

Intelligente Upload-Filter: Bedrohung für die Meinungsfreiheit?

Amélie P. Heldt

Hans-Bredow-Institut, Hamburg

1. Einleitung

»Wie ist es möglich, Informationen über die Welt und über die Gesellschaft als Informationen über die Realität zu akzeptieren, wenn man weiß, wie sie produziert werden?«¹

An diese klassische Frage der Publizistik schließt sich heutzutage folgende an: *wie* ist es möglich, Informationen (...) zu akzeptieren, wenn man weiß, wer oder was *zwischen* dem Kommunikator und dem Receptor steht? Algorithmen bestimmen große Teile unseres Medienkonsums online, sei es in der Produktion, in der Aufbereitung oder im Austausch zwischen Nutzern. Die Einführung der Database of Hashes von Facebook, Twitter, YouTube und Microsoft im März 2017 stellt ein Beispiel dar, anhand dessen eine konkrete Prüfung erfolgen kann. In dieser Datenbank werden digitale Fingerabdrücke (sogenannte »Hashes«) von Inhalten gesammelt, die als »terroristisch« oder »extremistisch« markiert wurden. Zweck ist es, effizienter gegen Terrorpropaganda online vorzugehen, allerdings wirft dieses Filtersystem wichtige Fragen für die Ausübung der Meinungs- und Informationsfreiheit auf.

¹ Luhmann, Realität der Massenmedien, S. 215, im Original kursiv.

Dieser Beitrag untersucht das Bedrohungspotenzial von intelligenten Filtern für die Kommunikationsfreiheiten (Meinungs- und Informationsfreiheit) am Beispiel von Upload-Filtern bei Informationsintermediären. Dafür bedarf es zunächst einer Bestandsaufnahme der Rolle von algorithmischen Entscheidungen in den Online-Medien (1.), sprich in der Online-Mediennutzung (1.1) und der Definition sowie der Anwendung von intelligenten Filtern in diesem Rahmen (1.2). Im zweiten Teil soll dieser Sachverhalt verfassungsrechtlich eingeordnet werden (2.).

2. Algorithmisches Entscheiden in der öffentlichen Kommunikation

2.1. Rolle von Algorithmen in der Online-Mediennutzung

2.1.1. Die Funktion von Algorithmen: sortieren und priorisieren

Algorithmus nennt man ein Verfahren zur schrittweisen Umformung von Zeichenreihen.² In der publizistischen und rechtswissenschaftlichen Diskussion wird unter dem bisher vorherrschenden Begriff der »Algorithmen« eine in Programmiersprache(n) transformierbare Vorgehensweise verstanden, nach der ein Rechner eine Aufgabe in endlicher Zeit bewältigt.³ Dank solcher Programme können Informationsintermediäre für ihre Nutzer Inhalte klassifizieren. Dienste des Typs Intermediär zeichnen sich durch eine Vermitt-

² <https://www.duden.de/rechtschreibung/Algorithmus>; Internetquellen sind, soweit nicht anders angegeben, auf dem Stand vom 29. Januar 2018.

³ so Martini, JZ 72, 1017 (1017); m.w.N. auf Hoffmann-Riem, AöR 142, 1 (2).

lungsleistung zwischen Inhalten oder Inhaltsangeboten und Nutzern aus.⁴ Der Terminus wird als Oberbegriff für Angebote wie Suchmaschinen, Plattformen für nutzergenerierte Inhalte, App-Plattformen, Micro-Blogs und soziale Netzwerke genutzt. Die algorithmische Selektionsfunktion steht aufgrund ihrer zunehmenden Relevanz bei der mittelbar-inhaltlichen Einflussnahme von Intermediären im Mittelpunkt dieses Beitrages (nicht der Begriff des Intermediärs selbst). Vor dem Hintergrund der aktuell vorherrschenden Angebotsstruktur sind Meinungsbildungsprozesse im Netz ohne Intermediäre nicht mehr denkbar, weil sie Informations- und Kommunikationspraktiken mittlerweile in vielfältiger Weise durchdringen. Zugleich sind Intermediäre aber nur ein Baustein im Prozess der Meinungsbildung und greifen an verschiedenen Stufen dieses Prozesses unterschiedlich stark ein.⁵

2.1.2. Meinungsbildung und ihre Merkmale

Die individuelle Meinungsbildung umfasst die Freiheit eines jeden, sich seine Meinung zu bilden. Bei dieser Freiheit handelt es sich um die grundlegende Voraussetzung für die Ausübung der Meinungsäußerungs- und Meinungsverbreitungsfreiheit (zum Schutzbereich weiter unten). Jenseits der verfassungsrechtlichen Abgrenzungsschwierigkeit zur Informationsfreiheit lässt sich die individuelle Meinungsbildung wie folgt definieren: Meinungsbildung ist abhängig von den jeweiligen Wertvorstellungen, der Lebenslage, dem Wissen und den bisherigen Erfahrungen der Menschen. Sie bilden sich

⁴ Schulz/Dankert, Die Macht der Intermediäre, Friedrich-Ebert-Stiftung 2016, S. 15, im Original kursiv.

⁵ Schmidt/Merten/Hasebrink/Petrich/Rolfs, Zur Relevanz von Online-Intermediären für die Meinungsbildung, Arbeitspapiere des Hans-Bredow-Instituts Nr. 40, S. 7.

eine Meinung darüber, wie die Gesellschaft, in der sie leben, aussehen sollte und welche politischen Entscheidungen sie gutheißen oder aber ablehnen.⁶ Eine entscheidende Rolle in diesem Prozess spielen die Medien, insbesondere die Massenmedien. Zu den herkömmlichen Medien wie Presse und Rundfunk sind die sogenannten Informationsintermediäre – wie oben bereits erwähnt – gestoßen.

Individuelle und öffentliche Meinungsbildung sind nicht voneinander zu trennen und doch umfassen sie unterschiedliche Aspekte des Rechts auf freie Meinung. Bereits in seiner Leitentscheidung »Lüth« hat sich das Bundesverfassungsgericht dazu geäußert: der Bürger kann seine Freiheit zu einem privaten, eigennützigen Zweck ausüben oder als »Beitrag zum geistigen Meinungskampf in einer die Öffentlichkeit wesentlich berührenden Frage«.⁷ Tatsächlich benutzt das Bundesverfassungsgericht die Termini politische Meinungsbildung und Bildung einer öffentlichen Meinung als Synonyme, wobei letztere nicht auf politische Inhalte beschränkt ist, sondern auch Unterhaltung beinhaltet.⁸ Auf eine einheitliche Definition der öffentlichen Meinung konnte man sich bisher nicht einigen. Fest steht, dass sie sich *frei* bilden muss. So betont Kloepfer, dass »nicht die öffentliche Meinung an sich für die *freiheitlich*-demokratische Ordnung maßgebend ist, sondern nur die öffentliche Meinung, die in einem *freien* Meinungsbildungsprozess zustande gekommen ist. [...] Deshalb muss die Demokratie vor allem den *freiheitlichen* Entstehungsprozess der öffentlichen Meinung sichern [...].«⁹ Im Mittelpunkt steht also die *Freiheit* – ohne dieses Merkmal kann nicht von Meinungsbildung die Rede sein.

⁶ Hasebrink, Meinungsbildung und Kontrolle der Medien, bpb.

⁷ BVerfGE 7, 198 (212).

⁸ BVerfGE 12, 205 (263).

⁹ Kloepfer, Handbuch des Staatsrechts, § 42 Rn. 12, Hervorhebungen durch Verfasserin.

Angesichts des zunehmenden Einflusses von Intermediären und ihrer algorithmischen Entscheidungsstrukturen ist es fraglich, ob dieser freiheitliche Prozess der Meinungsbildung hinreichend geschützt ist. Fakt ist, dass Algorithmen mittlerweile eine ähnliche, wenn nicht sogar noch weiterreichende Macht bei der Herstellung von Öffentlichkeit zugeschrieben wird als dem Journalismus.¹⁰ Anders gesagt übernehmen die technischen Beteiligten an öffentlicher Kommunikation eine zunehmend bedeutsame Rolle bei der Herstellung der kommunikativen Grundlage unserer Gesellschaft.¹¹

2.1.3. Suchmaschinen & Newsfeeds

Deutsche Internetnutzer nennen Google, Facebook, YouTube, WhatsApp und Twitter in dieser Reihenfolge am häufigsten als Quellen von oder Kontaktvermittler zu Informationen über das Zeitgeschehen in Politik, Wirtschaft und Kultur.¹² Das sind die »big five«, die bei der Mediennutzung im Netz ausschlaggebend sind. Die beiden ersten Dienste, Google und Facebook, nutzen Algorithmen, um – im Fall der Suchmaschine – die gezielte Suche nach Informationen im Internet und – im Fall des Newsfeed im sozialen Netzwerk¹³ – die Sortierung der relevantesten Neuigkeiten aus dem digitalen Freundeskreis zu ermöglichen. Die Sortierung und Priorisierung erfolgt wie bereits angesprochen nach möglichst personalisierten Kriterien, die vom Algorithmus ausgewertet werden, um dem Nutzer ein »maßgeschneidertes« Ergebnis zu präsentieren (»People Analytics«).

¹⁰ Loosen/Scholl, 2.

¹¹ Hans-Bredow-Institut, Medien- und Kommunikationsbericht (2017), 209.

¹² Ecke, Wie häufig und wofür werden Intermediäre genutzt?, 21.

¹³ Ansammlung bzw. Auflistung auf der Startseite von auf der Kommunikationsplattform veröffentlichten Inhalten.

Der Vergleich zum Medienkonsum am analogen Zeitungskiosk ist kaum vorstellbar, denn übertragen darauf würde der Kioskinhaber einem Leser nur noch jene Zeitungen anbieten, die »zu ihm passen« – ohne dass der Leser erfahren dürfte, ob und wie der Verkäufer seine Auswahl getroffen hat. Darüber hinaus wäre er nicht wirklich in der Lage, eine abweichende Wahl zu treffen und dürfte nur die Zeitungen lesen, die für ihn ausgesucht wurden. Der Medienkonsument wird in einer solchen Konstellation einerseits gewissermaßen entmündigt und andererseits gelingt er an viel spezifischere Informationen, nach denen er womöglich sucht. Ob der Begriff des *freien* Meinungsbildungsprozesses darauf anwendbar ist, erscheint allerdings problematisch.

2.2. Intelligente Filter zur Verhinderung von illegalem Content

Aus den vorstehenden Erläuterungen zu Intermediären und algorithmischen Entscheidungen ergibt sich ihre wichtige Position in der heutigen digitalen Medienlandschaft. Hinzu kommen die Inhalte, die von Nutzern hochgeladen und auch als Informationsquellen wahrgenommen werden. Bei der Bekämpfung von strafbaren Online-Inhalten in Verbindung mit algorithmischen Entscheidungen¹⁴ liegt der Fokus bei intelligenten Filtern, genauer gesagt bei sogenannten Upload-Filtern (wörtlich übersetzt »Hochladfilter«). In diesem Abschnitt werden zunächst die Funktionen von Upload-Filtern analysiert, um in einem zweiten Teil das Konstrukt der »Database of Hashes« als ersten Prototyp zu untersuchen.

¹⁴ Im Folgenden geht es um solche Algorithmen, die Inhalte in Informationsintermediären sortieren und priorisieren, wenn nicht anders spezifiziert.

2.2.1. Upload-Filter

Im Rahmen von Suchmaschinen und Newsfeeds ist eine der Hauptfunktionen von Algorithmen, Inhalte nutzerorientiert zu sortieren und je nach Profil unterschiedlich zu präsentieren. Ein sogenannter Upload-Filter durchsucht nutzergenerierte Inhalte, solange sie noch im Cache sind, also bereits im Pufferspeicher¹⁵ des jeweiligen Intermediärs aber noch nicht für andere Nutzer sichtbar.

Die wichtigsten Merkmale des Upload-Filters sind, dass er bestimmte Inhalte erkennt und dann automatisch löscht. Das heißt, dass bei diesen beiden Schritten kein Mensch die Entscheidung trifft, sondern der Algorithmus. Der einzige »human in the loop« ist der ursprüngliche Programmierer des Filters, einen zusätzlichen Content-Moderator gibt es nicht. Anwendungsbereich kann die Suche nach Verstößen gegen geltendes Recht sein; das Merkmal der Illegalität ist der Definition des Upload-Filters allerdings nicht inhärent, denn wonach gefiltert wird, hängt von der Programmierung ab.

Eine andere Kategorie des Upload-Filters ist der Re-Upload-Filter. Der Unterschied ist, dass letzterer Inhalte erkennt und löscht, die beim ersten Upload als illegal markiert wurden. Beispielsweise kann Content, der in sozialen Netzwerken gemeldet und moderiert¹⁶ wurde, beim zweiten Hochladen erkannt und sofort gelöscht werden. Dabei kann der Algorithmus insoweit selbstlernend sein, als dass er trotz kleiner Veränderungen am ursprünglichen Inhalt diesen dennoch als Verstoß erkennt. Ein Umgehen des Mechanismus wird immer schwieriger, wenn es sich im Kern um denselben Con-

¹⁵ <https://www.duden.de/suchen/dudenonline/Pufferspeicher>

¹⁶ Bspw. von Moderationsdienstleistern wie das Bertelsmann SE & Co. KGaA-Tochterunternehmen Avarto.

tent handelt. Durch das Markieren der Inhalte als illegal wird der Algorithmus trainiert, sie als solche zu erkennen. Ein Standardbeispiel ist die von Microsoft entwickelte Software »PhotoDNA«, die seit 2008 eingesetzt wird, um die Verbreitung kinderpornographischer Bilder und Videos im Netz zu verhindern. Wie oben bereits erwähnt, können Algorithmen auch auf andere Zwecke trainiert werden als die Ahndung illegaler Inhalte. So trainiert das soziale Netzwerk Facebook beispielsweise einen Algorithmus auf die Erkennung von Selbstmordsabsichten und Löschung von Selbstmordvideos.¹⁷

2.2.2. Database of Hashes als erster Prototyp

2.2.2.1. Kontext des EU Internet Forums

Die EU-Kommission gründete 2015 das EU Internet Forum, welches die Innenminister der EU-Länder, hochrangige Vertreter von führenden Unternehmen der Internetbranche, von Europol und des Europäischen Parlaments sowie den EU-Koordinator für die Terrorismusbekämpfung versammelt. Ziel des Forums ist ein gemeinsames Konzept auf der Grundlage einer öffentlich-privaten Partnerschaft zur Aufspürung und Bekämpfung schädlicher Online-Inhalte.¹⁸ 2016 stellte die EU-Kommission den Verhaltenskodex zur Bekämpfung illegaler Hassrede im Internet¹⁹ vor. Damit verpflichteten sich die Unternehmen Facebook, Twitter, YouTube und Microsoft²⁰ gegen illegale Hassrede im Internet vorzugehen. Der Verhaltenskodex enthält konkrete Verpflichtungen für die IT-Unternehmen wie, zum Bei-

¹⁷ »Mit Künstlicher Intelligenz gegen Selbstmord-Video«, <http://s.fhg.de/r58>

¹⁸ Pressemitteilung der Europäischen Kommission, IP/15/6243.

¹⁹ Im Folgenden: Verhaltenskodex oder Code of Conduct.

²⁰ Im Folgenden: IT-Unternehmen.

spiel, die Mehrheit der Meldungen in Bezug auf die Entfernung illegaler Hassreden in weniger als 24 Stunden zu prüfen und solche Inhalte zu entfernen oder den Zugang dazu zu sperren.²¹

2.2.2.2. Database of Hashes

Im EU Internet Forum wurde im März 2017 der erste Prototyp der Database of Hashes vorgestellt – eine gemeinsame Datenbank der o.g. IT-Unternehmen.²² Beim Hashing (to hash = kleinhacken) sammeln die IT-Unternehmen digitale Fingerabdrücke (sog. »Hashes«) von Inhalten, die als »terroristisch« oder »extremistisch« markiert wurden und speichern sie in der Datenbank, die für alle vier IT-Unternehmen zugänglich ist. Wenn die Beiträge markiert wurden, können sie auf keiner der vier Plattformen mehr hochgeladen werden²³, weil sie vom Filter erkannt werden. Durch den Austausch der Daten sollen Bilder und Videos schneller identifiziert und das Löschen von »terroristischer Propaganda« beschleunigt werden.²⁴

Im jüngsten Informationsblatt der EU-Kommission zur Bekämpfung illegaler Hassrede²⁵ weist die Kommission erneut auf die Verpflichtungen der IT-Unternehmen aus dem Code of Conduct hin und fordert »proaktive Maßnahmen um illegale Inhalte aufzuspüren und

²¹ Code of Conduct on countering illegal hate speech online, abrufbar unter <http://s.fhg.de/ny6>

²² An dieser Stelle der Hinweis, dass Google als meistgenutzte Suchmaschine an der Database of Hashes nicht teilnimmt, aber das Tochterunternehmen YouTube.

²³ Monroy, Social media companies launch upload filter to combat »terrorism and extremism«, abrufbar unter <http://s.fhg.de/9e2>

²⁴ Piontek, Warum die Upload-Filter der Internetkonzerne eine Gefahr für die Meinungsfreiheit sind, abrufbar unter <http://s.fhg.de/7gM>

²⁵ Stepping up the EU's efforts to tackle illegal content online, September 2017, MEMO/17/3522.

pro aktiv zu löschen«, sowie »automatische Aufspürtechnologien, insbesondere um das Wiedererscheinen von illegalem Content online zu verhindern«. Diesen Aufforderungen kamen die IT-Unternehmen wohl nach – der Trend zur automatischen Löschung nimmt zu. Am 6. Dezember 2017 trafen sich die Vertreter der IT-Unternehmen zum dritten EU Internet Forum in Brüssel. Sie berichteten, dass die meisten Inhalte bereits gelöscht werden, bevor sie online gehen. Darunter befinden sich Videos, die erstmals hochgeladen werden und weder bei den Firmen noch bei Polizeibehörden mit einer Aufforderung zur Löschung hinterlegt sind.²⁶ Die »Database of Hashes« sei jetzt voll einsatzfähig und umfasse bisher mehr als 40.000 Hashes für bekannte terroristische Videos und Bilder.²⁷

In einem offiziellen Statement geht Susan Wojcicki, CEO von YouTube, genauer auf den Einsatz von intelligenten Filtern zur Bekämpfung von Terrorpropaganda ein.²⁸ Demnach hat die Videoplattform seit Juni 2017 über 150.000 Videos wegen »gewalttätigem Extremismus« gelöscht. Durch Machine Learning können fünfmal mehr Videos als vorher gelöscht werden. 98 Prozent der heutzutage wegen »gewalttätigem Extremismus« gelöschten Videos wurden von lernenden, algorithmen-basierten Systemen markiert. YouTube schätzt die durch den Einsatz von intelligenten Filtern »ersetzte« menschliche Arbeitskraft auf 180.000 Mitarbeiter à 40 Stunden/Woche seit Juni 2017. Das Unternehmen kündigte auch an, den Einsatz von intelligenten Filtern zu erweitern, u. a. auf Jugendschutz und Hassrede.

²⁶ Monroy, »EU-Internetforum«, abrufbar unter <http://s.fhg.de/Y69>

²⁷ EU-Kommission – Pressemitteilung, abrufbar unter <http://s.fhg.de/6kw>

²⁸ <http://s.fhg.de/Ve4>

2.2.2.3. Kritik

Der Einsatz solcher intelligenten Filter in digitalen Kommunikationsräumen wirft wichtige Grundsatzfragen auf, einschließlich ihrer normativen Grundlage (nämlich dem Verhaltenskodex als Selbstverpflichtung, nach Aufforderung des Exekutivorgans EU-Kommission). Es ist fraglich, ob eine solche Vorgehensweise die IT-Unternehmen nicht zu weit verpflichtet oder ihnen Aufgaben überträgt, die im Kern öffentlich-rechtlich sind. Darüber hinaus fordert die Politik immer mehr »proaktive Kontrollmaßnahmen«, ohne den Handlungsbereich und die Befugnisse genau abzustecken. So ist der Begriff »Terrorismuspropaganda« nicht im Code of Conduct definiert, sondern der Auslegung der IT-Unternehmen überlassen.

In der verfassungsrechtlichen Prüfung solcher Mechanismen sind die Grenzen, aber auch die Mindestvoraussetzungen der Meinungsfreiheit genauer unter die Lupe zu nehmen. Zensuraktivitäten des Staates dürfen nicht in der Weise »ausgelagert« werden, dass er zensurgleiches Handeln privater Akteure staatlich fordert oder gar entsprechende Rechtspflichten vorsieht, beziehungsweise negative Sanktionen für den Fall der Verletzung verhängt.²⁹

3. Eine Gefahr für die Kommunikationsfreiheiten?

Der Einsatz intelligenter Filter durch Private auf Veranlassung des Staates könnte die Nutzer digitaler Kommunikationsräume (wie beispielsweise soziale Netzwerke der oben genannten IT-Unternehmen) in ihrer Meinungs- und Informationsfreiheit verletzen. In diesem Abschnitt wird die mögliche Grundrechtsverletzung geprüft,

²⁹ Hoffmann-Riem, AK-GG Art. 5 Abs. 1, 2 Rn. 94; Bethge, in Sachs GG Art. 5 Rn. 135a.

wobei es nicht um den Einzelfall der Database of Hashes geht, sondern um die im vorherigen Satz dargestellte, abstrakte Konstellation. Die Prüfung erfolgt in drei Schritten: Ist der Schutzbereich eröffnet, liegt ein Eingriff in den Schutzbereich vor und ist dieser Eingriff gerechtfertigt?

3.1. Kommunikationsfreiheiten im Grundgesetz

Art. 5 Abs.1 S.1 GG schützt die Meinungs- und Informationsfreiheit, jene Grundrechte die die Grundlage für unser mediales Zusammenleben bilden (»un des droits les plus précieux de l’homme« nach Art. 11 der Erklärung der Menschen- und Bürgerrechte von 1789). Die Meinungsfreiheit ist ein hohes Gut und wichtiger Teil der freiheitlich demokratischen Grundordnung der Bundesrepublik. Ihr sachlicher Schutzbereich ist weit, er umfasst Werturteile und wahre Tatsachenbehauptungen, unabhängig von ihrem Inhalt und ihrem Wert. Persönlich darf jedermann dieses Grundrecht ausüben. Geschützt wird die positive und negative Meinungsfreiheit, also auch das Recht sich nicht zu äußern.

Die Informationsfreiheit ist das sogenannte »Zwillingsgrundrecht« zur Meinungsfreiheit, denn der Sich-Äußernde möchte gehört werden und vice-versa. Die Gewährleistung freier Informationstätigkeit und freien Informationszugangs ist ein wesentliches Anliegen des Grundgesetzes.³⁰ Der Schutzbereich umfasst allgemein zugängliche Quellen und die schlichte Entgegennahme von Informationen³¹, also das Recht sich aktiv und passiv zu informieren und Zugang zu Informationen zu kriegen, welche geeignet und bestimmt sind, der Allgemeinheit Informationen zu verschaffen.³² Das Internet fällt unter

³⁰ BVerfGE 97, 228 (256).

³¹ Jarass in Jarass/Piero, Art. 5 Rn. 22, 25.

³² BVerfGE103, 44 (60).

den Begriff der allgemein zugänglichen Quelle, weil es auf Anhiieb keine Zugangsbeschränkungen enthält. Zwar kann es sich bei zugangsgeschützten Bereichen anders verhalten, aber Intermediäre stellen nicht allein wegen eines eventuellen Log-in-Erfordernisses einen geschlossenen Kommunikationsraum dar, sondern sind weitgehend einem unbestimmten Personenkreis³³ und somit allgemein zugänglich.

3.2. Eingriff in den Schutzbereich

3.2.1. Freiheitsbeeinträchtigung

Die enge Interpretation des Eingriffsbegriffs schließt nicht-formelles Handeln des Staates aus und wird heute kaum noch vertreten. Stattdessen interpretiert man mittlerweile auch schlicht tatsächliches Staatshandeln als Eingriff («moderner Eingriffsbegriff»)³⁴, um einen umfassenden Schutz zu gewährleisten. Die Debatte rund um den verfassungsrechtlichen Eingriff würde an dieser Stelle zu weit führen. Wichtig ist hier, ob es dem Staat zugerechnet werden kann, dass er Private zu einer bestimmten Handlung gegenüber Bürgern auffordert, also mittelbar eingreift. Wenn man der herrschenden Meinung folgt, so kann ein mittelbarer Eingriff des Staates nur angenommen werden, wenn dem Staat das Verhalten des Privaten zurechenbar ist. Hierzu ist erforderlich, dass es dem Grundrechtsträger aufgrund des staatlichen Handelns nicht mehr möglich ist, seine Grundrechte in vollem Umfang zu verwirklichen, die Beeinträchtigung dem Staat zurechenbar ist und eine bestimmte Erheblichkeit

³³ so auch Ladeur, MMR 2001, 787 (791).

³⁴ Roth, Faktische Eingriffe in Freiheit und Eigentum, S. 33 (m.w.N.).

erreicht.³⁵ Zielt der Staat gerade auf das beeinträchtigende Verhalten des Privaten ab, so ist die Zurechnung wegen des intentionalen Eingriffs zu bejahen.³⁶ Wenn der Staat die privaten Betreiber von digitalen Kommunikationsräumen de facto verpflichtet, inhaltsbezogene Kontrollen und Löschungen hinsichtlich des User-generated Content durchzuführen, sind diese Voraussetzungen erfüllt. Demnach sind der Verhaltenskodex und dessen Umsetzung als mittelbarer Eingriff zu werten, denn die Gründung eines staatlichen Rahmens mit konkreten Pflichten zur Inhaltsfilterung zielt auf exakt solche Vorkehrungen wie Upload-Filter ab (auch wenn dieser Rahmen nicht regulatorischer Natur ist).

3.2.2. Eingriff durch den Abschreckungseffekt?

Als Nebeneffekt von Upload-Filtern kommt der sogenannte Abschreckungseffekt in Frage. Darunter versteht man mittelbare und nicht finale, überindividuelle Auswirkungen vornehmlich staatlichen Handelns auf die tatsächliche Grundrechtsausübung.³⁷ Da grundsätzlich der Staat Adressat von Grundrechten ist, ergibt sich in Bezug auf Abschreckungseffekte die Frage, wie mit solchen Abschreckungswirkungen auf die Grundrechtsausübung umzugehen ist, die von Privaten ausgehen.³⁸ Bei der Verhaltensbeeinflussung durch Private ergeben sich im Ergebnis keine oder kaum Unterschiede aus der (eventuell fehlenden) Intention von Abschreckung, da der Einsatz von Upload-Filtern die innersubjektive Entscheidungsfreiheit sich zu äußern beeinträchtigt.

³⁵ Oermann/Staben, *Der Staat* Bd. 52, 630 (637).

³⁶ Voßkuhle, Kaiser, *JuS* 2009, 313 (313).

³⁷ Staben, *Der Abschreckungseffekt*, 4.

³⁸ Staben, *Der Abschreckungseffekt*, 73.

Häufiges Argument gegen den Abschreckungseffekt des Einsatzes von Upload-Filtern ist die (vermutete) Rechtswidrigkeit der Inhalte, wenn es um Terrorpropaganda und Hate Speech geht. Warum sollte der Abschreckungseffekt eine Grundrechtsverletzung begründen, wenn der Inhalt an sich rechtswidrig ist? Dabei wird nicht berücksichtigt, dass der Grundrechtsträger einerseits die Rechtswidrigkeit seiner Äußerung meistens nicht einschätzen kann³⁹ und andererseits die Rechtswidrigkeit den Eingriff rechtfertigt, aber nicht den Schutzbereich verschließt. Das pauschale Ablehnen von Abschreckungseffekten aufgrund der Rechtswidrigkeit der gefilterten Inhalte geht daher fehl. Wenn es aber gar nicht erst zu einer Äußerung kommt, ist eine »Schere im Kopf« des Nutzers nicht wegzudenken.

Zusammenfassend lässt sich festhalten, dass ein Eingriff sowohl in mittelbarer Form als auch durch den Abschreckungseffekt solcher Upload-Filter angenommen werden muss. Das Negieren einer Beeinträchtigung der Meinungsfreiheit durch Upload-Filter käme einer Leugnung der Relevanz algorithmischer Entscheidungen in den Kommunikationsprozessen des Web 2.0 gleich.

3.2.3. Rechtfertigung des Eingriffs

Der Einsatz von Upload-Filtern zur Bekämpfung von Terrorpropaganda und der Verbreitung strafbarer Inhalte könnte gerechtfertigt sein, denn die Meinungsfreiheit ist nicht grenzenlos. Gemäß Art. 5 Abs. 2 GG findet sie ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und dem Recht der persönlichen Ehre (sogenannte Schrankentrias). Um die technische Umsetzung dieser Schranken im Netz geht es bei der Anwendung von intelligenten Filtern: was in der analogen Welt verboten ist, gilt auch für das Internet.

³⁹ So auch Oermann/ Staben, *Der Staat* Bd. 52, 630 (647).

3.3. Schutz vor Terrorpropaganda ja, aber nicht so.

Es reicht nicht, dass der Eingriff in die Meinungsfreiheit erfolgt, um vor terroristischen und extremistischen Inhalten zu schützen oder um das Strafrecht durchzusetzen. Um dem hohen Stellenwert der Kommunikationsfreiheiten gerecht zu werden, müssen auch die sogenannten Schranken-Schranken beachtet werden. Das Zensurverbot ist beispielweise ein absolutes Verbot, das immer respektiert werden muss und bei Filtern besonders relevant ist.

3.3.1. Klassischer Zensurbegriff

Mit Zensur ist nach herrschender Meinung begrifflich (nur) die Vorzensur gemeint,⁴⁰ also die Verpflichtung, vor Herstellung oder Verbreitung eines Mediums dieses einer staatlichen Stelle zur vorherigen Genehmigung dieser Veröffentlichung vorzulegen.⁴¹ Nach herrschender Meinung ginge eine entsprechende Anwendung des Zensurverbots auf private Akteure zu weit. Laut *Hoffmann-Riem* sind Kontrollen des inhaltlichen Angebots im Internet und dessen Filterung jedoch nur insoweit von der privatautonomen Gestaltungsmacht erfasst, als sie Personen betreffen, die über vertragliche Beziehungen zu dem jeweiligen Provider und ähnlichem verfügen und in die Kontrolle und Filterung eingewilligt haben.⁴² Auch *Löffler* sieht die freie Entwicklung des Geisteslebens nur dann gewährleistet, wenn als Adressaten des Zensurverbots auch nicht-staatliche Institutionen und Instanzen angesehen werden, die einen maßgeblichen Einfluss auf das Geistesleben besitzen.⁴³ Diese Ansicht lässt

⁴⁰ BVerfGE 33, 52 (71); 47, 198 (236); 87, 209 (230).

⁴¹ BVerfGE 47, 198 (236); 87, 209 (230).

⁴² Hoffmann-Riem, AK-GG Art. 5 Abs. 1, 2 Rn. 95.

⁴³ Löffler, NJW 1969, 2225 (2227).

sich mit Blick auf den Schutzzweck gut vertreten, denn das Zensurverbot soll die typischen Gefahren einer Präventivkontrolle von Meinungsäußerungen bannen. Faktisch setzt der Upload-Filter an der Stelle an, die unter dem formellen Zensurbegriff verboten ist: die Äußerung wird vor der Veröffentlichung einer Prüfung unterzogen und beim Vorliegen eines bestimmten Inhalts verboten. Kann man diesen Effekt nur unter Verweis auf den klassischen Zensurbegriff negieren? Genügen im Zeitalter digitaler Kommunikationsräume nicht bereits vergleichbare nicht-staatliche Vorkehrungen, die den gleichen Zweck erfüllen?

3.3.2. Private Zensur?

Das wesentliche Merkmal der Zensur, wie sie sich geschichtlich entwickelt hat, ist die planmäßige Überwachung und Überprüfung des Geisteslebens durch eine für die Meinungsbildung oder Meinungs- bzw. Informationsverbreitung maßgebliche Instanz.⁴⁴ Wenn sich große Teile der öffentlichen Meinungsbildung auf digitale Kommunikationsräume verschoben hat, die von privaten Unternehmen betrieben werden, muss dieser Umstand berücksichtigt werden. Schließlich dient die Zensur dazu, den Prozess der freien Meinungs- und Willensbildung zum Schutze öffentlicher Ansichten zu beeinflussen und ihn in einer bestimmten Richtung zu unterbinden.⁴⁵ Wenn der Staat Private verpflichtet, diese Vor-Zensur an seiner Stelle durchzuführen, kommt es zu einer Umgehung des Verbots.

⁴⁴ Löffler, NJW 1969, 2225 (2225).

⁴⁵ vgl. Noltenius, Die freiwillige Selbstkontrolle der Filmwirtschaft und das Zensurverbot des Grundgesetzes, 107.

Dagegen wird angeführt, dass Intermediäre ohnehin Entscheidungen über Inhalte fällen⁴⁶ und das zusätzliche Nudging⁴⁷ durch den Staat keinen Unterschied mache. Dem kann nicht zugestimmt werden. Vielmehr bedarf es einer adäquaten verfassungsrechtlichen Einordnung, die der heutigen Stellung von Intermediären im Meinungsbildungsprozess entspricht, nämlich als unumgehbare Verbindung zwischen Inhalten und Rezipient. Soweit Provider zu einzelnanlassunabhängigen Kontrollen und Sperrungen entsprechender Inhalte des Internets verpflichtet werden, kommen solche mittelbaren Eingriffe in die Meinungs- und Informationsfreiheit der Nutzer einer Zensur gleich und sind verfassungswidrig.⁴⁸

3.4. Für die Informationsfreiheit

Spiegelbildlich lassen sich die für die Meinungsfreiheit erläuterten Effekte auf die Informationsfreiheit übertragen. Sie ist wie das Grundrecht der freien Meinungsäußerung eine der wichtigsten Voraussetzungen der freiheitlichen Demokratie.⁴⁹ Durch den Einsatz von Upload-Filtern werden dem Nutzer Inhalte und somit Informationen vorenthalten – einen Eingriff kann man kaum verneinen. Die nicht zu beanstandende Annahme, von einem Nutzer hochgeladene Inhalte verstoßen gegen Strafgesetze, bedeutet trotzdem nicht, dass das Informationsrecht zwangsläufig zurücktreten muss.⁵⁰

⁴⁶ Eifert, NJW 2017, 1450, (1451).

⁴⁷ Begriff der Verhaltensökonomik, geprägt von Richard Thaler und Cass Sunstein; wörtliche Übersetzung »leichtes Stupsen«.

⁴⁸ vgl. Schulze-Fielitz, in Dreier, GG Art. 5 I, II Rn. 201; Hoffmann-Riem, Der Staat 42, 193 (221).

⁴⁹ BVerfGE 27, 71 (81); vgl. BVerfGE 7, 198 (208).

⁵⁰ BVerfGE 27, 71 (85).

4. Ergebnis und Ausblick

Dass die Nutzung von Upload-Filtern zur Kontrolle von nutzergenerierten Inhalten durch IT-Unternehmen auf Veranlassung des Staates eine Verletzung der Meinungs- und Informationsfreiheit bedeutet, steht im Ergebnis fest. Um solche Eingriffe zu rechtfertigen, bedarf es einer gesetzlichen Grundlage, die die Meinungsmacht der Intermediäre im Auge behält und im Sinne der Wechselwirkungstheorie⁵¹ die Schranken-Schranken von Art. 5 GG beachtet. Dabei ist insbesondere das Zensurverbot in Verbindung mit dem Grundsatz »keine Flucht ins Privatrecht« zu beachten. Gleichwohl ist der Balanceakt zwischen Sicherheit und Kommunikationsfreiheit kein einfacher und angesichts der Massen an täglich generierten Daten gibt es keine offensichtliche Lösung.

Auch ein Blick auf die Nutzung von Upload-Filtern zu anderen Zwecken hilft nur bedingt:

4.1. Neue Filter – alte Debatte?

Beim verdachtsunabhängigen Scannen und Löschen von Nutzerinhalten ist eine Parallele zur Vorratsdatenspeicherung⁵² erkennbar, bei der Daten verdachtsunabhängig massenhaft gespeichert wurden. Nach der Aufhebung des deutschen Umsetzungsgesetzes durch das Bundesverfassungsgericht 2010⁵³ hat zuletzt der EuGH einer quasi unbegrenzten Erhebung persönlicher Daten eine klare Absage erteilt.⁵⁴ Diese immer noch nicht abgeschlossene Debatte um die Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58/EG könnte im Zusammenhang mit Upload-Filtern wieder aufleben. Die verdachtslose

⁵¹ BVerfGE 7, 198 (209).

⁵² EU-Richtlinie 2002/58/EG

⁵³ BVerfGE 125, 260.

⁵⁴ EuGH (Große Kammer), Urt. v. 21.12.2016, ECLI:EU:C:2016:970.

Protokollierung und Speicherung sämtlicher Verkehrsdaten ist laut dem EuGH Ausnahmefällen vorbehalten und in der Form von Art. 15 Abs. 1 nicht erforderlich. Das Gericht stellt in seinem Urteil klare Bedingungen für die Umsetzung der Richtlinie auf.⁵⁵

4.2. Filter im Urheberrecht

Eine sehr ähnliche Position vertritt der EuGH im Hinblick auf das Urheberrecht. Man kommt beim Thema Upload-Filter nicht umhin, einen Blick auf den aktuellen Entwurf der EU-Richtlinie über das Urheberrecht im digitalen Binnenmarkt zu werfen. In Art. 13 ist die Rede von Maßnahmen zum Schutze der Werke, bzw. konkreter von »Maßnahmen wie beispielsweise wirksame Inhaltserkennungstechniken«.⁵⁶ Diese Pflicht trifft die »Diansteanbieter der Informationsgesellschaft«, also unter anderem die o. g. IT-Unternehmen. Auch hier ist der Wortlaut nicht eindeutig und den Unternehmen wird die konkrete Umsetzung überlassen. Der europäische Gerichtshof hat sich in den Vorlageentscheidungen *Scarlet/SABAM*⁵⁷ und *SABAM/Netlog*⁵⁸ klar gegen die Anordnung von Filtermechanismen ausgesprochen. Bei der Abwägung überwiegt laut EuGH die unternehmerische Freiheit der Provider, aber auch der Schutz personenbezogener Daten und die Informationsfreiheit.⁵⁹ Wenn der Entwurf von Art. 13 des Entwurfs der Urheberrechtsrichtlinie in der aktuellen Form in Kraft tritt, so sind die oben geprüften Grundrechtsverletzungen zu befürchten.

⁵⁵ EuGH, Urt. v. 21.12.2016, ECLI:EU:C:2016:970 Rn. 106.

⁵⁶ COM(2016) 593 final.

⁵⁷ EuGH (Dritte Kammer), Urt. v. 24.11.2011 - C-70/10.

⁵⁸ EuGH (Dritte Kammer), Urt. v. 16. 2. 2012 - C-360/10.

⁵⁹ EuGH, C-70/10, Rn. 49-50.

4.3. Inthaltekontrolle

Die Rolle von Algorithmen und die Zulässigkeit von Upload-Filtern sind zentrale Fragen der digitalen Medienlandschaft. Einerseits sind die Mengen an Informationen ohne Intermediäre nicht mehr zu bewältigen, andererseits nimmt deren Meinungsmacht stetig zu und die Konsequenzen kann zur Zeit niemand abschätzen. Gleichzeitig verbreiten sich strafrechtlich unzulässige Inhalte – wie die o. g. Terrorpropaganda oder Hassrede. Darauf reagierte der deutsche Gesetzgeber 2017 mit der Verabschiedung des Netzwerkdurchsetzungsgesetzes. Jenes soll der effizienteren Rechtsdurchsetzung bei Beschwerden über rechtswidrige Inhalte im Netz dienen, regelt aber nicht den Einsatz inhaltsfilternder Algorithmen. Aber schon hier befürchtet man sogenanntes Overblocking, also dass die sozialen Plattformen in der Praxis mehr sperren und löschen als erforderlich, um dem finanziellen Risiko des Bußgelds zu entgehen.⁶⁰ In diesem Kontext wird noch klarer, dass jegliche Form der Vorabkontrolle und -löschung durch private Upload-Filter verhindert werden muss, ganz im Sinne des absoluten Zensurverbots von Art. 5 Abs. 1 S. 3 GG.

Das Anwenden dieser Maßstäbe auch bei der Verpflichtung privater Akteure (wie die o. g. IT-Unternehmen) ist – angesichts der Macht dieser Akteure im digitalen Meinungsbildungsprozess – keine pauschale Absage an die Bekämpfung von terroristischen oder extremistischen Inhalten im Netz, allerdings sollte Rechtsdurchsetzung nicht auf Kosten der Meinungs- und Informationsfreiheit erfolgen.

⁶⁰ Drexl, ZUM 2017, 529 (540).

Quellen

- Baudrillard, J. (1978). *Requiem für die Medien*. Kool Killer oder Der Aufstand der Zeichen.
- Bethge, H., Sachs (Hrsg.) (2014). Grundgesetz-Kommentar, 7. Aufl. 2014, München.
- Drexl, J. (2017)., *Bedrohung der Meinungsvielfalt durch Algorithmen*. ZUM 2017, 529.
- Ecke, O., (2016). Wie häufig und wofür werden Intermediäre genutzt? - Die quantitative Perspektive der Zusatzbefragung in der MedienGewichtungs-Studie, *Die Medienanstalten*, <http://s.fhg.de/3HR>
- Eifert, M. (2017). Rechenschaftspflichten für soziale Netzwerke und Suchmaschinen. *NJW* 2017, S. 1450.
- Ernst, C. (2017). Algorithmische Entscheidungsfindung und personenbezogene Daten. *JuristenZeitung* 72, S. 1026.
- Eskens, S., Helberger, N., Moeller, J. (2017). Challenged by news personalisation: five perspectives on the right to receive information, *Journal of Media Law*.
- Grzeszick, B., Maunz/Dürig (Hrsg.) (2017). Grundgesetz-Kommentar, 81. EL. Hans-Bredow-Institut, Medien- und Kommunikationsbericht (2017), S. 209.
- Hartl, K. (2016). *Suchmaschinen, Algorithmen und Meinungsmacht – Eine verfassungs- und einfach rechtliche Betrachtung*.
- Hasebrink, U. (2016). Dossier »*Meinungsbildung und Kontrolle der Medien*, Bundeszentrale für politische Bildung, 09.12.2016, <http://s.fhg.de/zrH>.
- Hoffmann-Riem, W. (2017). *Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht*, AöR 142, 1.
- Hoffmann-Riem, W. (2001). Alternativkommentar-Grundgesetz, Art. 5, Lo-seblattsammlung 3. Aufl., München.
- Hoffmann-Riem, W. (2003). Mediendemokratie als rechtliche Herausforderung, *Der Staat* 42, S. 193.
- Jarass, H. D. Jarass/Pieroth (Hrsg.) (2014). Grundgesetz-Kommentar, 13. Aufl., München.

- Klein, Hans H. Maunz/Dürig (Hrsg.) (2017). Grundgesetz-Kommentar, 80. EL Juni 2017, München.
- Kloepfer, M. Isensee/Kirchhof (Hrsg.) (2005). Heidelberg: *Handbuch des Staatsrechts*, Band III, 3. Aufl.
- Koreng, A. (2010). *Zensur im Internet*.
- Ladeur, K.-H. (2001). *Ausschluss von Teilnehmern an Diskussionsforen im Internet – Absicherung von Kommunikationsfreiheit durch »netzwerk gerechtes« Privatrecht*, MMR 12/2001, S. 787 (791).
- Lischka, K., Stöcker, C. (2017). *Digitale Öffentlichkeit – Wie algorithmische Prozesse den gesellschaftlichen Diskurs beeinflussen*, Gütersloh: Bertelsmann-Stiftung.
- Löffler, M. (1969). *Das Zensurverbot der Verfassung*, NJW 1969, S. 2225-2256.
- Loosen, W., Scholl, A. (2017). *Journalismus und (algorithmische) Wirklichkeitskonstruktion. Epistemologische Beobachtungen*, M&K 65 (2) S. 348-366.
- Luhmann, N. (1996). *Die Realität der Massenmedien*. Opladen.
- Martini, M. (2017). *Algorithmen als Herausforderung für die Rechtsordnung*, JuristenZeitung 72, S. 1017.
- Microsoft. (2016). *A Cloud for Global Good*, Denkschrift, Microsoft Corporation.
- Monroy, M. (2017). *Social media companies launch upload filter to combat »terrorism and extremism«*, European Digital Rights (EDRi), abrufbar unter <http://s.fhg.de/9e2>.
- Monroy, M. (2017a). *»EU-Internetforum«: Viele Inhalte zu »Extremismus« werden mit Künstlicher Intelligenz aufgespürt*, auf netzpolitik.org, abrufbar unter <http://s.fhg.de/Y69>.
- Noltenius, J. (1958). Göttingen: *Die freiwillige Selbstkontrolle der Filmwirtschaft und das Zensurverbot des Grundgesetzes*.
- Oermann, M., Staben, J. (2013). *Mittelbare Grundrechtsreingriffe durch Abschreckung? – Zur grundrechtlichen Bewertung polizeilicher »Online-Streifen« und »Online-Ermittlungen« in sozialen Netzwerken*, *Der Staat* Bd. 52, 630 (637)

Piontek, H. (2016). *Warum die Uploadfilter der Internetkonzerne eine Gefahr für die Meinungsfreiheit sind*, netzpolitik.org.

Roth, W. (1994). Berlin: *Faktische Eingriffe in Freiheit und Eigentum – Struktur und Dogmatik des Grundrechtstatbestandes und der Eingriffsrechtfertigung*.

Ruttloff, M. *Der verwaltungsrechtliche Vertrag und das Recht der allgemeinen Geschäftsbedingungen*, DVBI 2013, 1415.

Schmidt, J-H., Merten, L., Hasebrink, U., Petrich, I., Rolfs, A. (2017). *Zur Relevanz von Online-Intermediären für die Meinungsbildung*, Arbeitspapiere des Hans-Bredow-Instituts Nr. 40.

Schnabel, C. (2008). *Böse Zensur, gute Filter?*, MMR 2008, 281.

Schulz, W., Dankert, K. (2016). *Die Macht der Intermediäre*, Friedrich-Ebert-Stiftung.

Schulze-Fielitz, H., Dreier (Hrsg.). (2013). *Grundgesetz Kommentar*, Bd. I, 3. Aufl.

Seeger, C. *Aktueller Begriff: Einsatz und Einfluss von Algorithmen auf das digitale Leben*, Wissenschaftlicher Dienst, Deutscher Bundestag.

Staben, J. (2016). Tübingen: *Der Abschreckungseffekt auf die Grundrechtsausübung*, S. 4.

Voßkuhle, A., Kaiser, A.-B. (2009). *Der Grundrechtseingriff*, JuS 2009, S. 313.

Waddell, K. (2016). *»A tool to delete beheading videos before they even appear online«*, TheAtlantic.com.

YouTube (2017), Mitteilung über Aktivitäten gegen Terrorismus und Extremismus, abrufbar unter <http://s.fhg.de/Ve4>.

Über die Autorin

Amélie P. Heldt

Amélie Heldt ist seit Mai 2017 Junior Researcher am Hans-Bredow-Institut für Medienforschung an der Universität Hamburg, im Forschungsprogramm »Transformation öffentlicher Kommunikation«.

Sie studierte französisches und deutsches Recht in Paris und Potsdam. Nach dem ersten Staatsexamen absolvierte sie ein Zusatzstudium in Design-Thinking am Hasso-Plattner-Institut und arbeitete in der Rechtsabteilung eines marktführenden Musiklabels. Ihr Rechtsreferendariat leistete sie am Kammergericht in Berlin ab; mit Stationen u.a. bei der Stiftung Oper, im »grünen« Bereich der Kanzlei Raue LLP und bei der GIZ in Kambodscha. In ihrem Promotionsvorhaben beschäftigt sie sich mit Meinungsfreiheit und Informationsintermediären.