Universität Kassel

Messenger & Co: Das Unsichtbare regulieren?

Tahireh Panahi, Paul Zurawski

Forschungsmonitoring
Forschungsprojekte im Profil

Messenger und ähnliche Dienste sind aus dem modernen Kommunikationsalltag kaum noch wegzudenken. Die dortige Kommunikation findet teilweise „im Unsichtbaren" statt. Für an einem Chat unbeteiligte Dritte, wie Sicherheits- und andere Behörden, aber auch teilweise für die Diensteanbieter selbst ist die dort stattfindende Kommunikation aus einer Vielzahl von technischen und praktischen Gründen oftmals nicht einsehbar. Zudem findet dort keine Moderation statt und es gibt kaum technische Möglichkeiten der Überwachung oder auch nur der Kenntnisnahme durch Nutzermeldungen. Diese „Unsichtbarkeit" der Kommunikationskanäle ist aus einer Vielzahl von Gründen problematisch. Zum einen werden sie für Kriminalität und die Planung krimineller (insbesondere terroristischer) Taten genutzt. Zum anderen finden in ihnen Radikalisierungsvorgänge von der Öffentlichkeit unbemerkt statt. Eine aktuelle Digitalstudie ergab, dass 33 Prozent der Befragten die Vernetzung krimineller oder extremistischer Gruppen über Ende-zu-Ende-verschlüsselte Messenger als Gefahr für die Demokratie einschätzen (Initiative D21 e. V., 2022/2023).[1] Wie die Lage genau aussieht, ist indes unklar, da die meisten unsichtbaren Kommunikationsdienste auch für Wissenschaftler*innen keinen Datenzugang ermöglichen, wodurch nur wenige direkt auf Messenger- und Messenger-ähnliche Dienste bezogene empirische Studien vorliegen.

Aktuelle Regulierungen, wie das Netzwerkdurchsetzungsgesetz (NetzDG), der Medienstaatsvertrag (MStV) und der Digital Services Act (DSA), sind auf diese unsichtbare Kommunikation nicht anwendbar. Sie wurden gerade auf die sichtbaren, öffentlichen Bereiche sozialer Medien zugeschnitten. Mit Regelmäßigkeit werden daher technische und rechtliche Lösungen vorgeschlagen, um diese Schwierigkeiten zu bewältigen. Neue Regulierungsansätze finden sich etwa im Verordnungsentwurf der EU-Kommission für eine Verordnung zur Festlegung von Vorschriften für die Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern. Soweit sie *technisch* überhaupt umsetzbar sind, begegnen solche Vorschläge zahlreichen *rechtlichen* Bedenken. Insbesondere die Grundrechte der Nutzer*innen, aber auch der Diensteanbieter werden von solchen Lösungen erheblich beeinträchtigt.

In diesem Beitrag wird zunächst die Konfliktlage der unsichtbaren Kommunikationsräume anhand sozio-technischer Features der Dienste

[1] *Ironischerweise verwendet der aufgrund von Extremismus und massenweise Desinformation kritisierte Dienst Telegram derzeit mit Ausnahme der „geheimen Chats" standardmäßig keine Ende-zu-Ende-Verschlüsselung (vgl. https://telegram.org/faq/de#f-wie-verschlusselt-ihr-nun-genau-daten).*

erklärt. Sodann bemüht sich dieser Beitrag um die Ausleuchtung des Spannungsfeldes zwischen notwendigem Eingreifen und grundrechtlich gebotener Zurückhaltung und versucht, hier juristische Lösungsansätze zu skizzieren.

Unsichtbarkeit

In diesem Beitrag wird der Begriff der „Unsichtbarkeit" gewählt, um Kommunikationsvorgänge zu beschreiben, die für Dritte uneinsehbar in Messengerdiensten und ähnlichen Kanälen stattfinden.

Begriff

Zunächst ist anhand von technischen Features zu klären, was unter den Begriff der Unsichtbarkeit fällt. Einerseits fallen unter den Begriff die klassischen, dedizierten (inzwischen meist Ende-zu-Ende-verschlüsselten) Messengerdienste wie Signal, WhatsApp, Threema oder iMessage. Hinzu kommen aber auch hybride Dienste, die sowohl öffentliche als auch private Kommunikationsfunktionen in einer Anwendungsoberfläche vereinen, wie Telegram. Zudem können (untergeordnete) Messaging-Nebenfunktionen von Online-Plattformen, wie Facebook oder Instagram, LinkedIn, Twitter, aber auch von Spieleverkaufs- und Multiplayerplattformen wie Steam und Playstation Network oder Online-Spielen wie „World of Warcraft" unter diesem Begriff firmieren. Für Teile dieser „unsichtbaren" Kommunikationen haben sich in verschiedenen Kontexten die Begriffe „Going Dark" (insbesondere für die Nutzung Ende-zu-Ende-verschlüsselter Messengerdienste (siehe etwa Schulze, 2017, S. 23 ff.; Lindner & Unterreitmeier, 2023)), „Dark Social" (ursprünglich aus dem Bereich der Site Traffic Analyse (Madrigal, 2012)) oder „Black Box" (dann oft für einzelne Dienste oder nur Teile der Dienste) etabliert.[2] Doch über die vollständige technische Unmöglichkeit der Ausleuchtung der Kommunikation durch beispielsweise Strafverfolgungs- und Sicherheitsbehörden hinaus geht es bei der „unsichtbaren" Kommunikation auch um Räume, die nicht technisch, aber doch faktisch zumindest teilweise uneinsehbar sind, in denen die Kommunikation somit zu einem gewissen Grad unsichtbar ist.

[2] *Da die Begriffe „Dark Social" und „Black Box" eine diskriminierende Konnotation auslösen können, wird im weiteren Verlauf auf die Verwendung verzichtet.*

Schattierungen der Sichtbarkeit

Die Sichtbarkeit von Kommunikation ist keine absolute Größe, sondern weist unterschiedliche Grade auf. Dabei ist es gerade im Angesicht oftmals weitreichender, technische, organisatorische und nutzungsmodale Differenzen ignorierender Regulierungsvorschläge wichtig zu differenzieren, welcher Grad der (Un-)Sichtbarkeit es ist, der reguliert und besser ausgeleuchtet werden soll und wie dies tatsächlich umzusetzen ist – nur so können sinnvolle Regeln beschlossen werden.

Als vollständig unsichtbar ist solche Kommunikation zu werten, die nur den Teilnehmer*innen und ihren Endgeräten bekannt ist, die also nicht bei der Übertragung abgefangen oder (halb-)öffentlich mitgelesen werden kann. Hier sind vor allem Ende-zu-Ende-verschlüsselte Messenger, etwa die weit verbreiteten Dienste von WhatsApp, Signal und Threema (Beisch & Koch, 2021, S. 486 ff.), und die weniger verbreitete Ende-zu-Ende-verschlüsselte E-Mail (Berger, 2017) sowie das Dark Web zu nennen.

Technisch weniger geschützt, aber in den meisten Fällen den Blicken Unbeteiligter verborgen, ist die Kommunikation über abfangbare, aber ansonsten private Kanäle, wie un- oder lediglich durchgangsverschlüsselte Messengerdienste und -funktionen, Messenger- und Chat-Dienste mit privaten Servern oder Peer-to-Peer-Übertragung, E-Mail, SMS, und auch die Direktnachrichtenfunktionen zahlreicher sozialer Netzwerke und Online-Plattformen. Stattdessen schützt hier eine Kombination von Faktoren die Kommunikation des/der Einzelnen vor Einsicht: zunächst die schiere Anzahl an ausgetauschten Nachrichten, sodann die auf Seiten des Dienstanbieters organisatorisch und technisch nicht vorgesehene Einsichtnahme und zuletzt die Notwendigkeit, für einen umfassenden Überblick gezielte Abfangmaßnahmen bei einer Vielzahl von Nutzer*innen, Anbietern oder Datenübertragungswegen vorzunehmen. Im Einzelfall kann in diese Kommunikation Einsicht genommen werden, doch in ihrer Masse ist auch sie unsichtbar für Unbeteiligte.

In der öffentlichen Wahrnehmung der letzten Zeit als besonders gefährlich wahrgenommen, doch rein technisch eher wenig unsichtbar, sind geschlossene Gruppen als Teilbereich sozialer Medien. Hier findet (zumindest in der Theorie) eine Moderation durch die Gruppenverwaltung

und teils sogar den Diensteanbieter statt, und ein Mitlesen ist nach Mitgliedschaft in der Gruppe problemlos möglich – soweit keine technischen Hürden bestehen, ist auch ein technisches Auslesen der Inhalte am Backend meist kein Problem – hier ist es einzig die Unkenntnis über die Gruppen, die der Kommunikation in ihnen eine geringe Unsichtbarkeit gewährt. Insbesondere sehr mitgliedsstarke Gruppen sind ein interessantes Phänomen, da ihre Kommunikation durch ihre Mitgliederzahl gegebenenfalls als öffentlich gelten kann, aber zugleich für Außenstehende unsichtbar ist (öffentlich, aber unsichtbar).

Zuletzt sind die fast völlig sichtbaren Postings in öffentlichen Gruppen, Foren oder auf den News-Feeds sozialer Netzwerke zu bedenken – hier wird (auch gesetzlich vorgeschrieben) aktive Moderation betrieben.

*Akteur*innen der Unsichtbarkeit*

Verschiedene Akteur*innen haben aufgrund ihrer technischen und organisatorischen oder rechtlichen Stellung und Befähigung verschiedene Potenziale, die Unsichtbarkeit aufzuheben, und verschiedene Funktionen im Umgang mit der Kommunikation, weshalb eine Differenzierung zum besseren Verständnis der Problematik und auch möglicher Lösungsansätze hilfreich ist. In Anbetracht der Frage nach der Regulierung der Unsichtbarkeit werden hier lediglich die legitimen Akteur*innen betrachtet, Hacker*innen und Leaker*innen sowie andere Personen und Gruppen, die sich unerlaubten Zugang zur Kommunikation Dritter verschaffen, bleiben außen vor.

Während die meisten Nutzer*innen dadurch charakterisiert werden, lediglich (Kommunikations-)Inhalte (ihre eigenen, also von ihnen verschickte oder an sie gerichtete, sowie öffentliche) einsehen zu können, haben sie in manchen Diensten (teils sogar in den reinen Messengerdiensten) die Möglichkeit, meldend tätig zu werden und so an der Moderation von Inhalten mitzuwirken. Mitunter statten Dienste die Inhalteersteller*innen, neben der charakteristischen One-to-Many-Kommunikation, ebenfalls mit der Möglichkeit direkter Moderation, also des Löschens von Inhalten und des Auslesens weiterer organisatorisch-technischer Daten über die Nachricht/das Posting und den/die Nutzer*in, aus, wodurch die Diensteanbieter einerseits eigene Moderations- und Meldepflichten auslagern können, andererseits Inhalteersteller*innen eine gewisse Hoheit über ihre Content

Spaces erhalten. Die Diensteanbieter selbst, auf deren Servern die Inhalte liegen und deren Funktion in Übermittlung und Hosting der Inhalte und Kommunikation liegt, haben technisch Zugriff auf die Metadaten und, je nach Stufe der Verschlüsselung der Inhalte (Ende-zu-Ende oder lediglich Transport), möglicherweise sogar auf die Inhalte der Kommunikation. Ein tatsächliches Zugreifen erfolgt jedoch meist nur nach nutzerseitiger Meldung oder behördlicher Anfrage oder Anordnung.

Sicherheits- und andere Behörden und staatliche Akteur*innen erhalten in diesem System unsichtbarer Kommunikation auf drei Arten Einblick: Weitergabe oder Meldung von Inhalten durch andere Akteur*innen (beispielsweise Privatanzeigen strafbarer Inhalte von Nutzer*innen oder –teilweise verpflichtende – Meldungen und Anzeigen von Diensteanbietern von im Moderationssystem aufgefallenen strafbaren Inhalten), Frontend- oder menschlicher Zugriff durch manuelles oder automatisiertes Monitoring von mehr oder weniger sichtbaren Inhalten (Crawler für öffentliche Inhalte, Undercovermitgliedschaft in Gruppen oder direkte Kommunikation mit Einzelpersonen) und Backend- oder technischer Zugriff durch das Abfangen (und gegebenenfalls Entschlüsseln) der Inhalte auf den Servern oder Endgeräten, mit oder ohne Zustimmung von deren Eigentümern. Zu Weitergabe und Zugriff können die anderen Akteur*innen auch durch Regulierungen gezwungen werden, sodass, außerhalb unüberwindbarer technischer Hindernisse (die oft genug ebenfalls Angriffen durch den Gesetzgeber ausgesetzt sind (Krempl, 2023a; Holland, 2023)), eine theoretisch allumfassende Einsichtnahme ermöglicht werden könnte.

Konfligierende Interessenlage

Die beschriebene Unsichtbarkeit wird unterschiedlich rezipiert. Auf der einen Seite bestehen Vorzüge des Unsichtbaren im daraus resultierenden Schutz der Privatsphäre und der personenbezogenen Daten der Nutzer*innen. Zudem ist die Unsichtbarkeit für den Selbstschutz von zum Beispiel Whistleblowern oder aber auch politischer Aktivist*innen und marginalisierter Gruppen in Unrechtsregimen essenziell. Ella Jakubowska, EDRi, betont, dass die Privatsphäre nicht als eine Art abstraktes Konzept verstanden werden sollte, sondern als ein lebenswichtiges Menschenrecht

(Reuter, 2022). Ein aktuelles Beispiel stellt die Unterstützung protestierender Menschen im Iran im Zuge der „Frau Leben Freiheit“ Bewegung durch Messengerdienste wie Telegram und Signal, aber auch das Dark Web dar (Check Point Research Team, 2022). Auch russische Oppositionelle greifen auf solche Kommunikationswege zurück (Thier, 2020).

Auf der anderen Seite bestehen durch die Unsichtbarkeit auch rechtlich relevante Gefahren. Allgemein bietet Unsichtbarkeit Personen die Möglichkeit, unbemerkt Straftaten zu begehen (zumindest für die öffentlichen Kommunikationsräume von Telegram siehe Jünger & Gärtner, 2020). Zudem wird von einer Radikalisierung durch Messengerdienste ausgegangen, zum Beispiel von Reichsbürgergruppierungen (NZZ, 2022). Relevant ist auch, dass in solchen unsichtbaren Kommunikationsräumen Desinformation und Propaganda verbreitet werden (Jünger & Gärtner, 2021). Solche Inhalte sind nicht immer rechtswidrig, aber dennoch gesellschaftlich problematisch. Eine übergreifende Frage ist auch, inwiefern unsichtbare Kommunikation für eine Demokratie notwendig oder schädlich ist. Befürchtet wird etwa, dass dadurch, dass Debatten nicht mehr in der Öffentlichkeit geführt würden, die demokratische Konsensfindung unmöglich würde. So käme es zu einer Entfremdung aus der Demokratie (So etwa Florian Flade, zitiert von RND.de, 2021).

Ein weiteres grundlegendes Problem besteht darin, dass es kaum Datenzugangsmöglichkeiten für Wissenschaftler*innen zu unsichtbarer Kommunikation gibt. Mangels dieser empirischen Möglichkeit ist es schwierig, die Evidenz dieser Vor- und Nachteile überhaupt zu ermitteln. Die hier aufgeführten Vor- und Nachteile sind daher allenfalls heuristisch zu verstehen.

Schließlich ist die mangelnde effektive Rechtsdurchsetzung ein vorherrschendes Problem.

Grundrechtliches Spannungsverhältnis

Unsichtbare Kommunikation unterliegt einem besonderen grundrechtlichen Schutz, wenngleich auch auf dieser Ebene ein Spannungsverhältnis zu anderen Grundrechten besteht. Es können sowohl Grundrechte der Nachrichten verbreitenden Nutzer*innen, der Nachrichten empfangenden Nutzer*innen als auch der Unternehmen betroffen sein, soweit sie im Einzelfall als juristische Personen des Privatrechts grundrechtsfähig sind.

Fernmeldegeheimnis

Unsichtbare Kommunikation wird durch das Fernmeldegeheimnis nach Art. 10 Abs. 1 S. 1 GG beziehungsweise Art. 7, 8 GrCh geschützt. Dieses Grundrecht schützt die Vertraulichkeit der unkörperlichen Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs (Durner, 2022, S. 78; BVerfGE 67, 157 (172); 106, 28 (35 f.) 115, 166 (182); 120, 260 (309); 130, 151 (179)). Damit dient es dem Schutz der Privatsphäre (BVerfGE 85, 386 (395 f.)) und der Würde des Menschen (BVerfGE 113, 348 (391); Jarass, 2022, Rn. 1a). In erster Linie gewährleistet das Fernmeldegeheimnis die Vertraulichkeit des Kommunikationsinhalts und soll der öffentlichen Gewalt die Möglichkeit verwehren, sich Kenntnis vom Inhalt der Kommunikation zu verschaffen (Durner, 2022, S. 80). Als entwicklungsoffenes Auffanggrundrecht (ebd. S. 79) erfasst das Fernmeldegeheimnis alle technisch verfügbaren Mittel der unkörperlichen Kommunikation, so auch die in diesem Beitrag gegenständlichen Messengerdienste (KG, 2018, S. 119; Soiné, 2014, S. 248 ff.). Nach herrschender Meinung sind ausschließlich nichtöffentliche Kommunikationsvorgänge vom Fernmeldegeheimnis geschützt (Pagenkopf, 2018, Rn. 14b), was mit dem hier verwendeten Begriff der „Unsichtbarkeit“ deckungsgleich ist. Deutlich wird, wie wichtig auch in dieser Hinsicht eine Differenzierung der einzelnen Kommunikationsfunktionen bei Hybrid-Medien und Diensten mit Messenger-Nebenfunktionen ist. Allerdings wird gerade aufgrund dieser Hybridisierung der Dienste von anderen vertreten, *jegliche* Betätigung im Internet dem Schutz des Fernmeldegeheimnisses zu unterstellen (Marosi & Skobel, 2018, S. 837 ff.; Durner, 2022, S. 87). Dies würde jedoch zum einen nicht der historischen Entwicklung des Grundrechts, das zunächst auf das Fernmeldewesen angelegt war (Ogorek, 2023, Rn. 35), entsprechen. Zum anderen würde dies eine unsachgemäße Gleichbehandlung

von Ungleichem bedeuten, mit der die Bekämpfung der aus der unsichtbaren Kommunikation erwachsenden Gefahren erschwert werden würde.

In zeitlicher Hinsicht endet der Schutz des Fernmeldegeheimnisses in dem Moment, in dem die Nachricht bei dem/der Empfänger*in angekommen und der Übertragungsvorgang beendet ist (Durner, 2022, S. 89). Eingriffe in das Fernmeldegeheimnis können durch das Abhören, die Kenntnisnahme und das Aufzeichnen des Inhalts der Kommunikation, aber auch durch die Erfassung ihrer äußeren Umstände, die Auswertung des Inhalts und die Verwendung gewonnener Daten gegeben sein (Durner, 2022, S. 78).

Das Fernmeldegeheimnis aus Art. 10 Abs. 1 S. 1 GG ist Lex specialis zum allgemeinen Persönlichkeitsrecht, vor allem zum Recht auf informationelle Selbstbestimmung (Jarass, 2022, Rn. 2; BVerfGE 115, 166 (188 f.); 124, 43 (56 f.); 125, 260 (310); 155, 119 (Rn. 100)). Auch das Recht auf freie Meinungsäußerung aus Art. 5 Abs. 1 S. 1 GG tritt ebenfalls zurück, soweit die Schutzbereiche sich überschneiden (Jarass, 2022, Rn. 2; BVerfGE 113, 348 (364); 100, 313 (358);110, 33 (53); Durner, 2022, S. 289).

Meinungs- und Informationsfreiheit

Relevant ist auch die Meinungs- und Informationsfreiheit aus Art. 5 Abs. 1 S. 1 beziehungsweise S. 2 GG, Art. 11 GRCh und Art. 10 EMRK. Zwar tritt das Grundrecht auf freie Meinungsäußerung hinter das Fernmeldegeheimnis zurück (siehe oben). Indes ist bei manchen Kommunikationsfunktionen von vor allem Hybrid-Medien umstritten, ob eine öffentliche oder nichtöffentliche Kommunikation vorliegt (vor allem bei mitgliedsstarken Gruppen), sodass in diesen Fällen das Grundrecht auf Meinungsfreiheit nicht durch die Lex specialis verdrängt und damit relevant sein kann.

Die Meinungsfreiheit hat konstitutive Bedeutung für die menschliche Person und die freiheitlich-demokratische Ordnung (BVerfG, 1992, S. 1441). Art. 5 Abs. 1 S. 1 GG schützt Meinungsäußerungen und Tatsachenbehauptungen, welche Grundlage für die Meinungsbildung sind (Grabenwarter, 2022, S. 25). Ausgenommen vom grundrechtlichen Schutz ist – jedenfalls nach der Rechtsprechung des BVerfG – die Schmähkritik, also Wertungen von Personen oder Sachen, bei denen es primär um eine Verunglimpfung der Person oder Sache geht (Schulze-Fielitz, 2013, Rn. 70) sowie erwiesen unwahre und bewusst

unwahre Tatsachenbehauptungen (BVerfGE 54, 208 (219)). Auf europäischer Ebene erfolgt der Ausschluss solcher unwahrer Tatsachenbehauptungen grundsätzlich nicht auf Schutzbereichs-, sondern Rechtfertigungsebene, wobei dies für historische Tatsachen umstritten ist (Bernsdorff, 2019, Rn. 13).

Die Informationsfreiheit nach Art. 5 Abs. 1 S. 2 GG schützt grundsätzlich nur den Zugang zu allgemein zugänglichen Informationsquellen (Schulz, 2021, Rn. 30). Zum Teil wird jedoch von der Literatur vorgeschlagen, auch individuell eröffnete Informationsquellen in den Schutzbereich einzugliedern, um der Bedeutung solcher Kommunikationsvorgänge in der Demokratie Genüge zu tun (Schulz, 2021, Rn. 30).

Regulatorische Maßnahmen, die die Unsichtbarkeit der Kommunikation betreffen, könnten in die Meinungs- und Informationsfreiheit der Nutzer*innen eingreifen, da sie diese davon abhalten könnten, ihre Meinung frei durch das Medium ihrer Wahl kundzutun beziehungsweise Nachrichten vom Sender ihrer Wahl zu empfangen.

Berufs- und Eigentumsfreiheit beziehungsweise Unternehmensfreiheit

Zudem kann je nach Maßnahme die Berufs- und Eigentumsfreiheit der Unternehmer*innen aus den Art. 12 und Art. 14 GG beziehungsweise Art. 16. GrCh betroffen sein (Volkmann, 2019, Rn. 20; Jung, 2023, S. 149). Berufsfreiheit und Eigentumsgarantie schützen gemeinsam die (allgemeine) Wirtschaftsfreiheit beziehungsweise Freiheit der unternehmerischen Betätigung (Scholz, 2022, S. 109). Zur Berufsausübungsfreiheit zählen auch der Inhalt, die Bezeichnung, die in Anspruch genommenen Mittel und der gegenständliche Umfang der Berufsausübung (Kämmerer, 2021, Rn. 54). Die Unternehmensfreiheit nach Art. 16 GrCh umfasst auch die Art und Weise, wie man sein Unternehmen führt und betreibt (Jarass, 2021, Rn. 10). Auf die Art 12 und Art. 14 GG können sich inländische und ausländische natürliche Personen sowie nach Art. 19 Abs. 3 GG inländische juristische Personen des Privatrechts berufen (Axer, 2023, Rn. 37).

Regulatorische Vorgaben, die die Unsichtbarkeit von Kommunikation in Messengerdiensten betreffen, würden damit grundsätzlich auch in die Freiheit der Diensteanbieter aus den Art. 12 und 14 GG beziehungsweise Art. 16. GrCh eingreifen.

Geltende Rechtslage

Bislang gelten für unsichtbare Kommunikationsvorgänge andere Vorschriften als für öffentliche Social Media Beiträge. Die Differenzierung zwischen diesen beiden Kategorien setzt zumeist bei der Telemediendienst-eigenschaft an, welche von einschlägigen Normen voraussetzt wird (zum Beispiel § 1 Abs. 1 MStV, § 1 Abs. 1 S. 1 NetzDG). Die Telemediendienste werden nach § 1 Abs. 1 TMG negativ vom Telekommunikationsdienst abgegrenzt. Nur wenn kein Telekommunikationsdienst vorliegt, kann ein Telemedium gegeben sein (Setz, 2022, S. 182). Indes gelten Messagingfunktionen grundsätzlich als interpersonelle Telekommunikationsdienste im Sinne des § 3 Nr. 61 lit. b TKG und daher nicht als Telemedien. Damit sind relevante Normen des Netzwerkdurchsetzungsgesetzes und des Medienstaatsvertrags nicht anwendbar.

Mit dem Digital Services Act (DSA) hat die EU einen neuen Rechtsakt erlassen, der zu einem vertrauenswürdigen und sicheren Online-Umfeld beitragen soll (Erwägungsgrund Nr. 9 des DSA). Dieser ist gemäß Art. 3 DSA auf verschiedene Arten von Vermittlungsdiensten anwendbar. Die für den Online-Kommunikationskontext besonders relevanten Online-Plattformen umfassen gemäß Art. 3 lit. i) DSA jedoch nur die öffentlichen Kommunikationsfunktionen von Online-Plattformen. EG 14 stellt klar, dass interpersonelle Kommunikationsdienste im Sinne der Richtlinie (EU) 2018/1972, unter anderem Instant-Messaging-Dienste, nicht in den Anwendungsbereich fallen sollen. Problematisch ist dies indes für besonders mitgliedsstarke geschlossene Gruppen. Diese könnten durch ihre Mitgliederzahl als „öffentlich“ gelten. Hierfür mangelt es im DSA jedoch an ausreichenden Abgrenzungskriterien.

Dagegen sind auf Messengerfunktionen andere Gesetze anwendbar, so etwa das Telekommunikationsgesetz, das Telekommunikations-und-Telemedien-Datenschutz-Gesetz sowie die Polizeigesetze und Strafprozessordnung und das Geheimdienstrecht mit ihren Überwachungsregelungen. Auch im Digital Markets Act werden Messengerfunktionen angesprochen: Die Verordnung ist auch auf nummernunabhängige interpersonelle Kommunikationsdienste nach Art. 1 Abs. 2, Abs. 3 lit. b) DMA anwendbar, sofern diese „Torwächter“ (engl. Gatekeeper) im Sinne des Art. 2 Nr. 1 DMA sind. Indes bezwecken die interpersonelle Telekommunikationsdienste

betreffenden Vorschriften nicht, die oben genannten Gefahren, die von der unsichtbaren Kommunikation ausgehen, zu bekämpfen, sondern vielmehr, die „Bestreitbarkeit und Fairness der Märkte im digitalen Sektor" zu gewährleisten (EG 7 S. 1 DMA). Problematisch könnte es sein, dass Torwächter gemäß Art. 7 Abs. 1 DMA verpflichtet sind, für die Interoperabilität der grundlegenden Funktionen von nummernunabhängigen interpersonellen Kommunikationsdiensten mit den nummernunabhängigen interpersonellen Kommunikationsdiensten anderer Anbieter zu sorgen.

Auch der EU Verhaltenskodex gegen Desinformation enthält Verpflichtungen, die eigens Messengerdienste betreffen (Commitment Nr. 25, Commitment Nr. 6 Measure 5). Jedoch handelt es sich hierbei nicht um verbindliche Regelungen, sondern um eine Ko-Regulierung, mit grundsätzlich nur selbstverpflichtender Wirkung. Nur im Ausnahmefall kann in Verbindung mit Vorschriften des DSA eine zumindest mittelbare Bindungswirkung eintreten.

Regulierungsvorschläge im Diskurs

Um die Nachteile und Gefahren, die mit der unsichtbaren Kommunikation einhergehen, einzudämmen, sind grundsätzlich verschiedene Ansätze denkbar. Konkret sind einige Lösungsvorschläge im Diskurs, von denen manche bereits als Gesetzesvorschläge vorliegen:

a) Verordnungsentwurf zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (2022/0155 (COD) sogenannte „Chatkontrolle")
b) Geplantes Gesetz gegen digitale Gewalt
c) Entschlüsselung
d) Upload-Filter
e) Interoperabilität/offene technische Standards
f) Nutzerseitige Report-Funktionen
g) Offene APIs (Forscher*innen, Sicherheitsbehörden)
h) Content und Membership Moderationspflichten

Im Folgenden sollen zwei Regulierungsvorschläge näher beleuchtet werden.

Chatkontrolle

Vertieft werden soll an dieser Stelle die geplante Verordnung zur „Chatkontrolle“. Mit der vorgeschlagenen Verordnung sollen die bisher freiwilligen Scanning-Aktivitäten der großen Internetkonzerne (unter anderem Facebook/Meta, Microsoft, Google/Alphabet) von unverschlüsselten Messenger- und E-Mail-Nachrichten sowie gehosteten Dateien und gepostetem Content auf Kindesmissbrauchsdarstellungen verpflichtend gemacht und ausgeweitet werden, um dann auch bisher untätige Anbieter und nicht gescannte Dienste zu erfassen. Ähnliche Vorschläge finden sich in der Online Safety Bill im Vereinigten Königreich und dem US-amerikanischen STOP CSAM Act.

Hier soll die Unsichtbarkeit von Kommunikationskanälen also aufgehoben werden, um Kinder und Jugendliche gefährdende (und teils kriminelle) Inhalte aufzudecken und so zu deren Schutz beizutragen. Technisch müssten diese Kanäle dann auf vorgegebene Inhalte und Muster (automatisiert) gescannt werden. Geht es um bisher Ende-zu-Ende-verschlüsselte Messenger, bedeutet die Verpflichtung zur Überprüfung technisch die faktische Abschaffung dieser sicheren Kommunikationswege. Vollständig unsichtbare Räume im Sinne der obigen Konzeption würden damit zwar nicht verboten, aber faktisch verunmöglicht, rechtskonform angeboten zu werden.

Dies stellt einen massiven Eingriff in die oben dargelegten Kommunikationsgrundrechte dar und sieht sich zahlreichen Widersprüchen in Form der beschriebenen Interessen an unsichtbarer Kommunikation ausgesetzt (Tuchtfeld, 2022; Zurawski, 2022, 01240). Zudem nutzen auch die von diesen „Chatkontrollen“ eigentlich geschützten Kinder und Jugendlichen die unsichtbaren Kommunikationsräume für ihre Entwicklung in einem unbeobachteten Rahmen. Es drohte widersprüchlich eine Gefährdung der Privatsphäre und Schutzräume dieser sich entwickelnden jungen Menschen, indem beispielsweise einvernehmliches „Sexting“ zwischen Minderjährigen zum Auslöser von Strafverfolgung wird (Siepmann, 2022; dpa, 2022).

Diese massenhafte Chatkontrolle wäre somit ein nicht mit elementaren Aspekten der Kommunikationsgrundrechte vereinbarer Eingriff in die unsichtbare Kommunikation, was inzwischen auch zahlreiche Gutachten (selbst der dafür plädierenden EU-Organe) belegen (Meineck, 2023; Kurz, 2023; Krempl, 2023b).

Gesetz gegen digitale Gewalt

Weitere Vorschläge zur Bekämpfung der Gefahren, die von unsichtbarer Kommunikation ausgehen, finden sich im Eckpunktepapier des Bundesjustizministeriums zum geplanten „Gesetz gegen digitale Gewalt" (BMJ, 2023). Durch das Gesetz sollen künftig die Rechte der von digitalen Rechtsverletzungen Betroffenen gestärkt werden. Unter „digitaler Gewalt" werden dabei jegliche Persönlichkeitsrechtsverletzungen im digitalen Raum zusammengefasst (ebd. S. 1). Unter anderem soll die Rechtsdurchsetzung gegenüber Anbietern von Messengerdiensten verbessert werden. Konkret sind drei Verfahrensrechte geplant. Erstens soll die private Rechtsdurchsetzung durch ein gerichtliches Auskunftsverfahren gestärkt werden. Zweitens sieht das Eckpunktepapier einen Anspruch auf richterlich angeordnete Accountsperren vor. Als dritte Maßnahme ist vorgesehen, dass soziale Netzwerke dazu verpflichtet werden sollen, einen inländischen Zustellungsbevollmächtigten zu benennen.

Auswirkungen auf die Sichtbarkeit von Kommunikation hat vor allem der Auskunftsanspruch. Dieser soll sowohl auf Telemediendiensteanbieter als auch auf Anbieter von Messengerdiensten anwendbar sein (ebd. S. 3). Auf solche Telekommunikationsdienste im Sinne des § 3 Nr. 61 TKG ist das bisher bestehende Auskunftsverfahren nach § 21 Abs. 2 TTDSG mangels Erfüllung der Telemedieneigenschaft nicht anwendbar. Während das Auskunftsverfahren nach § 21 Abs. 2 TTDSG auf die Herausgabe von Bestandsdaten beschränkt war, sollen künftig auch Nutzungsdaten, zum Beispiel IP-Adressen, aber auch Inhalte der Kommunikation herausgegeben werden müssen, soweit dies verhältnismäßig und für die Rechtsverfolgung erforderlich sei. In einem Erläuterungspapier des Bundesjustizministeriums vom 25.04.2023 wurde klargestellt, dass hierunter auch Direktnachrichten, also One-to-one-Kommunikation, fallen sollen (BMJ, 2023). Dies ist hinsichtlich des Fernmeldegeheimnisses problematisch, da dieses sowohl die Informationen über Beginn und Dauer der Kommunikation als auch die Kommunikationsinhalte schützt (siehe oben). Ob der Eingriff hier gerechtfertigt werden kann, ist zweifelhaft. Zu begrüßen ist, dass die Maßnahme unter einem Richtervorbehalt stehen würde. Problematisch ist vor allem, dass die Maßnahme auf jegliche Persönlichkeitsrechtsverletzungen anwendbar wäre. Zudem ist es bedenklich, dass durch die neue Maßnahme Nutzer*innen davon abgehalten werden könnten, ihre

Meinung frei zu äußern, da sie den Auskunftsanspruch fürchten. Damit wäre der Auskunftsanspruch – zumindest in der geplanten Form – grundrechtswidrig und würde kein geeignetes Mittel gegen die Gefahren der unsichtbaren Kommunikation darstellen.

Fazit und Ausblick

Wie gezeigt wurde, sind die aktuellen Lösungsvorschläge des Verordnungsentwurfs zur Chatkontrolle und des Eckpunktepapiers zum Gesetz gegen digitale Gewalt nicht dazu geeignet, die Gefahren der unsichtbaren Kommunikation grundrechtskonform zu regulieren.

Anschließend an diese rechtliche Kritik muss auch ein faktischer Effekt bedacht werden. Je mehr ein technisch zugänglicherer Dienst überwacht, reguliert und/oder moderiert wird, desto mehr steigt die Nachfrage nach unzugänglicheren Diensten. Die eingeschränkten Nutzer*innen wandern in unsichtbarere, weniger regulierte und regulierbare Dienste ab. Hierbei handelt es sich vor allem um Dienste, die eine Free-Speech-Absolutism-Agenda verfolgen, womit zum Teil auch die Duldung rechtswidriger und problematischer Inhalte einhergeht (Hummel, 2021). Zudem sind diese Dienste durch ihre technischen Features der Filterblasenbildung und Radikalisierung förderlich. Dies wird etwa an Telegram deutlich, der als „Hafen der Verbannten“ fungierte, nachdem andere Social Media Konzerne ihre Moderationspraxis – auch aufgrund neuer Gesetze – verschärften (Jünger & Gärtner, 2020, S. 6). Durch die Nachfrage nach unzugänglicheren Diensten werden zudem immer mehr Angebote generiert. Beispiele der jüngsten Vergangenheit waren etwa zum Beispiel selbstlöschende, verschlüsselte Chats bei Telegram, DMs bei Twitter und die Umstellung des Facebook-Messengers zur E2E-Verschlüsselung.

Zurück im „Sichtbaren“ bleiben nun unbescholtene Nutzer*innen, die nun verstärkt Eingriffen in ihre Kommunikationsgrundrechte und Privatsphäre ausgesetzt sind. So lastet nicht nur eine negative Wirkung auf den Grundrechten unbescholtener Nutzer*innen. Durch die Abwanderungstendenzen in unsichtbarere Bereiche entsteht auch ein gegenteiliger Effekt für die Ziele der Sicherheit und Strafverfolgung. Zwar

werden die „Mainstream"-Kommunikationsdienste, wie die herkömmlichen Messengerdienste, in aller Regel ohnehin nicht von gut organisierten kriminellen oder terroristischen Organisationen zur Kommunikation verwendet. Jedoch können Radikalisierungsprozesse und Recruiting gerade in diesen Räumen erfolgen (Gerster et al., 2021).

Regulierung dieser „unsichtbaren" Bereiche, und insbesondere der Messenger-Dienste, muss also mit Fingerspitzengefühl und Augenmerk für die (grund-)rechtlichen und faktischen Nuancen und Widersprüchlichkeiten der Technologie vorgenommen werden und sich nicht in Schnellschüssen zur Sichtbarmachung erschöpfen.

Literatur

Axer, P. (2023). GG Art. 14 [Eigentum, Erbrecht und Enteignung]. In V. Epping, C. Hillgruber (Hrsg.), Beck'scher Online-Kommentar Grundgesetz. München: C.H. Beck.

Bernsdorff, N. (2019). GRCh Art. 11 Freiheit der Meinungsäußerung und Informationsfreiheit. In J. Meyer, S. Hölscheidt, *Charta der Grundrechte der Europäischen Union Kommentar*. Baden-Baden: Nomos Verlagsgesellschaft.

Bernzen, A. K., Grisse, K. & Kaesling, K. (2022). *Immaterialgüter und Medien im Binnenmarkt*. Baden-Baden: Nomos Verlagsgesellschaft.

Durner, W. (2022). GG Art. 10 [Brief-, Post- und Fernmeldegeheimnis]. In G. Dürig, R. Herzog & R. Scholz (Hrsg.), *Grundgesetz Kommentar*. München: C.H. Beck, 99.

Gerster, L. et al. (2021). *Stützpfeiler Telegram. Wie Rechtsextreme und Verschwörungsideolog:innen auf Telegram ihre Infrastruktur ausbauen*. Berlin: Institute for Strategic Dialogue.

Grabenwarter, C. (2022). GG Art. 5 Abs. 1 [Meinungs-, Presse-, Rundfunk-, Film- und Informationsfreiheit, Schranken], Art 5 Abs. 2. In G. Dürig, R. Herzog, & R. Scholz (Hrsg.), *Grundgesetz Kommentar.* München: C.H. Beck, 99.

Jarass, H. D. (2021). EU-Grundrechte-Charta Art 16 Unternehmerische Freiheit. In H. D. Jarass (Hrsg.), *Charta der Grundrechte der Europäischen Union Kommentar*. München: C.H. Beck.

Jarass, H. D. (2022). GG Art. 10 [Brief-, Post- und Fernmeldegeheimnis]. In H. D. Jarass, B. Pieroth (Hrsg.), *Grundgesetz für die Bundesrepublik Deutschland Kommentar*. München: C.H. Beck.

Jung, L. (2023). Schutz der Demokratie durch inhaltsneutrale Regulierung digitaler Medien. *DÖV, 4,* 141–150.

Jünger, J., Gärtner, C. (2020). *Datenanalyse von rechtsverstoßenden Inhalten in Gruppen und Kanälen von Messengerdiensten am Beispiel Telegram*. Düsseldorf: Landesanstalt für Medien NRW.

Jünger, J., Gärtner, C. (2021). *Die Verbreitung und Vernetzung problembehafteter Inhalte auf Telegram*. Düsseldorf: Landesamt für Medien NRW.

Kämmerer, J.-A. (2021). GG Art. 12 [Berufsfreiheit]. In I. v. Münch, P. Kunig (Hrsg.), *Grundgesetz-Kommentar*. München: C.H. Beck,

KG (2018). Akteneinsicht in TKÜ-Aufzeichnungen. *NStZ, 38 (2),* 119–120.

Lindner, J. F., Unterreitmeier, J. (2023). *Going dark – Signals Intelligence im IT-Zeitalter*. Tübingen: Mohr Siebeck.

Marosi, J., Skobel, E. (2018). Von Menschen und Maschinen. *DÖV, 20,* 837–845.

Ogorek, M. (2023). GG Art. 10 [Brief-, Post- und Fernmeldegeheimnis]. In V. Epping, C. Hillgruber (Hrsg.), *Beck'scher Online-Kommentar Grundgesetz*. München: C.H. Beck.

Pagenkopf, M. (2018). GG Art. 10 [Brief-, Post- und Fernmeldegeheimnis]. In M. Sachs (Hrsg.), *Grundgesetz Kommentar*. München: C.H. Beck.

Scholz, R. (2022). GG Art. 12 Berufsfreiheit. In G. Dürig, R. Herzog & R. Scholz, *Grundgesetz Kommentar*. München: C.H. Beck, 99.

Schulz, W. (2021). GG Art. 5 [Recht der freien Meinungsäußerung, Medienfreiheit, Kunst- und Wissenschaftsfreiheit]. In M. Paschke, W. Berlit, C. Meyer & L. Kröner (Hrsg.), *Hamburger Kommentar Gesamtes Medienrecht*. Baden-Baden: Nomos Verlagsgesellschaft.

Schulze-Fielitz, H. (2013). GG Art. 5 Abs. 1-2 [Meinungs- und Pressefreiheit, Rundfunk- und Filmfreiheit; Freiheit der Kunst und der Wissenschaft]. In H. Dreier (Hrsg.), *Grundgesetz-Kommentar*. Tübingen: Mohr Siebeck, Band 1.

Schulze, M. (2017). Going Dark? Dilemma zwischen sicherer, privater Kommunikation und den Sicherheitsinteressen von Staaten. *APuZ, 67 (46/47),* 23–28.

Setz, T. (2022). Desinformation in Messenger-Diensten und Hybrid-Medien – Sind NetzDG und MStV geeignete Blaupausen für die EU? In A. K. Bernzen, K. Grisse & K. Kaesling (Hrsg.), *Immaterialgüter und Medien im Binnenmarkt. Europäisierung des Rechts und ihre Grenzen* (S. 175-199). Baden-Baden: Nomos Verlagsgesellschaft.

Soiné, M. (2014). Personale verdeckte Ermittlungen in sozialen Netzwerken zur Strafverfolgung. *NZfS, 34 (5),* S. 248–251.

Volkmann, C. (2019). RStV § 59 Aufsicht. In G. Spindler & F. Schuster (Hrsg.), *Recht der elektronischen Medien Kommentar*. München: C.H. Beck.

Zurawski, P. (2022). EU-Kommission: Vorschlag „Chatkontrolle" – Verhältnisse der Überwachung. *ZD-Aktuell, 12,* 01240.

Internetquellen

Beisch, N., Koch, W. (2021). 25 Jahre ARD/ZDF-Onlinestudie: Unterwegsnutzung steigt wieder und Streaming/Mediatheken sind weiterhin Treiber des medialen Internets. *Media Perspektiven, 10/2021.* Abgerufen von https://www.ard-zdf-onlinestudie.de/files/2021/Beisch_Koch.pdf

Berger, D. (2017). Umfrage: Nur 16 Prozent der Deutschen verschlüsseln ihre Emails. *heise online*, 22.05.2017. Abgerufen von https://www.heise.de/news/Umfrage-Nur-16-Prozent-der-Deutschen-verschluesseln-ihre-E-Mails-3720597.html

Bundesministerium der Justiz (2023). Eckpunkte des Bundesministeriums der Justiz zum Gesetz gegen Digitale Gewalt. Pressemitteilung Nr. 25/2023 v. 12.04.2023. Abgerufen von https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/2023_Digitale_Gewalt.html?nn=110490

Check Point Research Team (2022). Hacker groups take to Telegram, Signal and Darkweb to assist protestros in Iran [Web Log Eintrag], 28.09.2022. Abgerufen von https://blog.checkpoint.com/2022/09/28/hacker-groups-take-to-telegram-signal-and-darkweb-to-assist-protestors-in-iran/

dpa (2022). Kinderschutzbund gegen anlasslose Scans verschlüsselter Nachrichten. *EU-Info*. Deutschland, 08.05.2022. Abgerufen von https://www.eu-info.de/dpa-europaticker/316232.html

Holland, M. (2023). Chatkontrolle: Spanien plädiert für EU-Verbot von Ende-zu-Ende-Verschlüsselung. *heise online*, 23.05.2023. Abgerufen von https://www.heise.de/news/Chatkontrolle-Spanien-plaediert-fuer-EU-Verbot-von-Ende-zu-Ende-Verschluesselung-9062428.html

Hummel, T. (2021). Messengerdienst Telegramm – Darknet für die Hosentasche. *Deutschlandfunk Kultur*, 24.08.2021. Abgerufen von Messengerdienst Telegram - Darknet für die Hosentasche (deutschlandfunkkultur.de)

Initiative D21 e. V. Digitalstudie 2022/2023, 38. Abgerufen von https://initiatived21.de/uploads/03_Studien-Publikationen/D21-Digital-Index/2022-23/d21digitalindex_2022-2023.pdf

Krempl, S. (2023a). „Going Dark": Schwedische EU-Ratsspitze startet Angriff auf Verschlüsselung. *heise online*, 26.01.2023. Abgerufen von https://www.heise.de/news/Going-Dark-Schwedische-EU-Ratsspitze-startet-Angriff-auf-Verschluesselung-7471023.html

Krempl, S. (2023b). EU-Ministerrat lehnt Datenentschlüsselung bei Chatkontrollen ab. *heise online*, 04.07.2023. Abgerufen von https://www.heise.de/news/EU-Staaten-Chatkontrolle-soll-ohne-Datenentschluesselung-auskommen-9207058.html

Kurz, C. (2023). Wissenschaftler warnen: Chatkontrolle ist der falsche Weg. *netzpolitik.org*, 04.07.2023. Abgerufen von https://netzpolitik.org/2023/wissenschaftler-warnen-chatkontrolle-ist-der-falsche-weg/

Madrigal, A. C. (2012). Dark social: We have the whole history of the web wrong. *The Atlantik*. Abgerufen von https://www.theatlantic.com/technology/archive/2012/10/dark-social-we-have-the-whole-history-of-the-web-wrong/263523/

Meineck, S. (2023). EU-Parlament: Ausschuss will Chatkontrolle an vier Stellen nutzen. *netzpolitik.org*, 29.06.2023. Abgerufen von https://netzpolitik.org/2023/eu-parlament-ausschuss-will-chatkontrolle-an-vier-stellen-stutzen/

NZZ (2022). NZZ Akzent: Täglich ein Stück Welt. *Neue Zürcher Zeitung*, 07.12.2022. Abgerufen von https://unternehmen.nzz.ch/nzz-akzent-taeglich-ein-stueck-welt-07-dezember-2022/

RND (2021). ARD-Sendung „Anne Will". Wurden „Reichsbürger" vor der Razzia gewarnt? Innenministerin Faeser: „Das war nicht gewollt". *Redaktionsnetzwerk Deutschland*, 12.12.2022. Abgerufen von https://www.rnd.de/politik/anne-will-am-11-12-2022-wurden-reichsbuerger-vor-razzia-gewarnt-faeser-das-war-nicht-gewollt-KL2HKEO225BCPF3DBUMHR6BNLY.html

Reuter, M. (2022). Werbeveranstaltung für Chatkontrolle: Kuscheln mit Kutscher. *netzpolitik.org*, 19.11.2022. Abgerufen von https://netzpolitik.org/2022/werbeveranstaltung-fuer-chatkontrolle-kuscheln-mit-kutcher/

Siepmann, C. (2022). Schülerin über Chatkontrolle: Jugendschutz bedeutet Datenschutz. *netzpolitik.org*, 25.05.2022. Abgerufen von https://netzpolitik.org/2022/schuelerin-ueber-chatkontrolle-jugendschutz-bedeutet-datenschutz/

Thier, J. (2020). Was haben Verschwörungstheoretiker, Oppositionelle und Terroristen gemeinsam? Sie nutzen Telegram. Was die App von Whatsapp unterscheidet. *Neue Zürcher Zeitung*, 26.10.2020. Abgerufen von https://www.nzz.ch/feuilleton/telegram-ein-messenger-fuer-oppositionelle-und-terroristen-ld.1579729

Tuchtfeld, E. (2022). „Vielen Dank, Ihre Post ist unbedenklich": Wie die Europäische Kommission das digitale Briefgeheimnis abschaffen möchte. *Verfassungsblog*, 25.05.2022. Abgerufen von https://verfassungsblog.de/vielen-dank-ihre-post-ist-unbedenklich/