Christian Möller

Zwischen Freiheit und Zensur

Die Frage der Internet Governance danach, wie das Internet reguliert werden soll, lässt sich nicht einfach beantworten. Technisch ist vieles möglich – oftmals jedoch auf Kosten von Freiheitsrechten. Die Umsetzung ist dabei trotz der globalen Natur des Internets national äußerst unterschiedlich. Welches Maß an unerwünschten Inhalten muss eine demokratische Gesellschaft als Preis für die Freiheit des Internets aushalten?

Grenzenloses Internet?

Googelt man in Deutschland „youporn.com“, findet man unter den Suchergebnissen zwar eine Reihe einschlägiger ähnlicher Angebote, aber keinen Link auf die Startseite des Angebots selbst. Gibt man die URL jedoch in die Adresszeile des Browsers ein, erreicht man das (wie der Name vermuten lässt) eindeutig pornografische Angebot ohne jede weitere ernst zu nehmende Altersüberprüfung. Dieses Beispiel zeigt deutlich die rechtlichen, technischen und wirtschaftlichen Herausforderungen bei der Regulierung des Internets, der Internet Governance. Pornografie ist in Deutschland (bis auf einige Ausnahmen für geschlossene Benutzergruppen) nach § 184 StGB sowohl im Fernsehen als auch im Internet (den sogenannten Telemedien) verboten. Während dieses Verbot im Fernsehen umfassend beachtet wird, sieht es in der Realität des Internets offenbar anders aus: Sogenannte Tube-Seiten machen pornografische Inhalte mit einem Mausklick und ohne jede Altersbeschränkung kostenlos zugänglich (Schmidt 2019, S. 29 ff.).

In Deutschland ist eine Reihe von Akteuren für die Verfolgung von unzulässigen Inhalten im Internet zuständig: Neben Staatsanwaltschaften sind dies u. a. die Landesmedienanstalten, die Bund-Länder-Institution jugendschutz.net sowie zunehmend die Betreiber von Webplattformen, die sogenannten Intermediäre. Außerdem wird die Bundesprüfstelle für jugendgefährdende Medien (BPjM) auf Antrag aktiv und indiziert jugendgefährdende Inhalte auch ausländischer Angebote im Internet. Dabei werden jugendgefährdende Telemedien – anders als Trägermedien wie CDs, DVDs, Blu-rays, Bücher etc., die in die öffentlichen Listenteile A und B aufgenommen werden – in die nicht öffentlichen Listen C und D aufgenommen. Die Geheimhaltung soll verhindern, dass der „Index“ der BPjM quasi als Empfehlungskatalog für einschlägige Webseiten missbraucht werden kann (bereits 2014 wurde diese Liste dennoch – zumindest in Teilen – von Hackern veröffentlicht.)

Diese landläufig „Indizierung“ genannte Listenaufnahme ist auch der Grund dafür, dass die großen Tube-Seiten nicht in den Suchergebnissen (SERPs) von Google, Bing und Co. auftauchen. Die großen Suchmaschinenbetreiber haben sich im Verhaltenssubkodex der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter e. V. (FSM) bereits 2004 freiwillig dazu verpflichtet, „indizierte“ Telemedien nicht mehr zu listen. Die oben erwähnten geheimen Listenteile C und D werden im sogenannten BPjM-Modul elektronisch zur Verfügung gestellt, das somit eine Blacklist zur Filterung indizierter Internetseiten aus den Suchergebnissen darstellt. YouPorn mag durch seine nahezu ikonografische Bekanntheit – steht das Angebot doch stellvertretend für eine Vielzahl von Tube-Angeboten – von diesem Ausschluss aus den deutschen SERPs nicht weiter betroffen sein, für andere Angebote hingegen gilt: Was es bei Google nicht gibt, gibt es nicht.

Dies gilt freilich nur für die (deutschsprachigen) Suchergebnisse.[1] Die Tube-Angebote selbst und andere illegale Inhalte sind auch aus Deutschland heraus weiterhin zugänglich, wenn man nur ihre genaue URL kennt. Zudem werden in den SERPs nach wie vor eine Reihe benachbarter Seiten gelistet, die in ihren Inhalten den indizierten Seiten in nichts nachstehen. Hier herrscht also offenkundig ein Problem bei der Durchsetzung deutschen Rechts bei der Verfolgung ausländischer Internetangebote. Die – privaten – Suchmaschinenbetreiber dienen in ihrer Mittlerfunktion als Intermediäre also als Erfüllungsgehilfen des deutschen Jugendmedienschutzes, der ansonsten online ein Exekutivdefizit hat.

Pornwall und Great Firewall

Einen anderen Weg ist man beispielsweise in England gegangen, wo seit Jahren Filtermaßnahmen auf Ebene der Internet Service Provider (ISP) vorgeschrieben sind (Möller 2019, S. 315). Bereits 2004 begann die British Telecom trotz der technischen Probleme und einiger Proteste mit der Einrichtung des Systems Cleanfeed, das auf Grundlage einer Liste der Internet Watch Foundation (IWF) Internetinhalte blockiert. 2013 führten die vier größten ISP auf Druck der Regierung Filter für alle Kunden ein, die u. a. den Zugang zu Angeboten wie Pornografie, Cybermobbing, Drogen, Selbstmord oder Hacker-Tools sperren sollen. Mit dem Digital Economy Act von 2017 wurde das Filtern von Pornografie ohne entsprechende Altersverifikation dann verpflichtend für alle ISP. Kunden, die diese Filter nicht wünschen, müssen sich aktiv dagegen aussprechen (Opt-out). Ironisch wird der Filter „Pornwall“ genannt – Kritiker befürchten jedoch, dass die Maßnahmen nicht nur Pornografie betreffen, sondern der Beginn eines „Censorship Creep“ in England sind.

In Deutschland wurde eine Diskussion um das Filtern und Blockieren von Internetinhalten im Zuge des Gesetzes zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen (Zugangserschwerungsgesetz) geführt, das der damaligen Familienministerin Ursula von der Leyen den Spitznamen „Zensursula“ einbrachte. Das Gesetz wurde zwar 2010 eingeführt, faktisch jedoch niemals angewandt und im Dezember 2011 wieder aufgehoben.

Andere Länder sind weniger zimperlich, wenn es um die Regulierung oder Restriktion des Internets geht: Vor allem Saudi-Arabien und China sind für ihre Filtersysteme bekannt, aber auch eine Reihe weiterer Länder nutzt Internetfilter, um unerwünschte politische Äußerungen zu unterbinden, unter ihnen Nordkorea, Äthiopien, Syrien, Iran, Burma, Vietnam u. v. m. Die Great Firewall of China ist sprichwörtlich geworden für die umfassende Kommunikationskontrolle über das Internet.

2010 entschied sich Google, aufgrund von Zensurmaßnahmen und Hackerangriffen seinen chinesischen Ableger google.cn zu schließen bzw. in das liberalere Hongkong umzuziehen. Zu diesem Zeitpunkt war China jedoch schon lange nicht mehr auf ausländische Internetdienste angewiesen. Neben einer technischen Kontrolle des Internetverkehrs war bereits damals eine Reihe von inländischen Anbietern entstanden, die sich bis heute den chinesischen Regeln fügen und dabei wirtschaftlich äußerst erfolgreich sind. Dazu gehören die Suchmaschine Baidu, die Handelsplattform Alibaba, der Messenger QQ, das soziale Netzwerk Weibo oder die allumfassende Social-App WeChat. Zusammen mit der Verwendung von internationalisierten Domainnamen (IDN) ist so eine ausdifferenzierte, linguistisch und kulturell chinesisch geprägte Internetlandschaft entstanden, die in einigen Bereichen sogar über das Angebot außerhalb Chinas hinausgeht.

Der Internet-Governance-Experte Kleinwächter schrieb bereits 2005: „Die Chinesen haben sich schon seit längerem partiell vom globalen Internet abgenabelt und innerhalb ihrer .cn Domain de facto ein Intranet errichtet mit einem eigenen Root Server System […]. Vom .cn-Netz kommt man nur über kontrollierte Übergänge zu dem, was die Chinesen das ‚internationale Internet‘ nennen. Und was mit dem ‚internationalen Internet‘ passiert, […] interessiert die Chinesen nur, insofern ihre eigenen Interessen tangiert werden.“ (Kleinwächter 2005)

China wählt hier einen Ansatz der Kommunikationskontrolle, mit dem unerwünschte (ausländische) Inhalte blockiert werden, das wirtschaftliche Potenzial des Internets jedoch genutzt werden soll. Bisher gelingt diese Gratwanderung offenbar gut. Mit zunehmender Bedeutung als Weltmacht bekommt Chinas Ansatz auch international größeres Gewicht. Russland verfolgt mit dem Konzept des RuNet einen ähnlichen Ansatz. Genau wie in China zeichnet sich auch das RuNet durch ein großes linguistisch und kulturell angepasstes Angebot an Internetinhalten und -diensten aus, einschließlich Suchmaschinen (Yandex), sozialen Netzwerken (VKontakte und Odnoklassniki) oder Blogs (LiveJournal). Der Iran verfolgt mit dem Halal-Net einen ähnlichen Ansatz, um bestimmte Vorstellungen von religiöser Moral und Scharia-Gesetzgebung im Internet zu implementieren. Auch Saudi-Arabien setzt bereits seit 2001 umfangreiche Filtermaßnahmen ein, um Pornografie, Glücksspiel oder religiöse Inhalte zu blockieren. In Turkmenistan

– einer Diktatur, in der es keinerlei unabhängige Medien gibt – ist der Internetzugang generell nur für einen kleinen Teil der Bevölkerung überhaupt möglich. Dieser beschränkte sich zudem lange Zeit auf das Turkmenet, ein turkmenischsprachiges Intranet ohne Zugang zum WWW (siehe auch Deibert/Palfrey u. a. 2010).

Vom Mythos des Cyberspace, ein grenzenloser und unabhängiger Raum zu sein, fern von Regierungen und Industrie, den die Internetpioniere und Hacktivisten der 1980er- und 1990er-Jahre geprägt haben, ist nicht viel übrig geblieben. Auch die Einschätzung des Usenet-Pioniers und Mitbegründers der Electronic Frontier Foundation (EFF) John Gilmore, dass die Struktur des Internets Zensur unmöglich mache („The Net interprets censorship as damage and routes around it." [zitiert nach: Elmer-Dewitt 1993]), hat sich in der weiteren Entwicklung nicht bewahrheitet. In vielen Ländern der Welt ist Internetzensur an der Tagesordnung. Menschenrechtsorganisationen wie Freedom House oder Reporter ohne Grenzen berichten regelmäßig über den Stand der Lage in den einzelnen Ländern und benennen die „Feinde des Internets".

In der Türkei beispielsweise sind neben einer zeitweisen Totalblockade von Twitter oder YouTube nach Expertenberichten rund 50.000 Webseiten gesperrt. In einem Verfahren vor dem Europäischen Gerichtshof für Menschenrechte (EGMR) urteilte dieser Ende 2012, dass die willkürliche Blockade des gesamten Dienstes Google Sites gegen Art. 10 der European Court of Human Rights (ECHR) verstoße, da die Maßnahmen nicht auf der Grundlage von bestehenden Gesetzen getroffen worden seien. Die Sperre von Google Sites wurde daraufhin wieder aufgehoben, allerdings verschärfte das Parlament die gesetzlichen Eingriffsmöglichkeiten weiter (Akdeniz 2016).

Die entscheidende Frage ist also nicht, ob man das Internet regulieren kann, sondern wie tief man in die technische Infrastruktur des Netzes eingreifen möchte und welche Freiheitseinschränkungen man bereit ist zu akzeptieren. Oder anders herum: welches Maß an unerwünschten Inhalten eine demokratische Gesellschaft als Preis für die Freiheit des Internets aushalten muss.

Domestizierung des Internets

Onlinekommunikation findet heute zu einem erheblichen Teil nicht mehr im öffentlichen Raum des Internets statt, sondern auf privaten Plattformen: Google, Apple, Facebook und Amazon – die sogenannte GAFA-Industrie – und weitere soziale Netzwerke wie Twitter oder TikTok stellen die Räume, in denen Nutzer sich bewegen und austauschen. Aus Feld, Wald und Wiese des frühen Internets wurde quasi eine Shopping-Mall, in der die Regeln der jeweiligen Betreiber herrschen. Und die Hausherren können diese Regeln prinzipiell auch einfach durchsetzen: Inhalte können entfernt, Nutzer blockiert oder Konten gesperrt werden. YouTube tut dies bei Copyrightverletzungen, Facebook geht entschieden gegen Nacktheit vor und Twitter hat kürzlich jegliche politische Werbung untersagt.

Neben die staatliche Kontrolle des Internets treten also auch die Hausordnungen der sogenannten Intermediäre. Diese müssen jedoch nicht immer deckungsgleich mit nationalen Gesetzen oder gesellschaftlichen Moralvorstellungen sein. Die Debatte um Fehl- und Desinformation auf den sozialen Netzwerken zeigt wieder einmal, wie schwer sich Staaten und private Akteure weltweit mit der einvernehmlichen Regulierung von Inhalten tun.

Kontrolle in Echtzeit?

Was sich im Bereich der unerwünschten und illegalen On-Demand-Inhalte bereits als schwierig erweist, wird durch die technischen Fortschritte im Bereich des Livestreamings von Videos noch weiter verschärft: Der Attentäter von Christchurch übertrug ein Livevideo seiner Tat auf Facebook, der Attentäter von Halle streamte seine Tat live auf Twitch.

In beiden Fällen wurden die Videos nach Bekanntwerden gelöscht und das Wiedereinstellen weitgehend verhindert. Technische Instrumente wie die automatische Erkennung identischer Videoinhalte mithilfe von Hashwerten, die ursprünglich u. a. zur Verhinderung von Urheberrechtsverstößen erprobt wurden, helfen hier gegen die massenhafte Verbreitung. Wie so häufig gilt jedoch, dass Inhalte, die einmal im Internet veröffentlicht wurden, nicht so einfach wieder verschwinden. Spätestens wenn die Videos bearbeitet oder als Screencast abgefilmt und neu verbreitet werden, ändern sich die Hashwerte und das Katz-und-Maus-Spiel beginnt von Neuem. Wie man diesem und anderem Missbrauch des Livestreamings begegnen kann, war auch Thema auf dem UN Internet Governance Forum (IGF), das im November 2019 in Berlin zusammenkam. Endgültige Antworten gab es noch keine – außer der Feststellung, dass alle Stakeholder zusammen an Lösungen arbeiten müssten. Und: dass trotz aller Schwierigkeiten auch die Freiheit des Internets bewahrt werden müsse. Denn eine Regulierung bis hin zu einer völligen Abschottung ist möglich, würde aber gleichzeitig auch das Ende des Internets, wie wir es kennen, bedeuten.

Anmerkung:

1 Nutzt man beispielsweise die internationale Version von Google unter google.com, sehen die Suchergebnisse durchaus anders aus als in der deutschen Version der Suchmaschine.

Literatur:

Akdeniz, Y.: *Media Freedom on the Internet: An OSCE Guidebook*. Wien 2016

Deibert, R./Palfrey, J. u. a. (Hrsg.): *Access Controlled. The Shaping of Power, Rights, and Rule in Cyberspace.* Cambridge 2010

Elmer-Dewitt, P.: *First Nation in Cyberspace.* In: TIME, 06.12.1993 (Nr. 49). Abrufbar unter: http://kirste.userpage.fu-berlin.de

Kleinwächter, W.: *Erbsenzählen nach der Cyberschlacht.* In: Telepolis, 24.11.2005. Abrufbar unter: https://www.heise.de

Möller, C.: *Kommunikationsfreiheit im Internet: Das UN Internet Governance Forum und die Meinungsfreiheit.* Wiesbaden 2019

Schmidt, R.: *Feministische und ethische Pornografie. Revolution einer Branche oder Randerscheinung?.* Baden-Baden 2019

Dr. Christian Möller ist Medienwissenschaftler und Professor für Corporate Communication an der Hochschule für Medien, Kommunikation und Wirtschaft (HMKW) in Berlin sowie Leiter des Instituts für angewandte Publizistik (ifap) an der Fachhochschule Kiel. Seit 2011 ist er Prüfer bei der Freiwilligen Selbstkontrolle Fernsehen (FSF).