wirtschaftliche und wettbewerbliche Umfeld kurz beschrieben.

Anschließend wird dargelegt, wie sich **wichtige Sicherheitskriterien und die Art und Weise der Datenverarbeitung** auf die Datenschutzfreundlichkeit eines Dienstes auswirken können und wie sich die Branche praktisch dazu stellt (siehe dazu Kapitel D.). Im Anschluss werden die Ergebnisse gewürdigt. Es

wird mit der Perspektive der Verbraucherinnen und Verbraucher und dem Stand der Technik zunächst eine Orientierung für die Bewertung eingeführt, bevor aus den Ermittlungsergebnissen zu den Sicherheitskriterien Rückschlüsse auf das, was wünschenswert wäre, gezogen werden. Dem schließt sich eine **rechtliche Einordnung** an. Fraglich ist, wie die gängige Praxis vieler bekannter Messenger- und Video-Dienste, das Kontaktverzeichnis der Nutzerinnen und Nutzer hochzuladen und zu synchronisieren, aus datenschutzrechtlicher Sicht zu bewerten ist. Untersucht wird ferner, inwieweit Messenger- und Video-Dienste entsprechend der Ermittlungsergebnisse beim Datentransfer in Drittländer und beim Speichern auf Servern in Drittländern die datenschutzrechtlichen Vorschriften einhalten. Schließlich geht es darum, ob das Informationsverhalten der Dienste zur Ende-zu-Ende-Verschlüsselung lauterkeitsrechtliche Transparenzpflichtverstöße auslösen kann. Das Kapitel endet mit einem Fazit, ob und inwieweit die Verbraucherinnen und Verbraucher am besten mit der gegenwärtigen Situation umgehen können.

Es schließen 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 E.). Den theoretischen Erwägungen folgen auch hier Ermittlungsergebnisse, die als Indikator für das Wechselverhalten der Verbraucherinnen und Verbraucher interpretiert werden können.

Danach geht es um den nächsten Schwerpunkt dieses Berichts, die Untersuchung der Leitfrage, ob und inwieweit **Interoperabilität zu einem höheren Datenschutzniveau** führen könnte (Kapitel F.). Vorausgeschickt wird zunächst eine begriffliche, rechtliche und wissenschaftliche Einordnung (dazu unter F.I). Anders als in verbraucherrechtlichen Vorschriften können nach Wettbewerbs- und Telekommunikationsrecht - unter hohen Voraussetzungen und in einem festgelegten Verfahren - die Behörden eine Interoperabilitätsverpflichtung aussprechen. Inzwischen wird der rechtliche Rahmen für Messenger- und Video-Dienste durch den Digital Markets Act ergänzt. Dieser trat im November 2022 in Kraft und hat zu einer Konkretisierung des rechtlichen Umfeldes der Messenger- und Video-Dienste in Sachen Interoperabilität geführt. So werden nämlich designierten Diensten, sog. „Gatekeeper“ im Sinne des DMA, Vorschriften zur Interoperabilität bestimmter Basisfunktionen auferlegt. Die Komplexität der Leitfrage legen auch die zahlreichen wissenschaftlichen Untersuchungen nahe, zu denen anschließend ein kurzer Überblick gegeben wird. Darauf folgt eine kurze Beschreibung der Möglichkeiten der technischen Umsetzung und Gestaltung. Die Unterschiede liegen nicht nur in der technischen Eingriffstiefe und im erforderlichen Aufwand. Die Maßnahmen unterscheiden sich auch nach Reichweite und notwendigem Ausmaß an Konsensbereitschaft der Beteiligten. Wesentlich für die zukünftige Marktentwicklung bei Messenger- und Video-Diensten einschließlich Interoperabilität ist schließlich das Verhalten der Verbraucherinnen und Verbraucher (dazu unter F.II).

Im Anschluss werden die Ermittlungsergebnisse zur Interoperabilität ausführlich vorgestellt (dazu unter F.III). Zusätzlich zu den Ausführungen im Zwischenbericht wurde aufgenommen, wie sich die Branche zur funktionellen und technischen Gestaltung und zur Standardisierung stellt (dazu unter F.III.3.b und c). Am Ende des Kapitels können erste Schlussfolgerungen gezogen werden (dazu unter F.IV). Jegliche behördliche oder gesetzgeberische Maßnahmen, die sich auf die Beseitigung von Problemlagen richten, sind so zu gestalten, dass auch **Chancen für die weitere Marktentwicklung erhalten** werden. Von Interesse ist in diesem Zusammenhang auch, wie sich die im Vorfeld geäußerten Meinungen der Messenger- und Video-Dienste und die aktuellen gesetzgeberischen Pläne im Vergleich darstellen. Welche Szenarien für die weitere Entwicklung der Branche sind im Hinblick auf Interoperabilität angesichts des Verbraucherverhaltens denkbar und wie ist damit umzugehen?

Vor diesem Hintergrund werden in Kapitel G. **konkrete Ansätze** vorgestellt, wie das Datenschutzniveau bei Messenger- und Video-Diensten verbessert werden könnte. Das Bundeskartellamt hatte die Dienste in seinem Fragebogen gebeten, verschiedene vorgeschlagene Maßnahmen zu kommentieren und zu bewerten (dazu unter G.I). Vor dem Hintergrund dieser Ermittlungsergebnisse hat das Bundeskartellamt einige Aspekte aufgegriffen, die dem Datenschutz in wettbewerblichen Prozessen ein stärkeres Gewicht verleihen können (dazu unter G.II). Dazu werden zunächst Verbesserungen für datenschutzfreundliche Messenger- und Video-Dienste vorgestellt, die zeitnah und mit vergleichsweise wenig Aufwand umgesetzt werden können. Anschließend wird die Rolle zielgerichteter Information für die nachfragenden Verbraucherinnen und Verbraucher erörtert. Wird sich das Datenschutzniveau auf diese Weise - marktgetrieben - unter den gegebenen Rahmenbedingungen verbessern? Den Abschluss des Kapitels bilden Ausführungen zu einer vergleichenden und transparenten Bewertung der Datenschutzqualität - zum Rating - einem Instrument, das geeignet scheint, beide Marktseiten zu motivieren, Datenschutz als Wettbewerbsparameter zu begreifen und aktiv in Auswahlprozessen zu berücksichtigen (dazu unter G.III).

Der Bericht schließt mit **Handlungsempfehlungen zur Verbesserung des Datenschutzniveaus** bei Messenger- und Video-Diensten (dazu unter H.). Aufgrund der Vielfalt der Branche und der vielen nachhaltigen Geschäftsmodelle und freien Anwendungen neben den bekannten Marktführern möchte das Bundeskartellamt mit diesem Bericht nicht nur einen Beitrag zu mehr Transparenz leisten. Es sollen vielmehr gesamtwirtschaftlich förderliche, konkrete Hinweise für Verbesserungen des Verbraucherschutzes gegeben werden. Alle Bereiche und Beteiligten sind in eine solche Datenschutzstrategie einzubeziehen, sowohl das System der verbraucherrechtlichen Rechtsdurchsetzung (dazu unter H.I) als auch die Verbraucherinnen und Verbraucher (dazu unter H.II) sowie die Messenger und Video-Dienste selbst (dazu unter H.III.). Abschließend werden Merkmale eines innovationsfreundlichen und verbraucherorientierten Interoperabilitätskonzepts vorgestellt, das

zugunsten aller genannten Adressaten positiv wirken und Datensicherheit und Datenschutz fördern kann (dazu unter H.IV).

B. Verfahrensgang

I. Verbraucherrechtliche Sektoruntersuchung

Das Bundeskartellamt hat im November 2020 eine verbraucherrechtliche Sektoruntersuchung „Messenger-Dienste“ nach § 32e Abs. 5 GWB eingeleitet.[12]

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 Marktteilnehmenden und Expertinnen und Experten geführt, um die Untersuchungsthemen zu spezifizieren und die Befragung vorzubereiten.

Am 31. Mai 2021 hat das Bundeskartellamt umfangreiche Fragebögen[13] an die Betreiberinnen und Betreiber von 53 Messenger- und Video-Diensten im In- und Ausland versendet. Zwei Befragte wurden nachträglich wieder von der Liste der Adressaten genommen. 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.[14] Die Angaben dieser Dienste bilden die Basis der nachfolgend dargestellten Ermittlungsergebnisse.

Das Bundeskartellamt hat am 4. November 2021 den Zwischenbericht zur Sektoruntersuchung vorgelegt.[15] Die Ergebnisse des Zwischenberichts sind in den Abschlussbericht eingegangen. Aus dem Zwischenbericht wurden, teilweise mit kleinen Änderungen, die Ausführungen zur Branche (Kapitel C.),

---

12 Vgl. *Bundeskartellamt*, 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.

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

14 Siehe Liste der einbezogenen Dienste im Anhang.

15 Vgl. *Bundeskartellamt*, Pressemitteilung vom 04.11.2021, abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2021/04_11_2021_SU_Messenger-Dienste_Zwischenbericht.html?nn=9624654.

zur Datenportabilität (Kapitel E.) sowie in Teilen einzelne Abschnitte von Kapitel F. über die Ermittlungsergebnisse zur Interoperabilität (siehe F.III.4 und F.III.5) übernommen.

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 BSI wird durch das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik[16] 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 dem 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, Meta-Daten/Datenschutz und Interoperabilität.

---

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

17 Das BSI hat u. a. ein umfangreiches Informationsangebot für Verbraucherinnen und 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. *BSI*, abrufbar unter: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/auftrag_node.html.

18 Vgl. *Bundeskartellamt*, Pressemitteilung vom 22.01.2021, abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2021/22_01_2021_Zusammenarbeit_BSI_BKartA.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 Verbraucherinnen und Verbraucher dazu benötigen und welche Funktionen die Messenger- und Video-Dienste den Verbraucherinnen und Verbrauchern anbieten (hierzu unter I.). Anschließend wird kurz erläutert, in welchem Verhältnis Messenger- und Video-Dienste zu anderen Kommunikationsformen stehen (hierzu unter II.). Da die technische Entwicklung für die Untersuchungsthemen eine große Rolle spielt, wird auch dargelegt, wie offene Standards in der Branche entwickelt werden (hierzu unter III.). Den Abschluss des Kapitels bilden erste Ermittlungsergebnisse zu den Branchenteilnehmenden, zur Finanzierung, zu Nutzungszahlen und zur Wettbewerbssituation (hierzu unter IV.).

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.[19] Das heutige Angebot der Messenger- und

[19] Vgl. *Wikipedia,* abrufbar unter: https://de.wikipedia.org/wiki/Chat.

Video-Dienste geschieht auf Basis der gleichen Technik. Die Nutzerinnen und 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 die Empfängerin oder 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.[20]

Während der **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 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 Verbraucherinnen Verbraucher zunehmend über Videokonferenzen kommunizierten, von

---

[20] 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.

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.[21] 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.[22] OTT-1- Dienste können zwar Sprachübertragungen über das Internet ermöglichen (Internettelefonie) und so in Konkurrenz zu klassischen Telefoniediensten treten.[23] Sie sind aber unabhängig von Festnetz- oder Mobilfunkanschlüssen und erlauben daher keine Verbindung zu klassischen Telefoniediensten 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.[24] **Short Message Service** (Kurznachrichtendienst, SMS) ist ein Telekommunikationsdienst, durch den

---

[21] Vgl. *Bundesnetzagentur (2022)*, Nutzung von Online-Kommunikationsdiensten in Deutschland, Ergebnisse der Verbraucherbefragung, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/OTT.pdf?__blob=publicationFile&v=6, S. 9 f.

[22] 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.

[23] *Body of European Regulators for Electronic Communications (BEREC),* Report on OTT services, Januar 2016, S. 14 f., abrufbar unter: https://www.berec.europa.eu/sites/default/files/files/document_register_store/2016/2/BoR_%2816%29_35_Report_on_OTT_services.pdf.

[24] Vgl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Telefonie.

Textnachrichten, die meist „Kurzmitteilungen“ oder „SMS“ genannt werden, übertragen werden können.[25] SMS basiert auf der GSM[26]-Technologie.

Anders als die rufnummernbasierten Sprachtelefonie und SMS ist **E-Mail** (Electronic Mail für „elektronische Post“) genauso wie Messenger-Dienste webbasiert und zählt 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 SMTP[27]-, IMAP[28]- und POP[29]-Protokollen.[30] Die verschiedenen E-Mail-Server sind über das E-Mail-Protokoll miteinander verknüpft, so dass Nachrichten zwischen verschiedenen Anbietern versendet

---

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

26 GSM (Global System for Mobile Communications, Globales System für mobile Kommunikation) ist ein Mobilfunkstandard für volldigitale Mobilfunknetze, der hauptsächlich für Telefonie, aber auch für leitungsvermittelnde und paketvermittelnde Datenübertragung sowie Kurzmitteilungen genutzt wird. Es ist der erste Standard der sog. zweiten Generation („2G“) als Nachfolger der analogen Systeme der ersten Generation, vgl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Global_System_for_Mobile_Communications.

27 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. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol.

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

29 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. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Post_Office_Protocol.

30 Vgl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/E-Mail.

werden können.[31] 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.

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"[32] stattfinde 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.[33] Es gebe jedoch sich deutlich unterscheidende Funktionalitäten zwischen sozialen Netzwerken und consumer communications apps.[34] 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.[35]

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 Nachrichtenaustauch vermischen** und dass diese Entwicklung fortschreitet. Hier dürften im Zuge der weiteren Entwicklung

---

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

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

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

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

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

ohnehin Veränderungen stattfinden. Möglicherweise werden auch **Virtual Reality**[36] **und Augmented Reality**[37] in die Standardfunktionen von Messenger- und Video-Diensten sowie Sozialen Netzwerken aufrücken. Bei diesen neuen Funktionen können sich Nutzerinnen und Nutzer mit Hilfsmitteln, wie z. B. den sog. VR-Brillen in Echtzeit - während sie sich in ihrer normalen Umgebung befinden - 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. Verfahren der Standardisierung

Messenger- und Video-Dienste funktionieren auf Basis von (Kommunikations-) Protokollen[38] und weiteren technischen 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 Bedeutung für die Branche der Messenger- und

---

[36] „Virtuelle Realität“ (VR) bezeichnet ein digitales, am Computer geschaffenes Abbild der Realität. Eigene VR-Brillen lassen die Nutzerinnen und Nutzer in eine neue, künstlich erschaffene Welt eintauchen, die täuschend echt wirkt. So können sie in Unterwasserwelten mit Walen schwimmen, ein Schiffswrack erkunden oder durch ihr 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, oder *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Virtuelle_Realit%C3%A4t.

[37] 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 die Nutzerin oder 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 der Mechanikerin nützliche Informationen über das technische Bauteil, das sie reparieren soll, vgl. *Deutsche Telekom*: Einfach erklärt – Augmented und virtuelle Realität, abrufbar unter: https://www.telekom.com/de/konzern/details/virtuelle-realitaet-486114.

[38] 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.

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 Netzwerktechnikerinnen und Netzwerktechnikern, Herstellenden, Netzbetreibenden, Forschenden sowie Anwenderinnen und Anwendern, die sich mit der technischen Weiterentwicklung des Internets befasst, um dessen Funktionsweise zu verbessern.[39]

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.[40] 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. [41]

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.[42]

---

[39] Vgl. *IETF*, abrufbar unter: https://www.ietf.org/about/, vgl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Internet_Engineering_Task_Force.

[40] Vgl. *W3C*, abrufbar unter: https://www.w3.org/, vgl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/World_Wide_Web_Consortium und weitere öffentlich verfügbare Quellen.

[41] Vgl. *Wikipedia*, abrufbar unter: https://en.wikipedia.org/wiki/WebRTC.

[42] Vgl. *NETPLANET*, https://www.netplanet.org/organisation/standardisierung.shtml.

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 Society[43] 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 Entwicklerinnen und Entwickler entsenden, um so die Entscheidungsfindung in einer Working Group zu beeinflussen.[44] Ziel könne die Verbreitung eigener Software-Patente über den jeweiligen Standard (sog. **Standardessentielle Patente**, SEP, standard essential patents) sein.[45] 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“[46] 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 (SEPs) offenzulegen. Allerdings werden weder Mitglieder noch die Organisation selbst nach relevanten Patenten suchen oder bei offengelegten Patenten prüfen,

---

43 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, vgl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Internet_Society.

44 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, siehe *Netplanet*, abrufbar unter: https://www.netplanet.org/organisation/standardisierung.shtml.

45 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.

46 *Wirtschaftswoche* vom 4. Mai 2020: Brummen fürs Internet, abrufbar unter: https://www.wiwo.de/technologie/digitale-welt/web-standards-brummen-fuers-internet/25779644.html.

inwieweit sie für den Standard wesentlich sind.[47] Zum anderen wird die Deklarierung 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.[48]

Dieses Verfahren der Entwicklung offener Standards über Standardisierungsorganisationen berührt auch die Fragestellungen der Sektoruntersuchung. Inzwischen hat die IETF die Arbeiten an einem Standard abgeschlossen, 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**[49]**, MLS**). 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). Im ersten Quartal 2023 hat sich erstmals eine neue Arbeitsgruppe MIMI bei der IETF getroffen, die sich mit offenen Lösungen für interoperables Messaging beschäftigen wird.[50]

IV. Ermittlungsergebnisse

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

---

47 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.

48 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 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/.

49 Vgl. https://datatracker.ietf.org/wg/mls/about/, vgl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Messaging_Layer_Security.

50 Vgl. *IETF*, Messaging Layer Security: Secure and Usable End-to-End Encryption, abrufbar unter: https://www.ietf.org/blog/mls-secure-and-usable-end-to-end-encryption/ sowie golem, IETF standardisiert Protokoll für sichere Gruppenchats, abrufbar unter: https://www.golem.de/news/messaging-layer-security-ietf-standardisiert-protokoll-fuer-sichere-gruppenchats-2303-173089.html.

der Branche den Verbraucherinnen und Verbrauchern eine gute Orientierung und Information über mögliche Alternativen jenseits der allgemein bekannten, großen Dienste.

1. Branchenteilnehmende, Funktionen und Geschäftsmodelle

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 Marktteilnehmenden. 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 im Messaging und Videoconferencing viele **weltweit tätige, diversifizierte Technologiekonzerne und global agierende Digitalkonzerne**, die bereits in anderen Märkten erfolgreich sind und starke Stellungen innehaben.
Dies sind z.B. Cisco als u.a. Hersteller von Netzwerktechnik und Endgeräten mit dem Videoconferencier Webex, Google als Hersteller von Betriebssystemen und Suchmaschine mit Google Meet, Social-Media-Plattformbetreiber Meta (ehemals Facebook) mit WhatsApp und Facebook Messenger, Betriebssystem- und Softwarehersteller 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 regionale bzw. nationale Dienste, 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 **Open Source-Bereich**, zu dem Dienste 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 Verbraucherinnen und 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 Nutzerinnen 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 werden, vom Dienstanbieter vorgegeben.
Freie Messenger-Systeme funktionieren ähnlich wie E-Mail-Dienste. Sie fußen technisch auf einem Standardprotokoll (meist XMPP oder Matrix), so dass die Nutzerinnen und Nutzer Nachrichten über verschiedene Messenger-Clients hinweg austauschen können. Gesprächspartnerinnen und -partner 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. Nutzerinnen und 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 XMPP, Matrix und Systeme, die die für E-Mail genutzten Protokolle verwenden. Darüber hinaus gibt es weitere freie Messenger-Systeme wie Goldbug, Mattermost u. v. a. mehr.
XMPP (Jabber) ist ein föderiertes, dezentrales System für Instant Messaging, das unabhängig von einem zentralen Diensteanbieter genutzt werden kann. Das erweiterbare Basisprotokoll ist von der Internet Engineering Task Force (IETF) standardisiert und definiert, wie Clients und Server sowie Server untereinander Datenpakete austauschen können. Welche Informationen in diesen Paketen konkret übertragen werden, ist über Erweiterungen definiert. Diese Erweiterungen, XEPs (XMPP Extension Protocol) genannt, werden über die XMPP Standards Foundation (XSF) - das Standardisierungsgremium - standardisiert. Es existieren Erweiterungen für alle möglichen Einsatzzwecke, wie z. B. OMEMO für die Ende-zu-Ende-Verschlüsselung.[51] Um auf Basis von XMPP chatten zu können, muss ein Nutzerkonto bei einem beliebigen Server vorhanden oder angelegt sein. Ähnlich wie bei E-Mail werden Nutzerinnen und

[51] Vgl. *Golem,* OMEMO: Endlich auf vielen Geräten verschlüsselt chatten, 12. Oktober 2016, abrufbar unter: https://www.golem.de/news/omemo-endlich-auf-vielen-geraeten-verschluesselt-chatten-1610-123621.html.

Nutzer über benutzername@server identifiziert. Sie können ihren eigenen Server betreiben. Hierfür sind jedoch ein gewisses technisches Verständnis und Engagement erforderlich. Deshalb gibt es sehr viele verschiedene öffentliche Anbieterinnen und Anbieter, auf deren Server dann die Verwaltung von Konten, Adressbüchern und Chatverläufen der Nutzerinnen und Nutzer für ggfs. mehrere Geräte erfolgen kann. 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.[52] 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 definiert. Anders als XMPP besteht Matrix nicht aus unterschiedlichen oder erweiterbaren Modulen. Bei neuen oder veränderten Anforderungen wird das Protokoll als Einheit geändert oder ergänzt. Auch über Matrix können die Nutzerinnen und Nutzer, unabhängig von ihren genutzten Clients, in Echtzeit miteinander kommunizieren. In der Philosophie von Matrix ist grundsätzlich jeder Chat ein Raum. Der Fokus liegt auf der Ausfallsicherheit von Chaträumen. Chaträume werden unter allen beteiligten Servern der Teilnehmenden synchronisiert (auf jedem beteiligten Server sind alle Nachrichten des Raumes gespeichert). Das bedeutet bei einem eventuellen Ausfall eines Servers, dass alle Teilnehmenden von anderen Servern den Chatraum ganz normal weiternutzen können.[53]

Für Matrix wurde der wohl bekannteste Client Element in die Untersuchung einbezogen. Matrix wird nach Angaben von Element an vielen deutschen Universitäten und der BWI[54] - dem IT-Systemhaus der

---

52 Vgl. für eine ausführliche Darstellung *Initiative Freie Messenger*, abrufbar unter: https://www.freie-messenger.de/xmpp/.

53 Vgl. *Initiative Freie Messenger,* Matrix, abrufbar unter: https://www.freie-messenger.de/matrix/.

54 Siehe *BWI*, Open-Source: „Matrix“ ist einheitlicher Messenger-Standard für die Bundeswehr, abrufbar unter: https://www.bwi.de/news-blog/news/artikel/open-source-matrix-ist-einheitlicher-messenger-standard-fuer-die-bundeswehr 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.

Bundeswehr - eingesetzt. Gematik[55] hat das Matrix-Protokoll als Standard für das Messaging im Gesundheitswesen ausgewählt.[56]

E-Mail als Messaging-System zeichnet sich durch eine große Erreichbarkeit aus. Jede Nutzerin und jeder Nutzer kann mit beliebiger E-Mail-Adresse kommunizieren, ohne dass die Empfängerin oder 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 IMAP[57] und SMTP[58]. [59] Das System E-Mail ist in der Sektoruntersuchung durch den Client „Delta Chat“ vertreten.

Messenger- und Video-Dienste bieten **verschiedene 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 Verbraucherinnen und 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 Nutzerinnen und 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 Funktionen hinzugekommen. Viele Dienste haben den Versand von Textnachrichten und Dateien einige Jahre früher angeboten als Telefonie und

---

55 Gematik trägt die Gesamtverantwortung für die Telematikinfrastruktur (TI), die zentrale Plattform für digitale Anwendungen im deutschen Gesundheitswesen. Mit der Definition und Durchsetzung verbindlicher Standards für Dienste, Komponenten und Anwendungen in der TI will Gematik gewährleisten, dass diese zentrale Infrastruktur sicher, leistungsfähig und nutzerfreundlich ist und bleibt, vgl. https://www.gematik.de/.

56 Siehe *Gematik*, TI-Messenger, abrufbar unter: https://www.gematik.de/anwendungen/ti-messenger.

57 Das Internet Message Access Protocol (IMAP) ist ein Netzwerkprotokoll, das ein Netzwerkdateisystem für E-Mails bereitstellt, vgl. *Wikipedia,* abrufbar unter: https://de.wikipedia.org/wiki/Internet_Message_Access_Protocol.

58 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*, abrufbar unter: https://de.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol.

59 Vgl. für detaillierte Ausführungen *Initiative Freie Messenger*, abrufbar unter: https://www.freie-messenger.de/matrix/.

Videotelefonie. In einzelnen Fällen ist auch erkennbar, dass der Austausch in einer Gruppe erst später möglich war als die Kommunikation mit einer einzigen Gesprächspartnerin oder 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 nicht immer betrieben. Einige Befragte haben auch darauf hingewiesen, dass ihnen nicht bekannt ist, ob die Nutzerinnen und Nutzer den Dienst z. B. als Telefonkonferenz oder Videokonferenz nutzen, da Letzteres sich nur durch Einschaltung der Kamera unterscheide.

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, WeChat) 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.[60]

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 Geschäftskundinnen und 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 Nutzerinnen und Nutzer grundsätzlich ablehnen oder weil diese Informationen ausschließlich dem jeweiligen Diensteanbieter bzw. der Serverbetreiberin oder dem Serverbetreiber bekannt sind.

---

[60] In der verbraucherrechtlichen Sektoruntersuchung nach § 32 e GWB ist eine Marktabgrenzung nicht erforderlich. Die Ausführungen dieses Abschnitts sind somit nicht geeignet, eine solche zu beschreiben, sondern dienen der Strukturierung der Branche.

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 genutzt werden kann. Über Smartphone/Tablet können ebenfalls 38 Dienste verwendet werden. Über einen Webbrowser bieten nach eigenen Angaben nur 16 der befragten Dienste Zugang an. 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. Verbraucherinnen und 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 konnten 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 hauptsächlich 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 Diensten 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 Abbildung 1 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 Meeting
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

Abbildung 1: Nutzungszahlen

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. Die Befragung ist nicht mit einer kartellrechtlichen Marktabgrenzung zu verwechseln, die für die verbraucherrechtliche Sektoruntersuchung nicht notwendig ist. Die Fragen waren vielmehr darauf ausgerichtet, grundlegende wettbewerbliche Zusammenhänge zu beleuchten, die für jegliche verbraucherrechtliche Handlungsempfehlung eine Rolle spielen könnten.

Zu der Frage, aus welchen **Gründen** sich die Nutzerinnen und 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 Nutzerinnen und Nutzer. Nur knapp ein Drittel der Messenger- und Video-Dienste hat angegeben, dass sie ihre Nutzerinnen und 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 Netzwerkeffekte entstehen. Nach Angaben einiger Befragter haben die Nutzerinnen und Nutzer ihren Dienst darüber hinaus auch wegen der einfachen Handhabung, dem Verzicht auf Werbung, der Integration mit anderen Systemen/Geräten, der Infrastruktur in Europa, der Gestaltung als Open Source-Dienst, der Nutzung eines internationalen Standards (XMPP) oder aufgrund der guten Qualität des Dienstes gewählt. Ein Dienst erläuterte, seine Nutzerinnen und Nutzer schätzten besonders die Möglichkeit, Interoperabilität über Bridges herzustellen.

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-Konferenzanbietern 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 (Nutzerinnen und Nutzer/Werbekundinnen und -kunden) 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 Nutzerinnen und 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 Marktteilnehmenden 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, Datensicherheit und Qualität. Ausländische Dienste planen danach teilweise, sich stärker auf das lokale Angebot auszurichten. Kleine freie Messenger-Clients haben häufig keine wesentliche Ausweitung ihres Dienstes geplant. Sie haben teilweise angegeben, kein wirtschaftliches Interesse zu verfolgen. Auch die Verbesserung der Interoperabilität mit anderen Diensten wurde von Diensten als Ziel benannt.

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 Nutzerinnen und Nutzer parallel mehrere Dienste nutzen (sog. Multi-Homing) und Netzwerkeffekte verhindert würden, wenn Nutzerinnen und Nutzer ohne Registrierung andere Dienste (z. B. auf Einladung) nutzen können. Schließlich wurden von einem Dienst der intensive Wettbewerb und die hohe Wettbewerbsdynamik in dieser Branche betont.

Ergänzend zu diesen Einschätzungen der Branchenteilnehmenden bzgl. der Wettbewerbssituation bei Messenger- und Video-Diensten sei an dieser Stelle auf die Verbraucherbefragung der

Bundesnetzagentur[61] verwiesen, mit der u. a. erfasst wurde, welcher Anteil der Befragten jeweils bestimmte Dienste nutzt:

Abbildung 2: Nutzungsanteile Messenger- und Video-Dienste[62]

[61] *Bundesnetzagentur* (2022), Nutzung von Online-Kommunikationsdiensten in Deutschland, Ergebnisse der Verbraucherbefragung 2021, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/OnlineKom/befragung_kurz21.pdf?__blob=publicationFile&v=3.

[62] Quelle: Eigene Darstellung auf Basis von Bundesnetzagentur (2022), Nutzung von Online-Kommunikationsdiensten in Deutschland, Ergebnisse der Verbraucherbefragung 2021, S. 13.

Abbildung 2 verdeutlicht, dass sich die Präferenzen der Verbraucherinnen und Verbraucher bei der Auswahl ihrer Messenger- und Video-Dienste im Vergleich zur vorausgegangenen Untersuchung kaum verändert haben. WhatsApp liegt hier im 93 Prozent weit vorne, gefolgt von Facebook Messenger mit 39 Prozent. Unter den Diensten, die von den Verbraucherinnen und Verbrauchern vor allem zum Messaging eingesetzt werden, liegen Telegram und Signal mit 16 bzw. 13 Prozent Nutzungsanteil weit hinter WhatsApp. Die führenden Video-Dienste liegen deutlich abgeschlagen hinter den Diensten aus der Meta-Gruppe mit Nutzungsanteilen unter 15 Prozent. Andere Messenger-Dienste folgen weit abgeschlagen mit einstelligen Nutzungsanteilen. Es scheint, als würde der von den Diensten beschriebene lebhafte Wettbewerb in der Branche die Position des führenden Dienstes bisher nicht berühren. Eine genauere Analyse der Wettbewerbssituation würde eine kartellrechtliche Marktabgrenzung voraussetzen, die für die verbraucherrechtliche Sektoruntersuchung - wie eingangs bereits erwähnt - nicht notwendig ist.

D. Aspekte des Datenschutzes bei Messenger- und Video-Diensten

Das Bundeskartellamt hat die Messenger- und Video-Dienste für diese Sektoruntersuchung im Sommer 2021 direkt befragt. Den Themen Datensicherheit und Datenverarbeitung nach der EU-Datenschutzgrundverordnung (DSGVO)[63] hat es in seinem Fragebogen jeweils einen eigenen Abschnitt gewidmet. Beide Themen sind nicht nur für die Verbraucherinnen und Verbraucher wichtig, um selbständig einen sicheren Dienst auswählen zu können. Sie spielen auch für die rechtliche Analyse nach der DSGVO und dem UWG eine Rolle.

I. Datensicherheit

Verbraucherinnen und 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.[64] Die in diesen Untersuchungen präsentierten Ergebnisse sind größtenteils durch die Auswertung von Publikationen oder der Webseiten der einbezogenen Messenger- und Video-Dienste entstanden. Das Bundeskartellamt hat die Branche zu ihren technischen Grundlagen sowie ihren Einschätzungen zu verschiedenen Datenschutzthemen direkt befragt.

1. Netzwerkstruktur

a) Hintergrund

Welchen Einfluss der jeweilige Messenger- und Video-Dienst als Dienstbetreiber hat, bestimmt nachhaltig die Netzwerkstruktur, d. h. ob ein Messenger- und Video-Dienst zentral über einen bestimmten Server (siehe dazu Abbildung 3) oder föderal über ein Netzwerk unabhängiger Server organisiert ist (siehe Abbildung 4). Bei **zentraler Organisation** gibt es einen Server, bei dem sich jede Nutzerin und jeder Nutzer anmelden muss, und einen Client (App, Software), der vom Dienstbetreiber

---

63 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 vom 04.05.2016, S. 1 - DSGVO.

64 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; *Mobilsicher*, Verschiedener Messenger-Apps kurz vorgestellt, abrufbar unter: https://mobilsicher.de/suche/messenger; *Kuketz*, Messenger-Matrix, abrufbar unter: https://www.kuketz-blog.de/messenger-matrix-uebersicht-vergleich-der-aktuellen-messenger/; *Initiative Freie Messenger*, abrufbar unter: https://www.freie-messenger.de/systemvergleich.

bereitgestellt wird. Alle wesentlichen Entscheidungen liegen damit in der Hand des Dienstbetreibers. Als Vorteil eines zentralisierten Messenger- und Video-Dienstes wird z. B. die höhere Flexibilität angeführt, die in einem sich schnell ändernden Ökosystem notwendig sei. Der zentrale Dienstbetreibende könne schneller auf Veränderungen reagieren und z. B. mögliche Sicherheitslücken durch zentrale Updates für alle Nutzerinnen und Nutzer zum selben Zeitpunkt beheben.[65] Hinzu kämen Qualitätsvorteile. Alle Nutzerinnen und Nutzer könnten wegen des zentralen Servers stets die gleiche Version des Clients nutzen, wodurch alle Nutzerinnen und Nutzer von den aktualisierten Funktionen profitieren könnten.

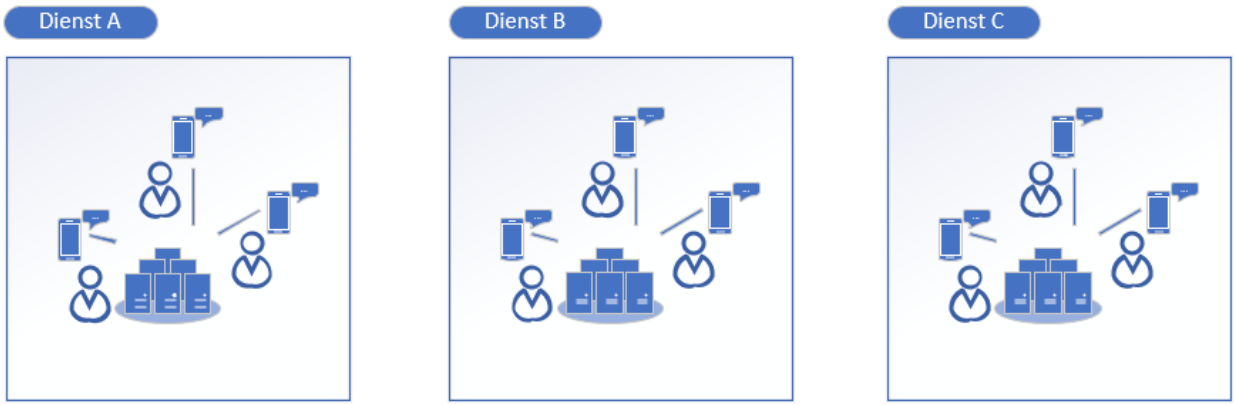


Abbildung 3: Zentralisierte Messaging-Systeme[66]

Bei dezentraler Server-Organisation, der sog. **Föderation,** werden die Server verschiedener Serverbetreiber miteinander verknüpft. Es wird ein Netzwerk unabhängiger Server gebildet, ähnlich wie es bei E-Mail der Fall ist. Vorteile sind hier, dass Nutzerinnen und Nutzer miteinander kommunizieren können, ohne von einem zentralen Dienstanbieter abhängig zu sein. Ferner liegen Meta-Daten bei föderierten Systemen nicht an einer zentralen Stelle vor, sondern nur bei den beteiligten Serverbetreibenden, die die Nutzerinnen und Nutzer - wenn sie möchten - selbst auswählen können. Föderation ermöglichen z. B. die beiden freien Protokolle XMPP und Matrix.[67]

---

65 Siehe zum Beispiel auch *Bundesnetzagentur* (2021): Interoperabilität zwischen Messengerdiensten – Überblick der Potentiale und Herausforderungen, 9. Dezember 2021, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/OnlineKom/diskussionspapier_IOP.pdf?__blob=publicationFile&v=3.

66 In Anlehnung an *Bundesnetzagentur* (2021): Interoperabilität zwischen Messengerdiensten – Überblick der Potentiale und Herausforderungen, 9. Dezember 2021, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/OnlineKom/diskussionspapier_IOP.pdf?__blob=publicationFile&v=3.

67 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/.

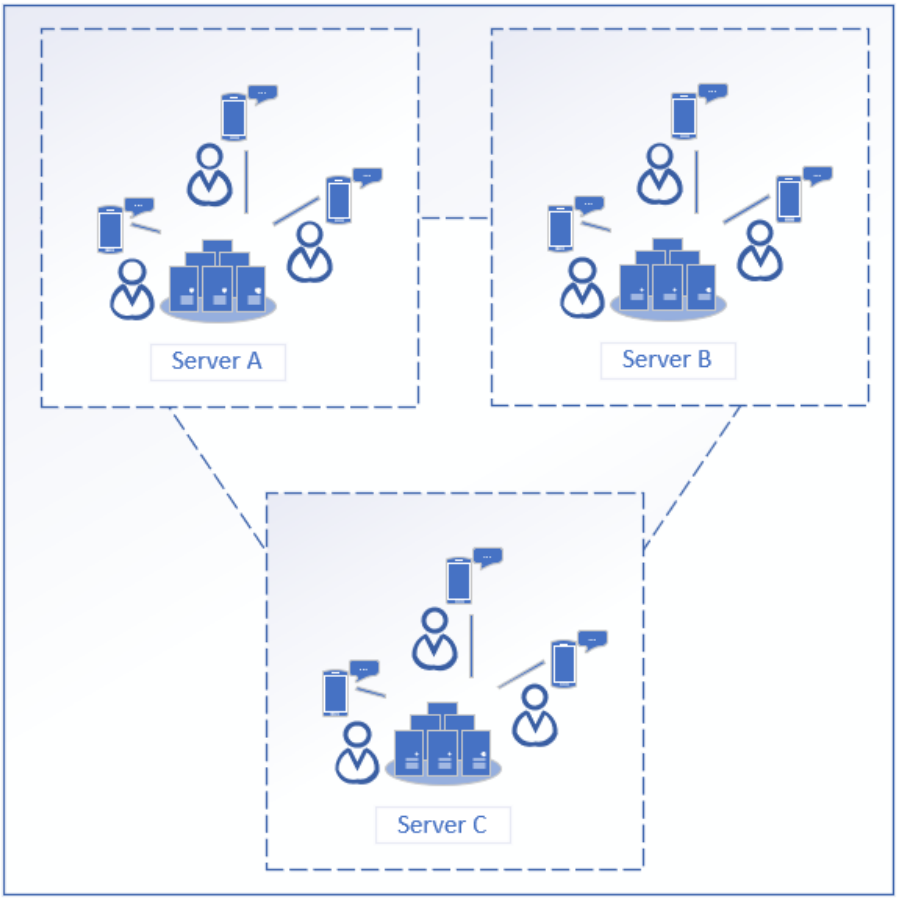


Abbildung 4: Föderiertes Messaging-System[68]

b) Ermittlungsergebnisse

Die Mehrheit der Messenger- und Video-Dienste hat angegeben, dass die zugrunde liegende Netzwerkstruktur zentral verwaltet wird, meist durch das eigene Unternehmen.
Eine föderale Serverstruktur nutzen mehr als 40 Prozent der Dienste. Hierzu zählen z. B. BigBlueButton, Blabber.im, Conversations, Delta Chat, Discord (nur für Video/VOIP), Element, Fastviewer, iMessage / FaceTime, Jabber, Monal, Nextcloud Talk, Quicksy, Rocket.Chat, Trillian, Yaxim, Viber.
Zwei freie Messenger Clients weisen darauf hin, dass das System (XMPP) in der Regel dezentral und föderiert betrieben werde – allerdings oft auch z. B. firmenintern als Insellösung (zentral) zum Einsatz

[68] In Anlehnung an *Bundesnetzagentur* (2021): Interoperabilität zwischen Messengerdiensten – Überblick der Potentiale und Herausforderungen, 9. Dezember 2021, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/OnlineKom/diskussionspapier_IOP.pdf?__blob=publicationFile&v=3

komme. Darüber hinaus sei auch eine serverlose Kommunikation mit entsprechenden Einschränkungen möglich. Welche dieser Strukturen genutzt werde, liege in der Hand der Endnutzerinnen und Endnutzer. Von Seiten mehrerer XMPP-Clients wird ebenfalls darauf hingewiesen, dass einige geschlossene Messaging-Systeme auf Basis von XMPP entstanden sind. Dies betreffe sowohl den Facebook Messenger als auch WhatsApp, Google Talk und den KIK-Messenger. Das bedeute, dass die beteiligten Firmen das standardisierte und öffentliche Protokoll XMPP (und „ejabberd“ als eine der frei verfügbaren Open Source Server-Implementierungen von XMPP) verwendet hätten, um auf deren Basis durch proprietäre (firmeninterne) Erweiterungen, die sie nicht in den öffentlichen Standardisierungsprozess haben zurückfließen lassen, ihr Produkt zu kreieren.

2. Zusammenarbeit mit Standardisierungsorganisationen

a) Hintergrund

Entsprechend der Bedeutung technischer Funktionalitäten verfügt auch die Branche der Messenger- und Video-Dienste über eine gewisse technische Selbstorganisation durch international anerkannte Standardisierungsorganisationen. Grundsätzlich verabschieden Standardisierungsorganisationen interne Regelwerke zum Umgang mit geschützten Technologien (siehe hierzu nochmals C.III).
Wenn Messenger- und Video-Dienste Techniken einsetzen, die von der Branche in Standardisierungsgremien vereinheitlicht und dokumentiert wurden, sind die Vorteile für die Nutzerinnen und Nutzer, dass ein branchenweit anerkannter technischer Stand umgesetzt wird, der sich am Markt durchgesetzt hat und der von den verschiedensten Anwenderinnen und Anwendern begutachtet und geprüft wurde.

b) Ermittlungsergebnisse

Knapp die Hälfte der Dienste hat eine Zusammenarbeit mit Standardisierungsorganisationen bestätigt. Dazu zählen die Dienste, die ein standardisiertes Protokoll verwenden, wie z. B. die XMPP-Clients, die mit der XSF zusammenarbeiten, die Matrix.org Foundation sowie außerdem Delta Chat, Google Meet, Meet.jit.si, Loopup, Slack, Swyx, Threema, Tixeo, Webex, Zoom.
Unter den Standardisierungsorganisationen wird die **Internet Engineering Task Force (IETF)** sehr häufig genannt. Ihr Schwerpunkt liegt - wie in Kapitel C.III beschrieben - auf der Standardisierung der im Internet eingesetzten Kommunikationsprotokolle. Bei der IETF handelt es sich um eine offene, internationale Freiwilligenvereinigung von Netzwerktechnikern und - technikerinnen, Herstellerinnen und Herstellern, Netzbetreiberinnen und -betreibern, Forschenden sowie Anwenderinnen und Anwendern, die sich mit der technischen Weiterentwicklung des Internets befasst, um dessen Funktionsweise zu verbessern.

Daneben existieren weitere Standardisierungsgremien, die für die Dienste, oder auch bestimmte Gruppen der Dienste, besonders wichtig sind. Von vielen freien Messenger-Clients wurde die Organisation **XMPP Standards Foundation (XSF)** genannt. Die XSF ist eine gemeinnützige Stiftung, die das XMPP-Protokoll spezifiziert und weiterentwickelt. Der offene Standard Matrix wird von der Stiftung „**The Matrix.org Foundation**“ geführt und verwaltet.
Weitere Nennungen waren die ISO, NIST, ANSSI, W3C, die OpenPGP Working Group oder die Autocrypt.org-Standardisierungs-Community:
Die **Internationale Organisation für Normung (ISO)** ist die internationale Vereinigung von Normungsorganisationen. Sie erarbeitet internationale Normen in allen Bereichen mit Ausnahme der Elektrik und der Elektronik, für die die Internationale elektrotechnische Kommission (IEC) zuständig ist, und mit Ausnahme der Telekommunikation, mit der sich die Internationale Fernmeldeunion (ITU) beschäftigt.
Entsprechend der Internationalität des Geschäfts nennen die Dienste auch ausländische Behörden, die ähnliche Aufgaben wahrnehmen, wie es das BSI in Deutschland tut. Das **National Institute of Standards and Technology (NIST)** ist eine Bundesbehörde im Geschäftsbereich des Handelsministeriums der Vereinigten Staaten mit Sitz in Gaithersburg (Maryland). Das Institut veröffentlicht die Federal Information Processing Standards (FIPS, Standards für die Informationsverarbeitung), die für US-Behörden gelten und ist für Standardisierungsprozesse zuständig. Im Bereich der Kryptographie sind hier beispielsweise die Verschlüsselungsalgorithmen DES und AES zu nennen. Die **Agence nationale de la sécurité des systèmes d’information (ANSSI)** ist auf französischer Seite als Behörde für die Informationssicherheit zuständig. Sie ist dem Generalsekretariat für Verteidigung und nationale Sicherheit (Secrétariat général de la défense et de la sécurité nationale, SGDSN) angegliedert, welches direkt dem französischen Premierminister untersteht.
Das **World Wide Web Consortium (W3C)** ist eine Mitgliedsorganisation zur Standardisierung der Techniken im World Wide Web. 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.
Die **OpenPGP Working Group** ist eine Arbeitsgruppe bei der IETF, die an der Standardisierung des am meisten genutzten Verschlüsselungsstandards für E-Mails „OpenPGP“ arbeitete. **Autocrypt.org** ist eine Standardisierungsrichtlinie zur Umsetzung von Ende-zu-Ende-Verschlüsselung von E-Mails.

3. Standards / Protokolle

a) Hintergrund

Kommunikationsprotokolle definieren die Regeln für die Datenübertragung zwischen den Endpunkten der Kommunikation. Sie können als die Sprache eines Messaging- und Video-Systems bezeichnet werden oder – technischer formuliert – als Regelsatz, nach welchem die Datenübertragung zwischen zwei oder mehreren Endpunkten der Kommunikation abläuft. Ein Kommunikationsprotokoll legt somit Vorgaben für die Übertragung von Daten zwischen Kommunikationspartnern fest. Die **Programmierschnittstelle** oder API (Application Programming Interface) wird von der Software zur Anknüpfung an das jeweilige System bereitgestellt.[69] Das Protokoll regelt auch die **Verschlüsselung**, die aufgrund der Komplexität des Themas und der besonderen Bedeutung auch für Interoperabilität und rechtliche Fragen gesondert im Anschluss dargestellt wird (siehe dazu D.I.4.).

Im Rahmen der Befragung sollten die Messenger- und Video-Dienste dem Bundeskartellamt mitteilen, ob sie eigene, sog. **proprietäre** Protokolle verwenden. Proprietär werden Soft- und Hardware oder Dateiformate, Protokolle oder Programmierschnittstellen (APIs) genannt, die auf herstellerspezifischen Entwicklungen basieren und die wegen rechtlicher Regelungen (Patente, Lizenzbestimmungen) eingeschränkt verwendet werden können oder deren Quellcode nicht verfügbar ist. Hier sei auf den Prozess von Innovation, Diffusion und Standardisierung verwiesen. Innovation wird in diesem Fall von der Wirtschaft getrieben. Die Innovationen schlagen sich in den Details der Protokolle nieder und diese dann in der Entwicklung der notwendigen Programme (Source Code). Diese Entwicklungen sind erst einmal geistiges Eigentum der Dienste. Die Protokollspezifikation ist die wichtige Ebene, da sie das Ziel hat, die Interoperabilität unterschiedlicher Implementierungen sicherzustellen. Hieraus entwickeln sich idealerweise dann die Standards, in die nur diejenigen Funktionen Eingang finden, die sich im Markt durchgesetzt haben.

Ob proprietär – wie im allgemeinen Sprachgebrauch üblich – hier auch ein bestehendes Eigentumsverhältnis anzeigt, ist nicht eindeutig geklärt. Im Gegensatz dazu können **Open Source-**

[69] Siehe zur API Kapitel F.I.3.

Produkte von jedem nach Belieben studiert, benutzt, verändert und kopiert werden.[70] Ihr Quellcode liegt offen.[71]

Proprietäre Protokolle können somit nicht oder nicht vollständig von Dritten auf ihre jeweilige Funktionsweise überprüft werden. Wenn der Quellcode firmeneigener Protokolle offengelegt wird, können zumindest fachkundige Nutzerinnen und Nutzer oder Prüfinstitutionen deren Gestaltung nachvollziehen und z. B. feststellen, in welcher Form ein Messenger- oder Video-Dienst Inhalte Ende-zu-Ende-verschlüsselt. So wurde in der Vergangenheit bei einem Dienst bekannt, dass die Ende-zu-Ende-Verschlüsselung beworben wurde, obwohl tatsächlich „nur" transportverschlüsselt wurde.[72] Nach Einschätzung des BSI lassen sich in Open Source-Produkten solche Aussagen vergleichsweise einfach verifizieren. Das BSI weist hier allerdings auch auf den hohen Anspruch solcher Vorhaben hin, da moderne Messenger- und Video-Dienste eine „enorme Menge an Source Code"[73] aufweisen.

Wenn der Quellcode nicht offen liegt oder Nutzerinnen und Nutzer ihren Dienst nicht selber überprüfen können oder möchten, können **Zertifizierungen** oder **Sicherheitsaudits** hilfreich sein, um die Datensicherheit einzuschätzen und das Vertrauen in diese zu erhöhen. Das BSI verweist in diesem Zusammenhang auf unabhängig durchgeführte Sicherheitsaudits, auf eine Zertifizierung des Anbieters nach ISO 27001 oder die Veröffentlichung der kryptographischen Designkriterien.[74]

b) Ermittlungsergebnisse

Das Bundeskartellamt hat die Messenger- und Video- Dienste um Auskunft gebeten, welche Protokolle/Standards sie beim Austausch verwenden, inwieweit die Quellcodes öffentlich einsehbar sind

---

70 Siehe *IT-Business*, abrufbar unter: https://www.it-business.de/was-ist-proprietaer-a-911656/, Stand: 19. Januar 2022. So z. B. auch erklärt bei *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Open_Source.

71 Vgl. *Bundeszentrale für politische Bildung*: Dossier Open Source, abrufbar unter: https://www.bpb.de/gesellschaft/digitales/opensource/, *Red Hat*: Was ist Open Source, abrufbar unter: https://www.redhat.com/de/topics/open-source/what-is-open-source#, *Chip*: Open Source – was ist das genau?, abrufbar unter: https://praxistipps.chip.de/open-source-was-ist-das-genau_12877.

72 Siehe hierzu auch Kapitel D.III.4.d.bb.

73 *BSI*, Moderne Messenger – heute verschlüsselt, morgen interoperabel?, November 2021, S. 10, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

74 *BSI*, Moderne Messenger – heute verschlüsselt, morgen interoperabel?, November 2021, S. 10, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

oder ob es sich um proprietäre und firmeneigene Protokolle handelt, und ob die Protokolle regelmäßig überprüft werden.
Viele der Befragten nannten als verwendete Protokolle bzw. Standards die Transportverschlüsselung (TLS)[75], den Web Real-Time Communication-Standard (WebRTC)[76], der für die Videokommunikation verwendet wird, das Extensible Messaging and Presence Protocol (XMPP)[77], das Double Ratchet-Protokoll, das Matrix-Protokoll, welches auf Double Ratchet basiert, sowie AES (siehe für beide Kapitel D.I.4.a.) und SIP[78].

aa) Einsehbarkeit der Quellcodes / Open Source

Etwas mehr als 40 Prozent der befragten Dienste haben angegeben, dass der Quellcode von Server und Client einsehbar ist (All-in-One Messenger, BigBlueButton, Blabber.im, Conversations, Delta.Chat, Dino, Element, Gajim, Google Meet, Jabber, Meet.jit.si, Monal, Nextcloud Talk, Quicksy, Rocket.Chat, Swyx, Threema, Univado, Yaxim). Dies ist vor allem bei den freien Messenger Clients und natürlich Open Source-Diensten der Fall. Darunter fielen auch Dienste, welche explizit mit Datenschutz werben.
Bei den **freien Messenger-Clients** ist bei der Einordnung in die genannten Kategorien zwischen „Client“ und dem „System“ (insb. dem Protokoll) zu unterscheiden. Das Protokoll XMPP, welches einige der befragten freien Messenger-Clients verwenden, sei Open Source, d. h. der Quellcode liege offen vor und könne von jedem eingesehen und verwendet werden. Das Protokoll sei durch die XSF standardisiert worden. Es existierten aber sowohl quelloffene als auch proprietäre, kommerzielle Server und Clients. So weisen die XMPP-Clients Blabber.im und Yaxim darauf hin, dass die von ihnen verwendeten Server ebenfalls quelloffen sind. Andere Clients erklären, dass quelloffene Server von den Nutzerinnen und Nutzern gewählt werden können (Dino, Gajim). Auch der Client Delta Chat, der die für E-Mail

---

75 TLS (Transport Layer Security) ist ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet; auch bekannt unter der Vorgängerbezeichnung Secure Sockets Layer (siehe SSL-Zertifikat).

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

77 XMPP (Extensible Messaging and Presence Protocol) ist ein offener Standard eines Kommunikationsprotokolles, welches von der Internet Engineering Task Force (IETF) als RFC 6120, 6121 und 6122 veröffentlicht wurde. XMPP basiert auf dem XML-Standard und ermöglicht den Austausch von Daten, vergl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Extensible_Messaging_and_Presence_Protocol.

78 SIP steht für Session Initiation Protocol, ein Protokoll, um über das Internet zu telefonieren, für weitere Einzelheiten siehe: https://www.computerlexikon.com/begriff-sip.

verwendeten Protokolle nutzt, erläutert, der Quellcode von vielen E-Mail-Servern sei einsehbar, von anderen E-Mail-Servern aber auch nicht. Es sei Nutzerinnen und Nutzern aber ohne Beschränkungen möglich, einen Server mit offenem Quellcode zu wählen oder im Zweifel selbst einen zu betreiben. Die Matrix.org Foundation bestätigt ebenfalls, das Matrix-Protokoll sei Open Source.
Open Source ist allerdings nicht gleichbedeutend damit, dass der Dienst oder alle Funktionen des Dienstes den Verbraucherinnen und Verbrauchern kostenfrei zur Verfügung stehen. Vielmehr gibt es auch **entgeltliche Lösungen**. Nextcloud ist ein Softwarehersteller, dessen Kunden Nextcloud (Talk) auf ihren Servern selbst betreiben. Nextcloud Talk basiert auf WebRTC und ist **Open Source** - Software, die auf der Webseite heruntergeladen werden kann. Da Nextcloud frei verfügbar ist, ebenso die Apps, wird nach Angaben des Dienstes „Nextcloud Enterprise“ verkauft, eine „Software für Unternehmen, welche auch Support enthält“. Die „Plattform“ Rocket.Chat führt aus, der Code von Client und Server sei Open Source genauso wie die Funktionen für Geschäftskunden, auch wenn diese nicht kostenfrei erhältlich sind. Meet.jit.si verwendet die Jitsi Meet - Open Source - Software für Videokonferenzen, die u. a. auf dem WebRTC - Standard basiert. Meet.jit.si wird von dem Unternehmen 8x8 gehostet.
Google Meet erklärt, der Dienst verwende den freien Open Source-Standard WebRTC, der von Google 2011 als Open Source - Projekt veröffentlicht worden sei. Die Spezifikationen wären durch das World Wide Web Consortium (W3C) und die IETF veröffentlicht worden. Auch Threema, ein Dienst, der gegen Entgelt mit zahlreichen Maßnahmen für Datensicherheit und Datenschutz wirbt, legt seinen Quellcode offen.

bb) Proprietät und Open Source

Etwa ein Drittel der Dienste deklarierte ihre genutzten Protokolle als proprietär und als Firmeneigentum. Dazu gehören bekannte Dienste wie Discord, Line, Tixeo, TeamViewer Meeting, Viber, Webex, WhatsApp, Zoom.
Einige Messenger- und Video-Dienste verwenden sowohl **proprietäre als auch Open Source-Protokolle**. Adobe hat das eigene proprietäre Netzwerkprotokoll RTMP[79] entwickelt. Es gebe Open-Source-Implementierungen des Protokolls; die Implementierung in „Adobe Connect“ sei aber „closed source“. GotoMeeting und GotoWebinar nutzen ein Mix proprietärer und standardisierter Protokolle (TLS, HTTP, WSS, RTC, WebRTC), um sichere Kommunikation über Audio- und Videotelefonie sowie Screensharing und Chat bereitzustellen. Auch Skype gibt an, TLS und das Double Ratchet-Protokoll zu verwenden, aber auch ein eigenes Protokoll und TLS zu nutzen. Viber bezieht sich ebenfalls auf das Double Ratchet-

[79] Vgl. *Wikipedia*, abrufbar unter: https://en.wikipedia.org/wiki/Real-Time_Messaging_Protocol.

Protokoll, so wie es in der „Open Whisper[80] Signal - Anwendung genutzt werde. Darauf basiere Vibers Ende-zu-Ende-Verschlüsselung. Vibers Implementierung sei aber von Grund auf neu und verwende nicht Signals Quellcode. Trillian realisiert seinen eigentlichen Dienst über das eigene Protokoll „IMPP“. Eine Dokumentation zu IMPP sei online erhältlich.[81] Föderation funktioniere aber mit XMPP.

cc) Sicherheits-Audits / App-Testings

Gut 40 Prozent der Dienste haben angeführt, dass der Quellcode von Server und Client regelmäßig durch unabhängige Sicherheitsaudits und App-Testings evaluiert wird (z. B. Conferencing & Collaboration, Conversations, Delta Chat, Discord, Franz, Google Meet, Meet.jit.si, Loopup, Nextcloud Talk, Quicksy, Rocket.Chat, TeamViewer Meeting, Tixeo, The Matrix.org Foundation, Threema, Webex, WhatsApp, Zoom.) Dazu gehören auch viele der Dienste, die ihr Protokoll als proprietär bezeichnen. Zwei Dienste erklären, die Quellcodes von Server und Client könnten nur im Wege einer wirksamen Vertraulichkeitserklärung eingesehen werden. Sie würden aber regelmäßig durch unabhängige Sicherheitsaudits und App-Tests evaluiert.
Die Art der Überprüfungen und die entsprechenden Anlässe sind branchenweit sehr unterschiedlich. Häufig werden auch mehrere **Maßnahmen kombiniert**. Diese Maßnahmen können **interner oder externer Art** sein. So wird beispielsweise erläutert, es werde jährlich ein Penetrationstest[82] und ein Sicherheitsaudit durch eine externe Stelle durchgeführt. Ein führender Video-Dienst erklärt, ein Experte evaluiere mindestens einmal im Jahr die Produkte und Dienstleistungen. Ein anderer Dienst gibt an, der Quellcode werde regelmäßig vor Veröffentlichung einer neuen Version evaluiert. Verschiedene Dienste

---

[80] Open Whisper System war ein Softwareunternehmen, welches mit der Entwicklung des Protokolls und der App des Messengers Signal begann. Es ging in die gemeinnützige Signal Technology Foundation ein, durch welche Signal seit 2018 entwickelt wird. Die offiziellen Server werden von einer Tochtergesellschaft der Stiftung, der Signal Messenger LLC, betrieben, vgl. *IT-Times*: Signal - was hinter dem beliebten Instant Messenger steckt, abrufbar unter: https://www.it-times.de/news/signal-was-hinter-dem-beliebten-instant-messenger-steckt-132617/ sowie *Wikipedia*, abrufbar unter: https://en.wikipedia.org/wiki/Open_Whisper_Systems.

[81] Vgl. Trillian, abrufbar unter: https://trillian.im/impp/.

[82] Ein Penetrationstest ist ein gezielter, erlaubter Versuch, in IT-Systeme einzudringen, um die IT-Sicherheit zu verbessern, siehe z. B. *itexperts*, abrufbar unter: https://www.itexperst.at/penetrationstest-definition-abgrenzung-ueberblick .

verweisen auf sog. **Bug Bounty-Programme**[83], z. B. auch auf „HackerOne“[84], um Schwachstellen und Angriffspunkte ihres Systems zu identifizieren. Ein weit verbreiteter Video-Dienst erläutert, die Quellcodes von Server und Client würden regelmäßig durch interne und externe Sicherheitsexperten evaluiert. Die internen Überprüfungen würden ständig laufen und würden automatisiert und händisch durchgeführt über das SAST-Verfahren[85].

Der Name der überprüfenden Institution und ob die entsprechenden Berichte öffentlich sind, wurde nur vereinzelt angegeben. So werden z. B. die französische nationale **Agentur für Sicherheit der Informationssysteme (ANSSI**) und der von ihr zertifizierte CSPN - Standard genannt. Die „Certification de Sécurité de Premier Niveau“ (CSPN) wurde von der französischen ANSSI geschaffen, um eine Alternative zu den Bewertungen der international anerkannten CC-(Common Criteria-) Zertifizierung[86] zu bieten.[87] Tixeo weist darauf hin, dass mit Datum 15. Juni 2022 die **sofortige, gegenseitige**

---

[83] Ein Bug Bounty-Programm ist eine von Unternehmen, Interessenverbänden, Privatpersonen oder Regierungsstellen betriebene Initiative zur Identifizierung, Behebung und Bekanntmachung von Fehlern in Software unter Auslobung von Sach- oder Geldpreisen für die Entdecker, vgl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Bug-Bounty-Programm.

[84] HackerOne ist eine Schwachstellenkoordinierungs- und Bug-Bounty - Plattform, die Unternehmen mit Penetrationstestenden und Cybersicherheitsforschenden verbindet. Es gilt als das größte Cybersicherheitsunternehmen seiner Art. Bis Mai 2020 hatte das Netzwerk von *HackerOne* 100 Millionen Dollar an Prämien gezahlt, siehe *Wikipedia*, abrufbar unter: https://en.wikipedia.org/wiki/HackerOne sowie *HackerOne*, abrufbar unter: https://www.hackerone.com/.

[85] Static Application Security Testing (SAST) ist eine Möglichkeit, den Quellcode eines Programms automatisch zu testen und zu analysieren, ohne ihn auszuführen, um Sicherheitslücken zu Beginn des Softwareentwicklungszyklus zu erkennen. Die Überprüfungen der Sicherheit erfolgen früh in der Entwicklung, siehe *Dev-Insider*, abrufbar unter: https://www.dev-insider.de/was-ist-sast-a-1002595/ sowie *Parasoft*, abrufbar unter: https://de.parasoft.com/blog/what-is-sast-static-application-security-testing/.

[86] Die Common Criteria sind ein internationaler Standard zur Prüfung und Bewertung der Sicherheitseigenschaften von IT-Produkten.

[87] Die Tests werden in begrenzter Zeit und mit begrenztem Arbeitsaufwand durchgeführt (typischerweise zwei Monate, 25 bis 35 Personentage. vgl. *Stormshield*, Qualifizierte Sicherheitslösungen – die Entscheidung für eine vertrauenswürdige Lösung, abrufbar unter: https://www.stormshield.com/de/news/qualifizierte-sicherheitslosungen-die-entscheidung-fur-eine-vertrauenswurdige-losung/.

Anerkennung von IT-Sicherheitszertifikaten zwischen ANSSI und BSI beschlossen wurde.[88] Mit Inkrafttreten des Abkommens werden bereits gültige Zertifikate in beiden Programmen als gleichwertig anerkannt. Zukünftig erteilte Zertifikate werden mit ihrer Veröffentlichung automatisch anerkannt.
Tixeo habe für seine standardmäßige Ende-zu-Ende-Zertifizierung 2021 die erneute CSPN-Zertifizierung der ANSSI erhalten. Damit seit die CSPN Zertifizierung ab sofort auch für Deutschland gültig. Einzelne Dienste verweisen außerdem auf Standards von ISO und dem BSI.
Ein freier Messenger-Client hat bereits zwei externe Sicherheitsaudits im Rahmen von Förderprogrammen durchgeführt, und erwartet zukünftig weitere. Ein anderer freier Client erklärt, dass aufgrund der schlechten Spenden-/Fördersituation kein Geld für unabhängige Sicherheitsaudits vorhanden sei. Damit war der Wunsch nach Fördermitteln oder direkt finanzierten Audits verbunden.

4. Verschlüsselung

a) Hintergrund

Das Thema Verschlüsselung wird inzwischen nicht nur in der Fachöffentlichkeit, sondern auch in der allgemeinen Verbraucheröffentlichkeit intensiv diskutiert. Allerdings unterliegt die Verschlüsselung von Nachrichten bereits einem langen Entwicklungsprozess, der sich fortsetzt.

aa) Verfahren

In den 90er-Jahren wurden, z. B. beim Chat-Programm ICQ, Nachrichten noch unverschlüsselt versendet. Inzwischen wird bei der sog. **Transportverschlüsselung** die Nachricht während ihres Transportweges verschlüsselt (verschlüsselter Kanal), liegt aber außerhalb des Übertragungsweges und an den Endpunkten unverschlüsselt vor, kann also sowohl von Nutzerinnen und Nutzern des Messenger- und Video-Dienstes selbst als auch vom Serverbetreiber eingesehen werden. Die genutzte Technologie ist der Standard „Transport Layer Security“, der bereits seit 1994 existiert.

Anders als bei der Transportverschlüsselung wird bei der **Ende-zu-Ende-Verschlüsselung („E2E-Verschlüsselung“)** die Nachricht verschlüsselt und so über alle Übertragungsstationen hinweg

---

[88] Der ehemalige Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI), Arne Schönbohm, und der Generaldirektor der ANSSI, Guillaume Poupard, haben ein Abkommen zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten unterzeichnet. Das Abkommen bezieht sich auf die Programme CSPN (Certification de Sécurité de Premier Niveau) und BSZ (Beschleunigte Sicherheitszertifizierung. Vgl. BSI, Gegenseitige Anerkennung von IT-Sicherheitszertifikaten zwischen ANSSI und BSI, abrufbar unter: https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/ANSSI_BSI_IT-Sicherheitszertifikate_220615.html.

versendet. Nur die Kommunikationspartner als Endpunkte der Kommunikation können die Daten entschlüsseln.
Die größte Sicherheit bietet aus theoretischer Perspektive unabhängig von Einzelfällen dementsprechend ein kombinierter Einsatz von Transport- und Ende-zu-Ende-Verschlüsselung (siehe Abbildung 5).

Die kombinierte Verwendung beider Verschlüsselungsverfahren kann veranschaulicht werden, wenn der zu verschlüsselnde Inhalt einer Nachricht mit einem Gegenstand verglichen wird, der am Flughafen aufgegeben wird. Bei der Transportverschlüsselung befindet sich das Gepäck während des Flugs geschützt im Rumpf des Flugzeugs. Dort ist es während des Fluges nicht erreichbar. Allerdings kann beim Abflug und bei der Ankunft am Flughafen dann jeder auf den Gegenstand zugreifen. Ein Ende-zu-Ende-verschlüsselter Gegenstand wird beim Abflug in ein sicheres Behältnis gepackt, das sich erst wieder bei der Ankunft vom Besitzer öffnen lässt. Nicht nur während des Flugs, sondern auch bereits vorher und nachher können so keine Dritten auf das Gepäck bzw. den verschlüsselten Inhalt zugreifen.[89]

Zur Verschlüsselung kommen verschiedene kryptographische Verfahren wie die symmetrische oder die asymmetrische Verschlüsselung mit öffentlichen und privaten Schlüsseln zum Einsatz.
Der Unterschied zwischen der symmetrischen Verschlüsselung und der asymmetrischen Verschlüsselung liegt in der Anzahl der Schlüssel. In der **symmetrischen Kryptographie** wird zum Verschlüsseln und Entschlüsseln derselbe Schlüssel verwendet. Hieraus resultiert das Schlüsselaustauschproblem. Damit ein Kommunikationspartner die verschlüsselte Nachricht entschlüsseln kann, muss er den Schlüssel kennen, der auch zum Verschlüsseln verwendet wurde. Hört nun ein Dritter bei Übertragung des Schlüssels den Kommunikationskanal ab, könnte dieser anschließend die gesamte Kommunikation entschlüsseln oder selbst unbemerkt verschlüsselte Nachrichten senden. Deshalb muss die Schlüsselübertragung geheim ablaufen, was oft aufgrund physikalischer Entfernungen ein Problem darstellt.

[89] Vgl. *CYQUEO*: Ende-zu-Ende-Verschlüsselung und Transportverschlüsselung – was ist der Unterschied?, abrufbar unter: https://cyqueo.com/magazin/ende-zu-ende-verschluesselung-und-transportverschluesselung-was-ist-der-unterschied/.

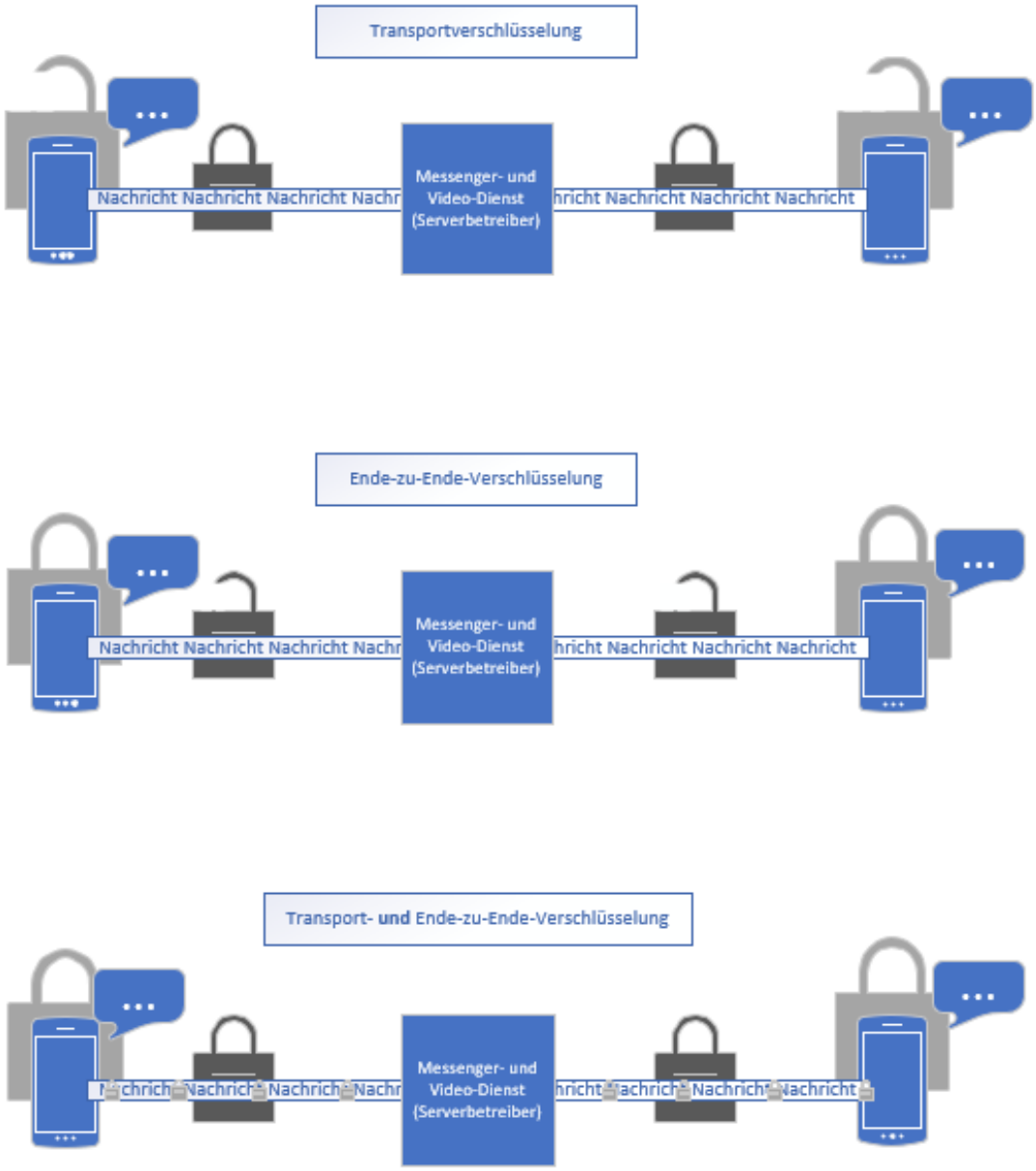


Abbildung 5: Transport- und Ende-zu-Ende-Verschlüsselung separat und kombiniert[90]

Ein bekanntes symmetrisches Verschlüsselungsverfahren ist der **Advanced Encryption Standard (AES)**. Der Standard wird meistens zusammen mit anderen Verschlüsselungsverfahren implementiert, so z. B.

[90] Eigene Darstellung in Anlehnung an *Initiative Freie Messenger*, Verschlüsselungsarten und Kombinationsmöglichkeiten, abrufbar unter: https://www.freie-messenger.de/dateien/begriffe/Verschl%C3%BCsselung.PDF.

auch als Basis der Transportverschlüsselung. Das AES Verschlüsselungsverfahren ist eine Blockchiffre[91], deren Blockgröße von der AES Encryption Variante abhängt. Die Varianten der AES Verschlüsselung, AES-128, AES-192 und AES-256 enthalten in ihrer Bezeichnung die Länge des Schlüssels in Bit. Die sicherste AES Variante ist damit AES-256.[92]

Dahingegen gibt es bei der **asymmetrischen Verschlüsselung** zwei Schlüssel. Mit einem Schlüssel wird die Nachricht verschlüsselt und mit dem anderen Schlüssel wieder entschlüsselt. Hierbei ist der Schlüssel zum Verschlüsseln öffentlich zugänglich und muss nicht geheim übertragen werden, wie dies bei der symmetrischen Verschlüsselung der Fall ist. Der zweite Schlüssel ist der private Schlüssel, welchen die Empfängerin oder der Empfänger zum Entschlüsseln verwendet. Im besten Fall ist nur die Empfängerin oder der Empfänger im Besitz des privaten Schlüssels.[93] Eine bekannte asymmetrische Verschlüsselungsmethode ist das **RSA-Verfahren** (benannt nach den Entwicklern R. Rivest, A. Shamir und L. Adleman). Mit dem RSA-Verfahren können digitale Daten über einen bestimmten Algorithmus umgerechnet und unkenntlich gemacht werden. Für die Entschlüsselung ist der sog. RSA-Schlüssel notwendig. Allerdings wird nicht derselbe Schlüssel zum Ver- und Entschlüsseln verwendet, sondern ein Schlüsselpaar aus einem privaten und dem öffentlichen Schlüssel. Der private Schlüssel muss für eine sichere RSA-Verschlüsselung geheim gehalten werden.[94]

Die Sicherheit der Kommunikation wird schließlich durch weitere kryptographische Prinzipien und Eigenschaften bestimmt. „**Authentizität**“ besagt, dass die Urheberin oder der Urheber von Daten oder die Absenderin 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 Kenntnis des Langzeitschlüssels nicht nachträglich zu entschlüsseln. „**Backward Secrecy**“ („Future Secrecy“, „Post-Compromise Security“) garantiert, dass verschlüsselte

---

91 Vgl. *Chip*, AES Verschlüsselung: Standard einfach erklärt, abrufbar unter: https://praxistipps.chip.de/aes-verschluesselung-standard-einfach-erklaert_121070. Eine Blockchiffre teilt zu verschlüsselnde Daten in festgelegte Blockgrößen auf. Deren Inhalte werden in mehreren Runden untereinander vermischt und verschoben.

92 Siehe z. B. *Studiflix*, abrufbar unter: https://studyflix.de/informatik/aes-verschlusselung-1611 sowie *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Advanced_Encryption_Standard.

93 Siehe *Studiflix*, abrufbar unter: https://studyflix.de/informatik/symmetrische-verschlusselung-1610.

94 Siehe *Datenschutz.org*, abrufbar unter: https://www.datenschutz.org/rsa-verschluesselung/.

Nachrichten geheim bleiben, auch nachdem in der Vergangenheit ein Schlüssel kompromittiert wurde.[95] (Plausible) **Deniability** ermöglicht, das Versenden einer Nachricht im Nachhinein glaubhaft abstreiten zu können.

bb) Umsetzung der Ende-zu-Ende-Verschlüsselung

Die Ende-zu-Ende-Verschlüsselung wird über unterschiedliche Verfahren umgesetzt, je nachdem, welche Kommunikationsform verwendet wird. Für die Verschlüsselung von E-Mails werden z. B. OpenPGP[96] und S/MIME[97] eingesetzt. Für Textnachrichten gilt das sog. **Double Ratchet - Protokoll**[98] (häufig auch Signal - Protokoll genannt) als Stand der Technik. Es setzt auch die im vorausgegangenen Abschnitt beschriebenen kryptographischen Prinzipien um. Wie das BSI ausführt, ist eine der grundlegenden Ideen des Protokolls, mit jeder versendeten Nachricht **stets auch neue (Sitzungs-) Schlüssel** zu versenden und die alten zu löschen. Das Schlüsselmaterial werde „also quasi wie bei einer Ratsche „vorwärts geratscht", sodass es für einen Angreifer nicht möglich ist, von einem späteren zu einem früheren Zeitpunkt zurückzukehren und vorangegangene Nachrichten zu entschlüsseln"[99].
Das Double Ratchet - Protokoll setzt also die **asymmetrische Public-Key-Verschlüsselung** um: 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 Nutzerin B an Nutzer A schreibt, wird ihre Nachricht mit dem öffentlichen Schlüssel von A so verschlüsselt, dass nur A

---

95 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/.

96 OpenPGP ist ein standardisiertes Datenformat für verschlüsselte und digital signierte Daten. Auch wird das Format von Zertifikaten festgelegt, die landläufig auch als „Schlüssel" bezeichnet werden, siehe *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/OpenPGP.

97 Secure / Multipurpose Internet Mail Extensions (S/MIME) ist ein Standard für die Verschlüsselung und das Signieren von MIME-Objekten durch ein asymmetrisches Kryptosystem. Ein typischer Anwendungsfall ist z. B. E-Mail, vgl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/S/MIME.

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

99 *BSI*, Moderne Messenger – heute verschlüsselt, morgen interoperabel?, November 2021, S. 10, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html und die dort angegebene Literatur.

die Nachricht entschlüsseln und somit lesen kann. Das verschlüsselte Dokument wird über den Server zu A gesendet. A erhält das Dokument, welches mit seinem privaten Schlüssel entschlüsselt wird.[100] Der Inhalt der Nachricht kann somit nicht von Dritten, auch nicht von dem Messenger- und Video-Dienst selber gelesen werden (siehe Abbildung 6):

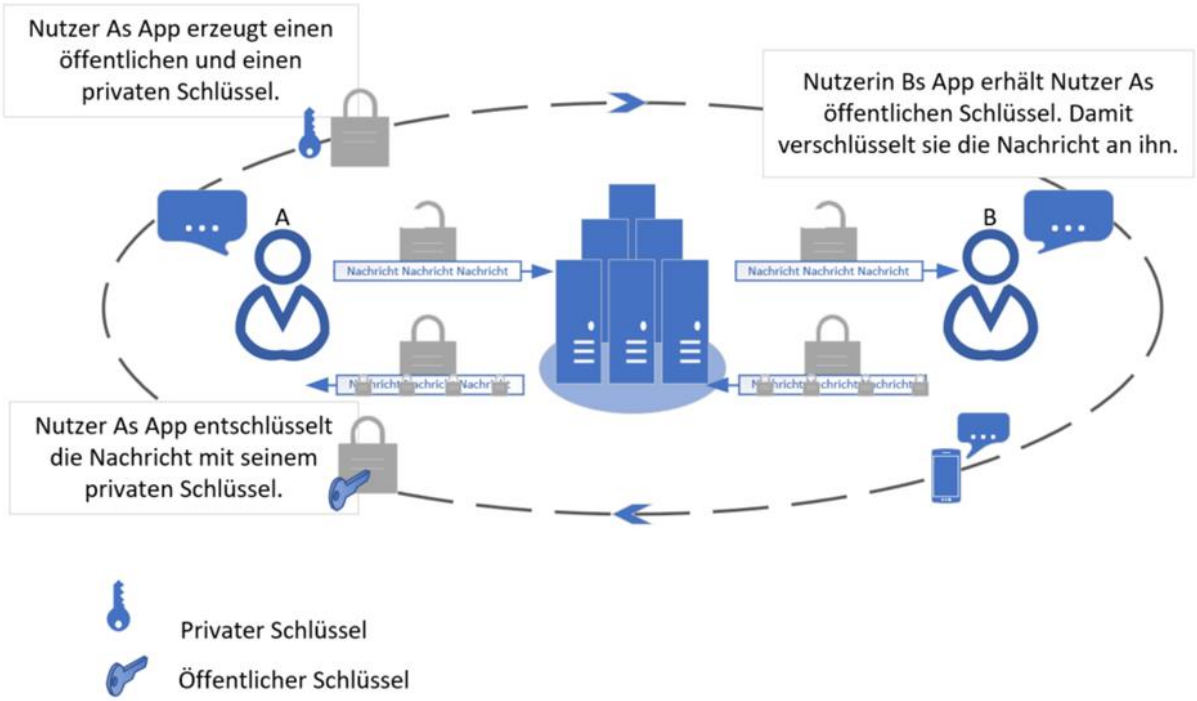


Abbildung 6: Asymmetrische Verschlüsselung[101]

Auch die freien Messaging-Systeme XMPP und Matrix nutzen für die Verschlüsselung eine Implementierung des Double Ratchet-Protokolls, die Forward Secrecy, glaubhafte Abstreitbarkeit als auch die Synchronisation von Nachrichten, wenn die beteiligten Clients offline sind, ermöglicht.
Das entsprechende Verfahren bei XMPP ist **OMEMO (OMEMO Multi-End Message and Object Encryption)**, eine Erweiterung für sichere Multi-Client-Ende-zu-Ende-Verschlüsselung beim bilateralen

[100] Es sei nochmals darauf hingewiesen, dass die privaten Schlüssel fortwährend neu ausgehandelt werden, um die kryptographischen Eigenschaften der Perfect Forward Secrecy, Backward Secrecy, und (Plausible) Deniability zu erreichen.

[101] Eigene Darstellung in Anlehnung an *Mobilsicher*, Das asymmetrische Verschlüsselungsverfahren, abrufbar unter: https://mobilsicher.de/ratgeber/ende-zu-ende-verschluesselung-einfach-erklaert.

Austausch per Textnachrichten („Chat“). Es ist ein offener Standard, der von allen Nutzerinnen und Nutzern frei verwendet und implementiert werden kann.[102]

Bei **Matrix** basiert die Verschlüsselung auf den „Olm- und Libolm – Algorithmen“. Bei Matrix wird für einen Chat unabhängig von der Zahl der Teilnehmenden ein Raum erstellt. Chat - Räume werden zwischen den beteiligten Servern synchronisiert.[103] Eine optionale Ende – zu - Ende-Verschlüsselung von Raum zu Raum realisiert Olm dann mittels einer Double Ratchet-Algorithmus-Implementierung. Dadurch können gespeicherte Konversationsdaten nur von Raum-Teilnehmenden gelesen werden. Ist dies konfiguriert, sind über Matrix transportierte Daten für Matrix-Server nur als verschlüsselter Text sichtbar. Sie können nur von autorisierten Teilnehmerinnen und Teilnehmern des Raumes gelesen werden. Mit „Megolm“ besteht eine Olm-Erweiterung für größere Chaträume. Beide wurden in einem kryptographischen Review des Unternehmens NCC Group geprüft und die Resultate veröffentlicht und vom Matrix Team adressiert.[104] Die Überprüfung wurde vom Open Technology Fund[105] finanziert.[106]

---

[102] Vgl. Conservation, abrufbar unter: https://conversations.im/omemo/, vgl. XMPP, abrufbar unter: https://xmpp.org/extensions/xep-0384.html. Im Internet sind Übersichten einsehbar, die informieren, inwieweit die Verschlüsselungstechnik bereits in die verschiedenen Clients integriert wurde, siehe Omemo-Top https://omemo.top/.

[103] Alle Matrix-Server, die an einer Kommunikation beteiligt sind, speichern den Chat-Verlauf auf unbegrenzte Zeit. Auf dem eigenen Matrix-Server (Homeserver) kann eine Nachricht auf Wunsch gelöscht werden. Der Homeserver wird nach einer erneuten Bestätigung diesen Löschwunsch an alle Matrix-Server weitergeben, die an der Kommunikation beteiligt waren. Ob der Löschwunsch auf den anderen beteiligten Matrix-Servern allerdings umgesetzt wird, ist ungewiss, vgl. *Kuketz* IT Security, Element: Messaging über die Matrix – Messenger Teil 7, abrufbar unter: https://www.kuketz-blog.de/element-messaging-ueber-die-matrix-messenger-teil7/.

[104] Siehe *NCC Group*: Olm cryptographic review, abrufbar unter: https://pentestreports.com/reports/iSEC/NCC_Group_Olm_Cryptogrpahic_Review_2016_11_01.pdf sowie *Matrix.org*, Matrix's 'Olm' End-to-end Encryption security assessment released**,** abrufbar unter: https://matrix.org/blog/2016/11/21/matrixs-olm-end-to-end-encryption-security-assessment-released-and-implemented-cross-platform-on-riot-at-last.

[105] Vgl. https://www.opentech.fund/. Nach eigenen Angaben ist der *Open Technology Fund (OTF)* eine unabhängige gemeinnützige Organisation, die sich der Förderung der globalen Internetfreiheit verschrieben hat. OTF unterstützt Projekte, die repressiver Zensur und Überwachung entgegenwirken um Bürgerinnen und Bürgern weltweit zu ermöglichen, ihre grundlegenden Menschenrechte online auszuüben.

[106] Siehe *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Matrix_(Kommunikationsprotokoll).

Für die **Verschlüsselung bei Audio-/Video-Chats und SIP-Telefonie** wird zumeist das WebRTC-Protokoll, in der Regel im Zusammenspiel mit DTLS-SRTP (Datagram Transport Layer Security – Secure Real-Time Transport Protocol[107]), eingesetzt.[108] **WebRTC** (Web Real Time Communication, deutsch Web-Echtzeitkommunikation) ist ein offener Standard, der eine Sammlung von Kommunikationsprotokollen und Programmierschnittstellen (API) definiert, die Echtzeitkommunikation über Rechner-Rechner-Verbindungen ermöglichen.[109] Auf einen „offenen Standard" können alle Interessierten zugreifen, diesen einsetzen und weiterentwickeln. WebRTC ist vom World Wide Web Consortium (W3C) und der IETF standardisiert worden. Web Real Time Communication basiert auf den Programmiersprachen HTML (Hyper Text Markup Language) und JavaScript. Sie werden vom jeweiligen Webbrowser gelesen und wiedergegeben, egal welche Browser genutzt werden. Dadurch wird eine Kommunikation zwischen mehreren Rechnern im Web ermöglicht und alle Nutzerinnen und Nutzer können den Transfer von Daten wie Videos, Dokumente oder Fotos über den Browser in Anspruch nehmen.[110]

---

[107] Bei dem Secure Real-Time Transport Protocol handelt es sich um die verschlüsselte Variante des Real-Time Transport Protocol (RTP). Das Protokoll wurde im März 2004 von der Internet Engineering Task Force (IETF) vorgestellt. Es eignet sich besonders zur verschlüsselten Übertragung von Kommunikation über das Internet und findet auch bei der IP-Telefonie zunehmend Verwendung. Das Kryptosystem verwendet den Advanced Encryption Standard (AES). Je nach Implementierung kann das Protokoll entweder zur Transportverschlüsselung bei der Sprachdatenübertragung zwischen einem Endgerät auf Kundenseite und dem Server des Kommunikationsanbieters (Provider) oder zur vollständigen Ende-zu-Ende-Verschlüsselung zwischen Kommunikationspartnerinnen und -partnern genutzt werden, siehe *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Secure_Real-Time_Transport_Protocol.

[108] Vgl. *BSI*, Moderne Messenger – heute verschlüsselt, morgen interoperabel?, November 2021, S. 10, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

[109] Vgl. *NordVPN*: Was ist WebRTC und wie deaktiviert man es?, abrufbar unter: https://nordvpn.com/de/blog/was-ist-webrtc/.

[110] Vgl. *NordVPN*: Was ist WebRTC und wie deaktiviert man es?, abrufbar unter: https://nordvpn.com/de/blog/was-ist-webrtc/ sowie *Placetel*: WebRTC – Definition, Funktion und alles Wichtige zur Anwendung, abrufbar unter: https://www.placetel.de/ratgeber/webrtc. Die ausdiovisuelle Übertragung bei der Echtzeitkommunikation via Browser erfolgt über das Secure Real-Time Transport Protocol (SRTP). Es kommt auch bei der IP-Telefonie zur Anwendung. Die verschlüsselte Verbindung wird durch das Verschlüsselungsprotokoll DTLS (Datagram Transport Layer Security) gewährleistet.

cc) Technische Einschränkungen bei der Ende-zu-Ende-Verschlüsselung

Die Verschlüsselung von **Textnachrichten in Gruppen** gilt noch als aufwendig und ist abhängig von der Gruppengröße komplex. Der Austausch in Gruppen wird aktuell verschlüsselt, indem alle Einzelchats aller Gruppenmitglieder untereinander verschlüsselt werden. Wie das BSI in seiner Publikation „Moderne Messenger“ zeigt, wächst der Verschlüsselungsaufwand quadratisch mit der Anzahl der Teilnehmenden. „Der quadratische Aufwand bei der Verschlüsselung von Gruppenchats stellt einen der Hauptgründe dar, der zur Gründung einer IETF-Arbeitsgruppe geführt hat, die sich mit einer Weiterentwicklung des Double-Ratchet-Protokolls beschäftigt hat, dem **Messaging Layer Security-Protokoll (MLS)**, welches insbesondere ein effizientes Gruppenhandling ermöglichen soll“[111]. Eine Entwurfs-Version von MLS wird nach Angaben der IETF bisher z. B. von Webex verwendet. Andere Dienste (u.a. Matrix) planten, MLS einzusetzen. Auch die seit Beginn des Jahres 2023 aktive MIMI-Arbeitsgruppe der IETF berücksichtige MLS in ihren Lösungen zum interoperablen Messaging.[112]

Auch bei **Videokonferenzen und Webinaren** unterliegt die Ende-zu-Ende-Verschlüsselung zur Zeit technischen Einschränkungen. Generell erfordert die Ende-zu-Ende-Verschlüsselung, dass die Teilnehmenden technisch in der Lage sind, die notwendigen Verschlüsselungsfunktionen bereitzustellen und anzuwenden. Alle Teilnehmenden müssen sich auf dem gleichen Sicherheitsniveau bewegen. Im Umkehrschluss kann eine E2E-Verschlüsselung nicht erreicht werden, sobald eine Teilnehmerin oder ein Teilnehmer das geforderte Sicherheitsniveau unterschreiten.

Dieser Fall tritt z. B. dann ein, wenn Teilnehmende einen **WebRTC-Client** einsetzen. WebRTC ist ein direkt im Browser verankertes Protokoll, welches nur zwischen zwei Endpunkten Ende-zu-Ende verschlüsseln kann. Bei mehr als zwei Teilnehmenden einer Videokonferenz sind dies jeweils das Endgerät der Nutzerin oder des Nutzers mit dem Server des Dienstes, was den Anforderungen der Ende-zu-Ende-Verschlüsselung nicht mehr entspricht. Diese Aspekte spiegeln sich in den Ermittlungsergebnissen wider. Das WebRTC-Protokoll wird nach Angaben der befragten

---

[111] *BSI*, Moderne Messenger – heute verschlüsselt, morgen interoperabel?, November 2021, S. 10, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

[112] Vgl. *IETF*, Messaging Layer Security: Secure and Usable End-to-End Encryption, abrufbar unter: https://www.ietf.org/blog/mls-secure-and-usable-end-to-end-encryption/ sowie *golem*, IETF standardisiert Protokoll für sichere Gruppenchats, abrufbar unter: https://www.golem.de/news/messaging-layer-security-ietf-standardisiert-protokoll-fuer-sichere-gruppenchats-2303-173089.html.

Branchenteilnehmenden am häufigste n eingesetzt, um Audio- und Videotelefonie zu verschlüsseln. Die verwendenden Dienste haben auch zum größten Teil angegeben, Videokonferenzen in der Gruppe nicht Ende-zu-Ende verschlüsseln zu können.[113]

Mit bestimmten **Funktionen**, die Nutzerinnen und Nutzer in Videokonferenzen gerne verwenden, kann die Ende-zu-Ende-Verschlüsselung derzeit technisch nicht verbunden werden: Zu diesen Funktionen gehören z. B. die **Einwahl aus dem öffentlichen Telefonnetz** oder die **Aufzeichnung von Meetings** durch den anbietenden Dienst. Dies ist nur möglich, wenn der Dienstbetreiber auf den Datenstrom zugreifen kann, um den Audioanruf einzubinden bzw. die Daten aufzuzeichnen. Auch die **Anbindung bestimmter externer Geräte** (z. B. Raumkonferenzsystem-Geräte, die auf dem SIP-Protokoll basieren) ist unter Ende-zu-Ende-Verschlüsselung nicht möglich, da dazu die verschiedenen Protokolle synchronisiert werden müssten. Führende Dienste haben auf eben solche und weitere Einschränkungen, wie beispielsweise die **Verwendung von „Assistenten“** ausdrücklich hingewiesen.

Große Videokonferenzen für **Webinare mit mehreren Hundert Teilnehmenden** können zur Zeit technisch nicht durch E2E-Verschlüsselung gesichert werden. In diesem Anwendungsfall ist es notwendig, zu prüfen, ob der anbietende Dienst einen Video-Dienst-Standort in Deutschland betreibt und dieser sicherheitstechnisch geprüft wurde (beispielsweise durch ein BSI C5 Testat). Transportverschlüsselung und der sichere Betrieb des Video-Dienstes in Deutschland sollten hierfür das

---

[113] In der Vergangenheit ist eine spezielle Interpretation der Ende-zu-Ende-Verschlüsselung bei einem Videokonferenzanbieter aufgefallen, die nicht der eigentlichen Definition eines Schutzes der Daten, die zwischen den Endgeräten der beteiligten Nutzer versendet werden, entspricht. Als Endpunkt der Kommunikation wurden eben nicht die Nutzerinnen und Nutzer selbst, sondern die beteiligten Systeme verstanden. Dies sind bei Videokonferenzen oft nicht die Geräte der Nutzer, sondern das Gerät jedes Nutzers mit dem Server des genutzten Dienstes. Dies entspricht einer Transportverschlüsselung. Aufgrund der darauf ausgelösten öffentlichen Kritik in der Presse und den ebenfalls öffentlich berichteten Nachbesserungen, geht das Bundeskartellamt davon aus, dass der Beantwortung des Fragebogens die korrekte Definition der Ende-zu-Ende-Verschlüsselung zugrunde gelegt wurde, sofern sich dies nicht aus den Erläuterungen der Befragten ohnehin schließen lässt. Siehe z. B. auch *datenschutz notizen*, abrufbar unter: https://www.datenschutz-notizen.de/ende-zu-ende-verschluesselung-von-videokonferenzen-1825597/ sowie *The Intercept*, Zoom meetings aren’t end-to-end endrypted, despite misleading marketing, 31. März 2020, abrufbar unter: https://theintercept.com/2020/03/31/zoom-meeting-encryption/ und *Golem*, Zoom wirbt mit Ende-zu-Ende-Verschlüsselung – die es nicht gibt, vgl. https://www.golem.de/news/homeoffice-neue-sicherheitsluecken-in-zoom-entdeckt-2004-147670-2.html.

Kriterium sein. Ferner ist darauf zu achten, dass die Identität der Teilnehmenden zweifelsfrei festgestellt werden kann („Authentisierung“). Ende-zu-Ende-Verschlüsselung stellt die Integrität der übermittelten Daten sicher. Ohne eine vorherige zweifelsfreie Authentisierung sorgt sie zwar für den Schutz der übermittelten Daten, stellt aber nicht sicher, wer diese Daten empfangen kann.

b) Ermittlungsergebnisse

Zu der Frage, ob und wie bei den jeweiligen Diensten verschlüsselt wird, hat das Bundeskartellamt zwischen Textnachrichten, Telefon und Video differenziert sowie unterschieden, ob Nutzerinnen und Nutzer sich bilateral oder in einer Gruppe austauschen. Allerdings bieten nicht alle Dienste vollumfänglich die Verschlüsselung aller vom Bundeskartellamt genannten Funktionen an. Die Ende-zu-Ende Verschlüsselung ist bei vielen Messenger- und Video-Diensten eine Option, die von den Nutzerinnen und Nutzern eingestellt werden kann (siehe für die Einzelheiten dazu Abschnitt bb).

aa) Verschlüsselung der Funktionen

Gesamtbetrachtung

Bei der Interpretation der Ermittlungsergebnisse ist zu berücksichtigen, dass manche Dienste nicht alle Funktionen anbieten und dass es technische Einschränkungen bei der Ende-zu-Ende-Verschlüsselung gibt (siehe hierzu den vorausgegangen Abschnitt D.I.4.a)cc)). Hinzu kommt, dass die diversen Optionen, die bei der Verschlüsselung bestehen, von den Diensten unterschiedlich im Fragebogen umgesetzt wurden. So haben z. B. einzelne Befragte alles angekreuzt einschl. „keine Verschlüsselung“, andere haben keine der genannten Kategorien gewählt und lediglich die Möglichkeit genutzt, einen Kommentar einzugeben. Die Zahlenangaben können somit nur als eine grobe Orientierung verstanden werden.
29 Dienste verwenden nach eigenen Angaben für **Textnachrichten** die Transportverschlüsselung sowohl für den bilateralen Austausch als auch in der Gruppe. Die Ende-zu-Ende-Verschlüsselung setzen 22 Dienste bilateral und 19 für den Austausch in der Gruppe ein. Beide Verschlüsselungsarten kombiniert verwenden 16 Dienste bilateral und 13 in der Gruppe. Beim Austausch per **Telefonie** betreiben 22 Dienste Transportverschlüsselung beim bilateralen Telefonat, 18 auch in der Gruppe. Ende-zu-Ende verschlüsseln 18 Dienste bei Einzelgesprächen und 6 in der Gruppe. Beide Verschlüsselungsarten nutzen nach eigenen Angaben 12 Dienste für den bilateralen Austausch und 4 für die Gruppenkommunikation. Beim **Austausch per Video** ist die Zahl der Dienste, die die Transport- und Ende-zu-Ende-Verschlüsselung nutzen, etwas höher als beim Telefonieren. Bei bilateralen Videogesprächen setzen 25 Dienste die Transport- und 21 Dienste die Ende-zu-Ende-Verschlüsselung ein. In der Gruppe geben 22 Dienste an, die Transportverschlüsselung einzusetzen. 11 Dienste nennen die Ende-zu-Ende-Verschlüsselung. Beide Arten der Verschlüsselung nutzen 13 Dienste, zum Teil jedoch nur für die bilaterale Videotelefonie.

	Textnachrichten		Telefonie		Videotelefonie	
	Bilateral	**Gruppe**	**Bilateral**	**Gruppe**	**Bilateral**	**Gruppe**
Transport-verschlüsselung	29	29	22	18	25	22
Ende-zu-Ende-Verschlüsselung	22	19	18	6	21	11
Kombinierter Einsatz	16	13	12	4	13	5

Abbildung 7: Art der Verschlüsselung nach Funktionen

Als Gründe, warum eine bestimmte Funktion nicht verschlüsselt wird, werden - abgesehen von den **technischen Einschränkungen** - verschiedene Faktoren genannt. Dazu zählen Wahlmöglichkeiten der Nutzerinnen und Nutzer, Verfügbarkeit nur für Geschäftskundinnen und -kunden, Eigenentwicklungen, Browser-Voraussetzungen, Kompatibilitätsprobleme oder noch nicht abgeschlossene Entwicklungen.

Videokonferenzanbieter

Einige führende Videokonferenzanbieter erläutern zunächst, wie sie die vom Bundeskartellamt genannten **Funktionen interpretieren**, da dies für die Umsetzung der Ende-zu-Ende-Verschlüsselung maßgeblich sei. Grundsätzlich sei bei der Kategorie „Telefon“ zwischen dem Audiokanal eines Meetings und der externen Einwahl in ein Meeting, z. B. über das öffentliche Telefonnetz, zu unterscheiden. Ähnlich sei es bei der Kategorie „Chat“ bzw. „Textnachrichten“. Hier sei zwischen dem Austausch von Textnachrichten während eines Meetings („Meeting Chat“) und der ggf. eigenständigen Chat-Funktion des Dienstes zu differenzieren.
Im Detail gibt es jedoch Unterschiede insofern, dass nicht alle Funktionen jeder Kundengruppe angeboten werden oder bestimmte Funktionen unternehmensspezifisch definiert werden. Adobe stellt klar, unter „Telefon“ werde der Audiokanal eines Meetings verstanden und nicht die integrierbare Telefonkonferenzanbindung. Google Meet erklärt, die Chat-Funktion sei an die Videokonferenzfunktion gebunden. Die Nutzerinnen und Nutzer könnten nur ihren anderen Videokonferenzteilnehmerinnen und -teilnehmern während der Videokonferenz Nachrichten senden. Die Einwahl über das öffentliche Telefonnetz stünde nur den Business-Kundinnen und -Kunden zur Verfügung, nicht den Verbraucherinnen und Verbrauchern, die die kostenfrei erhältliche Version nutzen.

Slack definiert Textnachrichten als Nachrichten, die innerhalb der Slack-Anwendung zwischen den Nutzerinnen und Nutzern geschrieben werden. Auch Telefonie und Videotelefonie würden als "messenger-intern" verstanden. Es könnten keine Anrufe zu öffentlichen Telefonnummern gemacht werden. Nutzerinnen und Nutzer könnten sich nur mit anderen Slack-Nutzerinnen und Nutzern in ihrem Team oder anderen Teams verbinden, soweit ihr Administrator das gestatte.
Auch Webex erläutert die Bedeutung der vom Bundeskartellamt vorgegebenen Funktionen „Text", „Telefon", „Video". „Text" werde interpretiert als „online messaging", also als Chat-Funktion. Telefon werde bezogen auf das „Webex Calling feature", über das Nutzer und Nutzerinnen Kolleginnen und Kollegen innerhalb des Unternehmens oder Kontakte außerhalb über die Webex-Plattform anrufen könnten.[114] "Video" entspreche „Cisco's Webex online conferencing/meetings" - Angebot, unabhängig davon, ob Nutzerinnen und Nutzer aus dem öffentlichen Telefonnetz oder per VOIP anrufen würden und unabhängig davon, ob sie ihre Kamera einschalten – sich per Video austauschen - oder nicht.
Auch Zoom lässt wissen, „Text" beziehe sich auf „Meeting Chat". Zooms Messaging Funktion umfasse eigentlich zwei Funktionen, den ständigen Chat („Zoom Team Chat") und eben den Chat während eines Meetings („Meeting Chat"), welcher derzeit aktiv als Text-Datei gespeichert werden müsse, wenn er nach dem Meeting erhalten bleiben solle. Die Teilnehmerinnen und Teilnehmer einer Videokonferenz könnten nur während des Meetings über „Meeting Chat" Nachrichten austauschen, danach nicht mehr. Die Kategorie „Telefon" entspreche „Zoom Phone" („Enterprise cloud phone system") und nicht der Einwahl in ein Zoom-Meeting über das öffentliche Telefonnetz. „Video" werde interpretiert als Videokonferenz im Sinne des geteilten Inhalts während eines Zoom-Meetings oder -Webinars.
Zur **Verschlüsselung ihrer Funktionen** machen die führenden Videokonferenzanbieter die folgenden Ausführungen:
Webex gibt an, grundsätzlich für **alle angebotenen Arten des Austauschs die Transport- und die Ende-zu-Ende-Verschlüsselung** zu nutzen. Bereits seit 2008 könnten die Administratorinnen und Administratoren der Kundinnen und Kunden für Videokonferenzen (Audio/Video, 1:1 oder in der Gruppe) die vollständige Ende-zu-Ende-Verschlüsselung auf den Software Clients Mac OS, Windows, Android, Apple iOS aktivieren. Allerdings gelten die grundsätzlichen technischen Einschränkungen bei der Ende-zu-Ende-Verschlüsselung. Für neue Funktionen einschließlich der Direktwahl in Webex-Teams (Arbeitsgruppen), die aktuell nicht die E2E-Verschlüsselung unterstütze, sei die Umsetzung des MLS-Standards in der Entwicklung, auf dessen Basis die Ende-zu-Ende-Verschlüsselung für alle Konferenz-

[114] Siehe Cisco, abrufbar unter: https://www.cisco.com/c/en/us/solutions/collaboration/webex-calling/index.html.

Funktionen angewendet werden könne. Webex biete mit dem Zero-Trust-Ansatz sowohl Authentisierung als auch E2E-Verschlüsselung.
Zoom erklärt, die Ende-zu-Ende-Verschlüsselung könne für „Meeting Chat“ eingestellt werden. Auch für bilaterale Telefonate über „Zoom Phone“ sei für manche Kundinnen und Kunden ein entsprechendes Upgrade verfügbar. Telefonate in der Gruppe würden nicht Ende-zu-Ende verschlüsselt. Bei den Videokonferenzen könne die Ende-zu-Ende-Verschlüsselung aktiviert werden.
Bei Skype kann der **bilaterale Austausch** per Telefon, Video und Textnachricht Ende-zu-Ende-verschlüsselt werden, nicht aber der Austausch in der Gruppe.
Google Meet verschlüssele auf Basis des **TLS Protokolls**. Alle Google Cloud Produkte einschließlich Google Meet würden regelmäßig einer unabhängigen Überprüfung von Sicherheit, Datenschutz und Compliance unterzogen. Wenn die Teilnehmerinnen und Teilnehmer eines Videomeeting sich per Telefon einwählten, käme das TLS Protokoll natürlich nicht zum Einsatz. Auch Adobe, Slack und Microsoft Teams verwenden die Transportverschlüsselung.

Freie Messenger und Open Source-Dienste

Element kann nach eigenen Angaben **alle angebotenen Funktionen** einschließlich Gruppenkommunikation Ende-zu-Ende verschlüsseln. Auch Meet.jit.si kann nach eigenen Angaben für alle angebotenen Funktionen einschließlich Gruppenkommunikation die Ende-zu-Ende-Verschlüsselung einsetzen. Verwendet wird das Double Ratchet-Protokoll und DTLS-SRTP.
Jabber weist darauf hin, dass die Client-Software die OMEMO-Verschlüsselung unterstützen müsse, ansonsten erfolge die Text-Kommunikation und Dateiübertragung nur TLS-verschlüsselt. Übertragene Dateien würden OMEMO-verschlüsselt auf dem Server zwischengespeichert („Encryption at rest“). Telefonie und Video-Telefonie nutzen DTLS-Verschlüsselung. Blabber.im, Conversations, Dino, Quicksy können die Ende-zu-Ende-Verschlüsselung **außer für den Gruppenaustausch per Telefon oder Video** für alle ihre Funktionen verwenden. Sie nutzen WebRTC (DTLS-SRTP). Blabber.im erläutert, es würde OMEMO oder OpenPGP nach Wahl der Nutzerinnen und Nutzer für Textnachrichten und AES 256 für Dateitransfers in verschlüsselten Chats genutzt. DTLS-SRTP käme für Audio/Video-Anrufe zum Einsatz, TLS als Transportverschlüsselung. Bei Quicksy werden für Textnachrichten OMEMO und OpenPGP eingesetzt. Bei Telefonie wird DTLS-SRTP verwendet und über OMEMO verifiziert. Delta Chat erläutert, es könne Ende-zu-Ende verschlüsselt werden, da der Dienst die OpenPGP- und Autocrypt-Standards für den Austausch von Textnachrichten und Dateien erfülle. Auf die eingesetzte Verschlüsselung bei der Video-Telefonie habe Delta Chat keinen Einfluss, Jitsi beispielsweise sei aber ein WebRTC-Dienst.

Weitere Messenger

Alle von ihnen angebotenen **Leistungen einschließlich Gruppenkommunikation Ende-zu-Ende verschlüsseln** können nach eigenen Angaben Ginlo, iMessage / FaceTime, Threema und WhatsApp.

Ginlo setzt WebRTC ein, iMessage / FaceTime nennt SRTP. WhatsApp verweist auf seine Implementierung auf Basis des Signal-Protokolls (Double Ratchet). Gruppenanrufe befänden sich nach Angaben von Threema derzeit zwar in einer Beta-Phase, würden aber voraussichtlich noch vor Ende 2022 breit ausgerollt. Diese Audio- und Videoanrufe in Gruppen wären Ende-zu-Ende verschlüsselt. Die Verschlüsselung der Inhalte entspreche dabei bei Threema dem Standard der Audio- und Videoanrufe zwischen zwei Personen. Die Kommunikation bei Threema sei Ende-zu-Ende verschlüsselt und zusätzlich transportverschlüsselt mit Forward Secrecy und Key Pinning[115]. Für Audio-/Videoanrufe werde WebRTC mit SRTP und DTLS-SRTP 1.2 für Schlüsselaustausch genutzt. Die Sitzungsschlüssel für DTLS seien kryptographisch an die Ende-zu-Ende-Verschlüsselung normaler Threema-Nachrichten gebunden.

Außer für den Gruppenaustausch per Telefon oder Video setzen Line und auch Viber die Ende-zu-Ende-Verschlüsselung für ihre wesentlichen Leistungen - teils mit Einschränkungen - ein. Line habe ein eigenes Verfahren für die Ende-zu-Ende-Verschlüsselung namens “Line Letter Sealing” implementiert. „Line Letter Sealing“ decke Textnachrichten (in bilateralen Chats und in Gruppenchats mit bis zu 50 Mitgliedern), Standortnachrichten (in bilateralen Chats und in Gruppenchats mit bis zu 50 Mitgliedern), Audioanrufe (1:1-Anrufe) sowie Videoanrufe (1:1-Anrufe) ab. Es werde jedoch derzeit nicht auf Video- und Audiodaten angewendet, die als herunterladbare Dateien (Anhänge) gesendet werden. Die Einzelheiten sind - so Line - öffentlich dokumentiert und erhältlich.[116] Viber erläutert wiederum, das eigene Protokoll für die Ende-zu-Ende-Verschlüsselung nutze die gleichen Konzepte des Double Ratchet-Protokolls, wie es in der „Open Whisper Signal-Anwendung“ verwendet werde. Nichtsdestotrotz sei Vibers Implementierung von Grund auf neu und würde nicht den Quellcode von Signal verwenden. Zusätzlich würde WebRTC für die Audio-/Videokommunikation genutzt.

---

[115] Key Pinning ist ein Mechanismus zum Absichern des HTTPS-Protokolls gegen Man-in-the-Middle-Angriffe mit gefälschten, jedoch von einer anerkannten Zertifizierungsstelle (certificate authority) signierten Zertifikaten, siehe z. B. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/HTTP_Public_Key_Pinning.

[116] Vgl. *LINE Letter Sealing*, abrufbar unter: https://scdn.line-apps.com/stf/linecorp/en/csr/line-encryption-whitepaper-ver2.0.pdf.

Facebook Messenger nutzt für Textnachrichten die Transportverschlüsselung, Audio- und Videotelefonate (ausgenommen „secret conversations“)[117] werden mit SRTP[118] verschlüsselt. Bei Facebook Messenger sei Inhalt hauptsächlich in „geheimen Unterhaltungen“ Ende-zu-Ende verschlüsselt.

Einige Dienste nannten **weitere oder zusätzliche** (Verschlüsselungs-) Methoden wie etwa SRTP, RTSP[119], AES[120] in Bezug auf Telefon- und Videokommunikation sowie „Vollverschlüsselung“[121].

bb) Aktivierung der Ende-zu-Ende-Verschlüsselung

Geschäftskundinnen und Geschäftskunden, die Business-Lösungen der Messenger- und Video-Dienste nutzen, profitieren von vielfältigen Einstellungsmöglichkeiten, die sie entsprechend ihrer Bedürfnisse

---

[117] Technical Whitepaper, siehe *Facebook*, abrufbar unter: https://about.fb.com/wp-content/uploads/2016/07/messenger-secret-conversations-technical-whitepaper.pdf.

[118] Bei dem Secure Real-Time Transport Protocol handelt es sich um die verschlüsselte Variante des Real-Time Transport Protocol (RTP). Das Protokoll wurde im März 2004 von der Internet Engineering Task Force (IETF) vorgestellt. Es eignet sich besonders zur verschlüsselten Übertragung von Kommunikation über das Internet und findet auch bei der IP-Telefonie zunehmend Verwendung. Das Kryptosystem verwendet den Advanced Encryption Standard (AES). Je nach Implementierung kann das Protokoll entweder zur Transportverschlüsselung bei der Sprachdatenübertragung zwischen einem Endgerät auf Kundenseite und dem Server des Kommunikationsanbieters (Provider) oder zur vollständigen Ende-zu-Ende-Verschlüsselung zwischen Kommunikationspartnerinnen und -partnern genutzt werden, siehe *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Secure_Real-Time_Transport_Protocol.

[119] Das Real-Time Streaming Protocol (RTSP) ist ein Netzwerkprotokoll zur Steuerung der kontinuierlichen Übertragung von audiovisuellen Daten (Streams) oder Software über IP-basierte Netzwerke. Mit ihm wird die Session zwischen Empfänger und Server gesteuert, siehe *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Real-Time_Streaming_Protocol.

[120] AES (Advanced Encryption Standard) ist ein symmetrisches Verschlüsselungsverfahren, d. h. der Schlüssel zum Ver- und Entschlüsseln ist identisch. Der Rijndael-Algorithmus besitzt variable, voneinander unabhängige Block- und Schlüssellängen von 128, 160, 192, 224 oder 256 Bit, siehe *Wikipedia*, abrufbar unter https://de.wikipedia.org/wiki/Advanced_Encryption_Standard.

[121] Der Dienst definiert dies so, dass alle Nachrichten nicht nur während des Transportes, sondern auch auf allen beteiligten Endgeräten verschlüsselt werden. Die privaten Schlüssel dazu generiere jede Nutzerin, jeder Nutzer automatisch selbst mit der Vergabe eines Gerätepasswortes pro Endgerät. Da sich diese Schlüssel nur auf dem Gerät der jeweiligen Nutzerin oder des jeweiligen Nutzers befinden, habe weder der Dienst noch ein Dritter Zugriff auf sie.

vornehmen können. Verbraucherinnen und Verbraucher aber sind sich womöglich nicht bewusst, welche Möglichkeiten bestehen und welche Bedingungen sie bei den von ihnen genutzten Anwendungen vorfinden. Es dürfte häufig unklar sein, ob die Ende-zu-Ende-Verschlüsselung standardmäßig aktiviert ist oder ob es sich um eine Option handelt, die aktiviert werden muss, ggf. gegen **Entgelt oder wenn weitere Voraussetzungen** vorliegen. Daher hat das Bundeskartellamt die Messenger- und Video-Dienste aufgefordert, darzulegen, wie die Ende-zu-Ende-Verschlüsselung aktiviert werden kann und welche Besonderheiten dabei bestehen.

Gesamtbetrachtung

Von den Diensten, die die Ende-zu-Ende-Verschlüsselung einsetzen, haben 13 angegeben, dass die Ende-zu-Ende-Verschlüsselung **automatisch und unveränderbar aktiviert** ist (BigBlueButton, Fastviewer, Ginlo, iMessage/ FaceTime, Loopup, Monal[122], Nextcloud Talk, TeamViewer Meeting, Threema, Tixeo, Trillian, Viber, Webex, WhatsApp). Bei 8 Diensten ist die Option automatisch aktiviert, kann aber bei 6 dieser Dienste durch die Nutzerinnen und Nutzer, bei einem Dienst durch ihn selbst und bei zwei weiteren sowohl durch Nutzerinnen und Nutzer als auch durch den Dienst selbst verändert werden.

Bei 10 Diensten ist die Ende-zu-Ende-Verschlüsselung **nicht automatisch aktiviert**, kann aber durch die Nutzerin oder den Nutzer eingestellt werden. Ein Multi-Messenger führt aus, der Funktionsumfang werde ausschließlich durch die eingebundenen dritten Dienste bestimmt.

In allen Gruppen von Diensten sind die **Mechanismen, über die die Ende-zu-Ende-Verschlüsselung aktiviert werden** kann, ähnlich. Die meisten Dienste verweisen auf die „Einstellungen“, um die Ende-zu-Ende Verschlüsselung zu aktivieren. Viele Dienste machten auf das Tippen eines Symbols aufmerksam. Auch Meeting-Passwörter und die Aktivierung durch einen Administrator werden erwähnt. Wahlmöglichkeiten weisen insbesondere bei den freien Messenger-Clients einen hohen Stellenwert auf. Bei Videokonferenzanbietern kann häufig der jeweilige Administrator über das Verschlüsselungsniveau der Teilnehmerinnen und Teilnehmer bestimmen.

[122] Dies gilt nach Angaben des Messenger-Clients ab Version 5.3.1. Die Ende-zu-Ende-Verschlüsselung sei dann standardmäßig für 1:1 und Gruppen-Chats aktiviert, sofern diese dies unterstützen.
Die Nutzerinnen und Nutzer könnten weiterhin im Chatfenster erkennen, ob eine Kommunikation verschlüsselt werde oder nicht. Die Verschlüsselung könne weiterhin über das Schlosssymbol deaktiviert und später aktiviert werden. Öffentliche anonyme Gruppen wären technologisch bedingt nicht Ende-zu-Ende verschlüsselt.

Videokonferenzanbieter

Bei GotoMeeting ist das Passwort einzugeben, dass das Meeting schützt. Bei Skype muss „Private Conversation“ gewählt werden, um Ende-zu-Ende-verschlüsselt zu kommunizieren. Webex nutzt immer Verschlüsselung, damit Textnachrichten, Dateien, Whiteboards und andere Inhalte nur verschlüsselt übertragen und gespeichert werden, sobald sie das Gerät des Teilnehmers oder der Teilnehmerin verlassen. Unternehmen können wählen, ob sie den Cloud-Key-Management-Server (KMS) nutzen oder einen KMS selber betreiben möchten und damit die in Webex genutzten Schlüssel selber verwalten. Unternehmen können unterschiedliche Arten von Videokonferenzen und deren Anforderungen an die Art der E2E- bzw. Transportverschlüsselung als „Meeting-Templates“ (Vorlage mit bestimmten technischen Einstellungen) definieren. Der Host könne aus diesen Templates das für das geplante Meeting geeignete auswählen. Für Videokonferenzen können die Nutzerinnen und Nutzer selbst entscheiden, ob diese verschlüsselt werden sollen. Der Administrator könne aber auch Verschlüsselung für alle oder nur einige Nutzerinnen und Nutzer oder für alle Meetings aktivieren. Auch könne der Host bei Planung des Meetings vorgeben, ob der Standardlevel an Sicherheit gelten solle oder ob Ende-zu-Ende-Verschlüsselung verwendet werden müsse (beispielsweise nach Inhalt der Diskussion). Die Übernahme des Schlüsselmanagements (Key Management) erfordere die Etablierung eines umfangreichen Prozesses zur Erzeugung, sicheren Aufbewahrung und sicheren Verteilung von Schlüsseln. Verlust oder Kompromittierung des Master-Keys sei mit dem Verlust oder Kompromittierung des vollständigen Datenbestands im System gleich zu setzen.
Bei Zoom finden sich detaillierte Instruktionen für Inhaberinnen und Inhaber eines Accounts und Administratoren im „Help Center“ des Dienstes.

Freie Messenger /Open Source-Dienste

Bei freien Messenger-Diensten können die Nutzerinnen und Nutzer häufig selbst entscheiden, ob und welche Verschlüsselung sie nutzen. Die Wahl des verwendeten Serverbetreibers bestimme dann, ob und wie verschlüsselt werde.
Der freie Messenger – Client Delta Chat erklärt, die Verschlüsselung könne nicht vollständig abgeschaltet werden, aber Nutzerinnen und Nutzer könnten wählen, dass sie „lieber nicht“ verschlüsseln. Allerdings würden sie auf verschlüsselte Nachrichten anderer dann trotzdem verschlüsselt antworten, wie vom https://autocrypt.org -Standard gefordert. Bei Dino müssen Nutzerinnen und Nutzer für Textnachrichten/Dateien OpenPGP- oder OMEMO-Verschlüsselung auswählen, bei Telefonie/Video sei die Ende-zu-Ende-Verschlüsselung automatisch aktiviert, jedoch ohne Authentication/Deniability, falls OMEMO-Verschlüsselung nicht durch Nutzerinnen und Nutzer aktiviert wird. Bei Gajim sei die Ende-zu-Ende-Verschlüsselung eine einfach erreichbare Einstellung direkt im Chat. Auch bei meet.jit.si finden Nutzerinnen und Nutzer die Einstellung in den Meeting-

Sicherheitseinstellungen. Bei Monal ist das Schlosssymbol anzutippen, um bei neuen Versionen des Messenger-Clients die Ende-zu-Ende-Verschlüsselung deaktivieren und bei älteren Versionen aktivieren zu können.[123] Bei Rocket.Chat muss der Schlüssel gespeichert werden, der beim ersten Login erstellt wird. Außerdem müsse der Server Administrator die entsprechende Einstellung vornehmen.

Weitere Messenger

Bei Facebook Messenger sei der Inhalt hauptsächlich in geheimen Unterhaltungen Ende-zu-Ende verschlüsselt. Nutzerinnen und Nutzer müssten „Geheime Unterhaltungen" auswählen und die gleichnamige Option durch Tippen aktivieren.[124] Damit wären verschiedene Einschränkungen verbunden: „Secret Conversations" funktioniere nur mit iOS und Android Betriebssystemen. Secret Conversations ermöglichten nur begrenzte Funktionen und könnten derzeit nicht als Gruppennachricht verwendet werden. Auch Dateiversand (Gifs), Audio- oder Videotelefonie und Zahlungen wären nicht möglich.[125]

Einige Messenger- und Video-Dienste streben an, ihre Verschlüsselungsmöglichkeiten zu verbessern oder zu erweitern. Bei Dino werde die Ende-zu-Ende-Verschlüsselung mit OMEMO langfristig standardmäßig aktiviert, aber durch Nutzerinnen und Nutzer abschaltbar sein. Auch bei Monal soll die Ende-zu-Ende-Verschlüsselung in Zukunft automatisch aktiviert werden, wenn Langzeittests genügend Stabilität ergeben haben. GotoWebinar führt aus, LogMeIn würde an erweiterten Anwendungsmöglichkeiten der Ende-zu-Ende-Verschlüsselung arbeiten. Facebook Messenger (Meta) erklärt, es werde auf einen globalen Rollout von standardmäßiger Ende-zu-Ende-Verschlüsselung von persönlichen Nachrichten und Anrufen via Messenger in 2023 hingearbeitet.[126]

Vereinzelt wird darauf hingewiesen, die Ende-zu-Ende-Verschlüsselung in Gruppen sei mit dem MLS-Standard in Entwicklung.

---

[123] Die E2E-Verschlüsselung ist nach Angaben des Messenger-Clients seit Version 5.3.1 standardmäßig für 1:1 und Gruppen-Chats aktiviert, sofern diese dies unterstützen.

[124] Siehe *Facebook* 2017, Messenger secret conversations, Technical Whitepaper, abrufbar unter: https://about.fb.com/wp-content/uploads/2016/07/messenger-secret-conversations-technical-whitepaper.pdf.

[125] Siehe *Facebook*, Geheime Unterhaltungen, abrufbar unter: https://www.facebook.com/help/messenger-app/1084673321594605.

[126] Siehe *Facebook*, Testing End-to-End Encrypted Backups and More on Messenger, abrufbar unter: https://about.fb.com/news/2022/08/testing-end-to-end-encrypted-backups-and-more-on-messenger/

cc) Bessere Verschlüsselung gegen Entgelt

Darüber hinaus hat das Bundeskartellamt die Branche gefragt, ob die Verschlüsselung gegen Entgelt weiter verbessert werden kann. Hier kristallisierte sich heraus, dass die weit überwiegende Mehrheit der Dienste **keine zusätzliche Verschlüsselung gegen Entgelt** anbietet. Ein Dienst bietet die Verschlüsselung ruhender Daten für Geschäftskundinnen und -kunden gegen Entgelt an. Die Kundinnen und Kunden könnten außerdem die Verschlüsselung auf verschiedenen Ebenen widerrufen. Lediglich ein weiterer Dienst erläuterte, ein Angebot für weitreichendere Kontrolle über die Verschlüsselungsverfahren zu machen, die Ende-zu-Ende-Verschlüsselung sei aber unabhängig davon grundsätzlich im Abonnement eingeschlossen.

dd) Schlüsselmanagement

Lokaler Verbleib der Schlüssel

Knapp zwei Drittel der Dienste gaben an, dass der **Schlüssel lokal generiert wird und der private Schlüssel auf dem Endgerät** verbleibt.

Facebook Messenger erläutert, dass hauptsächlich bei „geheimen Unterhaltungen“ verschlüsselt werde, und dass die kryptographischen Schlüssel für diese Funktion lokal generiert und auf dem Endgerät verbleiben würden. "Geheime Unterhaltungen" wären aber nicht die einzige Funktion, für die im Rahmen von Facebook Messenger kryptographische Schlüssel lokal generiert und gespeichert würden. Andere Funktionen wie die Transportverschlüsselung generierten ebenfalls solche Schlüssel.

TeamViewer Meeting gibt an, die Schlüssel für das Endgerät sowie der private Schlüssel würden lokal generiert, wobei der private Schlüssel vom Schlüssel des Endgeräts extrahiert werden könne zum Zwecke der Passwort-Regenerierung. Webex führt aus, bei transportverschlüsselten Meetings erstellten die Server die kryptographischen Schlüssel und transferierten diese über TLS zu den Clients. Bei der Ende-zu-Ende-Verschlüsselung werde der Schlüssel durch den Host erstellt und an die Clients der Teilnehmenden weitergegeben. Bei der fortschrittlichen Version der Ende-zu-Ende-Verschlüsselung, die gerade implementiert werde – dem Messaging Layer Security – Standard - werde der Schlüssel durch jeden Teilnehmenden-Client generiert auf Basis der Informationen, die über MLS ausgetauscht würden. Unternehmen können wählen, ob sie den Cloud-Key-Management-Server nutzen oder einen KMS selber betreiben möchten und damit die in Webex genutzen Schlüssel selber verwalten. Zoom hält fest, der Schlüssel werde in Ende-zu-Ende verschlüsselten Meetings von den Geräten der Teilnehmenden erstellt, nicht von den Zoom-Servern. Verschlüsselte Inhalte der Kundinnen und Kunden könnten also nicht durch Zoom gelesen werden, da der dazu notwendige Schlüssel nicht auf den Zoom-Servern vorliege. In einem Meeting ohne Ende-zu-Ende-Verschlüsselung würden die Schlüssel durch die Zoom-Server erstellt und gemanagt.

Sicherer Export und Import

Acht Dienste bestätigten den **sicheren Export und Import** des kryptographischen Schlüssels, wenn auch teilweise abhängig von bestimmten Voraussetzungen, z. B. Art der Funktion.

Discord erläutert, bei Textnachrichten würden die asymmetrischen Schlüssel lokal generiert und würden das Gerät nicht verlassen. Die „Server TLS Schlüssel" würden von Cloudflare[127] gemanagt. Für Audio und Video-Austausch würde ein Kurzzeit-Schlüssel („ephemeral encryption key") auf dem Server generiert und an die Clients für die Gespräche überstellt. Dieser Schlüssel verfalle nach dem Anruf und werde nicht wiederverwendet.[128] Facebook Messenger hält nochmal fest, Inhalte seien hauptsächlich bei „secret conversations" Ende-zu-Ende-verschlüsselt. Für „secret conversations" würden die kryptographischen Schlüssel lokal generiert und der private Schlüssel verbleibe auf dem Endgerät.[129] Line erklärt, es gebe ein „Pairing Protocol, welches den Transfer der privaten Schlüssel zwischen zwei User Clients über einen „out-of-band channel" erlaube. Eine generelle Möglichkeit, private Schlüssel zu im- oder exportieren gebe es nicht. Tixeo erläutert, es würden keine kryptographischen Schlüssel ex- oder importiert. Es komme das Diffie-Hellman Verfahren zum Tragen. Dabei werde nicht der geheime

---

[127] Cloudflare, Inc. ist ein US-amerikanisches Unternehmen, das ein Content Delivery Network, Internetsicherheitsdienste und verteilte DNS-Dienste bereitstellt, die sich zwischen dem Besucher und dem Hosting-Anbieter des Cloudflare-Benutzers befinden und als Reverse Proxy für Websites fungieren. Ein **Content Distribution Network** ist ein Netz regional verteilter und über das Internet verbundener Server, mit dem Inhalte – insbesondere große Mediendateien – ausgeliefert werden. Ein Reverse-Proxy ist ein Proxy in einem Rechnernetz, der Ressourcen für einen externen Client von einem oder mehreren internen Servern holt, siehe *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Cloudflare sowie *Cloudflare*, abrufbar unter: https://www.cloudflare.com/de-de/.

[128] Mehr Informationen zum Audio- und Videoaustausch siehe *Discord*, abrufbar unter: https://blog.discord.com/how-discord-handles-two-and-half-million-concurrent-voice-users-using-webrtc-ce01c3187429.

[129] Weitere Einzelheiten über den Schlüsselaustausch sind erhältlich bei *Facebook*, abrufbar unter: https://about.fb.com/wp-content/uploads/2016/07/messenger-secret-conversations-technical-whitepaper.pdf.

Sitzungsschlüssel übertragen, sondern nur das Ergebnis einer Rechenoperation.[130] Keiner der Dienste differenzierte nach Betriebssystemen. Zwei Messenger- und Video-Dienste erläutern, die kryptographischen Schlüssel wären an das Gerätekonto gebunden und darin gespeichert. Ein neues Gerät bekomme automatisch auch neue Schlüssel.

ee) Kryptographische Prinzipien

Insgesamt findet die Eigenschaft „Authentication" bei Messenger- und Video-Diensten am häufigsten Verwendung, gefolgt von „Perfect Forward Secrecy". „Deniability" und „Future/Backward Secrecy" werden demgegenüber weniger genutzt.

	Textnachrichten		**Telefonie**		**Videotelefonie**	
	Bilateral	**Gruppe**	**Bilateral**	**Gruppe**	**Bilateral**	**Gruppe**
Authentication	27	25	21	15	24	18
Deniability	13	13	6	4	7	5
Perfect Forward Secrecy	19	17	12	7	17	14
Future/Backward Secrecy	11	9	6	3	8	5

Abbildung 8: Verwendung kryptographischer Prinzipien nach Funktionen

Für den Austausch in der Gruppe liegen die Nennungen grundsätzlich etwas niedriger (siehe Abbildung 8).

[130] Der Diffie-Hellman-Schlüsselaustausch ist ein Verfahren, mit dem sich ein gemeinsamer Sitzungsschlüssel zwischen zwei Kommunikationspartnern sicher über ein potenziell unsicheres Übertragungsmedium vereinbaren lässt. Der geheime Schlüssel wird niemals übertragen. Der Schlüssel wird über andere übermittelte Informationen berechnet. Für externe Angreifer, die das Medium abhören, ist das Berechnen des gemeinsamen Sitzungsschlüssel mit vertretbarem Aufwand mathematisch nicht möglich, siehe *Security Insider*, abrufbar unter: https://www.security-insider.de/was-ist-der-diffie-hellman-schluesselaustausch-a-799443/. Diffie-Hellman basiert auf dem Verfahren des „diskreten Logarithmus". Siehe zum "diskreten Logarithmus z. B. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Diffie-Hellman-Schl%C3%BCsselaustausch.

Bei bilateralen **Textnachrichten** wenden 27 Dienste „Authentication“ an, 13 „Deniability“, 19 „Perfect Forward Secrecy“ und 11 „Future/Backward Secrecy“. Für die Kommunikation in Gruppen sind die Werte nur unwesentlich geringer.
Im Bereich der **Telefonie** 1:1 hat knapp die Hälfte der Dienste „Authentication“ genannt. 12 von 44 Diensten haben „Perfect Forward Secrecy“ angegeben. 6 von 44 Diensten nutzen „Deniability“, genauso wie „Future Secrecy/Backward Secrecy“. Für Gruppen sind diese Anteile für alle Eigenschaften der Verschlüsselungsverfahren deutlich geringer.
Bei der **Videokommunikation** 1:1 wendet etwas mehr als die Hälfte der Befragten „Authentication“ an. „Perfect Forward Secrecy“ nennen zwei Fünftel der Dienste. Bei „Deniability“ sowie „Future Secrecy/Backward Secrecy“ sind es 7 von 44 bzw. 8 von 44 Messenger- und Video-Diensten. Für den Austausch in Gruppenkommunikation sind die Werte in allen Kategorien auch hier niedriger als beim bilateralen Austausch.
WhatsApp gibt an, alle vier Eigenschaften bei jeder Art des Austauschs umzusetzen. Die Kommunikation über Blabber.im, Dino, GotoMeeting, GotoWebinar, Viber, Webex ist gemäß den Antworten der Dienste ebenfalls zu einem hohen Anteil von den genannten Eigenschaften geprägt.

ff) Verschlüsselung der Daten auf dem Endgerät und Ablageverschlüsselung

13 Messenger- und Video-Dienste geben an, die Daten auf dem Endgerät der Nutzerinnen und Nutzer zu verschlüsseln: Conferencing & Collaboration (für Windows), Element, Fastviewer, Ginlo, GotoWebinar, iMessage / FaceTime, Line, Skype (für „private conversations“), TeamViewer Meeting, Threema, Tixeo, Webex. Die Dienste, die verschlüsseln, nennen als Verfahren am häufigsten AES mit 256 Bit Schlüssellänge. Erwähnt werden auch RSA sowie Cypher Suite[131] und SQL Cipher[132].
Dementsprechend werden vereinzelt **Unterschiede je nach Betriebssystem oder Endgerät der Nutzerin oder des Nutzers** bei den Verschlüsselungsverfahren des eigenen Messenger- und Video-Dienstes beschrieben. So verwendet ein Videokonferenz-Dienst für den installierten Client Mac's den Systemschlüssel, um die auf dem Gerät gespeicherten Daten zu verschlüsseln. Unter Windows werde mit RSA verschlüsselt. Mobile Apps verwendeten SQLCipher, das eine AES-256-Bit-Verschlüsselung einer lokalen Datenbank biete. Bei einem ausländischen Dienst ist die vollständige Verschlüsselung auf dem Endgerät nur bei Desktop Clients und Browser-Erweiterungen möglich. Ein führender Video-Dienst

---

[131] Eine Cipher Suite (Chiffrensammlung) ist eine standardisierte Sammlung kryptographischer Verfahren, beispielsweise zur Verschlüsselung, vgl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Cipher_Suite.

[132] SQL Cipher ist eine Open Source-Software, die eine transparente 256-Bit-AES-Verschlüsselung von Datenbankdateien bereitstellt, siehe GitHub, abrufbar unter: https://github.com/sqlcipher.

erläutert, wenn sein Client genutzt werde, seien Inhalte auf dem Endgerät verschlüsselt. Wenn ein Web-Browser verwendet werde, seien Inhalte nicht unbedingt auf dem Endgerät verschlüsselt. Die Stärke der Verschlüsselung und weitere Details hingen vom Browser ab und auch von den mit der Kundin oder dem Kunden verabredeten Verschlüsselungsmethoden.
Ferner wird von verschiedenen Diensten auf Unterschiede je nach **implementiertem Client** hingewiesen. Auch die **Art der verwendeten Funktion** kann entscheidend dafür sein, ob verschlüsselt wird oder nicht. So wird z. B bei einem bei Verbraucherinnen und Verbrauchern beliebten Video-Dienst Verschlüsselung mit AES nur für „private conversations“ eingesetzt.

Ein weiterer Sicherheitsaspekt bei Messenger- und Video-Diensten in diesem Zusammenhang ist, ob eine **Ablageverschlüsselung** besteht. Ablageverschlüsselung (sog. Data at Rest) ist auf Daten gerichtet, die in irgendeiner Form auf Speichermedien gespeichert sind. Der Nachrichtenverlauf auf dem Endgerät und ggf. bei Backups kann so vor unerwünschtem Zugriff geschützt und nur von der Messenger-App ausgelesen werden.

22 Messenger- und Video-Dienste haben angegeben, dass eine Ablageverschlüsselung existiert. Mit Betriebssystemherstellern verbundene Dienste und mehrere freie Messenger und andere Dienste weisen ebenfalls auf die **Möglichkeiten der Betriebssysteme** hin, wenn es um die Verschlüsselung der Daten auf dem Endgerät geht, wie z. B. Speicherverschlüsselung oder Geräteverschlüsselungen bei mobilen Betriebssystemen oder (Festplatten-) Verschlüsselung bei iOS und MacOS. Ein freier Messenger-Client weist darauf hin, dass die Apps außerdem auf einem Handy gegeneinander vor Datenzugriffen geschützt seien. Man empfehle Nutzerinnen und Nutzern in der Regel, ihre gesamten Daten zu verschlüsseln und nicht nur die Messaging-Datenbank.
BigBlueButton erklärt, es würden **keine Daten** auf dem Endgerät gespeichert. Meet.jit.si äußert sich ähnlich. Die einzigen Daten, die auf den Endgeräten der Nutzerinnen und Nutzer gespeichert würden, seien die optionalen Informationen über andere Meeting-Teilnehmerinnen und - Teilnehmer.

5. Weitere Sicherheitsmaßnahmen

a) Zwei-Faktor-Authentisierung

aa) Hintergrund

Wenn Verbraucherinnen und Verbraucher Messenger- und Video-Dienste nutzen, können sie dafür sorgen, dass Dritte keinen unerwünschten Zugriff auf ihr Konto haben und sie selbst eindeutig

gegenüber dem Messenger- und Video-Dienste **authentifiziert** sind.[133] Dies kann mit der sog. Zwei-Faktor-Authentisierung erreicht werden, sofern sie als Option in einem System zur Verfügung steht.
Bei der **Zwei-Faktor-Authentisierung (2FA)**[134] bzw. Multi-Faktor-Authentisierung (MFA) wird nicht nur ein einziges persönlich gewähltes und feststehendes Passwort oder Kennwort, sondern mindestens ein weiteres zusätzliches Authentisierungsmerkmal verwendet. Wichtig ist, dass die Faktoren dabei aus verschiedenen Kategorien stammen. Der erste Faktor könnte also z. B. aus dem Bereich „Wissen" stammen (z. B. Passwort, PIN), der zweite zum „Besitz" gehören (z. B. Chipkarte, TAN-Generator) oder auf Biometrie zurückgehen (z. B. Fingerabdruck, Gesichtserkennung).[135]
Die zusätzlichen Faktoren haben meist gemeinsam, dass sie einmalig erstellt werden und nur für kurze Zeit gültig sind – es wird ein sogenanntes **Time-based One-time Password (TOTP**) generiert. Ist das Passwort einmal genutzt oder wird es in einem bestimmten Zeitraum nicht eingesetzt, verfällt es. Selbst wenn Dritte das eigentliche Passwort kennen, haben sie nur wenige Möglichkeiten, auch das TOTP zu erlangen, bzw. keine Zeit, dieses herauszufinden.[136]

---

133 *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.

134 Das BSI erläutert, die Begriffe Authentisierung und Authentifizierung würden im allgemeinen Sprachgebrauch oft synonym verwendet, beschrieben aber verschiedene Teilprozesse, z. B. eines Anmeldevorgangs. Ein Benutzer authentisiere sich an einem System mittels eindeutiger Anmeldeinformationen (z.B. Passwort oder Chipkarte). Das System überprüft daraufhin die Gültigkeit der verwendeten Daten, es authentifiziere den Nutzer oder die Nutzerin, siehe *BSI*, abrufbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html.

135 Vgl. *BSI*: Zwei-Faktor-Authentisierung - Mehr Sicherheit für Online-Konten und vernetzte Geräte, abrufbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html.

136 Die Internet Engineering Task Force (IETF) hat den Time-based One-time Password Algorithm 2011 im RFC 6238 veröffentlicht, um für mehr Sicherheit im Internet zu sorgen. Siehe beispielsweise *IONOS SE*: Time-based One-time Password: TOTP erklärt, abrufbar unter: https://www.ionos.de/digitalguide/server/sicherheit/totp/, *Twilio*: TOTP, abrufbar unter: https://www.twilio.com/docs/glossary/totp, *Security Insider*: Was ist TOTP?, abrufbar unter: https://www.security-insider.de/was-ist-totp-a-875708/.

Der **Ablauf** einer 2FA-Transaktion ist normalerweise so, dass die Nutzerin oder der Nutzer zunächst ihre Zugangsdaten eingeben, um auf die gewünschte Website zu gelangen oder den gewünschten Dienst zuzugreifen. Ein Authentisierungsserver überprüft das Kennwort. Ist es richtig, ist die Nutzerin oder der Nutzer für den zweiten Faktor qualifiziert. Dieser wird der Nutzerin oder dem Nutzer durch den Authentisierungsserver als eindeutiger Code zur Verfügung gestellt. Durch die Bestätigung der zusätzlichen Authentisierung bestätigen die Nutzerinnen und Nutzer ihre Identität.[137]
Der zweite Faktor kann auf verschiedenen Wegen zu den Nutzerinnen und Nutzern gelangen: Per E-Mail, per SMS oder per Sprachanruf, durch auf Biometrie basierende 2FA, als One-Klick-Login / Push-Benachrichtigung sowie als auf Hardware-Token-basierte 2FA oder über Software-Token/ TOTP-basierte 2FA.[138]
Die Zwei-Faktor-Authentisierung mittels **SMS** war lange Zeit das am meisten verwendete Verfahren. Dafür hinterlegt die Nutzerin oder der Nutzer die eigene Mobilfunknummer beim jeweiligen Messenger- und Video-Dienst oder sonstigem Online-Dienst. Wenn sich etwa am PC mit eigenem Nutzernamen und Passwort bei einem Dienst eingeloggt wird, schickt dieser eine SMS mit einem weiteren Code auf das jeweilige Mobiltelefon. Diesen Code geben die Nutzerinnen und Nutzer anschließend auf der Internetseite des Online-Dienstes ein.[139] Weniger verbreitet ist das Verfahren, den zweiten Faktor **per E-Mail** als Code oder Zusatzpasswort zuzusenden. In jedem Fall sollte dafür laut Stiftung Warentest ein anderer E-Mail-Account angegeben werden als der, der für den Login genutzt wird. Sonst kann ein Angreifer, der das Passwort des E-Mail-Kontos kennt, auch die Einmal-Codes abfangen. Anstatt sich den

---

137 Siehe z. B. *IT Security Blog*: 2FA: Zwei-Faktor-Authentifizierung mit TOTP, abrufbar unter: https://itsecblog.de/2fa-zwei-faktor-authentifizierung-mit-totp/.

138 Vgl. *Geekflare*: Die 7 besten Zwei-Faktor-Authentifizierungs-Apps zum Schutz Ihrer E-Mail- und Social-Media-Konten, abrufbar unter: https://geekflare.com/de/two-factor-authentication-apps/.

139 Die Stiftung Warentest hat bereits im Jahr 2017 darauf hingewiesen, dass die Webseite den Code meistens nur innerhalb eines kurzen Zeitraums akzeptiert. Das erhöhe die Sicherheit weiter. Noch sicherer werde das Verfahren, wenn Nutzer über die Einstellungen ihres Smartphones verhinderten, dass es die SMS auf dem Sperrbildschirm anzeigt – und damit für jedermann sichtbar ist. Dies kann über die „Einstellungen“ beim jeweiligen Betriebssystem verhindert werden, vgl. *Stiftung Warentest*: So funktioniert Zwei-Faktor-Authentifizierung, abrufbar unter: https://www.test.de/Online-Konten-schuetzen-mit-2FA-So-funktioniert-Zwei-Faktor-Authentifizierung-5177936-0/.

Code zusenden zu lassen, können sich Nutzerinnen und Nutzer von einigen Diensten auch **anrufen** lassen. Der Code wird dann von einer Computerstimme angesagt.[140]

Bei **biometrischen Systemen** wird beim Login geprüft, ob eines der zuvor erfassten einzigartigen körperlichen Merkmale (Fingerabdruck, Gesicht, Retina) bei Nutzerin oder Nutzer vorliegt. Wie das BSI erläutert, sind biometrische Merkmale im Normalfall nicht "geheim", so dass eine Lebenderkennung wichtig ist, damit die Systeme nicht z. B. mit einem Foto ausgetrickst werden können.[141]

Die Verwendung eines **Hardware-Tokens** gilt als besonders sicher und findet mehr und mehr Verwendung. Als zweiter Identifikationsfaktor wird ein persönliches USB-Gerät („Token“) genutzt. Dabei handelt es sich um einen speziellen USB-Stick, auf dem ein digitaler Sicherheitsschlüssel einprogrammiert ist. Für die Initialisierung stecken Nutzerinnen und Nutzer diesen Stick in die USB-Schnittstelle ihres Rechners. Nach Eingabe von Nutzernamen und Passwort auf der Webseite des genutzten Dienstes drücken sie auf Aufforderung eine Taste auf diesem Stick, woraufhin der Vorgang freigegeben wird.

Wenn Dienste „**One-Click-Login**“ oder „**Push-Benachrichtigungen**“ einsetzen, müssen die Nutzerinnen und Nutzer keinen zweiten Code eingeben. Stattdessen erscheint eine Nachricht auf dem Smartphone, die die Nutzerin oder der Nutzer bestätigen muss. Diese sog. Push-Benachrichtigungen sind Meldungen, die ohne das Öffnen der jeweiligen App auf dem Smartphone erscheinen.

Die zeitbezogenen Einmalpasswörter können schließlich auch in einer **Authentisierungs-App** alle paar Sekunden erzeugt werden. Nutzerinnen und Nutzer müssen sich hierfür einmalig eine kostenlose TOTP-App auf dem Smartphone installieren. Die gewünschte App kann aus dem App-Store des Smartphones heruntergeladen werden. Anschließend müssen die Sicherheitseinstellungen der Website oder des Dienstes, die die Nutzerin oder der Nutzer mit einer 2FA verwenden möchte, auf dem Rechner geöffnet werden. Danach kann die 2FA ausgewählt und aktiviert werden. Der angezeigte QR-Code für die Einrichtung der 2FA muss mit der App gescannt werden. Die Authentisierungs-App ist dann mit dem

---

[140] Vgl. *Stiftung Warentest*, abrufbar unter: https://www.test.de/Online-Konten-schuetzen-mit-2FA-So-funktioniert-Zwei-Faktor-Authentifizierung-5177936-0/.

[141] Vgl. *BSI*, Zwei-Faktor-Authentisierung - Mehr Sicherheit für Online-Konten und vernetzte Geräte, abrufbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html.

Dienst verbunden und erzeugt alle dreißig Sekunden einen neuen einmaligen Code.[142] Nutzerinnen und Nutzer können die Authentisierungs-App auch ohne Mobilfunknetz bzw. Internetverbindung verwenden.

bb) Ermittlungsergebnisse

Die Hälfte der Messenger- und Video-Dienste hat angegeben, den Identitätsnachweis mittels einer Kombination zweier unterschiedlicher und insbesondere unabhängiger Faktoren anzubieten. Die Zwei-Faktor-Authentisierung sollte eine Option ein, die die Nutzerinnen und Nutzer einstellen können (so z. B. bei Discord, Element, Facebook Messenger, Google Meet, GotoMeeting, GotoWebinar, Nextcloud Talk, Rocket.Chat, Skype, Slack, Snapchat, Microsoft Teams, TeamViewer Meeting, Threema, Trillian, Webex, WhatsApp, Zoom). Google gibt an, zukünftig die 2FA nicht mehr nur zu empfehlen, sondern automatisch einbinden zu wollen.[143] Bei einigen Messenger- und Video-Diensten ist die 2FA nur für Geschäftskundinnen und -kunden möglich oder voreingestellt (z. B. bei Trillian oder Microsoft Teams). Ein Multi-Messenger erläutert, ob eine 2FA angeboten werde, hänge vom jeweiligen Dienst ab. Meet.jit.si weist darauf hin, da es bei Jitsi keine Konten gebe, existiere auch keine Authentisierung.
Die Branche insgesamt verwendet eine Reihe von Methoden, von denen die Dienste dann individuell eine bestimmte Auswahl umsetzen.
Einige große Dienste bieten den Nutzern **verschiedene Optionen für die 2FA** an. Bei einer großen „Plattform“ müssen Nutzerinnen und Nutzer, wenn sie ihr Password beim Login eingeben, zusätzlich einen Code von ihrer Time-based One-time password (TOTP) Authenticator App, einen Backup Code oder einen einmalig verwendbaren Code, der ihnen per SMS zugeschickt wird, eingeben. Auch bei einem führenden Messenger-Dienst können Nutzerinnen und Nutzer für die Zwei-Faktor-Authentisierung zwischen drei Sicherheitsverfahren wählen: Entweder geben sie einen zusätzlichen

---

[142] Siehe z. B. *datamate*: Die sieben besten 2FA-Apps für Android und iOS, abrufbar unter: https://www.datamate.org/die-7-besten-2fa-apps-fuer-android-und-ios/, *Web.de* Blog: "OTP-App" – was ist das?, abrufbar unter: https://web.de/email/tipps/posts/was-ist-eine-otp-app/286/, *pcvisit*: Zwei-Faktor-Authentifizierung: Das sind die besten Apps, abrufbar unter: https://www.pcvisit.de/blog/2020/07/23/zwei-faktor-authentifizierung-das-sind-die-besten-apps/.

[143] Im Mai 2021 haben Google, Apple und Microsoft angekündigt, die Unterstützung für einen gemeinsamen passwortlosen Anmeldestandard zu erweitern, der von der FIDO Alliance und dem World Wide Web Consortium entwickelt worden ist, siehe Apple Newsroom, abrufbar unter: https://www.apple.com/de/newsroom/2022/05/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard/.

Sicherheitscode auf einem kompatiblen Gerät ein oder sie nutzen Login-Codes von einer Authentication App Dritter oder sie lassen sich einen Code per SMS zusenden. Der Dienst eines großen Digitalkonzern erläutert ebenfalls, dass es bei seinem Dienst verschiedene Verfahren gibt, wie u. a. Sicherheitsschlüssel, Authenticator und „SMS text message“. Ein bekannter Video-Dienst nennt als eine Option, „authentication apps“ zu nutzen, die die TOTP unterstützen wie Google Authenticator, Microsoft Authenticator, and FreeOTP. Nutzerinnen und Nutzer könnten sich alternativ von diesem Dienst einen Code via SMS oder Anruf zustellen lassen als zweiten Faktor im Authentisierungsprozess. Auch zwei weitere Dienste nennen TOTP Authenticator Apps oder die Sicherheits-SMS bzw. -E-Mail. Darüber hinaus wird ebenfalls auf TOTP sowie 2FA-Geräte verwiesen. Bei einem Dienst, der mit hoher Sicherheit wirbt, wird ein Gerätepasswort plus privater Schlüssel verwendet. Bei einem weiteren solchen Dienst kann die E-Mail-Adresse und/oder Handynummer verknüpft und der Code per E-Mail oder SMS zugesendet werden.

Bei einem bei Verbraucherinnen und Verbrauchern beliebten Dienst können Nutzerinnen und Nutzer eine E-Mail-Adresse eingeben und einen „zweistufigen Verifikations-Code“ einsetzen.

Einige Dienste verweisen auf die **Dienstleister oder „Identity Provider**“, die 2FA, MFA und Single Sign-On anbieten. Ein führender Video-Dienst erklärt, die Administratoren und Administratorinnen der Kundinnen und Kunden könnten die eigene Multi-Factor-Authentication (MFA) aktivieren, die mit OTP (one time password)-Lösungen wie Duo, Microsoft Hello oder Google Authenticator liefen.[144] Diese „Identity providers“ würden MFA für die Nutzer-Authentisierung anbieten. Alternativ könne auch Single Sign-On[145] eingestellt werden. Bei einem weiteren Video-Dienst können die Nutzerinnen und Nutzer ebenfalls Single Sign-on (SSO) mit Zwei-Faktor-Authentisierung einführen.[146] Für die Authentifizierung

---

144 Siehe *Webex*, abrufbar unter: https://help.webex.com/en-us/52szeq/Enable-Multi-Factor-Authentication-Integration-in-Webex-Control-Hub.

145 Siehe *Oasis*, abrufbar unter: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.pdf.

146 Bei Single Sign-on (SSO) kann eine Nutzerin oder ein Nutzer nach einer einmaligen Authentifizierung an einem Arbeitsplatz auf alle Rechner und Dienste, für die er lokal berechtigt (autorisiert) ist, vom selben Arbeitsplatz aus zugreifen, ohne sich bei den einzelnen Diensten jedes Mal zusätzlich anmelden zu müssen. Wechselt die Nutzerin oder der Nutzer den Arbeitsplatz, wird die Authentifizierung, wie auch die lokale Autorisierung, hinfällig, siehe *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Single_Sign-on.

könne auch Twilio[147] als 2FA-Anbieter genutzt werden. Auch zwei andere Video-Dienste verweisen auf „identity provider“ Dritter, einschließlich Azure AD[148], Okta[149], and OneLogin[150], die die Zwei-Faktor-Authentisierung anbieten und mit denen sich die Nutzerinnen und - Nutzer des Dienstes verbinden können.

Bei den Messenger- und Video-Diensten, die mit den Herstellern der großen Betriebssysteme verbunden sind, ist die 2FA an ein entsprechendes **Konto** gebunden (Skype, Teams, Google Meet). Nutzerinnen und Nutzer, die Facebook Messenger verwenden möchten, müssen ohnehin bei Facebook registriert sein.

---

147 Twilio ist ein US-amerikanisches Unternehmen, welches eine Cloud-Kommunikationsplattform als Platform as a Service betreibt. Es hat seinen Sitz in San Francisco. Über Twilio können Softwareentwicklerinnen und -entwickler und Unternehmen mithilfe einer Webdienst-Programmierschnittstelle programmgesteuert Anrufe tätigen und empfangen, Textnachrichten senden und empfangen sowie andere Kommunikationsfunktionen ausführen, vgl. *Wikipedia*, https://de.wikipedia.org/wiki/Twilio oder *Twilio*, https://www.twilio.com/de/.

148 Azure Active Directory ist ein cloud-basierter Dienst von Microsoft zur Verwaltung von Identitäten und Zugriffsrechten, vgl. *Cloudcomputing Insider*, abrufbar unter: https://www.cloudcomputing-insider.de/was-ist-azure-active-directory-azure-ad-a-946693/. Der Enterprise-Identitätsdienst *Azure Active Directory* (Azure AD) bietet Single Sign-On (SSO) und mehrstufige Authentifizierung (Multi-Factor-Authentication), siehe https://azure.microsoft.com/de-de/services/active-directory/.

149 Okta, Inc. ist ein börsennotiertes Unternehmen für Identitäts- und Zugriffsmanagement mit Sitz in San Francisco. Es bietet Cloud-Software an, die Unternehmen dabei hilft, die Benutzerauthentifizierung in Anwendungen zu verwalten und abzusichern, und die es Entwicklern ermöglicht, Identitätskontrollen in Anwendungen, Website-Webdienste und Geräte zu integrieren. Okta vertreibt sechs Dienste, darunter einen Single-Sign-On-Dienst, mit dem sich Nutzerinnen und Nutzer über einen zentralen Prozess bei einer Vielzahl von Systemen anmelden können. Es bietet auch API-Authentifizierungsdienste an. Die Dienste von Okta basieren auf der Amazon-Web-Services-Cloud, vgl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Okta_Inc. oder *Okta Inc.*, abrufbar unter: https://www.okta.com/de/.

150 OneLogin, Inc. ist ein Cloud-basierter Anbieter von Identitäts- und Zugriffsverwaltung, der eine einheitliche Zugriffsverwaltungsplattform für Unternehmen und Organisationen auf Unternehmensebene entwirft, entwickelt und verkauft, siehe *Wikipedia*, abrufbar unter: https://en.wikipedia.org/wiki/OneLogin oder *OneLogin* abrufbar unter: https://www.onelogin.com/de.

b) Sicherheitskopie (Backup)

aa) Hintergrund

Die Messenger- und Video-Dienste mussten schließlich angeben, ob Nutzerinnen und Nutzer ein Backup ihrer Daten erstellen können. Ein Backup bezeichnet eine Kopie vorhandener Daten auf einem weiteren Medium, um sich vor Datenverlust durch Hardware-Ausfälle, Software-Probleme, Naturkatastrophen oder Bedrohungen von außen wie Malware zu schützen. Die Sicherheitskopie kann auf einer externen Festplatte, der Festplatte des Computers oder auch auf einem USB-Stick erstellt werden. Auch online können die Daten gesichert werden.[151]

bb) Ermittlungsergebnisse

Zwei Drittel der Dienste haben angegeben über eine solche Funktion zu verfügen. Dazu zählen Adobe, Blabber.im, Conversations, Delta Chat, Dino, Discord, Element, Facebook Messenger, Gajim, Ginlo, GotoMeeting, GotoWebinar, IMessage/FaceTime, Meet.jit.si, Line, Quicksy, Rocket.Chat, Skype, Snapchat, Teams, Threema, Tixeo, Trillian, Viber, Webex, WhatsApp, Zoom.
Bei einigen Diensten sind die Möglichkeiten an diverse Voraussetzungen oder an bestimmte Funktionen gebunden. Bei einem Dienst bestehe die Möglichkeit, einen Export eines Chatverlaufs herzustellen, nur für angemeldete Nutzerinnen und Nutzer mit geeigneten Berechtigungen im Raum (Veranstalterrolle). Die Möglichkeit, eine Aufzeichnung der Audio/Video-Spuren im Raum herzustellen, erfordere dieselben Berechtigungen. Um ein Backup im engeren Sinne handelt es sich dabei nicht. Ferner wird erklärt, die Sicherung des Chatverlaufs sei nicht möglich, aber Nutzerinnen und Nutzer könnten Anrufe während der Konferenz aufzeichnen. Ein bekannter Video-Dienst unterscheidet in diesem Zusammenhang zwischen seiner eigenen Chat-Funktion, und Meeting-Chat, dem Chat während eines Meetings. Bei der Chat-Funktion könne ein Backup durchgeführt werden, bei Meeting-Chat sei dies nur unter bestimmten Bedingungen möglich, z. B., wenn ein Meeting aufgezeichnet werde oder der Chat als Text-Datei gespeichert werde, sofern dies durch den Administrator aktiviert worden sei.
Beim einem Open Source-Client können Nutzerinnen und Nutzer ihre Videomeetings in ihren eigenen „Dropbox accounts“ speichern. Ein populärer Dienst bietet Ende-zu-Ende-verschlüsselte Sicherheitskopien an.

---

[151] Vgl. z. B. Storage-Insider, abrufbar unter: https://www.storage-insider.de/was-ist-ein-backup-eine-datensicherung-a-621411/ oder *CHIP*, abrufbar unter: https://praxistipps.chip.de/was-ist-ein-backup-einfach-erklaert_41415.

II. Datenverarbeitung

Ein 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 (bei ausgewählten Fragen) ob Praktiken der Dienste den rechtlichen Vorgaben – der europäischen DSGVO – entsprechen.

1. Registrierung

a) Hintergrund

Bei der Registrierung werden die Verbraucherinnen und Verbraucher von den meisten Messenger- und Video-Diensten aufgefordert, persönliche Daten anzugeben. Allerdings kann das Ausmaß der Datenpreisgabe sehr unterschiedlich sein. Bei Anwendungen für Geschäftskundinnen und Geschäftskunden spiegelt die Vielfalt der Wahlmöglichkeiten bei der Registrierung die Kundenwünsche wider, die so unternehmensindividuell umgesetzt werden können.
Das Bundeskartellamt hat die Messenger- und Video-Dienste befragt, welche Voraussetzungen mindestens erfüllt werden müssen, um ihren Messenger-/Video-Dienst für Austausch per Textnachrichten, Telefon oder Video (jeweils 1:1 und Gruppe) in Deutschland als Administrator/Administratorin/Host bzw. als Teilnehmende nutzen zu können (dazu unter b)aa)). Als mögliche Voraussetzungen waren die Angabe einer E-Mail-Adresse, der Klick auf eine Bestätigungsmail, die Angabe eines Namens, einer Telefonnummer, die ID-Vergabe durch den Anbieter, die Vergabe eines Passwortes und die Zustimmung zu der Datenschutzerklärung, zu den Nutzungsbedingungen und zu den AGB genannt. Darüber hinaus konnten andere Voraussetzungen angegeben werden. Gegebenenfalls sollten die Angaben erläutert werden. Dabei war zwischen den Rollen „Host/Administratorin/ Administrotor“ und „Teilnehmende“ zu unterscheiden (dazu unter b)bb)).

b) Ermittlungsergebnisse

aa) Registrierungsanforderungen

<u>Gesamtbetrachtung</u>

Einzelne Messenger- und Video-Dienste halten fest, die Registrierung gelte für alle Funktionen und Services. Die Unterschiede zwischen den Registrierungsanforderungen für den Austausch per Textnachricht, Telefonie oder Videotelefonie sind nach den Ermittlungsergebnissen nicht erheblich, auch wenn die Anforderungen beim Austausch per Video durchschnittlich etwas höher liegen. Sowohl beim Austausch über Textnachrichten als auch per Telefonie und Videotelefonie sind die Registrierungsvoraussetzungen für die Rolle „Host“ durchschnittlich etwas höher als bei der Teilnahme.

Am häufigsten fordern Messenger- und Video-Dienste für die Registrierung im Durchschnitt die **Vergabe einer ID und eines Passworts sowie die Zustimmung zu Datenschutzerklärung, Nutzungsbedingungen und AGB**. Dahinter folgen die Angabe einer Email-Adresse und danach die eines Namens.

Freie Messenger / Open Source

Für die Nutzung von XMPP sind grundsätzlich die ID-Vergabe und ein Passwort obligatorisch. Datenschutzerklärungen, Nutzungsbedingungen und AGB werden von Server-Anbietenden meist öffentlich dokumentiert und beim Anlegen des Kontos über ein Webformular bestätigt. Gleiches gilt für Messaging über die E-Mail-Architektur.

Die freien Messenger-Clients erläutern in diesem Zusammenhang die Trennung zwischen Anwendung und System oder Diensteanbieter. Drei XMPP-Clients stellen klar, ein Client könne mit beliebigen XMPP-Diensten (Servern) genutzt werden (ähnlich wie Email). Die Nutzerinnen und Nutzer könnten einen beliebigen XMPP-Server verwenden, bei dem sie ein Konto einrichten. Sämtliche Voraussetzungen in der Frage des Bundeskartellamts variierten je nachdem, welchen „Dienstanbieter“, z. B. Serverbetreiber, die Verbraucherinnen und Verbraucher wählen. Diese stellten unterschiedliche Anforderungen, die z. B. die Zustimmung zu AGB und die Angabe einer E-Mail-Adresse enthalten könnten. Ein weiterer XMPP-Client pflichtet bei, die Nutzung von öffentlichen oder privaten XMPP-Diensten Dritter, z. B. Serverbetreibern, verlange unter Umständen die Angabe personenbezogener Daten oder die Zustimmung zu Nutzungsbedingungen. Dies sei jedoch nicht strikt notwendig, um den Client zu nutzen, insbesondere, wenn die Nutzerin oder der Nutzer selbst Dienstanbieter sei.

E-Mail-Client Delta Chat erläutert, die Nutzerinnen und Nutzer könnten jede beliebige E-Mail-Adresse verwenden, um Nachrichten zu senden und zu empfangen. Weder die Betreiberin „Merlinux GmbH“ noch irgendein mit ihr verbundener Akteur oder Akteurin erhielten Kenntnis von dieser E-Mail-Adresse, geschweige denn von Passwörtern oder Nachrichten. Dies ergebe sich aus der strikten Trennung von Apps und Nachrichtentransport, eine lang etablierte Praxis im E- Mail-System. Das Delta Chat - Projekt und die Angebote in den App Stores zeigten, dass dies ohne größeren Verlust von „Usability“ und „Convenience“ möglich sei. Die (Video-)Telefonie werde bei Delta Chat über die Einbindung von Jitsi-Instanzen verwirklicht. Die Nutzerinnen und Nutzer können sich hierbei eine Jitsi-Instanz aussuchen, auf der ein Raum eröffnet werden soll. Hierbei würden keine personenbezogenen Daten an Jitsi übermittelt. Außer Jitsi könnten allerdings auch andere Dienste wie BigBlueButton verwendet werden. Auch von diesen Nutzungen erhalte die merlinux GmbH keine Kenntnis, da nur Kommunikation zwischen der installierten App und den Video-Servern stattfinde, in die Delta Chat grundsätzlich keinen Einblick habe, auch keinen verschlüsselten.

Rocket.Chat argumentiert ähnlich wie die freien Messenger-Clients. Der Dienst sei Open Source und in höchstem Maße anpassungsfähig an die Bedürfnisse der Nutzerinnen und Nutzer. Alle Arten der

Registrierung könnten verlangt werden, das sei aber die Entscheidung des jeweiligen Serveradministrators und würde nicht vom Dienst selbst vorgeschrieben. Gerade für den Austausch per Telefon und Video hänge es davon ab, welcher Dienst dafür eingebunden werde.
Beim Matrix-Client Element müssen Nutzerinnen und Nutzer über ID und Passwort verfügen und Datenschutzerklärung, Nutzungsbedingungen und AGB zustimmen. Für Textnachrichten ist außerdem eine E-Mail-Adresse mit Klick auf eine Bestätigungsmail erforderlich.
Bei der Open Source-Anwendung für Videokonferenzen Jitsi Meet müssen keine Nutzerkonten angelegt und Registrierungsdaten eingegeben werden. Bei der vom Bundeskartellamt befragten Anwendung meet.jit.si. erfasst die Betreiberin „8×8“ Netzwerk- und Nutzerinformationen einschließlich der IP-Adressen der Teilnehmenden eines Meetings, der spezifischer URL, über die das Meeting gehostet wird und ggf. Informationen über die Telefonnummern, die sich in das Meeting einwählen (sofern die Audio-Verbindung über Telefoneinwahl geschieht).[152] Auch BigBlueButton (BBB) ist Open Source Software, insb. für Online Learning und Audio-/Videokonferenzen. Basierend auf BBB gibt es unterschiedliche Betreiber mit unterschiedlichen Geschäftsmodellen, die die individuelle Konfiguration und die Registrierungsanforderungen bestimmen.

Weitere Messenger- und Video-Dienste

Bei vielen bekannten Diensten muss bei der Registrierung ein **Konto** angelegt werden. Bei Discord müssen Nutzerinnen und Nutzer dazu einen Benutzernamen und ein Passwort vergeben und entweder eine E-Mail-Adresse oder Telefonnummer angeben. Dies gelte zumindest dann, wenn sie sich ein- und ausloggen möchten oder wenn Sie den Dienst auf verschiedenen Geräten nutzen möchten. Ansonsten könnten sie sich zunächst auch mit einem Benutzernamen und ihrem Geburtsdatum anmelden. Wer den Facebook Messenger nutzen möchte, müsse zunächst ein Facebook-Account anlegen. Dazu müsse der Name, entweder eine E-Mail-Adresse oder eine Mobilfunknummer, Passwort, Geburtsdatum, Geschlecht angegeben werden. E-Mail-Adresse oder Mobilfunknummer müssten bestätigt werden. Nutzerinnen und Nutzer könnten den Messenger auch dann nutzen, wenn sie ihr Facebook-Konto deaktiviert hätten. Teilnehmende müssten sich nur dann nicht mit Namen und Passwort identifizieren, wenn der „Guest Chat mode“ im „Chat Plugin“ eingestellt werde, der von einer Webseite Dritter gehostet werde.[153]
Auch bei Snapchat muss für die Anlage eines Kontos entweder die E-Mail-Adresse oder die Telefonnummer angegeben werden genauso wie Name, Passwort und Geburtsdatum (wegen der

---

[152] Vgl. *meet.jit.si* Privacy Supplement, abrufbar unter: https://jitsi.org/meet-jit-si-privacy/.

[153] Siehe *Meta for Developers*, abrufbar unter: https://developers.facebook.com/docs/messenger-platform/discovery/facebook-chat-plugin.

Altersfreigabe), außerdem ist die Zustimmung zu Nutzungsbedingungen und Datenschutzerklärung notwendig. Bei Snapchat wird nicht zwischen „Administratorinnen / Administratoren / Hosts“ und Teilnehmenden unterschieden.
Wie weitere Dienste es mit dieser Unterscheidung halten und welche Implikationen auf die Datenerfassung dies hat, wird im nächsten Kapitel kurz dargestellt.

bb) Die Rollen „Host“ und „Teilnehmerin“/„Teilnehmer“

Das Bundeskartellamt hat für die Sektoruntersuchung zwischen den Funktionen eines Host (auch Organisatorin/Organisator, Administratorin/Administrator) und einer Teilnehmerin oder eines Teilnehmers unterschieden. Danach wurde Host als Sammelbegriff für eine Person oder Institution verwendet, die aktiv einen Austausch über Textnachrichten, Telefonie oder Videotelefonie starten und andere Teilnehmende dazu einladen kann sowie ggfs. weitere Berechtigungen inne hat (z. B. Stummschalten von Teilnehmern, Löschen von Gruppen, Entfernen von Teilnehmende etc.). Demgegenüber bezeichnet Teilnehmerin oder Teilnehmer jede Person oder Institution, die lediglich auf „Einladung“ eines Host an einem Austausch über Textnachrichten, Telefonie oder Videotelefonie (einzeln oder in Gruppen) teilnehmen kann.
Die Unterscheidung zwischen „Host“ oder „Teilnehmerin/Teilnehmer“ ist den Verbraucherinnen und Verbrauchern wahrscheinlich vor allem von den **Videokonferenzanbietern** bekannt, die spätestens seit Beginn der Pandemie bei vielen zum Alltag gehören. Fast alle der Messenger- und Videodienste, die antworteten, machten Angaben sowohl zur Rolle „Host“ als auch zur Rolle „Teilnehmerin / Teilnehmer“. Bei den Videokonferenzanbietern gibt es einige Gemeinsamkeiten bei der Definition dieser Rollen, aber auch viele Unterschiede und Konfigurationsmöglichkeiten, aus denen Kundinnen und Kunden auswählen können. Grundsätzlich sind bei der **Rolle als „Host/Administratorin/Administrator“** mehr Registrierungsdaten erforderlich als bei Teilnehmenden. Die Hosts selber können allerdings häufig auch bestimmen, mit welchen Daten sich die Teilnehmenden registrieren müssen. Dazu kann die **Anlage eines Kontos** mit den entsprechenden Dateneingaben erforderlich sein.
Bei GotoMeeting brauchen Administratorinnen/Administratoren/Hosts ein solches Konto, um den Dienst nutzen und Audio- und Videokonferenzen sowie den Chat starten zu können. Die Registrierung dafür erfordere den Namen, E-Mail-Adresse, Passwort und eine User-ID sowie die Zustimmung zu LogMeIns „Terms of Service“ und „Privacy Policy“, die beide online erhältlich seien. Teilnehmende eines Meetings, das ein Host gestartet hätte, müssten sich aber nicht registrieren. Die Angabe eines Namens oder einer E-Mail-Adresse sei dann optional. Auch bei Webex müssen sich Teilnehmende einer Videokonferenz - anders als der Host - nicht mit E-Mail-Adresse und Passwort registrieren. Die Angabe eines Namens sei bei Webex nicht nötig. Eine Administratorin oder ein Administrator eines Firmenkunden könne aber vieles einstellen, z. B., dass alle Nutzerinnen und Nutzer ihren Vor- und

Nachnamen eingeben müssten. Bei Videokonferenzen mit mehreren Parteien über Webex müssten die Teilnehmenden eine E-Mail-Adresse eingeben, deren Gültigkeit würde aber nicht überprüft, das typische Format einer E-Mail-Adresse reiche aus. Es würde auf Basis dieser E-Mail-Adresse kein Nutzerkonto erstellt. Auch Microsoft Teams erläutert, als “unauthenticated guest” müsse keine gültige E-Mail-Adresse oder Name eingegeben werden. Es müsse nur den Nutzungsbedingungen einschließlich der Datenschutzerklärung zugestimmt werden. Nach Angaben von Teams sind die Registrierungsanforderungen bei Business-Versionen von Teams für Hosts und Teilnehmende ansonsten identisch, nämlich E-Mail-Adresse, Name, ID, Passwort sowie Zustimmung zu Nutzungsbedingungen, Datenschutzerklärung und AGB.[154]

Auch beim Open Source-Angebot Nextcloud Talk unterscheiden sich die Registrierungsanforderungen je nach Rolle. Nextcloud Talk bietet keinen eigenen Dienst an. Kundinnen und Kunden betreiben Nextcloud (Talk) auf ihren Servern selbst. Jede Person, die einen Benutzeraccount auf der Nextcloud Instanz mit Nextcloud Talk habe, könne je nach Konfiguration Nextcloud Talk als Host nutzen. Nach der initialen Erstellung eines Benutzerkontos auf Nextcloud, würden keine weiteren Daten mehr benötigt, um Videokonferenzen, Chats oder Telefonate durchzuführen. Als Teilnehmerin oder Teilnehmer seien keine Daten notwendig, selbst der Name müsse nicht zwingend angegeben werden (Standard sei einfach "Gast", wenn nicht anders definiert).

Auch wenn Nutzerinnen und Nutzer das **kostenfreie Angebot** eines Video-Dienstes nutzen, muss dazu bei einigen Diensten ein **Konto** angelegt werden, dessen Registrierungsanforderungen weitgehend denen eines Business-Angebots entsprechen. Das ist z.B. bei Google Meet der Fall. Google Meet erläutert, Verbraucherinnen und Verbraucher, die die kostenfreie Version nutzen wollten, müssten zunächst ein Google-Konto anlegen, um Zugang zu Google Meet zu haben. Das sei unabhängig davon, ob sie sich als „Host“ oder „Teilnehmerin“ oder „Teilnehmer“ sähen. Dazu müssten eine E-Mail-Adresse, der Name, eine ID und ein Passwort eingegeben werden. Außerdem sei die Zustimmung zu Datenschutzerklärung, Nutzungsbedingungen und AGB notwendig. Wenn Nutzerinnen und Nutzer bereits ein Konto hätten, gebe es keine zusätzlichen Registrierungsanforderungen, um Google Meet zu nutzen. Beim Business-Angebot dagegen könnten registrierte „Hosts“ Teilnehmende einladen, die kein Google-Konto hätten, z. B. für ein unternehmensübergreifendes Video-Meeting.

---

[154] Microsoft Teams weist darauf hin, dass die Antworten im Fragebogen sich auf die Business-Versionen von Teams bezögen, die als Teil von Microsoft 365 und Office 365 angeboten würden. Zwar wäre in der Zwischenzeit auch eine Verbraucher-Version von Teams erhältlich, das wäre aber erst nach Fristende zur Beantwortung des Fragebogens der Fall gewesen.

Als Teilnehmende eines **kostenfreien Angebots muss mit Funktionseinschränkungen** im Vergleich zum entgeltlichen Angebot gerechnet werden. Zoom beispielsweise hat zur Rolle „Host“ ausgeführt, dass der Fragebogen aus der Perspektive der Nutzerinnen und Nutzer beantwortet worden sei, die das kostenfreie Angebot nutzen und als Host/Administratorin/Administrator auftreten wollten. Als Host auf Basis der kostenfreien Version müssen Name, E-Mail-Adresse, Klick auf Bestätigungs-E-Mail, Geburtsdatum und ein Passwort eingegeben sowie der Datenschutzerklärung und den Nutzungsbedingungen zugestimmt werden. Des Weiteren sei die Kategorie „Teilnehmende“ aus der Perspektive von Nutzerinnen und Nutzern ausgefüllt worden, die zu Meetings von Hosts/Administratorinnen/Administratoren eingeladen worden wären, die sich aber nicht registriert hätten. Teilnehmende müssten nur der Datenschutzerklärung und den Nutzungsbedingungen zustimmen. Diese Nutzerinnen und Nutzer könnten nur den Chat während eines Meetings nutzen, nicht die eigene Chat-Funktion von Zoom.
Wenn Video-Dienste sich **ausschließlich an Konsumentinnen und Konsumenten** richten, muss dies aber nicht heißen, dass die Registrierungsanforderungen niedriger sind als bei Diensten, die sich hauptsächlich an Firmenkundinnen und - kunden richten, insb. dann, wenn ein Konto angelegt werden muss. Skype z. B. wird von Microsoft als „consumer communication service“ bezeichnet. Nutzerinnen und Nutzer müssen E-Mail-Adresse, Name, ID und Passwort eingeben. Eine Unterscheidung in Administratorinnen/Administratoren/Hosts oder Teilnehmer gibt es dabei nicht. Bei Snapchat wird nach der Anlage eines Kontos ebenfalls nicht zwischen Administratorinnen/Administratoren und Teilnehmenden unterschieden.

<u>Weitere Messenger- und Video-Dienste</u>

Die bekannten Messenger- und Video-Dienste, die bei Verbraucherinnen und Verbrauchern besonders beliebt sind, unterscheiden nicht zwischen Administratorinnen / Administratorinnen und Teilnehmenden. Dies gilt z. B für Discord, iMessage / FaceTime, Snapchat, Threema, Viber sowie WhatsApp. Auch bei Facebook Messenger sind die Anforderungen gleich, soweit die Informationen betroffen sind, die zur Verfügung zu stellen sind, um Administratorin oder Administrator oder Teilnehmerin oder Teilnehmer sein zu können. Für Teilnehmende der Videofunktion sind weniger Datenangaben erforderlich, sofern Administratorinnen und Administratoren nicht zusätzliche Anforderungen stellen.

<u>Freie Messenger / Open Source-Dienste</u>

Bei den freien Messaging-Systemen und Open Source-Anwendungen ist die Unterscheidung zwischen Administratorinnen/Administratoren/Hosts und Teilnehmenden grundsätzlich nicht vorgesehen, hängt aber letztendlich von der Gestaltung durch den jeweiligen (Server-) Betreiber ab. So verlangt z. B. auch die vom Bundeskartellamt befragte BigBlueButton-Anwendung „vicole“ von Administratorinnen und

Administratoren E-Mail-Adresse, Klick auf Bestätigungs-E-Mail, Passwort sowie Zustimmung zu AGB, Nutzungsbedingungen und Datenschutzerklärung, während Teilnehmende nur ihren Namen eingeben müssen. Bei Delta Chat als freier Messenger-Client gibt es die Unterscheidung aufgrund der „E-Mail-Architektur“ nicht.

2. Umgang mit Kontakten

a) Hintergrund

Die Frage, wie ein Messenger- und Video-Dienst mit den **Kontakten** der Nutzerinnen und Nutzer umgeht, d. h. ob auf das Kontaktverzeichnis bzw. Adressbuch der Nutzerin oder des Nutzers zugegriffen wird, betrifft weniger die Dienste, die sich mit Videokonferenzen, vor allem im Geschäftskundensegment, beschäftigen. Die Kundinnen und Kunden führen Videokonferenzen innerhalb eines festgelegten Kreises von Teilnehmenden durch. Vertraulichkeit und Diskretion der dort geteilten Informationen sicherzustellen, ist wesentlicher Teil des Geschäftsmodells dieser Videokonferenzanbieter. Häufig kann die Administratorin oder der Administrator der Kundinnen und Kunden bestimmen, welche Registrierungsanforderungen an Teilnehmende gestellt werden.
Bei Diensten mit dem Schwerpunkt Messaging für Verbraucherinnen und Verbraucher, insb. bei entgeltfreien Angeboten, kann dies anders sein. Nicht nur die Telefonnummern der Nutzerinnen und Nutzer selbst, auch die Telefonnummern aus ihren Adressbüchern werden dann auf den Server hochgeladen und ggf. eingeblendet (Contact Discovery). So können auch Telefonnummern von Nutzerinnen und Nutzern auf die Server der Dienste gelangen, die bei dem jeweiligen Dienst nicht registriert sind und in die AGB nicht eingewilligt haben.
Ein datenschutzorientierter Messenger- und Video-Dienst hat erklärt, dass gerade bei der konkreten Implementierung von Synchronisierungen „riesige Unterschiede“, was den Schutz der Privatsphäre angeht, bestünden, denen in dieser Betrachtung Rechnung getragen werden sollte. Dazu zählten nicht nur die Art der Informationen (Daten), die übertragen werden, sondern auch, ob dabei verschlüsselt werde, ob die Daten für die Betreiberin oder den Betreiber lesbar seien und ob sie von ihm gespeichert würden.
Nicht nur für die Verbraucherinnen und Verbraucher selbst, sondern auch für eine datenschutzrechtliche Bewertung von Messenger- und Video-Diensten ist die Frage, wie mit den Daten, insbesondere zur Identität der Nutzerinnen und Nutzer und ihrer Kontaktpersonen umgegangen wird, besonders wichtig. Das Bundeskartellamt hat daher Auskünfte verlangt, welche Voraussetzungen die Nutzerinnen und Nutzer erfüllen müssen, um den jeweiligen Dienst nutzen zu können.

b) Ermittlungsergebnisse

Fünf Messenger- und Video-Dienste, die sich nicht schwerpunktmäßig auf Videokonferenzen ausrichten, verlangen für den Austausch die **Angabe einer Telefonnummer**, als teilnehmende Person oder als Host. Zwei Dienste setzen die Angabe einer Telefonnummer nur für die Host-Funktion voraus. Ansonsten ist die Angabe der Telefonnummer bei Messenger- und Video-Diensten, die schwerpunktmäßig Videokonferenzen betreiben, nicht verpflichtend. Bei einem Video-Dienst ist die Angabe einer Telefonnummer z. B. nur dann erforderlich, wenn Nutzerinnen und Nutzer sich als Teilnehmende oder Host per Telefon austauschen möchten.

In Bezug auf die Datenverarbeitung bei der **Synchronisation des Kontaktverzeichnisses** hat zunächst fast ein Drittel der Messenger- und Video-Dienste angegeben, eine derartige Synchronisation vorzunehmen; überwiegend waren dies international tätige Dienste mit hohen Nutzerzahlen. Die Nutzerinnen und Nutzer willigen dabei offenbar jeweils in ähnlicher Form ein: Sie wählen das optionale Feature aus bzw. stimmen auf einer konkreten **Schaltfläche der App** zu, dass Daten erfasst und weitergegeben werden, oder sie wählen die entsprechende Option in den **Einstellungen** ihres Endgerätes. Im Falle des Facebook Messengers muss die Synchronisation von Kontakten sowohl über eine Schaltfläche in den Einstellungen als auch separat in den Einstellungen des jeweiligen Endgerätes gestattet werden.

Einzelne Dienste, die zu marktstarken, weltweit tätigen Konzernen gehören, haben betont, dass die Nutzerinnen und Nutzer das Kontaktverzeichnis aktiv synchronisieren müssen. Auch Threema betont in diesem Zusammenhang, **die Synchronisation sei vollständig optional**. Da Threema nicht auf Handynummern als Identifikator basiere, komme es zu keinerlei funktionalen Einschränkungen. Threema weist darauf hin, dass im Rahmen dieses Contact Discovery nur die „minimalsten Informationen“ übertragen würden, diese wären verschlüsselt und für den Betreiber nicht lesbar. Sie würden lediglich kurz im Arbeitsspeicher gehalten und nicht gespeichert. Auch Zoom erklärt, es werde nicht standardmäßig synchronisiert, sondern nur eine Synchronisierungsoption angeboten. Demgegenüber haben drei freie Messenger-Clients explizit darauf hingewiesen, dass bei ihnen das Kontaktverzeichnis nicht synchronisiert wird.

Eine fehlende Einwilligung zur Verarbeitung führt bei keinem der anderen betroffenen Dienste dazu, dass den Nutzerinnen und Nutzern die Verwendung des Dienstes unmöglich wird. Sie kann lediglich gewisse Einschränkungen zur Folge haben. So wiesen einige Dienste z. B. darauf hin, dass dann „Freunde“ nicht gefunden werden können oder nur begrenzt Kontaktvorschläge unterbreitet werden. Die Mehrheit der befragten Dienste führt entsprechend den Ermittlungsergebnissen keine Synchronisation des Kontaktverzeichnisses durch.

3. Speicherort der Daten

Weniger als ein Drittel der Dienste speichert mindestens eine Datenkategorie innerhalb der EU – also innerhalb des Anwendungsbereichs der DSGVO. Konkret werden dabei die Daten vor allem in Deutschland, aber auch in Frankreich oder den Niederlanden gespeichert. Dies lässt den Schluss zu, dass eine deutliche Mehrheit der Dienste ihre Daten außerhalb der EU speichert.
Sieben Dienste haben explizit angegeben, mindestens eine Datenkategorie nur in den USA zu speichern. Ein Viertel der Befragten hat im Durchschnitt angegeben, eine Datenkategorie in einer Public Cloud zu speichern - zumeist durch eines der Technologieunternehmen Google (Alphabet), Amazon, Apple oder Microsoft. Freie Messenger-Clients haben darauf hingewiesen, dass der Ort der Datenspeicherung von der Serverauswahl der Nutzerinnen und Nutzer abhängig ist. Einige Dienste unterhalten Speicher-Infrastrukturen in der EU und in Drittländern, insb. den USA. Es blieb teilweise unklar, wohin Daten der EU-Bürgerinnen und Bürger transferiert werden. Teilweise war dies von diversen Konstellationen abhängig.

4. Weitere Ermittlungsergebnisse

Im Rahmen der Ermittlungen hat das Bundeskartellamt die Messenger- und Video-Dienste auch zu weiteren Aspekten der Datenverarbeitung befragt. Themen der Befragung waren insbesondere die Erfassung, der Zweck die Speicherung, die Weitergabe und die Löschung einzelner Datenkategorien, die Einwilligung zur Datenverarbeitung, die Widerrufsmöglichkeiten, die Funktionseinschränkungen bei fehlender Einwilligung sowie die Information der Nutzerinnen und Nutzer über die Datenverarbeitung. Mehrere Dienste haben im Rahmen der allgemeinen Anmerkungen zu diesem Thema explizit darauf hingewiesen, dass sie ihr Vorgehen beim Datenschutz als mit den Vorgaben der DSGVO vereinbar erachten.
Für die verschiedenen Fragen nach Umfang und Art der Datenverarbeitung hatte das Bundeskartellamt im Fragebogen sieben verschiedene Datenkategorien vorgegeben und definiert (Abbildung 9):

Die Fragen wurden von insgesamt 36 Diensten plausibel und auswertbar beantwortet. Einige freie Messenger-Clients und ein Multimessenger haben hier keine detaillierten Angaben gemacht, sondern

➔ **Persönliche Daten:**

Vor- bzw. Nachname des Nutzers, Benutzername oder Pseudonym (z.B. Alias/Nickname), Geburtsdatum, Alter, Geschlecht, Nationalität, E-Mail-Adresse, Telefonnummer, Postanschrift, Kontoinformationen, private Schlüssel für Verschlüsselung

➔ **Geräte- / Konfigurationsdaten:**

IP-Adresse, Betriebssystem, Netzbetreiber, Gerätetyp, Geräte IDS, IMEI (15-stellige Seriennummer bei Smartphones), Benutzerkonten, Passwörter, Fingerabdruck, Zertifikate, installierte Apps, Region- und Spracheinstellungen

➔ **Standort- / Bewegungsdaten:**

Aufenthaltsorte, Aufenthaltszeitpunkte, Aufenthaltsdauer, Bewegungsprofile

➔ **Kontakte / Daten Dritter:**

Kontaktverzeichnis, Adressbücher

➔ **Gruppenmitgliedschaften:**

Teilnehmer oder Organisator (Host) in Chatgruppen, Telefonkonferenzen, Videokonferenzen

➔ **Nutzungsverhalten:**

Häufigkeit und Dauer der Messenger-App-Nutzung, Online-/Offline-Status, Browserverlauf/Browserchronik, Nutzung verschiedener Endgeräte, Art der Geräte, Zeitpunkte / Dauer / Teilnehmer eines Austauschs per Textnachricht / Telefonat / Videotelefonat (jeweils 1:1 oder in Gruppen)

Abbildung 9: Datenkategorien

darauf hingewiesen, dass die Entscheidung über die Datenerfassung/-verarbeitung nicht bei ihnen selbst liege, sondern bei dem jeweiligen Serverbetreiber oder eingebundenen dritten Diensten. Die meisten Messenger- und Video-Dienste haben außerdem festgehalten, dass ihre Angaben zur Datenverarbeitung gleichermaßen für den Austausch per Textnachricht, Telefon oder Video, jeweils bilateral oder in der Gruppe gelten. Einige Dienste, bei denen diesbezüglich Unterschiede bestehen, haben erläutert, dass Gespräche per Video oder Telefonie (anders als Textnachrichten) nicht nachträglich gespeichert werden.

a) Anlass und Zwecke der Datenerfassung

Anlass

Das Bundeskartellamt hat die Dienste gefragt, ob sie Daten aus den genannten Kategorien bei der Registrierung, bei der Nutzung bzw. bei der Synchronisation des Kontaktverzeichnisses erfassen. Die nachfolgende Abbildung 10 zeigt, wie viele Dienste jeweils angegeben haben, bei den verschiedenen Aktionen Daten aus der betreffenden Kategorie zu erfassen:

Fast alle Dienste haben hier angegeben, bei der **Registrierung** persönliche Daten der Nutzerinnen und Nutzer zu erfassen, die Hälfte der Dienste erhebt danach auch Geräte- bzw. Konfigurationsdaten. Keiner der Dienste erfasst bei der Registrierung bereits die Kontakte der Nutzerinnen und Nutzer. Einige Dienste haben darauf hingewiesen, dass bei ihnen keine Registrierung erforderlich ist (z. B. als eingeladene Teilnehmerin oder Teilnehmer bei einer Videokonferenz) und insofern bei dieser Aktion auch keine Daten erfasst werden können.

Bei der **Nutzung** von Messenger- bzw. Video-Diensten werden von deutlich mehr Diensten Daten erfasst als bei der bloßen Registrierung. Laut Befragung erhalten die meisten Dienste hier persönliche Daten, Geräte-/Konfigurationsdaten, Gruppenmitgliedschaften, Nutzungsverhalten sowie Inhalte. Einige Dienste erfassen bei der Nutzung auch Standort-/Bewegungsdaten bzw. Kontakte/Daten Dritter.

In Bezug auf die **Synchronisation des Kontaktverzeichnisses** haben die befragten Dienste deutlich zurückhaltender geantwortet. Fast ein Drittel der Messenger- und Video-Dienste hat hier angegeben, die Kontakte der Nutzerinnen oder Nutzer bzw. die Daten Dritter zu erfassen (siehe zu den Ermittlungsergebnissen D.II.2.b)). Nur vereinzelt erhalten die Dienste danach auch sonstige Daten.

Einzelne Dienste haben an dieser Stelle auch auf die **Erfassung weiterer Daten** hingewiesen. Hierzu gehören die Dauer und die Anzahl der Teilnehmenden eines Gesprächs, die Möglichkeit des

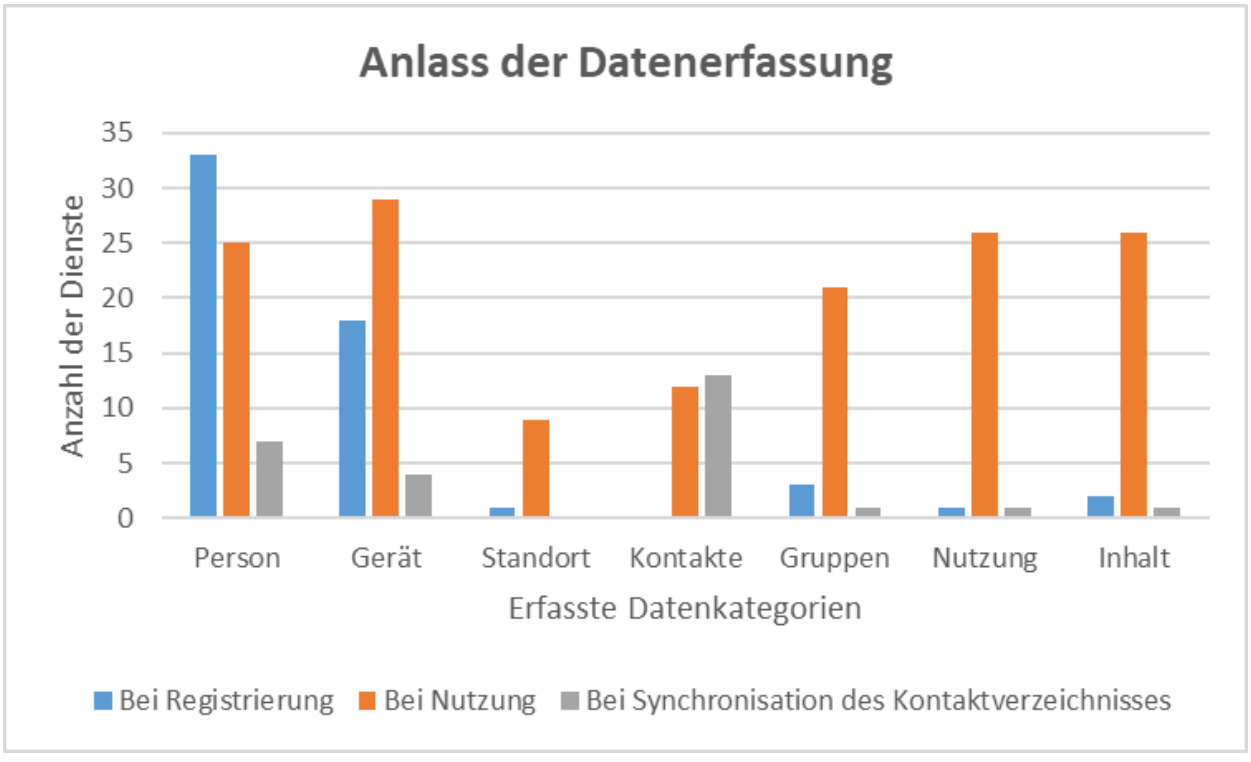


Abbildung 10: Anlass der Datenerfassung

Standortteilens mit anderen Nutzerinnen und Nutzern und die Erfassung des Standorts im Falle eines Notrufs.

Zweck

Ein weiterer Fragenblock betraf den Zweck der Datenerfassung. Die Messenger- und Video-Dienste sollten hier jeweils beantworten, inwieweit sie die einzelnen Datenkategorien für die Funktionalität, für eigene Werbezwecke oder für die Weitergabe an Dritte erfassen. Die nachfolgende Abbildung 11 zeigt die Verteilung der Antworten:

Fast alle der Messenger- und Video-Dienste haben erklärt, persönliche Daten und Geräte-/ Konfigurationsdaten für die **Funktionalität des Dienstes** zu sammeln. Mehr als die Hälfte der Dienste hat dies auch für die Datenkategorien „Nutzungsverhalten“, „Gruppenmitgliedschaften, Kontakte/ Daten Dritter“ und „Inhalte“ genannt. Nur rd. ein Drittel der Dienste sammelt entsprechend der Ermittlungsergebnisse Standort-/Bewegungsdaten der Nutzerinnen und Nutzer für die Funktionalität des Dienstes. Hierzu zählten u. a. die beliebten Dienste Skype, Snapchat und Microsoft Teams. Als Gründe für die Datenerfassung wurden verschiedentlich u. a. die Leistung und Verlässlichkeit des eigenen Messenger- und Video-Dienstes bzw. dessen Verbesserung genannt sowie die Überprüfung von Spamverdachtsfiltern oder die Verbesserung der Interaktion mit den Nutzerinnen und Nutzern.

Deutlich weniger Befragte erfassen Daten **für eigene Werbezwecke**. Als Beispiele für eigene Werbezwecke wurden u. a. Service-Empfehlungen per E-Mail, ein Online Sticker Shop und

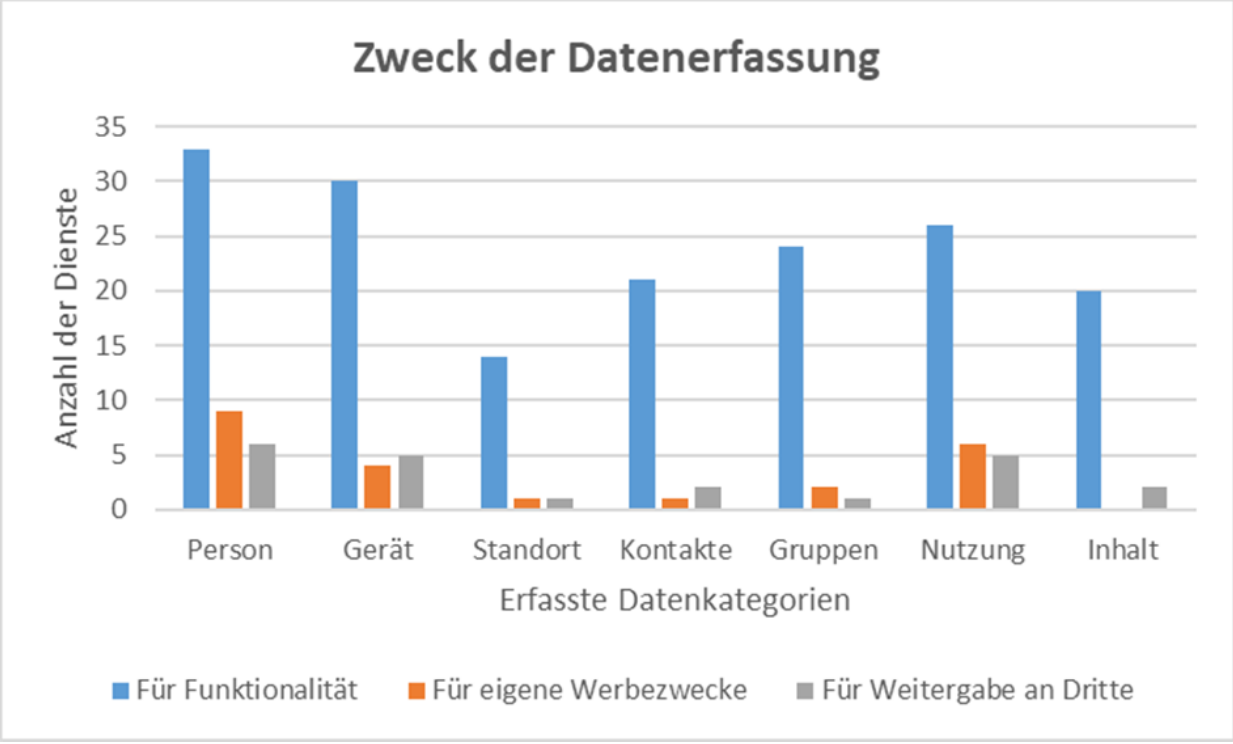


Abbildung 11: Zweck der Datenerfassung

personalisierte Produktempfehlungen sowie Marketingzwecke genannt. Nur einzelne Dienste nutzen hierfür nach eigenen Angaben persönliche Daten, Nutzungsdaten und Geräte-/Konfigurationsdaten. Nur ein bzw. zwei Dienste gaben dies für die Datenkategorien „Gruppenmitgliedschaften“, „Standort-/

Bewegungsdaten“ bzw.“ Kontakte/Daten Dritter“ an. Kein Dienst hat in der Befragung angegeben, Inhalte für eigene Werbezwecke zu erfassen.
Ein ähnliches Bild ergab sich bei der Frage, welche Datenkategorien die Messenger- und Video-Dienste registrieren, um sie **an Dritte weiterzugeben**. Ein kleiner Teil der Dienste gibt persönliche Daten, Geräte- /Konfigurationsdaten bzw. Daten über das Nutzungsverhalten an Dritte weiter; die übrigen Datenkategorien wurden hier lediglich von ein bzw. zwei Diensten genannt. Einzelne Dienste haben erläutert, dass sie ggfs. Daten an Strafverfolgungsbehörden weiterreichen. Einige der befragten Video-Dienste stellen die erfassten Daten nach eigener Aussage für Unterauftragsverarbeiter („subprocessors“) bereit.

b) Weitergabe und Löschen der Daten

Jeweils deutlich weniger als die Hälfte der Messenger- und Video-Dienste gibt gemäß den Ermittlungsergebnissen einzelne Kategorien an Daten **intern** weiter und verarbeitet diese. Die betreffenden Dienste begründeten dies insbesondere damit, Marketing, Sicherheit und Performance verbessern oder die Weitergabe an Behörden sicherstellen zu wollen. Drei populäre Dienste mit hohen Nutzerzahlen haben erläutert, dass Mitarbeiter innerhalb des Konzerns unter gewissen Voraussetzungen Zugang zu den Daten haben, auch wenn keine explizite Weitergabe der Daten erfolge.
Deutlich anders fielen die Antworten bzgl. der Datenweitergabe **an Dritte** aus: Nur jeweils ein Dienst hat im Rahmen der Befragung angegeben, persönliche Daten bzw. Geräte-/Konfigurationsdaten an Facebook (inzwischen firmierend unter „Meta“) weiterzugeben, teilweise unter Hinweis auf die explizite Einwilligung der Nutzerinnen und Nutzer. Eine Datenweitergabe an Google wurde bzgl. jeder der sieben Datenkategorien jeweils von wenigen einzelnen Diensten bestätigt, mit einem leichten Schwerpunkt bei den Kategorien Geräte-/ und Konfigurationsdaten und Nutzerverhalten. Einige Messenger- und Video-Dienste nannten dabei explizit die Nutzung der „Google Cloud“ sowie von „Google Analytics“. Wenige einzelne Dienste haben zudem angegeben, Geräte-/ und Konfigurationsdaten, Daten zum Nutzungsverhalten oder persönliche Daten sowie Inhalte an externe Datenanalysten weiterzugeben. Als Erläuterung wurde hier die Analyse der Servicequalität genannt, namentlich der Analyst „Amplitude“. Ansonsten werden von einzelnen Diensten Daten an Subunternehmer, Strafverfolgungsbehörden oder Geschäftspartner übertragen; weitergegeben werden danach teilweise persönliche Daten, Geräteinformationen und Nutzerverhaltensdaten.
Das Bundeskartellamt hat auch Auskünfte zum **Löschen der Daten** eingeholt. Insbesondere für die Datenkategorien „Geräteinformationen“ und „Nutzungsverhalten“ haben mehrere Messenger- und Video-Dienste angegeben, dass diese in einem Zeitraum von 0 bis 12 Monaten gelöscht werden. Einige Dienste haben allerdings erläutert, dass der Zeitpunkt des Löschens je nach Art der Daten variiere. So werden teilweise z. B. Daten von Privatkundinnen und -kunden früher gelöscht als Daten von

Geschäftskundinnen und -kunden. Videoaufnahmen oder Sprachnachrichten werden eher gelöscht als andere Inhalte und auch für gespeicherte Bewegungs-/Standortdaten gelten kürzere Zeiträume bis zum Löschen. Mehrere Dienste haben angegeben, dass die (automatische) Löschung der Daten nach Vertragsende bzw. nach Löschen des Kontos geschieht. Einige Dienste betonen aber auch, dass die Daten auf Wunsch der Nutzerinnen und Nutzer gelöscht werden.
Zu der Frage, unter welchen Voraussetzungen es möglich ist, ein Nutzerkonto zu löschen, haben sich die Befragten sehr unterschiedlich geäußert. Bei zwei Open-Source-Diensten kann kein Konto gelöscht werden, da keine Daten gespeichert bzw. kein Konto angelegt werden. Bei manchen Diensten müssen die Administratorinnen und Administratoren und die Betreiberinnen und Betreiber von Servern das Löschen umsetzen, bei anderen können die Nutzerinnen und Nutzer dies selbst tun.

c) Einwilligung in die Datenverarbeitung

Zur Frage nach **Anlass und Form der Einwilligung** in die Datenverarbeitung äußerten mehrere hauptsächlich große Messenger- und Video-Dienste explizit, dass Nutzerinnen und Nutzer aktiv in die Datenverarbeitung bei der Registrierung einwilligen. In welcher konkreten Form diese Einwilligung erfolgt, wurde jedoch nur teilweise erläutert. Manche Dienste haben darauf verwiesen, dass bei ihnen gar keine Registrierung erforderlich ist. Einige andere Dienste haben auch erklärt, dass die Nutzerinnen und Nutzer in die Datenverarbeitung gegenüber Dritten (z. B. dem Server-Administrator) einwilligen müssen.
Zu der Frage, in welcher Form die Nutzerinnen und Nutzer ihre Einwilligung zur Datenverarbeitung **widerrufen** können, haben die befragten Messenger- und Video-Dienste sehr unterschiedliche Angaben gemacht. Unter anderem nannten einige Dienste die Möglichkeit, direkten Kontakt aufzunehmen, durch entsprechende Einstellungen bei der Einwilligungserklärung zu widerrufen oder die entsprechende Einstellung auszuschalten sowie durch Löschen des Kontos zu widerrufen. Einzelne Dienste haben auch angegeben, dass ein Widerruf nicht oder nur begrenzt möglich sei, da sonst die Funktionalität des Dienstes nicht mehr gewährleistet werden könne. Insbesondere einige freie Messenger wiesen darauf hin, dass bei ihnen keine Weitergabe der Daten stattfinde und folglich auch weder Einwilligung noch Widerruf erforderlich wären.
Eine weitere Frage betraf die möglichen Folgen in Form von **Einschränkungen und Nachteilen** für die Nutzerinnen und Nutzer des Messenger- oder Video-Dienstes, wenn die Einwilligung in die Datenverarbeitung nicht erteilt bzw. widerrufen wird. Explizit hat das Bundeskartellamt hier abgefragt, inwieweit Funktionen des Messenger- und Video-Dienstes eingeschränkt werden bzw. sonstige Nachteile entstehen, wenn die Einwilligung für eine der oben definierten sieben Datenkategorien nicht vorliegt.

Für den Fall einer fehlenden Einwilligung zur Verarbeitung von **persönlichen Daten, von Geräte-/ Konfigurationsdaten und von Standort-/Bewegungsdaten** haben kleinere Dienste angegeben, dass ihr Messenger- und Video-Dienst ohne diese Daten nicht verwendet werden kann. Andere Dienste erklären, dass in diesem Fall bestimmte Funktionen eingeschränkt wären, wie das Teilen des Standortes mit anderen Nutzerinnen und Nutzern oder die Verwendung von Geofiltern. In Bezug auf die fehlende Einwilligung für die Verarbeitung von **Kontakten oder Daten Dritter** haben einzelne größere Dienste darauf hingewiesen, dass die Nutzerinnen und Nutzer ihre „Freundinnen und Freunde" nicht finden können, wenn das Kontaktverzeichnis nicht synchronisiert wird. Andere Dienste erläuterten, Kontaktvorschläge nur begrenzt automatisiert zu unterbreiten. Wenige kleinere Messenger- und Video-Dienste äußerten, dass die Nutzerinnen und Nutzer den Dienst ohne Informationen über **Gruppenmitgliedschaften, Nutzungsverhalten und Inhalte** nicht nutzen können. Als teilweise Einschränkung aufgrund fehlender Einwilligung oder Widerruf der Verarbeitung dieser Daten wurden von anderen Diensten hier relevante Empfehlungen, Tags/Erwähnungen, Warnungen, personalisierte Werbung, Kommunikation mit anderen Nutzerinnen und Nutzern und Offlinedatenspeicher genannt. Vier Dienste merkten hingegen explizit an, dass es auch ohne diese Daten zu keinen Einschränkungen in Deutschland komme. Ergänzend haben einige Dienste noch darauf hingewiesen, dass ohne die Einwilligung in die Nutzung der Kamera bzw. des Mikrofons keine (Video-)Telefonate bzw. Video-/ Sprachnachrichten möglich seien.

d) Information der Nutzerinnen und Nutzer über Datenverarbeitung und Einwilligung

Die überwiegende Mehrheit der Befragten informiert die Nutzerinnen und Nutzer über Erfassung, Speicherung und Weitergabe der Daten sowie das Einwilligungsmanagement in der **Datenschutzerklärung**. Gut ein Viertel der Messenger- und Video-Dienste nutzt dazu die eigene Website. Nur rund ein Fünftel der Dienste liefert die betreffenden Informationen in den Nutzungsbedingungen bzw. den AGBs. Zu ihren Angaben nannten die Befragten jeweils die betreffenden Links. Die Inhalte der so verlinkten Informationen konnten allerdings im Rahmen der Sektoruntersuchung nicht im Einzelnen überprüft werden. Als weitere Informationsquelle zum Thema Datenverarbeitung wurden von einigen freien Messenger- und Video-Diensten auch die Auftragsdatenverarbeitungverträge genannt bzw. auf die Serverbetreibenden verwiesen.

III. Würdigung

Die Ermittlungsergebnisse haben gezeigt, dass die technische Gestaltung der Messenger- und Video-Dienste komplex und vielfältig ist und sich in ständiger Entwicklung befindet. Eine Bewertung, was notwendig oder wünschenswert ist, erscheint vor dem Hintergrund der mannigfaltigen Vorlieben von Nutzerinnen und Nutzern ein komplexes Unterfangen zu sein. Entsprechend seinem Auftrag in dieser Sektoruntersuchung untersucht das Bundeskartellamt die Sicherheitskriterien vor allem aus der Perspektive der Nutzerinnen und Nutzer, die allerdings in diesem Punkt mit den Interessen der Branche in die gleiche Richtung zeigt (siehe dazu unter 1). Das Ziel eines besonders datenschutzfreundlichen Dienstes kann grundsätzlich auf mehreren Wegen erreicht werden, auch wenn es einige Kriterien gibt, die die Dienste immer umsetzen sollten. Diese stammen sowohl aus dem Bereich der technischen Datensicherheit, als auch aus der Datenverarbeitung (siehe hierzu unter 2 und 3). Die rechtlichen Vorgaben sind einzuhalten (siehe unter 4). Grundsätzlich ist die verbraucherrechtliche Sektoruntersuchung nicht auf Einzelkritiken bestimmter Branchenteilnehmer ausgerichtet. Sektoruntersuchungen nehmen die **gesamte Branche** in den Blick. Auf Grundlage einer Checkliste für Datensicherheit und Datenverarbeitung lassen sich zwischen den verschiedenen Gruppen an Diensten aber Unterschiede erkennen, die für die Verbraucherinnen und Verbraucher wichtig sind (siehe dazu unter 5).

1. Datenschutz im Lichte von Verbraucher- und Brancheninteressen

Das Anliegen dieser Sektoruntersuchung ist, dass die Daten der Verbraucherinnen und Verbraucher besser geschützt werden, wenn sie Messenger- und Video-Dienste nutzen. Deshalb wird zunächst die Situation der Nutzerinnen und Nutzer bei der Auswahl von Messenger- und Video-Diensten hinterfragt (siehe hierzu Abschnitt a). Das Diensteangebot, dem sich die Verbraucherinnen und Verbraucher gegenübersehen, sollte ihre Daten auf Basis von Verfahren auf dem Stand der Technik bestmöglich schützen und in Sachen Datenschutz zukunftsfähig sein, nicht zuletzt, wenn Interoperabilität praktisch an Bedeutung gewinnen sollte (siehe Abschnitt b).

a) Perspektive der Nutzerinnen und Nutzer

Wenn die Nutzerinnen und Nutzer bei der Auswahl ihres Messenger- und Video-Dienstes auf sich allein gestellt sind, stehen sie zahlreichen Kriterien gegenüber, nach denen sie ihren Messenger- und Video-Dienst auswählen können. Die Auswahl kann sich danach richten, welche Dienste die Freundinnen und Freunde, Bekannten oder Freizeiteinrichtungen, wie Sportvereine, verwenden. Für viele private Nutzerinnen und Nutzer ist besonders relevant, dass sie ein kostenloses Angebot wahrnehmen können und über den jeweiligen Dienst möglichst viele Kontakte erreichen. Andere Kriterien können bestimmte Funktionen sein, die ein Dienst besonders gut umsetzt, wie z. B. Videokommunikation in der Gruppe,

oder bestimmte Einstellungen, wie z. B. die Sprache, wenn mit bestimmten Nationalitäten kommuniziert werden soll (z. B. Verwandte aus dem asiatischen Raum infolgedessen einige ausländische Dienste auch in Deutschland - wenn auch geringe - Marktanteile inne haben). Datensicherheit und Datenschutz können somit als Kriterien im Vergleich zur Zahlungsbereitschaft in den Hintergrund treten, was sie auch in vielen Fällen tun (siehe dazu auch Kapitel F.II.), auch wenn es Nutzerinnen und Nutzer gibt, denen Datenschutz besonders wichtig ist und/oder die - was das notwendige Wissen angeht - besonders fachkundig sind.

Viele der in diesem Bericht dargelegten Sicherheitskriterien können Nutzerinnen und Nutzer bei einem Messenger- und Video-Dienst nicht ohne weiteren Zeitaufwand erfassen und bewerten, sofern sie sich ihrer Existenz überhaupt bewusst sind. Die Frage, wer einen Messenger- und Video-Dienst verwendet und wofür - also die Entscheidung zwischen **„geschäftlich" und „privat**" - ist dabei weniger maßgeblich als es auf den ersten Blick scheint. Daher hat das Bundeskartellamt Messenger- und Video-Dienste, die sich hauptsächlich an Geschäftskunden richten und ein Entgelt für ihre Leistungen verlangen, in die Sektoruntersuchung eingebunden.

Zwar besteht bei **Geschäftskundinnen und -kunden** die Hoffnung, dass sich geschäftliche Nutzerinnen und Nutzer der geltenden Datenschutzgesetze bewusst sind, wenn sie Entscheidungen treffen. Zwar dürften Vertraulichkeit und die Sicherheit der geschäftlichen Daten ein erklärtes Ziel bei geschäftlicher Verwendung von Messenger- und Video-Diensten sein. Vermutet werden kann auch, dass viele geschäftliche Nutzerinnen und Nutzer fachkundiges Personal beschäftigen, welches Auswahl und Integration eines Messenger- und Video-Dienstes entsprechend der internen Vorgaben und mit Blick auf die Datenschutzgesetze begleitet bzw. umsetzt.

Ohne weiteres kann aber nicht vorausgesetzt werden, dass diese Annahmen im **Einzelfall** zutreffend sind. Möglicherweise stehen nicht Datenschutz und Datensicherheit, sondern die Umsetzung individueller Anforderungen, die auf den Geschäftszweck zugeschnitten sind, bei der Auswahl eines Messenger- und Video-Dienstes im Vordergrund. Vielleicht ist die Sicherheit der Daten nicht entscheidend, sondern eher bestimmte Funktionen und Features oder die Teilnahme über verschiedene Geräte.

Dass sich geschäftliche Nutzerinnen und Nutzer für einen datenschutzfreundlichen Dienst entscheiden, ist auch deshalb besonders wichtig, da **private Nutzerinnen und Nutzer davon abhängig sein können.** Geschäftskunden spielen als **Multiplikatoren** eine große Rolle. Die Kundinnen und Kunden eines Unternehmens oder Lernende an Schulen, Universitäten oder anderen Bildungseinrichtungen sind gezwungen, als Teilnehmende den Messenger- und Video-Dienst zu nutzen, über den das Unternehmen oder die Bildungseinrichtung Videokonferenzen oder Webinare organisiert. Sie entscheiden darüber meistens nicht selbst. Wie die Ermittlungsergebnisse gezeigt haben, ermöglichen die meisten Videokonferenzanbieter den jeweiligen Administratoren weitreichende Entscheidungsbefugnisse über

die Einstellungen. Daher müssen die entsprechenden Organisatoren gut informiert und sensibilisiert sein und für die Sicherheit und den Schutz der Daten aller Teilnehmerinnen und Teilnehmer sorgen. Schließlich kann ein Dienst - selbst wenn er eigentlich aus geschäftlichen Gründen verwendet wird - auch privat genutzt werden, nicht nur von der geschäftlichen Nutzerin oder dem geschäftlichen Nutzer selbst, sondern z. B. auch von seinen Angehörigen und Freundinnen und Freunden.
Wenn branchenweit ein höheres Datenschutzniveau erreicht werden soll, müssen gerade die Verbraucherinnen und Verbraucher, bei denen Datenschutzaspekte weniger Priorität genießen, erreicht und über Sicherheitskriterien informiert werden. Gleiches gilt für die Nutzerinnen und Nutzer, die als Host oder Administrator für die Teilnehmerinnen und Teilnehmer Entscheidungen treffen.

b) Stand der Technik und Interoperabilität

Ein höheres Datenschutzniveau geht nicht nur auf entsprechende Wünsche der Nachfragerinnen und Nachfrager zurück. Es liegt auch im Bemühen der anbietenden Dienste, sich rechtskonform zu verhalten und ggf. mehr zu tun als Mindeststandards umzusetzen. Unabhängig davon, ob die Nachfragenden den erforderlichen Druck auf die Angebotsseite ausüben können, sollten die Dienste Datensicherheit technisch bestmöglich umsetzen und für zukünftige Entwicklungen gerüstet sein.
Das deutsche Recht unterscheidet in verschiedenen Gesetzen die unbestimmten Rechtsbegriffe des „Stands von Wissenschaft und Technik“ (§ 7 Abs. 2 Nr. 3 Atomgesetz), den „Stand der Technik“ (§ 5 Abs. 1 Nr. 2 Bundes-Immissionsschutzgesetz) und die „anerkannten Regeln der Technik“ (§ 3 Abs. 1 des Gesetzes über technische Arbeitsmittel) als sicherheitstechnische Anforderungen, denen die jeweiligen Anlagen oder Gegenstände genügen sollen, um behördlich genehmigt zu werden.[155] Das Bundesverfassungsgericht hat in der **Kalkar-Entscheidung**[156] diese unbestimmten Rechtsbegriffe ausgelegt (sog. Drei-Stufen-Theorie). Dem Gesetzgeber wird ein bestimmter Gestaltungsspielraum bei deren Verwendung überlassen. In Anlehnung an die Kalkar-Entscheidung wird zwischen dem „Stand der Technik“, dem „Stand der Wissenschaft und Forschung“ und den „allgemein anerkannten Regeln der

[155] Vgl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Stand_der_Wissenschaft#Risikobetrachtung.

[156] Siehe BVerfG, Beschluss vom 8. August 1978 – 2 BvL 8/77 Rdnr. 90 ff., 96 ff

Technik“[157] unterschieden. Die strengsten Maßstäbe setzt der Stand von „Wissenschaft und Technik“. Das Anforderungsprofil stellt auf die neuesten technischen und wissenschaftlichen Erkenntnisse ab. Dagegen ist mit den „anerkannten Regeln der Technik“ verbunden, dass allgemein wissenschaftlich anerkannte und praktisch bewährte Erkenntnisse umgesetzt werden. Der „**Stand der Technik**“ ist in der Mitte einzuordnen. Von einer schon erreichten allgemeinen Anerkennung, die für die anerkannten Regeln der Technik gefordert ist, wird hier abgesehen. Es handelt sich aber um einen fortgeschrittenen Entwicklungsstand, der zur Erreichung bestimmter praktischer Schutzzwecke als gesichert angesehen werden darf. Der Stand der Technik gibt wieder, was technisch notwendig, geeignet, angemessen und vermeidbar ist. Der Stand der Technik ist – wie bereits eingangs erwähnt – beispielhaft legaldefiniert in § 3 Abs. 6 Bundes-Immissionsschutzgesetz.[158] Er findet sich auch in weiteren nationalen Gesetzen, wie § 9 Abs. 1 Telekommunikationsgesetz (TKG)[159], § 13 Abs. 7 Telemediengesetz (TMG)[160] und § 8a Abs 1 S. 2 BSI-Gesetz (BSI-G)[161] sowie zur Einstufung von Verschlüsselungsmaßnahmen in der Anlage zu § 9 BDSG[162] a. F.

Auch in die **Datenschutzgesetzgebung** hat der Stand der Technik Einzug gehalten. Für die Eignung technischer und organisatorischer Maßnahmen nach Art. 32 Abs. 1 DSGVO ist eine Abwägung neben

---

[157] Als Beispiel für anerkannte Regeln der Technik werden die DIN-Vorschriften des Normenausschusses Bauwesen im Deutschen Institut für Normung e.V., die Vorschriften des Verbandes Deutscher Elektrotechniker e.V. (VDE-Vorschriften) und die Vorschriften des Deutschen Vereins des Gas- und Wasserfaches e.V. (DVGW), aber auch VDI-Richtlinien und die Durchführungsverordnungen der Landesbauordnungen genannt. Die Normen, Arbeitsblätter und Richtlinien würden nicht immer dem aktuellen technischen Kenntnisstand entsprechen. Sie würden nicht immer Regeln enthalten, die sich langfristig bewähren oder bewährt haben. Deswegen können auch höherwertige Leistungen gefordert sein, vgl. *KomNet*, abrufbar unter: https://www.komnet.nrw.de/_sitetools/dialog/43529.

[158] Siehe *Bundesminsterium der Justiz*, abrufbar unter https://www.gesetze-im-internet.de/bimschg/. Vgl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Stand_der_Technik#cite_note-5, *Der Bausachverständige*, abrufbar unter: https://www.derbausv.de/zeitschrift/aktuelle-ausgabe/was-sind-allgemein-anerkannte-regeln-der-technik/ sowie Heise, abrufbar unter: https://www.heise.de/select/ix/2017/7/1499358051209829.

[159] Telekommunikationsgesetz, abrufbar unter: https://dejure.org/gesetze/TKG.

[160] Telemediengesetz, abrufbar unter: https://de.wikipedia.org/wiki/Telemediengesetz.

[161] BSI-Gesetz, abrufbar unter: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html.

[162] Bundesdatenschutzgesetz, außer Kraft getreten am 25.05.2018 aufgrund des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU).

weiteren Kriterien[163] nach dem „Stand der Technik“ zu treffen. Auch wenn eine Definition des Stands der Technik in der DSGVO fehlt, wird die Referenz auf den Begriff als Dynamisierung der DSGVO interpretiert.[164]

Sowohl für eine digitale Branche mit hoher Entwicklungsgeschwindigkeit als auch die involvierten Behörden ist relevant, wie der "Stand der Technik" zu einem bestimmten Zeitpunkt zu interpretieren ist. Das BSI erläutert, dies lasse sich anhand existierender nationaler oder internationaler Standards und Normen von beispielsweise DIN, ISO, DKE oder ISO/IEC oder anhand erfolgreich in der Praxis erprobter Vorbilder für den jeweiligen Bereich ermitteln. Der Stand der Technik sei nicht nur ein gängiger juristischer Begriff, sondern bei technischen Fragen auch bewährter Beurteilungsmaßstab. Die **technische Entwicklung sei schneller als die Gesetzgebung**. Daher habe es sich in vielen Rechtsbereichen seit vielen Jahren bewährt, in Gesetzen auf den "Stand der Technik" abzustellen, statt zu versuchen, konkrete technische Anforderungen bereits im Gesetz festzulegen. Da sich die notwendigen technischen Maßnahmen je nach konkreter Fallgestaltung unterscheiden können, sei es aber nicht möglich, den "Stand der Technik" allgemeingültig und abschließend zu beschreiben.[165]

Bei der Einordnung der Ermittlungsergebnisse folgt das Bundeskartellamt der herrschenden Meinung der Rechtsprechung im Datenschutz und der Auffassung des BSI. Dies geschieht insbesondere auch vor dem Hintergrund der **Interoperabilitätsregelung**, die in den am 1. November 2022 in Kraft getretenen **Digital Markets Act** Eingang gefunden hat. Messenger- und Video-Dienste werden von den neuen Vorschriften unterschiedlich stark betroffen sein. Dies richtet sich sicherlich vor allem danach, ob ein Messenger- und Video-Dienst als zentraler Plattformdienst eines als Gatekeeper klassifizierten Unternehmens, der gewerblichen Nutzerinnen und Nutzern als wichtiges Zugangstor dient, benannt wird. Dieser muss ein interoperables Standardangebot - im Wortlaut des Art. 7 Abs. 4 DMA „Referenzangebot“ - bereitstellen. Aber unabhängig davon, ob ein Dienst als Gatekeeper gelten oder Zugang zum Selbigen beantragen wird, hat die gegenwärtige technische Konzeption Einfluss darauf, ob viel oder wenig Aufwand betrieben werden muss, um die Sicherheit und den Schutz der Daten zu

---

[163] Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, vgl. *Simitis, Spiros, Hornung, Gerrit, Döhmann, Indra*, Kommentar zum Datenschutzrecht, Artikel 32, 26 , Baden Baden 2019.

[164] Vgl. *Simitis, Spiros, Hornung, Gerrit, Döhmann, Indra*, Kommentar zum Datenschutzrecht, Artikel 32, 22 , Baden Baden 2019.

[165] Vgl. *BSI*, abrufbar unter: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/stand-der-technik-umsetzen_node.html.

gewährleisten, wenn an einem Interoperabilitätsregime teilgenommen werden soll oder muss. Die Anforderungen der Datenschutzgesetze sind jederzeit zu erfüllen. Jegliche Festlegungen im Rahmen eines solchen **Interoperabilitätsregimes** sollten auf den Stand der Technik verweisen. Das Bundeskartellamt schließt sich hier den Äußerungen verschiedener Branchenteilnehmer an, die in ihren Antworten auf den Fragebogen des Bundeskartellamts auf diese Zusammenhänge hingewiesen hatten (siehe dazu F.III.5).

Auch für die Verbraucherinnen und Verbraucher stellen sich im Zuge der im Digital Markets Act enthaltenen Interoperabilitätsverpflichtung für Gatekeeper neue Fragen zu Sicherheit und Schutz ihrer Daten. Dies ist nicht nur der Fall, wenn ihr Messenger- und Video-Dienst als Gatekeeper entsprechend benannt wird und anderen Messenger-Diensten Zugang gewähren muss. Wenn der eigene Messenger-Dienst Zugang beantragt, muss ebenfalls geklärt werden, ob und wie die Daten der Nutzerinnen und Nutzer geschützt werden. D.h. es muss nachvollziehbar sein, welche Sicherheitskriterien bereits implementiert wurden sowie ob und wie sie unter Interoperabilität greifen können.

2. Sicherheitskriterien im Check – nur zusammen stark

Einige der Sicherheitskriterien, zu denen das Bundeskartellamt ermittelt hat, sind - jeweils allein betrachtet - kein Indikator für die Datenschutzqualität eines Dienstes. Vielmehr ist das Gesamtbild - oder besser das Zusammenspiel mit anderen Kriterien - entscheidend.

a) Netzwerkstruktur, Standards, Protokolle – ein zweiter Blick lohnt sich

Die Netzwerkstruktur, die Zusammenarbeit mit Standardisierungsorganisationen und das verwendete Protokoll einschließlich dessen Einsehbarkeit als Sicherheitskriterien können von den meisten Verbraucherinnen und Verbrauchern nicht ohne Weiteres eingeschätzt und mit der Datenschutzqualität in Beziehung gesetzt werden. Dazu ist zunächst einmal das notwendige Problembewusstsein und ein über Allgemeinwissen hinausgehendes Verständnis und Interesse sowie erheblicher Zeitaufwand notwendig, um überhaupt herauszufinden, ob die Information verfügbar ist oder nicht, d.h. ob die Messenger- und Video-Dienste die Informationen bereitstellen.

Eine knappe Mehrheit der vom Bundeskartellamt befragten Messenger- und Video-Dienste fußt auf einer zentralisierten Netzwerkstruktur. Nutzerinnen und Nutzer müssen sich dann beim Server des Dienstbetreibers anmelden und auch dessen Client (App, Software) nutzen. Alle wesentlichen Entscheidungen liegen damit in der Hand des Dienstbetreibers.

Die Art der **Netzwerkstruktur** allein indiziert noch keine eindeutige Aussage zur Datenschutzqualität eines Dienstes. Sie kann ein Indikator für die Unabhängigkeit vom Dienstbetreiber selbst sein, insbesondere, was den Verbleib von Meta-Daten angeht. Auch im Hinblick auf eine mögliche Interoperabilität spielt die Netzwerkstruktur eine Rolle, nämlich bei der Frage, wie eine

serverübergreifende Kommunikation umgesetzt werden kann. Nach Angaben des BSI liegt die Entwicklung von entsprechenden Konzepten für föderierte Systeme noch in den Anfängen.[166]
Eine föderale Netzwerkstruktur wird vor allem mit **freien Messenger-Systemen** verbunden. Meta-Daten fallen bei föderierten Systemen eben nicht zentral an, sondern liegen i. A. beim jeweiligen Serverbetreiber der Nutzerinnen und Nutzer vor. Verbraucherinnen und Verbraucher sollten sich hier aber bewusst sein, dass jedes freie Messaging-System auch zentral als Insel-Lösung, z. B. innerhalb eines Unternehmens oder eines Vereins, betrieben werden kann. Es muss also auch genau hingeschaut werden, wer die Verantwortung für Datensicherheit und Datenschutz trägt und wie sie wahrgenommen wird, wenn mit den freien Protokollen XMPP oder Matrix geworben wird. Gerade das freie Messaging-System Matrix kann als Beispiel gelten, um für eine differenzierte Betrachtung zu werben. So werden Chaträume nach dem Grundkonzept von Matrix grundsätzlich auf allen am jeweiligen Chat beteiligten Servern repliziert.[167] D. h., die jeweiligen Daten liegen auf allen Servern vor, nicht nur auf dem Home-Server der Nutzerinnen und Nutzer.
Wenn Messenger- und Video-Dienste Standards, z. B. der IETF einsetzen, kann dies für die Nutzerinnen und Nutzer ein Qualitätssignal sein. Eine **Zusammenarbeit mit Standardisierungsorganisationen** ist in der Branche weit verbreitet. Diese Zusammenarbeit kann allerdings unterschiedlicher Gestalt sein. Einige der führenden Dienste, die mit großen Konzernen verbunden sind, bringen sich auf internationaler Ebene ein und setzen eigene Impulse, was die technische Weiterentwicklung angeht. Fast alle Messenger- und Video- Dienste setzen standardisierte Techniken ein, wenn sie diese auch nicht selbst entwickelt und maßgeblich beeinflusst haben. Hier sind vor allem das **Double Ratchet-Protokoll**[168] für den Austausch und der **WebRTC-Standard** für die Audio-/Videokommunikation zu nennen.
Die Ermittlungsergebnisse haben gezeigt, dass 40 Prozent der befragten Messenger- und Video-Dienste den Quellcode des von ihnen verwendeten **Kommunikationsprotokolls** offenlegen. Umgekehrt

---

166 Vgl. *BSI*, abrufbar unter: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/stand-der-technik-umsetzen_node.html.

167 Siehe u.a. *Initiative Freie Messenger*, abrufbar unter: https://www.freie-messenger.de/sys_matrix/.

168 Es gilt als Stand der Technik, wie auch das BSI näher erläutert hat. Neben den klassischen Sicherheitseigenschaften der Kryptographie (Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit, (Nicht-) Abstreitbarkeit) weist das Protokoll einige weitere Sicherheitseigenschaften auf, die insbesondere bei Messenger- und Video-Diensten von besonderer Bedeutung sind. Siehe *BSI*, Moderne Messenger – heute verschlüsselt, morgen interoperabel?, November 2021, S. 10, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

formuliert, mehr als die Hälfte der Messenger- und Video-Dienste veröffentlicht den Quellcode ihres Protokolls nicht. Das Protokoll ist ein wesentlicher und zentraler Teil eines Messaging-Systems, sozusagen seine Sprache und somit ausschlaggebend dafür, wie weitere Funktionen, wie die Verschlüsselung, umgesetzt werden. Dies betrifft auch Datenschutzaspekte. Hier ist z. B. auch an die kryptographischen Prinzipien und Eigenschaften zu denken. Unter den Diensten mit einem einsehbaren Protokoll sind viele freie Messenger-Clients, die ohnehin die Open Source-Philosophie verkörpern. Einige andere Messenger- und Video-Dienste nutzen proprietäre und einsehbare Protokolle parallel. Wenn das Protokoll nicht einsehbar ist, erschwert das die **Überprüfbarkeit durch Dritte**. Die Verständlichkeit technischer Informationen ist für Laien natürlich begrenzt, selbst wenn sie verfügbar sind. Allerdings existieren neben fachkundigen Nutzerinnen und Nutzern, die sich für Datenschutz und Datensicherheit einsetzen und Webseiten[169] zur Information der Verbraucherinnen und Verbraucher gestalten auch fachkundigen Behörden und Institutionen, die die notwendige Fachkompetenz besitzen. Nachvollziehbar ist, dass Dienste, die Messaging und Videokonferenzen als Kernleistungen anbieten und dafür bezahlt werden, ihre Entwicklungen zunächst schützen, bis sich diese am Markt durchgesetzt haben und diese erst dann den Standardisierungsorganisationen vorlegen. Letzteres sollte dann aber auch geschehen.

Unter Sicherheitsaspekten schwer durchschaubar wird es aber, wenn - wie in der Branche der Messenger- und Video-Dienste - nicht wenige Branchenteilnehmer zwar Standards anwenden, einige davon - beispielsweise das Protokoll - aber **individuell weiterentwickelt und angepasst** haben und diese Weiterentwicklungen nach Marktdurchdringung nicht mehr den Standardisierungsorganisationen vorgestellt wurden. In den Ermittlungen wurde auf das Protokoll von WhatsApp verwiesen, welches auf Basis von XMPP entstanden sei. Die diversen Weiterentwicklungen seien mit der „Entwickler-Öffentlichkeit“ nicht mehr geteilt worden. Vielmehr sei ein geschlossenes System konzipiert worden. Nachteilig sind solche Entwicklungen auch für jegliche **Interoperabilitätsbestrebungen**, z. B. in Fragen der Ende-zu-Ende-Verschlüsselung über Messenger-Grenzen hinweg.

Sicherheitsaudits durch bekannte oder weniger bekannte Institutionen können hier nur **begrenzt Ersatz für eine fehlende Einsehbarkeit** bieten, da die Vielfalt der Möglichkeiten Vergleiche erschwert und auf Seiten der überprüfenden Dritten sehr umfassende Kenntnisse der verschiedenen Prüfverfahren notwendig sind, um Einschätzungen ableiten zu können.

---

[169] Vgl. z. B. *Initiative Freie Messenger*, abrufbar unter: https://www.freie-messenger.de/, *Kuketz*, abrufbar unter: https://www.kuketz-blog.de/, *Golem*, abrufbar unter https://www.golem.de/sonstiges/leitbild.html u. v. m.

b) Verschlüsselung – alles geht, nichts muss?

Wie im Abschnitt D.I.4.a) dargestellt wurde, können Messenger- und Video-Dienste die Daten der Nutzerinnen und Nutzer beim Versand auf zwei verschiedene Arten schützen. Eine Transportverschlüsselung macht es Dritten unmöglich, die versendeten Daten bei der Übertragung zwischen dem Client der Nutzerin oder des Nutzers und dem Server zu lesen. Allerdings hat der Serverbetreiber oder die Serverbetreiberin nach wie vor Zugang zu den Daten, da sie auf dem Server im Klartext vorliegen. Um dies zu verhindern, ist – so das BSI – „eine zusätzliche Verschlüsselung der Inhalte zwischen den Endpunkten der Kommunikation, also den Nutzer-Clients von Sender und Empfänger(n) auf den Endgeräten notwendig, was mittels einer Ende-zu-Ende-Verschlüsselung erreicht werden kann“[170].

Das Bundeskartellamt hat der Ende-zu-Ende-Verschlüsselung in den Ermittlungen viel Raum gewidmet, da sie in der Öffentlichkeit häufig als das entscheidende Kriterium für Datensicherheit interpretiert wird. Auch wenn es nicht auf die Verschlüsselung allein, sondern auf das Zusammenwirken mit weiteren Sicherheitskriterien ankommt, hat die Verschlüsselung aufgrund der zeitweiligen Medienpräsenz im Zuge von unzutreffenden Angaben dazu durch einzelne Dienste eine herausgehobene Stellung erlangt. Ferner wird sie im Zusammenhang mit Diskussionen über Interoperabilität gerne als Beispiel für eine erhebliche Herausforderung genannt. Das Bundeskartellamt hat dieses sicherheitsrelevante Thema daher unter verschiedenen Aspekten näher beleuchtet.

aa) Gruppenchat und Videokonferenzen

Die Ermittlungsergebnisse lassen vermuten, dass jedenfalls **Textnachrichten** branchenweit verschlüsselt werden, da keiner der befragten Dienste angegeben hat, nicht zu verschlüsseln bzw. nicht verschlüsseln zu können. Stand der Technik ist - wie dargestellt - inzwischen die Ende-zu-Ende-Verschlüsselung, die idealerweise mit einer Transportverschlüsselung, die schon länger standardisiert ist, verbunden wird. Einige der befragten bekannten Dienste haben nur die **Transportverschlüsselung** implementiert. Da viele dieser Dienste bei Verbraucherinnen und Verbrauchern sehr beliebt sind, wäre hier eine zusätzliche Ende-zu-Ende-Verschlüsselung, die dem Stand der Technik entspricht, wünschenswert. Das BSI hat in seiner Publikation „Moderne Messenger – heute verschlüsselt, morgen interoperabel?“ den

---

[170] *BSI*, Moderne Messenger – heute verschlüsselt, morgen interoperabel?, November 2021, S. 10, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

hohen Aufwand beschrieben, den eine Verschlüsselung bei Gruppenchats derzeit verursacht.[171] Die meisten Dienste, die die Ende-zu-Ende-Verschlüsselung einsetzen, können dies bei der Kommunikation in Gruppen daher nicht sicherstellen, wie die Ermittlungen des Bundeskartellamts bestätigt haben. Wie bereits oben beschrieben, werden in der Branche verschiedene Protokolle oder auch individuelle Varianten des Double Ratchet-Protokolls eingesetzt. Diese Individualisierungen umfassen auch die Verschlüsselung als eine wesentliche Eigenschaft des Protokolls, gerade bei Interoperabilität, also über Messenger-Grenzen hinweg. Die Verschlüsselung gilt als das Hemmnis, das im Zusammenhang mit Interoperabilität am häufigsten angeführt wird. Der **MLS - Standard** wird als der Standard bezeichnet, der diese Hürde beseitigen könnte, sofern die übrigen Voraussetzungen – wie oben erwähnt geeignete Schnittstellen und eine angepasste Netzwerkinfrastruktur – geschaffen würden. Die Implementierung des MLS-Standards durch die Dienste ist abzuwarten. Eine schnelle Diffusion im Markt wäre wünschenswert.

Nicht nur beim Gruppenchat, auch bei **Videokonferenzen und Webinaren** unterliegt die Ende-zu-Ende-Verschlüsselung zur Zeit **technischen Einschränkungen**. Generell erfordert die Ende-zu-Ende-Verschlüsselung, dass die Teilnehmenden technisch in der Lage sind, die notwendigen Verschlüsselungsfunktionen bereitzustellen und anzuwenden. Alle Teilnehmenden müssen sich auf dem gleichen Sicherheitsniveau bewegen. Im Umkehrschluss kann eine E2E-Verschlüsselung nicht erreicht werden, sobald eine Teilnehmerin oder ein Teilnehmer das geforderte Sicherheitsniveau unterschreiten. Dieser Fall tritt z. B. dann ein, wenn Teilnehmende einen **WebRTC-Client** einsetzen. WebRTC ist ein direkt im Browser verankertes Protokoll, welches nur zwischen zwei Endpunkten Ende-zu-Ende verschlüsseln kann. Bei mehr als zwei Teilnehmenden einer Videokonferenz sind dies jeweils das Endgerät der Nutzerin oder des Nutzers mit dem Server des Dienstes, was den Anforderungen der Ende-zu-Ende-Verschlüsselung nicht mehr entspricht. Diese Aspekte spiegeln sich in den Ermittlungsergebnissen wider. Das WebRTC-Protokoll wird nach Angaben der befragten Branchenteilnehmenden am häufigsten eingesetzt, um Audio- und Videotelefonie zu verschlüsseln. Die

[171] Gruppenchats werden derzeit verschlüsselt, indem diese als Einzelchats aller Gruppenmitglieder untereinander verschlüsselt werden. Bei einer Gruppe mit n Mitgliedern gibt es n(n−1)/2 dieser Einzelchats, sodass der Verschlüsselungsaufwand quadratisch mit der Anzahl der Teilnehmer wächst und bei größeren Gruppen (>100 Teilnehmer) schnell zum Problem wird, vgl. *BSI*, Moderne Messenger – heute verschlüsselt, morgen interoperabel?, November 2021, S. 10, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

verwendenden Dienste haben auch zum größten Teil angegeben, Videokonferenzen in der Gruppe nicht Ende-zu-Ende verschlüsseln zu können.

Mit bestimmten **Funktionen**, die Nutzerinnen und Nutzer in Videokonferenzen gerne verwenden, kann die Ende-zu-Ende-Verschlüsselung derzeit technisch nicht verbunden werden: Wenn Nutzerinnen und Nutzer Aufnahmefunktionen („recording features“) verwenden, sich vom öffentlichen Telefonnetz oder einem standardisierten SIP-Videogerät in ein Meeting einwählen oder einen Assistenten verwenden, ist es den Diensten nicht möglich, Ende-zu-Ende zu verschlüsseln. Verbraucherinnen und Verbraucher können diese **Funktionen als „Indiz“**[172] interpretieren, dass die Ende-zu-Ende-Verschlüsselung zu hinterfragen ist, falls damit geworben wird oder sich bei der Nutzung die technischen Einschränkungen in Erinnerung rufen.

Große Videokonferenzen für **Webinare mit mehreren Hundert Teilnehmenden** können zur Zeit technisch nicht durch E2E-Verschlüsselung gesichert werden. In diesem Anwendungsfall ist es notwendig, zu prüfen, ob der anbietende Dienst einen Video-Dienst-Standort in Deutschland betreibt und dieser sicherheitstechnisch geprüft wurde (beispielsweise durch ein BSI C5 Testat). Transportverschlüsselung und der sichere Betrieb des Video-Dienstes in Deutschland sollten hierfür das Kriterium sein. Ferner ist darauf zu achten, dass die Identität der Teilnehmenden zweifelsfrei festgestellt werden kann („Authentisierung“). Ende-zu-Ende-Verschlüsselung stellt die Integrität der übermittelten Daten sicher. Ohne eine vorherige zweifelsfreie Authentisierung sorgt sie zwar für den Schutz der übermittelten Daten, stellt aber nicht sicher, wer diese Daten empfangen kann.

bb) Automatische Aktivierung

Gerade in Expertenkreisen wird gerne darauf verwiesen, dass nicht jede Kommunikation unbedingt verschlüsselt sein muss (z. B. das Kochrezept von Oma) oder dies nicht gewünscht ist (z. B. aus geschäftlichen Gründen). Es wird auch angeführt, dass E-Mail meistens unverschlüsselt genutzt wird. Sicherlich können IT-kompetente Verbraucherinnen und Verbraucher oder viele geschäftliche Nutzerinnen und Nutzer selbst entscheiden, wann sie verschlüsseln möchten und wann nicht und schätzen diese Freiheit.
Die meisten Verbraucherinnen und Verbraucher dürften sich des Umstands, dass hier **Entscheidungsmöglichkeiten** bestehen können, aber überhaupt nicht bewusst sein. Auch der notwendige Zeitaufwand für die entsprechende Recherche verbunden mit geringerer Wertschätzung für Verschlüsselung im Vergleich zu anderen Eigenschaften des gewünschten Messenger- und Video-

[172] Quelle: Ermittlungen. Vgl. *datenschutz notizen*, abrufbar unter: https://www.datenschutz-notizen.de/ende-zu-ende-verschluesselung-von-videokonferenzen-1825597/.

Dienstes können dazu führen, dass nicht verschlüsselt wird. Daher sollte gerade bei den kostenfreien Angeboten für Verbraucherinnen und Verbraucher eine **automatisch aktivierte Ende-zu-Ende-Verschlüsslung**, soweit dies technisch derzeit möglich ist, integriert werden, um die Datensicherheit weiter zu verbessern. Die Möglichkeit, die Ende-zu-Ende-Verschlüsselung abzustellen, z. B. für versierte Nutzerinnen und Nutzer, könnte vorgehalten werden.
Die Sicherheit einer Ende-zu-Ende-Verschlüsselung hängt insbesondere auch vom **Schlüsselmanagement** ab. Idealerweise sollten die Kommunizierenden allein über die Schlüssel verfügen, nicht der jeweilige Serverbetreiber. Denn wenn der Schlüssel auf dem Server des Dienstes erzeugt und dann an die Endgeräte verteilt wird, könnte der Dienstbetreiber mit Hilfe des ihm bekannten Schlüssels die versendeten Daten entschlüsseln. Zu den Diensten, die angegeben haben, dass der **Schlüssel lokal generiert wird und der private Schlüssel auf dem Endgerät** verbleibt, zählen viele freie Messenger-Clients, Open Source-Dienste und auch Video-Dienste.
Mit der Ausrichtung auf Geschäftskundinnen und -Geschäftskunden gehen gerade bei Video-Diensten viele Wahlmöglichkeiten der Nutzerinnen und Nutzer einher, wenn sie die Rolle des Host innehaben. Je nach gewähltem Modell können u.a. bestimmte Arten der Verschlüsselung und des Schlüsselmanagements implementiert werden. Ein führender Video-Dienst weist darauf hin, dass die Übernahme des Schlüsselmanagements (Key Management) die **Etablierung eines umfangreichen Prozesses zur Erzeugung, sicheren Aufbewahrung und sicheren Verteilung von Schlüsseln** bedarf. Verlust oder Kompromittierung des Master-Keys sei mit dem Verlust oder Kompromittierung des vollständigen Datenbestands im System gleich zu setzen. Nutzerinnen und Nutzer, die nicht fachkundig sind, sei somit angeraten, diese Aufgabe in die Verantwortung des ausgewählten Dienstes zu legen, gerade wenn sie als Administrator für die Teilnehmenden den sicherheitstechnischen Rahmen eines Austausches per Video festlegen.

c) Weitere Sicherheitsaspekte

Weitere Sicherheitsverfahren wie die Verschlüsselung der Daten auf dem Endgerät, die Ablageverschlüsselung, die Zwei-Faktor-Authentisierung oder das Erstellen von Sicherheitskopien werden in der Branche teilweise praktiziert. Die Zwei-Faktor-Authentisierung als Option und die Ablageverschlüsselung werden jeweils von der Hälfte der Dienste angeboten. Backups können bei zwei Dritteln der befragten Dienste erstellt werden. Die Verschlüsselung der Daten auf dem Endgerät wird von etwas weniger als zwei Dritteln der Befragten praktiziert. Bei allen diesen Sicherheitsverfahren erscheinen **Bemühungen um einen höheren Verbreitungsgrad** erforderlich.
Über eine **Zwei-Faktor-Authentisierung** können sich Nutzerinnen und Nutzer gegenüber ihrem Messenger- und Video-Dienste authentifizieren, wenn das jeweilige Messenger-System für dieses Verfahren geöffnet ist. Ihre Identität wird über zwei unterschiedliche Komponenten nachgewiesen, die

aus den Kategorien Wissen (z. B. Passwort, PIN, Antwort auf Sicherheitsfrage), Besitz (z. B. Smartcard, TAN-Liste) oder Biometrie (z. B. Fingerabdruck, Gesichtserkennung) stammen. Ähnlich wie bei der Ende-zu-Ende-Verschlüsselung müssen die Nutzerinnen und Nutzer diese Option aktiv wählen, wenn sie sie nutzen wollen. Hier wäre es für die Datensicherheit von Vorteil, wenn die Zwei-Faktor-Authentisierung vor allem bei Versionen von Anwendungen, die die Verbraucherinnen und Verbrauchern bevorzugen (z. B. kostenfreie Angebote, Probeangebote, die Basisfunktionen bereitstellen), voreingestellt wäre. Die Systeme, die das Verfahren bisher nicht integrieren, sollten sich um eine entsprechende Öffnung bemühen.

Bei den weiteren oben genannten Sicherheitsaspekten wäre ein höherer Verbreitungsgrad in der Branche ebenfalls wünschenswert. Die Verschlüsselung ist z.B. erst vollständig, wenn eine **Verschlüsselung der Daten auf dem Endgerät und auch insbesondere eine Ablageverschlüsselung** eingerichtet ist, also wenn auch die im Endgerät gespeicherten Daten verschlüsselt werden. Die Dienste, die hier aktiv sind, verwenden mit AES[173] und RSA[174] Verfahren, die dem Stand der Technik entsprechen. Außerdem sind bei den verschiedenen Messenger- und Video-Diensten teilweise **individuelle Regelungen und Voraussetzungen** zu beachten, was die Anwendung für die Nutzerinnen und Nutzer herausfordernd machen kann. Nicht selten ist die Verschlüsselung an die Art des Endgeräts oder Betriebssystems oder die gewählte Funktion oder Verschlüsselungsart gebunden. Verbraucherinnen und Verbraucher müssen genau hinschauen, ob bei der von ihnen gewählten Verwendung der App auf dem Endgerät verschlüsselt wird oder nicht. Einige Dienste verweisen auf die Möglichkeiten der Betriebssysteme, die von den Verbraucherinnen und Verbrauchern für eine Ablageverschlüsselung genutzt werden können

---

[173] Siehe auch Kapitel D.I.4.a, Advanced Encryption Standard (AES). Der Standard wird meistens zusammen mit anderen Verschlüsselungsverfahren implementiert, so z. B. auch als Basis der Transportverschlüsselung. Das AES-Verschlüsselungsverfahren ist eine Blockchiffre, deren Blockgröße von der AES Encryption Variante abhängt. Die Varianten der AES Verschlüsselung, AES-128, AES-192 und AES-256 enthalten in ihrer Bezeichnung die Länge des Schlüssels in Bit. Die sicherste AES Variante ist damit AES-256.

[174] Siehe auch Kapitel D.I.4.a. Das RSA-Verfahren (benannt nach den Entwicklern R. Rivest, A. Shamir und L. Adleman) ist eine bekannte asymmetrische Verschlüsselungsmethode. Mit dem RSA-Verfahren können digitale Daten über einen bestimmten Algorithmus umgerechnet und unkenntlich gemacht werden. Für die Entschlüsselung ist der sog. RSA-Schlüssel notwendig. Allerdings wird nicht derselbe Schlüssel zum Ver- und Entschlüsseln verwendet, sondern ein Schlüsselpaar. Aus einem privaten und dem öffentlichen Schlüssel. Der private Schlüssel muss für eine sichere RSA-Verschlüsselung geheim gehalten werden.

Bei **Sicherheitskopien** ist die Situation vergleichbar. Viele Dienste bieten diese Funktion an, allerdings mit unterschiedlichem Umfang und Voraussetzungen. Bei einigen Diensten müssen Verbraucherinnen und Verbraucher viel Zeit und Anstrengungen investieren, da diverse Einzelheiten und Voraussetzungen zu beachten sind.

Der Datensicherheit wäre es jedenfalls zuträglich, wenn die genannten Sicherheitsverfahren von denjenigen Diensten integriert würden, die dies bisher nicht tun. In jedem Fall sollte klar kommuniziert werden, welche Möglichkeiten die Nutzerinnen und Nutzer ggf. selbst ergreifen können, um ihre Daten auf dem Endgerät zu schützen und zu sichern.

3. Die Krux mit den (Meta-) Daten

Nicht nur zur technischen Sicherheit, sondern auch zur Datenverarbeitung hat das Bundeskartellamt den Messenger- und Video-Diensten Fragen gestellt. Dies sollte dem Überblick über die branchenweiten Praktiken dienen. Die Praktiken einzelner Messenger- und Video-Dienste werden seit langem intensiv öffentlich diskutiert und kritisiert und waren teils auch Gegenstand behördlicher Verfahren. Ob und inwieweit branchenweit darüber hinaus weiterer Untersuchungsbedarf im Hinblick auf rechtliche Fragen bestehen könnte, sollte durch die Ermittlungen im Rahmen der Sektoruntersuchung abgeschätzt werden können.

Das Bundeskartellamt hat für die Zwecke der Sektoruntersuchung zum Thema „Datenverarbeitung“ die Datenkategorien „Persönliche Daten“, „Geräte- und Konfigurationsdaten“, „Standort- und Bewegungsdaten“, „Kontakte/Daten Dritter“, „Gruppenmitgliedschaften“, „Nutzungsverhalten“ und „Inhalte“ gebildet (siehe Abbildung 9 in Kapitel D.II.4). Diese Kategorien sollten jeweils unverschlüsselte, verschlüsselte aber auch (teil-)anonymisierte, gehashte, ergänzte, angereicherte oder generierte Daten umfassen.

Nicht ausdrücklich gekennzeichnet wurden dabei die sog. Meta-Daten. **Meta-Daten** sind strukturierte Daten, die Informationen über Merkmale anderer Daten enthalten.[175] Sie umfassen beispielsweise Informationen darüber, wann jemand online ist und wie viele Geräte er verwendet, welche Kontakte bestehen und welche IP-Adressen diese haben.[176] Bei der Kommunikation über Messenger- und Video-Dienste fallen immer Meta-Daten an. Das kann beispielsweise technische Ursache haben und betrifft z. B. den Server, der Zeitpunkt und Zeitdauer der Verbindungen mit den Clients der Nutzerinnen und

---

[175] Vgl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Metadaten.

[176] Vgl. z. B. *Initiative Freie Messenger*, abrufbar unter: https://www.freie-messenger.de/geheimnisse/privat/.

Nutzer registriert.[177] Bei anderen (Meta-) Daten bestehen Spielräume. Ihre Erfassung dient lediglich internen Zwecken der Messenger- und Video-Dienste und könnte vermieden werden.

Meta-Daten können von Messenger- und Video-Diensten zu verschiedenen **Zwecken** genutzt werden, z. B. um die Funktionsweise des Dienstes zu verbessern. Sie können aber auch dazu dienen, Nutzerprofile anzulegen oder personalisierte Werbung zu platzieren. Wie eingangs dieses Kapitels bereits erwähnt, gelten einzelne populäre Dienste in der Öffentlichkeit als Inbegriff eines Geschäftsmodells, bei dem Daten für eigene Werbezwecke, insb. **personalisiere Werbung und Bildung von Nutzerprofilen oder zur Weitergabe an Dritte** erfasst werden.

Ergebnis der Ermittlungen des Bundeskartellamts war, dass fast alle der Messenger- und Video-Dienste nach eigenen Angaben Daten für die Funktionalität des Dienstes sammeln. Dies betrifft vor allem persönliche Daten und Geräte-/Konfigurationsdaten. Mehr als die Hälfte der Dienste erfasst auch Daten zum „Nutzungsverhalten", „Gruppenmitgliedschaften", „Kontakte/Daten Dritter" und „Inhalte". Immerhin noch rd. ein Drittel der Dienste sammelt „Standort-/Bewegungsdaten" der Nutzerinnen und Nutzer für die Funktionalität des Dienstes. Der Umgang mit Kontakten der Verbraucherinnen und Verbraucher und Daten Dritter durch die Dienste wird beim Hochladen des Kontaktverzeichnis virulent und ist Gegenstand einer rechtlichen Prüfung im folgenden Kapitel D.III.4.

Bei einem weiteren viel diskutierten Thema – der **Weitergabe von Daten an Dritte** – ging es ebenfalls darum, einen branchenweiten Überblick zu gewinnen, da detaillierte Analysen nur Gegenstand von Einzelverfahren, ggf. auch auf Basis anderer Rechtsgrundlagen, sein können und auch bereits waren oder sind. Gefragt wurde für die Zwecke der Sektoruntersuchung insbesondere nach der **Weitergabe von Daten an die großen Internetkonzerne**. Nur jeweils ein Dienst hat im Rahmen der Befragung angegeben, persönliche Daten (Zoom) bzw. Geräte-/Konfigurationsdaten an Facebook (inzwischen firmierend unter „Meta") weiterzugeben, teilweise unter Hinweis auf die explizite Einwilligung der Nutzerinnen und Nutzer. Die Datenweitergabe an Google wurde etwas häufiger bestätigt. Gleiches gilt für Datenanalysten. Ansonsten werden den Angaben zufolge von einzelnen Dienste Daten an Subunternehmer, Strafverfolgungsbehörden oder „Geschäftspartnerinnen und – partner" übertragen. Weitergegeben werden danach teilweise persönliche Daten, Geräteinformationen und Nutzerverhaltensdaten. Da unter den Branchenteilnehmenden – wie bereits mehrfach erwähnt – einige Großkonzerne sind, die auf Märkten, die das Messaging und Videoconferencing ebenfalls betreffen (z. B.

---

[177] Sollen Meta-Daten 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 Briar. Vgl. *Briar*, abrufbar unter: https://briarproject.org/).

Betriebssysteme, Kommunikationstechnik) eine starke Position haben, verdient die **interne Datenweitergabe** besondere Aufmerksamkeit.

Informationen über Zwecke der Datenerfassung und Datenweitergabe stehen den Verbraucherinnen und Verbrauchern nicht in einer leicht zugänglichen Weise zur Verfügung.[178] Grundsätzlich sollte in der **Datenschutzerklärung** beschrieben werden, in welchem Umfang Meta-Daten erfasst und wann sie gelöscht werden. Allerdings erfordert deren Studium einigen Zeitaufwand und die Bereitschaft, sich durch tendenziell schwer lesbare Texte zu kämpfen. Nach Erfahrungen des Bundeskartellamts in anderen Sektoruntersuchungen wird von den Verbraucherinnen und Verbrauchern meistens nicht ausreichend Zeit investiert, um alle Inhalte zu erfassen und Anbietende gehen oft nicht mit erforderlicher Sorgfalt an die Formulierung der entsprechenden Texte.[179] Die **Datensparsamkeit eines Dienstes** könnte aus weiteren Indizien abgeleitet werden, deren Erschließung von den Nutzerinnen und Nutzern aber auch einige Anstrengungen verlangt. Das **Geschäftsmodell** könnte als eine Art erstes **Indiz für den Zweck der Datenerfassung** und das Ausmaß der Datenweitergabe gelten. Danach gäbe die Verwendung der Daten für Werbezwecke Anlass zu Bedenken. Aber auch das Geschäftsmodell ist den Verbraucherinnen und Verbrauchern bei dem Großteil der Messenger- und Video-Dienste nicht in ausreichendem Maße bekannt. Zusätzlich könnte auch ein **einsehbarer Source Code**[180] Aufschluss über die Datensparsamkeit eines Dienstes geben. Allerdings erfordert die Analyse hier - wie bereits erläutert - natürlich nicht nur den Zugang zur Information, sondern insbesondere fachliche Kenntnis und Expertise und wieder viel Zeit, um Bewertungen vornehmen zu können.[181]

Zumindest im Vergleich besser verständlich könnte hier eine Auskunft **über den Standort des Servers** sein, die auch Rückschlüsse auf die Datensparsamkeit eines Messenger- und Video-Dienstes zulässt. Die Datenschutzgesetze sind weltweit unterschiedlich. Wenn der oder die Server eines Messenger- und Video-Dienstes in Deutschland oder der EU stehen, gilt die europäische DSGVO, mit der im Vergleich zu

---

178 Siehe zu den hohen Anforderungen an die Verbraucherinnen und Verbraucher bei der Informationssuche unter F.II. und G.II.2.

179 Vgl. *Bundeskartellamt*, Sektoruntersuchung Smart-TV, Juli 2020, abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_SmartTVs_Bericht.pdf?__blob=publicationFile&v=5. Siehe auch F.II.

180 In Kapitel D.I.1.b wurde dargelegt, dass Quellcode von Server und Client von etwas mehr als 40 Prozent der befragten Dienste einsehbar ist, und zwar vor allem bei den freien Messenger-Clients, Open Source-Diensten und Dienste, welche explizit mit Datenschutz werben.

181 Vgl. *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.

anderen Jurisdiktionen hohe Anforderungen an den Datenschutz einhergehen. Allerdings kann nicht davon ausgegangen werden, dass dieser Zusammenhang allen Verbraucherinnen und Verbrauchern bekannt ist und Interesse dafür besteht. Außerdem gilt auch hier, dass die Information gesucht werden muss, da sie im Allgemeinen nicht zentral auf den Internetseiten von Messenger- und Video-Diensten platziert ist.

Die Ermittlungen des Bundeskartellamts lassen vermuten, dass eine deutliche Mehrheit der befragten Messenger- und Video-Dienste ihre Daten außerhalb der EU speichert. Sieben Dienste haben explizit angegeben mindestens eine Datenkategorie nur in den USA zu speichern. Einige Dienste unterhalten Speicher-Infrastrukturen in der EU und in Drittländern, insb. den USA. Es blieb teilweise unklar, wohin Daten der EU-Bürgerinnen und Bürger transferiert werden.

Aufgrund der **unterschiedlichen Datenschutzstandards in der Europäischen Union und den USA**, die gerade in der Digitalwirtschaft wirtschaftlich eng verbunden sind, kommt der rechtlichen Bewertung dieser Frage eine besondere Bedeutung zu. Dies verdeutlichen auch andauernde Diskussionen und Aktivitäten in der (Fach-) Öffentlichkeit. Das Bundeskartellamt greift diesen Aspekt daher ihn einer gesonderten rechtlichen Analyse auf (siehe dazu den folgenden Abschnitt D.III.4).

Ein wesentlicher Aspekt von sicheren Messenger- und Video-Diensten vor diesem Hintergrund ist auch das **Löschen** der Daten, was in der Branche nicht einheitlich gehandhabt wird, wie die Ermittlungsergebnisse zeigen. Es bestehen nicht nur zwischen den Messenger- und Video-Diensten große Unterschiede. Auch intern können sich die Praktiken bei Messenger- und Video-Diensten nach Art der Datenkategorie, nach geschäftlicher oder privater Nutzung oder nach Art der Funktion (Videoaufnahmen, Sprachnachrichten oder andere Inhalte) unterscheiden.

Immer wenn **Nutzer-Konten** angelegt werden müssen, um einen Dienst verwenden zu können, werden von den Verbraucherinnen und Verbrauchern umfangreiche Dateneingaben verlangt. Demgegenüber existieren Dienste, bei denen keine Konten angelegt werden müssen. Wer sich für diese entscheidet, kann die Preisgabe der persönlichen Daten so eingeschränken. Wenn es um das **Löschen eines Kontos** geht, entscheiden Serveradministratorinnen und -administratoren oder Nutzerinnen und Nutzer über den Vorgang. Wenn Open Source-Dienste eingesetzt werden, stellt sich die Frage oft nicht, da Konten erst gar nicht angelegt werden müssen. Einige Dienste löschen Daten automatisch nach Vertragsende oder Kontoauflösung, andere auch auf Wunsch der Nutzerinnen und Nutzer.

Schließlich beeinflusst auch die **Einbindung in das Betriebssystem**, was mit den Meta-Daten geschieht. Selbst wenn Meta-Daten seitens des Dienstes zeitnah gelöscht werden, können diese gleichwohl durch das Betriebssystem des Endgeräts, bei Mobilgeräten und insbesondere 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.

Mit Inkrafttreten des Digital Markets Act am 1. November 2022 könnte die Datenverarbeitung durch die Interoperabilitätsverpflichtung von Gatekeepern noch mehr in den Fokus geraten. Wenn Messenger-übergreifender Austausch praktiziert ist und die Daten der Nutzerinnen und Nutzer durch mehrere Hände gereicht werden, steigen die Anforderungen an die Datensicherheit. Verantwortlichkeiten werden geklärt werden müssen (siehe dazu Kapitel F.IV.4) Für die Verbraucherinnen und Verbrauchern dürfte die (datenschutzrechtliche) Einschätzung von Messenger- und Video-Diensten noch herausfordernder werden als sie es jetzt schon ist.

4. Rechtliche Einordnung

Wie bei der Erörterung der einzelnen Sicherheitskriterien und der Datenverarbeitung bereits angedeutet, können die genannten Praktiken beim Umgang mit den Daten nicht nur ganz praktisch zu Sicherheitsdefiziten führen. Sie können auch gegen geltendes Verbraucherrecht verstoßen. Die Analyse ausgewählter Rechtsfragen ist Gegenstand dieses Kapitels.
Den rechtlichen Rahmen bilden das Gesetz gegen den unlauteren Wettbewerb und die Datenschutzgrundverordnung. Zusätzlich wird in diesem rechtlichen Zusammenhang (nochmals) kurz auf die Reichweite des Instruments der Sektoruntersuchung verwiesen. Anschließend geht es um die konkreten Rechtsfragen. Das Bundeskartellamt konzentriert sich dabei auf Aspekte, die für die Verbraucherinnen und Verbraucher beim Messaging und bei Videokonferenzen besonders wichtig sind und auf die sie besonderes Augenmerk richten sollten und können. Nach einer kurzen Einführung zum rechtlichen Rahmen (dazu unter a)) werden drei rechtliche Fragestellungen aufgegriffen. Dies betrifft zum einen den Umgang mit den Kontakten der Verbraucherinnen und Verbraucher, wenn das Kontaktverzeichnis hochgeladen und synchronisiert wird (dazu unter b)). Zum anderen wird erörtert, wie ein internationaler Datentransfer einschließlich Datenspeicherung der Dienste aussehen muss, wenn die aktuelle Rechtsprechung auf Basis der DSGVO berücksichtigt wird (dazu unter c)). Abschließend geht es um lauterkeitsrechtliche Verstöße und die Frage, ob die Dienste das

Transparenzgebot einhalten oder die Verbraucherinnen und Verbraucher durch das Vorenthalten von Informationen in die Irre führen (dazu unter d)).

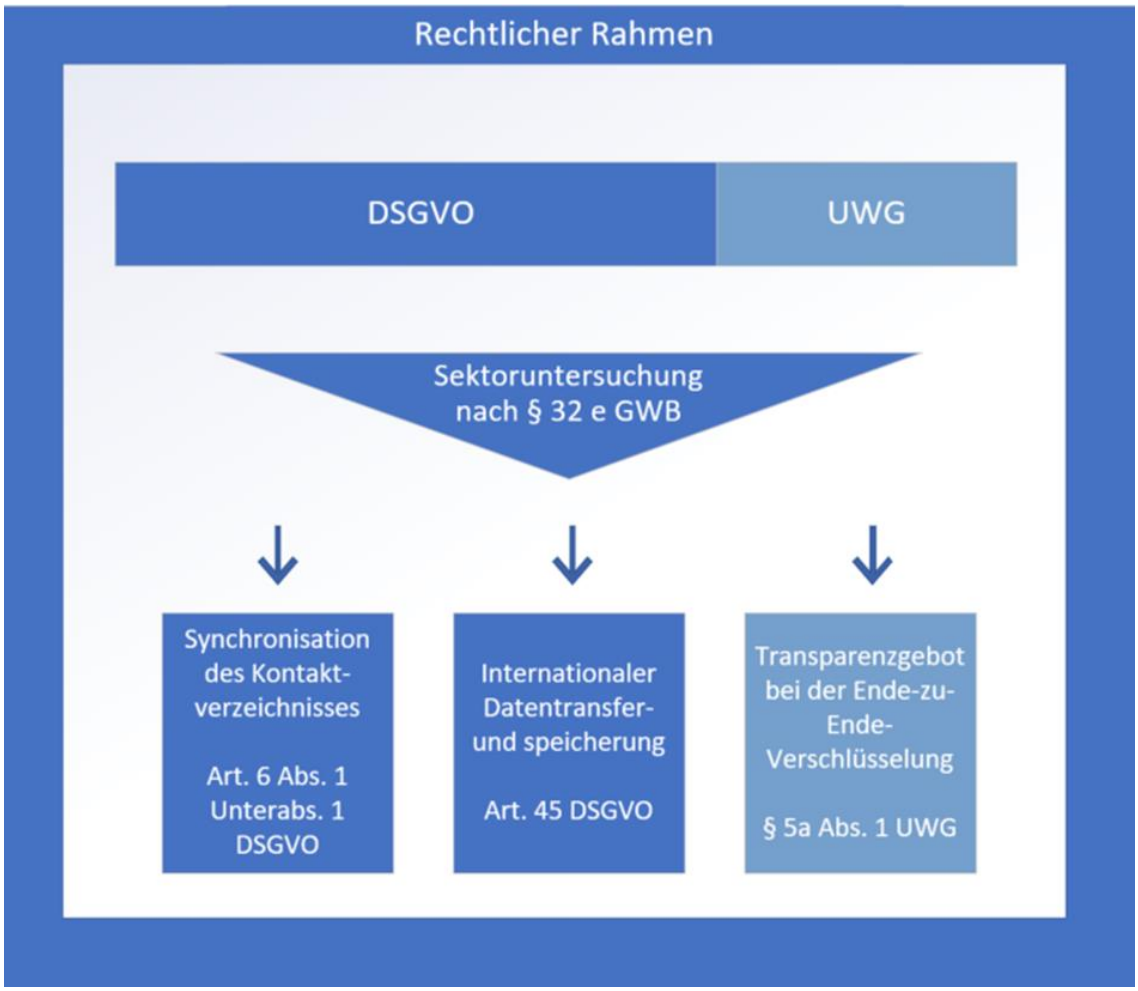


Abbildung 12: Rechtlicher Rahmen und rechtliche Untersuchungsthemen

a) Rechtlicher Rahmen

Die Praktiken der Messenger- und Video-Dienste müssen sich an den Bestimmungen des **UWG** messen lassen. Es hat gemäß § 1 Abs. 1 UWG zum Ziel, nicht nur Mitbewerber und sonstige Marktteilnehmer, sondern auch Verbraucherinnen und Verbraucher vor unlauteren geschäftlichen Handlungen zu schützen. Nach § 1 Abs. 2 UWG ist auch das Interesse der Allgemeinheit an einem unverfälschten Wettbewerb schützenswert. In den Gesetzesmaterialien zu den neuen Befugnissen des Bundeskartellamts gemäß § 32e Abs. 5 GWB wird das UWG ausdrücklich erwähnt.
Einschlägige Rechtsgrundlagen sind im Wesentlichen § 5 Abs. 1 UWG (irreführende geschäftliche Handlungen) und § 5a Abs. 1 UWG (Irreführung durch Unterlassen).
Als weitere Rechtsgrundlage findet die **DSGVO** seit dem 25. Mai 2018 in Deutschland und der gesamten Europäischen Union Anwendung. Die DSGVO ist aktuell das für die Einordnung von

Datenschutzverstößen mit Abstand wichtigste Regelwerk und bildet auch in den nachfolgenden Ausführungen den wesentlichen Prüfmaßstab in Datenschutzfragen. Entscheidend für die Anwendbarkeit der DSGVO ist die „Verarbeitung“ sog. „personenbezogener Daten“ (Art. 4 Nr.1 DSGVO). Das Bundeskartellamt kann in der Sektoruntersuchung Messenger- und Video-Dienste allerdings nicht Einzelfälle unter die genannten Vorschriften subsumieren und dabei alle in den Blick genommenen Messenger- und Video-Dienste einbeziehen. Denn die Prüfungstiefe einer verbraucherrechtlichen Sektoruntersuchung als beratendes und analysierendes Instrument ist gegenüber einem Verwaltungsverfahren im Sinne von § 54 Abs. 1, Abs. 2 Nr. 2 GWB, das sich *gegen* ein Unternehmen richtet, begrenzt. So wäre es für den **gerichtsfesten Nachweis eines Verstoßes gegen Verbraucherrecht** durch einen bestimmten Messenger- und Video-Dienst insbesondere erforderlich, die konkreten Verhältnisse im Einzelfall sowie ggf. auch die jeweiligen Erwartungen der Verbraucherinnen und Verbraucher aufzuklären.

Eine solche Nachweisführung gegen ein Unternehmen im Einzelfall würde die Möglichkeiten der vorliegenden Sektoruntersuchung übersteigen. Für die Verfolgung der Verstöße wäre ein **Verwaltungsverfahren**, das sich gegen ein einzelnes Unternehmen richtet, das richtige Instrument. Dort stünden den betroffenen Messenger- und Video-Diensten auch entsprechende Verteidigungsrechte zu. Zudem könnten in der Entscheidung zu einem solchen Verfahren in größerem Umfang Betriebs- und Geschäftsgeheimnisse angeführt werden als es in einem Sektoruntersuchungsbericht möglich ist, der für die allgemeine Öffentlichkeit bestimmt ist. Gleiches gilt ggf. für Verpflichtungszusagen der Unternehmen, die in einem Verwaltungsverfahren zur Lösung entgegengenommen werden können. Dem Bundeskartellamt wurden im Rahmen der 9. GWB-Novelle jedoch derartige Durchsetzungsbefugnisse im Verbraucherschutz zunächst bewusst nicht übertragen.

b) Synchronisation des Kontaktverzeichnisses

Nach dem Ergebnis der Ermittlungen synchronisiert fast ein Drittel der befragten Messenger- und Video-Dienste grundsätzlich das Kontaktverzeichnis der Nutzerinnen und Nutzer, darunter auch weit verbreitete Dienste wie Facebook Messenger, Skype, Snapchat, Threema, WhatsApp und Zoom (siehe zu den Ermittlungsergebnissen D.II.2.b)). Dabei werden die **Telefonnummern der Kontaktpersonen der Nutzerinnen und Nutzer** erfasst, nicht zwingend unmittelbar auch deren weiteren Kontaktinformationen. Die Nutzerinnen und Nutzer müssen diesem Vorgang, der später dann automatisch in Abständen wiederholt wird, zuvor zustimmen.

Solche Kontaktpersonen der Nutzerinnen und Nutzer, die den Dienst nicht nutzen („Nicht-Nutzerin“ bzw. „Nicht-Nutzer“), deren Telefonnummern aber im synchronisierten Kontaktverzeichnis enthalten ist, stimmen deren Erhebung notwendigerweise nicht gegenüber dem betreffenden Messenger- und Video-Dienst zu, da er ihnen bis dato unbekannt ist. Die Einwilligung der Nicht-Nutzerinnen und -Nutzer

lässt sich auch nicht dadurch konstruieren, dass sie konkludent bei der Weitergabe einer Telefonnummer erfolgt. Nicht-Nutzerinnen und Nicht-Nutzern lässt sich nicht unterstellen, schon bei der Weitergabe der Telefonnummer zu antizipieren, dass diese über den Eintrag in ein Kontaktverzeichnis eines Mobiltelefons durch einen Synchronisierungsprozess an einen oder mehrere Messenger- und Video-Dienste gelangt.[182]

Der Dienst ist aber auch in Bezug auf die Synchronisierung der Telefonnummer von Nicht-Nutzerinnen und -Nutzern für die Einhaltung der DSGVO verantwortlich und benötigt insofern für diesen Verarbeitungsvorgang eine anderweitige Legitimation. Er kann sich nicht darauf zurückziehen, die Nutzerin oder der Nutzer sei selbst verantwortlich, die Einwilligung von den Nicht-Nutzerinnen und -Nutzern unter den eigenen Kontakten einzuholen, und er als Dienst insoweit lediglich Auftragsverarbeiter.

Dass dem betreffenden Messenger- und Video-Dienst in diesem Zusammenhang die Rolle eines **Verantwortlichen im Sinne von Art. 4 Nr. 7 DSGVO** und nicht bloß eines Auftragsverarbeiters (für die Nutzerin oder den Nutzer) nach Nr. 8 zukommen dürfte, ergibt sich aus Folgendem:

Verantwortlicher ist diejenige Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogenen Daten entscheidet. Nach den von der Art. 29 - Datenschutzgruppe entwickelten Grundsätzen geht es bei der Abgrenzung zum Auftragsverarbeiter um die Zuordnung der Verantwortlichkeit in typisierter Form. Deshalb ist darauf abzustellen, warum der Prozess der Datenverarbeitung stattfindet und wer ihn initiiert hat. Verantwortlichkeit soll dort alloziert werden, wo der faktische Einfluss liegt; nur technische Fragen können auf den Auftragsverarbeiter delegiert werden, nicht essentielle Fragen wie „welche Daten sollen erhoben werden“.[183]

Die Einbeziehung von Telefonnummern der Nicht-Nutzerinnen und Nicht-Nutzer im Kontaktverzeichnis durch den Messenger- und Video-Dienst dient dazu, Nutzerinnen und Nutzern später Hinzutretende unter ihren Kontakten unmittelbar nach deren Registrierung automatisch anzuzeigen. Auch wenn sich dies in einem Mehrwert für die Nutzerinnen und Nutzer niederschlagen mag, liegt der **faktische Einfluss** über den gesamten Prozess beim Messenger- und Video-Dienst, der dieses Feature bei der Entwicklung seines Produkts erstellt hat und der die technischen Abläufe kontrolliert. Die Nutzerin oder der Nutzer hingegen können nicht einmal mit vertretbarem Aufwand in Erfahrung bringen, welche der eigenen

---

[182] Ablehnend auch AG Bad Hersfeld, Beschluss vom 20.03.2017, Az. F111/17 EASO, Tz. 96, 107.

[183] Vgl. Art. 29-Datenschutzgruppe, Opinion 1/2020, S. 40 ff.

Kontakte den Dienst bereits verwenden oder nicht. Die **datenschutzrechtliche Verantwortung** liegt also beim betreffenden Dienst.[184]

Zum rechtskonformen Handeln des Dienstes gehört in diesem Zusammenhang jedenfalls eine datenschutzrechtliche Legitimation nach Art. 6 Abs. 1 Unterabs. 1 DSGVO.

Die Telefonnummer der Nicht-Nutzerin oder des Nicht-Nutzers stellt ohne Weiteres ein personenbezogenes Datum im Sinne von Art. 4 Nr. 1 DSGVO dar. Ihr Hochladen und Speichern ist eine Verarbeitung nach Art. 4 Nr. 2 DSGVO. Selbst wenn ein Dienst neben der Telefonnummer keine weiteren Informationen über die Nicht-Nutzerin oder den Nicht-Nutzer erhebt, handelt es sich gleichwohl um ein personenbezogenes Datum, weil die Nicht-Nutzerin oder der Nicht-Nutzer bereits damit identifizierbar wird. So kann der Dienst weitere Informationen über sie oder ihn mittels eines Anrufs oder einer Recherche in sozialen Netzwerken recherchieren.[185] Der Personenbezug entfällt auch nicht dort, wo ein Dienst nach Erhebung der Telefonnummer der Nicht-Nutzerin oder des Nicht-Nutzers einen kryptografischen Hashwert erstellt und die Telefonnummer selbst anschließend unwiderruflich löscht. Dies gilt jedenfalls dann, wenn dieser Hashwert mit weiteren in einer Liste gespeichert wird, die wiederum mit denjenigen Nutzerinnen und Nutzern verknüpft ist, aus deren Kontakteverzeichnissen die ursprünglichen Telefonnummern stammen.[186] Messenger- und Video-Dienste können auf diese Weise die konkrete Nutzerin oder den konkreten Nutzer darüber informieren, sobald Nicht-Nutzerinnen und Nutzer unter ihren Kontakten zu Nutzerinnen und Nutzern werden, so dass ein Personenbezug besteht.

Eine Legitimation qua Einwilligung der Nicht-Nutzerin oder des Nicht-Nutzers nach Art. 6 Abs. 1 Unterabs. 1 Buchst. a) DSGVO scheidet wie gesehen aus. Alternativ kann sich die Legitimation aus Buchst. f) ergeben, wonach - verkürzt gesagt - die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder einer dritten Person in **Abwägung mit den Freiheitsrechten der betroffenen Dateninhaberin oder des betroffenen Dateninhabers** erforderlich ist. Die Herleitung einer Legitimation aufgrund berechtigter Interessen dürfte hier aber schwerfallen oder zumindest einen hohen Begründungsaufwand erfordern.

Eine erfolgreiche Begründung mag noch gelingen für das **kurzfristige Hochladen der Telefonnummern** aus dem Kontakteverzeichnis. Denn auf diese Weise lässt sich ermitteln, welche unter ihnen zu einem bereits beim Dienst registrierten Kontakt gehört, um es der Nutzerin oder dem Nutzer anschließend

---

[184] Vgl. ausführlich Data Protection Commission/Ireland, Entsch. vom 20.08.2021, Az. IN-18-12-2, Tz. 145 „*WhatsApp Ireland Limited*".

[185] Vgl. Data Protection Commission/Ireland, Entsch. vom 20.08.2021, Az. IN-18-12-2, Tz. 83, 91 „*WhatsApp Ireland Limited*".

[186] Europäischer Datenschutzausschuss, Bindende Entsch. nach Art. 65 DSGVO Nr. 1/2021 vom 28.07.2021, Tz. 156.

anzuzeigen. Werden die bei dieser Gelegenheit miterhobenen Telefonnummern der Nicht-Nutzerinnen und Nicht-Nutzer anschließend gelöscht, dürften deren Schutz-Interessen dasjenige des Dienstes an einer effizienten Vernetzungsmöglichkeit voraussichtlich nicht überwiegen.
Nicht ohne Weiteres gilt dies für das anschließende Speichern der Telefonnummer von Nicht-Nutzerinnen und Nicht-Nutzern, sei es in klarer oder gehashter Form. Der damit generierte Vernetzungsvorteil ist nur noch gering. Die spätere Unterrichtung der Nutzerin oder des Nutzers über neu hinzutretende Nutzerinnen und Nutzern unter seinen Kontakten kann nämlich dem Grunde nach auch ohne die in Rede stehende **langfristige Telefonnummer-Speicherung** erfolgen. Sobald die bisherige Nicht–Nutzerin oder der bisherige Nicht-Nutzer registriert ist und der Verarbeitung der Daten zugestimmt hat, kann sie oder er bei der nächsten Auslesung des Kontaktverzeichnisses als neue Nutzerin oder neuer Nutzer angezeigt werden. Bei - unterstellt - täglicher Synchronisierung dürfte der verbleibende zeitliche Verzug gegenüber der unmittelbaren Benachrichtigung nach erfolgter Registrierung der bisherigen Nicht-Nutzerin bzw. des bisherigen Nicht-Nutzers kaum ins Gewicht fallen. Werden die Telefonnummern der Nicht-Nutzerinnen und Nicht-Nutzer also vom Dienst gespeichert, geht er ein hohes Risiko ein, dass sein Interesse an einer effizienten Vernetzungsmöglichkeit und der Attraktivität seines Produkts von den Rechten der Nicht-Nutzerin oder des Nicht-Nutzers überwogen werden.

c) Internationaler Datentransfer / Datenspeicherung

Das Bundeskartellamt hat die Ermittlungen nicht nur auf die konkreten rechtlichen Untersuchungsthemen ausgerichtet. Es war auch bestrebt, einen umfassenden Überblick über den Prozess der Datenverarbeitung der Messenger- und Video-Dienste zu bekommen. Führende Dienste stehen in diesem Zusammenhang in ständiger Kritik. Daher erschien es geboten, auch die Praktiken der anderen Branchenteilnehmenden abzufragen. Auf diese Weise wurden auch Antworten der Dienste zur Frage der Datenspeicherung und damit auch zum Datentransfer erfasst.
Nach vorläufiger Auffassung des Bundeskartellamts gemäß den Ermittlungsergebnissen unterliegen einige Messenger- und Video-Dienste hier dem Risiko, sich nicht rechtskonform zu verhalten. Dies betrifft vor allem diejenigen Dienste, die die Daten deutscher Nutzerinnen und Nutzer in den USA speichern. Im Folgenden wird zunächst der geltende Rechtsrahmen erläutert (dazu unter aa), bevor anschließend - aufgrund der Ermittlungsergebnisse - auf die besonderen rechtlichen Anforderungen an Datentransfers in die USA eingegangen wird (dazu unter bb).

aa) Rechtliche Grundlagen des internationalen Datentransfers in der Europäischen Union

Der Schutz personenbezogener Daten von Bürgerinnen und Bürgern der Europäischen Union (EU) durch die Regeln der DSGVO geht über die EU-Grenzen hinaus. Die Messenger- und Video-Dienste - die

jeweiligen Verantwortlichen - müssen prüfen, ob die allgemeinen Voraussetzungen für einen Datentransfer – auch zum Zwecke der Datenspeicherung in einem Drittland – erfüllt sind.
So dürfen Daten in Länder außerhalb der EU und des Europäischen Wirtschaftsraums nur übermittelt werden, wenn sichergestellt ist, dass ein **angemessenes Datenschutzniveau** in dem so genannten Drittland herrscht (Art. 45 DSGVO). Gemäß Kapitel V DSGVO kann dieses Datenschutzniveau auf verschiedenen Wegen sichergestellt oder erreicht werden. Daten können auf Basis von sog. **Angemessenheitsbeschlüssen** transferiert werden.[187] Angemessenheitsbeschlüsse hat die Europäische Kommission derzeit mit Andorra, Argentinien, Faröer Inseln, Großbritannien, Guernsey, Israel, Isle of Man, Japan, Jersey, Kanada, Neuseeland, Südkorea, Schweiz und Uruguay.[188] Das sog. Datenschutzschild (EU-US Privacy Shield), das die EU mit den USA vereinbart hatte, ist hingegen nicht mehr in Kraft. Existiert kein Angemessenheitsbeschluss, bedeutet dies, dass das jeweilige Drittland oder eine Organisation kein angemessenes Schutzniveau bieten. Wenn trotzdem Daten übermittelt werden sollen, muss dies von weiteren Schutzmaßnahmen - **Garantien nach Art. 46 DSGVO** - begleitet werden. Der Datentransfer kann mit Standarddatenschutzklauseln oder verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules, BCR) sowie mit genehmigten Verhaltensregeln (Code of Conduct) /Zertifizierungsmechanismen abgesichert werden.[189]
Die **Standarddatenschutzklauseln** können von der Europäischen Kommission oder anderen europäischen Aufsichtsbehörden erlassen werden. Außerdem sind auch individuelle Vertragsklauseln möglich, um eine Datenübermittlung abzusichern. Die Europäische Kommission hat im Juni 2021 Standardvertragsklauseln erlassen.[190] Seit dem 27. September 2021 sind nur noch die aktuellen Klauseln zu verwenden. Standarddatenschutzklauseln anderer Aufsichtsbehörden und individuell ausgehandelte

---

[187] Vgl. *BfDi* zum internationalen Datentransfer, abrufbar unter: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Europa-Internationales/Internationaler_Datentransfer.html;jsessionid=4FF79D8D39D5B5ED7D0E9734B6AD8F99.intranet242.

[188] Vgl. *Europäische Kommission*, abrufbar unter: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de.

[189] Für Behörden sind weitere Mechanismen vorgesehen. Sie können z. B. internationale Abkommen nutzen oder eine Verwaltungsvereinbarung verwenden. Beide müssen den betroffenen Personen durchsetzbare Datenschutzrechte und Rechtsbehelfe gewähren. Der Europäische Datenschutzausschuss hat Leitlinien dazu erarbeitet. Behörden mit Strafverfolgungsfunktionen übermitteln Daten auf Grundlage des Bundesdatenschutzgesetzes.

[190] Siehe Durchführungsbeschluss EU 2021/914, abrufbar unter: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=de.

Klauseln müssen im europäischen Kreis abgestimmt und durch die EU-Kommission genehmigt werden.[191]

Wenn Daten in Drittländer übertragen werden sollen, können auch **verbindliche interne Datenschutzvorschriften (Binding Corporate Rules, BCR)** den Transfer absichern. Dieses Instrument wird vor allem von international tätigen Konzernen mit internem Datenfluss, auch in Drittländer, verwendet. Grundlage sind Regeln, wie mit personenbezogenen Daten umzugehen ist. Diese Regeln müssen mit durchsetzbaren Rechten für die betroffenen Personen verbunden sein. Sie müssen für die gesamte Unternehmensgruppe gelten, d. h. rechtlich bindend sein. Die jeweilige nationale Aufsichtsbehörde muss sich mit den europäischen Partnern abstimmen und die Genehmigung von der Europäischen Kommission einholen.[192] Ähnlich ist es bei branchenweiten **Verhaltensregeln** oder von der zuständigen Aufsichtsbehörde genehmigten **Zertifizierungsmechanismen**. Entsprechende Leitlinien sind beim Europäischen Datenschutzausschuss in Bearbeitung.

Wenn weder ein Angemessenheitsbeschluss noch geeignete Garantien existieren, kann eine Datenübermittlung in ein Drittland ausnahmsweise als **strenge Ausnahme nach Art. 49 DSGVO** zulässig sein. Dies ist auf besondere explizit genannte Konstellationen begrenzt, z. B. wenn die Datenübermittlung aus wichtigen Gründen des öffentlichen Interesses notwendig ist. Den Erläuterungen des Bundesbeauftragten für den Datenschutz zufolge ist Art. 49 eng auszulegen und darf nicht für regelmäßige Datentransfers genutzt werden, die eine Vielzahl an Personen betreffen.[193]

bb) Ermittlungsergebnisse im Lichte der aktuellen Rechtsprechung zum Datentransfer in die USA

Wie im vorausgegangenen Abschnitt bereits erwähnt, ist das Datenschutzschild – der Angemessenheitsbeschluss für die USA – nicht mehr rechtskräftig.

Der Europäische Gerichtshof hat im Sommer 2020 ein wegweisendes Urteil zum internationalen Datentransfer erlassen, was zunächst zu großer Unsicherheit führte, inwieweit eine datenbasierte

---

[191] Siehe *BfDi* zu Standarddatenschutzklauseln, abrufbar unter: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Europa-Internationales/Internationaler_Datentransfer.html;jsessionid=4FF79D8D39D5B5ED7D0E9734B6AD8F99.intranet242.

[192] Vgl. zum Genehmigungsverfahren bei verbindlichen internen Datenschutzvorschriften *Europäische Kommission*, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en.

[193] Vgl. *BfDI* zu Ausnahmen nach Art. 49 DSGVO unter: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Europa-Internationales/Internationaler_Datentransfer.html.

Zusammenarbeit mit den USA noch stattfinden kann. Im sog. **Schrems II-Urteil**[194] hatte der Europäische Gerichtshof bestätigt, dass personenbezogene Daten von Bürgerinnen und Bürgern der EU, die in ein Drittland übermittelt werden, dort einen „im Wesentlichen gleichwerten Schutz“ wie unter der europäischen DSGVO erhalten müssen. Der EuGH hat für das **US-amerikanische Schutzniveau** ein im Wesentlichen gleichwertiges Datenschutzniveau verneint.[195] Im Zuge dessen wurde der Angemessenheitsbeschluss der EU-Kommission zum EU-US-Datenschutzschild (Privacy-Shield-Beschluss 2016/1250) für ungültig erklärt. Unter dem Datenschutzschild dürfen personenbezogene Daten folglich nicht mehr in die USA übermittelt werden.

Demgegenüber hat das Gericht den Beschluss der EU-Kommission über **Standardvertragsklauseln und BCR** als geeignete Garantie für wirksam erklärt. Allerdings müssen dann **zusätzliche Maßnahmen** getroffen werden, die die Daten der Bürgerinnen und Bürger der EU vor dem unbeschränkten Zugriff der US-Sicherheitsbehörden bewahren. Die zusätzlichen Maßnahmen können grundsätzlich auf technischer, organisatorischer und / oder rechtlicher Ebene implementiert werden. Das Gericht betonte, dass diese dann im Drittland auch wirksam sein und praktisch zur Verfügung stehen müssen.

Außerdem können Daten weiterhin im **Ausnahmefall gemäß Art. 49 DSGVO** transferiert werden, sofern das von der DSGVO vorgesehene Regel-Ausnahme-Verhältnis beachtet und die in Art. 49 genannten Bedingungen erfüllt würden (z. B. Anforderungen an eine ausdrückliche, informierte und freiwillige Entscheidung).[196]

Eine Übergangsfrist hat das Gericht nicht eingeräumt.

Hintergrund des Verfahrens waren die Aktivitäten des Bürgerrechtlers und Datenschutzaktivisten Max Schrems, der seit einigen Jahren gegen Meta vorgeht. Am Beispiel der US-amerikanischen Plattform

---

[194] Rechtssache C-311/18 „Schrems II“, abrufbar unter: https://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=DE.

[195] Siehe *Der Bundesbeauftragte für den Datenschutz*, Informationsschreiben zur Auswirkung der Rechtsprechung des EuGH auf den internationalen Datentransfer (Rechtssache C-311/18 „Schrems“), 08. Oktober 2020, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Rundschreiben/Allgemein/2020/Rundschreiben-Informationen-Schrems-II.html?nn=339632.

[196] Siehe *Der Bundesbeauftragte für den Datenschutz*, Informationsschreiben zur Auswirkung der Rechtsprechung des EuGH auf den internationalen Datentransfer (Rechtssache C-311/18 „Schrems“), 08. Oktober 2020, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Rundschreiben/Allgemein/2020/Rundschreiben-Informationen-Schrems-II.html?nn=339632.

lässt er gerichtlich überprüfen, ob personenbezogene Daten von EU-Bürgerinnen und -Bürgern in Länder außerhalb der EU (und des EWR) übertragen werden dürfen.[197] 2015 wurde im Zuge eines solchen Verfahrens - sog. **Schrems I - Urteil**[198] des EuGH - das Safe Harbour-Abkommen, der Vorgänger des Privacy Shields - für ungültig erklärt.

Vor dem Obersten Gerichtshof Österreichs (OGH) ist seit Erlass des Urteils „Schrems II“ eine neue Beschwerde von Max Schrems gegen Meta verhandelt worden, die aber zur Frage rechtskonformer Datentransfers weniger Bezug hat.

Im Zuge des Schrems II – Urteils müssen die Verantwortlichen innerhalb der Dienste ihre Datenübermittlungen in Länder außerhalb der Europäischen Union überprüfen und ggf. auf eine neue Grundlage stützen. Wenn geeignete Garantien nach Art. 46 DSGVO eingesetzt werden, muss überprüft werden, ob und welche zusätzlichen Maßnahmen notwendig sind, um die Daten im Drittland zu schützen. Das Ergebnis der Prüfung ist zu dokumentieren. Die **Dokumentation** muss so gestaltet sein, dass die Aufsichtsbehörde nachvollziehen kann, dass die Vorschriften der DSGVO eingehalten werden. Wenn sich als Ergebnis der Prüfung ergibt, dass der Datentransfer unzulässig ist, dieser aber fortgeführt wird, ist dies dem Bundesbeauftragten für den Datenschutz zu melden.

Nach den Ergebnissen der Ermittlungen speichert eine Reihe von Diensten mindestens eine Datenkategorie nur in den USA (siehe D.II.3.).[199]

Da der US-Datenschutzschild durch den Europäischen Gerichtshof für unwirksam erklärt wurde, wäre der Datentransfer in die USA unzulässig, sofern er nicht durch geeignete Garantien einschließlich zusätzlicher Maßnahmen abgesichert wird. Der Verdacht auf unzulässige Praktiken im internationalen Datentransfer gemäß DSGVO kann an dieser Stelle nicht ausgeräumt werden. Dem Bundeskartellamt

---

197 Vgl. Handelsblatt, abrufbar unter: https://veranstaltungen.handelsblatt.com/cybersecurity/internationaler-datentransfer-nach-schrems-ii/.

198 Rechtssache C-362/14 „Schrems I“, abrufbar unter: https://curia.europa.eu/juris/liste.jsf?language=de&num=C-362/14.

199 Soweit darüber hinaus ein Viertel der Befragten erklärt hat, mindestens eine Datenkategorie in einer öffentlichen Cloud von außerhalb der EU ansässigen Technologie-Unternehmen zu speichern, kann hieraus nicht ohne Weiteres auf eine Datenspeicherung in den USA geschlossen werden. So hat das OLG Karlsruhe in vergaberechtlichem Zusammenhang entschieden, allein aufgrund der Tatsache, dass ein Tochterunternehmen eines US-amerikanischen Konzerns beauftragt wird, könne man nicht davon ausgehen, dass es aufgrund der Konzernbindung zu rechts- und vertragswidrigen Weisungen an das Tochterunternehmen kommen wird bzw. das europäische Tochterunternehmen durch seine Geschäftsführer gesetzeswidrigen Anweisungen der US-amerikanischen Muttergesellschaft Folge leisten wird, vgl. OLG Karlsruhe, Beschl. v. 07.08.2022, Az. 15 Verg 8/22, openJur 2022, 16869.

liegen keine Informationen vor, inwieweit der Datentransfer in die USA von den betroffenen Messenger- und Video-Diensten mit Garantien und zusätzlichen Maßnahmen abgesichert wird. Zwar bietet die Europäische Kommission eine Übersicht[200] an, welche Unternehmen über genehmigte verbindliche interne Datenschutzvorschriften (BCR) verfügen. Auf dieser Liste war aber nur einer der vom Bundeskartellamt befragten Messenger- und Video-Dienste zu finden, der in den Ermittlungsergebnisse allerdings - zumindest nicht explizit - angegeben hatte, Daten von EU-Bürgerinnen und Bürgern in den USA zu speichern.
Die Verwendung von Standardvertragsklauseln und die vom EuGH geforderten zusätzlichen Maßnahmen haben die Dienste in ihren Antworten nicht thematisiert.

cc) Neuer Datenschutzschild auf dem Weg?

Seit Erlass des Schrems-II-Urteil vom Juli 2020 haben die EU und die USA über einen **neuen Privacy Shield** verhandelt. Er soll die Weitergabe persönlicher Daten von EU-Bürgerinnen und Bürgern an in den USA ansässige Empfänger ermöglichen. Ende März 2022 wurde eine „grundsätzliche Einigung“ erzielt. Einen Rechtstext und nähere Informationen gibt es aktuell noch nicht. In einer gemeinsamen Erklärung teilten beide Seiten mit, dass neue Regeln den Zugriff der US-Geheimdienste auf die Daten auf das beschränken würden, was notwendig und verhältnismäßig sei, um die definierten nationalen Sicherheitsziele verfolgen zu können. Zudem solle es einen unabhängigen Rechtsschutzmechanismus geben, der Beschwerden von EU-Bürgerinnen und Bürgern über den Datenzugriff der US-Geheimdienste untersuche und Abhilfemaßnahmen anordnen könne.[201]
Es bleibt somit abzuwarten, wann Datentransfers in die USA auf eine neue rechtliche Grundlage gestellt und welche Regelungen im Detail vereinbart werden.

d) Informationsmängel im Zusammenhang mit der Ende-zu-Ende-Verschlüsselung

Das Bundeskartellamt hat der Verschlüsselung vor allem als wesentliches technisches Element für die Sicherheit der Daten und damit auch für den Schutz der Daten viel Raum in den Ermittlungen gewidmet. In der Vergangenheit sind immer wieder Sicherheitsmängel bei Messenger- und Video-Diensten im

---

200 Siehe *Europäische Kommission,* abrufbar unter: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en.

201 Siehe Gemeinsame Erklärung der *Europäischen Kommission* und der *Vereinigten Staaten* zum Transatlantischen Datenschutzrahmen vom 25. März 2022, abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/IP_22_2087. Siehe auch *MDR*, abrufbar unter: https://www.mdr.de/nachrichten/welt/politik/datenschutz-abkommen-einigung-europa-usa-privacy-shield-100.html.

Zusammenhang mit der Verschlüsselung thematisiert worden. Wie in D.I.4.a)cc) bereits erläutert, war bei einem Videokonferenzanbieter eine individuelle Interpretation **der Ende-zu-Ende-Verschlüsselung** aufgefallen, die nicht der eigentlichen technischen Definition der Ende-zu-Ende-Verschlüsselung entspricht. Möglicherweise hat die Verschlüsselung aufgrund dieser zeitweiligen Medienpräsenz ihre herausgehobene Stellung unter den Sicherheitsaspekten erlangt. Sie wird in der Öffentlichkeit jedenfalls häufig als das entscheidende Kriterium für Datensicherheit wahrgenommen, während andere in diesem Bericht beschriebene Aspekte öffentlich nicht erwähnt werden. Im Zusammenhang mit Diskussionen über Interoperabilität hat die Verschlüsselung ebenfalls regelmäßig als Beispiel hergehalten, um die besonderen Herausforderungen einer solchen Maßnahme beispielhaft zu veranschaulichen. Auch aus diesen Gründen hat das Bundeskartellamt das Thema „Verschlüsselung“ nicht nur sicherheitstechnisch, sondern auch im Hinblick auf eine eigenständige rechtliche Analyse untersucht.

Schließlich ist die Verschlüsselung auch ein Beispiel für die weitreichenden **Informationsmängel**, denen sich die Verbraucherinnen und Verbraucher in einer technisch basierten Branche wie den Messenger- und Video-Diensten gegenübersehen und die von den beteiligten Behörden angegangen werden müssen, um nachhaltige Verbesserungen im Verbraucherschutz erzielen zu können.

Das Bundeskartellamt hat im Jahr 2020 - als erste Überlegungen zur Sektoruntersuchung Messenger- und Video-Dienste aufkamen – eine **Recherche mittels einer Stichprobe** von rd. 40 Messenger-Diensten[202] durchgeführt, wie die Verbraucherinnen und Verbraucher durch die Dienste über Sicherheitsaspekte, insb. die Verschlüsselung, informiert werden. Damals ergab sich ein unübersichtliches und unklares Bild. Fast alle Messenger-Dienste hatten Informationen zu den unternehmensbezogenen Sicherheitsstandards auf ihren Websites veröffentlicht. Teilweise waren die Informationen transparent dargestellt und verständlich, teilweise waren sie jedoch kaum zu durchdringen. Der Großteil der Messenger-Dienste führte auf ihren Homepages eigene Rubriken zum Thema Sicherheit. Diese enthielten dann in unterschiedlicher Tiefe Informationen zum Verfahren der Verschlüsselung. Teilweise fanden sich unter der entsprechenden Rubrik weitere Verlinkungen, die zu weiteren Informationen führen. Auffallend war, dass die meisten Dienste lediglich Schlagworte angaben, deren konkreter Inhalt sich nicht direkt entnehmen ließ. So hatten beispielsweise Dienste mit einer „sicheren bzw. starken Verschlüsselung“ geworben. Erst mit weiterer Recherche oder durch Lesen der Datenschutzrichtlinien klärte sich z. B. die Art und der Grad der Verschlüsselung. In dem Zusammenhang kam es auch gelegentlich zu undurchsichtigen Verweisen. So war insbesondere bei den Angaben führender Messenger-Dienste nicht immer zu erkennen, wann sich die Angaben nur auf die

[202] Die in der Stichprobe enthaltenen Dienste entsprachen nicht vollumfänglich den späteren Adressaten bzw. den Diensten, die den Fragebogen beantwortet haben.

Nutzung des Messenger-Dienstes bezogen und wann sie für den Account generell relevant waren. Darüber hinaus wurden oft allgemeine Datenschutzhinweise von speziellen Informationen zur Sicherheit der Kommunikation nicht getrennt, was den Informationsfluss erschwerte. So ließen sich z. B. bei den Messenger-Diensten von einzelnen Betriebssystemherstellern Informationen einzig aus der Datenschutzerklärung ziehen. Teilweise fanden sich darüber hinaus bei einzelnen Diensten auch für die Lesenden widersprüchliche Angaben.
Nichtsdestotrotz gab es auch positive Beispiele. So machten einige Dienste konkrete Angaben sowie entsprechende Erklärungen zu Fachbegriffen oder führten Einstellungsmöglichkeiten auf. Verschiedene Merkblätter oder auch gut ausgestaltete FAQ-Bereiche erleichterten die Informationsbeschaffung. Hinzu kamen separate Erklärvideos oder Anleitungen, wie das persönliche Profil sicherer gestaltet werden kann.
Aufgrund der divergierenden Ergebnisse, die keine eindeutige Bewertung zuließen, hat das Bundeskartellamt mögliche lauterkeitsrechtliche Verstöße – Missachtung des Transparenzgebotes gemäß § 5a UWG – im Untersuchungsspektrum belassen.

aa) Lauterkeitsrechtliche Grundlagen

Messenger- und Video-Dienste müssen die Verbraucherinnen und Verbraucher im Einklang mit den Regeln des UWG informieren. Relevant ist in diesem Zusammenhang § 5a Abs. 1 UWG, wonach es eine Irreführung darstellt, wenn den Verbraucherinnen und Verbrauchern eine wesentliche Information vorenthalten wird, die für eine informierte Entscheidung benötigt wird und deren Vorenthalten geeignet ist, eine geschäftliche Entscheidung zu veranlassen, die ansonsten nicht getroffen worden wäre. Durch § 5a Abs. 1 UWG entsteht folglich eine Transparenzpflicht für wesentliche Informationen.[203] Ein Transparenzpflichtverstoß kann vorliegend gegeben sein, wenn die Nutzerinnen und Nutzer über **sicherheitsrelevante Aspekte** eines Messenger- oder Video-Dienstes nicht angemessen informiert werden.

bb) Lauterkeitsrechtliche Versäumnisse

Zwischen der Recherche des Bundeskartellamts zur Verschlüsselung und dem Rücklauf der Ergebnisse der Ermittlungen liegt ein gutes Jahr. Die technische Entwicklung ist in dieser Zeit vorangeschritten. Wie das BSI bereits in seiner Veröffentlichung im November 2021 festgehalten hat, gilt die Ende-zu-Ende-Verschlüsselung als Stand der Technik. Der Eklat um die spezielle und technisch nicht zutreffende Interpretation der Ende-zu-Ende-Verschlüsselung bei einem Videokonferenzanbieter hat sich inzwischen geklärt. Als Endpunkt der Kommunikation wurden eben nicht die Nutzerinnen und Nutzer selbst - wie es

[203] *Dreher/Kulka* Wettbewerbs- und Kartellrecht § 3 Rn. 383.

die Ende-zu-Ende-Verschlüsselung erfordert - sondern die beteiligten Systeme verstanden (siehe dazu auch Kapitel D.I.4.a) cc)). Dies können bei Videokonferenzen nicht die Geräte der Nutzerinnen und Nutzer untereinander, sondern das Gerät jeder Nutzerin oder jedes Nutzers mit dem Server des genutzten Dienstes sein, was einer Transportverschlüsselung entspricht.[204] Aufgrund der darauf ausgelösten öffentlichen Kritik in der Presse und den ebenfalls öffentlich berichteten Nachbesserungen geht das Bundeskartellamt davon aus, dass der Beantwortung des Fragebogens die korrekte Definition der Ende-zu-Ende-Verschlüsselung zugrunde gelegt wurde, sofern sich dies nicht aus den Erläuterungen der Befragten ohnehin schließen lässt.

Die befragten Dienste haben den Fragebogen des Bundeskartellamts zur Verschlüsselung und insbesondere zur Ende-zu-Ende-Verschlüsselung zum größten Teil ausführlich beantwortet. Videokonferenzanbieter haben auf die technischen Beschränkungen verwiesen, die eine Ende-zu-Ende-Verschlüsselung z. B. bei Webinaren mit sehr vielen Teilnehmenden oder beim Einsatz bestimmter Funktionen nicht zulassen. Zu diesen **Funktionen bei Videokonferenzen** gehören z. B. die Einwahl aus dem öffentlichen Telefonnetz oder die Aufzeichnung von Meetings durch den anbietenden Dienst sowie die Anbindung bestimmter externer Geräte (z. B. Raumkonferenzsystem-Geräte, die auf dem SIP-Protokoll basieren) oder die Verwendung von „Assistenten“. Der hohe **Aufwand bei der Verschlüsselung von Gruppenchats** spiegelt sich ebenfalls in den Ermittlungsergebnissen wider. Nur fünf Dienste haben angegeben, alle ihre Funktionen mit der Ende-zu-Ende-Verschlüsselung auszustatten (siehe hierzu nochmals Kapitel D.I.4.a) und b)).

Für einen lauterkeitsrechtlichen Transparenzpflichtverstoß wäre in diesem Zusammenhang zu belegen, ob Informationen zur Sicherheit der Kommunikation, wie beispielsweise das Verwenden einer besonderen Verschlüsselungsmethode, als wesentlich im Sinne des § 5a Abs. 1 UWG zu bewerten sind, ob die vorenthaltenen Informationen für das Treffen einer informierten geschäftlichen Entscheidung erforderlich sind und ob sie geeignet sein können, die Entscheidung der Nutzerinnen und Nutzer eines Messenger- und Video-Dienstes so zu beeinflussen, dass sie sich bei Offenlegung der relevanten Fakten möglicherweise anders entschieden hätten. Nachstehend sollen die **rechtlichen Risiken** aufgezeigt werden, die sich für Messenger- und Video-Dienste in Bezug auf ihre **Informationspraxis zu**

---

[204] Siehe z. B. auch *datenschutz notizen*, https://www.datenschutz-notizen.de/ende-zu-ende-verschluesselung-von-videokonferenzen-1825597 sowie *The Intercept*, Zoom meetings aren’t end-to-end endrypted, despite misleading marketing, 31. März 2020, abrufbar unter: https://theintercept.com/2020/03/31/zoom-meeting-encryption/ und *Golem*, Zoom wirbt mit Ende-zu-Ende-Verschlüsselung – die es nicht gibt, vgl. https://www.golem.de/news/homeoffice-neue-sicherheitsluecken-in-zoom-entdeckt-2004-147670-2.html.

sicherheitsrelevanten Eigenschaften ergeben. Eine abschließende Bewertung kann nicht geleistet werden, sie bedarf letztendlich der Klärung im konkreten Fall.

Zunächst ist für die von § 5a Abs. 1 UWG vorausgesetzte **Wesentlichkeit** einer Information zu hinterfragen, ob die Verbraucherin oder der Verbraucher überhaupt davon ausgehen kann, Informationen zur Sicherheit der Kommunikation durch die Ende-zu-Ende-Verschlüsselung zu erhalten. Bei der Nutzung von Messenger- und Video-Diensten geht es naturgemäß um die Verarbeitung personenbezogener Daten. Ihr Schutz sowie der sichere Umgang mit ihnen ist erklärtes Ziel des Datenschutzrechts. Darüber hinaus werden die Nutzerinnen und Nutzer während des Anmeldeprozesses meist dazu aufgefordert, die speziellen Datenschutz- und Nutzungsbestimmungen zu akzeptieren. Somit können und dürfen die Verbraucherinnen und Verbraucher davon ausgehen, Informationen zur Sicherheit ihrer Daten zu erhalten. Im zweiten Schritt kommt es darauf an, ob die fehlenden Informationen für die Entscheidung der Verbraucherin oder des Verbrauchers wichtig ist.[205] Hier sind nun auch die Interessen der Dienste, wie beispielsweise der zeitliche und kostenmäßige Aufwand oder bestehende Geheimhaltungsbelange im Rahmen einer Interessenabwägung zu berücksichtigen.[206] Die **Zumutbarkeit der Informationsbeschaffung** für den Dienst steht im Mittelpunkt.[207] Sie ist jedenfalls dann gegeben, wenn die Bereitstellung der Information dem Standard an Fachkenntnissen und der Sorgfalt entspricht und davon ausgegangen werden kann, dass die Dienste gegenüber den Nutzerinnen und Nutzern gemäß den anständigen Marktgepflogenheiten und dem Grundsatz von Treu und Glaube die Informationen angeben.[208] Nach dem Ergebnis der Ermittlungen stellen die Dienste umfangreiche Informationen zur allgemeinen Datensicherheit, teilweise auch zur Verschlüsselung und zur Ende-zu-Ende-Verschlüsselung öffentlich bereit, wenn auch in unterschiedlicher Weise und Qualität. Die im Internet öffentlich zugänglichen Fundstellen haben die Dienste größtenteils gegenüber dem Bundeskartellamt auf entsprechende Anforderung im Fragebogen offengelegt. Einige von ihnen werben mit ihrem hohen Sicherheitsstandard, auch bei der Verschlüsselung. Es spricht so gesehen viel dafür, dass es sich um eine **wesentliche Information** handelt.

Dass den Verbraucherinnen und Verbrauchern vom Dienst wesentliche Informationen zur Datensicherheit, insb. zur Ende-zu-Ende-Verschlüsselung, im Sinne des § 5a Abs. 1 UWG „**vorenthalten**“ werden, lässt sich im vorliegenden Zusammenhang vor allem daran messen, ob die Informationen nach § 5a Abs. 2 Nr. 2 UWG lediglich **in unklarer, unverständlicher oder zweideutiger Weise** bereitgestellt

---

[205] MüKo-UWG/*Alexander* § 5a Rn. 223.

[206] BGH, Urteil vom 21.07.2016 – I ZR 26/15 „*LGA tested*“ Rn. 33.

[207] *Köhler/Bornkamm/Feddersen/Köhler* UWG § 5a Rn. 3.15.

[208] Vgl. EuGH, Urteil vom 07.06.2016 – C-310/15 „*Deroo-Blanquart*“ Rn. 33f.

werden. So ist eine Information insbesondere dann unverständlich, wenn der Durchschnittsverbraucher die Bedeutung oder den Sinn nicht versteht. Fachausdrücke oder besondere Abkürzungen sind in dem Zusammenhang relevant.[209] Es sind auch Fälle eingeschlossen, in denen ein Dienst für verschiedene Informationen unterschiedliche Schriftgrößen oder sogar Sprachen verwendet, die die Informationen so undurchdringbar und unverständlich und so letztendlich nutzlos für die Verbraucherinnen und Verbraucher machen. Entscheidend für die Informationspflicht der Messenger- und Video-Dienste könnten daher auch die Gestaltung der Website und die beschriebenen Methoden der Informationsbereitstellung sein. Zwar führen knapp die Hälfte der untersuchten Dienste entsprechende Rubriken auf ihren Websites, jedoch wurde in diesen meist weiter auf die allgemeinen Bestimmungen oder generell gehaltene FAQs bzw. das jeweilige Support-Center verwiesen. Die Verbraucherinnen und Verbraucher können sowohl auf der Startseite als auch unter der Überschrift „Sicherheit“ nur Schlagworte finden. Diese sind dann zwar in verständlicher Sprache geschrieben und mit Skizzen erklärt, tiefergehende Informationen über Folgen, Einschränkungen oder Sonderfälle finden sich an dieser Stelle jedoch nicht. Werden konkrete Angaben gesucht, ist es meist erforderlich die Datenschutzbestimmungen zu lesen. Diese sind in den allermeisten Fällen dann jedoch in englischer Sprache formuliert. Insbesondere undurchsichtige Verweise oder Weiterleitungen auf andere Websites könnten für ein tatbestandliches **Vorenthalten** von Bedeutung sein.

Für einen Transparenzpflichtverstoß könnte es aber vorliegend an der **Veranlassung zu einer sonst nicht getroffenen Handlung** nach § 5a Abs. 1 Nr. 2 UWG fehlen, da die Marktentwicklung weit vorangeschritten ist, die Ende-zu-Ende-Verschlüsselung als Stand der Technik gilt und branchenweit eingesetzt wird (auch wenn es vor diesem Hintergrund bemerkenswert ist, dass einige bekannte Dienste sie noch nicht umsetzen). Wenn aber die Ende-zu-Ende-Verschlüsselung derart weit verbreitet ist, macht es möglicherweise aus Sicht der Verbraucherinnen und Verbraucher jedenfalls in Bezug auf diese Sicherheitseigenschaft keinen wesentlichen Unterschied, bei welchem Dienst sie sich registrieren. Eine möglichst genaue Vorhersage des Verbraucherverhaltens hinsichtlich der Verwendung und Auswahl von Messenger-Diensten in Abhängigkeit vom Verschlüsselungsstandard ist allerdings verlässlich nicht möglich, wie in diesem Bericht an verschiedenen Stellen bereits deutlich wurde. Gegebenenfalls müsste eine entsprechende Verbraucherbefragung durchgeführt werden, die jedoch im Rahmen einer Sektoruntersuchung nur legitim erscheint, wenn mit Aufklärungschancen zu rechnen wäre. Auch das dürfte aber unsicher sein. Allein der Begriff der Verschlüsselung ist interpretationsbedürftig. Die Unterscheidung in die verschiedenen Varianten Transportverschlüsselung und Ende-zu-Ende-

[209] *Köhler/Bornkamm/Feddersen/Köhler* UWG § 5a Rn. 3.30.

Verschlüsselung erfordert Fachwissen, dass bei den Verbraucherinnen und Verbrauchern nicht vorausgesetzt werden kann.

Eine gewisse Bedeutung für die Einschätzung der geschäftlichen Relevanz dürfte daher der **Einordnung des Verbraucherverhaltens aus der Unternehmenssicht** zuzurechnen sein. Informationen, wie die einzelnen Messenger- und Video-Dienste ihre Nutzerinnen und Nutzer an den eigenen Dienst binden, könnten dafür hilfreich sein. So würden sie insbesondere Aufschluss darüber geben, aus welchen Gründen sich die Nutzerinnen und Nutzer für den jeweiligen Dienst entscheiden. Das Bundeskartellamt hat die Dienste in den Ermittlungen dementsprechend befragt. Der überwiegende Teil der befragten Branchenakteure hatte angeben, dass sie u. a. für das hohe Datenschutzniveau bzw. die hohe Datensicherheit geschätzt werden. Dies steht allerdings in Widerspruch oder zumindest nicht in Einklang mit anderen Ermittlungsergebnissen: Das Bundeskartellamt hatte die Messenger- und Video-Dienste um Auskunft gebeten, wo die Nutzerinnen und Nutzer über die Verschlüsselung informiert werden. 60% der Dienste haben die Webseite / Internetadresse genannt, deren Schwächen bei der Informationsübermittlung bereits geschildert wurden. Nur jeder neunte Dienst hat zusätzliche Informationen zu Verschlüsselungsmethoden angegeben. Circa ein Drittel der Dienste erklärte, dass es keine Informationen zur Verschlüsselung für die Nutzerinnen und Nutzer gibt.

Das Bundeskartellamt hat die Branche außerdem aufgefordert zu schildern, ob die **Verschlüsselung gegen Entgelt** weiter verbessert werden kann. In der bereits erwähnten, den Ermittlungen vorausgegangenen Recherche war nur bei einzelnen wenigen Diensten Produktdifferenzierung in Abhängigkeit vom Verschlüsselungsstandard ersichtlich. In den Ermittlungen kristallisierte sich dann ebenfalls heraus, dass die weit überwiegende Mehrheit der Dienste keine zusätzliche Verschlüsselung gegen Entgelt anbietet. Ein befragter Dienst ermöglicht die Verschlüsselung ruhender Daten für Geschäftskunden gegen Entgelt. Die Kunden könnten außerdem die Verschlüsselung auf verschiedenen Ebenen widerrufen. Lediglich ein weiterer Dienst gab an, ein Angebot für weitreichendere Kontrolle über die Verschlüsselungsverfahren zu machen, die Ende-zu-Ende-Verschlüsselung sei aber unabhängig davon grundsätzlich im Abonnement eingeschlossen.

Die Tatsache, dass die Dienste angegeben haben, wegen ihrer Datensicherheit ausgewählt zu werden, dann aber **keine bessere Verschlüsselung gegen Entgelt** anbieten, mag mit strategischem Antwortverhalten im Rahmen einer verbraucherrechtlichen Untersuchung zu erklären sein. Es könnte aber auch daran liegen, dass es nach wie vor viele kostenfreie Angebote, d.h. ohne regelmäßiges Entgelt für die Verwendung der App, gibt.

Letztendlich wird sich ein Transparenzverstoß durch Informationsmängel in Bezug auf die Verschlüsselungsart nicht leicht begründen lassen. Auch wenn Sicherheitseigenschaften zu den wesentlichen Informationen gerechnet werden können, dürfte ihre geschäftliche Relevanz infolge der

Marktentwicklung hin zu Ende-zu-Ende-Verschlüsselung als Branchenstandard und aufgrund der nicht ohne weiteren Ermittlungsaufwand einschätzbaren Verbrauchersicht nur schwer zu begründen sein.

5. Fazit – eine Checkliste für den „Hausgebrauch“

Die Datensicherheit bei Messenger- und Video-Diensten wird nicht allein durch einzelne Sicherheitsaspekte, wie z. B. Art und Ausmaß der Verschlüsselung, bestimmt. Vielmehr geht es um das Zusammenspiel verschiedener Kriterien, die für sich allein genommen noch keine Aussage über die Datenschutzfreundlichkeit zulassen.

Für Außenstehende wird die Analyse dadurch erschwert, dass bei vielen Kriterien verschiedene Facetten denkbar sind und eine Bewertung diese Vielschichtigkeit berücksichtigen muss. So sollte ein geschlossenes Messaging-System mit einem proprietären, d.h. nicht offen liegenden Quellcode nicht ohne weiteres verdächtig werden, Datenschutzprobleme zu bergen. Dienste mit einem proprietären Quellcode können das **Vertrauen in die Implementierung** erhöhen, wenn unabhängige Sicherheitsaudits, Zertifizierungen nach ISO 27001 durchgeführt oder die kryptographischen Designkriterien veröffentlicht werden, was von einigen Diensten auch praktiziert wird.[210]

Ein anderes Beispiel für die Komplexität einer Bewertung ist die Ende-zu-Ende-Verschlüsselung. Die **technischen Einschränkungen und Voraussetzungen** sowie die oft praktizierte **Umsetzung als Option**, die die Nutzerinnen und Nutzer einstellen müssen, lassen nicht fachkundige Außenstehende im Ungewissen, wie es bei den verschiedenen Diensten um die Datenschutzqualität in dieser Frage konkret bestellt ist.

Während Verbraucherinnen und Verbraucher die speziellen Ausprägungen der Sicherheitskriterien von Messenger- und Video-Diensten kaum überprüfen und bewerten können, erscheint es für sie machbar, zumindest die Existenz der einzelnen Sicherheitsmaßnahmen festzustellen und quasi eine „Checkliste“ (Abbildung 13) zu führen. Eine **klare, verbraucherorientierte Kommunikation** der Dienste zu dem, was praktiziert wird, was bereits voreingestellt ist und wo Optionen bestehen sowie was nicht möglich ist, wäre hilfreich und wünschenswert.

Als relevante Kriterien für die Datensicherheit hat das BSI **Protokoll und Verschlüsselung auf dem Stand der Technik** (z. B. das Double Ratchet-Protokoll), die **Einhaltung internationaler Standards** und einen **einsehbaren Quellcode** besonders hervorgehoben. Verbraucherinnen und Verbraucher müssen bei der Ende-zu-Ende-Verschlüsselung an die technischen Einschränkungen denken, wenn sie die Angaben der

---

[210] Vgl. *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.

Dienste dazu überprüfen. Wenn internationale Standards eingehalten und nicht individualisiert werden, sind auch die Anforderungen an Interoperabilität leichter zu erfüllen. Dieser Punkt ist folglich für mögliche Gatekeeper im Sinne des DMA oder interessierte antragstellende Messenger- und Video-Dienste besonders wichtig. Die Einsehbarkeit des Quellcodes dürfte für die Mehrheit der Verbraucherinnen und Verbraucher kein Vorteil sein, da für dessen Bewertung erhebliche Fachkenntnisse erforderlich sind. Einige lassen stattdessen zumindest Sicherheitsaudits von renommierten Institutionen durchführen und veröffentlichen diese. Zwar gelten diese in fachlicher Hinsicht nicht als gleichwertiger Ersatz für die Einsehbarkeit. Für interessierte Verbrauchende könnten die entsprechenden veröffentlichen Bewertungen oder Gütesiegel aber viel besser verständlich und damit ein Indiz für die Datenschutzfreundlichkeit des Dienstes sein. Sofern der Quellcode offen liegt und bewertet werden kann, sollten auch diese Bewertungen den Verbrauchenden verständlich kommuniziert werden. Ansonsten können sie die Information nicht nutzen.

Weitere Säulen eines Sicherheitsnetzes sind die **Zwei-Faktor-Authentisierung** und eine **Ablageverschlüsselung**.[211] Beide Verfahren werden auch in anderen Bereichen praktiziert (z. B. Zwei-Faktor-Authentisierung beim Online-Banking oder Ablageverschlüsselung am Heimcomupter) und sollten für die interessierten Verbrauchenden nachvollziehbar sein.

[211] Vgl. *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.

Unter den Kriterien für eine sparsame Verarbeitung der Daten ist zunächst besonders der **Serverstandort** mit seinen Implikationen für die Datenschutzgesetzgebung und rechtskonforme Datenspeicherung hervorzuheben. So sollten Daten europäischer Nutzerinnen und Nutzer auch in der Europäischen Union gespeichert werden.

Abbildung 13: Checkliste

Ein weiterer Punkt ist die Synchronisation des Kontaktverzeichnisses, auf die verzichtet werden sollte. Der rechtkonforme **Umgang mit den Kontakten** der Nutzerinnen und Nutzer ist aus datenschutzrechtlicher Sicht essentiell für die Datenschutzqualität, da die Nutzerinnen und Nutzer hier nicht nur über die eigenen, sondern auch über Daten Dritter entscheiden. Der Verweis auf die Datenschutzerklärung als der Ort, wo Verbraucherinnen und Verbraucher nachlesen können, wie die Dienste mit ihren Daten umgehen, ist zwar richtig, reicht aber nicht aus, da die Verbraucherinnen und Verbraucher ihr aus den verschiedenen genannten Gründen keine Beachtung schenken. Des Weiteren

kann das **Geschäftsmodell** eines Messenger- und Video-Dienstes als erstes Indiz für die **Intensität der Datenweitergabe** gelten.

Bei Messenger- und Video-Diensten handelt es sich um eine Branche, die insbesondere auf Seiten der größeren Teilnehmenden technologische und digitale Entwicklungen und Innovationen hervorbringt. Konkurrierende Dienste zeichnen sich durch innovative Geschäftsmodelle und Spezialisierungen auf Basis besonderer Services und Funktionen aus. Nicht nur auf Seiten der freien Systeme und Anwendungen gibt es **viel Expertise und Engagement in Sachen Unabhängigkeit und Schutz der persönlichen Daten** der Nutzerinnen und Nutzer. Allerdings sind in der Branche gleichzeitig - wie gezeigt - **verschiedene Praktiken zu bemängeln**. Die Ergebnisse der Sektoruntersuchung legen den Schluss nahe, dass verschiedene Dienste bei Datenschutz und Datensicherheit die Expertise und Möglichkeiten nicht so nutzen, wie es aus Sicht der Nutzerinnen und Nutzer wünschenswert und technisch möglich wäre.

Dies lässt sich gerade aus Sicht der Verbraucherinnen und Verbraucher aber nur schwer an einzelnen Gruppen an Diensten festmachen. So schneiden nach den Ermittlungsergebnissen beispielsweise **freie Messaging-Systeme** und **Open Source-Dienste** bei einer Vielzahl der Kriterien gut ab. Allerdings ist die Frage, wie Datensicherheit im Detail gestaltet wird, hier letztendlich vom ausgewählten Serverbetreibenden abhängig. Gleiches gilt für Open Source-Dienste, wenn diese in bestehende Clients eingebunden werden. Auch hier eröffnen sich dem Dienstbetreiber viele Optionen, Datensicherheit zu gestalten.

Generell eröffnen sich den Nutzerinnen und Nutzern beim Messaging und bei Videokonferenzen **viele Wahlmöglichkeiten**, die teilweise ein gewisses Bewusstsein für sicherheitsrelevantes Handeln erfordern, wie z. B. die gerade erwähnte Auswahl des Serverbetreibenden oder auch die Optionen bei der Ende-zu-Ende-Verschlüsselung. Umgekehrt können Verbraucherinnen und Verbraucher, wenn sie bereit sind, sich zu informieren, ein **weites Feld an Möglichkeiten** vorfinden, um ihren Messenger so zu gestalten bzw. den Client zu finden, dass ihre Anforderungen bestmöglich erfüllt werden und der erwählte Dienst aufgrund von Datensparsamkeit und der Verwendung internationaler Standards auch im Hinblick auf Interoperabilität zukunftsfähig ist.

Auch **Videokonferenzdienste** bieten ihren Nutzerinnen und Nutzern viele Optionen. In weiten Teilen ist das der Ausrichtung auf die Wünsche von Geschäftskundinnen und Geschäftskunden geschuldet. Ein **hohes Sicherheitsniveau** kann geboten werden, gerade bei Diensten, die sich hauptsächlich an Geschäftskundinnen und -kunden wenden. Letztendlich liegt sicherheitsbewusstes Handeln aber häufig in der **Verantwortung des jeweiligen Host** oder der Administratorin oder des Administrators, unabhängig davon, ob diese Rolle geschäftlich oder privat ausgeführt wird.

Was die zu bemängelnden Praktiken oder das fehlende Engagement angeht, so betrifft dies zum einen die **Verschlüsselung**. Einzelne Messenger- und Video-Dienste, die bei Verbraucherinnen und

Verbrauchern beliebt sind, und auch einzelne bekannte Video-Dienste überraschen damit, dass sie Sicherheit **nicht auf dem Stand der Technik** umsetzen und es zum Beispiel bei einer Transportverschlüsselung belassen oder die Ende-zu-Ende-Verschlüsselung nur bei bestimmten Funktionen einsetzen, was nicht mit technischen Restriktionen begründet werden kann. Ferner wäre wünschenswert, dass branchenweit weitere Sicherheitsverfahren, wie die Verschlüsselung der Daten auf dem Endgerät, die Ablageverschlüsselung, die Zwei-Faktor-Authentisierung sowie Backups in der Branche einen höheren Verbreitungsgrad hätten.

Zum anderen sei auf die rechtliche Analyse verwiesen. Einige Dienste speichern **Daten im europäischen Ausland** oder der genaue Speicherort bleibt unklar. Auch die **Synchronisation des Kontaktverzeichnisses** in Folge derer Daten Dritter rechtswidrig verarbeitet werden, wird von verschiedenen Diensten betrieben. Wenn Nutzerinnen und Nutzer **Konten** anlegen müssen, wie es bei Diensten großer Konzerne, die ein digitales Ökosystem betreiben, der Fall ist, werden viele Daten bereits dadurch erfasst.

Festzuhalten ist, dass die Bewertung der Datenschutzpraxis für die Verbraucherinnen und Verbraucher schwierig und komplex bleibt.

E. Datenportabilität als Übergang zur Interoperabilität?

Mit Art. 20 Abs. 1 DSGVO hat der Gesetzgeber den Verbraucherinnen und 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.[212] Fraglich ist, ob die Konzeption der Norm grundsätzlich die Bedürfnisse der Nutzerinnen und Nutzer von Messenger- und Video-Diensten einfangen kann (siehe dazu unter I.). Zweifel bestehen zudem an der praktischen Bedeutung der Vorschrift für die Nutzerinnen und 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 Inanspruchnahme der Übermittlung gespeicherter personenbezogener Daten gemäß Art. 20 DSGVO gefragt (dazu unter III.).

I. Einordnung und Anspruch der Vorschrift

Gemäß Art. 20 Abs. 1 DSGVO können Verbraucherinnen und Verbraucher die sie betreffenden personenbezogenen Daten, die einem Verantwortlichen bereitgestellt wurden, in einem strukturierten, gängigen und maschinenlesbaren Format erhalten oder dem neuen Verantwortlichen direkt übermitteln lassen. Der Verbraucherin oder 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.[213] So wird vereinzelt vorgebracht, es handele sich um eine Vorschrift mit rein verbraucherschutz- und

---

[212] 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; *Yoo* (2020): Unpacking data portability, *CPI* antitrust chronicle November 2020, abrufbar unter: https://www.competitionpolicyinternational.com/unpacking-data-portability/; *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.

[213] *Kühling/Buchner/Herbst,* DSGVO, Art. 20 Rn. 4.

wettbewerbsrechtlichen Zielen, anstelle von datenschutzrechtlichen Zielen.[214] Nach überwiegender Auffassung stellt das Recht auf Datenportabilität jedoch genauso ein Gestaltungsrecht dar, wie andere Betroffenenrechte.[215] Entscheidend bei der systematischen Einordnung sei vielmehr, dass die Norm neben rein datenschutzrechtlichen Zielen eben auch andere, insbesondere wettbewerbs- und binnenmarktpolitische Ziele verfolge. So stärke das Recht die Selbstbestimmung der Verbraucherinnen und Verbraucher und fördere gleichzeitig den Wettbewerb zwischen den Anbietern sozialer Netze.[216] Die Vorschrift soll den Verbraucherinnen und Verbrauchern somit offenbar nicht nur ermöglichen, ihre Daten zu erhalten. Sie soll sie 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.[217] Somit beruht der Ursprung der Vorschrift zwar weniger auf dem klassischen Datenschutzrecht i. S. d. Schutzes personenbezogener Daten, er trägt dennoch aufgrund der verbraucherschützenden und marktregulierenden Aspekte zum übergreifenden Schutzzweck des Datenschutzrechts bei.[218]

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.

---

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

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

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

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

218 *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/*Schürnmann* 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/*Schürnmann* 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 „unverzüglich, 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 jede Nutzerin oder 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.[219] 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

---

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

wohl mit dem berechtigten 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 Kontaktverzeichnis 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 Nutzerinnen und 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 Chatteilnehmenden veröffentlichten Daten zusammensetzen. Sie sind nicht ausschließlich von der Anspruchstellerin oder 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 Verbraucherinnen und 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 Verbraucherinnen und 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 Verbraucherinnen und 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** Nutzerinnen und Nutzer die Übermittlung der gespeicherten personenbezogenen Daten beim jeweiligen Dienst beantragen können, haben fast alle befragten Branchenteilnehmenden 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 Art. 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 Nutzerinnen und 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 Nutzerinnen und 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 Nutzerinnen und 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.

F. Mehr Datenschutz durch Interoperabilität?

Interoperabilität ist ein sich dynamisch entwickelnder Begriff, der vielfach an verschiedene Verwendungen angepasst wird und für den Wettbewerbs- und Verbraucherschutz zu Beginn der Sektoruntersuchung Messenger- und Video-Dienste noch nicht eindeutig definiert worden war.[220] Als vorläufige Definition für die Zwecke dieser Sektoruntersuchung hatte das Bundeskartellamt Interoperabilität als die **Fähigkeit unabhängiger, heterogener Systeme oder Produkte verstanden, in verschieden hohem Maße zusammenzuarbeiten**. Aus Sicht der Verbraucherinnen und Verbraucher bezeichnet Interoperabilität die Möglichkeit, sich mit Nutzerinnen und Nutzern eines anderen als dem eigenen Messenger- und Video-Dienst austauschen zu können, ohne selber diesen anderen Dienst installiert oder sich dort registriert zu haben. [221]

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 Verbraucherinnen und Verbraucher keine Scheu mehr haben, den Messenger- und Video-Dienste zu wechseln, da sie von den bisherigen Kontakten nicht mehr ausgeschlossen werden. Um die gewünschten positiven, direkten Effekte auf das Datenschutzniveau zu erreichen, müssten sich die Verbraucherinnen und Verbraucher

---

[220] 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/, 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.

[221] 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.

allerdings datenschutzfreundlichen Messenger- und Video-Diensten zuwenden. Nach den Ergebnissen verschiedener Verbraucherbefragungen erscheinen Zweifel daran durchaus berechtigt (vgl. dazu F.II). 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 eine rechtliche, wissenschaftliche und begriffliche Einordnung vorgenommen (dazu unter I.) Von Interesse ist, inwieweit Interoperabilität bereits Eingang in gesetzliche Vorschriften auf nationaler und europäischer Ebene gefunden hat und was die Gründe dafür sind. Hinzuweisen ist hier insbesondere auf den Digital Markets Act, der in der Zwischenzeit - nach Veröffentlichung des Zwischenberichts zu dieser Sektoruntersuchung - zwischen EU-Kommission, EU-Parlament und EU-Ministerrat abschließend beraten wurde und in Kraft getreten ist. 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. Sind sie überhaupt geeignet, die komplexen Wirkungszusammenhänge zu beleuchten? Danach wird geklärt, wie Interoperabilität organisatorisch und technisch umgesetzt werden kann und wie sich die entsprechenden Regelungen des Digital Markets Act einordnen lassen.

Im Anschluss daran geht es um die Verbraucherinnen und Verbraucher und ihr nur schwer prognostizierbares Verhalten. Werden sie die von Politik und Datenschützern in sie gesetzten Hoffnungen erfüllen oder haben sie selbst ganz andere Wünsche (dazu unter II.)?

Vor diesem Hintergrund werden anschließend die Ermittlungsergebnisse zu Fragen der Interoperabilität präsentiert, die den Messenger- und Video-Diensten noch vor Aufnahme des Interoperabilitätsregimes in die Entwürfe zum Digital Markets Act gestellt wurden (dazu unter III.). Den Abschluss des Kapitels bilden Schlussfolgerungen, die sich aus dem Zusammenspiel von Ermittlungsergebnissen und den DMA-Regelungen ergeben. Mit welchen Auswirkungen auf das Datenschutzniveau ist zu rechnen? Da zum Zeitpunkt der Veröffentlichung dieses Berichts technische Spezifikationen und allgemeine Bedingungen von Referenzangeboten gemäß DMA möglicher Gatekeeper noch nicht bekannt waren, können nur einige grundlegende Anmerkungen aus verbraucherrechtlicher Perspektive gemacht werden (siehe dazu unter IV.).

I. Interoperabilität – eine begriffliche, rechtliche und wissenschaftliche Einordnung

1. 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 deutschen Wirtschaftsrecht waren bisher 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 Gesetz gegen Wettbewerbsbeschränkungen (GWB) sowie § 21 Abs. 2 des Telekommunikationsgesetzes (TKG).[222]

Mit der Aufnahme einer Interoperabilitätsverpflichtung in die Entwürfe zum Digital Markets Act im März 2022 hat sich das rechtliche Umfeld der Messenger- und Video-Dienste in Sachen Interoperabilität konkretisiert. Wegen der anhaltenden rechtspolitischen Diskussion über eine gesetzliche Verpflichtung von Messenger- und Video-Diensten zur horizontalen Interoperabilität hatte das Bundeskartellamt in seiner Untersuchung den befragten Unternehmen bereits vor der Einigung im Trilog zum DMA im März 2022 auch zu diesem Themenkomplex Fragen gestellt. Einzelne Messenger- und Video-Dienste hatten sich in ihren Antworten zum Fragebogen des Bundeskartellamts auf den im Jahr 2021 geltenden Rechtsrahmen für eine mögliche verpflichtende Interoperabilitätsmaßnahme bezogen. Dies sind § 19a GWB (vgl. dazu unten a)) und Art. 61 Abs. 2 Unterabs. 1 lit. c des Europäischen Kodex für elektronische Kommunikation[223] (siehe dazu unter b)), 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.[224] Der Digital Markets Act wird nun den rechtlichen Rahmen ergänzen und könnte weitreichende Auswirkungen für einige Messenger- und Video-Dienste haben (siehe dazu unten c)).

a) § 19a Gesetz gegen Wettbewerbsbeschränkungen (GWB)

Das Bundeskartellamt kann nach § 19a Abs. 1 GWB für Unternehmen eine überragende marktübergreifende Bedeutung für den Wettbewerb feststellen und darauf aufbauend entsprechenden Unternehmen nach § 19a Abs. 2 GWB bestimmte Verhaltensweisen untersagen. Anders als in der

---

[222] 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) vom 23.06.2021, BGBL. I 1858 – TKG.

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

[224] Vgl. etwa die interdisziplinäre Betrachtung von *Gerpott*, Interoperabilität von Messenger-Diensten und sozialen Netzwerken großer Online-Plattformen, CR 2022, 133 ff., *Kühling/Hildebrandt/Bulowski*, Die Zukunft der Interoperablitätsregulierung für OTT-Kommunikationsdienste, K & R 2022, 670 ff.

klassischen Missbrauchsaufsicht muss folglich nicht für jeden Einzelfall eine marktbeherrschende Stellung ermittelt werden, was die Rechtsdurchsetzung beschleunigen kann.

Nach § 19a Abs. 2 Satz 1 Nr. 5 GWB kann das Bundeskartellamt 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.

Das deutsche Recht knüpft mit § 19a GWB - anders als der Digital Markets Act - grundsätzlich nicht an einzelne (Arten von) Dienste(n) an, sondern ermöglicht das Unternehmen als Ganzes und auch marktübergreifende Wechselwirkungen von Diensten innerhalb eines digitalen Ökosystems zu berücksichtigen.[225]

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.

b) 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

---

[225] Bislang hat das Bundeskartellamt die überragende marktübergreifende Bedeutung für Alphabet (Google), Meta und Amazon festgestellt, vgl. BKartA, Beschl. v. 30.12.2021, Az. B7-61/21 „*Alphabet (Google)*“- Fallbericht v. 05.01.2022; BKartA, Beschl. v. 03.04.2023, Az. B9-67/21 „*Apple*“ – Fallbericht v. 05.04.2023, BKartA, Beschl. v. 02.05.2022, Az. B6-27/21 „*Meta*“ – Fallbericht v. 30.06.2022; BKartA, Beschl. 05.07.2022, Az. B2-55/21 „*Amazon*“ – Fallbericht v. 06.07.2022, . Siehe auch *Bundeskartellamt*, Stellungnahme zur öffentlichen Anhörung des Wirtschaftsausschusses zum Digital Markets Act, 25. April 2022, abrufbar unter: https://www.bundestag.de/resource/blob/891308/f13edcf322cc218da602e6dc4b58391b/ADrs-20-9-59_Stellungnahme-Mundt-data.pdf.

auferlegt werden, wenn die **durchgehende Konnektivität zwischen Endnutzerinnen und Endnutzern** gefährdet ist. Die Umsetzung des Kodex ist im TKG erfolgt.

Nach § 21 Abs. 2 TKG (neu) kann die Bundesnetzagentur im Falle einer Bedrohung der durchgehenden Konnektivität zwischen Endnutzerinnen und Endnutzern die Anbieter von nummernunabhängigen interpersonellen Telekommunikationsdiensten – und damit auch von Messenger-Diensten – verpflichten, ihre Dienste interoperabel zu machen. Die Bundesnetzagentur geht derzeit davon aus, dass gegenwärtig die durchgehende Konnektivität dadurch gewährleistet ist, dass Endnutzerinnen und Endnutzer nummerngebundene interpersonelle Telekommunikationsdienste, d. h. klassische Telekommunikationsdienste nutzen. „Künftige technische Entwicklungen und auch das Verhalten der Nutzerinnen und Nutzer könnten aber zu einer unzureichenden Interoperabilität zwischen interpersonellen Telekommunikationsdiensten führen“[226].

c) Digital Markets Act

Gemeinsam mit dem Gesetz über digitale Dienste, dem Digital Services Act (kurz DSA), ist der am 1. November 2022 in Kraft getretene Digital Markets Act eines der Kernelemente der EU-Digitalstrategie. [227]

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 zielt hier primär auf Wettbewerbsfragen, der DSA auf andere Bereiche der Plattformregulierung wie Online-Werbung, Haftungsfragen oder Inhaltemoderation.[228]

Im Digital Markets Act sind **Regeln** für bestimmte **große Online-Plattformen** vorgegeben. Mit regulatorischen Maßnahmen sollen gewerbliche Nutzerinnen und Nutzer sowie Endnutzerinnen und

---

[226] *Bundesnetzagentur*, Interoperabilität zwischen Messenger-Diensten, November 2021, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/OnlineKom/diskussionspapier_IOP.pdf?__blob=publicationFile&v=3.

[227] Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2065 sowie Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R1925.

[228] Vgl. *Netzpolitik.org*, abrufbar unter: https://netzpolitik.org/2021/plattformregulierung-europas-weg-in-die-digitale-zukunft/.

Endnutzer der von Gatekeepern bereitgestellten zentralen Plattformdienste in der gesamten Europäischen Union vor unfairen Praktiken der Gatekeeper geschützt werden.[229]
Im Herbst 2021 hatten das EU-Parlament, die EU-Kommission und die Mitgliedsstaaten die Verhandlungen über DSA-Vorschlag und DMA-Vorschlag[230] aufgenommen.
Im Dezember 2021 hatte das Plenum des Europäischen Parlaments einen gemeinsamen Standpunkt zum DMA angenommen und seine Verhandlungsposition festgelegt. Der **DMA-Entwurf** des Europäischen Parlaments sah - im Gegensatz zum Entwurf der EU-Kommission - eine Interoperabilitätsverpflichtung für Gatekeeper bezogen auf „nummernunabhängige interpersonelle Kommunikationsdienste“ („number-independent interpersonal communication services, hierunter fallen Messenger-Dienste) vor. Im DMA-Vorschlag der EU-Kommission spielte Interoperabilität bereits eine Rolle. Allerdings sollte Interoperabilität hier - anders als in § 19a GWB - insbesondere im Vertikalverhältnis der Marktteilnehmer Berücksichtigung finden.
Am 24. März 2022 kam es zu **einer Einigung im Trilog,** d. h. zwischen Vertreterinnen und Vertretern der EU-Kommission, des EU-Parlaments und des EU-Ministerrats. Danach muss der Gatekeeper auf Antrag eines anderen Messenger-Dienstes oder Marktneulings die notwendigen technischen Schnittstellen oder vergleichbare Lösungen bereitstellen, um Interoperabilität ohne die Auferlegung von Kosten zu ermöglichen. Die Vorschrift bezieht sich auf eine Interoperabilität der **Basisfunktionen - zunächst Textnachrichten -** einschließlich des Sicherheitsniveaus, das der Gatekeeper seinen eigenen Nutzern garantiert (einschließlich der Ende-zu-Ende-Verschlüsselung). Im Vergleich zum vorausgegangenen Entwurf wurde der Katalog der Basisfunktionen erweitert auf das Teilen jeglicher Dateien, nicht nur Bilder, Sprachnachrichten und Videos. Jeder Gatekeeper ist verpflichtet, ein **Referenzangebot** („reference offer“) zu veröffentlichen, das die wesentlichen technischen Details, die AGB sowie die notwendigen Informationen zur Datensicherheit und der Ende-zu-Ende-Verschlüsselung enthält. Anträge auf Interoperabilität bilateraler Textnachrichten müssen innerhalb von drei Monaten umgesetzt werden. Für die **Interoperabilität weiterer Funktionen** sind unterschiedliche Fristen vorgesehen, nach deren Ablauf einem Antrag auf Interoperabilität frühestens nachzukommen ist, nämlich für **Gruppen-Textnachrichten** zwei Jahre nach der Designierung zum Gatekeeper des jeweiligen Messenger-Dienstes und für **Videoanrufe** sowohl zwischen zwei als auch mehr Nutzerinnen und Nutzern vier Jahre nach der

---

[229] Vgl. DMA, Erwägungsgrund 7, abrufbar unter: https://data.consilium.europa.eu/doc/document/PE-17-2022-INIT/de/pdf.

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

Designierung des jeweiligen Messenger-Dienstes. Die Europäische Kommission darf ausnahmsweise die genannten Fristen verlängern, insbesondere wenn nur so Ende-zu-Ende-Verschlüsselung sichergestellt werden kann.

Die Europäische Kommission wird außerdem ermächtigt, durch delegierten Rechtsakt die Liste der Basisfunktionalitäten zu ändern und über Durchführungsrechtsakte („implementing act“) „operational and technical arrangements“ zu treffen.

Das Bundeskartellamt hat in seiner Stellungnahme zur öffentlichen Anhörung des Wirtschaftsausschusses zum Digital Markets Act das europäische Gesetzgebungsvorhaben begrüßt. Gleichzeitig hat es betont, dass zukünftig auch eine den DMA ergänzende Anwendung des Wettbewerbsrechts gegenüber den großen Digitalunternehmen erforderlich sein wird und dies ausführlich erläutert.[231]

Festzuhalten ist, dass das Wettbewerbs- und Sektorrecht nicht Grundlage der vorliegenden verbraucherrechtlichen Sektoruntersuchung ist. Allerdings hatte der deutsche Gesetzgeber dem Thema Interoperabilität bereits vor Erlass des Digital Markets Act eine hohe Bedeutung zugerechnet und dessen Komplexität aufgrund möglicher negativer Auswirkungen in den geltenden Rechtsvorschriften erwähnt. Dies hatte die Auffassung des Bundeskartellamts gestützt, dass eine Befragung der Branche ein fundierter Beitrag sein kann, um das Verhältnis der Effekte von Interoperabilität 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.

2. 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 a)). Anschließend werden wesentliche Erkenntnisse zur Theorie der Netzwerke (dazu unter b)) und mögliche Auswirkungen von Interoperabilität auf Wettbewerb und Innovation beschrieben

---

[231] Siehe für die Einzelheiten *Bundeskartellamt*, Stellungnahme zur öffentlichen Anhörung des Wirtschaftsausschusses zum Digital Markets Act, 25. April 2022, abrufbar unter: https://www.bundestag.de/resource/blob/891308/f13edcf322cc218da602e6dc4b58391b/ADrs-20-9-59_Stellungnahme-Mundt-data.pdf.

(dazu unter c)). Den Abschluss bildet eine kurze Zusammenfassung möglicher Effekte von Standardisierungsprozessen (dazu unter d)).

a) 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 Nutzerinnen und 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.[232] Im Folgenden soll ein Überblick **über diejenigen Erklärungsansätze** gegeben werden, die in vergleichsweiser enger Form mit dem Untersuchungsthema oder den Branchenteilnehmenden in Verbindung stehen.

b) 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 Netzwerke[233] - 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 Jahr 2021 veröffentlichte Bericht des Verbraucherzentrale Bundesverbands anschaulich belegt.[234]

Nutzerinnen und Nutzer von Messenger- und Video-Diensten schätzen diejenigen Netzwerke besonders, bei denen sie viele andere Nutzerinnen und Nutzer erreichen können (sog. positiver direkter Netzwerkeffekt).[235] Aus positiven Netzwerkeffekten können Selbstverstärkungseffekte resultieren: Große Netzwerke werden immer attraktiver für die Nutzerinnen und 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

---

[232] 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.

[233] 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.

[234] *Verbraucherzentrale Bundesverband* (2021), Interoperabiltiät 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.

[235] 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.

konzentriert, während die übrigen Wettbewerber nicht die erforderliche kritische Größe erreichen, sog. **Tipping**.[236] 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**).[237] 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.[238]

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.

c) Auswirkungen auf Wettbewerb und Innovation

Die Auswirkungen von Interoperabilität auf Wettbewerb[239] 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

---

[236] Vgl. *Bundeskartellamt*, B6-113/15, Arbeitspapier – Marktmacht von Plattformen und Netzwerken, Juni 2016, S. 104 ff. m.w.N., abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Think-Tank-Bericht.pdf?__blob=publicationFile&v=2.

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

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

[239] 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.

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.[240] 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 Nutzerinnen und Nutzer über die verschiedenen Kommunikationswege (Textnachrichten, Telefonie, Videotelefonie usw.) jeweils miteinander austauschen können. Dies birgt die Gefahr, dass einmal geschaffene interoperable Funktionen nicht mehr ausreichend weiterentwickelt werden. Wettbewerb um neue innovative Geschäftsmodelle sowie von der Nutzerin oder 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 Befürwortenden 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.[241] Als Beispiel kann das Internet selbst gelten, welches für

---

[240] *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.

[241] *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.

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.[242]

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"[243] 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.

d) 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, insbesondere 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.[244] 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.

---

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

[243] 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.

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

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 Akteurinnen und Akteure ab, die ihn umsetzen. **Anpassungskosten** entstehen, wenn Marktteilnehmende einen verpflichtenden Standard erfüllen müssen, den sie bisher nicht verwenden oder den sie nur mit erheblichem Aufwand implementieren können.[245]

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, diese Strukturen aufzubrechen.[246] 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 etablierten.[247] Nichtsdestotrotz kann in vielen Fällen eine Standardisierung bestimmter Technologien oder Funktionen entweder **aus Effizienzgründen oder aufgrund der individuellen Verdienstmöglichkeiten ein wichtiges Ziel der Marktteilnehmenden** sein.

Inwieweit Standardisierung eher Chancen oder eher Risiken birgt, hängt von den individuellen Gegebenheiten in einer Branche und dem wirtschaftlichen Umfeld ab. Wenn es um Interoperabilität geht, ist zu berücksichtigen, dass diese auf vielen verschiedenen Wegen umgesetzt und gestaltet werden kann, die jeweils mit Vorteilen und Nachteilen verbunden sind.

---

245 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.

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

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

3. 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 **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 bestimmte Anbieter verpflichtet, ihre Dienste interoperabel zu gestalten.[248]

In der Branche der Messenger- und Video-Dienste war es bisher dem Markt überlassen, Interoperabilitätsregelungen hervorzubringen. Dies hat sich mit Inkrafttreten des Digital Markets Act geändert, der eine asymmetrische Interoperabilitätsverpflichtung enthält. Wie oben beschrieben können sog. Gatekeeper unter den Messenger- und Video-Diensten verpflichtet werden, Wettbewerbern Zugang zu ihren Diensten zu ermöglichen.

Was die **technische Umsetzung** angeht, sollen an dieser Stelle nur grundlegende Überlegungen dargestellt werden, die für das Verständnis der Ausführungen der Branche notwendig sind. Grundsätzliche 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. Einzelheiten zur technischen Umsetzung des Digital Markets Act sind bisher nicht bekannt. Gatekeeper

[248] 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.

sollen eine Schnittstelle bereithalten und technische Errungenschaften, wie die Ende-zu-Ende-Verschlüsselung, gewährleisten.[249]

Grundsätzlich richtet sich die technische Umsetzung von Interoperabilität 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 „Dienstart Messenger- und Video-Dienst", die im Wettbewerb zueinanderstehen stehen, Interoperabilität hergestellt werden kann. Es geht also vordringlich 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.[250]

Nach den Erkenntnissen des Bundeskartellamts kann Interoperabilität grundsätzlich auf mehreren Wegen umgesetzt werden, mit denen eine unterschiedliche Intensität an technischer Verknüpfung einhergeht: Client Interoperabilität, Bridges und Converter u. ä., Serverschnittstellen und vollständige Standardisierung.

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 Verbraucherinnen und Verbraucher verschiedene Messenger-Systeme auslesen können. Die Nutzerinnen und Nutzer müssen dazu bei den jeweiligen Diensten registriert sein.

---

[249] In der von der *Bundesnetzagentur* am 3. Mai 2023 präsentierten Studie "Interoperability between Messaging Services - Secure Implementation of Encryption" stellen die Autoren Prof. Rösler und Prof. Schwenk mögliche technische Optionen technisch vertieft dar und erörtern Vor- und Nachteile sowie Herausforderungen, abrufbar unter: https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Technologien/__Onlinekomm/Study_InteropEncryption.pdf?__blob=publicationFile&v=1. Die Studie bezieht sieben Messenger- und Video-Dienste ein und beruht auf einer Untersuchung öffentlich erhältlicher technischer Dokumentationen und wissenschaftlicher Publikationen.

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

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.[251] Voraussetzung technischer Art ist grundsätzlich, dass alle partizipierenden Dienste eine öffentliche Schnittstelle implementieren und die eigene Programmierschnittstelle (API, siehe dazu den folgenden Abschnitt) 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.[252] Für diese Umsetzungsvariante sind mehr technische Vorkehrungen zu treffen als für die Interoperabilität der Clients.

Sofern ein **branchenweit standardisiertes Regime** angestrebt würde, wäre eine Übereinkunft in der Branche notwendig, ein standardisiertes frei zugängliches Messaging-System bzw. eine standardisierte Server-API oder ein standardisiertes 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 Nutzerinnen und Nutzern anderer Dienste umgehen zu können. Auch die diensteigenen Identifier müssten in die **einheitlichen Identifier** des interoperablen Systems

---

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

[252] 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. *Talend*, abrufbar unter: https://www.talend.com/de/resources/was-ist-eine-api/. 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/.

überführt werden. Die Clients hätten weniger Aufwand zu bestreiten. Sie müssten jedenfalls für die Kernfunktion Nachrichtenaustausch den Standard oder das standardisierte Protokoll übernehmen.[253] 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. Mit XMPP und Matrix gibt es bereits freie Messenger-Systeme mit offenen Standards.

Für die **Verbraucherinnen und 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.

Die Erkenntnisprozesse, die einer praktischen Umsetzung vorausgehen müssen, sind anspruchsvoll und komplex. 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.

II. Verbraucherverhalten

Mit den Verbraucherinnen und 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, da sie ihre bisherigen Kontakte dann auch 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 Verbraucherinnen und Verbraucher möglicherweise nicht, warum sie den Anbieter wechseln sollten. Wird weiterhin eine gewisse **Trägheit** im Wechselverhalten von Verbraucherinnen und Verbrauchern berücksichtigt, so könnte es theoretisch nicht auszuschließen sein, dass große Dienste durch Interoperabilität zusätzliche Nutzerinnen und Nutzer gewinnen.[254]

---

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

[254] Siehe auch *Bitkom,* Positionspapier, S. 5 f. für ein ähnliches Argument.

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 Verbraucherinnen und Verbraucher im Sinne eines verbesserten Datenschutzes von Interoperabilität profitieren würden. Unklar ist bereits, ob sie Interoperabilität überhaupt wünschen. 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 Verbraucherinnen und 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 Verbraucherinnen und Verbraucher zu Interoperabilität und Datenschutz stellen.

1. Interoperabilität oder Multi-Homing?

Die Bundesnetzagentur hat im Oktober / November 2019 bzw. im August 2021 jeweils eine Verbraucherbefragung zu Online-Kommunikationsdiensten durchgeführt und die Ergebnisse der Befragungen im Mai 2020 bzw. im Januar 2022 veröffentlicht. Die Berichte der Bundenetzagentur legen die Vielfalt des Verbraucherverhaltens bei der Nutzung von OTT-Diensten[255] offen.
Die Nutzerinnen und Nutzer von Messenger-Diensten können ohne größeren Aufwand mehrere Dienste parallel verwenden (sog. **Multi-Homing**[256]). Nach den Ergebnissen der Bundesnetzagentur verwendeten 2021 rund 73% aller Befragten mindestens zwei verschiedene Messenger-Dienste parallel. Damit betrieben nahezu drei Viertel der Befragten bereits Multi-Homing. Bei der Befragung im Jahr 2019 hatte dieser Anteil noch bei rund zwei Dritteln der Befragten (68%) gelegen, sodass hier eine deutliche

---

[255] Vgl. *Bundesnetzagentur (2020)*, Nutzung von OTT-Kommunikationsdiensten in Deutschland, Bericht 2020, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/OTT.pdf?__blob=publicationFile&v=6 sowie *Bundesnetzagentur (2022)*, Nutzung von Online-Kommunikationsdiensten in Deutschland, Ergebnisse der Verbraucherbefragung 2021, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/OnlineKom/befragung_kurz21.pdf?__blob=publicationFile&v=3.

[256] 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.

Zunahme zu verzeichnen ist. Multi-Homing ist grundsätzlich bei jüngeren Menschen stärker verbreitet als bei älteren. In der Altersgruppe der „bis 40-Jährigen“ nutzten danach im Jahr 2021 rund 87% der Befragten mindestens zwei OTT-Kommunikationsdienste. Im Durchschnitt werden in dieser Altersgruppe sogar rund vier verschiedene Dienste genutzt. In der Gruppe der „über 40-Jährigen“ ist Multi-Homing deutlich schwächer ausgeprägt. Hier verwendete 2021 gut ein Drittel der Befragten (35%) ausschließlich einen Dienst, im Jahr 2019 hatte dieser Anteil allerdings noch bei 46% gelegen.[257]
Ein Teil der Verbraucherinnen und Verbraucher trennt anscheinend bewusst verschiedene Messenger-Dienste derart voneinander, dass sie für bestimmte Personen nur über bestimmte Kanäle erreichbar sind.[258] So wird die Kommunikation mit z. B. guten Freundinnen und 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 Verbraucherinnen und Verbraucher.
Demgegenüber könnte sich ein gewisses Interesse an Interoperabilität daraus ergeben, dass ausweislich der Befragung der Bundesnetzagentur aus dem Jahr 2020 fast ein Drittel der OTT-Nutzerinnen und -Nutzer bereits eine Person kontaktieren wollte, diese aber nicht erreichen konnten, weil von dieser Person nicht derselbe Messenger-Dienst verwendet wurde.[259] Dementsprechend scheinen insbesondere **positive direkte Netzwerkeffekte** bei der Nutzung von OTT-Kommunikationsdiensten wichtig zu sein. Je mehr Kontakte von Nutzerinnen und Nutzern 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 aktuellem Bericht der Bundesnetzagentur dann aber kein eindeutiges Meinungsbild. 43% der befragten OTT-Nutzerinnen und - Nutzer finden es (eher) wichtig, dass Nutzerinnen und Nutzer verschiedener Dienste untereinander kommunizieren können, während 48% diese Aussage als eher nicht oder überhaupt nicht zutreffend beschreiben. Gleichzeitig sehen 51% (eher) keinen Bedarf darin, Nachrichten an Nutzerinnen und Nutzer anderer OTT-

---

[257] Vgl. *Bundesnetzagentur (2022)*, Nutzung von Online-Kommunikationsdiensten in Deutschland, Ergebnisse der Verbraucherbefragung 2021, S. 23 f.

[258] 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.

[259] Vgl. *Bundesnetzagentur (2020)*, Nutzung von OTT-Kommunikationsdiensten in Deutschland, Bericht 2020, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/OTT.pdf;jsessionid=8426B6FF000026EC292A4CF57D316608?__blob=publicationFile&v=6, S. 23.

Kommunikationsdienste versenden zu können. 43% wären hierzu jedoch gerne in der Lage.[260] Für den nahezu gleich hohen Anteil der Verbraucherinnen und 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 26% der befragten OTT-Nutzerinnen und - Nutzer an, dass sie grundsätzlich bereit wären, sich einen weiteren OTT-Dienst zu installieren, um eine bestimmte Nutzerin oder einen bestimmten Nutzer eines anderen Dienstes erreichen zu können. Zweitens kann immer noch auf die **klassischen Telekommunikationsdienste** wie SMS oder Telefonie zurückgegriffen werden, wenn Kommunikationspartnerinnen und -partner nicht über Messenger-Dienste erreichbar ist. Dies geben 84% der befragten OTT-Nutzerinnen und - Nutzer als vollkommen oder eher zutreffend an.[261]
Außerdem möchten 60% der Befragten nicht von Nutzerinnen und Nutzern anderer Dienste kontaktiert werden können. Für den Fall, dass eine solche Kontaktaufnahme dennoch möglich wäre, würden 88% der Befragten selber entscheiden wollen, ob sie den Kontakt ermöglichen.[262] Die Entscheidungshoheit zu behalten, scheint für viele Verbraucherinnen und 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. Verbraucherinnen und 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 Verbraucherinnen und Verbraucher unabhängig von Netzwerkeffekten eine enge Bindung zu bestimmten Messenger-Diensten unterhalten. Die Untersuchung basiert auf einer Befragung von 2044 Verbraucherinnen und Verbrauchern in Deutschland, die Messenger-Dienste wie Facebook Messenger, Line, Skype, WeChat and WhatsApp aber auch E-Mail und traditionelle Kommunikationsmittel verwendeten.[263]

---

[260] Vgl. *Bundesnetzagentur (2022)*, Nutzung von Online-Kommunikationsdiensten in Deutschland, Ergebnisse der Verbraucherbefragung 2021, S. 31.

[261] Vgl. *Bundesnetzagentur* (2022) Nutzung von Online-Kommunikationsdiensten in Deutschland, Ergebnisse der Verbraucherbefragung 2021, S. 30 f.

[262] Vgl. *Bundesnetzagentur (2022)*, Nutzung von Online-Kommunikationsdiensten in Deutschland, Ergebnisse der Verbraucherbefragung, S. 30 f.

[263] Vgl. *Arnold/Schneider/Lennartz*, Interoperability of interpersonal communications services – A consumer perspective, in: Telecommunications Policy,Vol. 44,Issue 3, April 2020, siehe *ScienceDirect,* abrufbar unter: https://www.sciencedirect.com/science/article/abs/pii/S0308596120300197.

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

2. Wunsch nach mehr Datenschutz?

Verbraucherinnen und 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 **Privacy Paradox** bezeichnet.[264] 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.[265] Gleichzeitig hat eine Studie der Bitkom aus dem Jahr 2018 ergeben, dass WhatsApp von 81% der Internetnutzerinnen und -nutzer 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

---

[264] 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 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, *Wiley Online Library*, 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, siehe ScienceDirekt, 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.

[265] *Sinus Institut/YouGov*, Studie zu Datenschutz: Mehrheit der Deutschen zweifelt an Datensicherheit (2018), abrufbar unter: https://www.sinus-institut.de/media-center/presse/mehrheit-der-deutschen-zweifelt-an-datensicherheit.

geringere Wertschätzung erfahren.[266] Die dahinterstehenden Ursachen sind komplex und dürfen auch die eingeschränkte **Wahlfreiheit** der Verbraucherinnen und Verbraucher („widerwillig“[267] – d. h. lediglich mit unerwünschter Datenpreisgabe oder überhaupt nicht[268]) sowie das Ausbleiben alternativer Angebote aufgrund fehlenden Wettbewerbs nicht ausblenden. Es könnte zudem ein **Marktversagen** vorliegen, soweit keine datenschutzfreundlichen Angebote am Markt verfügbar sind oder die Nutzerinnen und Nutzer das Datenschutzniveau einzelner konkurrierender Anbieter nicht oder jedenfalls nicht mit vertretbarem Aufwand in Erfahrung bringen können.[269]

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 Verbraucherinnen und Verbraucher in ihrer Handlungsfreiheit tatsächlich einschränken: Bei einer Allensbach-Studie aus dem Jahr 2019[270] gaben Nutzerinnen und 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

---

[266] *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.

[267] 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.

[268] 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 und die dort angegebene Literatur.

[269] 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.

[270] 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.

Möglichkeit dazu hätten. Dazu zählen z. B. die Weitergabe der Daten ins Ausland oder der Zugriff auf die Adressdaten der eigenen Kontakte.[271]

III. Ermittlungsergebnisse

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

1. Interoperabilität im Spannungsfeld von Datensicherheit und Investitionsbereitschaft

Es wird in den Antworten betont, zwischen Interoperabilität und Datenschutz gebe es keine direkte Beziehung. Interoperabilität habe keine Auswirkungen darauf, wie Messenger- und Video-Dienste persönliche Daten nutzen. Eine Untergrenze für das Datenschutzniveau im Markt würde durch geltende **Datenschutzgesetze** bestimmt. Aber wenn über Interoperabilitätsziele gesprochen werde, 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, insbesondere 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 insbesondere 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 Dienst verweist auf sein eigenes Geschäftsmodell, dessen „Herz“ Interoperabilität sei. Auch auf das freie Messaging-System Matrix wird Bezug genommen. Dort habe man die meisten Herausforderungen bereits gemeistert. Für erfolgreiche Standardisierungsprozesse gebe es ebenfalls

---

[271] 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.

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

2. Freiwillige 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 nur innerhalb eines Dienstes. Ansonsten müssen Nutzerinnen und Nutzer ihre Nachrichten über „kopieren und einfügen“ 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 Bridges[272] oder Bots[273] angeboten, die allerdings keine vollständige Interoperabilität gewährleisten können. Der Matrix-Client Element betont, die Bridges für Matrix wären für jede und jeden überall erhältlich, was auch andere Befragte erwähnen. Bridges bestünden zu Microsoft Teams, Slack, WhatsApp, Telegram, Signal, IRC, Discord und XMPP. 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.

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 Messenger- und Video-Dienste mit **Open Source-Philosophie** verfolgen Interoperabilität als Geschäftsstrategie oder Leitbild. So nutzen Anbieter wie BigBlueButton oder Meet.jit.si, 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 Nutzerinnen und Nutzer aller verbundenen Server miteinander kommunizieren können.

---

[272] 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/.

[273] 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. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Bot.

Außerdem wird u. a. eine sog. WebHooks-Schnittstelle[274] angeboten sowie **Bridges und Importer**[275]. Bei führenden Video-Diensten können Verbraucherinnen und 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**[276] (Application Programming Interface, Programmierschnittstelle) zur Verfügung. Es werden auch kostenpflichtige Add-ins angeboten. Auf diese Weise könnten Nutzerinnen und Nutzer von Microsoft Teams beispielsweise aus ihrer Benutzeroberfläche heraus einen Videoanruf zu Zoom starten.

Gerade was zweiseitige Regelungen oder auf bestimmte Anbieter ausgerichtete Interoperabilitätsabkommen betrifft, sind die Dienste, die sich insbesondere auf Geschäftskundinnen und - kunden 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 Geschäftskundinnen und -kunden wird Interoperabilität auch über **proprietäre APIs** initialisiert.

---

[274] 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. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/WebHooks.

[275] Ein Importer ist eine Softwareanwendung, die eine Datendatei oder Meta-Dateninformationen in einem Format einliest und über spezielle Algorithmen in ein anderes Format konvertiert, vgl. *Wikipedia*, abrufbar unter: https://en.wikipedia.org/wiki/Importer_(computing).

[276] 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 *Talend*, abrufbar unter: https://www.talend.com/de/resources/was-ist-eine-api/.

Zusatzleistungen im Bereich der Interoperabilität sind häufig kostenpflichtig. Bei Geschäftskundinnen und - kunden mit speziellen technischen Anforderungen sei für Videokonferenzen u. ä. mehr Aufwand erforderlich. Geschäftskundinnen und - kunden hätten meist spezielle Anforderungen, wie z. B. Videoräume mit Kameras, Mikrophonen, 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 Pepix[277] angeführt. Wenn Interoperabilität über proprietäre APIs hergestellt werden soll, könnten ebenfalls Dienstleister wie Software as a Service (SaaS)[278] -Unternehmen zum Einsatz kommen, wie z. B. das Unternehmen Mio[279], 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.[280]

3. Organisatorische und technische Umsetzung einer Interoperabilitätsverpflichtung

a) Verpflichtend oder freiwillig?

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 Dienste, oder eine freiwillige Initiative. Damit einher ging die Frage nach einer Beteiligung des eigenen Dienstes und den Gründen für die jeweilige Entscheidung.

Eine **gesetzliche Interoperabilitätsverpflichtung** für alle Messenger- und Video-Dienste halten nur vier Befragte (allesamt freie Messenger-Clients) für hilfreich. Es wird argumentiert, nur eine gesetzliche

---

277 Vgl. *Pexip*, abrufbar unter: https://docs.pexip.com/admin/interoperability.htm.

278 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 *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Software_as_a_Service.

279 Vgl. *Mio*, abrufbar unter: https://m.io/external.

280 Vgl. Univention, abrufbar unter: https://www.univention.de/produkte/univention-app-center/app-katalog/matterbridge/.

Verpflichtung könne die Nutzerinteressen wiederherstellen. Eine Öffnung gegenüber Wettbewerbern widerspreche den Geschäftszielen der großen Dienste. Hilfsweise sei auch eine Verpflichtung von Diensten ab einer gewissen Anzahl an Nutzerinnen und Nutzern denkbar.

Eine gesetzliche **Verpflichtung für die größten Messenger- und Video-Dienste** 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- und Video-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. Nutzerinnen und 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 Dienst führt aus, die „Betreiber der führenden Betriebssysteme" sollten mit einer Interoperabilitätsverpflichtung belegt werden. Ein weiterer Dienst wendet sich ebenfalls den marktstarken Akteuren zu. Diese sollten es wenigstens unterlassen, technische Vorkehrungen zu treffen, um Nutzerinnen und 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. Nur weniger als die Hälfte der Befürwortenden würde sich aber 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 Marktneulingen 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 Nutzerinnen 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, wie sie im Jahr 2021 noch erforderlich waren. Eine solche Verpflichtung dürfe nur auferlegt 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 Verbraucherinnen und Verbrauchern jederzeit möglich.

b) Funktionelle und technische Gestaltung

Auf die Frage, welche Funktionen interoperabel gestaltet werden sollten, wurden von etwas mehr als der Hälfte der Befragten **Textnachrichten dicht gefolgt von Gruppenchats** genannt. Telefonie und Videotelefonie folgen knapp dahinter mit ca. 40 Prozent der Nennungen.
Bei der Frage, wie Interoperabilität technisch umgesetzt werden soll, liegt die Umsetzung über **Serverschnittstellen** vorn, gefolgt von Bridges, einem gemeinsamen Protokoll oder mittels Multi-Messengern.
Als Verschlüsselungsmethode, die bei Interoperabilität zur Anwendung kommen sollte, nennt nicht ganz die Hälfte der Befragten die **Transportverschlüsselung**, dicht gefolgt von der Ende-zu-Ende-Verschlüsselung. Mehrere Befragte betonen, die Verschlüsselung müsse von Nutzerinnen und Nutzern selbst wählbar sein, da es für alle Kombinationen von Transportverschlüsselung und Ende-zu-Ende-Verschlüsselung Anwendungsfälle gebe.
Was die Ende-zu-Ende-Verschlüsselung angehe, hätten viele Dienste eigene Lösungen entwickelt. Diese auf einen bestimmten Standard zurück zu führen, wäre keine triviale Aufgabe. Es könne nur wiederholt werden, einen Standard für einen hoch dynamischen Sektor aufzuerlegen, sei komplex, auch wenn nur an eine sehr grundlegende Form der Interoperabilität gedacht werde. Dem stimmen einige Dienste zu, die sich auch allenfalls ein schmales Interoperabilitätsmodell vorstellen können, dass auf das Text-Messaging beschränkt ist. Interoperabilität sei „knifflig“. Man selbst habe über die letzten zwanzig Jahre Erfahrungen gesammelt. Es sollte eine Kern-Zusammenstellung von Funktionen geben (beispielsweise Text - Messaging), welche die **individuellen Innovationsmöglichkeiten** nicht behindere. Diese Probleme wären schon vor Jahren gelöst worden, aber die „existierenden Kräfte“ hätten keinen Grund gehabt, dies zu berücksichtigen. Daher wäre eine Gesetzgebung „mit Biss“ wichtig. Ein führender Video-Dienst äußert sich ähnlich. Die Verpflichtung sollte auf die **interoperablen Funktionen** beschränkt sein. Bestimmte besondere Funktionen interoperabel zu gestalten, beeinflusse die Innovationsdynamik, da die Nutzerinnen und Nutzer weniger geneigt wären, zu verschiedenen „Plattformen“ zu wechseln und die Dienste daher weniger Anreize hätte, neue und innovative Funktionen zu entwickeln. Perfekte Interoperabilität verknöchere die bestehenden Technologien, die verpflichtend würden.
Zwei US-amerikanische Dienste erklären, Text Messaging und Anforderungen an eine Ende-zu-Ende-Verschlüsselung wäre weniger problembehaftet als Interoperabilität im Audio-/Video-Bereich, auch wenn sogar interoperables Text Messaging einige Mühen und Kosten erfordere. **Standardisierte ServerSchnittstellen** wären für einen solchen Ansatz, der bilaterales Text Messaging oder Gruppen-Chat ermögliche, sinnvoll. **Standardisierte Identifier** wären ebenfalls hilfreich für konsistentes Messaging und die Verhinderung von Missbrauch. Einer der Dienste hält Multi-Messenger für die am wenigsten störende Maßnahme.

Zwei Dienste weisen darauf hin, dass die Interoperabilitätsverpflichtung nicht **Qualitätseinbußen** bedeuten dürfe. Interoperabilität könne nur in einem kleinen Rahmen umgesetzt werden für Text - Messaging über standardisierte Telekommunikationsprotokolle mit Transportverschlüsselung. Das würde bedeuten, die Ende-zu-Ende-Verschlüsselung für die Nutzerkommunikation zu eliminieren.
Die Wahl des Interoperabilitätsmodells, die Art der technischen Implementierung und die unterstützten „Unterfunktionen" im Detail sollten von der Branche mittels offener und transparenter Prozesse umgesetzt werden. Bei allem sollte **Raum für Entwicklung** gegeben werden. Im Falle, dass detailliertere gesetzliche Vorgaben gemacht würden, sollte die Interoperabilität von „Cloud-Diensten" direkt zwischen den Plattformen der Dienste entworfen werden. Eine Verpflichtung dürfe nicht dem MLS Standard zuvorkommen und so eine fortschrittliche Ende-zu-Ende-Verschlüsselung aufs Spiel setzen.
Außerdem gebe es **verschiedene Wege, Interoperabilität zu erreichen**, z. B. direkt, indem jeder einen Standard unterstütze oder indirekt über proprietäre API, über welche der Austausch hergestellt werden könne. Eine Interoperabilitätsverpflichtung dürfe nicht Funktionen und Innovationen einfrieren.
Ein Dienst schlägt vor, den **Betrieb von Apps von dem Betrieb der Nachrichtenübermittelung** zu trennen. Hierfür komme eine Pflicht für „große zentrale Infrastrukturen" infrage, für „alternative Clients" Zugang zu gewähren. Außerdem sei es sinnvoll, dass Apps von großen Anbietern eine Schnittstelle definieren sowie ein föderatives oder zumindest interoperatives Modell zum Betrieb von Servern zur Nachrichtenübermittelung ermöglichen. Die existierenden E-Mail-Server und E-Mail-Clients zeigten, dass dies grundsätzlich möglich sei. Zudem liefere das „Matrix.org Projekt" ein weiteres Beispiel dafür, dass eine Definition und Implementierung von Schnittstellen zwischen den verschiedenen Komponenten auf vielleicht modernere Weise als mit den E-Mail-Standards vorgenommen werden könne. Allerdings gelte es auch hier ggf. zu beachten, dass sich die Standardisierung nicht alleine in den Händen der jeweiligen Hauptakteure befinde.
Einige Dienste haben **keine näheren Ausführungen zur Umsetzung von Interoperabilität** gemacht, da sie dies grundsätzlich ablehnen. Bei diesen Diensten handelt es sich sowohl um führende Dienste, Dienste, die mit ihrem hohen Datenschutzstandard werben sowie auch Open Source-Anwendungen. Der Zwang zur Interoperabilität sei kontraproduktiv. Ein anderer Dienst führt aus, er würde dann die eigenen Nutzerinnen und Nutzer der Gefahr aussetzen, dass ihre Daten und Nutzungsverhalten anderen Marktteilnehmern mit fragwürdigen Businessmodellen in die Hände fallen. Das sei für den Dienst nicht hinnehmbar, da man absolute Vertraulichkeit garantiere. Ein bekannter Video-Dienst bezieht sich ebenfalls auf die Wünsche der Nutzerinnen und Nutzer. Eine gesetzliche Interoperabilitätsverpflichtung sei nicht in deren Interesse. Bei Video-Diensten bestehe bereits der gegenseitige Zugang über den Web-Browser. Alles was darüber hinausgehe, gefährde die besonderen Funktionalitäten der App insofern, als dass nur noch der kleinste gemeinsame Nenner möglich sei. Auch ein Open Source-Anbieter wiederholt, durch Interoperabilität könne die hohe Innovationsgeschwindigkeit bei Videokonferenzen behindert

werden. Wenn es eine Interoperabilitätsverpflichtung geben werde, müsse diese möglichst schmal gehalten werden, um Innovationen möglichst wenig zu erschweren. Die Regelungen sollten **von der Branche erarbeitet** werden.

Demgegenüber haben viele freie Messenger-Clients auf die **Vorteile von Standardisierung** gerade in Verbindung mit Interoperabilität hingewiesen. Das Bundeskartellamt hatte die Messenger- und Video-Dienste nach der Rolle internationaler Standards befragt. Die Ausführungen dazu sind im folgenden Kapitel nachzulesen.

c) Interoperabilität durch Standardisierung

Das Bundeskartellamt hat die Messenger- und Video-Dienste befragt, welche bestehenden Standards für den Austausch und für die Verschlüsselung genutzt werden könnten, um Interoperabilität herzustellen. Die Hälfte der befragten Messenger- und Video-Dienste hat geantwortet.

Für den **Austausch** wurden WebRTC, Matrix sowie vereinzelt Acitity Pub[281], RCS, SIP, RTP, SRTP sowie das standardisierte Protokoll XMPP, insbesondere von freien Messenger Clients, genannt. Ein Dienst erwähnte zwei Standards in Entwicklung, nämlich SFrame und Web Transport. Für die **Verschlüsselung** wurde OMEMO erwähnt, der Verschlüsselungsstandard aus der XMPP-Welt, sowie TLS und MLS, das Signal-Protokoll, AES sowie DTLS, PGP[282], RSA[283], XMPP, WebRTC und Matrix.

Mehrere freie Messenger-Clients führen aus, die **Nutzung einheitlicher Standards** sei für eine Interoperabilität unabdingbar. Mit XMPP sei bereits 1999 ein Standard für den Nachrichtenaustausch im weitesten Sinne geschaffen worden und werde seitdem durch die XSF (XMPP Standards Foundation) und die IETF weiterentwickelt. Die IETF hätte auch andere weit verbreitete Standards für E-Mail oder Webseiten (HTTP) entwickelt bzw. würde solche weiterhin entwickeln.

---

[281] ActivityPub ist ein 2018 veröffentlichtes, offenes, dezentrales Protokoll für soziale Netzwerke, das vom W3C verwaltet wird. Es bietet eine Client-zu-Server-API zum Erstellen, Hochladen und Löschen von Inhalten sowie eine Server-zu-Server-API für eine dezentrale Kommunikation, siehe *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/ActivityPub.

[282] PGP dient der Verschlüsselung von E-Mails und ist Basis von OpenPGP, einem weit verbreiteten E - Mail-Verschlüsselungsstandard, vgl. https://www.openpgp.org/.

[283] RSA (Rivest-Shamir-Adleman) ist ein asymmetrisches kryptographisches Verfahren, das sowohl zum Verschlüsseln als auch zum digitalen Signieren verwendet werden kann. Es verwendet ein Schlüsselpaar, bestehend aus einem privaten Schlüssel, der zum Entschlüsseln oder Signieren von Daten verwendet wird, und einem öffentlichen Schlüssel, mit dem man verschlüsselt oder Signaturen prüft. Der private Schlüssel wird geheim gehalten und kann nicht mit realistischem Aufwand aus dem öffentlichen Schlüssel berechnet werden, siehe Kapitel D.I.4.a oder siehe *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/RSA-Kryptosystem.

Außerdem wären zumindest sowohl der Facebook Messenger als auch WhatsApp, Google Talk und der KIK-Messenger sogar auf Basis von XMPP entstanden. Das bedeutet, dass die beteiligten Firmen das standardisierte und öffentliche Protokoll XMPP (und ejabberd als eine der frei verfügbaren Open Source Server-Implementierungen von XMPP) verwendet hätten, um auf deren Basis durch **proprietäre (firmeninterne) Erweiterungen, die sie nicht in den öffentlichen Standardisierungsprozess haben zurückfließen lassen**, ihr Produkt zu kreieren. Es wäre für diese Firmen ein Leichtes gewesen, ihre Veränderungen und Erweiterungen von Anfang an in den Standardisierungsprozess einzubringen, so dass alle davon profitiert hätten. Von untereinander inkompatiblen Insellösungen profitierten diese Unternehmen im Gegensatz zur Einhaltung von internationalen Standards aber weit mehr, da die Nutzerinnen und Nutzer so gezwungen wären, bei den großen Dienstanbietern ein Konto zu eröffnen, was es diesen Diensten erlaube, eine Menge Nutzerinnen und Nutzer auf sich zu vereinen und deren Daten zu sammeln und zu analysieren. Eine solche Machtposition lade auch zu Missbrauch der Daten ein, da die Nutzerinnen und Nutzer durch die entstandene Monopolposition nicht ohne weiteres auf andere Alternativen ausweichen könnten.

Mit E-Mail hingegen sei ein Nachrichtensystem geschaffen worden, das den Nutzerinnen und Nutzern die maximale Freiheit hinsichtlich der Wahl des Anbieters ermögliche (sie könnten sogar selbst seinen eigenen E-Mail-Server betreiben und damit unabhängig von fremden Anbietern sein). Ein ähnliches System für die Echtzeitkommunikation via „Chat“ und (Video-) Telefonie sei mehr als wünschenswert - ja, sogar wirtschaftlich sinnvoll und gesellschaftlich erforderlich.

Dabei sei die **verpflichtende Zusammenarbeit verschiedener Anbietersysteme** (angestrebte Interoperabilität) eine mögliche Lösung, um die großen Anbieter kostenloser Chat-Dienste zur Interoperabilität zu bringen. Für die Anbieter kommerzieller Chat-Dienste sei das Ziel durch öffentliche und private Ausschreibungen erreichbar, bei denen als wesentlicher Punkt das **Einhalten eines Standard-Protokolls** (XMPP) Bestandteil sein müsse. So könnten Anbieter unabhängig voneinander ihre Systeme entsprechend anpassen, wenn sie kommerzielle Nutzerinnen und Nutzer erreichen wollen.

Nach Ansicht der befragten Dienste sollten gerade in der Politik, der Verwaltung, in Behörden und Ämtern möglichst nur noch solche Lösungen zum Einsatz kämen, die diese Anforderung auch erfüllen oder absehbar auch erfüllen würden.

4. Auswirkungen von Interoperabilität

Das Bundeskartellamt hat die Branche schließlich auch zu den allgemeinen Auswirkungen von Interoperabilität ausführlich befragt. Die Ermittlungsergebnisse werden zunächst im Überblick dargestellt (dazu unter a)). Anschließend werden Ausführungen zu einzelnen Aspekten ausführlicher dargelegt (dazu unter b) bis g)).

a) Ermittlungsergebnisse im Überblick

Konkret wurden die Dienste danach gefragt, wie sich die Herstellung von Interoperabilität unter den Aspekten Nutzerzahlen, Umsätze, Wettbewerbsintensität, Datenschutzniveau, Datensicherheitsniveau und Innovationstätigkeit auf ihren Dienst auswirken würde. Die Befragten konnten dabei Antworten zwischen „sehr negativ“ (-2) und „sehr positiv“ (+2) auswählen.
Um die unterschiedlichen Antworten sinnvoll darstellen zu können, wurden die befragten Dienste soweit wie möglich fünf verschiedenen Gruppen zugeordnet und für jede dieser Gruppen eine separate Auswertung vorgenommen.

- Große geschlossene Messenger-Systeme (6 Dienste)
- Führende Videokonferenzdienste (4 Dienste)
- Konkurrierende Video-Dienste (9 Dienste)
- Freie Messenger Clients (12 Dienste)
- Open Source-Dienste (5 Dienste)

Insgesamt 7 befragte Dienste konnten **keiner dieser Gruppen eindeutig zugeordnet** werden und aufgrund ihrer Heterogenität auch keine eigene Gruppe bilden. Besonders relevante Einschätzungen bzw. Erläuterungen dieser Dienste werden in der nachstehenden Auswertung jedoch punktuell dargestellt.

Auf die Frage nach den Auswirkungen von Interoperabilität auf den eigenen Dienst haben sich für die verschiedenen Gruppen die folgenden durchschnittlichen Einschätzungen ergeben (siehe Abbildung 14):[284]

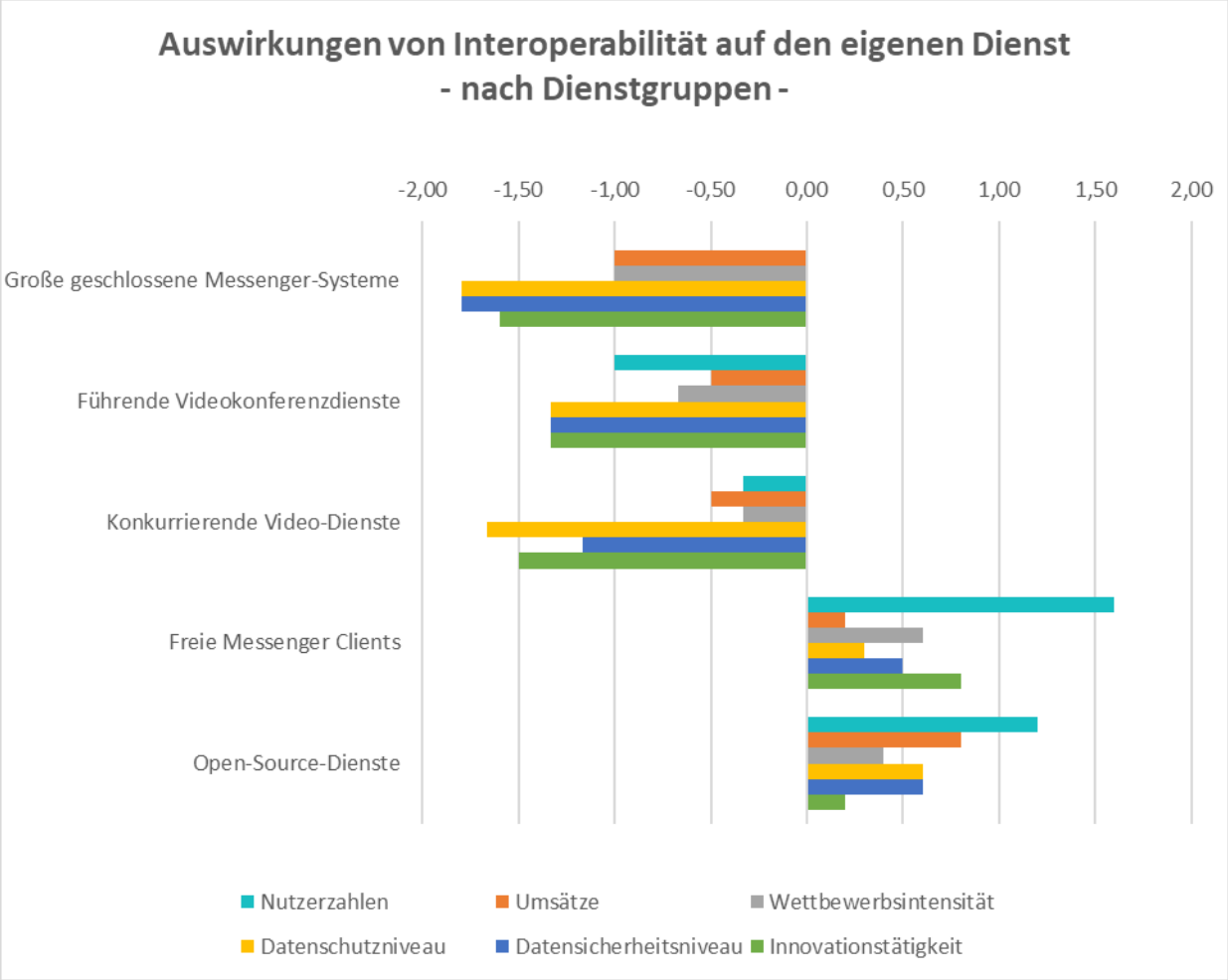


Abbildung 14: Auswirkungen von Interoperabilität auf den eigenen Dienst – nach Dienstgruppen

Werden die Ermittlungsergebnisse nicht nach den verschiedenen Gruppen von Diensten sondern nach den verschiedenen Auswirkungen von Interoperabilität ausgerichtet, ergibt sich folgendes Bild (siehe Abbildung 15):

[284] Bei der Bewertung der nachfolgend dargestellten Befragungsergebnisse ist zum einen zu berücksichtigen, dass den einzelnen Gruppen unterschiedlich viele Dienste angehören und zum anderen, dass die Marktbedeutung der einzelnen Dienste (und Gruppen) sehr unterschiedlich ist. Darüber hinaus werden lediglich Durchschnittwerte für jede Gruppe dargestellt; die Einschätzung einzelner Gruppenmitglieder kann hiervon durchaus abweichen. Der Durchschnittswert „O“ ist in der Graphik nicht sichtbar.

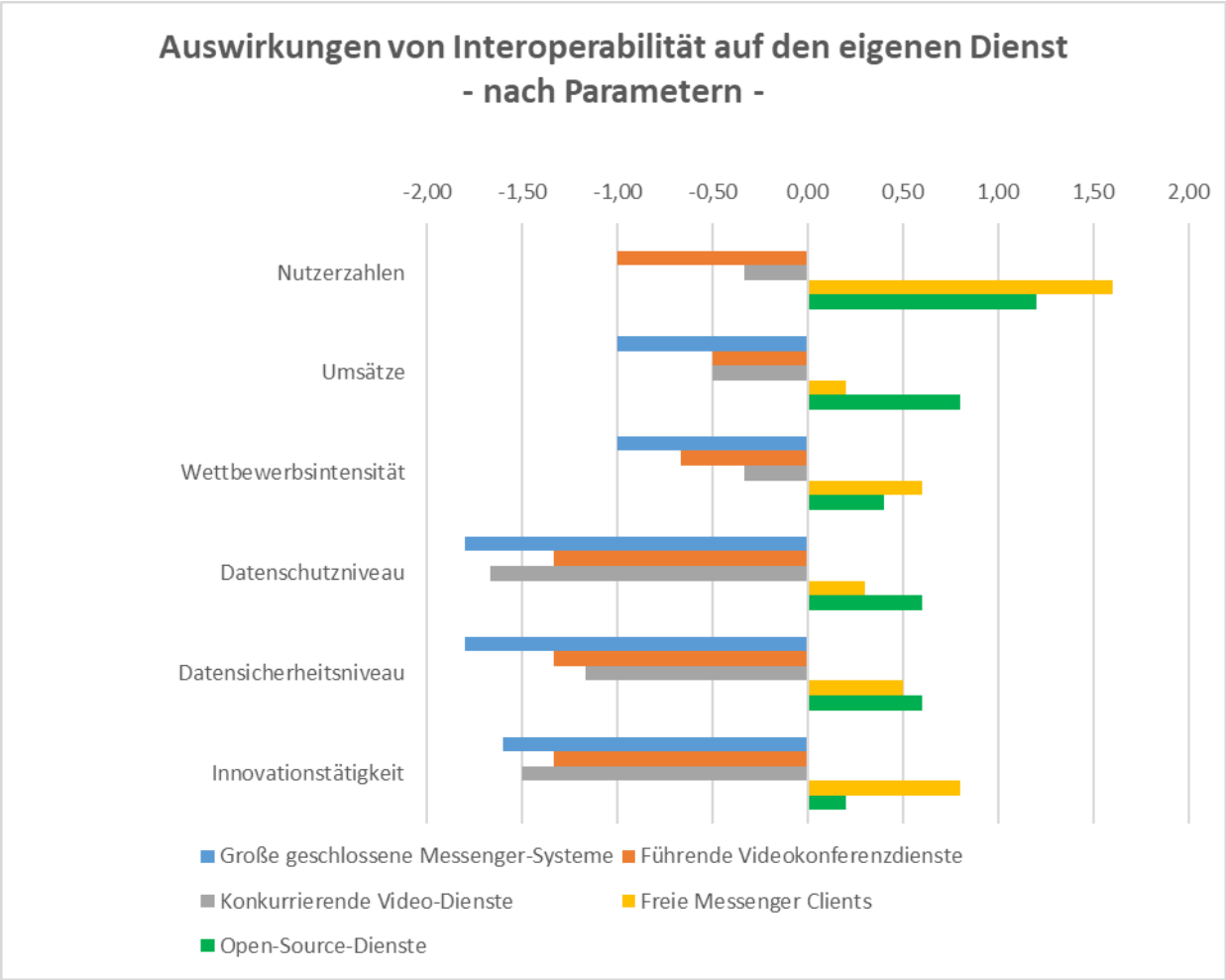


Abbildung 15: Auswirkungen von Interoperabilität auf den eigenen Dienst - nach Parametern

Die beiden Graphiken zeigen deutlich, dass sowohl die großen geschlossenen Messenger-Systeme als auch die Videokonferenz-Dienste für das eigene Unternehmen insgesamt mit negativen Auswirkungen von Interoperabilität rechnen. Besonders negativ haben sich dabei die großen geschlossenen Messenger-Systeme geäußert. Lediglich in Bezug auf die eigenen Nutzerzahlen erwarten diese Dienste im Durchschnitt keine Auswirkungen (beim Wert „0“ ist der Balken nicht sichtbar). Die stärksten negativen Effekte werden von den drei genannten Gruppen für das **Datenschutzniveau, das Datensicherheitsniveau und die Innovationstätigkeit** des eigenen Dienstes erwartet. Kritisch haben sich in diesem Zusammenhang auch Dienste geäußert, die mit besonders intensiven Datenschutzmaßnahmen werben. Diese sind in den oben definierten Gruppen nicht enthalten.
Die Gruppen der freien Messenger Clients und der (kleinen) Open-Source-Dienste erwarten hingegen positive Auswirkungen von Interoperabilität auf den eigenen Dienst. Besonders günstig wird die Entwicklung der eigenen Nutzerzahlen eingeschätzt. Die Open Source-Dienste rechnen dabei auch mit einer positiven Umsatzentwicklung.

Einige Dienste haben ihre Einschätzungen auch näher begründet. Manche Dienste betonen in diesem Zusammenhang allerdings auch die hohe Dynamik des Marktes, die eine Vorhersage der Entwicklungen nahezu unmöglich mache:

Mehrere freie Messenger Clients erwarten höhere **Nutzerzahlen** für den eigenen Dienst, da dieser bei Interoperabilität eine größere Aufmerksamkeit bekäme und leichter zugänglich wäre, wenn die „Bindung an Inselsysteme“ entfalle. Insgesamt würden sich nach dieser Einschätzung die Nutzerinnen und Nutzer - wie bei E-Mail - stärker auf verschiedene Dienste verteilen. Gleichzeitig weist ein freier Messenger-Client allerdings darauf hin, dass die Zahl der installierten Apps/Clients für die Branche insgesamt sinken würde, da Nutzerinnen und Nutzer bei Interoperabilität nicht mehr mehrere Dienste-Apps gleichzeitig installieren müssten. Zwei andere Dienste vermuten hingegen, dass die Nutzerinnen und Nutzer aus Bequemlichkeitsgründen eher **zu den Marktführern wechseln** würden, da die Differenzierungsmerkmale der kleineren Dienste durch Interoperabilität wegfielen. Ein führender Video-Dienst befürchtet, dass die mit erweiterter Interoperabilität verbundene Einigung auf den kleinsten gemeinsamen Nenner die Attraktivität und damit die Nachfrage nach Videokonferenzdienstleistungen insgesamt schmälern könnte.

In Bezug auf die **Umsätze** verweisen mehrere Dienste auf den - zumindest im Business-Bereich bestehenden - positiven Zusammenhang zwischen Nutzerzahlen und Umsatz. Zwei führende, bei den Verbraucherinnen und Verbrauchern beliebte Dienste erwarten einen Umsatzrückgang bei Business-Anwendungen, da Qualität und Nutzererlebnis durch Interoperabilität schlechter würden. Ein anderer (kostenpflichtiger) Dienst, der mit einem hohen Datenschutzniveau wirbt, weist darauf hin, dass auch private Nutzerinnen und Nutzer keinerlei Zahlungsbereitschaft mehr hätten, wenn das (vermeintlich) gleiche Produkt von einem anderen Dienst kostenlos angeboten würde.

Auch zu den Auswirkungen von Interoperabilität auf die **Wettbewerbsintensität** und die **Innovationstätigkeit** haben die befragten Dienste recht unterschiedliche Einschätzungen und Begründungen vorgetragen. Sowohl proprietäre als auch Open Source-Videokonferenzdienste geben an, dass der Wettbewerb zwischen den Diensten aktuell bereits intensiv sei und durch Interoperabilität eher reduziert würde, wenn diese Innovationen und Differenzierungsmöglichkeiten begrenze. Auch mehrere Dienste aller Gruppen gehen eher davon aus, dass die Innovationstätigkeit – wie bei Telekommunikation oder E-Mail – erlahmen würde und Interoperabilität allenfalls zu einer Stärkung der großen („amerikanischen“) Anbieter bzw. des Wettbewerbs zwischen diesen führen könnte. Mehrere freie Messenger-Clients bzw. Open-Source-Dienste erwarten hingegen eine Intensivierung des Wettbewerbs (zu ihren Gunsten) und folglich auch eine Verstärkung der Innovationstätigkeit, da Nutzerinnen und Nutzer bei Interoperabilität leichter wechseln könnten. Die Begründungen zu dieser zentralen Einschätzungsfrage zeigen deutlich, dass die Befragten unterschiedliche Vorstellungen davon

haben, ob bei Interoperabilität (hinreichende) **Differenzierungsmöglichkeiten** für die einzelnen Dienste erhalten bleiben oder nicht und wie die Nutzerinnen und Nutzer darauf reagieren.
Im Hinblick auf das **Datenschutzniveau** und das **Datensicherheitsniveau** weisen einzelne Dienste, darauf hin, dass „große Dienste mit schlechten Datenschutzstandards“ dann auch Zugriff auf die Daten anderer Dienste hätten. Ein gemeinsames Identitätsmanagement und die Vielzahl neuer Schnittstellen würde sich nach dieser Einschätzung negativ auf die Datensicherheit auswirken. Daneben wird von den Kritikern von Interoperabilität wiederum eine Vereinheitlichung auf dem kleinsten gemeinsamen Nenner befürchtet. Demgegenüber tragen einige Befürworter vor, dass Nutzerinnen und Nutzer dann zu Diensten mit einem besonders hohen Schutz- bzw. Sicherheitsniveau wechseln könnten. Die Standardisierung von Schnittstellen und die Dezentralisierung der Datenverarbeitung würde bereits zu einer Verbesserung des aktuellen Niveaus führen. Von einigen Diensten wird schließlich betont, dass der Datenschutz gesetzlich geregelt ist und Interoperabilität hierauf kaum Einfluss haben dürfte. Auch die Erläuterungen der Dienste zu dieser Aussage belegen, dass die Marktteilnehmer sehr unterschiedliche Vorstellungen von den Auswirkungen einer Interoperabilität auf **Datensicherheit und Datenschutz** haben. Dies ist vermutlich auf die unterschiedlichen Geschäftsmodelle und divergierende Einschätzungen des Verbraucherverhaltens zurückzuführen.
In einer weiteren Frage sollten die Messenger- und Video-Dienste angeben, inwieweit sie bestimmten **Aussagen zum Thema Datenschutz und Interoperabilität** zustimmen (siehe Abbildung 16). Die Thesen lauteten: „Das Datenschutzniveau bei Messenger- und Video-Diensten muss verbessert werden“, „Das Verschlüsselungsniveau bei Messenger- und Video-Diensten muss verbessert werden“, „Eine Interoperabilität von Messenger- und Video-Diensten ist grundsätzlich wünschenswert“, „Die Herstellung von Interoperabilität sollte gesetzlich vorgeschrieben werden“, „Eine gesetzlich vorgeschriebene Interoperabilität würde vor allem den großen Messenger- und Video-Diensten nutzen“, „Die Verbraucherinnen und Verbraucher in Deutschland wünschen sich eine Interoperabilität von Messenger- und Video-Diensten“. Die Skala der Antwortmöglichkeiten reichte auch hier wieder von „Stimme gar nicht zu“ (-2) bis „Stimme voll zu“ (+2).
Im Gegensatz zu freien Messenger-Diensten, Open Source-Diensten und Wettbewerbern der führenden Video-Dienste, sehen die großen Messenger-Dienste und die führenden Video-Dienste keinen Bedarf für eine **Verbesserung des Datenschutzniveaus**.

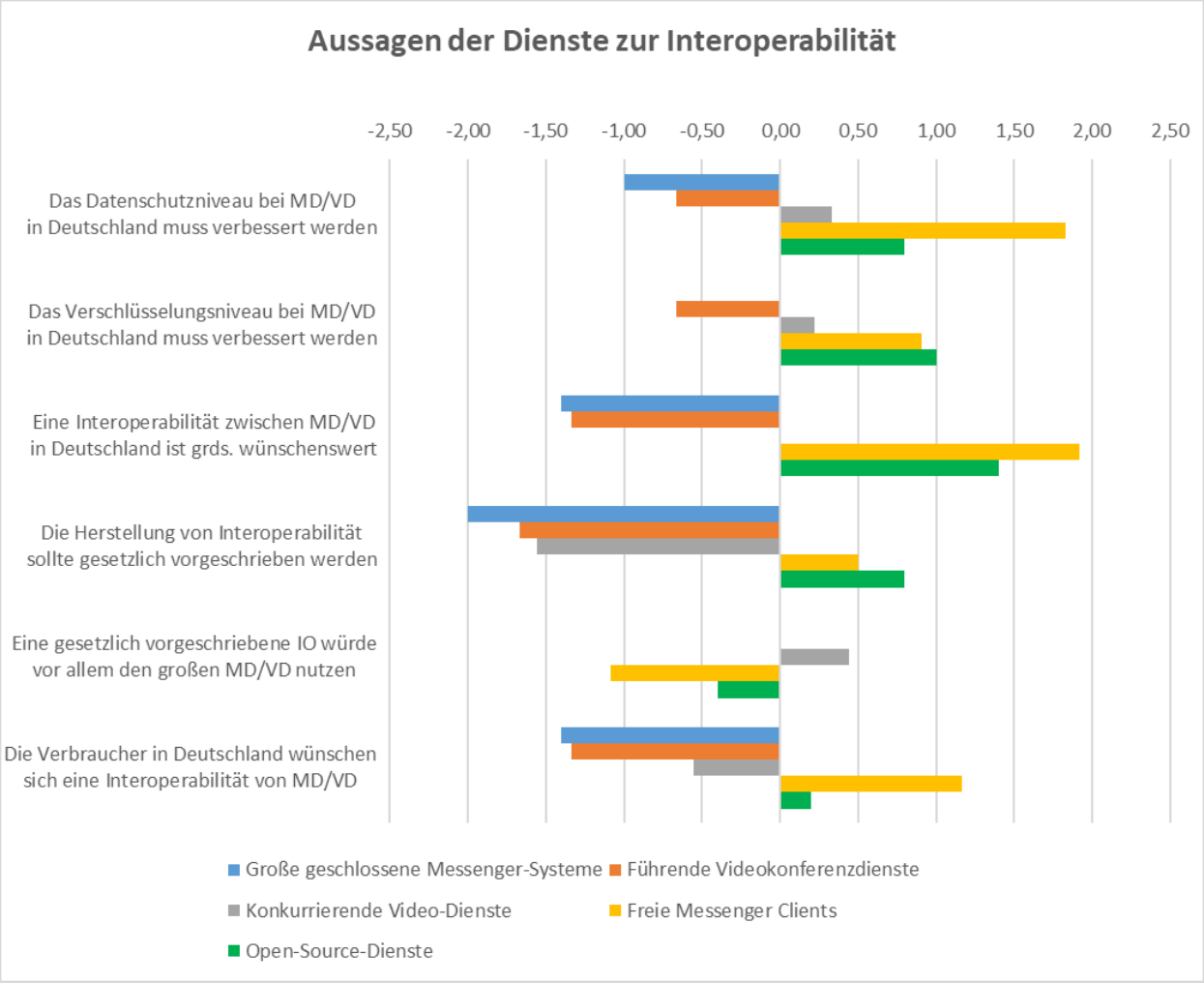


Abbildung 16: Aussagen zur Interoperabilität

Was das **Datenverschlüsselungsniveau** angeht, ergibt sich im Durchschnitt kein klares Meinungsbild der großen geschlossenen Messenger-Systeme (kein Balken bei Wert „0“), während die führenden Videokonferenzdienste ablehnend reagiert haben.

Die Aussage, dass eine **gesetzlich vorgeschriebene Interoperabilität** vor allem den großen Diensten nutzen würde, wird von den Betroffenen uneinheitlich bewertet (kein Balken): Zwei große Dienste stimmen dieser Aussage voll zu und zwei andere große Dienste stimmen dieser Frage gar nicht zu. Die Antworten der konkurrierenden Video-Dienste sind im Vergleich zu den großen Diensten etwas differenzierter: Sie sehen im Durchschnitt zwar einen leichten Verbesserungsbedarf und Vorteile für die großen Dienste, aber eher keinen Verbraucherwunsch.

Auch die Einschätzungen zu den genannten Thesen zeigen, dass die großen geschlossenen Messenger-Systeme und die führenden Videokonferenzdienste die Möglichkeit **einer gesetzlich vorgeschriebenen Interoperabilität** deutlich ablehnen. Im Gegensatz dazu fallen die Antworten der freien Messenger-Clients und der Open-Source-Dienste wiederum klar zugunsten von Interoperabilität aus, auch eine

entsprechende gesetzliche Vorschrift wird hier befürwortet. Die Gefahr, dass eine gesetzlich vorgeschriebene Interoperabilität vor allem den großen Messenger- und Video-Diensten nutzen würde, sehen diese Dienste insgesamt zwar eher nicht; zwei dieser Dienste stimmen dieser Aussage allerdings voll zu, genauso wie zwei besonders datenschutzorientierte Dienste, die in den genannten Gruppen und der graphischen Darstellung nicht enthalten sind.

Bei den (optionalen) Begründungen zu den abgegebenen Einschätzungen werden von einzelnen Diensten verschiedene Aspekte angesprochen, die in den folgenden Kapiteln ausführlich dargelegt werden und hier nur kurz zusammengefasst werden sollen: Mehrere Befragte tragen vor, dass die Nutzung eines gemeinsamen **internationalen Standards** wie XMPP entscheidend sei und dies z. B. bei öffentlichen Ausschreibungen berücksichtigt werden sollte. Einige Dienste weisen darauf hin, dass es für große Messenger- und Video-Dienste leichter wäre, den für die Herstellung von Interoperabilität erforderlichen **Technologieaufwand** zu bewältigen, während dies für kleine Dienste eine erhebliche Belastung darstelle. Zwei große, bei Verbraucherinnen und Verbrauchern beliebte Dienste betonen, dass allein die Regelungen des Europäischen Kodex für die elektronische Kommunikation (EKEK) für eine mögliche Interoperabilitätsverpflichtung maßgeblich wären und diese nicht durch abweichende nationale Vorschriften unterlaufen werden dürften. Eine Aufnahme einer Interoperabilitätsverpflichtung für Messenger-Dienste in den Pflichtenkatalog des DMA war zu diesem Zeitpunkt noch nicht absehbar.

Zu den **Wünschen der Verbraucherinnen und Verbraucher** tragen einige Dienste vor, dass diese sich über die Vielzahl unterschiedlicher Apps beschweren würden; andere Dienste betonen, dass die parallele Nutzung verschiedener Apps für die Verbraucherinnen und Verbraucher in Ordnung sei. Einzelne Dienste weisen zudem darauf hin, dass die Verbraucherinnen und Verbraucher nicht wirklich wüssten, was Interoperabilität tatsächlich bedeuten könnte.

Die Themen, die die Dienste am meisten umtreiben, sind jedoch mögliche Auswirkungen von Interoperabilität auf das Angebot innovativer Funktionen und die Möglichkeit, sich auch unter Interoperabilität zu differenzieren.

b) Innovationsanreize und Differenzierungsmöglichkeiten

Der weit überwiegende Teil der Befragten äußert, dass Interoperabilität und die damit einhergehende Standardisierung **Innovationsprozesse hemmen und Produktdifferenzierung schwächen** würde. Es müsse sich auf den kleinsten gemeinsamen Nenner geeinigt werden, was auch zu Fehlallokationen führe. Sowohl Dienste mit Schwerpunkt Messaging, die bei Verbraucherinnen und Verbrauchern besonders populär sind, als auch bekannte Video-Dienste argumentieren in dieser Frage einheitlich. Da die Angebote durch Interoperabilität einheitlicher würden, wären Kundinnen und Kunden weniger geneigt, zwischen den Diensten zu wechseln. Die Dienste 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 vor allem im Geschäftskundensegment. Es gebe eine Reihe von Diensten, die sowohl über den Preis als auch über die Entwicklung neuer Funktionen miteinander in intensivem Wettbewerb um Kundinnen und Kunden - insb. auch Geschäftskundinnen und - kunden - 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 Nutzerinnen und 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 Teilnehmende 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 Nutzerinnen und 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-Dienst zieht den Vergleich mit traditionellen Telefondiensten heran. Diese wären interoperabel, aber es gebe enge Grenzen, was jeder Dienst 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 Nutzerinnen und 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 Verbraucherinnen und Verbraucher zurückgehen. Zweitens werde die **Vormachtstellung der größten Akteure** zementiert. Abwanderungen bei kleinen Wettbewerbern wären absehbar, da sie ihrer Differenzierungsmöglichkeiten beraubt wären.

Auf mögliche zukünftige Open Source-Implementierungen eines Standards, z. B Open MLS, 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 Nutzerinnen und 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 Diensten 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.

c) Interessen der Verbraucherinnen und Verbraucher (Nutzererlebnis und Multi - Homing)

aa) Nutzererlebnis

Mehrere Dienste nehmen die Perspektive der Verbraucherinnen und Verbraucher ein und sorgen sich um das Nutzererlebnis. Unterschiedliche Einschätzungen ergeben sich insb. auch daraus, dass die Dienste 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 fortschrittliche Videokonferenzen 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 Nutzerinnen und Nutzer nicht mehr interessant. Das **Nutzererlebnis** sei dann minderwertig. Dies gelte auch, wenn es bei Interoperabilität nur zu einer

Vereinbarung über Basisfunktionen käme, und weitere **zusätzliche Funktionen** daneben betrieben werden könnten. Abgesehen davon, dass dies ebenfalls außerordentlich aufwendig sei, könne der Anspruch der heutigen Nutzerinnen und 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 Dienst 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 Dienst 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 Verbraucherinnen und 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 gegen Missbrauch anzugehen.
Auch ein anderer Befragter weist darauf hin, dass es für die Verbraucherinnen und 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 Nutzerinnen und Nutzern desselben Dienstes verwenden können.

bb) Multi - Homing

Schließlich weisen mehrere vorrangig von Verbraucherinnen und Verbrauchern genutzte Messenger- und Video-Dienste darauf hin, dass die Verbraucherinnen und 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 Verbraucherinnen und Verbrauchern diese Flexibilität nehmen.

Es gebe keine Hinweise, dass Verbraucherinnen und 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 Verbraucherinnen und Verbrauchern geschätzt. Die meisten Dienste könnten von verschiedenen Geräten ohne zusätzliche Kosten genutzt werden. Die Nutzerinnen und Nutzer könnten sich so ihre Messenger-Welt zuschneiden und bestimmte Funktionen für bestimmte Aufgaben oder Nutzergruppen verwenden (z. B. ein Dienst für Familie, Freundinnen und Freunde, einer für Geschäftliches usw.). Den Verbraucherinnen und Verbrauchern diese Möglichkeit zu nehmen, entspreche nicht den Grundsätzen der Wettbewerbspolitik.

d) 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 Dienste 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 Dienste geöffnet, die Datensicherheit nicht ernst nähmen. Die meisten Marktteilnehmer richten das Augenmerk aber auf die Verschlüsselung (dazu unter aa)) und Identitätsmanagement (dazu unter bb)).

aa) 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 funktioniere, 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 Nutzerinnen und Nutzer fähig sein, die anspruchsvolle Software zu betreiben. Ältere oder weniger gute Geräte wären hier im Nachteil, was Nutzerinnen und 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. Verbraucherinnen und Verbraucher könnten zu sicheren Messenger- und Video-Diensten wechseln.

bb) 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. Messenger- und Video-Dienste verwenden verschiedene **Identifier**, d. h. Identifizierungsmerkmale, anhand derer Nutzer eindeutig identifiziert und registriert werden können. Das kann - wie im Abschnitt D.II.1. beschrieben - z. B. eine Mobilfunknummer, eine E-Mail-Adresse, eine ID oder eine Chatkonto sein, die dann eingegeben bzw. erstellt werden müssen, um den Dienst nutzen zu können.[285]
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 **Meta-Daten** garantiert werden. Eine technische Lösung dafür existiere noch nicht.
Ein Dienst, der sich insbesondere an Nutzerinnen und Nutzer wendet, die auf Datenschutz großen Wert legen, resümiert, all dies sei sicherlich nicht im Sinne der Verbraucherinnen und Verbraucher. Für die Nutzerinnen und Nutzer werde die **Sicherheit der Kommunikation intransparent und ungewiss**. Der Anbieter führt auch an, die Nutzerinnen und Nutzer wüssten nicht, welche App das Gegenüber verwendet.

---

[285] 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/.

e) 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.

Nutzerinnen und Nutzer könnten bei Interoperabilität einfacher zu datenschutzfreundlichen und sicheren Diensten **wechseln**. Dienste, 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 Dienst 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 **Meta-Daten** geht. Kommunikations-Meta-Daten wären für den Datenschutz höchst brisant. Je mehr unterschiedliche Dienste 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 Verbraucherinnen und Verbraucher noch ihre Betroffenenrechte ausüben können. Die Dienste selbst müssten ihre Daten mit anderen Messenger- und Video-Diensten teilen und würden die Kontrolle über die Daten ihrer Nutzerinnen und Nutzer verlieren, wären aber weiterhin verantwortlich, alle Funktionen anzubieten.

f) 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 zwinge, sich auf den kleinsten gemeinsamen Nenner zu einigen. Dadurch leide die „User Experience“ im Zuge schlechterer Servicequalität, was sich insbesondere bei Geschäftskundinnen und -kunden 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 und Abnehmerinnen 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. Nutzerinnen und Nutzer würden sich auf die Dienste verteilen, wenn es keine geschlossenen Systeme mehr gebe. Es könnten mehr Nutzerinnen und Nutzer erreicht werden, so dass auch nicht mehr so viele Messenger gleichzeitig betrieben werden müssten. Bessere Austauschmöglichkeiten würden die Nutzerinnen und Nutzer auf bereits existierende Lösungen aufmerksam machen. Interoperabilität mit den bisher abgeschotteten großen Diensten steigere 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 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 Dienst resümiert mit „niemand bezahlt, wenn es das vorgeblich selbe gratis gibt“.

g) Wettbewerbsintensität

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

Einige Video-Dienste bezeichnen ihr Wettbewerbsumfeld als hoch kompetitiv. Etablierte bekannte Namen stünden mit Marktneulingen und Nischenanbietern im Wettbewerb. Ein Dienst 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 erwartet. 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 Nutzerinnen und Nutzer zu den großen Plattformen abwandern. Die Position der **Marktführer werde zementiert** und der Wettbewerb erlahme. Ein Dienst 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 Nutzerinnen und Nutzer größerer Dienste attraktiver werden. Auch einige andere freie Messenger-Clients erwarten demgegenüber eine **erhöhte Wettbewerbsintensität**, wenn die Verbraucherinnen und Verbraucher im Zuge von verpflichtender Interoperabilität nicht mehr an die Inselsysteme gebunden wären und leichter wechseln könnten.

5. Interoperabilität und Standardisierung im Lichte der Brancheninteressen

a) Der richtige Weg?

Die Auferlegung eines möglichen vollständigen Standardisierungsprozesses im Zuge eines insbesondere 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 verbliebe 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 nochmals, 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 Dienste 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 Dienste 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 Marktteilnehmenden 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 Marktteilnehmende** 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, müssten 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 identifiziere als auch die globalen Standards erarbeite und immer wieder weiterentwickele, um die Anforderungen zu erfüllen. Nur so könne verhindert werden, dass veraltete Technologien festgeschrieben werden.

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 Marktteilnehmenden, 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, insbesondere auch die Protokollstandardisierung, für das Internet entwickelt und deren Durchsetzung gefördert. Als Beispiel werden XMPP, TLS[286], SIP[287] und WebRTC genannt. Die IETF verfüge auch über die 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

---

[286] Transport Layer Security, auch bekannt unter der Vorgängerbezeichnung Secure Sockets Layer, ist ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet, vgl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Transport_Layer_Security.

[287] Das Session Initiation Protocol (SIP) ist ein Netzprotokoll zum Aufbau, zur Steuerung und zum Abbau einer Kommunikationssitzung zwischen zwei und mehr Teilnehmern, vgl. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Session_Initiation_Protocol.

Bereiche wie „Infrastruktur/Transport/Access Layer“ mit standardisierten Leistungen und weniger auf Anwendungsfälle bei dem hoch differenzierten Bereich „Service Layer“.

Etwas mehr als 25% der Messenger- und Video-Dienste sind der Auffassung, dass auch die **EU-Kommission** an einem Standardisierungsprozess beteiligt sein sollte.[288] 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 Dienste 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 Marktteilnehmenden - 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-Dienst - 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 Marktteilnehmenden 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 sowie die Matrix.org Foundation.

Inzwischen wurde auf europäischer Ebene – wie beschrieben - im DMA ein Interoperabilitätsregime beschlossen. Die von der Branche geäußerten Meinungen und Kommentare werden daher mit der

[288] Die hier ausgewerteten Antworten hat das Bundeskartellamt im Sommer 2021, deutlich vor der Trilog-Einigung über den DMA im März 2022, aufgenommen.

verabschiedeten Lösung verglichen und mit den Erwartungen zur zukünftigen Marktentwicklung in Verbindung gesetzt.

IV. Fazit und Schlussfolgerungen

Das Bundeskartellamt geht in diesem Bericht der Leitfrage nach, wie das Datenschutzniveau in Deutschland verbessert werden kann. Eine besondere Rolle spielt dabei, **welche Auswirkungen Interoperabilität auf das Datenschutzniveau** haben könnte. Verschiedentlich waren Erwartungen geäußert worden, dass Verbraucherinnen und Verbrauchern durch Interoperabilität der Wechsel zu datenschutzfreundlichen Messenger-Diensten erleichtert und dadurch die Datenschutzqualität in diesem Bereich gefördert werden kann. 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.

Das Bundeskartellamt hatte bereits im Zwischenbericht betont, dass politische Maßnahmen und rechtliche Vorgaben aufgrund der **Heterogenität der Branche** für die betroffenen Unternehmen und Anwendungen sehr unterschiedliche Auswirkungen haben können. Daraus ergeben sich Anforderungen für jegliche behördliche oder gesetzgeberische Maßnahmen, die sich auf die Beseitigung von Problemlagen richten. Dabei sollten nicht nur diese berücksichtigt, sondern auch **Chancen für die weitere Marktentwicklung erhalten** werden (dazu unter 1.). Das Bundeskartellamt hat im vergangenen Jahr 2021 ein Stimmungsbild zur Interoperabilität und den Auswirkungen auf das Datenschutzniveau ermittelt. Nachdem der deutsche Gesetzgeber mit § 19a GWB gegenüber dessen Adressaten auch Untersagungen hinsichtlich mangelnder Interoperabilität ermöglicht, ist nun auf europäischer Ebene im Digital Markets Act eine **Interoperabilitätsverpflichtung** für die „Gatekeeper“ der Branche der Messenger- und Video-Dienste initiiert worden. Zunächst wird festgehalten, dass Maßnahmen zur Verbesserung des Datenschutzniveaus bei einzelnen Diensten die wettbewerbliche Entwicklung der Branche insgesamt im Blick behalten sollten. Gesamtwirtschaftliche Effekte sind dabei einzubeziehen. Dann wird untersucht, wie sich die im Vorfeld geäußerten Meinungen der Branche und die aktuellen gesetzgeberischen Pläne im Vergleich darstellen (dazu unter 2). Anschließend stehen die Auswirkungen von Interoperabilität auf den Datenschutz und die damit einhergehenden Anstrengungen bei der Datensicherheit im Vordergrund. Wiederum sind es die Verhaltensweisen und Entscheidungen der Verbraucherinnen und Verbraucher, die maßgeblichen Einfluss auf die Bewertung haben (dazu unter 3).

1. Potential nutzen, Kollateralschäden vermeiden

Die Ermittlungen haben ein vielgestaltiges Bild der Branche gezeichnet. Dies betrifft nicht nur die unterschiedliche Verwendung und Einsatz der technischen Kriterien wie Protokolle, Server,

Verschlüsselung oder Identifier, die für die Datensicherheit und den Datenschutz eines Messengers maßgeblich sind. Darüber hinaus unterscheiden sich die Dienste auch hinsichtlich ihrer Funktionen, ihrer Geschäftsmodelle und ihrer wirtschaftlichen Bedeutung. Das Spektrum der Branchenteilnehmer geht weit über die bekannten und verbreiteten Messenger- und Video-Dienste hinaus.

In der Branche der Messenger- und Video-Dienste sind internationale diversifizierte Konzerne mit **breitem technologischem oder digitalem Spektrum** mit hohen Umsätzen tätig. Dies betrifft nicht nur WhatsApp und Facebook Messenger, die zum Digitalkonzern Meta gehören, sondern auch die Technologie-Konzerne Cisco mit Webex und auch weitere Digitalkonzerne wie Alphabet (Google) mit Google Meet und Google Chat[289] sowie Microsoft (Teams, Skype), jeweils mit erheblichen Machtpositionen, insbesondere bei Betriebssystemen für mobile und konventionelle Anwendungen. Viele führende Messenger- und Video-Dienste besitzen also nicht nur erhebliches Know-how, sondern auch starke Positionen in Bereichen, die für die Funktionen „Messaging“ und „Videokonferenzen“ wichtig sind. Hinzu kommen Großkonzerne, die ihren Schwerpunkt im Ausland haben, wie z. B. die japanische Line Corporation, die zur mächtigen und diversifizierten südkoreanischen Naver Corporation gehört, die erfolgreich eine Suchmaschine betreibt, oder WeChat als Teil der chinesischen Staatsmacht, die zwar weniger auf dem deutschen Markt präsent, aber nicht weniger erfolgreich sind als die hiesigen dominanten Unternehmen.

Nicht überraschend ist, dass diese Phalanx an Schwergewichten den Blick auf die anderen Branchenmitglieder versperrt. Dabei haben einige andere Dienste ihren Platz in der Branche gefunden und betreiben **nachhaltige Geschäftsmodelle**. Im Vergleich zu den großen Akteuren der Branche mögen diese „klein“ erscheinen, allein betrachtet werden jedoch durchaus bemerkenswerte, stabile Umsätze mit Fortführungsabsicht des Geschäftsbetriebs erzielt. Dies sind z. B. nationale oder auf deutschsprachige Regionen konzentrierte Dienste, Dienste, die mit besonderer Datenschutzqualität werben oder auf bestimmte Funktionen setzen (z. B. Webinare) sowie viele entgeltliche Open Source-Dienste bzw. Clients, die auf Open Source-Diensten basieren sowie unentgeltliche und freie Anwendungen, die sich aber z. B. im Bildungsbereich oder unter fachkundigen Nutzerinnen und Nutzern großer Beliebtheit erfreuen.

Im Ergebnis handelt es sich beim „Messaging“ und „Videoconferencing“ um ein weltweites Geschäft und eine Branche, die nicht nur auf Seiten der größeren Teilnehmenden **technologische und digitale Entwicklungen und Innovationen** hervorbringt. Konkurrierende Dienste zeichnen sich durch innovative Geschäftsmodelle und Spezialisierungen auf Basis besonderer Services und Funktionen aus und nicht

[289] Google Chat wurde nicht in die Untersuchung einbezogen, da der Dienst nach Auskunft von *Google* zu Beginn der Sektoruntersuchung gerade erst den Betrieb aufnahm.

nur auf Seiten der freien Systeme und Anwendungen gibt es **viel Expertise und Engagement in Sachen Unabhängigkeit und Schutz der persönlichen Daten der Nutzerinnen und Nutzer**. Allerdings legt die Marktverfassung den Schluss nahe, dass dieses Potential bisher nicht ausgeschöpft, nicht flächendeckend verteilt und nicht so zugunsten eines hohen Datenschutzniveaus eingesetzt wird, wie es genutzt werden könnte.

In den Ermittlungen ist von verschiedenen Seiten die Auffassung geäußert worden, dass es zu besseren Ergebnissen auch im Datenschutz gekommen wäre, wenn von Beginn an auf **internationale und offene Standards** gesetzt worden wäre. Das war aber nicht der Fall. Die Entwicklung ist anders verlaufen und mit dieser Realität muss nun umgegangen werden. Einzelne Branchenvertreter haben die Gelegenheit genutzt, ein geschlossenes Geschäftsmodell zu entwickeln, das aufgrund der neuartigen Kommunikationsmöglichkeiten und der Unentgeltlichkeit für die Verbraucherinnen und Verbraucher einerseits besonders attraktiv ist, andererseits hinsichtlich des Datenschutzes unerwünschte Ergebnisse hervorbringen kann.

Realität ist aber auch - die Sektoruntersuchung hat es offen gelegt - dass sich daneben viele andere Geschäftsmodelle entwickelt haben, die offenbar trotzdem gut funktionieren. Auch diese Geschäftsmodelle sind ein **Spiegel der Verbraucherwünsche**. Das Rad kann also nicht einfach zurückgedreht werden, um unerwünschte Auswirkungen zu beseitigen. Bei jeglichen Maßnahmen von gesetzgeberischer oder behördlicher Seite, die die Auflösung der Machtpositionen zum Ziel haben und im Namen der Verbraucherinnen und Verbraucher zugunsten des Schutzes ihrer persönlichen Daten durchgeführt werden sollen, ist zu prüfen, ob andere Geschäftsmodell Gefahr laufen, dabei beeinträchtigt zu werden.

Wenn Interoperabilität als eine solche Maßnahme eingeführt wird, sind eben nicht nur die notwendigen Investitionen in technische Veränderungen der Dienste oder die Entwicklung technischer Neuerungen für die Umsetzung zu berücksichtigen. Ebenso einzubeziehen sind mögliche positive oder negative Wohlfahrtseffekte durch **veränderte Innovationsanreize und Auswirkungen auf Geschäftsstrategien und Wettbewerbsintensität gerade auch der Marktteilnehmenden, die zu den führenden Diensten in Konkurrenz treten**. Die Analyse der Wirkungszusammenhänge gerade rund um das Thema Interoperabilität ist somit vielschichtig und komplex. Mit der Einführung von § 19a des Gesetzes gegen Wettbewerbsbeschränkungen hat der deutsche Gesetzgeber einen wichtigen Schritt getan. Auf europäischer Ebene wurde der Weg fortgesetzt und mündet nun zunächst im Digital Markets Act, der auch für Messenger- und Video-Dienste Veränderungen bedeuten kann.

2. Die künftigen Referenzangebote gemäß DMA - ein Rahmen für das Stimmungsbild?

Das Bundeskartellamt hat im Sommer 2021 ein „Stimmungsbild“ zu Fragen der Interoperabilität ermittelt. Die im DMA enthaltene Verpflichtung von Gatekeepern zur Interoperabilität war damals in

dieser Form noch nicht bekannt. Die Antworten der Messenger- und Video-Dienste bezogen sich vielmehr auf ein Interoperabilitätskonzept, dass von Seiten des Bundeskartellamts nicht näher definiert worden war, um Vorfestlegungen und gesteuerte Meinungsäußerungen zu vermeiden. Das in Art. 7 DMA normierte Konzept einer Interoperabilitätsverpflichtung sieht unter drei Aspekten Grenzen vor. Zunächst sind – dem Gesamtkonzept des DMA folgend – lediglich designierte Gatekeeper unter den Messenger-Diensten Adressaten der Verpflichtung. Des Weiteren lebt die Verpflichtung erst auf, sobald sich ein anderer Dienst mit einem entsprechenden Petitum (freiwillig) an den Gatekeeper wendet. Schließlich sind lediglich die Basisfunktionen von der Verpflichtung umfasst.

Insgesamt hatte die Befragung gezeigt, dass Interoperabilität von den betroffenen Unternehmen nicht rundheraus abgelehnt wird. Des Weiteren hatten die Antworten zutage gebracht, 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 weiter Open Source-Bereich, der Interoperabilität quasi als Geschäftsmodell verfolgt. Bei einigen Video-Diensten wird zumindest eine Erreichbarkeit auch für dritte Nutzerinnen und 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 Nutzerinnen und Nutzer verschiedene Messenger-Dienste über eine Softwareoberfläche bedienen und Inhalte lesen können.

Knapp die Hälfte der befragten Unternehmen hatte sich **offen gegenüber freiwilligen Interoperabilitätsvorhaben** gezeigt, wobei sich allerdings - asymmetrisch hierzu - nur weniger als die Hälfte daran beteiligen würde. Bei diesen Zahlen war zu berücksichtigen, dass die Befragten ihre Einschätzung für oder gegen eine freiwillige Interoperabilität jeweils mit zahlreichen Anmerkungen, Voraussetzungen, Hinweisen und Einschränkungen versehen hatten, da das Interoperabilitätskonzept vom Bundeskartellamt nicht näher spezifiziert worden war. Dies war allerdings mit der klaren Haltung eines Großteils der Branche einhergegangen, dass eine **gesetzliche Verpflichtung zur Interoperabilität nicht wünschenswert** ist. Für den Fall einer erzwungenen Interoperabilität hatten die Unternehmen mit einer ablehnenden Haltung insbesondere negative Effekte auf die Innovationstätigkeit und damit auch auf das Datensicherheits- und Datenschutzniveau beim Messaging und beim Audio-/Video-Austausch befürchtet.

Die Regelungen im **DMA** greifen einige dieser Aspekte auf. Sie sehen in Art. 7 eine asymmetrische Interoperabilitätsverpflichtung vor. Der DMA fordert also mehr als eine freiwillige Vereinbarung, beschränkt die Verpflichtung aber auf designierte Messenger- und Video-Dienste von Unternehmen, die zuvor als Gatekeeper eingeordnet wurden und knüpft die Verpflichtung an einen entsprechenden Antrag. Die Umsetzung des vom Gatekeeper zu erstellenden Referenzangebots dürfte damit nur die

Messenger- und Video-Dienste betreffen, die als nummernunabhängige interpersonelle Kommunikationsdienste klassifiziert werden. In den Ermittlungen des Bundeskartellamts hatte ein Fünftel der Befragten Branchenteilnehmer benannt, die ihrer Vorstellung nach mit einer Verpflichtung belegt werden sollten. Dabei handelte es sich um nach Umsätzen oder Nutzerzahlen führende Dienste, was den Kriterien, die an die Definition eines Gatekeepers gestellt werden, zumindest grundsätzlich nahekommt.

Die Interoperabilitätsverpflichtung des DMA bezieht sich auf **Basisfunktionalitäten** einschließlich des Versands sämtlicher Dateien, zunächst auf Textnachrichten und Sprachanrufe, dann nach einem Ablauf von zwei Jahren auf Gruppenchats und schließlich nach insgesamt vier Jahren auf Videoanrufe. Gegenüber dem Bundeskartellamt hatten sich viele Messenger- und Video-Dienste ein Dreivierteljahr zuvor - vor der Einigung im Trilog im März 2022 - für ein schmales Interoperabilitätsmodell aus Textnachrichten ausgesprochen, das Raum für Innovation bei anderen Funktionen lässt und Umstellungsaufwand minimiert. Allerdings wurde von einigen Diensten ein Paket interoperabler Funktionen nur dann als sinnvoll erachtet, wenn der Austausch per Text, Audio, Video und von Inhalten umfasst ist. Auch hier sind somit grundlegende Übereinstimmungen erkennbar, wenn der DMA hier auch eine zeitliche Staffelung vorsieht. Videotelefonie ist erst vier Jahre nach Designierung des jeweiligen Dienstes interoperabel zu gestalten.

Die vom Bundeskartellamt befragten Messenger- und Video-Diensten hatten sich eine Umsetzung von Interoperabilität nur auf Basis **globaler technischer Standards** vorstellen können. Bisher werden in Standardisierungsgremien technische Grundlagen (für Interoperabilität) in globalem Kontext erarbeitet. Die Branche hatte geäußert, es wäre andernfalls sehr aufwendig, weltweit unterschiedliche Anforderungen erfüllen und verschiedene Sets interoperabler Funktionen anbieten zu müssen. Inwieweit dieser Aspekt in den vom DMA eröffneten Möglichkeiten der Kommission, in Durchführungsvorschriften bzw. delegierten Rechtsakten Einzelheiten zu regeln, Einfang finden wird, bleibt abzuwarten (Art. 46 Abs. 1, Art. 12 Abs. 4 DMA).

Art. 7 Abs. 3 DMA verlangt von Gatekeepern jedenfalls, das den eigenen Endkundinnen und Endkunden angebotene Sicherheitsniveau, ggf. einschließlich der Ende-zu-Ende-Verschlüsselung, bei allen interoperablen Diensten beizubehalten. Wie bereits dargelegt, setzen die Dienste zum großen Teil individualisierte Protokolle und Verschlüsselungstechniken ein. Dies betrifft auch die Ende-zu-Ende-Verschlüsselung. Sie unterliegt technischen Einschränkungen und kommt bei einigen Diensten - unabhängig davon - nur bei bestimmten Funktionen zum Einsatz. Einige große Dienste setzen sie noch nicht ein. Sie muss häufig von den Nutzenden oder Hosts aktiviert werden. Hier sind **Schwierigkeiten bei der Umsetzung und ggf. sinkende Sicherheitsstandards** zu erwarten, sofern es nicht gelingt, den **Stand der Technik** festzuschreiben.

Generell wird die Art der technischen Umsetzung der Interoperabilität noch nicht näher beschrieben. Vom Gatekeeper wird lediglich verlangt, die notwendigen technischen Schnittstellen oder vergleichbare Lösungen bereitzustellen. In der Befragung des Bundeskartellamts haben die meisten Dienste sich für eine Umsetzung von Interoperabilität über **Serverschnittstellen** ausgesprochen, wenn auch alternative Methoden im Ranking nur knapp dahinter lagen.[290]

Es bleibt abzuwarten, welche Regelungen hier noch getroffen werden (müssen). Dies wird auch davon abhängen, ob und inwieweit die jeweiligen Referenzangebote der betroffenen Gatekeeper von den Messenger- und Video-Diensten nachgefragt, also entsprechende Anträge auf die Herstellung von Interoperabilität gestellt werden.

3. Datenschutz unter Interoperabilität zwischen Theorie und realer Herausforderung

Hinsichtlich der konkreten Auswirkungen von Interoperabilität auf die Datensicherheit und damit auf das Datenschutzniveau war die in der Befragung des Bundeskartellamts geäußerte Bewertung der Messenger- und Video-Dienste mehrschichtig: Einerseits wurde die eingangs schon erwähnte Argumentation vorgetragen: Dienste versprechen sich neue Möglichkeiten, wenn Erreichbarkeit bzw. große Nutzerzahlen kein Differenzierungsmerkmal mehr darstellen. Dies könnte mit einer Belebung der Wettbewerbsintensität verbunden sein. Die Verbraucherinnen und Verbraucher könnten bei einer Erreichbarkeit der Dienste untereinander zu datenschutzfreundlicheren Anbietern wechseln, **Datenschutz somit als Wettbewerbsvorteil höhere Bedeutung** erlangen und sich das Datenschutzniveau insgesamt erhöhen.

Andererseits hatten die befragten Unternehmen auch indirekte (negative) Effekte auf Datensicherheit und Datenschutz prognostiziert. 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 insbesondere für kleinere Anbieter eine Hürde darstellen

---

290 Zu technischen Optionen der Umsetzung von Ende-zu-Ende-Verschlüsselung unter Interoperabilität siehe auch *Bundesnetzagentur*, "Interoperability between Messaging Services - Secure Implementation of Encryption", April 2023, abrufbar unter: https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Technologien/Onlinekomm/Study_InteropEncryption.pdf?__blob=publicationFile&v=1. Die Studie bezieht sieben Messenger- und Video-Dienste ein und beruht auf einer Untersuchung öffentlich erhältlicher technischer Dokumentationen und wissenschaftlicher Publikationen.

könnten. Die technische Integration dürfte **hohen Aufwand** verursachen, gerade wenn beteiligte Messenger-Systeme selbst eine Architektur aus verschiedenen Servern betreiben, auf denen jeweils verschiedene Funktionen und Services verortet sind.

Relativ einig waren 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 hielten dagegen, die Schwierigkeiten bei Datensicherheit und Datenschutz könnten auf technischer Ebene behoben werden, letztlich sei alles eine **Frage der Investitionsbereitschaft**. Überwiegend hatten die befragten Messenger- und Video-Dienste jedenfalls von einer erzwungenen Interoperabilität kein höheres Datenschutzniveau erwartet. Einzelne hatten vielmehr betont, 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.

Das Bundeskartellamt stimmt mit vielen Stimmen aus der Branche überein, dass Interoperabilität **neue Anforderungen an Datensicherheit und Datenschutz** stellen wird. Im Wesentlichen ist nicht nur fraglich, wie ein Identitätsmanagement aussehen könnte. Das BSI hat bereits angemerkt, dass Erweiterungen an der Netzwerkinfrastruktur der Messenger-Server – z. B. am Domain Name System (DNS) – vorgenommen werden müssten.[291] Die Messenger- und Video-Dienste verwenden unterschiedliche Identifier, allerdings wird die Telefonnummer - wie die Ermittlungsergebnisse gezeigt haben (siehe D.II.2) - durchaus weniger genutzt als zunächst vermutet. Sie führt aber zur nächsten Frage, nämlich dem Umgang mit Kontakten der Nutzerinnen und Nutzer, unter Interoperabilität ggf. auch derjenigen der Nutzerinnen und Nutzer anderer Messaging-Systeme.

Auch wie schnell die **Probleme mit der Ende-zu-Ende-Verschlüsselung** in Gruppen ggf. über den MLS-Standard oder mögliche andere Weiterentwicklungen der IETF-Arbeitsgruppe MIMI - gelöst werden können, ist noch offen. Dies wird davon abhängen, inwieweit die Dienste den Standard und Open Source-Implementierungen umsetzen können und wollen. Zum jetzigen Zeitpunkt liegen den Messaging-Systemen zum größten Teil individuelle Protokolle zugrunde. Auch wenn viele auf eine gemeinsame Basis – das Double Ratchet-Protokoll – zurückgehen, reichen die entsprechenden Individualisierungen aus, um eine interoperable Ende-zu-Ende-Verschlüsselung zu verhindern.

---

[291] *BSI*, Moderne Messenger – heute verschlüsselt, morgen interoperabel?, November 2021, S. 10, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.html.

Auch die sehr unterschiedliche Netzwerkarchitektur der Messenger- und Video-Dienste - wie sie sich in den Ermittlungen gezeigt hat - ist herausfordernd, insbesondere wenn Funktionen verschiedenen Servern zugeordnet werden oder generell **föderierte Systeme miteinander interoperabel** gestaltet werden sollen. Das Thema Föderation, also eine Server-übergreifende Kommunikation, rücke mit dem MLS-Standard in greifbarere Nähe – so das BSI - auch wenn sich die Ausarbeitung von Konzepten hier noch in den Anfängen befinde und es bislang nur wenige praktische, kryptographisch abgesicherte Lösungsansätze gebe. Im Zuge der Ermittlungen hat Element (Matrix) ebenfalls im Sommer 2022 darauf hingewiesen, dass der Standard in der aktuellen Form leider keine vollständige Interoperabilität unterstützen könne, da dezentrale und föderierte Netzwerke nicht vollumfänglich unterstützt werden. Das MLS Protokoll müsse dazu erweitert werden. Inzwischen hat die IETF verkündet, dass die Arbeiten zum MLS-Standard abgeschlossen wurden. Auch Matrix plane, ihn einzusetzen.[292]

Schließlich stellen sich zahlreiche Fragen aus dem Bereich der Datenverarbeitung. Kritisch ist z. B. der Aspekt der **(Meta-) Datenüberwachung und -verantwortung**, wenn persönliche Daten der Nutzerinnen und Nutzer unter Interoperabilität durch noch mehr Hände gehen. Auch dafür, dass einige Dienste Kontaktverzeichnisse hochladen und andere nicht, stehen Lösungsansätze für die betroffenen Nutzerinnen und Nutzer noch aus.

Wie in diesem Bericht festgehalten, ist die **rechtskonforme Datenspeicherung** für einige Dienste eine Herausforderung und Anforderung, der sie nachkommen müssen. Unter Interoperabilität erhöht sich die Wahrscheinlichkeit, dass unterschiedliche Jurisdiktionen betroffen sind.

Die **Einordnung und Bewertung dieser Schwierigkeiten gerade aus gesamtwirtschaftlicher Perspektive** und das mögliche Entstehen weiterer Herausforderungen richtet sich nach dem Entwicklungsszenario, das zugrunde gelegt wird. D. h. entweder können die realen Gegebenheiten in den Blick genommen werden, wo das branchenweite Interesse an Interoperabilität mäßig zu sein scheint. Oder es kann ein marktweites Interoperabilitätsregime vorausgesetzt werden, im Zuge dessen weitgehende Standardisierungen umgesetzt werden müssten. Diese Perspektive scheint derzeit aber eher theoretisch interessant, z. B. als Referenzszenario für die Kosten-Nutzen-Analyse der Maßnahmen, die zukünftig tatsächlich getroffen werden. Eine Einschätzung wird schließlich dadurch erschwert, dass die genaue technische Umsetzung von Interoperabilität durch die zu benennenden Gatekeeper im DMA noch offen

---

[292] Vgl. *IETF*, Messaging Layer Security: Secure and Usable End-to-End Encryption, abrufbar unter: https://www.ietf.org/blog/mls-secure-and-usable-end-to-end-encryption/ sowie *Golem*, IETF standardisiert Protokoll für sichere Gruppenchats, abrufbar unter: https://www.golem.de/news/messaging-layer-security-ietf-standardisiert-protokoll-fuer-sichere-gruppenchats-2303-173089.html.

ist, diese aber ein wesentlicher Bestimmungsfaktor von Datensicherheit, Datenschutz und den notwendigen Investitionen in dieselben sein wird.

Die **tatsächliche aktuelle Ausgangssituation** lässt nach Auffassung des Bundeskartellamts nicht erwarten, dass sich die Branche der Messenger- und Video-Dienste innerhalb kürzester Zeit interoperabel miteinander austauschen wird. Es wird letztendlich von den Wünschen der Nutzerinnen und Nutzer der jeweiligen Dienste abhängen, ob das jeweilige interoperable Referenzangebot nachgefragt wird oder nicht. Die Einstellung **der Verbraucherinnen und Verbraucher** in Sachen Interoperabilität hält das Bundeskartellamt weiterhin für eine **schwer einschätzbare Größe**: Ob eine spürbar große Anzahl an Verbraucherinnen und Verbrauchern bei Interoperabilität tatsächlich, wie verschiedentlich erhofft, vermehrt zu datenschutzfreundlichen Anbietern wechseln würden, ist ausweislich aktueller Befragungen der Bundesnetzagentur[293] und des Verbraucherzentrale Bundesverbands[294] zu Nutzerinteressen und Wechselbereitschaft allenfalls als offen und eher als fraglich zu bezeichnen. Eventuell gäbe es auch gar keine nennenswerten Reaktionen der Verbraucherinnen und Verbraucher auf eine Interoperabilität von Messenger- und Video-Diensten, da sie mit ihren aktuellen Multi - Homing - Lösungen zufrieden sind und dies noch intensiver betreiben.

Nach Rückmeldungen aus dem Markt könnte die **größte Hoffnung darin liegen, ein Wechseln ganzer Verbrauchergruppen**, wie sie z. B. in Sportvereinen zu finden sind, zu ermöglichen, so dass der einzelnen Nutzerin und dem einzelnen Nutzer mühsame Überzeugungsarbeit bei den Kontakten erspart bleibt. Im Zuge eines Gründungsvorhabens wurde gegenüber dem Bundeskartellamt deutlich gemacht, dass offenbar auf Vereinsebene in Deutschland durchaus Interesse besteht, sich als Verein datenschutzfreundlichen Messengern zuzuwenden und sogar ein eigenes Angebot zu entwickeln. Für den Erfolg eines solchen Vorhabens wurde der **Anschluss an das Messaging-System von WhatsApp** als wesentlicher Faktor bezeichnet. Die Gatekeeper sollten im Idealfall selbst eine komplette Interoperabilität zu anderen Messenger - Diensten gestalten, aber auf jeden Fall zumindest ihre APIs frei zugänglich gestalten, so dass kleinere Anbieter interoperable Lösungen erarbeiten können. In den Ermittlungen des Bundeskartellamts haben auch viele freie Messenger-Clients und Open Source-Dienste auf die Wechselmöglichkeiten der Verbraucherinnen und Verbraucher hingewiesen, wenn Zugang zu den führenden Diensten bestünde. Es wurde mit steigenden Nutzerzahlen gerechnet. Im Zuge der

---

[293] *Bundesnetzagentur*, Nutzung von OTT-Kommunikationsdiensten in Deutschland, Mai 2020, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/OTT.pdf?__blob=publicationFile.

[294] *VZBV*, Interoperabilität bei Messengerdiensten, Mai 2021, abrufbar unter: https://www.vzbv.de/pressemitteilungen/messenger-dienste-regulierung-mit-augenmass.

getroffenen Zugangsverpflichtung im DMA würde nun zumindest die Chance bestehen, diese These zu „beleben“, also Neueinsteigern oder Wettbewerbern den Einstieg und Verbraucherinnen und Verbrauchern den Wechsel zu ermöglichen.

Sofern es nur vereinzelt zu Anträgen auf **bilaterale Interoperabilitätsvereinbarungen käme,** scheinen die Probleme lösbar und die notwendigen Investitionen tragbar zu sein. Es sind Lösungen über Schnittstellen geplant, die bereits in dieser grundlegenden Form im Markt von einigen Messenger- und Video-Diensten praktiziert werden. Die im DMA vorgesehene Beschränkung auf die Basisfunktionalitäten ist eine Konstruktion, durch die **Differenzierungsmöglichkeiten** - zumindest theoretisch - für die Dienste grundsätzlich erhalten werden können. Auf Seiten der Dienste wird dann jeweils individuell konkret geschaut werden müssen, ob und inwieweit die technische Konzeption der Dienste, die - wie in Kapitel D.I.1 beschrieben - sehr unterschiedlich ist, eine entsprechende Trennung in interoperable und andere Funktionen gewährleisten kann.

Für die Verbraucherinnen und Verbraucher stellt die DMA-Interoperabilitätspflicht neben dem Multi - Homing einerseits eine weitere Möglichkeit dar, um Nutzerinnen und Nutzer anderer Messenger-Dienste zu erreichen. Mit Hilfe der DMA-Regelung könnten sie grundsätzlich bei der Gruppenkommunikation weniger auf hier führende Dienste angewiesen sein, die bisher von Netzwerkeffekten profitieren. Inwieweit es andererseits - wie von bei Verbrauchern beliebten Diensten vorgetragen - zu **Einschränkungen des Nutzererlebnisses und sinkender Attraktivität des Produktes** kommt - lässt sich zu diesem Zeitpunkt nicht abschätzen und hängt von vielen Faktoren ab. Zunächst einmal davon, ob – wie oben beschrieben, die Verbraucherinnen und Verbraucher Interoperabilität wünschen und ihre Dienste dementsprechend „beauftragen“, ein Referenzangebot nachzufragen bzw. die Dienste sich neue Geschäftsmöglichkeiten versprechen. Ferner dürfte sich der Sektor weiterentwickeln. Zum einen betrifft dies die Umsetzung neuer Features für die Nutzerinnen und Nutzer. Wenn sich neue Funktionen schnell durchsetzen, könnte das interoperable Produkt tatsächlich an Attraktivität einbüßen. Dies wiederum hängt von der Wertschätzung und den Vorlieben der Verbraucherinnen und Verbraucher ab. Ob sie es wichtiger finden, mit Nutzerinnen und Nutzern anderer Dienste zu kommunizieren und sich bei ihren Nachrichten auf interoperable Features beschränken Würden oder ob sie lieber Multi - Homing betreiben und zu jedem Zeitpunkt die volle Vielfalt der Messaging-Funktionen nutzen, kann derzeit nicht eindeutig beantwortet werden. Gemäß dem im DMA veranlagten **Zeitplan für die Umsetzung des Referenzangebots** wird die Interoperabilität von Videotelefonie erst in vier Jahren verlangt, was in einem dynamischen Markt als ein recht langer Zeitraum erscheint. Zwar blieb dieser Punkt nicht unberücksichtigt insofern, als dass von gesetzgeberischer Seite entsprechende Veränderungen am Referenzangebot und den implementierten Fristen vorgenommen werden können. Doch erschwert ein solch **langer Umsetzungs- und damit auch Prognosezeitraum** seriöse Aussagen über die Eignung der Maßnahme. Zum anderen schafft die

technologische Entwicklung neue Möglichkeiten und ggf. Lösungen, wie es z. B. der MLS-Standard bei der Ende-zu-Ende-Verschlüsselung von Gruppenkommunikation oder die neu gegründete Arbeitsgruppe MIMI der IETF erwarten lässt, was auch jeglichen Interoperabilitätsbestrebungen zuträglich ist.
Falls Gatekeeper – anders als erwartet – eine Vielzahl von Einzellösungen umsetzen müssten, rückten die oben genannten Schwierigkeiten für den Datenschutz und die gesamtwirtschaftliche Kosten-Nutzen-Rechnung vermehrt ins Rampenlicht. Hier dürfte eine Vielzahl von Einzellösungen unter Kostenaspekten gesamtwirtschaftlich nachteilig sein und ein **branchenweit standardisiertes Regime** notwendig werden.[295] Aufgrund der Vielfalt der Branche, den vielen unterschiedlichen Geschäftsmodellen, die nicht auf personalisierter Werbung fußen und der unterschiedlichen technischen Ausgangssituation sowie den komplexen Verbraucherwünschen dürfte dann eine weitere Diskussion mit der Branche zu erwarten sein. Aufgrund der Ermittlungsergebnisse zur Sektoruntersuchung ist nach Ansicht des Bundeskartellamts für jeglichen regulatorischen Dialog bei entsprechenden Spielräumen eine **innovations- und investitionsschützende Auslegung**, die der technologischen Entwicklung Raum lässt, anzuregen.

---

[295] Ähnliche Überlegungen stellen auch die Autoren der BNetzA-Studie „Interoperability between Messaging Services – Secure Implementation of Encryption“, April 2023 an, die unterschiedliche Optionen für eine mögliche Umsetzung von Ende-zu-Ende-Verschlüsselung unter Interoperabilität untersuchen, abrufbar unter: https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Technologien/Onlinekomm/Study_InteropEncryption.pdf?__blob=publicationFile&v=1.

G. Ansätze für mehr wettbewerblichen Datenschutz

In den vorausgegangenen Kapiteln hat sich das Bundeskartellamt intensiv mit den konkreten Sicherheitseigenschaften und Praktiken der Datenverarbeitung bei Messenger- und Video-Diensten, verbraucherrechtlichen Verstößen der Dienste sowie der praktischen Relevanz rechtlicher Maßnahmen des Gesetzgebers - Datenportabilität und aktuell Interoperabilität - für den Messaging-Alltag der Verbraucherinnen und Verbraucher auseinandergesetzt.
Im Ergebnis entsteht der Eindruck, dass die Datenschutzqualität insb. auf Seiten der Verbraucherinnen und Verbraucher als Nachfragenden und auch bei einigen Diensten nicht die notwendige Beachtung innerhalb wettbewerblicher Auswahlprozesse findet, als dass sich das Datenschutzniveau marktgetrieben unter den gegebenen Rahmenbedingungen verbessern würde.
Dieses Kapitel ist nun darauf gerichtet, wie das Datenschutzniveau in Deutschland zeitnah verbessert werden könnte. Das Bundeskartellamt hatte die Messenger- und Videodienste in seinem Fragebogen um eine Meinungsäußerung dazu gebeten (dazu unter I.). Vor dem Hintergrund dieser Ermittlungsergebnisse hat das Bundeskartellamt einige Aspekte aufgegriffen, die dem Datenschutz in wettbewerblichen Prozessen ein stärkeres Gewicht verleihen können (dazu unter II.). Abschließend wird mit dem Rating ein Instrument vorgestellt und diskutiert, das geeignet scheint, sowohl die anbietenden Dienste als auch die nachfragenden Verbraucherinnen und Verbraucher zu motivieren, Datenschutz als Wettbewerbsparameter zu begreifen (dazu unter III.).

I. Ermittlungsergebnisse

Das Bundeskartellamt hat die Messenger- und Video-Dienste vor die Auswahl gestellt, mit welchen Maßnahmen das Datenschutzniveau in Deutschland verbessert werden kann. Die breiteste Zustimmung seitens der Dienste fanden die vom Bundeskartellamt vorgegebenen Kategorien „öffentliche Förderung Open Source-Projekte“ (45 %), der „Einsatz datenschutzfreundlicher Dienste im öffentlichen Bereich“ (41%) die „Aufklärung der Verbraucherinnen und Verbraucher“ (45%) sowie die „bessere Durchsetzung des Datenschutzrechts“ (43%). Viele Dienste haben diese Maßnahmen engagiert kommentiert. Die Maßnahmen „Standardisierung“, „Datenschutzaudits für Anbieter“ und „Maßnahmen der Wettbewerbsaufsicht“ fanden im Verhältnis dazu weniger Zustimmung.
Einige **führende Anbieter** äußerten, weitere **Maßnahmen zugunsten des Datenschutzes** wären nicht notwendig. Es bestehe bereits ein hohes Datenschutzniveau bei Messenger – und Video-Diensten in Deutschland, insb. wenn man sich mit den Business-Anwendungen beschäftige. Ein bei Verbraucherinnen und Verbrauchern populärer Dienst betont, man würde seinen deutschen Nutzerinnen und Nutzern bereits ein ausreichendes Niveau an Datenschutzmaßnahmen liefern. Die eigene Vision sei, die Welt privat zu verbinden. Man habe sich dem Datenschutz und der Datensicherheit verpflichtet, wie man es in den Antworten zu diesem Fragebogen ausgeführt habe. Man

strebe an, offen und transparent zu sein in Bezug auf die persönlichen Daten, die gesammelt würden, um den Dienst den deutschen Nutzerinnen und Nutzern zur Verfügung stellen zu können und diesen sicher zu gestalten. Informationen dazu wären auf der Webseite erhältlich. Andere große Dienste verweisen auf fehlende Marktkenntnis für Deutschland oder fehlenden Anlass, sich damit zu beschäftigen.

1. Förderung von Open Source und Standardisierung

In allen Anbietergruppen findet die öffentliche Förderung von Open Source-Projekten breite Zustimmung. Das bezieht sich zum einen auf die Förderung durch öffentliche Gelder, aber auch durch den Einsatz von Open Source-Diensten im öffentlichen Bereich.
Verschiedene freie Dienste haben nähere Ausführungen dazu gemacht: Solange der Markt von Firmen dominiert werde, die mit den Daten ihrer Nutzerinnen und Nutzer Geld verdienen, werde das **Datenschutzniveau** darunter leiden. Open-Source-Projekte mit öffentlicher Förderung könnten diesen Status Quo herausfordern und Nutzerinnen und Nutzern alternative Angebote machen. Je stärker Open Source gefördert werde, umso höher steige der Druck auf etablierte amerikanisch geprägte Anbieter.
Ein anderer Dienst weist darauf hin, dass wenn man nicht alles selbst entwickeln könne, **die finanzielle Bündelung der Kräfte und Investition** in Open Source-Projekte eine Möglichkeit sei, um gegenüber entwicklungsstärkeren Wettbewerbern wettbewerbsfähig zu bleiben.
Viele Probleme mit Messengern und Kommunikation generell gingen auch auf **kommerzielle Interessen** und die daraus resultierenden verschiedene Zwänge zurück, so dass Nutzerinnen und Nutzer die entsprechenden Systeme nicht ohne weiteres verlassen können. Die Wahl des Anbieters sei nicht mehr völlig frei und ein Anbieterwechsel mit erhöhtem Aufwand für die Nutzerin und den Nutzer verbunden. Freie Messenger-Systeme hätten in der Regel ein höheres Datenschutzniveau, da sie nicht von wirtschaftlichen Interessen beeinflusst würden. Nutzerinnen und Nutzer, die sich um Datensicherheit und Datenschutz kümmerten, hätten unter den freien Messenger-Clients mehr Wahlmöglichkeiten.
Mehrere Wettbewerber der großen Messenger- und Video-Dienste halten fest, die Förderung von Open Source beziehe sich nicht nur auf datenschutzfreundliche entgeltfreie Angebote. Sie sollte – so verschiedene Dienste - auch die **Förderung von Produkten innovativer Wettbewerber** der etablierten Dienste umfassen. Open Source sei nicht gleichbedeutend mit „kostenlos“. Open Source - Software sei die einzige Möglichkeit, **Vertrauen in Funktionalität und Sicherheit** einer Software zu generieren und eine schnelle Marktdurchdringung und mehr Flexibilität zu erreichen. So wären bereits Geschäftsmodelle entstanden, die nicht auf Verstößen gegen Datenschutzrecht gegenüber den Verbrauchern aufbauten.
Ein anderer Wettbewerber etablierter Dienste führt weiter aus, Open Source-Projekte emanzipierten die Kundinnen und Kunden: Sie könnten in die Software hineinblicken und damit objektiv überprüfen,

ob Versprechungen auch tatsächlich eingebaut wären. Sollte die Software einmal nicht mehr weiterentwickelt werden, könnten die Kundinnen und Kunden andere damit beauftragen, was deren Investitionen in die ursprüngliche Lösung sichere. Auch ließen sich Spezialfeatures realisieren, an die man selbst möglicherweise nicht gedacht habe. Und zu guter Letzt sehe man einen **Sicherheitsgewinn** für alle, wenn unabhängige Experten den Code sichten und auf Probleme aufmerksam machen können. Öffentlich gefördert werden sollten vor allem solche Systeme, die „nachhaltig" sind. Eine Förderung von Projekten, die bereits existierende **(internationale) Standards** einhalten sowie die Förderung von damit verbundenen Open Source - Projekten (oder die Beauftragung von Closed Source - Projekten, die öffentliche Schnittstellen unterstützen) trage maßgeblich zu einer solchen „Nachhaltigkeit" bei. Selbst wenn die beteiligten Firmen/Entwickler nicht mehr an einem Projekt weiterarbeiteten, sei der Quellcode immer noch frei verfügbar und andere Entwickler könnten den Code übernehmen und weiterentwickeln (beispielsweise sogar gefördert mit öffentlichen Geldern). Das bedeute, dass alle Veränderungen (egal ob öffentlich oder privat finanziert) immer der Allgemeinheit zu Gute kämen und keine öffentlichen Gelder in private Firmen oder Projekte fließen würden, dort versanden und kein für die Allgemeinheit „öffentliches nachhaltiges Gut" daraus entstehen würde. Verschwinde so eine Firma von der Bildfläche, sei das investierte Geld, anders als bei Open Source-Software, quasi unwiederbringlich verloren. Öffentliche Standards und die Förderung der Entwicklung von Open Source - Projekten sei essentiell für eine freie, nachhaltige und unabhängige Gesellschaft.
Auch US-amerikanische Dienste stimmen zu. Die Förderung von Open Source-Projekten zusammen mit Standardisierung sei die beste und effektivste Möglichkeit, um **Innovation voranzubringen**.
Generell hält ein Drittel der Befragten **Standardisierung** für geeignet, ein besseres Datenschutzniveau zu erreichen. Sie ermögliche Interoperabilität. Offene Standards könnten von einer Vielzahl von Personen eingesehen und kommentiert werden. Probleme mit Datenschutz und Datensicherheit könnten so schnell gefunden werden. Zudem würden wirtschaftliche Interessen der Dienstanbieter in der Regel weniger gewichtet, da auch Personen ohne wirtschaftliche Interessen am Standardisierungsprozess teilnehmen könnten. Standardisierung würde mehr Konkurrenz erschaffen, was grundsätzlich positiv sei. Es würde auch bedeuten, dass Daten nicht mehr nur in den Händen der drei größten Anbieter liegen. Die Produktentwicklung würde leichter und weniger risikoreich und am Ende weniger kostspielig.

2. Einsatz datenschutzfreundlicher Dienste im öffentlichen Bereich

Viele Messenger- und Video-Dienste verweisen auf eine mögliche **Vorbildfunktion der öffentlichen Hand.** Die Nutzung nicht DSGVO-konformer Messenger sei sowohl bei Ämtern als auch bei Unternehmen immer noch weit verbreitet. Wenn nicht-datenschutzfreundliche Dienste in öffentlichen

Bereichen genutzt würden, verschaffe das diesen Diensten aus Sicht der Nutzerinnen und Nutzer erhöhte Legitimität.

Nutzerinnen und Nutzer sollten einen selbstbestimmten Weg für ihre Behördenkommunikation wählen können, ohne ihre Daten an Dritte weiterzugeben. Hier wäre es beispielsweise auch möglich, dass Behörden z. B. eigene XMPP-Server betreiben und damit volle Datensouveränität wahren bzw. bekommen würden. Viele Universitäten, beispielsweise auch die HU Berlin würden schon derartige Systeme betreiben.[296] Öffentliche Institutionen sollten einen „**Open Source first" - Ansatz in ihren Ausschreibungen** verfolgen, um so auch Rechenschaft über die Verwendung öffentlichen Gelder ablegen zu können.)

Weiter wird ausgeführt, Open Source solle für die öffentliche Hand verpflichtend werden. Damit sei nicht gemeint, dass kostenlose Projekte neu ins Leben gerufen werden sollten, sondern dass Steuergelder in **Lösungen innovativer deutscher Unternehmen investiert** werden sollten. Am besten solle die **Regierung funktionierende Lösungen kaufen und selbst einsetzen**. Dies führe dazu, dass wettbewerbsfähige Produkte erschaffen und verbessert würden. Gegenüber staatlichen Förderungen im Allgemeinen sei man skeptisch, wenn aber Regierungen Produkte kaufen, um Technologien zu fördern und zu stimulieren, sei das zielführender als einfach nur Geld an diejenigen zu verteilen, die das beste Angebot schreiben könnten.

Ein anderer Wettbewerber der etablierten Dienste erläutert, Förderungen könnten für sich entwickelnde Unternehmen in Deutschland meistens eher Bürde als Hilfe sein - erst recht, wenn das betroffene Unternehmen Fachleute für seine Projekte und keine Experten für Förderungen und Lobbyarbeit in seinen Reihen hätte. Die Schwierigkeiten begännen beim Finden einer geeigneten Förderung, gingen über in großen bürokratischen Aufwand bei der Beantragung und reichten bis hin zu stark **einschränkenden Förderbedingungen**. Ähnlich sei es auch bei Ausschreibungen. Beispielsweise hätte man gerne an einer Ausschreibung eines Landesministeriums für einen Schulmessenger teilgenommen. Das sei an „künstlichen Limits" gescheitert. Die **Rahmenbedingungen der Ausschreibungen** – z. B. Anforderungen an den Mindestumsatz – hätten auch von etablierten Unternehmen nicht erfüllt werden können.

Sinnvoller wäre es, staatliche oder kommunale Stellen zu fördern, wenn diese dafür Open-Source-Produkte innovativer deutscher Unternehmen einsetzen. **Unternehmen wäre mit realisiertem Umsatz immer besser geholfen, als mit Fördergeldern**. Eigene Talente müssten sichtbar gemacht und die heimische IT-Branche gefördert werden. Digitale Technologien wären systemrelevant. Man dürfe sich nicht von Konzernen abhängig machen, auf die vielfältige ungewisse Einflüsse einwirken könnten. Die

---

[296] Siehe *HU Berlin*, abrufbar unter: https://www.cms.hu-berlin.de/de/dl/kommunikation/chat.

Open Source-Welt biete heute für alle Anwendungsfälle Lösungen, die nicht minder gut sind als die Massenware weniger Monopolisten. Und dort, wo es noch Bedarf gäbe, werde jeder deutsche Entwickler, jede deutsche IT-Firma mit Freude unterstützen, wenn der Kunde rufe.
Schließlich wurde im Rahmen der Ermittlungen auf den **Bildungssektor** verwiesen. Lehrkräfte und Eltern oder in höheren Klassen auch Lehrkräfte und Schülerinnen und Schüler kommunizierten in Gruppen häufig noch über beliebte weit verbreitete Messenger-Dienste. Auch für das Home Schooling werde vielfach ein führender Video-Dienst genutzt. Hinzu komme, dass große Digital- und IT-Konzerne in diesem Bereich massiv investieren, um Lehrkräfte und somit Schülerinnen und Schüler frühzeitig an die eigene Software - und dazu gehören natürlich auch Messaging-Apps - zu binden.[297]

3. Aufklärung der Verbraucherinnen und Verbraucher

Die Aufklärung der Verbraucherinnen und Verbraucher ist für alle Dienste-Gruppen ein wichtiger Aspekt einer zukünftigen Datenschutzstrategie. Diese Ansicht ist branchenweit vertreten.
Die Verbraucherinnen und Verbraucher müssten weiterhin für das Thema Datenschutz sensibilisiert werden. Es sei Teil der Entwicklung von **Medienkompetenz**. Derzeit bleibe die Aufgabe, Nutzer über die Gefahren unverschlüsselter Kommunikation zu informieren, quasi ausschließlich bei der **Zivilgesellschaft** hängen, während von staatlicher Seite immer wieder Wünsche nach dem Aufbrechen von Ende-zu-Ende - Verschlüsselung laut würden. Wissen über Datenschutz und vertrauenswürdige IT-Systeme als Teil der Medienkompetenz fehle sogar bei vielen Lehrkräften.
Den Verbraucherinnen und Verbrauchern die Bedeutung von Datenschutz zu vermitteln, würde nach Meinung zweier größerer Dienste dazu führen, dass diese den Datenschutz mehr wertschätzen und die entsprechenden Angebote auswählen, was wiederum ein Anreiz für die Wettbewerber wäre, datenschutzfreundlichere Produkte anzubieten.
Ein Dienst wendet ein, die Aufklärung der Verbraucherinnen und Verbraucher erfolge bereits in ausreichendem Umfang, habe aber durch **zentralisierte Marktmacht einzelner Unternehmen** nur beschränkte Auswirkungen. Ein anderer Dienst argumentiert ähnlich. Die Nutzerinnen und Nutzer sollten auch wirklich eine Wahl haben und selbst und frei diese Entscheidung treffen können, das könnten sie aktuell nicht. Ein Beispiel sei der Fragebogen des Bundeskartellamts, der ein Microsoft Word Dokument sei.
Ein Open Source - Dienst schlägt ein **Datenschutz-Rating** vor. Die meisten Verbraucherinnen und Verbraucher würden Datenschutzthemen nicht richtig nachvollziehen können und würden meistens

---

[297] Als Stichworte werden kostenlose Weiterbildungsprogramme der Digitalkonzerne für Lehrkräfte, die die konzerneigenen Produkte für das Lehren und Lernen einsetzen. Die Lehrerinnen und Lehrer erfüllten quasi die Funktion von Markenbotschaftern.

auch die Datenschutzerklärungen nicht lesen. Ein Rating würde zu wettbewerblicher Resonanz im Markt führen, da kein Messenger- oder Video-Dienst wegen eines im Vergleich zu seinen Wettbewerbern schlechteren Ratings Nutzerinnen und Nutzer verlieren wolle.

4. Weitere Ermittlungsergebnisse

Einige Messenger- und Video-Dienste kommentierten auch eine „bessere Durchsetzung des Datenschutzrechts", „Maßnahmen der Wettbewerbsaufsicht" und „Datenschutzaudits für Anbieter".
Zur Frage der **Durchsetzung des Datenschutzrechts** äußerte ein Dienst, Corona habe gezeigt, wie zahnlos der Tiger Datenschutz tatsächlich ist. Dass Zoom in so vielen Unternehmen eingesetzt werde, spreche nicht für die Durchsetzung des Datenschutzes. Ein anderer Dienst äußert, auch bei Abschluss von „AVV[298] und Co" mit dem Unternehmen würden die Daten durch den Einsatz des Cloud Acts[299] ggf. amerikanischen Behörden offengelegt. Ein Videodienst meint, die effektive Durchsetzung von Regelungen, wie z.B. des Cloud Act, werde großen Unternehmen schaden. Allerdings wären die Gesetze auch für kleinere Unternehmen schwierig umzusetzen, was nicht unterschätzt werden sollte. Auf eine gute Ausführung komme es an.
Datenschutzverstöße verschiedener Dienstanbieter (insbesondere aus den USA) würden weithin vermutet, durch Datenschutzbehörden, u.a. wegen Zuständigkeit der überforderten irischen Behörden aber **unzulänglich verfolgt**. Amerikanische „Chat-System-Anbieter" würden nicht hinreichend kontrolliert.
Ein Open Source - Dienst äußert, Deutschland hätte bereits ein starkes Datenschutzrecht. Sofern es in Sachen Datenschutz zu einem Vorfall bei einem Messenger- oder Video-Dienst komme, hätten die Datenschützer wahrscheinlich schon die Instrumente, um das Problem zu lösen. Ein weiterer Anbieter äußert sich ähnlich. Die **DSGVO** sei - was ein auf Prinzipien basierendes effizientes und verhältnismäßiges Datenschutzrecht angehe - eine „high water mark" und führend in der Welt.
Ein US-amerikanischer Dienst erklärt, die Durchsetzung der DSGVO durch die Datenschutzbehörden der Mitgliedsstaaten sei lückenhaft und hätte zu verzerrten Ergebnissen im internen Markt geführt. Es sei

---

[298] Einen Auftragsverarbeitungs-Vertrag (AV-Vertrag) muss nach DSGVO jedes Unternehmen abschließen, das personenbezogene Daten im Auftrag – also von einem Dienstleister verarbeiten lässt.

[299] Der Cloud Act (Clarifying Lawful Overseas Use of Data Act) ist ein seit 2018 bestehendes US-amerikanisches Gesetz zum Zugriff der US-Behörden auf gespeicherte Daten im Internet. Das Gesetz verpflichtet amerikanische Internet-Firmen und IT-Dienstleister, US-Behörden auch dann Zugriff auf gespeicherte Daten zu gewährleisten, wenn die Speicherung nicht in den USA erfolgt, siehe *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/CLOUD_Act.

klar, dass einige der größten Anbieter sich in der EU nach einem laxeren „main establishment regime“ umgeschaut hätten. Die Aufgabe des Europäischen Datenschutzausschusses[300] sei es, für angemessene Durchsetzungsstandards im internen Markt zu sorgen. Beispielsweise könne es für eine Verbesserung der Durchsetzungsstandards innerhalb der EU hilfreich sein, den Europäischen Datenschutzausschuss in eine echte Durchsetzungsbehörde umzustrukturieren. Der Europäische Datenschutzausschuss und die Datenschutzbehörden der Mitgliedsstaaten sollten auch Wege suchen, sicherzustellen, dass Privacy by Design - Prinzipien als „good practice“ in der Branche umgesetzt würden. Dies könne über verbindliche Richtlinien - basierend auf den Kernprinzipien der DSGVO - umgesetzt werden und missbräuchliche / dominante Unternehmen daran hindern, manipulative Design-Praktiken einzusetzen, um unlauter Zugang zu den Daten der Nutzerinnen und Nutzer zu erhalten. Als Beispiele werden der Britische ICO „„age appropriate design code (children‘s code)“[301] und der der „Australian eSafety Commissioner's

---

[300] Der Europäische Datenschutzausschuss (EDSA) ist eine unabhängige europäische Einrichtung, die zur einheitlichen Anwendung der Datenschutzvorschriften in der gesamten Europäischen Union beitragen und die Zusammenarbeit zwischen den EU-Datenschutzbehörden fördern soll. Der EDSA besteht aus Vertretern der nationalen Datenschutzbehörden und dem Europäischen Datenschutzbeauftragten (EDSB). EDSA kann allgemeine Leitlinien herausgeben, um Klarheit hinsichtlich der Begriffe in den europäischen Datenschutzgesetzen im Sinne einer einheitlichen Auslegung - insbesondere für verschiedenste Stakeholder - zu schaffen. Zur Sicherstellung der einheitlichen Anwendung ist er auch befugt, für nationale Datenschutzbehörden verbindliche Beschlüsse zu erlassen, vgl. *EDPB*, https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_de.

[301] Der „Kinderkodex“ (oder der Kodex für altersgerechtes Design) wurde vom Datenschutzbeauftragten des Vereinigten Königreichs (Information Commissioner's Office (ICO) erlassen und trat im September 2021 in Kraft. Er enthält 15 Standards, denen Online-Dienste folgen müssen. Dadurch wird sichergestellt, dass sie ihren datenschutzrechtlichen Verpflichtungen zum Schutz der Daten von Kindern im Internet nachkommen. Der Kodex gilt für „Dienste der Informationsgesellschaft, auf die Kinder zugreifen können, also die meisten gewinnorientierten Online-Dienste, wie z. B. Anwendungen, Suchmaschinen, Social-Media-Plattformen, Messenger-Dienste oder internetbasierte Sprachtelefondienste; Der Kodex gilt für Unternehmen mit Sitz im Vereinigten Königreich und Unternehmen außerhalb des Vereinigten Königreichs, die personenbezogene Daten von Kindern im Vereinigten Königreich verarbeiten, siehe z. B. *ICO*, https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/.

Office safety-by-design code“[302] genannt. Beides wären verpflichtende, rechtlich bindende Design Codes, die auf geltenden Gesetzen und Regulierungen basierten.

Ein Befragter äußert sich zu Geldstrafen. Wenn **Geldstrafen** auferlegt würden, müssten diese dergestalt ausfallen, dass sie auch bei Wiederholungstätern eine Veränderung auslösten. Wenn Verbraucherinnen und Verbrauchern wirklich durch Datenschutzverstöße geschadet würde, könnten Geldstrafen ein kleinerer Teil eines größeren Instrumentariums werden. Es solle auch zwischen zu vernachlässigenden Verstößen (nachlässiges Unternehmen, das nicht darauf geachtet hat) und landesweiten ausgefeilten Verstößen unterschieden werden, wenn Strafen verhängt würden.

Gut ein Viertel der befragten Dienste thematisiert **Maßnahmen der Wettbewerbsaufsicht**. Alle hier kommentierenden Dienste wenden sich gegen die starke Marktposition einzelner Dienste und ihr Verhalten. Diese hätten die globale Verfügbarkeit des Internet genutzt, um Monopolstrukturen aufzubauen und sich über nationale Rechtsprechung hinwegzusetzen. Dominante Unternehmen sollten nicht aufgrund von „Underperformance“ beim Datenschutz Wettbewerbsvorteile erringen können. Im zentralisierten Markt für Messenger-Dienste diktieren die großen Player ihren Nutzerinnen und Nutzern datenschutzfeindliche Nutzungsbedingungen und hinderten sie, zu wechseln. Dies komme missbräuchlichem Verhalten von Marktmacht nahe und die Behörden sollten Maßnahmen ergreifen, die Öffnung der Märkte zu erzwingen. Marktstarke Unternehmen würden für Dritte die Kommunikation mit den Nutzerinnen Nutzern ihres Dienstes unterbinden. Dadurch hätten innovative, datenschutzfreundlichere Systeme kaum Möglichkeiten, sich am Markt zu positionieren. Nach Auffassung eines Dienstes sollte eine Trennung von Nachrichtentransport und Apps eingehend geprüft werden.

Datenschutzaudits für Anbieter finden unter den Befragten weniger Beachtung. Ein Dienst erklärt, es wäre auf jeden Fall hilfreich, wenn die Regierung solche Audits durchführen würde, vor allem, wenn die Ergebnisse veröffentlicht werden würden. Ein Beispiel seien die Kontrollen der amtlichen Lebensmittelüberwachung in Baden-Württemberg.[303]

Ein anderer Dienst weist auf zwei Aspekte hin: Verpflichtende Audits für ausländische Dienste dürften schwer umsetzbar sein. Freiwillige Audits könnten das Ansehen datenschutzfreundlicher Dienste in der Öffentlichkeit erhöhen, beeinflussten aber vor allem den Wettbewerb zwischen

---

[302] Ein Modell für Branchenteilnehmer aller Größen und Reifegrade, das eine Anleitung zur Einbeziehung, Bewertung und Verbesserung der Benutzersicherheit bietet. Die Prinzipien machen die Benutzersicherheit zur grundlegenden Designüberlegung (Quelle: Australischer eSafety-Beauftragter).

[303] Siehe *MLR Baden Württemberg*, abrufbar unter: https://verbraucherinfo.ua-bw.de/lmk.asp?ref=3.

datenschutzfreundlichen Anbietern, während marktstarke Anbieter einfach keinen freiwilligen Audit durchführten, wenn zu erwarten wäre, dass das Ergebnis nicht positiv ausfällt.
Das Bundeskartellamt hat aus den Maßnahmen, die die Dienste kommentiert haben, diejenigen einer näheren Analyse unterzogen, die den meisten Zuspruch fanden (siehe dazu die folgenden Kapitel). Sie fügen sich ein in eine Strategie, Datenschutz sowohl auf Seiten der anbietenden Dienste als auch auf Seiten der nachfragenden Verbraucherinnen und Verbraucher als Differenzierungsmerkmal bzw. als Auswahlkriterium im Wettbewerb zu mehr Bedeutung zu verhelfen.

II. Datenschutz als Wettbewerbsparameter

Im Folgenden wird zunächst erörtert, wie Datenschutz auf der Angebotsseite – bei den Diensten – gefördert werden könnte. Bestehen Anknüpfungspunkte, die kurzfristig Erfolg versprechen (dazu unter 1.)? Anschließend geht es um die Frage, ob und wie Maßnahmen gestaltet werden müssen, damit die Verbraucherinnen und Verbraucher als Nachfragende zu datenschutzfreundlichen Diensten wechseln, trotz eines nachteiligen Informationsgefälles, was sich bisher zugunsten von Akteuren mit hoher Erreichbarkeit und einem entgeltfreien Angebot auswirkt. Hierzu werden Beiträge aus der Wissenschaft vorgestellt, die für die Auswahl von Maßnahmen Hinweise geben können (dazu unter 2.).

1. Stärkung datenschutzfreundlicher Dienste (Angebotsseite)

In den Ermittlungen haben sich viele Messenger-Dienste dazu geäußert, wie datenschutzfreundliche Messenger- und Video-Dienste gestärkt werden könnten. Ein Aspekt war die Förderung von Open Source und Standardisierung, wo Verbesserungen gewünscht wurden. Als weiterer Ansatzpunkt wurde der Einsatz datenschutzfreundlicher Dienste - nicht nur datenschutzfreundlicher Open Source-Anwendungen, sondern auch anderer datenschutzfreundlicher Dienste - im öffentlichen Bereich genannt. Damit verbunden ist die Hoffnung, so auch in anderen privatwirtschaftlichen Bereichen eine höhere Akzeptanz weniger bekannter datenschutzfreundlicher Anwendungen zu erreichen.
Bei Recherchen zu gegenwärtigen Fördermöglichkeiten ist das Bundeskartellamt - jenseits der großen Förderprogramme - auf nur wenige gezielte Förderprogramme für freie Anwendungen, kleine Unternehmen oder Start-Ups gestoßen. Erwähnenswert sind die Open-Source-Software-Strategie 2020-2023 unter dem Motto “Think Open” der EU-Kommission und der "Software-Sprint" des BMBF für „innovative Einzelprojekte kreativer Vordenker (freie Programmiererinnen und Programmierer) in den Bereichen Civic Tech, Data Literacy, Open Data und Open Source“. Das Bundeskartellamt hat daher bei Messenger- und Video-Diensten, die sich zur Förderung von Open Source ausführlicher geäußert haben um weitere Erläuterungen zum Thema gebeten.
Nach Ansicht von Branchenvertretern ist die wichtigste Organisation in Europa im Bereich der Förderung von Open Source - Kommunikationssoftware die „NLnet Foundation“, insbesondere in Zusammenarbeit

mit der „Next Generation Internet Initiative“[304] der Europäischen Kommission sowie der „Prototyp Fund“[305] des Bundesministeriums für Bildung und Forschung.[306]

Die **NLnet Foundation** unterstützt Organisationen und Menschen, die zu einer offenen Informationsgesellschaft beitragen. Sie war in den 1980er Jahren maßgeblich an der Verbreitung des Internets in ganz Europa beteiligt. [307] Die Europäische Kommission hat die **Next Generation Internet Initiative (NGI)** ins Leben gerufen, um talentierte Forscher und Innovatoren zu finanzieren und zu fördern, um die für das Internet von morgen erforderlichen Technologien zu entwickeln. Dabei geht es insbesondere um Open Source-Lösungen, die Vertrauen, Schutz der Privatsphäre, Sicherheit und Inklusion sowie eine europäische Open Source-Alternative zu kommerziellen Standardprodukten bieten.[308] „Das Gute an solchen Tools sei“ - so die Europäische Kommission - „dass Endnutzerinnen und -nutzer die volle Kontrolle über sie besitzen und sie gleichzeitig unsere Daten schützen, sodass wir alles besprechen können, was für unser Unternehmen vertraulich oder für unsere Familie intim ist. Selbst wenn die Internetverbindung unterbrochen ist, sind diese Apps nicht auf die Verbindung zu einem einzelnen Anbieter angewiesen, und viele von ihnen können auf unseren Endgeräten ohne Unterbrechung ausgeführt werden“[309]. Einige der vom Bundeskartellamt befragten Dienste - BigBlueButton, Conversations, DeltaChat, Dino, Meet.jit.si - haben von der Organisation Förderungen erhalten.[310] Die XSF bezeichnet die Förderplattform als beliebt und vergleichsweise leicht zugänglich, da

---

304 Nach dem ersten Projektjahr sind nun die ersten Entwicklungen verfügbar, die Vertrauen, Schutz der Privatsphäre, Sicherheit und Inklusion sowie eine europäische Open Source-Alternative zu kommerziellen Standardprodukten bieten.

305 Siehe *Prototype Fund*, abrufbar unter: https://prototypefund.de/.

306 Erwähnungswert sei schließlich noch der „Google Summer of Code“. Dabei handelt es sich um ein von Google organisiertes jährliches Programmierstipendium und nicht um ein langfristiges Förderprogramm. Nichtsdestotrotz wird es von Branchenvertretern als hilfreiches Programm bezeichnet, an welchem man sich bereits mehrfach beteiligt hätte. Siehe *Google*, abrufbar unter: https://summerofcode.withgoogle.com/ und *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Google_Summer_of_Code.

307 Vgl. *NLnet Foundation*, abrufbar unter: https://nlnet.nl/ und https://de.wikibrief.org/wiki/NLnet.

308 Vgl. *Next Generation Internet*, abrufbar unter: https://www.ngi.eu/about/.

309 Vgl. *Next Generation Internet*: Menschenzentrierte Technologien in Krisenzeiten, abrufbar unter: https://ngi.eu/wp-content/uploads/sites/48/2020/04/NGI4ALL_NGI-for-COViD19_DEU.pdf.

310 Eine Liste der aktuell geförderten Projekte ist einsehbar unter *NLnet Foundation* https://nlnet.nl/project/current.html.

sie sich dadurch auszeichne, auch kleine Finanzierungsbeträge zu stiften. Sie „könnte ein Beispiel für eine (weitere) deutsche Förderplattform sein“.

Der **Prototype Fund** ist ein Projekt der Open Knowledge Foundation[311] Deutschland, gefördert durch das Bundesministerium für Bildung und Forschung (BMBF). Gefördert werden Entwicklerinnen und Entwickler aus der Zivilgesellschaft, „die frei verfügbare nutzerzentrierte Technologien gestalten, welche - unabhängig von ihrer finanziellen Verwertbarkeit - die Grundlagen des (digitalen) Zusammenlebens und gesellschaftlichen Mehrwert schaffen“. Von 2016 bis 2024 werden in 16 Förderrunden jeweils ca. 25 innovative Projekte gefördert. Selbstständige Programmiererinnen und Programmierer und kleine Teams, die in Deutschland wohnen, können für jedes Projekt maximal 47.500 Euro erhalten. Die Ergebnisse müssen unter einer Open-Source-Lizenz öffentlich zugänglich gemacht werden.

Branchenvertreter kritisieren den starken **Fokus auf Innovation** bei der NLnet Foundation und den meisten Förderprogrammen. Gefördert würden entweder komplette Neuentwicklungen - wie beispielsweise durch den Prototype Fund - oder zumindest die Entwicklung neuer Funktionen für eine bestehende Open Source Software. Häufig reiche es aber nicht, einzelne innovative Ideen zu haben und umzusetzen. Projekte müssten zusätzlich weiterhin den marktüblichen Funktionsumfang haben, um konkurrenzfähig zu sein. Ein Projektvorhaben sei beim Prototype Fund abgelehnt worden, wohl auch, weil eine ähnliche Funktion bereits in einem zentralisierten System verfügbar war und es offenbar nicht als eine signifikante Innovation für Nutzerinnen und Nutzer betrachtet wurde, diese auf ein dezentrales System zu portieren.

Außerdem fließe ein nicht zu vernachlässigender Teil der Arbeit an Open Source - Projekten in die **Wartung von Software und eventuell benötigter Infrastruktur** (Server etc.). Der rein technische Betrieb dieser Infrastruktur (beispielweise Serverkosten etc.) werde fast nie gefördert. So würden immer neue Funktionen für eine Software entwickelt, die einschließlich der Infrastruktur aber nicht mehr auf Fehler überprüft werde. Das gelte auch für verbreitete Software, die bereits von vielen Menschen verwendet werde. Handelt es sich bei dieser Open Source - Software um eine „Bibliothek“, die von vielen anderen

---

311 Siehe *Open Knowledge Foundation, abrufbar unter:* https://okfn.de/ oder siehe *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Open_Knowledge_Foundation_Deutschland. Die Open Knowledge Foundation Deutschland e. V. (OKFDE) ist eine gemeinnützige Organisation mit Sitz in Berlin, die 2011 gegründet wurde. Sie setzt sich mit mehreren Projekten, unter anderem in den Bereichen Informationsfreiheit, Offenes Regierungshandeln, Open Data, Civic and Public Interest - Tech sowie Bildung für die Verbreitung und Nutzung von „offenem Wissen“ ein. Die Organisation ist Teil des internationalen Open Knowledge Netzwerkes aus insgesamt 24 Ländern. Die Vereinsarbeit ist unabhängig, überparteilich, interdisziplinär und nicht kommerziell.

Projekten – auch von proprietären Systemen genutzt werde, so erhalte das Problem der schlechteren Wartung immer mehr Gewicht, was von einem der Befragten mit weitergeleiteten, nachfolgend abgebildeten Comic [312] veranschaulicht wurde (siehe Abbildung 17).

Die fehlende Förderung zur **Wartung, Instandhaltung und Pflege** wichtiger und verbreitet eingesetzter Open-Source-Software sei auch ein entscheidender Grund für einige große **Sicherheitslücken** in den letzten Jahren gewesen.[313]

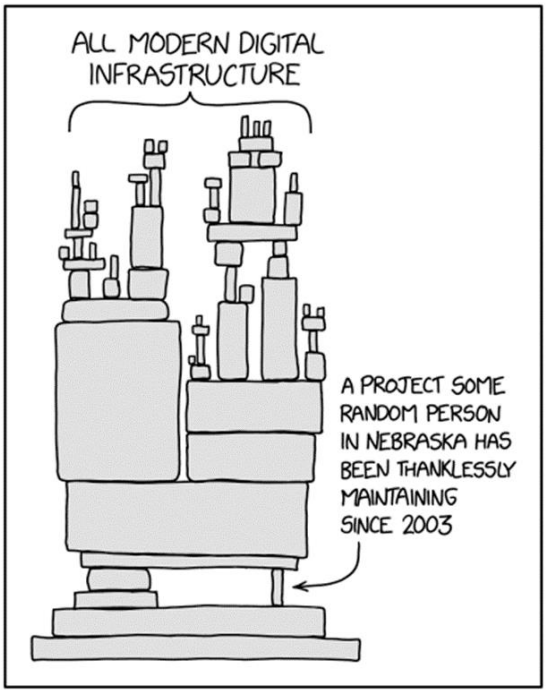


Abbildung 17: Folgen fehlender Wartung bei Open Source-Software

Ein Dienst erläutert, man versuche nun die Wartung der eigenen Infrastruktur über Spendengelder sicherzustellen. Wirklich planbar sei der Erfolg einer solchen Kampagne aber nicht. Die XSF führt aus,

---

312 Siehe https://xkcd.com/2347/. Quelle: Ermittlungen.

313 Beispiele seien die Schwachstelle „Log4Shell“ bei der Programmiersprache Java oder der inzwischen behobene Programmfehler in der Open Source Bibliothek OpenSSL „Heartbleed“, der das TLS-Protokoll betraf. Siehe zu “Log4Shell” *BSI*, Pressemeldung vom 16.12.21, Update: Warnstufe Rot: Schwachstelle Log4Shell führt zu extrem kritischer Bedrohungslage, abrufbar unter: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/211211_log4Shell_WarnstufeRot.html sowie zu „Heartbleed“, siehe Frankfurter Allgemeine Zeitung, „Heartbleed” ist noch nicht gestoppt, abrufbar unter: https://www.faz.net/aktuell/wirtschaft/netzwirtschaft/bsi-warnt-heartbleed-ist-noch-nicht-gestoppt-12898921.html.

schon mit kleinen Förderbeträgen könnten Wartung, Instandhaltung und Pflege nachhaltig betrieben werden.

Schließlich wird der in vielen Bereichen beklagte **Bürokratie- und Zeitaufwand**, der mit einer Antragstellung einhergeht, auch bei der Förderung von Open Source-Projekten als Hemmnis empfunden. Insbesondere gebe es keine leicht zugänglichen Informationen über Fördermöglichkeiten, diese müssten mit viel Zeitaufwand gesucht werden. Auch bei der Förderung von Open Source sei die Zeitspanne von der Beantragung der Gelder bis zur Auszahlung recht lang und die Bewilligung natürlich ungewiss. Daher würden nur größere Vorhaben überhaupt beantragt, kleinere Projekte wären schon längst implementiert bis die Gelder ausgezahlt würden.

Im öffentlichen Bereich ist das Bundeskartellamt auf Beispiele für den **Einsatz von Open Source** gestoßen, wenn auch zunächst weniger konkret im Bereich der Messenger- und Video-Dienste. Zu nennen ist beispielsweise die Open Source - Strategie des Landes Schleswig-Holstein[314]**,** die Open Source - Strategie „LiMux" der Stadt München[315] sowie die Initiative der Stadt Dortmund[316]**.** Verwiesen

---

[314] So hatte Schleswig-Holstein im 2017 geschlossenen Koalitionsvertrag der schwarz-grün-gelben Landesregierung festgehalten, alle Beamten und Angestellten des Landes einschließlich der Lehrkräfte mit Open Source-Software auszustatten. Der zuständige Digitalminister Jan Philipp Albrecht (Bündnis 90/Die Grünen) hat - Presseberichten zufolge - die Pläne inzwischen konkretisiert. Bis Ende 2026 soll Microsoft Office durch Libre Office und später Windows durch Linux ersetzt werden. Vgl. *Heise*, abrufbar unter: https://www.heise.de/news/Schleswig-Holsteins-Digitalminister-Albrecht-ueber-den-Wechsel-zu-Open-Source-6221361.html sowie *LinuxNews*, abrufbar unter: https://linuxnews.de/2021/11/schleswig-holstein-macht-ernst-mit-open-source/.

[315] In München war eine Open Source - Strategie verfolgt worden, die unter dem Schlagwort „LiMux" bekannt geworden war. Nach Schwierigkeiten war das Projekt 2017 eingestellt worden. Inzwischen bestehen aber Pläne, die Open Source-Strategie wieder fortzusetzen. Siehe *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/LiMux, *Deutschlandfunk Nova*, abrufbar unter: https://www.deutschlandfunknova.de/beitrag/linux-versus-microsoft-m%C3%BCnchen-will-wieder-zurueck-zu-mehr-open-source.

[316] Weiteres positives Beispiel ist die Stadt Dortmund, die zukünftig den Einsatz von Open-Source-Software gegenüber proprietärer Software priorisieren will und dies in einem „Memorandum zur Digitalisierung 2020 bis 2025" festgehalten hat. Vgl. *Der Neue Kämmerer*, abrufbar unter: https://www.derneuekaemmerer.de/digitalisierung/news/dortmund-setzt-auf-open-source-software-13460/, *Do-Foss*, abrufbar unter: https://blog.do-foss.de/beitrag/freie-software-ist-von-jetzt-an-standard-in-dortmund/, *Golem*, abrufbar unter: https://www.golem.de/news/verwaltung-dortmund-beschliesst-open-source-fuer-die-stadtverwaltung-2104-155449.html.

wird in den Ermittlungen auch auf die Corona-Warn-App für die Zeit nach Veröffentlichung des Quellcodes. Mehr als 65.000 freiwillige Software-Expertinnen und -experten hätten sich die bereits veröffentlichten Quellcodes angesehen und eigene Vorschläge für Verbesserungen gemacht.[317] Auch im Ausland wird ein Umstieg auf Open Source - Software in der Verwaltung thematisiert, so z. B. in der Schweiz[318], in der Stadt Barcelona[319] oder der Stadt Tirana, die bereits 2018 beschlossen hat, Open Source - Software einzusetzen. [320]

Speziell im Hinblick auf **Messenger- und Video-Dienste** setzen einige Hochschulen freie Messenger-Systeme, wie z. B. das Matrix-Protokoll, ein.[321] Dazu zählen z. B. die Universität Augsburg[322], die

---

317 Siehe *Die Bundesregierung*, abrufbar unter: https://www.bundesregierung.de/breg-de/suche/corona-warn-app-1757082, *ZEIT ONLINE*, abrufbar unter: https://www.zeit.de/digital/2020-05/corona-app-open-source-projekt-programmcode-quellcode sowie *Science Media Center*, abrufbar unter: https://www.sciencemediacenter.de/alle-angebote/fact-sheet/details/news/wie-apps-und-programmcode-ueberprueft-werden/.

318 In der Schweiz gibt der Bund mit einem neuen Leitfaden des Schweizer Bundes Empfehlungen und Hintergrundwissen über die Nutzung und Weiterverbreitung von Open Source Software (OSS) in der Bundesverwaltung, um deren Einsatz zu unterstützen. Siehe *Leitfaden des Schweizer Bundes,* abrufbar unter: https://www.pro-linux.de/news/1/27770/schweiz-neuer-leitfaden-unterst%C3%BCtzt-einsatz-von-oss-in-der-verwaltung.html.

319 Die Stadt Barcelona setzt in der Verwaltung keine Software von Microsoft - z. B. den E-Mail-Client Outlook - mehr ein, auch wenn Windows als Betriebssystem zunächst beibehalten wird. Der Umstieg auf Linux wurde geplant. Siehe auch *El Pais*, abrufbar unter: https://elpais.com/ccaa/2017/12/01/catalunya/1512145439_132556.html. Siehe *Heise*, abrufbar unter: https://www.heise.de/newsticker/meldung/Stadt-Barcelona-setzt-auf-Open-Source-und-Linux-3944797.html

320 Vgl. LibreOffice, abrufbar unter: https://blog.documentfoundation.org/blog/2018/11/22/municipality-of-tirana/.

321 Im Rahmen der Sektoruntersuchung konnte nicht überprüft werden, wie die Hochschulen das Matrix-Protokoll im Hinblick auf einen schützenden Umgang mit den Daten der Universitätsangehörigen und Studierenden umsetzen.

322 Vgl. *Universität Augsburg*, abrufbar unter: https://www.uni-augsburg.de/de/fakultaet/mntf/physik/facilities/itservices/elequick/.

Universität Bielefeld[323], die Ruhr Universität Bochum[324], die Technische Universität Chemnitz[325], die Technische Universität Dresden[326], die Universität Heidelberg[327], die Universität Innsbruck[328], die Leibniz Universität Hannover[329] oder die Universität Osnabrück[330]. Zu nennen ist hier auch wieder die Open Source -Strategie des Landes Schleswig-Holstein, im Rahmen derer ein freier Messenger - Client in der öffentlichen Verwaltung eingesetzt werden soll.[331]

Die in den Ermittlungen formulierten **Erwartungen der befragten Dienste an den öffentlichen Bereich** bezogen sich nicht allein auf eine Überprüfung der Förderpraxis und Einsatzmöglichkeiten für Open Source, sondern generell auf den **Einsatz datenschutzfreundlicher Dienste**. Damit ist die Hoffnung verbunden, auch in anderen Bereichen die Chancen weniger bekannter datenschutzfreundlicher Dienste zu erhöhen.

Die Erkenntnisse des Bundeskartellamts aus den Ermittlungen und eigenen Recherchen legen nahe, dass die öffentliche Hand ihren Einsatz datenschutzfreundlicher Messenger- und Video-Dienste ausbauen kann. Branchenvertreter und Interessenvertreter freier Messenger-Systeme haben zahlreiche Beispiele vorgelegt, dass erheblicher Einsatz und Überzeugungskraft notwendig ist, damit datenschutzfreundliche Messenger- und Video-Dienste, die **weniger bekannt sind als die etablierten Dienste**, in Erwägung gezogen werden. Wettbewerber etablierter Dienste haben auf **Ausschreibungsbedingungen** verwiesen,

---

323 Siehe *Universität Bielefeld*, abrufbar unter: https://uni-bielefeld.de/einrichtungen/bits/services/kommunikation/teamchat/howto/element-android/.

324 Vgl. *Ruhr Universität Bochum*, abrufbar unter: https://www.it-services.ruhr-uni-bochum.de/services/issi/element.html.de.

325 Vgl. *Technische Universität Chemnitz*, abrufbar unter: https://www.tu-chemnitz.de/urz/groupware/chat/doku/nutzen.html.

326 Vgl. *Ruhr Universität Bochum*, abrufbar unter: https://www.it-services.ruhr-uni-bochum.de/services/issi/element.html.de.

327 Vgl. *Universität Heidelberg, abrufbar unter*: https://www.urz.uni-heidelberg.de/de/service-katalog/collaboration-und-digitale-lehre/heichat.

328 Vgl. *Universität Innsbruck*, abrufbar unter: https://www.borncity.com/blog/2021/05/03/uni-innsbruck-setzt-auf-matrix-element-statt-auf-ms-teams/.

329 Vgl. *Universität Hannover*, abrufbar unter: https://www.luis.uni-hannover.de/de/services/kommunikation/matrix-messenger/.

330 Vgl. *Universität Osnabrück*, abrufbar unter: https://www.wiwi.uni-osnabrueck.de/fachbereich/edv_betreuung/anleitungen_hinweise/element_chat_ehemals_riot.html.

331 Siehe *Golem*, abrufbar unter: https://www.golem.de/news/messenger-schleswig-holstein-will-matrix-chat-fuer-verwaltung-2007-149687.html.

die die Chancen datenschutzfreundlicher Dienste eher verringern. Diese Praxis könnte überprüft werden und überlegt werden, ob nicht im Vergleich zur bisher gewählten Anwendung datenschutzfreundlichere Alternativen existieren und im öffentlichen Bereich zumindest zusätzlich eingesetzt werden können. Gerade dem öffentlichen Rundfunk und Fernsehen könnte dabei eine **Multiplikator-Wirkung** zukommen. Die Chance möglichst viele unterschiedliche Verbrauchergruppen zu animieren, datenschutzfreundliche Messenger-Systeme zu nutzen, indem diese als Kommunikationskanal jedenfalls wenigstens auch angeboten werden, bleibt bisher häufig - selbst bei bekannten Sendungen und Kanälen - ungenutzt. [332]

---

[332] Beispiele sind die Fernsehsendungen „ARD-Morgenmagazin“, siehe *ARD*, abrufbar unter: https://www.daserste.de/information/politik-weltgeschehen/morgenmagazin/specials/moma-bei-whatsapp-100.html; „Live nach Neun“, siehe *ARD*, abrufbar unter: https://www.daserste.de/information/politik-weltgeschehen/morgenmagazin/specials/moma-bei-whatsapp-100.html; die Radiosendung Kontrovers, siehe *ARD*, abrufbar unter: https://www.daserste.de/information/ratgeber-service/live-nach-neun/whatsapp-102.html, die Radiosender*; Bremen Eins*, abrufbar unter: https://www.bremeneins.de/kontakt/kontakt-startseite-116.html; *Bremen Zwei*, abrufbar unter: https://www.bremenzwei.de/kontakt/kontakt-startseite-114.html; *Bremen Vier*, abrufbar unter: https://www.bremenvier.de/kontakt/kontakt-startseite-100.html; *Bremen Next*, abrufbar unter: https://www.bremennext.de/kontakt/kontakt-136.html; COSMO, siehe *WDR*, abrufbar unter: https://www1.wdr.de/radio/cosmo/ueber-uns/kontakt/index.html; 1Live, siehe *WDR*, abrufbar unter: https://www1.wdr.de/radio/1live/on-air/kontakt/whatsapp260.html; hr*3*, abrufbar unter: https://www.hr3.de/service/hr3-per-whatsapp-erreichen-0800--33-33-307,whatsapp-112.html; rbb 88.8, abrufbar unter: https://www.rbb888.de/; *WDR 2*, abrufbar unter: https://www1.wdr.de/radio/wdr2/kontakt/index.html; S*R 1*, abrufbar unter: https://www.sr.de/sr/sr1/wir/sr1_social_media100.html; *SR 3*, abrufbar unter: https://www.sr.de/sr/sr3/service/sr3_social_media100.html; *UNSERDING*, abrufbar unter: https://www.unserding.de/unserding/unserding_bei_whatsapp_100.html; *SWR 4 Rheinland Pfalz*, abrufbar unter: https://www.swr.de/swr4/kontakt/kontakt-per-whatsapp-100.html; *MDR*, abrufbar unter: https://www.mdr.de/sachsenradio/whats-app-sprachnachricht-sachsenradio-100.html; das Morgenprogramm von *MDR* Sachsen-Anhalt, abrufbar unter: https://www.mdr.de/mdr-sachsen-anhalt/mdr-sachsen-anhalt-bei-whatsapp100.html sowie das Team des Podcasts „Ab 21“ von *Deutschlandfunk Nova*, abrufbar unter: https://www.deutschlandfunknova.de/podcasts/download/ab-21 auf WhatsApp erreichbar. Zudem nutzt der Radiosender 1Live *Snapchat*, abrufbar unter: https://www.snapchat.com/add/wdr1live. Per WhatsApp und Telegram erreichbar sind z. B. *Bayern 2*, abrufbar unter: https://www.br.de/radio/bayern2/service/newsletter/bayern-2-newsletter-whatsapp-telegram100.html; *SWR 1 Baden-Württemberg*, abrufbar unter: https://www.swr.de/swr1/bw/artikel-

Bei **Städten und Gemeinden** haben Stichproben ebenfalls ergeben, dass hier auf die am weitesten verbreiteten Messenger-Systeme gesetzt wird.[333]

Auch in **dem Bereich der Bundesverwaltung** bestehen Möglichkeiten, um die Kommunikation über datenschutzfreundliche und rechtskonforme Messenger-Systeme zu fördern, wie die Recherche gezeigt hat. Zu berücksichtigen ist dabei, dass öffentliche Stellen ihre Adressatinnen und Adressaten auch erreichen können müssen.

Im **Bildungsbereich** ist die Situation schwerer zu bewerten und zu überschauen. Für die **Kommunikation der Schule mit Lehrkräften, Eltern und Schülerinnen und Schülern** gibt es Handreichungen der

swr1-auf-whatsapp-100.html; *SWR 1 Rheinland Pfalz*, abrufbar unter: https://www.swr.de/swr1/rp/kontakt/article-swr-8188.html sowie S*WR 4 Baden-Württemberg*, abrufbar unter: https://www.swr.de/swr4/kontakt/index.html. Der WDR bietet an, Nutzerinnen und Nutzern über den Facebook Messenger oder über Telegram Nachrichten aus und für NRW zu senden. Darüber hinaus habe man über den Facebook Messenger auch die Möglichkeit, selbst nach Themen zu fragen oder – wie bei Siri und Alexa – sich ein wenig mit dem WDR aktuell Bot zu unterhalten. Vgl. *WDR*, abrufbar unter: https://www1.wdr.de/nachrichten/handy-nachrichten-wdr-aktuell-100~_redirectedFromOffline-true.html. Die „tagesschau" bietet an, zweimal täglich die aktuell wichtigsten Nachrichten und zudem Eilmeldungen per Messenger zu versenden. Diese Möglichkeit wird für die Messenger von Apple, Facebook, Telegram und Notify eröffnet. Einen Nachrichtenversand über WhatsApp könne man nicht anbieten, weil WhatsApp seit Ende 2019 keine Newsletter mehr dulde, vgl. *Tagesschau*, abrufbar unter: https://www.tagesschau.de/inland/messenger-113.html.

[333] So haben Stichproben ergeben, dass z. B. die Bonn Information auch über WhatsApp für Fragen und Anliegen zur Verfügung steht. Auch ein Ticket für eine Stadtrundfahrt oder für Stadtführungen könne über die diese App reserviert werden, siehe *Stadt Bonn*, abrufbar unter: https://www.bonn.de/bonn-erleben/anreisen/service-whats-app.php. Die Stadt Nürnberg informiert ihre Bürgerinnen und Bürger per Telegram und Notify über Wichtiges aus dem Nürnberger Stadtgebiet und der Stadtverwaltung. Die angemeldeten Bürgerinnen und Bürger bekämen von Montag bis Freitag einmal pro Tag das Update für Nürnberg. Außerdem informiere die Stadt ihre Bürger auch bei wichtigen Ereignissen mit einer Meldung, siehe *Stadt Nürnberg*, abrufbar unter: https://www.nuernberg.de/internet/stadtportal/messenger_anmeldung.html**.** Die Stadt Reutlingen bietet Corona-Nachrichten über Telegram und Notify an. Gemeinden sowie die zugehörigen gemeindlichen Institutionen (z. B. Gemeindewerke, Gemeindestrom oder KITA) bieten Bürgerservice über WhatsApp an, siehe z. B. *Gemeinde Wadgassen*, abrufbar unter: https://www.wadgassen.de/rathaus-service/buergerservice/whatsapp/ oder *Gemeinde Vettweiß*, abrufbar unter: *https*://www.vettweiss.de/news/news-archiv/whatsweiss.php.

Kultusministerkonferenz und verschiedener Schulministerien der Bundesländer.[334] Dies ist vor allem der Corona-Pandemie und den Anforderungen des Home Schooling geschuldet. Die Maßnahmen sind sehr unterschiedlich. Allerdings gehen viele Schulen davon abweichend doch eigene Wege, möglicherweise, weil die angebotenen Lösungen die praktischen Anforderungen nicht erfüllen.
Ob und wie die Verbraucherinnen und Verbraucher animiert werden könnten, **nicht nur praktikable, sondern auch gleichzeitig datenschutzfreundliche** Messenger- und Video-Dienste zu verwenden, wird im folgenden Kapitel erörtert.

2. Aktivierung der Nachfrageseite

Wie die Ermittlungsergebnisse gezeigt haben, sehen alle Messenger- und Video-Dienste die weitere Aufklärung der Verbraucherinnen und Verbraucher als wesentliches Element einer Datenschutzstrategie an. Das Bundeskartellamt teilt diese Auffassung. Sofern Initiativen dazu neu ausgerichtet und intensiviert würden, könnten datenschutzfreundliche Dienste möglicherweise bessere Chancen haben, sich gegenüber Wettbewerbern durchzusetzen. Daher werden im Folgenden zunächst die Informationsdefizite, die bei den Verbraucherinnen und Verbrauchern bestehen, näher beleuchtet (siehe a) und b)). Anschließend werden Konsequenzen für die Verbraucherpolitik erörtert, die sich an der Situation der Verbraucherinnen und Verbraucher ausrichten sollte (siehe c)).

a) Datenschutz als Qualitätseigenschaft?

Die Präferenzen der Verbraucherinnen und Verbraucher sind – was den Datenschutz angeht – kontextspezifisch, uneinheitlich und nicht immer wohlüberlegt (zum sog. Privacy Paradox siehe auch unter F.II.2).[335] Wenn sich Verbraucherinnen und Verbraucher für einen Messenger- und Video-Dienst entscheiden, handelt es sich um eine zusammengesetzte Transaktion.[336] Ihr Hauptaugenmerk liegt auf dem Produkt „Messaging und Videokonferenzen“, wohingegen die Datenverarbeitungstransaktion als

---

[334] Vgl. z. B. *Kultusministerkonferenz*, abrufbar unter: https://www.kmk.org/themen/bildung-in-der-digitalen-welt/distanzlernen.html sowie *Land Brandenburg*, abrufbar unter: https://bildungsserver.berlin-brandenburg.de/online-lernen-tools.

[335] Vgl. *Kerber*, Digital markets, data and privacy: Competition Law, Consumer Law and Data Protection, Joint Discussion Paper Series in Economics No. 14, 2016, S. 7, abrufbar unter: https://www.uni-marburg.de/fb02/makro/forschung/magkspapers/paper_2016/14-2016_kerber.pdf.

[336] Vgl. *Jentzsch*, State-of-the-Art of the Economics of Cyber-Security and Privacy, IPACSO – Innovation Framework for ICT Security Deliverable, 2016, S. 35, abrufbar unter: https://www.econstor.eu/bitstream/10419/126223/1/Jentzsch_2016_State-Art-Economics.pdf.

zeitlich nachgelagerter Effekt weniger Beachtung findet. Dies gilt auch für unentgeltliche Angebote, wo ggf. über die Datenverarbeitungstransaktion oder andere Funktionen bezahlt wird.
Messenger- und Video-Dienste werden erst dann in gewünschtem Ausmaß in Datenschutz investieren und dies verständlich kommunizieren oder sogar bewerben, wenn die Verbraucherinnen und Verbraucher Datensparsamkeit, Datenschutzkonformität und Datensicherheit als Qualitätsmerkmal eines Dienstes betrachten. Datenschutz könnte dann zum **Wettbewerbsvorteil** von Diensten werden. Bisher trifft dies nur auf einige Dienste zu, die mit vielen Maßnahmen zur Datensicherheit und zum Datenschutz werben, Datenschutz somit als komparativen Wettbewerbsvorteil einsetzen und dafür ein entsprechendes Entgelt verlangen.
Damit datensichernde und datenschützende Aktivitäten der Dienste flächendeckend zunehmen, sind die Verbraucherinnen und Verbraucher nicht nur zu informieren, sondern auch zu motivieren, die notwendigen Informationen von den Diensten einzufordern, indem nur die Clients derjenigen Messenger- und Video-Dienste verwendet werden, die **informierte Entscheidungen** ermöglichen.
Notwendig dazu ist aber nicht nur, die Verbraucherinnen und Verbraucher zu aktivieren und in ihnen das Bedürfnis zu wecken, datenschützende Dienste zu nutzen. Sie müssen sich auch mit vertretbarem Aufwand über die Datenschutzqualität des gewünschten Produktes „Messenger- und Video-Dienst“ informieren und vergleichen können. Derzeit ist das nur sehr eingeschränkt, z. B. über Webseiten von IT-Experten oder vergleichende Darstellungen von bestimmten Instituten, möglich. Die überprüften Merkmale richten sich hier allerdings meistens nach dem Aufgabenreich und den Kernkompetenzen der veröffentlichenden Institution. Die Informationen veralten zudem schnell, wenn sie von den Verbraucherinnen und Verbrauchern überhaupt gesucht und aufgefunden werden. Die Datenschutzqualität eines Dienstes ist so schwer festzustellen.
Ob und inwieweit die Verbraucherinnen und Verbraucher die Qualitätseigenschaften eines Produktes bewerten können, kann mit dem sog. **Qualitätsunsicherheitsansatz**[337] veranschaulicht werden. Dabei werden drei Güterkategorien gebildet, die sich danach unterscheiden, ob die Qualität eines Produktes vor und/oder nach dem Kauf beobachtet werden kann. Bei den sog. **Suchgütern** kennen die Verbraucherinnen und Verbraucher die Qualität des Produktes vor und nach dem Kauf. Bei den sog. **Erfahrungsgütern** kann die Qualität des Produktes erst nach dem Kauf beurteilt werden. Sog.

---

[337] Vgl. *Nelson*, Advertising as Information, in: Journal of Political Economy 1974, 729, abrufbar unter: https://www.jstor.org/stable/1837143?seq=1, sowie *Darby/Karni*, Free Competition and the Optimal Amount of Fraud, in: Journal of Law and Economics 1973, 67, abrufbar unter: https://www.journals.uchicago.edu/doi/10.1086/466756.

Vertrauensgüter kennzeichnet, dass die Qualität des Produktes den Verbraucherinnen und Verbrauchern auch nach dem Kauf noch verborgen bleibt.
Wenn es um die Datenschutzqualität geht, dürften einige Verbraucherinnen und Verbraucher diese derzeit als **Erfahrungsgut** beschreiben. Wie die Sektoruntersuchung gezeigt hat, können sich Verbraucherinnen und Verbraucher vor dem Kauf kaum einen Überblick über alle datenschutzrelevanten Eigenschaften des favorisierten Produktes machen. Die Datenschutzpraktiken und das Informationsverhalten der Dienste sind uneinheitlich und intransparent. Die Nutzerinnen und Nutzer stellen z. B. möglicherweise erst bei Verwendung eines Dienstes fest, dass sie personenbezogene Daten preisgeben müssen, z. B. auch für die Einrichtung eines Kontos, um bestimmte über die Grundfunktionen hinaus gehenden Funktionen nutzen zu können. Die meisten Verbraucherinnen und Verbraucher würden wahrscheinlich von einem **Vertrauensgut** sprechen. Bestimmte Gruppen von Verbraucherinnen und Verbrauchern blenden bisher jegliche datenschutzrechtlichen Aspekte bei ihren Entscheidungen aus, sei es aus Unkenntnis, Desinteresse, aus Zeitmangel oder einfach, weil sie angesichts der Komplexität der Informationsbeschaffung aufgegeben haben (siehe hierzu auch F.II.2.). Außerdem ist auch den interessierten und informierten Nutzerinnen und Nutzern meistens nicht bewusst, in welchem Ausmaß ihre Daten erhoben sowie von wem und wofür sie verwendet werden. Schließlich ist der tatsächliche Datenfluss nur mit erheblichem technischem Aufwand und im Hinblick auf die konkret übermittelten Inhalte häufig überhaupt nicht überprüfbar. Unter solchen Bedingungen können keine informierten Entscheidungen getroffen werden. Die Materie ist zu komplex, als dass die Verbraucherinnen und Verbraucher allein über eine Senkung der **Suchkosten**[338] ihren Informationsstand verbessern könnten. Vielmehr müssen die Informationen so aufbereitet werden, dass ihre Relevanz verstanden wird, sie verständlich sind bzw. in angemessener Zeit verstanden werden können.

[338] Suchkosten sollen hier weit interpretiert werden und umfassen die Kosten jeglicher alternativer bewerteter Verwendung von Ressourcen, die aufgewendet werden müssen, um Informationssuche zu betreiben.

b) Weniger Informationsgefälle - mehr Nachfrage nach Datenschutz?

In informationsökonomischen Ansätzen[339] geht es – über den o. g. Qualitätsunsicherheitsansatz hinaus – zunächst darum, **Qualitätsunsicherheit** zu verringern. Verbraucherinnen und Verbraucher können vor und nach „Vertragsabschluss", was die **(Datenschutz-) Qualität** des gewählten Dienstes angeht, unsicher sein. Zwei Varianten an Aktivitäten sind geeignet, Informationsnachteile abzubauen. Sog. **Screening-Aktivitäten zur Informationsbeschaffung** können sowohl außerhalb als auch innerhalb einer vertraglichen Beziehung unternommen werden. Screening kann alle denkbaren Suchaktivitäten umfassen. Es gehören sowohl alltägliche Sucharbeiten im Internet oder Recherche in anderen Medien dazu als auch komplexere Regelungssysteme, wie z.B. Selbstwahlschemata. Hier führt eine bestimmte vertragliche Bedingung dazu, dass nur derjenige den Vertrag schließt, der diese Bedingung erfüllt (vgl. Selbstbeteiligungsklausel bei Versicherungen).[340] Auch Aktivitäten zur **Informationsübertragung („Signaling")** können geeignet sein, Informationsnachteile abzubauen. Signaling kommt sowohl bei feststehenden, nicht veränderbaren Eigenschaften (sog. Indices) in Frage als auch bei Eigenschaften, die zwar beobachtbar sind, aber noch vom Informanten verändert werden können (Signale i. e. S.).[341] In letztere Kategorie dürfte die Datenschutzqualität einzuordnen sein, welche von Diensten an die Verbraucherinnen und Verbraucher über verschiedenste Maßnahmen signalisiert werden könnte. Probleme der asymmetrischen Informationsverteilung können jedoch nicht allein für Defizite des Marktmechanismus verantwortlich gemacht werden. Kritikerinnen und Kritiker

---

339 Vgl. die grundlegenden Arbeiten von *Stigler*, The Economics of Information, in: The Journal of Political Economy 1961, 213, abrufbar unter: https://home.uchicago.edu/~vlima/courses/econ200/spring01/stigler.pdf und *McCall*, The Economics of Information and Job Search, in: Quarterly Journal of Economics, 1970, S. 113 – 126. Informationsökonomische Ansätze sind Teil der Neuen Institutionenökonomik. Diese umfasst verschiedene theoretische Erklärungsansätze, die im Wesentlichen in vier Schulen unterteilt werden: Der Property-Rights-Ansatz oder Theorie der Verfügungsrechte, der Transaktionskostenansatz, der Prinzipal-Agent-Ansatz und informationsökonomische Ansätze, vgl. z. B. *Picot*, Ökonomische Theorien der Organisation – ein Überblick über neuere Ansätze und deren betriebswirtschaftliches Anwendungspotential, in: *Ordelheide/Rudolph/Büsselmann* [Hrsg.]: Betriebswirtschaftslehre und Ökonomische Theorie, 1991, S. 143.

340 Vgl. *Woratschek*, Betriebsform, Markt und Strategie, 1992, S. 96.

341 Vgl. *Spence*, Informational Aspects of Market Structure: An Introduction, in Quarterly Journal of Economics 1976, 591, 593. Die Effizienz der Informationsmaßnahmen kann anhand der Kosten für Signaling- und Screening-Aktivitäten beurteilt werden.

informationsökonomischer Erklärungsansätze verweisen auf weitere wichtige Einflussgrößen, die ebenfalls Auswirkungen auf das Verbraucherverhalten sowie die Effizienz von Marktergebnissen haben können. Dies können z. B. Transaktionskosten sein, die als Kosten der Anbahnung und Durchführung von Verträgen Informationskosten übersteigen. Maßnahmen, die den Informationsstand der Verbraucherinnen und Verbraucher verbessern, müssen aber vor allem ihre individuellen Eigenschaften und Wahrnehmungen – wie sie das Privacy Paradox beschreibt – einfangen können. Als theoretischer Hintergrund können neuere verhaltensökonomische Erklärungsansätze[342] dienen, aber auch die Neue Institutionenökonomik[343], welche in verschiedensten Forschungsbereichen verwendet wurde, um Austauschbeziehungen und ihre Risiken zu analysieren und sie risikominimierend und kosteneffizient zu gestalten. Der Verhaltensökonomik sind u. a. Überlegungen zu verdanken, wonach Informationen nicht in beliebiger Menge und in beliebig kurzer Zeit wahrgenommen und verarbeitet werden können. Ein zu großes, unübersichtliches Angebot an Entscheidungsalternativen wird eher dazu führen, dass Entscheidungen verweigert oder aufgeschoben werden.[344]

Mehr als verhaltensökonomische Ansätze bieten neoinstitutionenökonomische Erklärungstheorien verallgemeinerbare, einfach verständliche und klar strukturierte Empfehlungen, wie Informationsasymmetrien überwunden werden können. Sie eignen sich auch für die Analyse der Austauschbeziehung zwischen Unternehmen und Verbraucherinnen und Verbrauchern in Fragen von

---

[342] Wesentlich ist das Konzept der sog. „Beschränkten Rationalität" (bounded rationality). Vgl. *Simon,* Rational Choice and the Structure of Environments, in: Psychological Review 1956, 123, abrufbar unter: https://pdfs.semanticscholar.org/23a9/4ce42fe0d50f5c993f34d4c9602f8aeac507.pdf. Grundlage verhaltensökonomischer Erklärungsansätze sind empirische und experimentelle Beobachtungen sowie spieltheoretische Experimente.

[343] Vgl. für einen Überblick z. B. *Terberger*, Neo-institutionalistische Ansätze, 1994, und *Richter/Furubotn*, Neue Institutionenökonomik, 1996. Die Neue Institutionenökonomik umfasst verschiedene theoretische Erklärungsansätze, die im Wesentlichen in vier Schulen unterteilt werden: Der Property-Rights-Ansatz oder Theorie der Verfügungsrechte, der Transaktionskostenansatz, der Prinzipal-Agent-Ansatz und informationsökonomische Ansätze, vgl. *Picot*, Ökonomische Theorien der Organisation – ein Überblick über neuere Ansätze und deren betriebswirtschaftliches Anwendungspotential, in: *Ordelheide/Rudolph/Büsselmann* [Hrsg.]: Betriebswirtschaftslehre und Ökonomische Theorie, 1991, S. 143, sowie *Kaas*, Marketing und Neue Institutionenökonomik, in: *Kaas* [Hrsg.]: Kontrakte, Geschäftsbeziehungen, Netzwerke – Marketing und Neue Institutionenökonomik, 1995, S. 1. Auch wenn die verschiedenen Ansätze unterschiedliche Aspekte einer Transaktionsbeziehung in den Blick nehmen, basieren sie auf gemeinsamen Grundannahmen über die Motivation der Wirtschaftssubjekte.

[344] Gerne zusammengefasst als Politikwechsel von „Viel hilft viel!" zu „Keep it simple!".

Datenschutz als Produkteigenschaft. Die **Annahmen zum menschlichen Verhalten**[345] erinnern dabei an aktuelle Tendenzen in der Forschung zum **Verbraucherleitbild**. Zuletzt ist ein eher differenziertes Verbraucherleitbild mit verantwortungsvollen, verletzlichen oder vertrauenden Verbraucherinnen und Verbrauchern[346] diskutiert worden.[347] Es erscheint insofern inzwischen weitgehend Einigkeit zu bestehen, dass Unterschiede zwischen den Verbraucherinnen und Verbrauchern, was ihre Wahrnehmung, Emotion und Motivation angeht, zu berücksichtigen sind.[348] Ausgangspunkt der neoinstitutionenökonomischen Analyse sind gerade individuelle Verhaltensweisen der

---

345 Im neoinstitutionenökonomischen Modell wird vom Menschenbild des rational gesteuerten Homo Oeconomicus Abstand genommen, welches Grundlage klassischer mikroökonomischer Erklärungsansätze ist. Stattdessen werden verhaltensrelevante Determinanten u. a. psychologischer und soziologischer Art sowie kulturelle und persönlichkeitsbedingte Einflüssen einbezogen, vgl. z. B. *Richter/Furubotn*, Neue Institutionenökonomik, 1996, oder *Aufderheide/Backhaus*, Institutionenökonomische Fundierung des Marketing: Der Geschäftstypenansatz, in *Kaas* [Hrsg.]: Kontrakte, Geschäftsbeziehungen, Netzwerke, 1995, S. 43.

346 Die europäische Rechtsprechung stellt bislang auf den mündigen oder durchschnittlich informierten, aufmerksamen und verständigen Durchschnittsverbraucher ab, vgl. EuGH, Urteil vom 16.07.1998, C-210/96, Slg. 1998, I-4657, Rn. 31 – *Gut Springenheide*. Die deutsche Rechtsprechung hat dies übernommen und zuletzt mit der „situationsadäquaten Aufmerksamkeit“ weiter präzisiert, vgl. etwa BGH, Urteil vom 20.10.1999, Az. I ZR 167/97, juris Rn. 20 – *Orient-Teppichmuster*.

347 Vgl. *Micklitz*, Der vertrauende, der verletzliche oder der verantwortungsvolle Verbraucher? Plädoyer für eine differenzierte Strategie in der Verbraucherpolitik, Stellungnahme des Wissenschaftlichen Beirats Verbraucher- und Ernährungspolitik beim BMELV, 2010, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/Strategie_verbraucherpolitik_Wiss_Beirat BMELV_2010.pdf sowie *Pagel***,** Das Verbraucherleitbild in der digitalen Welt, Impulsvortrag, o. Jg., Hochschule Mainz**,** abrufbar unter: https://mffjiv.rlp.de/fileadmin/MFFJIV/Verbraucherschutz/Digital-Dialog_Impulsvortrag_210317_SP.pdf und *Ernste*, Verbraucherschutz und Verhaltens-ökonomik. Zur Psychologie von Verhalten und Kontrolle, IW Analysen 106, 2016, abrufbar unter: https://www.iwkoeln.de/studien/iw-analysen/beitrag/dominik-enste-mara-ewers-christina-heldman-regina-schneider-verbraucherschutz-und-verhaltensoekonomik-291323.html.

348 Vgl. *Becker*, Bundeskartellamt und Verbraucherschutz, ZWeR, 2018, 229, 244; so auch BDI, Studie Verbraucherleitbild und Positionsbestimmung zum mündigen Verbraucher, 2014, abrufbar unter: https://bdi.eu/media/publikationen/?publicationtype=Studien#.

Wirtschaftssubjekte bei Unsicherheit.[349] Auch die weiteren Annahmen entsprechen in ihren Grundzügen typischen beobachtbaren Verhaltensweisen der Nutzerinnen und Nutzer im Umgang mit Messenger- und Video-Diensten: Es wird Nutzenmaximierung angestrebt, aber nur eingeschränkt rational gehandelt. Die Kapazitäten der Verbraucherinnen und Verbraucher für die Informationsaufnahme sind beschränkt und (Datenschutz-) Risiken werden nicht einheitlich bewertet. Schließlich wird vorausgesetzt, dass Wirtschaftssubjekte – d. h. alle Marktteilnehmer, einschließlich Verbrauchern und Diensten – immer ihrem Eigeninteresse folgen, auch wenn dies zu Lasten ihrer Vertragspartner geht.[350] Vor diesem Hintergrund werden verschiedene Ausprägungen von **Informationsasymmetrien** analysiert, mit denen Verbraucherinnen und Verbraucher bei der Entscheidung für einen oder mehrere Messenger- und Video-Dienste umgehen müssen. In informationsökonomischen Ansätzen werden grundlegende Mechanismen vorgeschlagen, um Informationsnachteile zu mildern und Risiken zu reduzieren.
Neben der Qualitätsunsicherheit sind für die Verbraucher **zwei weitere Ausprägungen von Informationsasymmetrien** in Datenschutzfragen relevant, wenn sie Verträge mit Diensten schließen. Eine asymmetrische Informationsverteilung kann Ursprung von Konflikten sein, wenn der besser informierte Vertragspartner nach Vertragsschluss seinen Informationsvorsprung zu seinen eigenen Gunsten ausnutzt.[351] So können die Verbraucherinnen und Verbraucher die **Fairness des Dienstes nach eingegangener Vertragsbeziehung** vor und nach Vertragsabschluss nicht beurteilen oder abschätzen. Für die Analyse wird zwischen der Vertragspartei, die als „Prinzipal“ Aufgaben vergibt und bessere Informationen über das Kooperationsziel hat und nicht geschädigt werden will, und dem “Agenten“, der bessere Informationen über Gegenstand und Aufgabe besitzt, unterschieden.[352] Übertragen auf einen

---

[349] Es wird vom methodologischen Individualismus ausgegangen. Vgl. *Richter*, Sichtweise und Fragestellungen der Neuen Institutionenökonomik, in: Zeitschrift für Wirtschafts- und Sozialwissenschaften, 1990, 571, 573.

[350] Vgl. *Williamson*, Die ökonomischen Institutionen des Kapitalismus, 1990, S. 54.

[351] Opportunistisches Verhalten wird auch in einer einschlägigen BDI-Studie thematisiert, vgl. *BDI*, Verbraucherleitbild und Positionsbestimmung zum “Mündigen Verbraucher“, 2014, S. 14, abrufbar unter: https://bdi.eu/media/presse/publikationen/gesellschaft-verantwortung-und-verbraucher/BDI_Studie_zum_muendigem_Verbraucher.pdf.

[352] Diese Überlegungen sind Grundlage des sog. Prinzipal-Agent-Ansatzes, der sich ursprünglich auf Vertragsverhältnisse auf der gleichen Marktseite bezieht, aber auch für die Analyse anderer Vertragsverhältnisse genutzt werden kann. Vgl. für einen Überblick über den Prinzipal-Agent-Ansatz z.B. *Richter/Furubotn*, Neue Institutionenökonomik, 1996. *Matten* hat den Prinzipal-Agent-Ansatz genutzt, um das Verhältnis zwischen Unternehmen und Stakeholdern zu untersuchen, vgl. *Matten*, Management ökologischer Unternehmensrisiken, 1998, S. 198.

Vertragsabschluss zwischen Anbietern und Verbrauchern käme den Verbraucherinnen und Verbrauchern die Rolle des Prinzipals zu, während die Anbieter von Messaging- und Videoconferencing-Funktionen als Agenten agieren. Verletzt beispielsweise ein Dienst die Datenschutzrechte der Nutzerinnen oder Nutzer nach Vertragsschluss, was diesen nachträglich bekannt wird, so hatte er **verborgene Absichten** (sog. *Hidden Intention* oder *Hold-up*). Der Verbraucherin und dem Verbraucher entgeht Nutzen, wenn ihre und seine Investition in die Verwendung des Dienstes durch die Rechtsverletzung wertlos wird oder an Wert verliert.

Im Fall von **verborgenen Handlungen** (sog. *Hidden Action* mit *Moral Hazard*) bleibt der Verbraucherin oder dem Verbraucher (Auftraggeber) die Verletzung von Datenschutzrechten durch den Dienstanbieter (Agenten) vollständig unbekannt oder wird erst nach einiger Zeit deutlich. Von *Moral Hazard* könnte auch dann gesprochen werden, wenn Dienste beispielsweise mehr Daten der Verbraucherinnen und Verbraucher erfassen und verwerten würden als in den Datenschutzbestimmungen des Dienstes angegeben wird und die Verbraucherin oder der Verbraucher dies gar nicht oder viel zu spät entdeckt. Verbraucherinnen und Verbraucher könnten aufgrund dieser Risiken vor Vertragsabschlüssen zurückschrecken. Agenten (hier: Messenger- und Video-Dienste) können dem durch eine zielgerichtete **Risikokommunikation** begegnen. Kommuniziert werden können grundsätzlich alle Maßnahmen, die die Autorität der Verbraucherinnen und Verbraucher als Prinzipal erhöhen und die Sorge vor opportunistischem Verhalten mildern.[353]

Sofern Maßnahmen ergriffen werden, die die Informationsnachteile der Verbraucherinnen und Verbraucher senken, könnten diese zu mehr Eigeninitiative ermutigt werden. Datenschutzfreundliche Dienste hätten dann eine bessere Chance, wahrgenommen und ausgewählt zu werden. Dies wird aber nur dann gelingen, wenn das Bewusstsein der Verbraucherinnen und Verbraucher für den Schutz ihrer Daten geschärft werden kann. Die Datenschutzqualität von Messenger- und Video-Diensten muss aus ihrem Schattendasein heraustreten und sichtbar werden. Hier müssen weitere Maßnahmen unterstützend ansetzen.

c) Konsequenzen für die Verbraucherpolitik

Vereinfachend formuliert sind Maßnahmen zum Schutz der Verbraucherinnen und Verbraucher aus informationsökonomischer Sicht immer dann gerechtfertigt, wenn diese bestehenden Informationsasymmetrien ausgesetzt sind. Dies muss nicht zwangsläufig in staatlichen Maßnahmen

---

[353] Vgl. für eine praktische Anwendung der Erklärungsansätze zur Risikokommunikation *Matten*, Management ökologischer Unternehmensrisiken, 1998, S. 203. Bei moralischen Risiken in einzelwirtschaftlichen individuellen Vertragsbeziehungen auf der gleichen Marktseite können auch Anreiz- und Belohnungssysteme risikomindernd eingesetzt werden.

münden. Vielmehr werden marktliche Lösungen durchaus für geeignet gehalten, die Probleme von Adverser Selektion und Moral Hazard zu lösen. Auch das Bundeskartellamt bevorzugt grundsätzlich marktbezogene Lösungen, um Rechtsdurchsetzungsdefizite bzw. verbraucherrechtliche Schutzlücken zu schließen und um dem Datenschutz zu mehr Breitenwirkung zu verhelfen. Hierzu zählen zunächst Instrumente, die die Kosten der Informationssuche reduzieren und den Informationsstand der Verbraucherinnen und Verbraucher verbessern.[354] Inwieweit es gelingt, **Datenschutzqualität als Wettbewerbsparameter** voranzubringen, hängt also maßgeblich von der subjektiven Wahrnehmung der Verbraucherinnen und Verbraucher ab. Sie ist es letztendlich, die die Art und das Ausmaß der Informationsaufnahme und die Aktivitäten zur Informationssuche bestimmt.[355]

Wie oben gezeigt, sind die Probleme der asymmetrischen Informationsverteilung aber offenbar nicht allein dafür verantwortlich, dass Verbraucherinnen und Verbraucher Datenschutz bisher nur sehr eingeschränkt als Wettbewerbsparameter wahrnehmen. Wenn die Verbraucherinnen und Verbraucher **kein besonderes Interesse** daran haben, dass die Qualität eines Produktes oder einer Dienstleistung verbessert wird, lösen mehr Informationen oder einfacher auffindbare Informationen keine Verhaltensänderungen aus und das Marktergebnis verbessert sich nicht. Marktbezogene Maßnahmen, wie z. B. die Einführung von Informationspflichten oder Qualitätssiegeln führen dann nicht zum Erfolg. Was **Datenschutz als Qualitätseigenschaft** angeht, ist bisher ist nicht ersichtlich, dass viele Verbraucherinnen und Verbraucher die Auswahl ihres Messenger- und Video-Dienstes nach der Datenschutzfreundlichkeit richten. Wenn sie es doch versuchen, müssen sie mit sehr ungleich verteilten Informationen - zugunsten der Dienste, zu ihren Lasten - zurechtkommen. In einer technisch basierten

---

[354] Vgl. *Döring*, Verbraucherschutz aus Sicht der Informationsökonomik – Rechtfertigung, Maßnahmen und Erweiterungsbedarf, sofia-Diskussionsbeiträge, 2021, abrufbar unter: https://www.sofia-darmstadt.de/veroeffentlichungen/sofia-diskussionsbeitraege/sofia-dis-2021-4-doering. Aus wissenschaftlicher (insb. informationsökonomischer) Sicht könnten dies z. B. Informationspflichten für Anbieter, das Aufheben von Informationsbeschränkungen, die Definition von Standards oder das Verbot irreführender Information sein. Zulassungsbeschränkungen und ähnliche Maßnahmen werden gegenüber Informationspflichten kritischer betrachtet. Dies ist nicht der Fall, wenn Informationspflichten unbrauchbar sind, da sich deren Adressaten nicht für die Information interessieren oder zusätzliche Informationen die Informationsasymmetrien nicht ausgleichen können, wie es bei Vertrauensgütern – hier Datenschutz – zutrifft. Siehe z. B. *Sinn*, Verbraucherschutz als Staatsaufgabe, in: Perspektiven der Wirtschaftspolitik, 2003, Jg.4, S. 281 – 294, abrufbar unter: https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-2516.t01-2-00009m. Wenn diese Maßnahmen nicht ausreichen, kann ein eigenes staatliches Informationsangebot gerechtfertigt sein.

[355] Vgl. *Matten*, Management ökologischer Unternehmensrisiken, 1998, S. 203.

Branche ist es sogar noch komplizierter: Die Verbraucherinnen und Verbraucher müssten zunächst herausfinden, welche Informationen überhaupt relevant sind, dann diese suchen, sich ein grundlegendes Verständnis erarbeiten und abschließend aus mehreren Kriterien noch ein Gesamturteil bilden und vergleichen.

Die Messenger- und Video-Dienste als Anbieter von Messaging- und Videoconferencing-Leistungen verspüren dadurch **wenig Druck**, besseren Informationen zur Datenschutzpraxis ihres Dienstes eine höhere Priorität einzuräumen und sich zu bemühen, den Verbraucherinnen und Verbrauchern eine informierte Entscheidung zu ermöglichen. Im Zuge aktueller Entwicklungen treten weitere Herausforderungen hinzu: Die Interoperabilitätsregeln im DMA werden die Datensicherheit und damit den Datenschutz vor weitere Herausforderungen stellen. Die Dienste sind technisch unterschiedlich aufgestellt. Viele bekannte Dienste sind als geschlossenes System gestaltet worden. Die Daten aller Beteiligter können somit neuen Risiken ausgesetzt sein, wenn Interoperabilität eingeführt wird. Gleichzeitig kann die Informationslage für die Verbraucherinnen und Verbraucher noch undurchschaubarer werden.

Daher könnten nach derzeitiger Auffassung des Bundeskartellamts rein marktbezogene Maßnahmen nicht ausreichend sein, um Datenschutz als Wettbewerbsparameter zu etablieren. Staatliches Eingreifen kann dann eine Option darstellen, die geprüft werden muss. Das Bundeskartellamt greift den Vorschlag eines Branchenvertreters auf, der ein **Rating** in staatlicher Verantwortung vorgeschlagen hat, um nicht nur die ungleiche Informationsverteilung abzubauen, sondern sowohl die Messenger- und Video-Dienste als auch die Nutzerinnen und Nutzer in Sachen Datenschutz zu aktivieren.

Allerdings können sich die Probleme asymmetrischer Informationsverteilung auf die Beziehung zwischen **Verbraucherinnen und Verbrauchern und dem Intermediär** verlagern, wenn Informationsintermediäre wie Ratingagenturen in Anspruch genommen werden. Auch inwieweit die Ratingnote ein tatsächliches Qualitätsurteil ist, können die Nachfragerinnen und Nachfrager kaum unmittelbar bewerten. Das Rating muss so konzipiert sein, dass diese neuen Informationsprobleme minimiert werden und das Ziel, Datenschutz als Wettbewerbsparameter voranzubringen, bestmöglich umgesetzt wird.

III. Datenschutzqualität vergleichend und transparent bewerten

Im Folgenden werden zunächst Hintergrund und Begriff des Rating eingeführt und die grundsätzlichen Anforderungen für eine Übertragung auf den Datenschutzbereich dargelegt (dazu unter 1.). Dann wird untersucht, inwieweit es in Verbraucherrecht und -politik Anknüpfungspunkte für ein derartiges Informationsinstrument gibt (dazu unter **Fehler! Verweisquelle konnte nicht gefunden werden.**). A nschließend werden Vor- und Nachteile aus institutionenökonomischer Sicht skizziert (dazu unter 3.). Vor diesem Hintergrund werden konkrete Überlegungen zu einem Datenschutz-Rating formuliert und zu den Erkenntnissen aus den Ermittlungen in Verbindung gesetzt (dazu unter 4.).

1. Hintergrund und wesentliche Charakteristika

Der Begriff des „Rating“ ist insbesondere aus der Kreditwirtschaft bekannt. Dort handelt es sich dabei um eine Beurteilung der wirtschaftlichen Lage und der Bonität von Unternehmen, Institutionen oder Staaten. Unternehmen, die an einem Rating-Verfahren teilnehmen, werden anhand einer ordinalen Skala in eine Bonitätsstufe oder Rating-Klasse eingeordnet.

Wesentlicher Teil des Ratingverfahren ist das sog. **Scoring-Modell**. Dabei werden - ganz allgemein formuliert - statistische Methoden eingesetzt, um Eintrittswahrscheinlichkeiten für bestimmte (Schadens-)Ereignisse zu ermitteln mit dem Ziel, die Risiken aus bestehenden Informationsasymmetrien zu minimieren. Die Score-Werte – die in Rating-Noten bzw. -Klassen überführt werden – werden entsprechend **qualitativer und quantitativer Beurteilungskriterien** berechnet. So werden für ein Kreditrating beispielsweise einerseits Liquidität, Kapitalstruktur etc. untersucht, andererseits auch externe Einflussfaktoren, die sich aus Besonderheiten der Branche oder dem Länderrisiko ergeben. Diese Beurteilungskriterien werden mit Punktwerten versehen, gewichtet und summiert. Ergebnis ist eine Einschätzung der Ausfallwahrscheinlichkeit, die meist mit einer Buchstaben- und/oder Ziffernfolge dargestellt und veröffentlicht wird.[356]

Scoring-Modelle werden nicht nur von Unternehmen eingesetzt, beispielsweise für die Bewertung von Kunden, Vertriebsgebieten oder Produkten. Auch Online-Händler und Banken oder Versicherungen bewerten die Bonität ihrer Kundinnen und Kunden. Sie erhalten die Score-Werte für ihre (potenziellen) Kunden dabei häufig von darauf spezialisierten Unternehmen, den sog. Wirtschaftsauskunfteien. Gleichzeitig erstellen sie teilweise jedoch auch eigene Score-Werte aufgrund früherer Transaktionen der Kundinnen und Kunden und geben deren Daten an andere Unternehmen weiter.[357]

---

[356] Vgl. z. B. *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Rating; *Finanzen.net*, abrufbar unter: https://www.finanzen.net/wirtschaftslexikon/rating, *SpringerGabler*, abrufbar unter: https://www.gabler-banklexikon.de/definition/rating-60805, *Bundeszentralle für politische Bildung*, abrufbar unter: https://www.bpb.de/kurz-knapp/lexika/lexikon-der-wirtschaft/20479/rating/.

[357] Dieses Thema ist Gegenstand der Sektoruntersuchung „Scoring beim Online-Shopping“, die das *Bundeskartellamt* im März 2022 eingeleitet hat, vgl. https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Pressemitteilungen/2022/31_03_2022_SU_Scoring.pdf?__blob=publicationFile&v=5. Untersucht wird, ob sich Online-Händler bei der Durchführung der Bonitätsprüfungen an die daten- und verbraucherschutzrechtlichen Rahmenbedingungen halten. So soll beispielsweise der Frage nachgegangen werden, ob und wie Online-Händler die Erlaubnis zur Durchführung von Bonitätsprüfungen von den Bestellenden einholen.

Auch die Ratingverfahren für das Bonitätsrisiko werden sowohl von Banken für bankeninterne Bonitätsbeurteilungen als auch von unabhängigen Ratingagenturen durchgeführt. Die bekanntesten privaten Ratingagenturen für die Kreditwirtschaft sind Standard and Poor's[358], Moody's[359] und Fitch[360]. Die Ratingagenturen geben mit den Ratings keine Investitionsempfehlungen ab, sondern liefern ausschließlich eine Einschätzung des Ausfallrisikos.

Über das zugrundeliegende Scoring-Modell hinaus zeichnet sich ein Rating durch folgende **wesentliche Merkmale** aus. Zunächst ist ein Ziel zu formulieren. Übertragen auf den Bereich des Datenschutzes wäre dies **ausschließlich die Einschätzung des Datenschutzrisikos**[361] eines Messenger- und Video-Dienstes. Andere Kriterien, wie z. B. die Erreichbarkeit aufgrund der Nutzerbasis oder neue Funktionen im Sinne des Nutzererlebnisses, bleiben außen vor. Notwendig ist des Weiteren eine **Ratinginstanz**, die für das Verfahren verantwortlich ist und die die Ergebnisse veröffentlicht. Dabei kann es sich grundsätzlich sowohl um private Unternehmen als auch eine Behörde handeln. Notwendig ist allerdings ein gewisser Bekanntheitsgrad und eine **Reputation**, die Vertrauenswürdigkeit und Kompetenz verspricht, um bei den Marktteilnehmenden die notwendige Akzeptanz zu erreichen. Die Instanz sollte ferner unabhängig sein, in dem Sinne, dass es nicht zur Vermischung mit anderen Aufgaben in der Branche kommt.

Wie eben beschrieben, ist die Zusammenstellung von **Kriterien**, die den Score-Wert bilden einschließlich ggf. einer Gewichtung und Bezeichnung (z. B. AAA im Kreditbereich), Klassenbildung der Skala und Ranking wesentlicher Kern des Ratings. Das Rating muss anschließend **veröffentlicht** werden. Es muss eine **regelmäßige und ggf. anlassbezogene Neubewertung** stattfinden, da die Entwicklungsgeschwindigkeit der Branche hoch und entsprechende Veränderungen bei den Diensten zu erwarten sind. In ein Rating sollten idealerweise alle in Deutschland oder Europa tätigen Messenger- und Video-Dienste einbezogen werden, um **flächendeckend** ein hohes Datenschutzniveau zu erreichen. Möglicherweise muss in diesem Zusammenhang entschieden werden, ob die Teilnahme am Rating-Verfahren freiwillig oder verpflichtend sein soll.

---

[358] Vgl. *S&P Global*, abrufbar unter: https://www.spglobal.com/ratings/en/.

[359] Vgl. *Moody's*, abrufbar unter: https://www.moodys.com/.

[360] Vgl. *Fitch Ratings*, *Inc*., abrufbar unter: https://www.fitchratings.com/.

[361] Innerhalb eines solchen Rating-Verfahrens stellt sich das Datenschutzrisiko insgesamt als messbares graduelles Qualitätsmerkmal dar, dass sich aus den gewichteten Bewertungen von Einzelkriterien ergibt. Bei einzelnen dieser Kriterien mag ebenfalls ein gradueller Maßstab sinnvoll sein, beispielsweise bei der Umsetzung der Ende-zu-Ende-Verschlüsselung. Bei anderen Kriterien, wie z. B. der Datenspeicherung, scheint entsprechend der rechtlichen Voraussetzungen nur die Option "Verstoß" oder "Erfüllung der rechtlichen Anforderungen" denkbar, die mit einer geeigneten Bewertung in das Scoring-Modell eingeht.

2. Anknüpfungspunkte für ein Informationsinstrument im Verbraucherschutz

Sowohl in Deutschland als auch international hat sich nach bisheriger Kenntnis des Bundeskartellamts bisher kein Rating für das Datenschutzrisiko etabliert.

Einzelne Elemente eines Rating-Modells werden für den Lebensmittelbereich im sog. **Nutri-Score** umgesetzt, bei dem es sich um ein Scoring-Modell mit Bildsymbol handelt. Das Kennzeichen wurde von unabhängigen Wissenschaftlerinnen und Wissenschaftlern entworfen. Es soll den Verbraucherinnen und Verbrauchern dazu dienen, auf einen Blick beispielsweise zu erkennen, welches von zwei Müslis die gesündere Wahl ist. Dazu gibt der **Nutri-Score** anhand einer 5-stufigen Farbskala von A bis E Auskunft über den Nährwert eines Lebensmittels. Der Energiegehalt und die Gehalte ernährungsphysiologisch günstiger und ungünstiger Nährstoffe werden miteinander verrechnet und der Skala zugeordnet – von A (dunkelgrün) über C (gelb) bis E (rot). Die Farben Grün bis Rot helfen bei der Orientierung: Ein grünes A trägt eher zu einer gesunden Ernährung bei als ein rotes E.[362]

Interessierte Lebensmittelunternehmen können den Nutri-Score kostenfrei nutzen. Sie müssen sich lediglich bei der französischen Markeninhaberin, der "Santé publique France", einer Behörde im Geschäftsbereich des französischen Gesundheitsministeriums, anmelden und den Nutzungsvereinbarungen zustimmen. Unternehmen und ihre Marke(n), die mit dem Nutri-Score gekennzeichnet werden sollen, registrieren sich auf einem Onlineportal. Der Nutri-Score ist eine freiwillige Angabe auf der Vorderseite eines Lebensmittels. Er ergänzt die bereits bestehenden Pflichtkennzeichnungselemente, vor allem die Nährwerttabelle. Die Verwendung von erweiterten Nährwertkennzeichnungsmodellen, zu diesen zählt der Nutri-Score, ist **EU-weit einheitlich** geregelt. Das geltende EU-Recht sieht für die Verwendung von erweiterten Nährwertkennzeichnungen auf nationaler Ebene keine verpflichtende, sondern nur die freiwillige Anwendung vor.

Nicht nur im Lebensmittelbereich, sondern auch für verschiedene kriteriengeleitete Bewertungen von Messenger- und Video-Diensten sind Scoring-Modelle bereits verwendet worden. So sind die **jüngsten Veröffentlichungen zu Messenger- und Video-Diensten** nicht mit einem Rating wie im vorausgegangenen Kapitel beschrieben zu verwechseln. Das Anfang des Jahres 2022 von der Stiftung

---

[362] Als günstig eingestuft werden zum Beispiel die Gehalte an Ballaststoffen und Eiweiß sowie der Gehalt an Gemüse, Obst, Nüssen, Hülsenfrüchten und ausgewählten Speiseölen. Als ungünstig gehen die Energie und der Gehalt an gesättigten Fettsäuren, Salz und Zucker in die Bewertung ein. *Bundesministerium für Ernährung und Landwirtschaft*, Nutri-Score, abrufbar unter: https://www.bmel.de/DE/themen/ernaehrung/lebensmittel-kennzeichnung/freiwillige-angaben-und-label/nutri-score/nutri-score_node.html.

Warentest durchgeführte Testverfahren[363] und auch die im Sommer 2021 vom Hongkonger Verbraucherrat[364] veröffentlichten Messenger-Untersuchungen entsprechen eher Studien, stellen jeweils eine Momentaufnahme dar und urteilen zum größten Teil nach anderen als den in dieser Sektoruntersuchung untersuchten technischen Kriterien.

Die **Stiftung Warentest** stellte Funktionen und Anwenderfreundlichkeit in den Mittelpunkt ihrer Untersuchung, auch wenn einzelne Sicherheitskriterien, wie z. B. die Verschlüsselung und wesentliche Dokumente wie die Datenschutzerklärung ebenfalls bewertet wurden, aber mit geringerer Gewichtung.[365] Der Kreis der Teilnehmenden war begrenzt und von der Stiftung Warentest selbst ausgewählt. Es handelt sich ferner um eine einmalige Studie, die nicht regelmäßig oder anlassbezogen wiederholt wird. Die Untersuchung des **Hongkonger Consumer Council** (Verbraucherschutzbehörde) war ähnlich ausgerichtet. Die Behörde hat im Sommer 2021 laut Internetinformationen einen Bericht veröffentlicht, in dem die Funktionen und der Datenschutz von dreizehn Instant-Messaging-Apps untersucht wurden. Kriterien waren u.a. die Benutzerfreundlichkeit beim Einrichten von Konten, die Anrufqualität, die Benutzeroberfläche, die Vertraulichkeit von Informationen und die Gruppenfunktionen. Der Verbraucherrat gab die Ergebnisse in seinem Magazin *„CHOICE“ bekannt.* Auf den Webseiten des Verbraucherrats sind Informationen aus dem Choice-Journal nur in chinesischer Sprache erhältlich, daher konnte eine nähere Analyse nicht durchgeführt werden. Das gute Abschneiden

---

[363] Siehe *Stiftung Warentest*, Messenger-Apps im Vergleich, Februar 2022, abrufbar unter: https://www.test.de/Messenger-Apps-im-Vergleich-4884453-0/, Stand: 11. Mai 2022. Die Stiftung Warentest hat in den Bereichen “Funktionen”, “Einrichtung und Nutzung” und “Schutz der Privatsphäre” geprüft und die Bereiche mit 35%, 35% und 30% gewichtet.

[364] Es wurden 13 „Instant-Messaging-Apps“ untersucht, darunter Discord, Facebook Messenger, Google Chat, Kik, LINE, Olvid, Signal, Skype, Telegram, Threema, Viber, WeChat und WhatsApp. Die Studie besagte, dass LINE, Olvid, Threema und Signal in Bezug auf den Datenschutz die höchste Punktzahl (5 von 5) in der Kategorie Vertraulichkeit beim Senden von Informationen aufweisen. Unterdessen betrug die Punktzahl von WhatsApp 4,5 von 5, vgl. *Consumer Council*, abrufbar unter: https://www.marketing-interactive.com/consumer-council-line-and-signal-offers-highest-level-of-privacy-when-sending-data. Auf den Webseiten des Verbraucherrats sind Informationen aus dem Choice-Journal nur in chinesischer Sprache erhältlich, vgl. *Consumer*, abrufbar unter: https://www.consumer.org.hk/en/choice-magazine.

[365] Alle Untersuchungen fanden zwischen November 2021 und Januar 2022 statt. Die Prüfung der Funktionen ging mit 35 Prozent, Einrichtung und Nutzung ebenfalls mit 35 Prozent und Schutz der Privatsphäre mit 30 Prozent in das Ergebnis ein, vgl. Stiftung Warentest, Messenger - Apps im Vergleich – so haben wir getestet, abrufbar unter. https://www.test.de/Messenger-Apps-im-Vergleich-4884453-4884455/.

von insbesondere bei Verbraucherinnen und Verbrauchern beliebten, führenden Messenger-Diensten lässt vermuten, dass die zugrunde liegenden Kriterien nicht dem entsprachen, was das Bundeskartellamt für notwendig erachtet.

Das Verbraucherrecht bietet bisher keinen **rechtlichen Rahmen** für ein Rating, es ist bisher zumindest nicht explizit vorgesehen. Datenschutz- und Lauterkeitsrecht verpflichten lediglich zu geschäftlicher Transparenz. Die DSGVO enthält zumindest einen Anknüpfungspunkt, der näher in Augenschein genommen werden kann. So ist der freiwillige Einsatz von Datenschutzzertifikaten und standardisierten Bildsymbolen vorgesehen (Art. 42, 43 DSGVO), um die DSGVO-Konformität von Datenverarbeitungsvorgängen zu belegen. Konkret handelt es sich hierbei um einen Nachweis, dass die Pflichten zur Umsetzung geeigneter technischer und organisatorischer Maßnahmen gem. Art. 24 Abs. 1,3; Art. 25; Art. 32 Abs. 1,3 DSGVO sowie hinreichender Garantien i. S. d. Art. 28 Abs. 1,4 DSGVO, vgl. Rn. 12 erfüllt werden.[366] In Deutschland werden die Zertifizierungsstellen lt. Internetinformationen nun von der Deutschen Akkreditierungsstelle GmbH (DAkkS) zusammen mit den unabhängigen Datenschutzaufsichtsbehörden gemäß § 39 Bundesdatenschutzgesetz akkreditiert.[367]

Den Anforderungen eines Ratings dürfte dieses Verfahren nach Art. 42 DSGVO aus mehreren Gründen nicht entsprechen, auch wenn es Anknüpfungspunkte gibt. Unbekannte Unternehmen, die sich als Zertifizierer akkreditieren lassen, verfügen nicht über die notwendige **Reputation**, um Messenger- und Video-Dienste, von denen viele mit global führenden Konzernen verbunden sind, zur Teilnahme an einem Datenschutz-Rating zu veranlassen. Fraglich ist ferner, ob und inwieweit die DSGVO-Zertifizierung wegen des Bezugs auf die **technischen und organisatorischen Maßnahmen** für ein Rating von Messenger- und Video-Diensten geeignet ist. Zwar scheint der Gesamtzusammenhang die Sicherheitskriterien bei Messenger- und Video-Diensten einzufangen. Schließlich nennt die DSGVO hier „Pseudonymisierung“, „Verschlüsselung“, „Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit“ der Systeme der Datenverarbeitung sowie die „Wiederherstellbarkeit der Verfügbarkeit und des Zugangs nach einem Zwischenfall“, was eine gewisse Nähe zu den gewünschten Ratingkriterien, wie z. B. Einsehbarkeit des Quellcodes, Ende-zu-Ende-Verschlüsselung, Zwei-Faktor-Authentisierung und Standort Server entfaltet. Unterschiede liegen aber in der Interpretation, wie es am Beispiel

---

366 Ferner können Aufsichtsbehörden gemäß Artikel 63 und Artikel 70 Absatz 1 beim EDSA Kriterien für ein EU-weites Zertifizierungsverfahren nach Artikel 42 Absatz 5 zur Genehmigung einreichen. Ein aktuelles Problem ist aber die Übermittlung personenbezogener Daten in Drittstaaten, bei denen kein Angemessenheitsbeschluss vorliegt.

367 Vgl. *datenschutz notizen*, abrufbar unter: https://www.datenschutz-notizen.de/es-geht-voran-1-erfolge-auf-dem-langen-weg-zur-akkreditierung-nach-art-42-dsgvo-4227814/.

„Verschlüsselung“ offenbar wird. So ist hier in der DSGVO das Risiko angesprochen, Daten-Missbrauch im Sinne einer Entwendung der Daten, zu reduzieren. Verschlüsselung soll personenbezogene Daten für alle unbefugten Personen unzugänglich machen, wie es z. B. bei einer Festplatten- und Dateiverschlüsselung mit symmetrischen Verfahren geschieht. Asymmetrische Verschlüsselungsverfahren, wie sie bei der Ende-zu-Ende-Verschlüsselung eingesetzt werden, die den bilateralen Datenaustausch schützen sollen, sind ausdrücklich nicht gemeint.[368]

Demgegenüber sind die in der DSGVO genannten **Abwägungsfaktoren - Stand der Technik und Implementierungskosten** – auch in der Branche der Messenger- und Video-Dienste wichtige Aspekte, die gerade bei der Bewertung von Interoperabilitätsvorhaben relevant sind (vgl. Kapitel F.IV). Generell existiert bisher **kein expliziter Katalog für die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO**, so dass sich hier Spielräume ergeben könnten. Vielmehr kennt die Praxis der IT-Sicherheit verschiedene Maßnahmenkataloge, wie z. B. die BSI-Standards, die ISO/IEC 27001-Normen oder die Common Criteria, die alle keinen speziellen Fokus auf rechtlichen Datenschutzanforderungen haben.[369]

Bevor auf konkrete Überlegungen zu einer Einschätzung des Datenschutzrisikos eingegangen wird, sollen zunächst die Vor- und Nachteile des Rating aus wissenschaftlicher Sicht kurz in Grundzügen beleuchtet werden, um Hinweise für eine risikominimierende Gestaltung zu gewinnen.

3. Chancen und Risiken aus wissenschaftlicher Sicht

Aus wissenschaftlicher Perspektive sind Ratingagenturen als Intermediäre tätig, die Informationen zusammenstellen und in eine Bewertung überführen, die Dritten - hier den Verbraucherinnen und Verbrauchern - zur Verfügung gestellt wird (dazu unter a)), damit diese sich zielgerichteter, kostengünstiger und mit weniger Risiko informieren können. Auf diese Weise entstehen neue Beziehungen zwischen Verbraucherinnen und Verbrauchern, Intermediär und den zu bewertenden Diensten. Diese können insbesondere dem Intermediär und ggf. den Diensten Gelegenheit zu opportunistischem Verhalten geben, dem aber mit dem Reputationsmechanismus vorgebeugt werden kann (dazu unter b). In der nachfolgenden Darstellung stehen die **neuen Informationsbeziehungen und ihre risikominimierende Handhabung** im Vordergrund. Zu deren besserem Verständnis geschieht die Analyse zunächst unter der Voraussetzung der Tätigkeit einer Ratinginstanz und nicht mehrerer aktiver

---

[368] Vgl. *Simitis, Spiros, Hornung, Gerrit, Döhmann, Indra*, Kommentar zum Datenschutzrecht, Artikel 32, Rn 35, Baden Baden 2019.

[369] Vgl. *Simitis, Spiros; Hornung, Gerrit; Döhmann, Indra*; Kommentar zum Datenschutzrecht, Artikel 32, Rn 78, Baden Baden 2019.

Ratingagenturen. Dies erscheint aufgrund der Besonderheiten des Datenschutzrisikos auch näherliegend, was unter c) beschrieben wird.

a) Informationsgefälle mildern

Ein Rating könnte den Verbraucherinnen und Verbrauchern helfen, ihren Informationsstand zu verbessern, wenn die Dienste es als **Signaling-Instrument** nutzen. Ein Signal ist aus informatorischer Sicht vorteilhaft, wenn das interessierende Merkmal – hier die Datenschutzfreundlichkeit – schwer beobachtet werden kann, das Signal – hier das Rating – dagegen leicht. Letzteres erfordert z. B., dass das Rating veröffentlicht und regelmäßig aktualisiert wird.
Das Rating als Signal gewährleistet eine negative Korrelation zwischen Datenschutzrisiko und Erzeugungskosten des Rating, wie Gebühren, Aufwand für Informationszusammenstellung und Prüfung. Hat ein Dienst ein im Vergleich hohes Datenschutzrisiko, erhält er eine schlechte Note und muss mit Reaktionen seiner Stakeholder rechnen (Beschwerden, Abwanderungen, geringerem Umsatz, ggf. höheren Kapitalkosten), insb. wenn es sich um ein börsennotiertes Unternehmen oder um ein mit einem börsennotierten Konzern verbundenen Dienst handelt, bei denen jegliche Nachrichten eingepreist werden und die Erwartungen der Börsenteilnehmenden eine große Rolle spielen. Folglich dürften Dienste mit hohem Datenschutzrisiko weniger Anreize sehen, ein Rating durchzuführen und zusätzlich zu den Ratinggebühren die negativen Auswirkungen in Kauf zu nehmen. Für die Verbraucherinnen und Verbraucher heißt dies, dass sie von einem existierenden und besseren Rating auf ein geringes Datenschutzrisiko schließen könnten. Die bei Informationsasymmetrien bestehende Negativauswahl - soweit es keine zusätzlichen Informationen gibt, nehmen Verbraucherinnen und Verbraucher alle angebotenen Produkte als weitgehend identisch und durchschnittlich wahr - kann in eine Positivauswahl überführt werden. Für anbietende Dienste kann es sich lohnen, Qualitätsunterschiede offen zu legen, damit sie wahrgenommen werden. Die aus der asymmetrischen Informationsverteilung resultierenden Probleme adverser Selektion - es wird nur eine durchschnittliche Qualität am Markt wahrgenommen - können folglich durch Signale gemildert werden.[370]

[370] Vgl. für den Kreditbereich *Schaetzle* (2011), Ökonomische Funktionen von Ratingagenturen, Working Paper, Westfälische Wilhelms-Universität Münster, abrufbar unter: https://www.econstor.eu/handle/10419/55765 und die dort angegebene Literatur sowie auch Vgl. *Döring*, Verbraucherschutz aus Sicht der Informationsökonomik – Rechtfertigung, Maßnahmen und Erweiterungsbedarf, sofia-Diskussionsbeiträge, 2021, abrufbar unter: https://www.sofia-darmstadt.de/veroeffentlichungen/sofia-diskussionsbeitraege/sofia-dis-2021-4-doering.

Rating kann auch im Rahmen des **Screening-Ansatzes** verwendet werden. Die Rating-Instanz übernimmt für die Verbraucherinnen und Verbraucher die Suche und Beurteilung von Informationen über die Messenger- und Video-Dienste, womit Qualitäts- und Kostenvorteile gegenüber vielen einzelwirtschaftlichen Suchprozessen verbunden werden. Dass Verbraucherinnen und Verbraucher das Rating als Screening-Indikator nutzen, ist an verschiedene Voraussetzungen gebunden: Das Rating muss beobachtbar und standardisiert sein, aber auch differenziert genug gestaltet sein, z.B. über Kategorien, um als aussagekräftig erachtet zu werden.[371] Vor allem aber müssen die Verbraucherinnen und Verbraucher der Ratinginstanz Glaubwürdigkeit und Kompetenz zuerkennen, um die Suchaktivitäten zu „delegieren".

Rating erscheint auch geeignet, Risiken für die Verbraucherinnen und Verbraucher, die aus **Informationsasymmetrien nach Vertragsschluss** bestehen (sog. „Hold up" und „Moral Hazard"), zu senken. Hold up bezeichnet quasi den „Wortbruch" eines Vertragspartners nach Abschluss eines Vertrages, da die Vertragsparteien Ziele und Beweggründe voreinander vor Vertragsschluss verschwiegen haben (Hidden intention, siehe auch unter G.II.2.b). Moral Hazard beschreibt das „moralisches Risiko", welches aufgrund falscher Anreize oder ungleicher Informationen nach Vertragsschluss zweier Parteien ein opportunistisches Verhalten einer der beiden Vertragsparteien fördern kann (vgl. Kapitel G.II.2.b). Opportunistischem Verhalten kann durch **Anreize und entsprechende Maßnahmen** entgegengewirkt werden. Ein Rating sollte aus Sicht der Dienste Anreize setzen, wahrheitsgemäße Informationen zu übermitteln. Sofern ein zu beurteilendes Unternehmen nicht ausreichend kooperieren würde, hätte die Ratinginstanz z. B. die Möglichkeit, dieses Verhalten zu sanktionieren, indem das Ratingurteil nur auf Basis öffentlich erhältlicher Informationen erstellt wird, was zu einem schlechteren Ergebnis für das Unternehmen führen dürfte. Gerade bei der Datensicherheit sind viele technische Merkmale nicht öffentlich bekannt und verfügbar. Die Ratinginstanz könnte ein Ratingurteil beispielsweise ggf. auch zurückziehen, was in der Öffentlichkeit Fragen aufwerfen und sich für den jeweiligen Dienst nachteilig auswirken könnte.

Ein Rating muss unmittelbar angepasst werden, wenn neue Sachverhalte auftreten, die sich negativ auf das Ratingurteil auswirken können (anlassbezogenes Rating). Es könnte vor diesem Hintergrund auch

---

[371] Siehe für den Kreditbereich *Schaetzle* (2011), Ökonomische Funktionen von Ratingagenturen, Working Paper, Westfälische Wilhelms-Universität Münster, abrufbar unter: https://www.econstor.eu/handle/10419/55765 und die dort angegebene Literatur.

eine sog. „Überwachungsliste“ geführt und veröffentlicht werden. Auf dieser Liste werden die Namen der Rating-Petenten geführt, bei denen mit einer Veränderung des Ratings zu rechnen ist.

b) Reputation löst „Beziehungsprobleme“

Die Ratingagenturen, die auf den Finanzmärkten als Informationsintermediäre tätig sind, sind in der Vergangenheit bereits mehrfach in die Kritik geraten. Während der Finanzmarktkrise 2008 wurde ihnen beispielweise vorgeworfen, durch fehlerhafte Ratings die Krise mitverursacht zu haben.[372] Ist das Datenschutzrisiko als Ratingmerkmal zu bewerten, wären derart dramatische Auswirkungen von Fehleinschätzungen in Ratings wie auf den Finanzmärkten unwahrscheinlich. Das Datenschutzrisiko ist nicht direkt mit der Bonität eines Unternehmens verknüpft. Es ist auch nicht ersichtlich, dass das Datenschutzrisiko in relevantem Maße ausschlaggebend für Investitionsentscheidungen ist. Wenn es hingegen um die Bewertung des Ausfallrisikos eines Wertpapiers („Bonitätsrisiko“) mittels Rating geht, betrifft dies Investitionsentscheidungen von Verbraucherinnen und Verbrauchern und institutionellen Marktteilnehmern unmittelbar.

Nichtsdestotrotz sind solche Vorwürfe aus wissenschaftlicher Sicht nicht überraschend. Wenn Ratingagenturen als Informationsintermediäre zwischengeschaltet werden, entstehen als Folge ungleich verteilter Informationen zusätzliche **Prinzipal-Agent-Beziehungen einerseits zwischen Ratinginstanz und zu bewertenden Unternehmen sowie andererseits zu Verbraucherinnen und Verbrauchern**. Daraus eventuell resultierende Kosten der Überwachung und Bindung des Agenten (sog. Agency-Kosten) sind zu berücksichtigen und können über eine entsprechende Gestaltung des Rating gesteuert werden. Die Informationen zwischen **Ratinginstanz und Verbraucherinnen und Verbrauchern** sind zunächst ungleich verteilt. Letztere kennen die Qualifikation und Fachkenntnisse der Ratinginstanz nicht und können ihr Verhalten nicht beobachten. Um zu überprüfen, ob ein Rating sachlich richtig ist, müssten die Verbraucherinnen und Verbraucher zeit- und kostenintensive Anstrengungen leisten. Dies kann opportunistischem Verhalten der Ratinginstanz Tür und Tor öffnen. Signaling durch Rating wird dann

---

[372] Vgl. *Frankfurter Allgemeine Zeitung*, Die Macht der Rating-Agenturen, 30. April 2020, abrufbar unter: https://www.faz.net/aktuell/finanzen/finanzmarkt/kreditwuerdigkeit-die-macht-der-ratingagenturen-16748069.html; *ZEIT ONLINE*, Millionenstrafe für Moody's wegen geschönter Ratings, 14. Januar 2017, abrufbar unter: https://www.zeit.de/wirtschaft/2017-01/ratingagentur-moodys-millionenstrafe-finanzkrise; *Welt*, Die Rolle der Ratingagenturen in der Finanzkrise, 5. Februar 2009, abrufbar unter: https://www.welt.de/welt_print/article3149951/Die-Rolle-der-Ratingagenturen-in-der-Finanzkrise.html, abrufbar unter: https://www.welt.de/welt_print/article3149951/Die-Rolle-der-Ratingagenturen-in-der-Finanzkrise.html.

nicht mehr funktionieren, Überwachungsprobleme würden durch die Einschaltung des Intermediärs nicht gelöst, sondern verursacht.

Informationsasymmetrien bestehen zudem zwischen **Ratinginstanz und den zu bewertenden Diensten,** die sich dann ebenfalls zulasten der Verbraucherinnen und Verbraucher auswirken können. Insbesondere dann, wenn die Ratinginstanzen privatwirtschaftlich agieren, kann die Frage der **Finanzierung der Ratings** Abhängigkeiten begründen. Wenn die Ratinginstanz - was die Finanzierung angeht - von den zu bewertenden Unternehmen abhängt, könnte es zu Moral Hazard kommen, indem z. B. Ratings geschönt werden. Gerade wenn Ratinginstanzen zusätzlich Nebengeschäfte anbieten (wie z. B. Rating Advisory, Informationsveranstaltungen etc.) sind Interessenkonflikte wahrscheinlich. Während der Weltfinanzkrise 2008 soll es bei strukturierten Finanzprodukten zu Abhängigkeiten der Ratingagenturen von diesem Geschäftsfeld gekommen sein, was die Ratingergebnisse beeinflusst haben könnte. Privatwirtschaftliche Ratinginstanzen könnten ferner versuchen, nicht nur über zusätzliche Geschäfte, sondern über Kostensenkungen höhere Erträge zu erreichen, indem an der Qualität oder Aktualität der Ratings und damit den notwendigen Ressourcen gespart wird, was letztendlich nicht nur die Verbraucherinnen und Verbraucher, sondern auch die bewerteten Unternehmen schädigen würde. In einem Ratingprozess werden schließlich **vertrauliche Informationen** verarbeitet, die Mitarbeiter der Ratinginstanz für sich nutzen könnten statt diese in den Rating-Prozess einfließen zu lassen. Dieses „Insiderwissen“ kann der Ratinginstanz opportunistisches Verhalten ermöglichen, so dass es - wie bei den zuvor beschriebenen Aspekten auch - eben nicht zur besseren Information der Verbraucherinnen und Verbrauchern käme.[373] Entsprechende **Vereinbarungen zu Vertraulichkeit** und **einheitliche**

[373] Vgl. zur Manipulation von Informationen vgl. auch *Döring*, Verbraucherschutz aus Sicht der Informationsökonomik – Rechtfertigung, Maßnahmen und Erweiterungsbedarf, sofia-Diskussionsbeiträge, 2021, abrufbar unter: https://www.sofia-darmstadt.de/veroeffentlichungen/sofia-diskussionsbeitraege/sofia-dis-2021-4-doering.

Vorgaben zu Zeitpunkt und Ort der Veröffentlichung sind somit wichtige Voraussetzungen für eine bessere Information der Öffentlichkeit.[374]

Damit eine Ratinginstanz die mit ihr verbundenen Ziele erreichen kann und Informationsasymmetrien abgebaut werden können, müssen die Ratingqualität und die Akzeptanz des Ratings hoch sein. Hierbei kann der **Reputationsmechanismus** hilfreich sein.[375] Eine Ratinginstanz mit Reputation kann den Verbraucherinnen und Verbrauchern so signalisieren, dass ihre Interessen wahrgenommen werden und sie dem Urteil vertrauen können. Sie wird außerdem geneigt sein, diese Reputation nicht aufs Spiel zu setzen. Dies gilt insbesondere dann, wenn sie **Ratings fortlaufend („mehrperiodisch") durchführt** oder aktualisiert, so dass ihre zukünftigen Erträge von der heutigen Qualität ihres Urteils abhängen. Reputation kann dann zu sinkenden Monitoring-Ausgaben bei Verbraucherinnen und Verbraucher und Diensten führen.[376]

In der Literatur werden verschiedene Maßnahmen diskutiert, wie Reputation aufgebaut oder gesteigert werden kann. Dazu gehören z. B. **die Konzentration auf das Rating als Hauptgeschäftsfeld, die Reduzierung von Abhängigkeiten von bestimmten Unternehmen und der Ausschluss von**

---

[374] Auf den Finanzmärkten hat der Gesetzgeber ohnehin das "Verbot des Insiderhandels" und die "Ad hoc-Publizität" etabliert, da sich die in Rede stehenden Insiderinformationen - unabhängig von einem Zusammenhang mit Rating - unmittelbar an den Kapitalmärkten auf die Einschätzung des Bonitätsrisikos auswirken und Preisreaktionen auslösen können. Dies wäre bei Datenschutzinformationen unmittelbar nicht der Fall. Allerdings sind unter den Messenger- und Video-Diensten auch mit börsennotierten Unternehmen verbundene Dienste, so dass nicht auszuschließen ist, dass sich Informationen über mögliche Defizite in der Datenschutzpraxis und die unberechtigte Weitergabe dieser Informationen auf die Refinanzierungsmöglichkeiten dieser Dienste auswirken könnten.

[375] Weitere Möglichkeiten, die aber in diesem Zusammenhang weniger bedeutend sind, sind der Aufbau eines Markennamens, die Gewährung von Garantien oder Werbung, vgl. *Döring*, Verbraucherschutz aus Sicht der Informationsökonomik – Rechtfertigung, Maßnahmen und Erweiterungsbedarf, sofia-Diskussionsbeiträge, 2021, abrufbar unter: https://www.sofia-darmstadt.de/veroeffentlichungen/sofia-diskussionsbeitraege/sofia-dis-2021-4-doering.

[376] Vgl. *Schaetzle* (2011), Ökonomische Funktionen von Ratingagenturen, Working Paper Nr. 113, Westfälische Wilhelms-Universität Münster, abrufbar unter: https://www.econstor.eu/handle/10419/55765; *Heinke* (1998), Bonitätsrisiko und Credit Rating festverzinslicher Wertpapiere, Bad Soden, Ts./ Uhlenbruch.

Verflechtungen mit zu bewertenden Unternehmen.[377] Von hoheitlicher Seite muss dem Risiko entgegengewirkt werden, dass Ratingergebnisse mit regulatorischen Verpflichtungen verknüpft werden - wie es z. B. bei der Kapitalmarktregulierung der Fall ist - so dass sich Ratings zu „**Regulatory Licences**" wandeln könnten, die quasi an die Stelle von Regulierungsverfügungen und deren Umsetzung treten. Informationsverlust und Informationssteuerung entsprechend der Anforderungen der Regulierungsbehörden könnten die unerwünschten Folgen sein.[378] Die Unabhängigkeit des Ratingurteils stünde in Frage. Auf den Bereich des Datenschutzes übertragen, wäre darauf zu achten, dass die Ratingkriterien von anderen aufsichtsrechtlichen Prüfverfahren abgegrenzt werden und es nicht zu Vermischungen kommt.

Festzuhalten ist, dass die Einschaltung einer Ratinginstanz als Intermediär neue Beziehungen mit Informationsgefälle begründet, nämlich einerseits zu den zu bewertenden Diensten, andererseits zu den Verbraucherinnen und Verbrauchern. Risiken aus opportunistischem Verhalten der Ratinginstanz können gemildert werden, wenn **Abhängigkeiten reduziert** werden. Dies betrifft die Art und Weise, wie die Finanzierung gestaltet wird - wer bezahlt, die Konzentration auf Rating als einziges Geschäftsfeld, das Vermeiden von Verflechtungen und Vermischungen mit anderen Aufgaben, tragfähige Vereinbarungen zur Vertraulichkeit und zum Ort und Zeitpunkt der Veröffentlichung des Ratings sowie keine Verknüpfung mit regulatorischen Maßnahmen. Reputation der Ratinginstanz kann dann die Gefahren ungleich verteilter Information mildern, insb. dann, wenn Ratings fortlaufend durchgeführt werden.

c) Vertrauen durch Unabhängigkeit

Im vorausgegangenen Abschnitt wurde deutlich, dass viele **Schwierigkeiten aus Abhängigkeiten** von Ratingagenturen hervorgehen können. Diese kommen besonders zum Tragen, wenn Rating privatwirtschaftlich organisiert ist. Dass das Rating des Bonitätsrisikos auf den Finanzmärkten von drei privaten Ratingunternehmen durchgeführt wird, ist auf die historische Entwicklung zurückzuführen. Es

---

[377] Vgl. z. B. *Heinke* (1998), Bonitätsrisiko und Credit Rating festverzinslicher Wertpapiere, Bad Soden, Ts./ Uhlenbruch; Wappenschmidt (2009), Ratinganalyse durch internationale Ratingagenturen, Frankfurt am Main.

[378] Vgl. *Partnoy*, The Siskel and Ebert of Financial Markets?: Two thumbs down for the credit rating agencies, in: Washington University Law Quarterly, Jg. 77, Heft 3, abrufbar unter: https://journals.library.wustl.edu/lawreview/article/id/5968/ sowie auch Vgl. *Frankfurter Allgemeine Zeitung*, Die Macht der Rating-Agenturen, 30. April 2020, abrufbar unter: https://www.faz.net/aktuell/finanzen/finanzmarkt/kreditwuerdigkeit-die-macht-der-ratingagenturen-16748069.html.

hat seinen Anfang im 19. Jahrhunderts in den USA genommen, wo die landesweite Verbreitung der Eisenbahn einen hohen Finanzierungsbedarf auslöste. Der sich hierfür etablierende Kapitalmarkt war weitgehend anonym und intransparent, so dass Kreditgeber einem hohen Kreditrisiko ausgesetzt waren.[379] Nachdem zwei Unternehmer zunächst entsprechende Informationen sammelten und veröffentlichten, gründeten sie Anfang des 20. Jahrhunderts die bekannten Ratingagenturen, die bis heute tätig sind. Institutionelle Investoren und Anleger und Anlegerinnen haben ein hohes Interesse daran, nicht in bonitätsschwache Wertpapiere zu investieren und nutzen Ratings, um ihre Risiken zu reduzieren, was sie selbst derart nicht leisten könnten.

Für das Datenschutzrisiko erscheint es weniger sinnvoll, profitorientierte Unternehmen zu beauftragen. Es ist nicht zu erwarten, dass die Dienste bereit sind, ein solches Rating zu finanzieren. Ihre Datenschutzaktivitäten sind bisher offenbar weniger erfolgsrelevant als andere Kompetenzen. Verdienstmöglichkeiten für private Rating-Anbieter scheinen sich deshalb erstmal nicht zu eröffnen. Private Anbieter müssten außerdem nicht nur die entsprechenden Kompetenzen besitzen, sondern auch die notwendige Reputation, um die oben geschilderten Informationsprobleme zu mildern (siehe G.III.3.b).

Eine staatliche oder in anderer Weise von Profitinteressen unabhängige Instanz müsste neben der entsprechenden fachlichen Eignung über die notwendige Reputation verfügen, um das Vertrauen der Dienste sowie der Verbraucherinnen und Verbraucher in die Qualität des Rating zu gewinnen. Wesentliche Kriterien sind hier Unabhängigkeit in der Entscheidungsfindung und keine Vermischung mit anderen, z. B. regulatorischen Aufgaben, wie im vorausgegangenen Abschnitt c) dargelegt.

4. Besondere Eignung für die Datenschutzpraxis

Anders als viele andere informationsbezogene Maßnahmen ist das Rating nicht nur auf eine Marktseite, also entweder die Messenger- und Video-Dienste als Anbieter auf der einen Seite oder die Verbraucherinnen und Verbraucher auf der anderen Seite ausgerichtet. Vielmehr dürfte es beide Seiten - sowohl die Dienste als auch deren Nutzerinnen und Nutzer - zu mehr Initiative veranlassen. Außerdem lässt ein Vergleich der Anstrengungen der Implementierung mit den langfristigen positiven Auswirkungen erwarten, dass der Nutzen die Kosten deutlich überwiegen wird. Schließlich sind – was die Reichweite eines Rating angeht – unterschiedliche Gestaltungsoptionen denkbar

Ein Rating kann **Motivation für beide Marktseiten** sein. Nach den bisherigen Erkenntnissen in dieser Sektoruntersuchung könnte der Einsatz eines **Rating als Signal** für das Datenschutzrisiko in der Praxis allerdings erfolgversprechender sein als auf seine Wirkung als Screening-Indikator für die

[379] Siehe *Wikipedia*, abrufbar unter: https://de.wikipedia.org/wiki/Rating.

Datenschutzeigenschaften eines Messenger- und Video-Dienstes zu setzen. Während beim Screening die uninformierte Marktseite - die Verbraucherinnen und Verbraucher - das Informationsgefälle zu beseitigen versucht, stellt beim Signaling die besser informierte Seite eigeninitiativ Informationen bereit. Denn mehr als die Verbraucherinnen und Verbraucher könnten die Messenger- und Video-Dienste gegenüber einer veröffentlichten Datenschutzrisiko-Information sensibel sein, gerade wenn vage Vermutungen und Kritiken ihrer Datenschutzpraxis durch ein öffentlich geprüftes Urteil ersetzt werden. Datenschutz ist nicht nur „Gesetz“ - in Deutschland und Europa in Gestalt der DSGVO - sondern inzwischen auch zu einem sensiblen Thema geworden, das von der (Fach-) Öffentlichkeit aufmerksam verfolgt wird und auch im politischen Umfeld Beachtung findet. Dazu hat auch die ständige Auseinandersetzung mit den Praktiken einiger führender Branchenvertreter und öffentliches Nachdenken über staatliche Initiative wegen unerwünschter Praktiken und Entwicklungen beigetragen. Von daher darf vermutet werden, dass viele Messenger- und Video-Dienste ein **öffentlich negatives Zeugnis oder ein schlechteres Ranking als der wichtigste Wettbewerber** vermeiden möchten. Bei börsennotierten Unternehmen können schließlich Auswirkungen auf die Finanzierungskosten nicht ausgeschlossen werden.

Es ist aber auch vorstellbar, dass die Verbraucherinnen und Verbraucher nicht bei einem Messenger- und Video-Dienst registriert sein möchten, der **im Ranking den letzten Platz** einnimmt. Vielleicht möchte auch eine ihrer Kontaktpersonen lieber einen Messenger- und Video-Dienst nutzen, der ein niedrigeres Datenschutzrisiko aufweist als der bisher gewählte Dienst. Ein veröffentlichtes Rating-Urteil einer vertrauenswürdigen Instanz könnte hier die **glaubwürdige Information sein, die berufliche „Entscheider“ oder Ansprechpartner** für die Öffentlichkeit bei Behörden und Unternehmen benötigen, um über die DSGVO-Konformität eines Messenger- und Video-Dienstes und damit dessen Einsatzmöglichkeiten in der eigenen Institution zu entscheiden.

Insgesamt betrachtet sind für die Förderung des Datenschutzes als Wettbewerbsparameter auf staatlicher Seite Ressourcen aufzuwenden.

Umgekehrt sind - in der jetzigen Situation ohne Rating - die **Defizite im Marktmechanismus**, die aufgrund der gegenwärtigen Informationsasymmetrien bestehen und anhalten, auch nicht ohne monetäre Folgen. Die **bisherigen Wohlfahrtsverluste** insgesamt oder auch nur allein die Kosten von Verfahren der öffentlichen Hand auf Basis wettbewerbs-, datenschutz- und regulierungsrechtlicher Grundlagen gegen führende Branchenteilnehmer dürften erheblich sein. Wenn die Messenger- und Video-Dienste auf der einen Seite und Verbraucherinnen und Verbraucher auf der anderen Seite Datenschutz als wichtiges Kriterium in ihre Entscheidungen aufnähmen, könnten auch Fehlentwicklungen bei der Datenschutzpraxis einzelner Branchenvertreter - wie sie in der Öffentlichkeit diskutiert werden - zukünftig in die richtige Richtung gewendet werden.

Neben der Frage der gesamtwirtschaftlichen Kosten ist für eine praktische Umsetzung zu überlegen, auf welcher **politisch-administrativer Ebene** - weltweit, EU-weit oder national - das Rating umgesetzt werden sollte. Wie in diesem Bericht bereits mehrfach beschrieben wurde, ist die Branche der Messenger- und Video-Dienste sehr unterschiedlich aufgestellt und umfasst eine große Bandbreite von Unternehmen und freien Anwendungen mit **unterschiedlichen regionalen Schwerpunkten und Reichweiten**. Einige große Dienste werden weltweit von Verbraucherinnen und Verbrauchern verwendet und auch viele andere Dienste sind in mehreren Weltregionen aktiv. Daher wäre idealerweise ein weltweit einheitliches Ratingverfahren für das Datenschutzrisiko angeraten. Ganz abgesehen von Problemen der internationalen Koordination und Abstimmung dürften die unterschiedlichen datenschutzrechtlichen Rahmenbedingungen zwischen den verschiedenen Jurisdiktionen aber einem solchen weltweit einheitlichen Bewertungssystem entgegenstehen. Daher dürfte eine Umsetzung auf europäischer Ebene im **Geltungsbereich der DSGVO** näher liegen**.**

H. Empfehlungen

Die Sektoruntersuchung Messenger- und Video-Dienste gibt über ihre Ermittlungsergebnisse und deren rechtliche Einordnung hinaus wichtige Hinweise für den künftigen Umgang mit der verbraucherrechtlich teilweise unbefriedigenden Situation bei Messenger- und Video-Diensten. Aufgrund der Vielfalt der Branche und der vielen Geschäftsmodelle und freien Anwendungen neben den bekannten Marktführern möchte das Bundeskartellamt mit diesem Bericht einen Beitrag zu mehr Transparenz leisten und so gesamtwirtschaftlich förderliche konkrete Hinweise für Verbesserungen des Verbraucherschutzes geben.

Um dem Datenschutz beim Messaging und bei Videokonferenzen gleichwohl zu mehr Breitenwirkung zu verhelfen, sollte der verbraucherschutzfreundliche Umgang mit Daten der Nutzerinnen und Nutzer als Wettbewerbsparameter bei Messenger- und Video-Diensten gefördert werden. Dazu könnten verschiedene Maßnahmen ergriffen werden (siehe Abbildung 18).

Zunächst sollte die verbraucherrechtliche Rechtsdurchsetzung gestärkt und an den Anforderungen der digitalen Wirtschaft ausgerichtet werden (dazu unter I.). Außerdem sollte die Aufklärung der Verbraucherinnen und Verbraucher nicht nur intensiviert, sondern auch komprimiert und besser an ihre Bedürfnisse angepasst werden (dazu unter II.). Neben der Fürsorge für die Verbraucherinnen und Verbraucher sollte nicht vernachlässigt werden, bessere wettbewerbliche Bedingungen für datenschutzfreundliche Dienste zu schaffen, was mit relativ einfachen Mittel verwirklicht werden kann (dazu unter III.). Bisher können die Verbraucherinnen und Verbraucher noch nicht auf komprimierte Informationen zur Datenschutzqualität ihrer Dienste, wie sie z. B. ein Rating-Verfahren hervorbringen könnte, zurückgreifen. Daher ist bei der Gestaltung von Interoperabilitätsvorhaben darauf zu achten, dass diese nicht nur innovationsfreundlich, sondern auch verbraucherorientiert eingeführt werden (zu grundsätzlichen Bedingungen unter IV.).

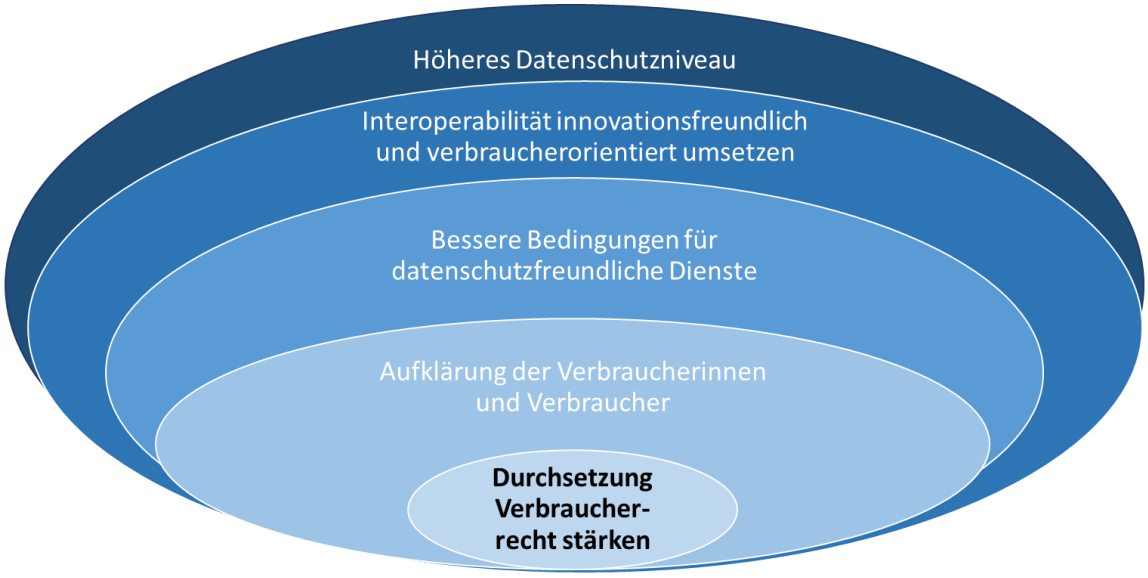


Abbildung 18: Handlungsempfehlungen für ein höheres Datenschutzniveau

I. Durchsetzung des Verbraucherrechts stärken

Das Bundeskartellamt hat drei rechtliche Fragestellungen untersucht, die für die Verbraucherinnen und Verbraucher beim Messaging und bei Videokonferenzen besonders wichtig sind. Die untersuchten Praktiken standen im Verdacht, nicht nur die Datensicherheit zu gefährden, sondern auch in Verbraucherrechtsverstößen zu münden.

Dieser Verdacht konnte bei zwei der drei Untersuchungsfelder im Rahmen dieser Sektoruntersuchung nicht ausgeräumt werden; bei dem dritten Untersuchungsfeld verblieb zumindest der Eindruck, dass Verbesserungen bei der Informationsversorgung zum Wohle der Verbraucherinnen und Verbraucher notwendig sind (dazu unter 1.).

Gleiches gilt für die Durchsetzung des Verbraucherrechts. Die digitale Wirtschaft stellt insb. aufgrund ihrer technischen Basis immer neue Herausforderungen. Eine behördliche Rechtsdurchsetzung kann hier einen sinnvollen Beitrag zur Bewältigung und Gestaltung leisten (dazu unter 2.).

1. Verbraucherrechtsverstöße und rechtliche Risiken

<u>Synchronisation des Kontaktverzeichnisses</u>

Die gängige Praxis vieler bekannter Messenger- und Video-Dienste, das Kontaktverzeichnis der Nutzerinnen und Nutzer hochzuladen und zu synchronisieren, führt dazu, dass auch die Kontaktdaten von Nicht-Nutzerinnen und Nicht-Nutzern erfasst werden. Diese können in die Synchronisation nicht gemäß Art. 6 Abs. 1 Unterabs. 1 Buchst. a) DSGVO einwilligen. Der synchronisierende Dienst ist ihnen nicht bekannt. Die datenschutzrechtliche Verantwortlichkeit kann dabei nicht auf die Nutzerin und den Nutzer abgewälzt werden, sondern liegt beim jeweiligen Dienst selbst. Die Telefonnummer der Nicht-

Nutzerin oder des Nicht-Nutzers stellt ein personenbezogenes Datum im Sinne von Art. 4 Nr. DSGVO dar und zwar auch dann, wenn außer der Telefonnummer keine weiteren Daten erhoben werden. Der Personenbezug besteht ebenfalls fort, wenn die Telefonnummer durch einen kryptographischen Hashwert ersetzt wird, der mit der Nutzerin oder dem Nutzer verknüpft ist, aus deren Kontaktverzeichnis die Telefonnummer stammt. Der Dienst würde für die Datenverarbeitung - also die langfristige Telefonnummer-Speicherung von Nicht-Nutzerinnen und Nicht-Nutzern - somit eine andere Legitimation benötigen. Nicht zu erwarten ist, dass sich diese aus der Wahrung berechtigter Interessen (Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO) des Verantwortlichen ergeben, die mit den Freiheitsrechten des betroffenen Dateninhabers abzuwägen sind. Der Vernetzungsvorteil erscheint gerade in zeitlicher Hinsicht bei unterstellter täglicher Synchronisierung zu gering. Lediglich hinter einem kurzfristigen Hochladen der Telefonnummern und anschließendem Löschen derjenigen Nummern von Nicht-Nutzerinnen und Nicht-nutzern mag ein berechtigtes Interesse stehen.

Internationaler Datentransfer / Datenspeicherung

Die Ermittlungsergebnisse zum Prozess der Datenverarbeitung legten nahe, dass sich einige Messenger- und Video-Dienste beim Datentransfer in Drittländer und beim Speichern auf Servern in Drittländern (Art. 45 DSGVO) nicht rechtskonform verhalten. Dies betraf vor allem diejenigen Dienste, die Daten deutscher Nutzerinnen und Nutzer in den USA speichern. Außerdem unterhalten weitere Dienste Server-Infrastrukturen in der EU und Drittländern, insb. den USA. Es blieb unklar, wohin Daten der EU-Bürgerinnen und Bürger transferiert werden. Teilweise war dies von diversen Konstellationen abhängig. Bei freien Messenger-Clients hängt der Ort der Datenspeicherung von der Serverauswahl der Nutzerinnen und Nutzer ab.
In Länder außerhalb der EU und des Europäischen Wirtschaftsraums dürfen Daten nur übermittelt werden, wenn ein angemessenes Datenschutzniveau in dem jeweiligen Drittland (Art. 45 DSGVO) sichergestellt ist. Allerdings ist der frühere Datenschutzschild (EU-US Privacy Shield), den die EU mit den USA verhandelt hatte, nach dem „*Schrems II*“ - Urteil des EuGH aus dem Sommer 2020 ungültig. Sofern die Verantwortlichen innerhalb der Dienste ihre Datenübermittlungen in Länder außerhalb der Europäischen Union inzwischen im Bedarfsfall nicht auf eine neue Grundlage, wie geeignete Garantien einschließlich zusätzlicher Maßnahmen, gestützt haben, wäre der Datentransfer unzulässig. Dieser Verdacht konnte bei der Mehrheit der Dienste nicht ausgeräumt werden, da keine Informationen über konkrete Absicherungsmaßnahmen vorliegen.

Informationsmängel im Zusammenhang mit der Ende-zu-Ende-Verschlüsselung

Das Bundeskartellamt hatte die Ende-zu-Ende-Verschlüsselung aus mehreren Gründen für eine rechtliche Analyse ausgewählt. So ist die Verschlüsselung als für den Laien komplexes technisches Thema ein Beispiel für die weitreichenden Informationsnachteile der Verbraucherinnen und

Verbraucher. Der Begriff der Ende-zu-Ende-Verschlüsselung war in der Öffentlichkeit außerdem mit Sicherheitsmängeln verbunden worden, nicht nur in der Sache selbst, sondern auch als Beispiel für die besonderen Herausforderungen, die mit Interoperabilität einhergehen können.
Für einen lauterkeitsrechtlichen Transparenzpflichtverstoß wäre zu belegen, ob Informationen zur Sicherheit der Kommunikation, wie beispielsweise das Verwenden einer besonderen Verschlüsselungsmethode, als wesentlich im Sinne des § 5a Abs. 1 UWG zu bewerten sind, ob die vorenthaltene Information für das Treffen einer informierten geschäftlichen Entscheidung erforderlich ist und ob sie geeignet sein kann, die Entscheidung der Nutzerinnen und Nutzer eines Messenger- und Video-Dienstes so zu beeinflussen, dass sie sich bei Offenlegung der relevanten Fakten möglicherweise anders entschieden hätten.
Nach Auffassung des Bundeskartellamts wird sich ein **Transparenzverstoß durch Informationsmängel** in Bezug auf die Verschlüsselungsart nicht leicht begründen lassen, auch wenn gewisse **rechtliche Risiken** bestehen. Zwar dürften nicht nur Sicherheitseigenschaften entsprechend der umfangreichen Informationsbereitstellung durch die Dienste zu den „wesentlichen Informationen“ gerechnet werden können. Es dürfte auch die unklare, unverständliche oder zweideutige Informations-Bereitstellung vieler Messenger- und Video-Dienste als „Vorenthalten“ zu deklarieren sein. Demgegenüber könnte aber die „**geschäftliche Relevanz**“ der Sicherheitseigenschaften nur schwer zu begründen sein. Die Marktentwicklung ist vorangeschritten. Die Ende-zu-Ende-Verschlüsselung hat sich als Branchenstandard etabliert, so dass es hinsichtlich dieser Sicherheitseigenschaft wahrscheinlich keinen Unterschied macht, wo Nutzerinnen und Nutzer sich registrieren. (Auch wenn vor diesem Hintergrund überraschend war, dass einige wenige bekannte Dienste die Ende-zu-Ende-Verschlüsselung nicht oder nur eingeschränkt umsetzen). Eine bessere Einschätzung der Verbrauchersicht hätte weiteren Ermittlungsaufwand wie etwa eine Verbraucherbefragung erfordert, mit welchem aufgrund der Komplexität der Begrifflichkeiten aber nur ungewisse Aufklärungschancen verbunden waren. Auch die Einordnung des Verbraucherverhaltens aus Unternehmenssicht blieb uneindeutig, da es viele kostenfreie Angebote der Messenger- und Video-Dienste gibt. Letztendlich musste eine abschließende Bewertung jeweils der **Klärung im Einzelfall** vorbehalten bleiben.

2. Rechtsdurchsetzung - Bestandsaufnahme und Perspektiven

Ohnehin ist die Ausgangssituation der **Verbraucherinnen und Verbraucher** bei der Durchsetzung ihrer Rechte nicht einfach, da es sich im Allgemeinen für sie nicht lohnt, bei datenschutzrechtlichen Problemen zu klagen. Ferner ist zu beobachten, dass einzelne Urteile nur schwerfällig auf die Gesamtheit der Verbraucherinnen und Verbraucher übertragen werden. Dass sich daraus eine sog. „rationale Apathie“ entwickelt, also die Entscheidung, aufgrund zu hohen Aufwands im Vergleich zu den Erfolgsaussichten nicht tätig zu werden, ist nicht überraschend.

Zudem sehen sich die Akteure der bewährten privaten Rechtsdurchsetzung bei Sachverhalten aus der **digitalen Wirtschaft neuen Anforderungen** gegenüber. Aufgrund des großen Einflusses technischer Gegebenheiten auf die Datenschutzqualität von Messenger- und Video-Diensten kann der Nachweis von Rechtsverstößen für die **Verbände** bei komplexen Sachverhalten aus der digitalen Wirtschaft generell herausfordernd sein. Dies gilt insb. dann, wenn kein Zugriff auf technische Informationen besteht, weil diese bei den Unternehmen liegen. Anders als bei weniger technisch basierten Fragestellungen, können dann keine belastbaren Schlüsse auf rechtliche Verstöße gezogen werden. **Behördliche Verfahren** wären dann das Mittel der Wahl, um die Informationen, wie es das Bundeskartellamt im Rahmen dieser Sektoruntersuchung getan hat, direkt bei den Unternehmen zu erheben.
Soweit Verstöße gegen das **Lauterkeitsrecht** und das bürgerliche Recht in Rede stehen, gibt es bisher ohnehin keine behördliche Rechtsdurchsetzung. Verbraucherschützende Vorschriften aus diesen Rechtsgebieten werden in Deutschland traditionell durch private Kläger durchgesetzt. Doch auch bei der **Durchsetzung des Datenschutzrechts** sehen befragte Messenger- und Video-Dienste Bedarf an einem Ausbau der behördlichen Durchsetzung. Während die DSGVO als Regelungswerk viel Zuspruch fand, wurden die Organisation auf europäischer Ebene und die Zuständigkeitsregeln kritisch betrachtet. Denn bei grenzüberschreitender Datenverarbeitung ist die Datenschutzbehörde am Sitz der Hauptniederlassung des Verantwortlichen federführend. Wenn sich Verfahren bei einzelnen Datenschutzbehörden sammelten, könne die große **Masse an DSGVO-Verstößen** zu einem Durchsetzungshemmnis werden.
Messenger- und Video-Dienste sind nicht nur in Deutschland und Europa aktiv, sondern häufig weltweit vernetzt. Demzufolge müssen die deutschen Rechtsdurchsetzungsakteure mit der **Internationalität der Branche** umgehen, wie die Ausführungen zum internationalen Datentransfer belegen.

II. Kontinuierliche Aufklärung der Verbraucherinnen und Verbraucher

Wie die Ermittlungsergebnisse im vorausgegangenen Kapitel gezeigt haben, besteht unter den Diensten Konsens, dass die Verbraucherinnen und Verbraucher weiter aufgeklärt und informiert werden müssen. Es muss klarer, praxisnäher und kontinuierlich über den schützenden Umgang mit den persönlichen Daten informiert werden. Dazu gehört zum Beispiel auch Wissen darüber, wie die Vertrauenswürdigkeit von IT-Systemen überprüft werden kann. Die **Entwicklung von Medienkompetenz** ist ein langfristiges Unterfangen, das bereits in der Grundschule beginnen und bis zum Einstieg in Ausbildung und Studium fortgesetzt werden sollte. Alle Bevölkerungsgruppen sollten in eine **Kommunikationsstrategie für den Datenschutz** integriert werden. Hier könnten die Informationskanäle genutzt werden, die Verbraucherinnen und Verbraucher bevorzugt nutzen, nämlich die internetbasierten digitalen Medien. Die weniger internet-affinen Bevölkerungsgruppen könnten zusätzlich über herkömmliche Medien, wie Fernsehen, erreicht werden. Bundesweite kontinuierliche Kampagnen fehlen bisher weitgehend.

Einfluss hat auch das Verhalten **öffentlicher Entscheidungsträger**. Dies betrifft insbesondere die Institutionen, die einen hohen Verbreitungsgrad haben und mit den Verbraucherinnen und Verbrauchern in direkten digitalen Kontakt treten, wie das öffentliche Fernsehen und Rundfunk, aber auch einzelne Behörden, Städte und Gemeinden. Es wäre zu prüfen, ob für die Kontaktaufnahme vermehrt datenschutzfreundliche Messenger- und Video-Dienste eingesetzt werden können.
Auch die Art und Weise, wie Messenger- und Video-Dienste selbst ihre Nutzerinnen und Nutzer über **Datensicherheit und Datenschutz informieren,** sollte, was Inhalt, Darstellung und Vermittlung angeht, verbessert werden, um die Suchkosten für die Verbraucherinnen und Verbraucher zu senken.

III. Bessere Bedingungen für datenschutzfreundliche Dienste

Die Situation datenschutzfreundlicher Messenger- und Video-Dienste könnte bereits mit vergleichsweise wenig aufwendigen Maßnahmen verbessert werden. Dies betrifft sowohl Investitionen in datenschutzfreundliche Dienste - also ihre Auswahl und ihren bezahlten Einsatz im öffentlichen Bereich - als auch eine Überprüfung der Förderung von Open Source - Entwicklungen. Auch hier steht bei allen Aspekten die Notwendigkeit einer besseren **zielgerichteten Informationsversorgung** im Vordergrund.

Verlässliche **Informationen zur DSGVO-Konformität von Messenger- und Video-Diensten** – gerade auch derjenigen Dienste, die nicht im Fokus des öffentlichen Interesses stehen - sind öffentlich kaum verfügbar. Möglicherweise könnten mit zielgerichteten Informationen - wie sie ein Rating des Datenschutzrisiko generieren würde - über die Branchenmitglieder und ihre datenschutzrechtlichen Kompetenzen auch bei der **Konzipierung von Ausschreibungen** Verbesserungen erreicht werden.
Auch was die **Förderung von Open Source** angeht, fehlt es offenbar bisher an verlässlich und einfach auffindbaren Informationen, hier für die interessierten Dienste. Hilfreich wäre - so die Branchenvertreter - eine **Übersicht in Form einer europäischen oder deutschen Webseite**, auf der alle Fördermöglichkeiten und die jeweiligen Förderkriterien dargestellt und eingesehen werden können. Von Open Source-Entwicklungen ohne fortbestehende Fehler, die Datensicherheit und Datenschutz beeinträchtigen, würde die allgemeine Öffentlichkeit profitieren, da die Entwicklungen allen Interessierten offenstehen. Daher könnte es dem Datenschutz zuträglich sein, wenn das bisherigen Förderspektrum, das auf Neuentwicklungen ausgerichtet ist, ausgeweitet würde. Es könnte sich positiv auf die Datensicherheit auswirken, wenn auch **Wartung und Pflege** der Open Source-Software einschließlich Fehlersuche und Fehlerbehebungen sowie der Betrieb der notwendigen Hardware und deren Wartung in Förderprogramme einbezogen werden.

IV. Interoperabilität innovationsfreundlich und verbraucherorientiert umsetzen

Wie das Bundeskartellamt im Zwischen- und Abschlussbericht erörtert hat, sind bei jeglichen Vorhaben zur Umsetzung und Gestaltung von Interoperabilität **Auswirkungen auf Innovation und Wettbewerb** zu beachten, beispielsweise wenn dazu notwendige Standardisierungen auf unterschiedliche technische Gestaltungen der Dienste treffen. Zwar ist das DMA-Interoperabilitätsregime auf Basisfunktionen beschränkt und asymmetrisch ausgestaltet. Allerdings sind die Architektur der Dienste und die technische Verortung der einzelnen Funktionen auf dieser sehr individuell, so dass Interoperabilität hier Vereinheitlichungen und Anpassungen in unterschiedlichem Ausmaß erfordern würde. Dies könnte auch die Innovationskräfte der Dienste unterschiedlich beeinträchtigen.[380]

Doch auch die **Perspektive der Verbraucherinnen und Verbraucher**, die Messenger- und Video-Dienste nutzen, ist zu berücksichtigen. Bisher können die Verbraucherinnen und Verbraucher nicht auf Ergebnisse von Rating-Verfahren oder ähnliche Methoden zurückgreifen, wenn sie nach prägnanten und vergleichenden Informationen über die Datenschutzqualität der Messenger- und Video-Dienste suchen (siehe dazu nochmals unter G.III.) Sofern zukünftig zwischen einzelnen Diensten oder in größeren Gruppen Interoperabilität praktiziert werden sollte, könnte die Informationslage für die Nutzerinnen und Nutzer noch undurchschaubarer werden. Der mit Interoperabilität verbundene Wunsch, Netzwerkeffekte zu entkräften und datenschutzfreundlichen Diensten bessere Chancen im Wettbewerb zu ermöglichen, indem die Verbraucherinnen und Verbraucher wechseln, könnte so konterkariert werden.

Die Verbraucherinnen und Verbraucher dürfen daher nicht auf sich selbst gestellt sein. Für Datenschutz und Datensicherheit muss Sorge getragen werden. Jegliche **Vorhaben zur Umsetzung und Gestaltung von Interoperabilität** sowie zur **Bewältigung der technischen Herausforderungen** müssen die Sicherheit und den Schutz der Daten aller Verbrauchenden im Blick behalten und alle von ihnen genutzten Dienste einbeziehen. Aufgrund der interdisziplinären Herausforderungen im Bereich der Messenger- und Video-Dienste - informationstechnologisch, verbraucher- und datenschutzrechtlich sowie ökonomisch - erscheint eine **Zusammenarbeit verschiedener Wissensträger** bei solchen Interoperabilitätsvorhaben sinnvoll. Angesichts der Dynamik der Branche und des Innovationspotentials der Technik erscheint es

---

380 Eine vertiefte technische Darstellung der Möglichkeiten einer Ende-zu-Ende-Verschlüsselung unter Interoperabilität bietet die BNetzA-Studie "Interoperability between Messaging Services - Secure Implementation of Encryption", April 2023, abrufbar unter: https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Technologien/Onlinekomm/Study_InteropEncryption.pdf?__blob=publicationFile&v=1. Die Studie bezieht sieben Messenger- und Video-Dienste ein und beruht auf einer Untersuchung öffentlich erhältlicher technischer Dokumentationen und wissenschaftlicher Publikationen.

geboten – wie im Zwischenbericht bereits ausgeführt - die Branche einzubeziehen, wie es auf Seiten der Europäischen Kommission anlässlich eines Workshops zu Interoperabilität im Februar 2023 grundsätzlich bereits praktiziert wurde.

Da die Branche – wie in diesem Abschlussbericht an verschiedenen Stellen betont – in technischer und kommerzieller Hinsicht vielfältig aufgestellt ist, sollten jegliche Regeln zur technischen Umsetzung **diskriminierungsfrei sein, solange der Stand der Technik gewährleistet ist.**

Wie diese Untersuchung gezeigt hat, haben die Verbraucherinnen und Verbraucher bei vielen Messenger- und Video-Diensten **Wahlmöglichkeiten**, ob sie bestimmte Funktionen einstellen oder nicht. So können die Verbraucherinnen und Verbraucher z. B. entscheiden, ob sie die Ende-zu-Ende-Verschlüsselung aktivieren oder nicht. Viele Dienste bieten auch verschiedene Varianten ihrer App an, wo in Abhängigkeit vom Entgelt unterschiedliche Funktionen genutzt werden können. Inwieweit damit auch unterschiedliche Stufen bei Sicherheitskriterien, beispielsweise Transportverschlüsselung oder Ende-zu-Ende-Verschlüsselung, einhergehen, ist häufig nicht eindeutig erkennbar. Für ein sicheres **Verbraucherprodukt unter Interoperabilität** wäre es wichtig, dass ein entsprechendes Regime vorsieht, bereits aktivierte Sicherheitskriterien beim messenger-übergreifenden Austausch zu erhalten.

Ferner sollte auch unter Interoperabilität eine **sparsame Verarbeitung der Daten** angestrebt werden. Das Bundeskartellamt hat in dieser Untersuchung die Frage des Serverstandorts, die Art des Geschäftsmodells und den Umgang mit Kontakten besonders hervorgehoben. Messenger- und Video-Dienste müssen Daten europäischer Nutzerinnen und Nutzer in der Europäischen Union speichern, um der europäischen DSGVO zu entsprechen. Die Daten der Nutzerinnen und Nutzer gelten in diesem Rechtsrahmen als besser geschützt als z. B. in den USA. Das **Geschäftsmodell** als erstes Indiz für die Intensität der Datenweitergabe können die Nutzerinnen und Nutzer vielleicht noch für den von ihnen unmittelbar genutzten Dienst heranziehen. Unter Interoperabilität bei Beteiligung weiterer Dienste könnten **Datenweitergabe und -verwertung** nicht mehr ohne weiteres zu überschauen sein. Einige Messenger- und Video-Dienste sind mit großen Konzernen verbunden, die auf benachbarten Geschäftsfeldern starke Positionen innehaben und ein „digitales **Ökosystem**“ unterhalten. Eine interne Weitergabe von Nutzerdaten könnte hier bereits ohne messenger-übergreifenden Austausch weite Kreise ziehen. Viele dieser Dienste können bislang nur genutzt werden, wenn Nutzerinnen und Nutzer Konten anlegen, die für verschiedene Funktionen genutzt werden. Teilweise wird bislang auch die Zustimmung zur Verarbeitung von Daten aus anderen Diensten vorausgesetzt.

Wie die Dienste mit den **Kontakten** der Nutzerinnen und Nutzer umgehen, ist schließlich ebenso essentiell für die Datenschutzqualität, da die Nutzerinnen und Nutzer hier nicht nur Verantwortung für die eigenen, sondern auch für Daten Dritter übernehmen. Ein eindeutig schützender Umgang sollte auch unter Interoperabilität bewahrt werden können.

Anhang: Einbezogene Dienste und Glossar

Einbezogene Dienste

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

Glossar

Begriff	Definition
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.

Begriff	Definition
Common Criteria (CC)	Internationaler Standard zur Prüfung und Bewertung der Sicherheitseigenschaften von IT-Produkten
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)	Das Gesetz über digitale Märkte (VO (EU) 2022/1925) zielt darauf, Bestreitbarkeit und Fairness von Märkten, auf denen große Online-Plattformen tätig sind, die von „Gatekeepern“ bereitgestellt werden, zu gewährleisten. Gemeinsam mit dem Gesetz über digitale Dienste ist es eines der Kernelemente der EU-Digitalstrategie.
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)	Das Gesetz über digitale Dienste (VO (EU) 2022/2065) zielt auf ein sicheres, vorhersehbares und vertrauenswürdiges Online-Umfeld, in dem Innovationen und insbesondere der Grundsatz des Verbraucherschutzes gefördert werden. Gemeinsam mit dem Gesetz über digitale Märkte ist es eines der Kernelemente der EU-Digitalstrategie.
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.

Begriff	Definition
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.
Identifier (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).
Key Pinning	Mechanismus zum Absichern des HTTPS-Protokolls gegen Man-in-the-Middle-Angriffe mit gefälschten, jedoch von einer anerkannten Zertifizierungsstelle (certificate authority) signierten Zertifikaten.
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.
Messaging Layer Security (MLS)	Messagingprotokoll, welches auf dem Double Ratchet Protokoll basiert und im Rahmen einer IETF-Arbeitsgruppe standardisiert wurde. Der Standard strebt ein verbessertes Gruppenmanagement sowie die Interoperabilität verschiedener Messenger an.
Messaging-System	Sammelbegriff für das gesamten System, das zum Messaging benötigt wird, bestehend aus Kommunikationsprotokoll, Anwendersoftware (App, Client), Serversoftware und Hardware.
MIMI- (More Instant Messaging Interoperability)-Arbeitsgruppe	Arbeitsgruppe der IETF, die an Lösungen für interoperables Messaging arbeitet und erstmals im Frühjahr 2023 zusammenkam.
Multiprotocol Clients / Multi (Protokoll-)Messenger	Software, die eine Vielzahl von Kommunikationsprotokollen beherrscht und den Gebrauch verschiedener Kommunikationsdienste über eine Oberfläche ermöglicht.
Nutzerin, Nutzer	Sammelbegriff für Organisatoren und Teilnehmende, die einen Messenger- oder Video-Dienst verwenden.

Begriff	Definition
OpenPGP	Standardisiertes Datenformat für verschlüsselte und digital signierte Daten. Auch wird das Format von Zertifikaten festgelegt, die landläufig auch als „Schlüssel“ bezeichnet werden.
Open Source	Software, deren Quelltext öffentlich und von Dritten eingesehen, geändert und genutzt werden kann.
Organisator, Organisatorin (Ersteller, Erstellering, Administrator, Administratorin, Host)	Sammelbegriff für eine Person oder Institution, die aktiv einen Austausch über Textnachrichten, Telefonie oder Videotelefonie starten und andere Teilnehmende dazu einladen kann sowie ggfs. weitere Berechtigungen inne hat (z. B. Stummschalten von Teilnehmenden, Löschen von Gruppen, Entfernen von Teilnehmenden 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 Nutzenden.
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.
RTSP (Real-Time Streaming Protocol)	Netzwerkprotokoll zur Steuerung der kontinuierlichen Übertragung von audiovisuellen Daten (Streams) oder Software über IP-basierte Netzwerke.
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)	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.
SRTP (Secure Real-Time Transport Protocol)	Verschlüsselte Variante des Real-Time Transport Protocol (RTP).

Begriff	Definition
SSO (Single Sign-on)	Nutzende können sich nach einer einmaligen Authentifizierung an einem Arbeitsplatz auf alle Rechner und Dienste, für die sie lokal berechtigt (autorisiert) ist, vom selben Arbeitsplatz zugreifen, ohne sich bei den einzelnen Diensten jedes Mal zusätzlich anmelden zu müssen.
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.
Teilnehmende, Teilnehmender	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.
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.
XMPP (Extensible Messaging and Presence Protocol)	Offener Standard eines Kommunikationsprotokolles, welches von der Internet Engineering Task Force (IETF) als RFC 6120, 6121 und 6122 veröffentlicht wurde.
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.