Don’t shoot the Messenger

Erik Tuchtfeld 2021-12-21T14:22:29

Telegram hat als Messenger-App eine bemerkenswerte Karriere absolviert. In den letzten Jahren war es die „Lieblings-Chat-App des Islamischen Staates“ (2015), „Putins Internet-Albtraum“ und nunmehr die „Brutstätte für Corona-Verschwörungen“, was zu der bemerkenswerten Zusammenfassung der NZZ führte, Telegram sei die Gemeinsamkeit von „Verschwörungstheoretikern, Oppositionellen und Terroristen“. Dass Telegram seit Jahren kein Liebling staatlicher Stellen auf der ganzen Welt ist, zeigt unter anderem die Existenz eines eigenen Wikipedia-Artikels mit dem Titel „Government censorship of Telegram Messenger“. Nun hat auch die deutsche Politik Telegram als zentrales Problem für den gesellschaftlichen Frieden entdeckt. Die Nutzung von Telegram zur Verbreitung von Mordaufrufen und Beleidigungen, zur Organisation (auch) rechtswidriger Demonstrationen und schließlich zur Planung von Attentaten führte dazu, dass die neue Bundesinnenministerin Faeser (SPD) betonte, dass man die fehlende Kooperation Telegrams nicht hinnehmen werde. Auch Justizminister Buschmann (FDP) unterstützt und kündigt ein energisches Vorgehen gegen Telegram an. Die Landesinnenminister bringen Geosperren ins Spiel oder wollen den Vertrieb der App über die App Stores von Google und Apple verhindern.

Bei der zum Teil sehr berechtigten Kritik an Telegram scheinen aber von Zeit zu Zeit grundsätzliche Kategorien der Kommunikationsregulierung, insbesondere die Unterscheidung zwischen privater (und damit grundsätzlich geheimer) und öffentlicher Kommunikation, durcheinandergebracht zu werden. Weil die Kontrolle privater Kommunikation eine auch in anderen Kontexten immer stärker werdende Forderung in gesetzgeberischen Vorhaben ist, sei zunächst auf die äußerst engen verfassungsrechtlichen Voraussetzungen hierfür hingewiesen.

Private Kommunikation

Telegram ist primär ein Messenger für das Versenden von Nachrichten an Freunde und Familie. Das betrifft in seiner ursprünglichsten Form den *privaten* Austausch von Informationen zwischen mindestens zwei Personen. Diese Art des Nachrichtenaustauschs ist grundrechtlich auf deutscher (Art. 10 GG) und europäischer Ebene (Art. 7 und 8 GrCh) und einfach-rechtlich unter anderem im Strafrecht (§§ 202 ff. StGB) sowie im deutschen (§ 3 TTDSG) und europäischen (Art. 5 und 6 ePrivacy-Richtlinie, Art. 2 Nr. 4, 7 EKEK) Telekommunikationsrecht umfangreich geschützt ist. Wie jedes Grundrecht gilt auch das Kommunikationsgeheimnis nicht absolut, die private Fernkommunikation gewährleistet aber „die freie Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch von Informationen und [schützt] damit zugleich die Würde des Menschen“ (BVerfG, Rn. 64 ff.). Mit dieser engen Anbindung an die Menschenwürde macht das Bundesverfassungsgericht die zentrale Bedeutung des Kommunikationsgeheimnisses (im Grundgesetz als „Brief-,

Post- und Fernmeldegeheimnis“ bezeichnet) deutlich: Nur wer grundsätzlich darauf vertrauen kann, dass der Austausch von Gedanken mit anderen frei von staatlicher Überwachung ist und dass privat bleibt, was privat ist, kann sich frei entfalten, seine Persönlichkeit entwickeln und sich durch den vertraulichen Austausch mit anderen eine eigene Meinung bilden.

Der grundrechtliche Schutz des (Tele-)Kommunikationsgeheimnisses schützt – in seiner Ausprägung als Abwehrrecht – zuallererst einmal vor staatlicher Intervention: Möchte der Staat einen Blick auf den Gedankenaustausch zwischen zwei oder mehreren Personen über eine räumliche Distanz werfen, ist das nur in Ausnahmefällen möglich. Diese Ausnahmefälle sind gesetzlich in den jeweiligen Ermächtigungsgrundlagen definiert und setzen zum Zwecke der Strafverfolgung unter anderem den (konkreten) Verdacht für eine schwere Straftat sowie eine richterliche oder – bei Gefahr im Verzug – staatsanwaltschaftliche Anordnung voraus (§§ 100a, 100e StPO). Möglich ist (Tele-)Kommunikationsüberwachung aber auch zur Gefahrenabwehr (vgl. § 54 PolG-BW) oder durch Geheimdienste (vgl. § 1 G10).

Das ist aber nicht alles, der Staat muss nicht nur selbst das Telekommunikationsgeheimnis achten, sondern ist auch verpflichtet, es gegenüber privaten Übergriffen zu schützen (BVerfG, Rn. 13). Es ist dem Staat also nicht nur grundsätzlich untersagt, private Kommunikation zu überwachen, er muss auch dafür Sorge tragen, dass Private dies nicht tun.

Besonders virulent wird dies in der aktuellen Debatte rund um die „Chatkontrolle“. Nachdem der Europäische Kodex für die elektronische Kommunikation (EKEK), der es großen Anbietern wie Facebook Messenger, Google Mail und anderen – offenkundig aus Versehen – verboten hat, private Kommunikation zu überwachen, protestierten diese gemeinsam mit Vertretern der Zivilgesellschaft energisch gegen die damit verbundene Einschränkung der bisher üblichen Überprüfung, ob Abbildungen von Kindesmissbrauch (CSAM-Material) über ihre Dienste geteilt werden. In Reaktion darauf wurde kurz vor dem Inkrafttreten des EKEK in diesem Sommer eine auf zwei Jahre begrenzte Ausnahmeregelung geschaffen, die es den Diensten *erlaubt* (sie aber nicht dazu verpflichtet), die über ihre Messenger verschickten Inhalte auf das Vorhandensein von CSAM-Material zu scannen. Schon diese gesetzgeberische Regelung wird unter anderem von der ehemaligen deutschen EuGH-Richterin Colneric als Verletzung des Kommunikationsgeheimnisses eingestuft.

Darüber hinaus plant die EU-Kommission als langfristige Lösung nun nicht nur die *Erlaubnis* zum Scannen solcher Inhalte, sondern eine generelle *Verpflichtung* aller Messenger (also auch Signal, Telegram, Whatsapp etc.), Nachrichten auf CSAM-Inhalte zu überprüfen. So wichtig das Ziel der Bekämpfung der Verbreitung von CSAM-Material ist, so evident grundrechtswidrig wäre eine solche Lösung. Übertragen in die analoge Welt entspricht dieses Scanning einer Pflicht der Post, jeden einzelnen Brief zu öffnen und zu überprüfen, ob er bestimmtes Material enthält. Diese Maßnahme würde den Wesensgehalt des Telekommunikationsgeheimnisses verletzen.

Dieser Ausflug in das Recht der privaten Kommunikation macht deutlich, dass Messengeranbieter, sei es Telegram oder andere Dienste, nicht nur nicht verpflichtet sind, private Kommunikation auf bestimmte Inhalte zu überprüfen, es ist ihnen sogar grundsätzlich – außerhalb des Bereichs von CSAM-Inhalten – verboten.

(Teil-)öffentliche Kommunikation

Entscheidend ist insbesondere bei Telegram die Frage, was öffentliche und was private Kommunikation ist. Denn öffentliche Kommunikation kann sich nicht auf das Kommunikationsgeheimnis berufen. So wie privat bleiben muss, was privat ist, kann nicht geheim sein, was öffentlich ist. Die staatliche Kenntnisnahme von Informationen, die öffentlich einsehbar sind, stellt schon keinen Grundrechtseingriff dar (BVerfG, Rn. 308).

Jedenfalls die Channels auf Telegram wird man dem Bereich der öffentlichen Kommunikation zuordnen können. Hier können nur wenige Personen Inhalte posten, die von einer unbegrenzten Anzahl an Personen eingesehen werden können. Das ist keinesfalls per se gefährlich: So informiert beispielsweise das Bundesgesundheitsministerium über den Fortgang der Pandemie auf Telegram. Das Prinzip ähnelt stark klassischen Blogs im Internet, in denen auf einer Webseite eine oder mehrere Personen Beiträge mit der Weltöffentlichkeit des Internets teilen. Auch öffentliche Gruppen werden nicht durch das Telekommunikationsgeheimnis geschützt. Hier können in Gruppen von (theoretisch) bis zu 200.000 Mitgliedern Nutzerinnen und Nutzer miteinander schreiben, jeder und jede kann den Gruppen beitreten und sämtliche Inhalte sind auch schon vor Beitritt öffentlich einsehbar. Das scheint auch auf europäischer Ebene so gesehen zu werden, so hat der Rat im Gesetzgebungsprozess um den Digital Services Act (DSA), der sich ausdrücklich nicht auf Messenger beziehen soll (EU-Kommission, ErwGr 14), im November die klarstellende Ergänzung vorgeschlagen, dass Nachrichten in „öffentlichen Gruppen oder offenen Kanälen“ trotzdem unter den DSA fallen sollten (Rat der EU, ErwGr 14).

Spannend wird es jedoch bei „privaten“ Telegram-Gruppen, deren Inhalte und Mitglieder nur für andere Mitglieder sichtbar sind. Auch diese können bis zu 200.000 Personen aufnehmen. Dies ist bei Konkurrenten wie WhatsApp, Threema (jeweils bis zu 256 Mitglieder) und Signal (bis zu 1000 Mitglieder) deutlich limitierter. Hier wird die Einordnung kaum noch pauschal zu lösen sein, sondern sich im Einzelfall nach der Qualifikation der Zugangsbeschränkung richten. Wird beispielsweise der Einladungslink für eine private Gruppe – mit diesem kann man der Gruppe ohne weitere Bestätigung beitreten – weiterverbreitet, ist die Kommunikation innerhalb der Gruppe so öffentlich oder privat wie die Kanäle, über die der Einladungslink verbreitet wird. Wird er öffentlich (in einem Channel oder auf einer Webseite) geteilt, handelt es sich daher auch bei der Kommunikation innerhalb der „privaten“ Gruppe um öffentliche Kommunikation. Werden die Nutzerinnen und Nutzer der Gruppe aber selbst bei großen Gruppen einzeln ausgewählt, beispielsweise angelehnt an das Web-of-Trust-Prinzip, bleibt es dabei, dass die Kommunikation individualisiert und vom Telekommunikationsgeheimnis geschützt– und damit von staatlicher und privater Überwachung und Moderation frei ist.

Telegram als soziales Netzwerk

Die Qualifikation der Kommunikation als privat oder öffentlich ist entscheidend für die Verantwortlichkeit des Kommunikationsdienstes. Private Kommunikation (auch mit hunderten Teilnehmerinnen und Teilnehmern) darf von einem Messenger nicht allgemein überwacht oder moderiert werden (von der oben dargestellten Ausnahme für CSAM-Inhalte abgesehen). Telegram ist also nicht nur nicht verpflichtet, aktiv in diese Konversationen einzugreifen, es ist durch deutsches und europäisches Recht vielmehr gehindert, dies zu tun.

Anders sieht es bei privaten quasi-öffentlichen und öffentlichen Gruppen sowie Kanälen aus. Diese sind nicht grundrechtlich durch das Telekommunikationsgeheimnis geschützt, sodass die allgemeinen Haftungsprinzipien für Hostingdienste greifen (wie es auch beim Hosting von Webseiten der Fall wäre). Telegram muss dementsprechend nicht aktiv nach rechtswidrigen Inhalten suchen, ist aber nach Kenntnis zur Löschung verpflichtet (*notice and takedown*, §§ 7, 10 TMG, Art. 14, 15 eCommerce-Richtlinie). Besonders umstritten ist die Frage, inwieweit Telegram darüber hinaus dem NetzDG unterliegt und deshalb beispielsweise ein effektives Beschwerdeverfahren einrichten und eine Ansprechperson im Inland benennen müsste (§§ 3, 5 NetzDG). Das Bundesjustizamt bejaht dies und hat (mit Screenshots den rechtswidrigen Zustand belegend!) Telegram eine – bisher unzustellbare – Aufforderung zur Anhörung in einem Bußgeldverfahren geschickt. Dabei konzentrierte sich die Debatte bisher vor allem auf die Frage der hierfür notwendigen Gewinnerzielungsabsicht. Die wird vom Bundesjustizamt bejaht, seitdem Telegram angekündigt hat, sich zukünftig auch durch Werbung finanzieren zu wollen. Dass trotz möglicher Gruppengrößen von 256 beziehungsweise 1000 Personen bisher weder WhatsApp noch Threema in den Fokus des Bundesjustizamtes gerieten, spricht dafür, dass auch das Bundesjustizamt private Gruppen, auch wenn sie hunderte Mitglieder haben, als die Anwendung des NetzDG ausschließende „Individualkommunikation“ einstuft (§ 1 NetzDG).

Das Recht und seine Durchsetzung

Telegram verletzt seine rechtlichen Pflichten. Sowohl im Hinblick auf ganz klassische notice-and-takedown-Verfahren als – wohl – auch bezüglich besonderer Verpflichtungen, die ihm durch das NetzDG auferlegt werden. Es ist für unseren demokratisch verfassten Staat mehr als unbefriedigend, weil sich ein privater Akteur den demokratisch beschlossenen Regeln entzieht. Durchsetzungsmöglichkeiten gibt es kaum: Telegram sitzt in Dubai – derzeit scheitert es schon an der Zustellung eines Anhörungsschreibens – und betont, dass es jederzeit seinen Sitz ändern werde, wenn sich die Arbeitssituation dort verschlechtert.

Erfolgsversprechender scheint es nun, Druck auf Google und Apple auszuüben, die mit ihrer Hoheit über die App Stores massiven Einfluss ausüben können. Trotzdem ist dieser Weg mehr als bedenklich: Die Entscheidungshoheit der Gatekeeper, die immer wieder kritisiert wird und das Gegenmodell zu einem offenen, freien

Internet darstellt, sollte nicht genutzt werden, um eigene Ziele durchzusetzen. Würde man diese Maßnahme auf die informatische Welt außerhalb der Smart Devices (Smartphone, Tablets etc.) übertragen, wäre sie in etwa vergleichbar mit der Anordnung gegenüber Microsoft, dass auf Windows bestimmte Programme nicht mehr von den Nutzerinnen und Nutzern installiert werden dürfen. In der Welt der PCs undenkbar, sollte staatliche Regulierung sich den Marktmissbrauch der Gatekeeper nicht zunutze machen – und sich damit selbst in Abhängigkeit begeben –, sondern ihn bekämpfen.

Dazu kommen praktische Bedenken: Bereits bestehende Installationen würden nach wie vor funktionieren, nur Updates könnten nicht mehr ausgeliefert werden. Außerdem ist Telegram nicht nur ein Messenger für mobile Betriebssysteme, sondern bietet auch davon unabhängige Desktopclients, deren Verbreitung aufgrund der im Vergleich äußerst offenen Konzeption von PC-Betriebssystemen nicht eingeschränkt werden kann. Der Messenger ist zudem als offenes System mit einer umfangreichen Schnittstelle (API) konzipiert, sodass es bereits jetzt dutzende alternativer Apps gibt, die Zugriff auf das Telegram-Netzwerk mit all seinen Kontakten, Channels und Gruppen bieten. Möchte man die Nutzung des Netzwerks unterbinden, müssten also auch die Programme vieler unabhängiger Entwicklerinnen und Entwickler gesperrt werden. Andere Alternativen wie beispielsweise Geoblocking sind nicht nur grundsätzlich abzulehnen, sondern auch nicht umsetzbar, wie Russland in jahrelangen Versuchen bewiesen hat.

Ein anderer Angriffsvektor ist der Aspekt, der erst die Anwendbarkeit des NetzDG ausgelöst hat: Die Monetarisierung von Telegram, also die Finanzierung durch Werbung. Wenn Unternehmen solche Werbung nicht auf Telegram schalten, wird der Dienst mittelfristig reagieren müssen. Bereits in der Vergangenheit hat Telegram in der Folge öffentlichen Drucks beispielsweise gezielt öffentliche IS-Kanäle abgeschaltet und hat eine Kontaktadresse für die Löschung rechtswidrigen Materials in öffentlichen Kanälen eingerichtet.

Staatliche Verantwortung wahrnehmen

Keine dieser Maßnahmen, sei es Druck über die Gatekeeper oder über die Monetarisierung, wird aber kurzfristig Wirkung entfalten. Außerdem werden sie auch keine Auswirkungen auf privaten Gruppen (mit ggf. hunderten Mitgliedern haben), in denen Hass und Hetze geteilt oder sogar terroristische Attentate geplant werden. Das betrifft nicht nur Telegram, sondern auch jeden vergleichbaren Anbieter. Diese private Kommunikation darf von den Diensten nicht allgemein überwacht werden.

Deshalb ist es umso wichtiger, dass der Staat seine Verantwortung im Internet stärker wahrnimmt und Rechtsdurchsetzung nicht als primäre Aufgabe der Privaten versteht. Öffentliche Kanäle und Gruppen sind für Ermittlungsbehörden ohne Weiteres einsehbar und werden oft von – in rechten Kreisen – prominenten Persönlichkeiten unter bürgerlichem Namen betrieben. Man denke hierbei nur an den Kanal von Attila Hildmann, der Monate lang strafbare Inhalte verbreiten konnte, bevor die Ermittlungsbehörden aktiv wurden, und der sich dann noch ins Ausland absetzen konnte. Werden Straftaten in diesem (digitalen) öffentlichen Raum

begangen, ist es Aufgabe des Staates, die Täterinnen und Täter zur Verantwortung zu ziehen. In großen geschlossenen Gruppen, bei denen der Verdacht besteht, dass Straftaten begangen werden, sollten verdeckte Ermittlerinnen und Ermittler eingesetzt werden (zu den geringen verfassungsrechtlichen Hürden u.a. BVerfG, Rn. 310). Dass die Mordpläne gegen den sächsischen Ministerpräsidenten durch ein Team von Investigativjournalistinnen und -journalisten von frontal21 aufgedeckt wurden, die ohne größeren Aufwand einer zunächst öffentlichen und dann privaten Telegramgruppe beitraten, zeigt, dass ganz klassische Ermittlungsarbeit der Schlüssel zur Abwendung dieser Gefahren sein kann. Ein allzu verengter Fokus auf die verwendete Technik statt auf die Menschen, die sich radikalisieren, wird das Problem nicht lösen können.
