PROTECT THE STACK

Infrastructure Providers Should Not Be Content Police

Schutz des Technologie-Stacks: Die Inhaltskontrolle ist nicht Aufgabe von Infrastrukturanbietern

Viele Menschen glauben, dass die Anbieter von Internetinfrastruktur mehr Verantwortung bei der Überwachung von Onlineinhalten und -aktivitäten übernehmen sollten. Einige Anbieter entscheiden ohne Zwang, Eingriffe vorzunehmen. Das ist ein gefährlicher Trend, dem Einhalt geboten werden sollte.

Die Forderung, alle Parteien des „Stacks“ in den Kampf gegen Hassrede einzubinden, mag verständlich sein. Ein solches Vorgehen bringt jedoch auch unbeabsichtigte Folgen mit sich, vor allem für die schwächsten Nutzer und Nutzerinnen. Von wenigen Ausnahmen abgesehen, sollten Regierungen solche Interventionen nicht anordnen, und Infrastrukturunternehmen sollten Inhalte nicht von sich aus zensieren.

Hintergrund

NutzerInnen und politische Entscheidungsträger kennen Plattformen wie Facebook, Twitter und YouTube gut. Aber diese Dienste sind nicht das Internet. Tatsächlich hängt das Funktionieren von Onlinekommunikation und -handel von einer breiten Palette an Dienstanbietern ab. Hierzu zählen Internetdienstanbieter und Telekommunikationsunternehmen (Comcast, Orange, MTN, Airtel, Movistar, Vodafone usw.), Domänenregistrierungsstellen (z. B. Namecheap, GoDaddy), Supportservices (z. B. Amazon Web Services), Zertifizierungsstellen (z. B. Let’s Encrypt), Zahlungsabwickler (u. a. PayPal und M-Pesa), E-Mail- sowie Chatanbieter und viele weitere. Zusammen werden diese Anbieter manchmal als der sog. „Technologie-Stack“ bezeichnet.

Die meisten NutzerInnen verwenden das Internet, ohne sich Gedanken über die Infrastrukturdienste zu machen, die ihm zugrunde liegen. Für die Meinungsäußerung, die Privatsphäre und die Sicherheit im Internet sind diese Dienste jedoch unerlässlich. Wenn also diese Anbieter – von denen viele wenig oder keinen Kontakt zu den NutzerInnen haben – aufgrund von Inhalten Eingriffe vornehmen, können ihre Entscheidungen riesige Auswirkungen auf die Menschenrechte haben, die nur schwer oder vielleicht gar nicht wieder rückgängig gemacht werden können.

Wo die Probleme und Gefahren für die Meinungsäußerung und Privatsphäre liegen, hängt von der Art des Dienstes ab. Jedoch spielen bei jedem Infrastrukturanbieter einige oder alle der folgenden Aspekte eine Rolle. Zusammengenommen zeigen sie deutlich,

warum sich Infrastrukturanbieter – mit wenigen Ausnahmen – aus der Überwachung von Inhalten heraushalten sollten.

Was versteht man unter „Technologie-Stack“?

„Stack“ ist ein Begriff aus der Informatik bzw. Softwaretechnik und bezeichnet eine Reihe von Werkzeugen, Prozessen, Programmiersprachen und Mechanismen, die gemeinsam zur Entwicklung einer Anwendung oder eines Produkts verwendet werden. Im Rahmen dieses Artikels wird der Begriff verwendet, um die Dienstanbieter, Plattformen, Prozesse und sonstigen Komponenten zusammenzufassen, die die Grundlage für das Internet, so wie wir es heute kennen, bilden.

Der Technologie-Stack schließt Plattformen für nutzergenerierte Inhalte, beispielsweise Facebook oder Twitter, ebenso ein wie die schon erwähnten Infrastrukturanbieter. Ganz oben im Stack befinden sich die Social-Media-Plattformen, während die Anbieter der Kerninfrastruktur – wie Ihr Internetdienstleister – ganz unten zu finden sind. Dazwischen liegen zahlreiche andere Dienste wie Zahlungsabwickler und Registrierungsstellen.

Die Gefahren für die Menschenrechte

1. Die meisten Infrastrukturdienste sind nicht in der Lage, Interventionsmaßnahmen nach dem Verhältnismäßigkeitsprinzip umzusetzen.

Die meisten Plattformen verfügen über eine ganze Reihe von Moderationsmöglichkeiten. Im Gegensatz dazu können Infrastrukturdienste häufig nicht so gezielt eingreifen, wie es nach Menschenrechtsstandards geboten ist. Twitter blockiert bestimmte Tweets; Amazon Web Services sperrt ganze Websites und Konten. Die Eingriffe betreffen damit weit mehr als den anstößigen Kommentar, der Anlass für die Maßnahme war. Besonders schlimm ist es, wenn Regierungen Telekommunikationsdienste vereinnahmen, um im gesamten Land das Internet zu kontrollieren.

Auch auf Domänenebene finden bedenkliche Interventionen statt, wenn beispielsweise Registrierungsstellen, die Einwendungen gegen Äußerungen auf einer Website haben, nicht nur diese Äußerungen ins Visier nehmen, sondern die gesamte Website sperren oder ihre Registrierung aufheben. So berichtet ARTICLE 19 über mehrere Fälle von „DNS-Missbrauch“, in denen die Aussetzung und Löschung von Domänennamen als Mittel zur Unterdrückung unliebsamer Meinungen diente.

Hier lassen sich Parallelen zum Urheberrecht ziehen, wo Domänennamen-Registrierungsstellen und Hostinganbieter wegen Rechtsverletzungen

im Zusammenhang mit einem einzelnen Dokument ganze Websites abschalten. Manchmal sind einzelne Dienste auch in der Lage, direkten Kontakt mit einer Nutzerin/einem Nutzer, deren/dessen Beitrag gegen Regeln verstößt, aufzunehmen und sie bzw. ihn um Löschung zu bitten. Kommt die Nutzerin oder der Nutzer dieser Bitte nicht nach, bleibt dem Dienst jedoch nur das harte Mittel der vollständigen Entfernung bzw. Sperre. Zudem gibt es bei einigen Diensten keine praktikable Möglichkeit, in irgendeiner Form direkt mit InhaltsurheberInnen zu kommunizieren.

2. Sich hiergegen zu wehren oder Rechtsmittel einzulegen ist vor allem für weniger einflussreiche NutzerInnen äußerst schwierig.

Die Menschenrechtsstandards und Grundsätze eines ordnungsgemäßen Verfahrens verlangen, dass Dienstanbieter NutzerInnen vor der Löschung oder Sperrung ihrer Beiträge bzw. ihres Konto informieren und ihnen die Möglichkeit geben, dagegen vorzugehen. Auf Infrastrukturebene sind solche Benachrichtigungen und das Einlegen von Rechtsmitteln größtenteils unmöglich. Häufig können Infrastrukturdienste mit InternetnutzerInnen nicht auf unmittelbarem Weg kommunizieren, d. h. die Dienste haben weder zur Urheberin/zum Urheber des anstößigen Kommentars noch zu ihrem/seinem Publikum direkten Kontakt. Im Gegensatz zu Plattformhosts, die an der Stelle eines entfernten Beitrags einen erklärenden Hinweis hinterlassen können (in der Praxis wird diese Maßnahme auch als „Tombstoning“ bezeichnet), fehlen Infrastrukturanbietern in der Regel die praktischen Möglichkeiten, NutzerInnen darüber zu informieren, wie und warum der Zugang zu Inhalten eingeschränkt wurde.

Hat ein Benutzer oder eine Benutzerin beispielsweise von einem Freund einen Link erhalten, der nicht funktioniert, können die beiden nicht ohne weiteres feststellen, ob das Problem ein fehlerhafter Link ist, der Besitzer der Website diese selbst offline geschaltet hat oder ob sie gesperrt wurde. NutzerInnen eines Dienstes, der von einem Zahlungsabwickler abhängt, stellen möglicherweise erschrocken fest, dass der Dienst nicht mehr verfügbar ist. Der Grund? Der Abwickler hat alle Zahlungen an diesen Dienst eingestellt, ohne die NutzerInnen zu informieren. So konnte Uber in Argentinien über Nacht keine Geschäfte mehr machen, nachdem ein Zahlungsabwickler per Gerichtsbeschluss dazu aufgefordert wurde, alle Zahlungen an den Dienst zu blockieren.

In der Kette vom Beitragsersteller bis zum Publikum sind NutzerInnen an die Geschäftsbedingungen jedes einzelnen Dienstanbieters gebunden, auch wenn sie gar nicht wissen, um welche Dienste es sich handelt oder wie sie diese kontaktieren können. Angesichts der möglichen Folgen von Verstößen und der Schwierigkeit, sich in den Einspruchsverfahren von unsichtbaren Diensten zurechtzufinden (so denn ein solches Verfahren überhaupt existiert), vermeiden viele NutzerInnen es lieber, kontroverse Meinungen zu veröffentlichen. Wenn zwischen einem Dienstanbieter und den BeitragserstellerInnen bzw. deren Publikum keine Beziehung besteht, ist es für das

Unternehmen auch wesentlich einfacher und preiswerter, Websites insgesamt zu sperren, als eine differenzierte Analyse des Nutzerkommentars vorzunehmen.

3. Eingriffe auf Infrastrukturebene haben Nebenwirkungen, die weniger einflussreiche Gruppen unverhältnismäßig stark beeinträchtigen.

Diejenigen, die Macht und Einfluss haben, nutzen allzu oft alle Zensurmethoden aus, um unpopuläre Stimmen verstummen zu lassen. So überrascht es denn auch wenig, dass das Blockieren der Infrastruktur ein beliebtes Vorgehen autoritärer Regierungen darstellt. Während der sozialen Unruhen in Ecuador im Oktober 2019 sahen sich InternetnutzerInnen dort wiederholt mit Netzblockaden konfrontiert. Die nigerianische Regierung zwang Internetdienstanbieter zu einer monatelangen Twitter-Sperre. Infolge einer zu weitgehenden Anwendung von US-Sanktionen hat AWS iranische NutzerInnen aus seinen Diensten ausgesperrt. Unter Berufung auf US-Vorschriften verweigerte Cloudflare einer Mastodon-Instanz, die eine in Australien ansässige Gruppe von SexarbeiterInnen gehostet hatte, den Dienst. Dazu kommen all jene Länder, die das Internet ganz abgeschaltet haben.

Selbst wohlmeinende EntscheidungsträgerInnen messen der Meinung von Randgruppen häufig nicht genügend Bedeutung bei. Auf Plattformebene tragen Unternehmen, die Inhalte moderieren, immer wieder dazu bei, Vorurteile gegenüber marginalisierten Gemeinschaften zu bestätigen und zu verstärken. Beispiele gibt es zuhauf: Als die #MeToo-Bewegung gerade auf ihrem Höhepunkt war, stufte Facebook die Aussage „Männer sind Müll“ als Hassrede ein. Twitter berief sich auf das Schikaneverbot, um das verifizierte Konto eines prominenten ägyptischen Foltergegners zu deaktivieren. Verschiedene Entscheidungen zur Inhaltsmoderation hinderten farbige Frauen daran, Freunden und Followern über Schikanen zu berichten, denen sie ausgesetzt waren. Twitter zensierte Tweets mit dem Wort „queer“, unabhängig vom Kontext als anstößig.

Selbst PatientInnen, die sich verschreibungspflichtige Arzneimittel nicht leisten können, sind davon betroffen. In dem Versuch, die Verwendung des Wortes „Opioid“ und ähnlicher Begriffe in Hashtags zu unterbinden, schloss oder sperrte Instagram Konten, von denen „anscheinend“ Opioide verkauft wurden. Dies führte u. a. zur Schließung des PharmacyChecker-Kontos, das selbst keine Arzneimittel vertreibt, sondern nur Verifizierungs- und Preisinformationen zu Online-Apotheken für PatientInnen und Pflegekräfte bereitstellt, die Medikamente aus dem Ausland beziehen wollen.

Nichts spricht dafür, dass Infrastrukturunternehmen besser als Plattformen in der Lage sind, solche Moderationsentscheidungen zu treffen. Viele Anhaltspunkte lassen vermuten, dass sie hierfür schlechter aufgestellt sind.

4. Staatliche und private Akteure könnten versucht sein, Zensurmechanismen für ihre Zwecke zu nutzen und die Kontrollen zu verstärken.

Einmal etablierte Zensurmechanismen können staatlichen, staatlich geförderten und privaten Akteuren neue Instrumente an die Hand geben, um Einfluss auf den öffentlichen Dialog zu nehmen. Sobald Verfahren und Instrumente zur Beeinflussung der Meinungsäußerung entwickelt oder ausgeweitet werden, können die Unternehmen mit einer Flut von Forderungen rechnen, diese in größerem Umfang anzuwenden. Auf Plattformebene setzen staatliche sowie staatlich geförderte Akteure Kontrollinstrumente systematisch dazu ein, um abweichende Meinungen zu unterdrücken. Cloudflare, ein Unternahmen, das Schutz vor DDos-Angriffen und zahlreiche andere Dienste bietet, berichtet, dass es, nachdem es seine Sicherheitsdienste für eine Neonazi-Website mit Verschwörungstheorien eingestellt hatte, einen dramatischen Anstieg von Anfragen autoritärer Regime verzeichnete, die Menschenrechtsorganisationen in gleicher Weise behandelt sehen wollten.

Auf dem Gebiet des Urheberrechts nutzen private Akteure regelmäßig einfache Verfahren zur Entfernung von Inhalten, um Kritiker zum Schweigen zu bringen. Es ist unwahrscheinlich, dass es auf der Infrastrukturebene anders sein wird.

5. Mangelnder Wettbewerb sowie Wechselkosten machen es schwer bis unmöglich, bestimmte Unternehmen für Fehler und Machtüberschreitungen zur Verantwortung zu ziehen.

Wenn ein Internetdienstanbieter die Abschaltung eines Accounts beschließt, kann die Nutzerin/der Nutzer in vielen Teilen der Welt nicht auf einen anderen Anbieter ausweichen; sie oder er wird faktisch vom Netz ausgeschlossen. Auf anderen Ebenen des Technologie-Stacks ist die Auswahl größer. So kann eine Nutzerin/ein Nutzer, deren/dessen Domänenname eingefroren wurde, mit seiner/ihrer Website zu einem anderen DNS-Anbieter wechseln. Bloß, weil es Ausweichmöglichkeiten gibt, ist das Problem jedoch nicht gelöst. Kosten und Aufwand eines Anbieterwechsel müssen ebenfalls berücksichtigt werden. Eine billige oder einfache Alternative ist eher selten. Mitunter sind staatliche Interessenvertreter zudem eng mit den Infrastrukturunternehmen verbandelt – so hält die kenianische Regierung 35 % der Anteile an der Telekommunikationsfirma Safaricom. Und selbst wenn ein Wechsel leicht möglich ist, nützt das nichts, wenn sämtliche Anbieter auf einer bestimmten Ebene des Stacks die gleichen Inhalte, Beitragsersteller und/oder Standpunkte zensieren, weil sie es für richtig halten oder diesbezüglich unter Druck gesetzt werden. Das trifft umso eher zu, als dass es sich um kleinere Dienstanbieter handelt, die mächtigen Regierungen und privaten Akteuren wenig entgegenzusetzen haben.

6. Interventionsvorgaben können kontraproduktiv sein.

Durch Eingriffe in die Onlinekommunikation werden die Ziele, denen die Eingriffe eigentlich dienen sollen, zum Teil untergraben. So hat das Bemühen, „extremistische“ Inhalte zu unterbinden, dazu geführt, dass Beiträge von JournalistInnen und MenschenrechtsaktivistInnen, die über Terrorismus und andere Verbrechen berichtet haben, blockiert oder gelöscht wurden. Durch den Druck, den Zugang zu Internetdiensten in bestimmten Ländern zu blockieren, gestaltet sich die Hilfe schwierig für Menschen, die einer staatlichen Zensur entgehen wollen und Zugang zu korrekten Informationen suchen.

7. Zensurmaßnahmen auf Infrastrukturebene können grundlegende Internetprotokolle aushebeln und ein Sicherheitsrisiko darstellen.

Bestimmte Zensurmaßnahmen von Infrastrukturanbietern – etwa die Einführung von Deep Packet Inspection (DPI) im Netz oder die Blockierung von DNS-Abfragen – können die Architektur des Internets nachteilig zulasten von Privatsphäre und Sicherheit verändern. Wenn DNS-Anbieter beispielsweise damit anfangen, Anfragen für bestimmte Domänen allein aufgrund ihrer Inhalten umzuleiten, ist das DNS vor böswilligen Manipulationen kaum noch sicher, da Computer „gute“ Umleitungen nicht von Website-Spoofingangriffen unterscheiden können. Wenn Zertifizierungsstellen digitale Zertifikate für Websites aufgrund von anstößigen Inhalten sperren, ist die „Vertrauenskette“, von der ein Großteil der Internetsicherheit abhängt, beeinträchtigt. Zudem können Eingriffe auf Infrastrukturebene die Fragmentierung des offenen Internets beschleunigen, weil dessen zentrale Gestaltungsprinzipien verletzt werden – zum einen, weil die Menschen neue Infrastrukturen bauen, um solche Eingriffe zu umgehen, und andererseits, weil Infrastrukturanbieter sich mit widersprüchlichen Vorschriften auseinandersetzen müssen, die in einem Land Sperrungen erfordern, in einem anderen wiederum nicht, je nachdem, wem sie gehorchen.

8. Regelkollisionen sind unvermeidlich.

Infrastrukturanbieter sind, wie internationale Dienstleister allgemein, schon jetzt mit kollidierenden Anforderungen konfrontiert, die auf den Gesetzen und Werten der Länder beruhen, in denen sie tätig sind. Die Einhaltung von einander widersprechenden Vorschriften ist nicht nur teuer, sondern mitunter auch gar nicht möglich. Machen sie bei der Inhaltskontrolle mit, fordern sie zusätzliche Auflagen geradezu hinaus, was in eine Abwärtsspirale führt, so dass sie in ihrem Dienst alle möglichen Inhalte sperren, um auch ja das zensurfreudigste Regime noch zufrieden zu stellen.

Fazit

Für Milliarden von Menschen in aller Welt ist das Internet eine unverzichtbare Ressource. Wir nutzen es zum Kommunizieren, Organisieren und Protestieren, für Arbeit und Schule, zum Einkaufen und Handeln, um Zugang zu staatlichen

Dienstleistungen zu erhalten und noch für viele andere Zwecke. Damit es diese Aufgaben weiterhin erfüllen kann, muss das Internet stark, flexibel und sicher sein. Wir benötigen Infrastrukturanbieter, die sich auf ihre Kernaufgabe konzentrieren: die Bereitstellung eines zuverlässigen und widerstandsfähigen Internets. Diese Aufgabe ist weitaus wichtiger und schützt die Menschenrechte auf wirksamere Weise als der Versuch, Zensurmechanismen zu entwickeln, die unweigerlich mehr Schaden als Nutzen anrichten.

Unterschrieben

Access Now

American Civil Liberties Union (ACLU)

ARTICLE 19

ARTICLE 19 México y Centroamérica

ASEAN Youth Forum

Asociación por los Derechos Civiles (ADC)

Asociația pentru Tehnologie si Internet (ApTI)

Association for Progressive Communications (APC)

Bits of Freedom

Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE)

Chaos Computer Club (CCC)

Citizen D / Državljan D

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

Comun.al, Laboratorio de resiliencia digital

Data Privacy Brasil Research Association

Derechos Digitales - América Latina

Digitale Gesellschaft Schweiz (Switzerland)

Don’t Delete Art (DDA)

Electronic Frontier Foundation (EFF)

Epicenter.works - for digital rights

European Center for Not-for-Profit Law (ECNL)

European Digital Rights (EDRi)

Fight for the Future (FFTF)

Förderverein Informationstechnik und Gesellschaft (Fitug e.V.)

Foundation for Media Alternatives (FMA)

Freemuse

Fundación Huaira

Fundación InternetBolivia.org

Fundación Karisma

Fundación Vía Libre

Global Forum for Media Development (GFMD)

Hiperderecho

Homo Digitalis

Instituto Nupef

Instituto Panameño de Derecho y Nuevas Tecnologías (IPANDETEC)

Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec)

Instituto de Referência em Internet e Sociedade (IRIS)

Intervozes - Coletivo Brasil de Comunicação Social

IT-Pol Denmark

Kandoo

Masaar - Technology and Law Community

National Coalition Against Censorship (NCAC)

Open Knowledge Foundation

OpenMedia

Open Rights Group

Red en Defensa de los Derechos Digitales (R3D)

Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)

SeguDigital

SMEX

Southeast Asia Freedom of Expression Network (SAFEnet)

TAPOL

Taraaz

The Sex Workers Project of the Urban Justice Center

The Tor Project

The William Gomes Podcast

The Woodhull Freedom Foundation

Usuarios Digitales