

MAXIMILIAN MIKE JOSHUA SCHMIDT

Uploadfilter: Zensur im 21. Jahrhundert?

Internet und Gesellschaft

46

Mohr Siebeck

Internet und Gesellschaft
Schriften des Alexander von Humboldt Institut
für Internet und Gesellschaft

Herausgegeben von

Jeanette Hofmann, Matthias C. Kettemann,
Björn Scheuermann, Thomas Schildhauer
und Wolfgang Schulz

46



Maximilian Mike Joshua Schmidt

Uploadfilter: Zensur im 21. Jahrhundert?

Mohr Siebeck

Maximilian Mike Joshua Schmidt, Geboren 1994; Studium der Rechtswissenschaften in Tübingen, München und Durham (UK); Wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Recht der Wirtschaftsregulierung und Medien der Universität Mannheim; Doktorand an der Universität Mannheim; Rechtsreferendariat am Brandenburgischen Oberlandesgericht; 2025 Promotion.
orcid.org/0009-0004-1378-7380

Zugl.: Mannheim, Univ., Diss. 2025.

ISBN 978-3-16-164751-2 / eISBN 978-3-16-164752-9
DOI 10.1628/978-3-16-164752-9

ISSN 2199-0344 / eISSN 2569-4081 (Internet und Gesellschaft)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über <https://dnb.dnb.de> abrufbar.

© 2026 Mohr Siebeck Tübingen.

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für die Verbreitung, Vervielfältigung, Übersetzung und die Einspeicherung und Verarbeitung in elektronischen Systemen. Das Recht einer Nutzung der Inhalte dieses Werkes zum Zwecke des Text- und Data-Mining im Sinne von § 44b UrhG bleibt ausdrücklich vorbehalten.

Gedruckt auf alterungsbeständiges Papier.

Mohr Siebeck GmbH & Co. KG, Wilhelmstraße 18, 72074 Tübingen, Deutschland
www.mohrsiebeck.com, info@mohrsiebeck.com

Vorwort

Die Dissertation entstand im Wesentlichen während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Recht der Wirtschaftsregulierung und der Medien, in den Jahren 2020 bis 2023. Es war eine Zeit, geprägt von der Corona-Pandemie zum einen und einer schweren persönlichen Erkrankung zum anderen. Umso erfreulicher, dass Dissertation, Pandemie und Erkrankung heute hinter mir liegen.

Den Anstoß gab die lebhafteste öffentliche Debatte um Artikel 13 – in der Endfassung Artikel 17 – der Richtlinie über das Urheberrecht im digitalen Binnenmarkt. Im Zuge der Debatte wurden „Uploadfilter“ zum Symbol grundrechtlicher Spannungen und zu einer Leitfrage moderner Plattformregulierung. Die Arbeit zeichnet den verfassungs- und unionsrechtlichen Rahmen dieser politischen Diskussion nach und ordnet ihn systematisch.

Ich danke zunächst den Herausgeberinnen und Herausgebern der Schriftenreihe „Internet und Gesellschaft“ für die Aufnahme.

Mein besonderer Dank gilt meinem Betreuer Prof. Dr. Ralf Müller-Terpitz für seine verständnisvolle, stets freundliche Begleitung und den großen Freiraum, den er mir als wissenschaftlichem Mitarbeiter zum Schreiben eingeräumt hat. Prof. Dr. Nadine Klass, LL.M., danke ich für die zügige Zweitbegutachtung. PD Dr. Hannes Beyerbach stand mir über die Jahre als Ratgeber und Freund zur Seite, hierfür gilt ihm mein Dank.

Von Herzen danke ich auch meiner Mutter, meinen beiden Brüdern sowie meinen Freunden Bosse, Chris und Jenny. Eure vielfältige Unterstützung hat diese Arbeit möglich gemacht.

Allen Genannten und den vielen Ungenannten sage ich: Danke.

Inhaltsübersicht

Vorwort	V
Inhaltsverzeichnis	IX
1. Kapitel: Einleitung	1
§ 1 Zensur im Wandel der Zeit	1
§ 2 Das Internet und dessen Regulierung	2
§ 3 Filteralgorithmen und Uploadfilter	3
§ 4 Gang der Untersuchung	4
2. Kapitel: Untersuchungsgegenstand Uploadfilter	7
§ 1 Lernende Algorithmen	7
§ 2 Der Filteralgorithmus	11
§ 3 Herausforderungen von Uploadfilter	31
§ 4 Existierende Uploadfilter	37
§ 5 Zusammenfassung	40
3. Kapitel: Uploadfilter de lege lata	41
§ 1 Gesetzliche Regelungen	41
§ 2 Filterpflichten in der nationalen Rechtsprechung	72
§ 3 Privatrechtliche Filter	79
§ 4 Zusammenfassung und Ausblick	84
4. Kapitel: Grundrechtlicher Schutz filterrelevanter Inhalte	87
§ 1 Verfassungsrechtliche Vorbemerkungen	87
§ 2 Schutz filterrelevanter Äußerungstatbestände	102

5. Kapitel: Grundrechtsbindung des Filternden	123
§ 1 Zurechenbarkeit privater Eingriffe	123
§ 2 Privatautonome Filterung: Drittwirkung der Grundrechte	135
6. Kapitel: Das Zensurverbot	153
§ 1 Das Zensurverbot des GG	153
§ 2 Zensur im Unionsrecht	184
§ 3 Zwischenergebnis	201
7. Kapitel: Zensur durch Uploadfilter	203
§ 1 Zeitpunkt der Filterung	203
§ 2 Automatisierte Filterung als Zensurverfahren	207
§ 3 Die Folgen der Filterung als funktionales Äquivalent	240
§ 4 Filterung durch Private	246
§ 5 Zwischenergebnis	250
8. Kapitel: Verhältnismäßigkeitserwägungen	251
§ 1 Staatlich induzierte Filterung	251
§ 2 Privatautonome Filterung	263
9. Kapitel: Zusammenfassung und Ergebnisse	269
§ 1 Technische Ausgestaltung von Filteralgorithmen	269
§ 2 Automatisierung und Privatisierung der Rechtsdurchsetzung	270
§ 3 Grundrechtlicher Schutz der filterrelevanten Äußerungstatbeständen	271
§ 4 Das Zensurverbot	271
§ 5 Zensur durch Uploadfilter	272
§ 6 Verhältnismäßigkeitserwägungen	273
Literaturverzeichnis	275
Sachregister	291

Inhaltsverzeichnis

Vorwort	V
Inhaltsübersicht	VII
1. Kapitel: Einleitung	1
§ 1 Zensur im Wandel der Zeit	1
§ 2 Das Internet und dessen Regulierung	2
§ 3 Filteralgorithmen und Uploadfilter	3
§ 4 Gang der Untersuchung	4
2. Kapitel: Untersuchungsgegenstand Uploadfilter	7
§ 1 Lernende Algorithmen	7
A. Maschinelles Lernen	7
B. Support Vector Machine	9
C. Neuronale Netze	9
§ 2 Der Filteralgorithmus	11
A. Filtertechniken	11
I. Information Retrieval	11
II. Filterung nach Metadaten	12
III. Kryptografisches Hashing	13
IV. Content Fingerprinting	14
B. Filterung nach Medien	16
I. Inhaltsfilter	16
1. Audiofilter	16
a) Problemstellung	17
b) Beispiele der algorithmischen Umsetzung	17
2. Bildfilter	19
a) Blockhash-Algorithmen	19
b) Alternative Verfahren	20
3. Videofilter	21
a) Globales Fingerprinting	21

b) Lokales Fingerprinting	22
c) Auswahl der Filtermethode	23
II. Text- und Sprachfilter	23
1. Blacklisting	23
2. Natural Language Processing	24
3. Language Fingerprinting	24
4. Text in Multimediadateien	26
a) Text in Bildern	26
b) Text im gesprochenen Wort	27
III. Zusammenfassung	27
C. Vergleich der Datensätze	28
I. Datensätze	28
II. Suchalgorithmus	29
D. Entscheidung des Filters	29
E. Zusammenfassung	30
§ 3 Herausforderungen von Uploadfilter	31
A. Technische Limitationen des Hashing	31
B. Präzision und Genauigkeit	31
C. Umgang mit Sprache und Kontextverständnis	32
I. Hate Speech	33
II. Erkennung von Ausnahmeregelungen: Beispiel Satire	34
III. Zusammenfassung	35
D. Rechtliche Wertungen	35
E. Zusammenfassung	36
§ 4 Existierende Uploadfilter	37
A. Verfügbarkeit von Uploadfilter	37
B. Uploadfilter im Einsatz	38
§ 5 Zusammenfassung	40
3. Kapitel: Uploadfilter de lege lata	41
§ 1 Gesetzliche Regelungen	41
A. Die DSM-RL und deren nationale Umsetzung	41
I. Art. 17 Abs. 4 lit. b DSM-RL	41
1. Verpflichtete	43
2. Systematik des Art. 17 DSM-RL	43
a) Haftungsregelungen	44
b) Sonstige Regelungen	44
3. Einsatz von Uploadfiltern	45
a) Uploadfilter als hohe branchenübliche Standards	45
b) Alternativen zum Einsatz von Uploadfiltern	48
4. Entsprechende Filtertechnologien	50

a) Content Fingerprinting	51
b) Alternative Filtermechanismen	52
5. Ausnahmeregelung des Art. 17 Abs. 7 DSM-RL	53
a) Verhältnis zu Art. 17 Abs. 9 DSM-RL	53
b) Ausgestaltung wirksamer Vorkehrungen	55
6. Zwischenergebnis	56
II. Nationale Umsetzungsakte	56
1. UrhDaG	56
a) Pflicht zum Einsatz von Uploadfiltern	57
b) Ausnahmeregelungen	58
c) Unionsrechtswidrigkeit der Ausnahmeregelungen	59
2. Umsetzung in sonstigen Mitgliedstaaten	60
3. Bewertung	61
B. Filterincentivierende Regelungen	62
I. Unionsrecht	62
1. Digital Services Act	62
a) Rechtswidrige Inhalte und Desinformationen	62
b) Behördliche Anordnung (Art. 9 DSA)	63
c) Good Samaritan Clause (Art. 7 DSA)	63
d) Meldeverfahren (Art. 16 DSA)	65
2. TCO-Verordnung	65
a) Anwendungsbereich und Entfernungsanordnungen	66
b) Einsatz von Uploadfiltern	67
aa) Proaktive Maßnahmen (Art. 6 TCO-E)	67
bb) Spezifische Maßnahmen (Art. 5 TCO-VO)	67
c) Filterpflicht durch die Hintertür	69
3. Richtlinie über audiovisuelle Mediendienste (AVMD-RL)	69
II. Nationale Regelungen	70
1. NetzDG	71
2. Loi Avia	71
III. Uploadfilter zur (Über-)Erfüllung von Haftungsregelungen	72
§ 2 <i>Filterpflichten in der nationalen Rechtsprechung</i>	72
A. Rechtlicher Rahmen	72
B. Darstellung der Rechtsprechung	73
I. Internetversteigerung I bis III	73
II. Jugendgefährdende Medien	74
III. Kinderhochstühle im Internet I bis III	75
IV. Rapidshare I bis II	76
V. Gema/Youtube	77
C. Zusammenfassung	78
§ 3 <i>Privatrechtliche Filter</i>	79
A. Soft law	79

I. Code of conduct on countering illegal hate speech	80
II. Empfehlung der Kommission zu wirksamen Maßnahmen im Umgang mit illegalen Inhalten	81
III. Europäisches Konzept zur Bekämpfung von Desinformation im Internet	82
B. Nutzungsbedingungen	82
I. Meta	82
II. Youtube	83
§ 4 Zusammenfassung und Ausblick	84
4. Kapitel: Grundrechtlicher Schutz filterrelevanter Inhalte	87
§ 1 Verfassungsrechtliche Vorbemerkungen	87
A. Anwendung paralleler Grundrechtsregime	87
B. Eingrenzung der zensurrelevanten Kommunikationsgrundrechte ...	89
I. Äußerungsfreiheiten des Art. 5 Abs. 1 S. 1 GG	90
II. Informationsfreiheit (Art. 5 Abs. 1 S. 1 Alt. 2 GG)	91
III. Kunst- und Wissenschaftsfreiheit (Art. 5 Abs. 3 S. 1 GG)	92
IV. Zusammenfassung und Konsequenzen	93
C. Abgrenzung der Äußerungsfreiheiten	93
I. Meinungsäußerungsfreiheit und Medienfreiheiten	93
II. Kunst- und Wissenschaftsfreiheit	95
D. Schutz der Kommunikation im Internet	96
I. Schutz des Mediums Internet	96
II. Schutz internetspezifischer Handlungen	97
1. Nutzergenierte Inhalte	97
2. Social Plugins	98
E. Person des Äußernden	99
I. Nutzer	99
II. Plattform	100
§ 2 Schutz filterrelevanter Äußerungstatbestände	102
A. Fake News und Hate Speech	102
I. Terminologie	103
1. Fake News	103
2. Hate Speech	103
II. Schutz von Fake News	105
1. Schutz unwahrer Tatsachenbehauptungen im Allgemeinen	105
2. Schutz von Fake News im Speziellen	108
III. Schutz von Hate Speech	108
1. Diffamation	109
a) Schmähkritik und Formalbeleidigungen	109
b) Verbale Gewalt	111

2. Extremistische, antidemokratische und rassistische Äußerungen	112
IV. Kritik an der Tatbestandslösung	114
1. Allgemeine Kritik in der Literatur	114
2. Kritik am Wahrheitserfordernis für Tatsachenbehauptungen	114
3. Hate Speech	115
4. Stellungnahme	116
B. Urheberrechtsverstöße	116
I. Inanspruchnahme fremden Eigentums als Äußerungshandlung	117
1. Nach dem Grundgesetz	117
2. Nach der Grundrechtecharta	119
II. Konsequenzen für urheberrechtswidrige Uploads	120
C. Absolut gemeinschaftsschädliche Äußerungen	120
D. Ergebnis	122
 5. Kapitel: Grundrechtsbindung des Filternden	123
§ 1 Zurechenbarkeit privater Eingriffe	123
A. Eingriffsbegriffe	124
B. Filterung aufgrund einer gesetzlichen Pflicht	125
C. Filterung aufgrund von Soft Law	126
I. Mangelnde Kausalität	126
II. Zurechenbarkeit	127
III. Zwischenergebnis	128
D. Eingriff durch unbeabsichtigte Nebenfolgen der Filterung	128
I. Eingriff durch Abschreckung der Nutzer	128
1. Abschreckung als tauglicher Eingriff	129
2. Chilling Effects: Wirkung und Zurechenbarkeit	130
3. Unterlassen rechtswidriger Äußerungen	132
II. Eingriff durch Overblocking	133
III. Zusammenfassung	135
§ 2 Privatautonome Filterung: Drittwirkung der Grundrechte	135
A. Drittwirkung der Grundrechte im Grundgesetz	136
I. Von der mittelbaren zur unmittelbaren Drittwirkung der Grundrechte	136
III. Wandel der jüngeren Rechtsprechung	137
1. Gesteigerte Grundrechtsbindung im analogen Raum	137
2. Gesteigerte Grundrechtsbindung im digitalen Raum	139
IV. Bewertung der Entscheidungen in der Literatur	141
1. Zur (un)mittelbaren Drittwirkung der Versammlungsfreiheit	141
2. Zur (un)mittelbaren Drittwirkung des Gleichheitssatzes	142

V. Stellungnahme und Resümee	143
B. Die Drittwirkung der Grundrechte im Unionsrecht	145
I. Mittelbare Drittwirkung	145
II. (Un)Mittelbare Drittwirkung in der neueren Rechtsprechung ...	146
1. (Un)Mittelbare Anwendbarkeit des Art. 21 GRCh	146
2. (Un)Mittelbare Anwendbarkeit des Art. 31 Abs. 2 GRCh	147
III. Bewertung der neueren Rechtsprechung durch die Literatur ...	148
IV. Stellungnahme	149
C. Zusammenfassung und Konsequenzen	150
I. Zusammenfassung: Grundrechtsbindung Privater	150
II. Konsequenzen für die Bindung von Onlineplattformen an die Äußerungsfreiheiten	151
6. Kapitel: Das Zensurverbot	153
§ 1 Das Zensurverbot des GG	153
A. Rechtsqualität	154
I. Subjektiv-rechtlicher Abwehranspruch	154
II. Das Zensurverbot als Eingriffsschranke	155
1. Relative Eingriffsschranke	155
2. Absolute Eingriffsschranke	156
III. Objektiver Charakter des Zensurverbots	157
IV. Konsequenzen	158
B. Das Zensurverbot in der Rechtsprechung	159
I. Zeitpunkt	160
II. Verfahren	161
1. Zensur i. e. S.	161
a) Form	161
b) Inhalt	162
c) Zusammenfassung: Zensur i. e. S.	163
2. Zensurgleiche Maßnahmen (Zensur i. w. S.)	163
III. Adressat	164
IV. Zwischenergebnis	165
C. Erweiternde Definitionsansätze in der Literatur	165
I. Zeitpunkt	165
1. Ausdehnung auf die Nachzensur	166
2. Ausdehnung auf die Wirkungsentfaltung	167
II. Verfahren	168
1. Materieller Zensurbegriff	168
2. Verbot faktischer Zensur	169
III. Adressaten	170
1. Staatliche Zensur durch Private	170
2. Drittwirkung des Zensurverbotes	171

D. Stellungnahme und Konsequenzen	172
I. Zeitpunkt	172
1. Nachzensur	172
2. Ausdehnung auf den Zeitpunkt der Wirkungsentfaltung ...	174
a) Argumente für und wider die Ausdehnung	174
b) Lösung	175
c) Exkurs: Zeitpunkt der Wirkungsentfaltung im Detail ...	177
3. Zusammenfassung	179
II. Verfahren	179
1. Stellungnahme	179
2. Lösung	180
III. Adressat	181
1. Zur unmittelbaren Drittwirkung	181
2. Zum staatlichen Handeln durch Private	181
3. Zur mittelbaren Ausstrahlwirkung	182
E. Zusammenfassung	183
§ 2 Zensur im Unionsrecht	184
A. Grundsätzliche Zulässigkeit präventiver Eingriffe	184
B. Zulässigkeit von Zensur im Unionsrecht	186
I. Terminologie: Zensur und vorbeugende Maßnahmen	186
II. Zensur und der Wesensgehalt der Äußerungsfreiheiten	187
1. Wesensgehalt der Äußerungsfreiheiten	188
2. Zensur als Verstoß gegen den Wesensgehalt	189
a) Deutung der EGMR-Rechtsprechung	190
b) Deutung der EuGH-Rechtsprechung und der Schlussanträge	192
c) Konsequenz	193
B. Zensur in der Verfassungsüberlieferung der Mitgliedstaaten	193
I. Allgemeines Zensurverbot	193
II. Begrenztes Zensurverbot	196
III. Mitgliedstaaten ohne explizites Zensurverbot	198
IV. Analyse der Gemeinsamkeiten	200
C. Zwischenergebnis: Zensur im Unionsrecht	201
§ 3 Zwischenergebnis	201
7. Kapitel: Zensur durch Uploadfilter	203
§ 1 Zeitpunkt der Filterung	203
A. Uploadfilter i. e. S.	204
B. Uploadfilter i. w. S.	204
I. Wirkungsentfaltung im Internet	205
II. Parallelwertung im Unionsrecht	205

III. Konsequenzen für den Einsatz von Uploadfiltern i. w. S.	206
§ 2 <i>Automatisierte Filterung als Zensurverfahren</i>	207
A. Zulässigkeit des Einsatzes von Filteralgorithmen	208
I. Unionsrecht	208
II. Deutsches Verfassungsrecht	209
B. Grenzen des Einsatzes von Filteralgorithmen	210
I. Grenzen der Filterung im Unionsrecht	210
1. Verbot allgemeiner Überwachungspflichten	210
a) Sekundärrechtliche Verankerung	210
b) Primärrechtliche Verwurzelung	211
c) Filterpflichten als allgemeine Überwachungspflichten	212
aa) Abgrenzungstheorien	212
bb) Darstellung der Rechtsprechung	213
(1) Ursprünglich enge Auslegung	213
(2) Wandel der Rechtsprechung	215
(3) Zusammenfassung	217
cc) Rezeption der dargestellten Rechtsprechung	217
d) Stellungnahme und Konsequenzen für Überwachungspflichten	219
aa) Fehlerhafte Deutung der SABAM-Grundsätze	219
bb) Argumente gegen ein allgemeines Filterverbot	220
cc) Zusammenfassung	221
e) Kriterien spezifischer Überwachungspflichten im Detail	221
aa) Rechtswidrigkeit	222
(1) Maßstab der Rechtswidrigkeit	222
(2) Kenntnis und Kennenmüssen	224
bb) Sinnlichkeit	226
cc) Kontextabhängigkeit	227
dd) Konsequenzen	228
f) Zusammenfassung	228
2. Vergleich: Vorratsdatenspeicherung	229
a) Zulässigkeit der spezifischen Vorratsdatenspeicherung	229
b) Allgemeine und unterschiedslose Vorratsdatenspeicherung	230
c) Schlussfolgerungen für Onlineüberwachungspflichten	232
II. Grenzen der Filterung im deutschen Recht	233
C. Konturen des Zensurverfahrens im digitalen Raum	234
I. Allgemeine Überwachungspflichten als eine Art Zensur	234
II. Verbot der anlassunabhängigen automatisierten Überwachung	236
III. Kritische Verdichtung anlassabhängiger Überwachungspflichten	238

VI. Zusammenfassung	240
§ 3 <i>Die Folgen der Filterung als funktionales Äquivalent</i>	240
A. Chilling Effects	241
B. Overblocking	242
I. Overblocking im Allgemeinen	242
II. Systematisches Overblocking	243
1. Diskrepanz technischer Möglichkeiten und rechtlicher Pflichten	244
2. Vorsätzliches Overblocking	244
III. Zusammenfassung	245
§ 4 <i>Filterung durch Private</i>	246
A. Filterung aufgrund staatlicher Einflussnahme	246
I. Problemstellung	246
II. Mittelbare Zensur durch die Plattformbetreiber	247
B. Filterung aufgrund einer privatautonomen Entscheidung	248
§ 5 <i>Zwischenergebnis</i>	250
8. Kapitel: Verhältnismäßigkeitserwägungen	251
§ 1 <i>Staatlich induzierte Filterung</i>	251
A. Gesetzliche und weiche Filterpflichten	251
I. Legitimer Zweck gesetzlicher Filterpflichten	251
II. Zulässigkeit weicher Filterpflichten	253
B. Ausgestaltung der Filterung	255
I. Notwendige Informationen	255
II. Parametrisierung	256
1. Robustheit der Filter	256
2. Weitere Abwägungskriterien und Handlungsalternativen ...	257
a) Umgang mit Übereinstimmungen	258
b) Zeitkritikalität	258
c) Gefährdungspotenzial	259
aa) Quantitatives Gefährdungspotenzial (Verbreitungspotenzial)	259
bb) Qualitatives Gefährdungspotenzial	260
e) Einfluss des Nutzers und Rechteinhabers	260
C. Schutzmechanismen	261
I. Präventive technische Schutzvorkehrungen	262
II. Verfahrensgarantien	263
§ 2 <i>Privatautonome Filterung</i>	263
A. Zulässigkeit einer privatautonomen Filterung	263
B. Grenzen der privatautonomen Filterung	264

I. Anlass der Filterung	265
II. Schutzmechanismen gegen Overblocking	266
C. Zwischenergebnis	267
9. Kapitel: Zusammenfassung und Ergebnisse	269
§ 1 Technische Ausgestaltung von Filteralgorithmen	269
§ 2 Automatisierung und Privatisierung der Rechtsdurchsetzung	270
§ 3 Grundrechtlicher Schutz der filterrelevanten Äußerungstatbeständen	271
§ 4 Das Zensurverbot	271
§ 5 Zensur durch Uploadfilter	272
§ 6 Verhältnismäßigkeitserwägungen	273
Literaturverzeichnis	275
Sachregister	291

1. Kapitel

Einleitung

§ 1 Zensur im Wandel der Zeit

Kommunikation stellt das Fundament menschlicher Gesellschaften dar. Erst sie ermöglicht, Gemeinschaften zu bilden und Ideen auszutauschen. Für die moderne demokratische Gesellschaft stellt der freie Austausch von Meinungen sogar eine *conditio sine qua non* dar.¹ Dementsprechend wurde der Meinungsfreiheit auch wiederholt das Prädikat als eines der „vornehmsten Rechtsgüter“² bzw. der „vitale(n) Basis aller Rechte“³ zugesprochen. Demgegenüber stellt Zensur die Antipode einer freien Kommunikationsordnung dar; liegt Zensur vor, kann es keine freie Kommunikationsordnung geben.⁴ Das Zensurverbot wird als „Proklamation der Freiheit des Geistes“,⁵ „absolutes Existenzminimum“⁶ der Geistesfreiheit oder auch „Wesensgehalt“⁷ der Äußerungsfreiheiten umschrieben.

Die Bedeutung der Kommunikation führt dazu, dass schon seit jeher die Mächtigen versuchen, die Kommunikation zu kontrollieren. Schon im alten Rom kam dem „Censor“ neben seiner Aufgabe als Steuereintreiber auch die Wahrung der Sitten und Moral zu.⁸ Seit dem Mittelalter stellte Zensur einen „Akt

¹ Siehe hierzu auch die Ausführungen des BVerfGE 7, 198 (208): „Das Grundrecht auf freie Meinungsäußerung ist als unmittelbarster Ausdruck der menschlichen Persönlichkeit in der Gesellschaft eines der vornehmsten Menschenrechte überhaupt (un des droits les plus précieux de l'homme nach Artikel 11 der Erklärung der Menschen- und Bürgerrechte von 1789). Für eine freiheitlich-demokratische Staatsordnung ist es schlechthin konstituierend, denn es ermöglicht erst die ständige geistige Auseinandersetzung, den Kampf der Meinungen, der ihr Lebenselement ist (BVerfGE 5, 85 [205]). Es ist in gewissem Sinn die Grundlage jeder Freiheit überhaupt, the matrix, the indispensable condition of nearly every other form of freedom“ (Cardozo).“

² BVerfGE 4, 85 (134).

³ BVerfGE 39, 1 (42).

⁴ Siehe *Koreng*, in: Goerlich (Hrsg.), *Rechtsfragen der Nutzung und Regulierung des Internet*, S. 3 (13); *Warg*, DÖV 2018, 473 (475).

⁵ *Bethge*, in: Sachs (Hrsg.), GG, Art. 5, Rn. 130.

⁶ *Fiedler*, Die formale Seite der Äußerungsfreiheit, S. 246.

⁷ *Cornils*, in: Löffler et al. (Hrsg.), *Presserecht*, § 1 LPG, Rn. 261; *Gucht*, Das Zensurverbot im Gefüge der grundrechtlichen Eingriffskautalen, S. 165 ff. 188 ff.; *Koreng*, in: Goerlich (Hrsg.), *Rechtsfragen der Nutzung und Regulierung des Internet*, S. 3 (13); *Nessel*, Das grundgesetzliche Zensurverbot, S. 124; *Pfeifer*, Zensurbehütete Demokratie, S. 99 ff., 111 ff.

⁸ Siehe zur Wortgeschichte u. a. *Franke*, UFITA 2002/1, 89; *Fölsing* in: Schiwy/Schütz (Hrsg.), *Medienrecht: Lexikon für Wissenschaft und Praxis*, S. 516; *Pfeifer*, Zensurbehütete

der Freiheitsbeschränkung“ durch die Kirche oder den Staat dar.⁹ Ein historisches Beispiel hierfür ist die Literaturzensur der Kirche durch den „*Index librorum prohibitorum*“ von 1564.¹⁰ Zensur von Schriften war zunächst ein repressives Instrument zur Sanktionierung unliebsamer Ideen.¹¹ Das Verständnis von Zensur wurde jedoch seit jeher durch den technischen Wandel geprägt. Die Erfindung des Buchdrucks führte dazu, dass die Zensur ein weit verbreitetes Mittel zur Kontrolle der Kommunikationsordnung wurde. Die mit dem Buchdruck einhergehenden exponentiellen Verbreitungsmöglichkeiten von Ideen führten dazu, dass ein repressives Unterdrücken von einzelnen Schriften nicht länger hinreichend war.¹² Zensur wandelte sich damit einhergehend von einem repressiven zu einem präventiven Instrument.¹³ Ohne eine vorherige Erlaubnis wurde der Buchdruck verboten.¹⁴

§ 2 Das Internet und dessen Regulierung

Seit der Zeit des Buchdrucks stand die technologische Entwicklung der menschlichen Kommunikation nicht still. Insbesondere das Internet ermöglicht eine milliardenfache Verbreitung von Informationen in Sekunden.¹⁵ Anders als bei traditionellen Medien hat der Nutzer außerdem die Möglichkeit der gestaltenden Teilnahme.¹⁶ Die damit einhergehende gesellschaftliche Bereicherung hat aber auch dazu geführt, dass eine Kontrolle des Internets nur schwer möglich ist.¹⁷ Folglich kam es zu einer weitgehenden Deregulierung der Onlinekommunikation. Gerade in seinen Frühzeiten glich das Internet einem rechtsfreien Raum.¹⁸ Neben vielen positiven Effekten birgt eine solche Deregulierung auch gesellschaftliche Risiken. Das Internet ermöglichte die Verbreitung strafbarer Inhalte (Kinderpornografie, *Hate Speech* etc.) und führte zu einer teilweisen „Verro-

Demokratie, S. 186 f.; *Rieder*, Die Zensurbegriffe des Art. 118 Abs. 2 der Weimarer Reichsverfassung und Art. 5 Abs. 1 S. 3 des Bonner Grundgesetzes, S. 52.

⁹ *Fölsing* in: *Schiwy/Schütz* (Hrsg.), *Medienrecht: Lexikon für Wissenschaft und Praxis*, S. 516 f.

¹⁰ Dabei handelte es sich um eine Auflistung von Büchern, deren Lektüre als schwere Sünde galt; siehe *Franke*, UFITA 2002/1, 89.

¹¹ *Hopf*, ZUM 2000, 739 (740).

¹² *Hopf*, ZUM 2000, 739 (740).

¹³ *Hoffmann-Riem*, in: *Denninger et al.* (Hrsg.), *AK-GG*, Art. 5 Abs. 1, 2, Rn. 93; *Hopf*, ZUM 2000, 739 (740); *Koreng*, in: *Goerlich* (Hrsg.), *Rechtsfragen der Nutzung und Regulierung des Internet*, S. 3 (8).

¹⁴ *Hopf*, ZUM 2000, 739 (740).

¹⁵ *Heermann/Selzer*, CR 2019, 271 (271 Rn. 1).

¹⁶ *Senftleben*, ZUM 2019, 369.

¹⁷ Vgl. *De Streel et al.*, *Online Platforms' Moderation of Illegal Content Online*, 13.

¹⁸ Vgl. *Kraetzig/Lennartz*, NJW 2022, 2524 (2525), die ein „Gefühl herabgesetzter Rechtsbefolgung hinsichtlich Recht wie Moral“ beschreiben.

hung“ der öffentlichen Debatte.¹⁹ Dies hatte Rufe nach einer wirksamen Regulierung des Internets zur Folge. Dabei zeichnen sich mehrere Phänomene ab. Zum einen ist es dem Staat kaum mehr möglich, die Regulierung selbst durchzusetzen, weshalb er zunehmend auf die Plattformbetreiber zurückgreift.²⁰ Diese stellen den sog. *Cheapest Cost Avoider* dar, d. h. denjenigen, der das Auftreten eines Schadens mit den geringsten Kosten verhindern kann.²¹ Zum anderen bedarf es neuer Instrumente der Inhalterregulierung.

§ 3 Filteralgorithmen und Uploadfilter

Ein solches Instrument der Regulierung stellen die sog. *Filteralgorithmen* dar. Ein Algorithmus ist ein Verfahren zur schrittweisen Lösung von Problemen.²² Ein Filter stellt wiederum eine Vorrichtung dar, mit deren Hilfe Stoffe voneinander getrennt werden.²³ Der Filteralgorithmus lässt sich somit als ein Verfahren beschreiben, das Daten voneinander trennt und systematisiert. Die Komplexität dieser Filteralgorithmen erreicht dabei ein hohes Maß an Varianz. So gibt es einfache Filter, die lediglich eine Datei mit einer anderen vergleichen, und intelligente Filter, die mittels künstlicher Intelligenz riesige Datenbanken nach Übereinstimmungen durchsuchen.²⁴

Dabei können Filter dem Zweck dienen, Informationen zugänglich zu machen oder solche vorzuenthalten.²⁵ Ein solcher *negativer Filter*²⁶ kann in vielerlei Gestalten kommen: So wirkt jeder *positive Filter*²⁷ auch negativ, indem er Informationen zulasten anderer priorisiert;²⁸ für diese Arbeit relevanter sind jedoch die Filter, die Informationen bewusst vorenthalten. Dabei ist weiter zu unterscheiden, ob die Informationen präventiv oder repressiv vorenthalten werden.²⁹ Der

¹⁹ So die Gesetzesbegründung des NetzDG, siehe BT-Drs. 18/12356, S. 1; Nolte, ZUM 2017, 552 (553).

²⁰ Balkin, Harvard L. Rev. 124 XIII, 2296 (2304); Schiff, MMR 2018, 366 (369) der einen Trend zur „Privatisierung der Rechtsdurchsetzung“ beschreibt.

²¹ Ausführlich dazu OLG Hamburg, GRUR-RS 2015, 14370 (Rn. 392); Beaucamp, Rechtsdurchsetzung durch Technologie, S. 134 f.; zum Konzept des „cheapest cost avoiders“ siehe Schäfer/Ott, Lehrbuch der ökonomischen Analyse des Zivilrechts, S. 279.

²² Grumm/Sommer, Programmierung, Algorithmen und Datenstrukturen, S. 315.

²³ „Filter, der oder das: Vorrichtung, Gerät, mit dessen Hilfe feste Stoffe von flüssigen oder gasförmigen Stoffen getrennt werden“, aus Duden – Deutsches Universalwörterbuch 2023.

²⁴ Sartor/Loreggia, The impact of algorithms for online content filtering or moderation – „Uploadfilters“, S. 36.

²⁵ Goldmann, Yale Journal of Law & Technology, 8 I (2006), 188 (190 ff.); Müller-Terpitz, ZUM 2020, 365.

²⁶ Vgl. Müller-Terpitz, ZUM 2020, 365.

²⁷ Vgl. Müller-Terpitz, ZUM 2020, 365.

²⁸ Goldmann, Yale Journal of Law & Technology, 8 (2006), 188 (190 ff.).

²⁹ Müller-Terpitz, ZUM 2020, 365 (365 f.).

präventive Filter wirkt dabei bereits, bevor der Upload der Öffentlichkeit zugänglich gemacht wurde, der repressive hingegen danach.³⁰ Abstrakt ausgedrückt versteht man unter einem Uploadfilter ein System, das sich im Upload befindende Inhalte mit einer Datenbank vergleicht und aufgrund des Ergebnisses dieses Vergleiches eine Entscheidung über die Verfahrensweise mit diesem Upload trifft.³¹ Notwendig sind dazu drei Komponenten: eine Datenbank, die die geschützten oder verbotenen Inhalte beinhaltet, eine Filtersoftware, die die Inhalte auf eine Übereinstimmung mit der Datenbank überprüft, und zuletzt eine Software, die aufgrund des Ergebnisses der Filterung eine autonome Entscheidung trifft.³² Bei präventiven Filtern geschieht all dies, während sich der Upload noch im *Cache* (= Pufferspeicher) der Plattform befindet, d. h., bevor der Upload von anderen Nutzern wahrnehmbar ist.³³

§4 Gang der Untersuchung

Gerade diese präventiven Filteralgorithmen haben in der öffentlichen Debatte einen Aufschrei ausgelöst. Rund um den Gesetzgebungsprozess der *Richtlinie zum digitalen Binnenmarkt* (DSM-RL)³⁴ und insbesondere deren Art. 17 Abs. 4 lit. b DSM-RL wurde die Diskussion um eine „automatisierte Zensur“ laut.³⁵ Diese Rhetorik begleitet auch die Debatte um andere Regelungen zum Einsatz von Filteralgorithmen.³⁶

Die vorliegende Arbeit nimmt die öffentliche Debatte zum Anlass, zu untersuchen, ob der Einsatz von Filteralgorithmen – und im Speziellen von Uploadfiltern – tatsächlich Zensur darstellt. Hierzu werden zunächst der technische (Kapitel 2) und der einfachgesetzliche Rahmen (Kapitel 3) des Einsatzes von Uploadfiltern dargestellt. Anschließend werden die verschiedenen filterrelevanten

³⁰ Müller-Terpitz, ZUM 2020, 365 (365 f.).

³¹ Vgl. Raul/Steinebach, ZUM 2020, 355 (358).

³² Raul/Steinebach, ZUM 2020, 355 (358 f.).

³³ Heldt in: Mohabbat/Thapa/Parycek (Hrsg.), (Un)berechenbar?, Algorithmen und Automatisierung in Staat und Gesellschaft, 392 (398).

³⁴ Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17. April 2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG (ABl. L 130/92).

³⁵ So etwa: Hurtz, Dieser Kompromiss gefährdet das freie Netz, Süddeutsche Zeitung, 13.2.2019, abrufbar unter: <https://www.sueddeutsche.de/digital/Uploadfilter-ergebnis-eu-urheberrecht-1.4329775> (zuletzt abgerufen am 15.7.2025); siehe auch die Petition Stop the censorship-machinery! Save the Internet!, abrufbar unter: <https://www.change.org/p/european-parliament-stop-the-censorship-machinery-save-the-internet> (zuletzt abgerufen am 15.7.2025).

³⁶ Breyer, Teilerfolg gegen Internetzensur: EuGH schränkt Uploadfilter stark ein, abrufbar unter: <https://www.patrick-breyer.de/teilerfolg-gegen-internetzensur-eugh-schraenkt-uploadfilter-stark-ein/> (zuletzt abgerufen am 15.7.2025).

ten Äußerungstatbestände auf ihren grundrechtlichen Schutz untersucht (Kapitel 4). Sodann wird die Frage beantwortet, ob eine Filterung überhaupt einen Grundrechtseingriff durch einen Verpflichteten darstellt (Kapitel 5). Anschließend wird der zweite Untersuchungsgegenstand – die Zensur – ausführlich dargestellt (Kapitel 6). Dabei wird auch die Frage beantwortet, ob das Recht der Europäischen Union ein Zensurverbot gleich jenem des Grundgesetzes kennt. Im Anschluss wird die hier aufgeworfene Frage beantwortet, ob – und gegebenenfalls wann – eine automatisierte Filterung Zensur darstellt (Kapitel 7). Abschließend werden anhand dieser Erkenntnisse Rahmen für den verhältnismäßigen Einsatz von Uploadfiltern skizziert (Kapitel 8).

2. Kapitel

Untersuchungsgegenstand Uploadfilter

Die rechtliche Analyse des Einsatzes von Uploadfiltern setzt ein technisches Verständnis der Thematik voraus. Dieses Kapitel vermittelt dementsprechend einen grundlegenden Einblick in die Materie, soweit er für die folgende Diskussion notwendig sein wird. Insbesondere werden dabei die Funktionsweise von Filteralgorithmen und deren technische Limitationen betrachtet.

§ 1 Lernende Algorithmen

Bevor Filteralgorithmen im Speziellen beleuchtet werden können, bedarf es eines grundlegenden Einblicks in die Funktionsweise von Algorithmen. Ein Algorithmus ist ein Verfahren zur schrittweisen Lösung von Problemen.¹ Frühere Algorithmen stellten noch Programme dar, die strikt den aufgestellten Rechenregeln folgten.² Solche Systeme werden auch als „nicht lernende Algorithmen“ bezeichnet.³ Änderungen in der Berechnung und die Bewertung der Ergebnisse sind vom Programmierer abhängig.⁴ Im Kontrast hierzu stehen „lernende Algorithmen“. Diese sind flexibler gestaltet und können ihre Regeln an die ihnen gestellten Herausforderungen anpassen.⁵ Sie stellen somit eine Form der künstlichen Intelligenz dar und sind auch zur Lösung komplexer Probleme fähig.⁶ Im Folgenden wird ein kurzer Überblick über das Konzept des maschinellen Lernens und zwei der Methoden – die *Support Vector Maschine* (deutsch auch System-Vektoren-Maschine) und neuronale Netzwerke – geboten.

A. Maschinelles Lernen

Frühere Algorithmen folgten vordefinierten Rechenregeln, um die ihnen gestellte Aufgabe zu bewältigen.⁷ Demgegenüber definieren Systeme des maschinellen

¹ Grumm/Sommer, Programmierung, Algorithmen und Datenstrukturen, S. 315.

² Kastl, GRUR 2015, 136.

³ Vgl. Beaucamp, Rechtsdurchsetzung durch Technologie, S. 80.

⁴ Vgl. Beaucamp, Rechtsdurchsetzung durch Technologie, S. 80.

⁵ Vgl. Beaucamp, Rechtsdurchsetzung durch Technologie, S. 80.

⁶ Sartor/Loreggia, The impact of algorithms for online content filtering or moderation – „Uploadfilters“, S. 36.

⁷ Vgl. Wischmeyer, AöR 143 (2018), 1 (12).

Lernens diese Regeln selbst und sind dabei auch flexibel. Hierzu wird das Programm im Rahmen des maschinellen Lernens mit einem großen Datensatz „gefüttert“, diese Daten werden im Anschluss abstrahiert, um damit generalisierende Rechenregeln zu formulieren.⁸ Angesichts der Überlegenheit maschinellen Lernens gegenüber anderen Methoden der Erzeugung künstlicher Intelligenzen werden die Begriffe heute auch als Synonyme verwendet.⁹ Die verschiedenen Verfahren des maschinellen Lernens können im groben in drei Kategorien unterteilt werden: *Supervised Learning*, *Unsupervised Learning* und *Reinforcement Learning*.¹⁰

Supervised Learning stellt dabei ein Verfahren dar, bei dem der Algorithmus anhand von bereits klassifizierten Beispielen trainiert wird.¹¹ *Supervised Learning* wird in erster Linie angewendet, wenn bereits bekannt ist, wie die Datensätze klassifiziert werden müssen.¹² Anhand des Beispieldatensatzes kann der Algorithmus seine eigenen Rechenregeln aufstellen.¹³ Technisch geschieht dies durch eine Klassifizierung der Beispieldaten und einer darauf gestützten Regression.¹⁴ Wichtig ist dabei jedoch, dass sowohl die Eingabewerte als auch die Ausgabevariablen vollständig sind.¹⁵ Beispiele für derartige Algorithmen sind z. B. die *Naive-Bayes-Algorithmen* und *Support Vector Machines*.¹⁶ Ein Anwendungsgebiet hierfür ist u. a. die Spracherkennung.¹⁷

Wenn jedoch die Klassifizierung eines Datensatzes noch nicht bekannt ist, kommen als Methoden des maschinellen Lernens das *Unsupervised Learning* sowie das *Reinforcement Learning* in Betracht.¹⁸ Beim *Unsupervised Learning* arbeitet der Algorithmus weitestgehend ohne menschlichen Input.¹⁹ Der Algorithmus erhält hierfür nur einen Datensatz ohne jegliche Kennzeichnung und arbeitet autonom daran, Muster in jenem Datensatz zu erkennen.²⁰ Dementsprechend wird dieses Verfahren des maschinellen Lernens auch häufig als *Pattern Discovery* bezeichnet.²¹ Eine besondere Form hiervon ist das *Reinforcement Learning*.

⁸ Dutt/Chandramouli/Das, Machine Learning, Kap. 1.4.1; siehe hierzu auch Ertel, Grundkurs Künstliche Intelligenz, 2021, S. 201 ff.; Wischmeyer, AöR 143 (2018), 1 (11 f.).

⁹ Wischmeyer, AöR 143 (2018), 1 (11 f.).

¹⁰ Dutt/Chandramouli/Das, Machine Learning, Kap. 1.5; Sartor/Loreggia, The impact of algorithms for online content filtering or moderation – „Uploadfilters“, S. 37.

¹¹ Sartor/Loreggia, The impact of algorithms for online content filtering or moderation – „Uploadfilters“, S. 37.

¹² Dutt/Chandramouli/Das, Machine Learning, Kap. 1.5.4

¹³ Dutt/Chandramouli/Das, Machine Learning, Kap. 1.5.1.

¹⁴ Dutt/Chandramouli/Das, Machine Learning, Kap. 1.5.1.1 und 1.5.1.2; Wischmeyer, AöR 143 (2018), 1 (12).

¹⁵ Ertel, Grundkurs Künstliche Intelligenz, 2016, S. 313.

¹⁶ Dutt/Chandramouli/Das, Machine Learning, Kap. 1.5.4.

¹⁷ Dutt/Chandramouli/Das, Machine Learning, Kap. 1.5.4.

¹⁸ Dutt/Chandramouli/Das, Machine Learning, Kap. 1.5.4.

¹⁹ Ertel, Grundkurs Künstliche Intelligenz, 2016, S. 313.

²⁰ Dutt/Chandramouli/Das, Machine Learning, Kap. 1.5.2.

²¹ Engl. für „Muster-Erkennung“, siehe Dutt/Chandramouli/Das, Machine Learning, Kap. 1.5.2.

Diese ähnelt dem *Unsupervised Learning*, jedoch mit dem entscheidenden Unterschied, dass der Algorithmus Feedback für seine Leistung erhält.²² Hierdurch können positive oder negative Ansätze des Algorithmus verstärkt werden.²³ Diese Methoden werden z. B. in Empfehlungssystemen verwendet.²⁴

B. Support Vector Machine

Für das Lernen des Algorithmus selbst gibt es eine Vielzahl mathematischer Verfahren wie z. B. statistische Regressionen, Entscheidungsbäume etc.²⁵ Eine der gängigen Lernmethode stellt die *Support Vector Machine* (SVM) dar.²⁶ Hierbei handelt es sich um eine Form des *Supervised Learnings*, d. h., die Klassifizierung des Datensatzes ist bereits bekannt.²⁷ SVMs sind ein mathematisches Verfahren, das besonders nicht linear separierbare Klassen erlernen und darauf basierende Vorhersagen treffen kann.²⁸ Anhand eines Beispieldatensatzes konstruiert die SVM einen *Maximum Margin Seperator*²⁹, eine Trennlinie im hochdimensionalen Raum mit dem größtmöglichen minimalen Abstand zu den jeweiligen Beispieldatensätzen.³⁰ Wo diese Trennlinie genau zu ziehen ist, wird anhand einer Optimierungsfunktion berechnet.³¹ Diese Trennlinie stellt die Entscheidungsgrenze zwischen den gesuchten Klassifizierungen dar.³² Besonders nützlich ist die Methode des maschinellen Lernens bei linear separablen Datensätzen.³³ Sobald der Algorithmus im Erstellen dieser Trennlinien hinreichend trainiert ist, kann er entsprechend auch für unbekannte Datensätze eine Klassifizierung der Inhalte vornehmen.

C. Neuronale Netze

Bei *neuronalen Netzwerken* handelt es sich um ein Verfahren des maschinellen Lernens, das versucht, die Neuronen und Synapsen des menschlichen Gehirns zu imitieren.³⁴ Eine Vielzahl an spezialisierten Algorithmen (den Neuronen) arbeiten

²² Dutt/Chandramouli/Das, Machine Learning, Kap. 1.5.3.

²³ Ertel, Grundkurs Künstliche Intelligenz, 2016, S. 313.

²⁴ Dutt/Chandramouli/Das, Machine Learning, Kap. 1.5.4.

²⁵ Sartor/Loreggia, The impact of algorithms for online content filtering or moderation – „Uploadfilters“, S. 38.

²⁶ Ertel, Grundkurs Künstliche Intelligenz, 2016, S. 298.

²⁷ Dutt/Chandramouli/Das, Machine Learning, Kap. 1.5.4.

²⁸ Ertel, Grundkurs Künstliche Intelligenz, 2021, S. 340; Russell/Norvig, Artificial Intelligence: A Modern Approach, 692 f.

²⁹ Englisch für „Maximale-Margin-Klassifizierung“.

³⁰ Russell/Norvig, Artificial Intelligence: A Modern Approach, S. 692

³¹ Ertel, Grundkurs Künstliche Intelligenz, 2016, S. 298.

³² Russell/Norvig, Artificial Intelligence: A Modern Approach, S. 692.

³³ Ertel, Grundkurs Künstliche Intelligenz, 2021, S. 340.

³⁴ Dutt/Chandramouli/Das, Machine Learning, Kap. 10.1; Ertel, Grundkurs Künstliche Intelligenz, 2016, S. 265.

hierfür miteinander, um so eine Problemlösung zu ermöglichen.³⁵ Grundsätzlich existieren mindestens drei Kategorien an Neuronen: *Input*-, *Hidden*- und *Output-Neuronen*.³⁶ Jeder dieser künstlichen Neuronen hat eine spezialisierte Aufgabe, für die er Eingaben erhält und hieraus eine Ausgabe errechnet.³⁷ Ein Neuron teilt seine Ergebnisse nur mit seinen Nachbarneuronen, wenn es diese für relevant bewertet. Die Relevanz wird anhand einer Aktivierungsfunktion berechnet.³⁸ *Input-Neuronen* können z. B. im Rahmen der Bilderkennung mit der Wahrnehmung von Konturen oder Farben betraut sein.³⁹ Die *Hidden-Neuronen* errechnen anschließend die Bedeutung dieser Informationen und kombinieren die Daten mehrerer *Input-Neuronen*.⁴⁰ Schließlich errechnen die *Output-Neuronen* aus den erhaltenen Informationen die finale Ausgabe.⁴¹

Um einen Lerneffekt zu erzielen, werden die neuronalen Netzwerke typischerweise zunächst anhand eines Beispieldatensatzes mit vordefinierten Ergebnissen trainiert.⁴² Anschließend wird überprüft, ob das neuronale Netzwerk die Ergebnisse des Beispieldatensatzes an einem unbekannten Datensatz reproduzieren kann, wobei durch menschliches Feedback Fehler erkannt und korrigiert werden können.⁴³ Hierdurch erfolgt eine ständigen Neukalibrierung der Gewichtung verschiedener *Outputs* und der Schwelle, wann jener *Output* weitergesendet wird.⁴⁴

Eine Sonderform der neuronalen Netzwerke stellt das sog. *Deep Learning* dar.⁴⁵ Dabei wird ein vielschichtiges neuronales Netzwerk genutzt, das in der Lage ist, auch komplexere Probleme zu lösen.⁴⁶

³⁵ Sartor/Loreggia, The impact of algorithms for online content filtering or moderation – „Uploadfilters“, S. 38.

³⁶ Englisch für „Eingabe-, Versteckte- und Ausgabe-Neuronen“; vgl. Russell/Norvig, Artificial Intelligence: A Modern Approach, S. 750 ff.

³⁷ Krogh, Nature Biotechnology 32 (2008), S. 195.

³⁸ Dutt/Chandramouli/Das, Machine Learning, Kap. 10.3; Sartor/Loreggia, The impact of algorithms for online content filtering or moderation – „Uploadfilters“, S. 38

³⁹ Dickson, What are Artificial Neural Networks?, abrufbar unter: <https://bdtechtalks.com/2019/08/05/what-is-artificial-neural-network-ann/> (zuletzt abgerufen am 15.7.2025).

⁴⁰ Russell/Norvig, Artificial Intelligence: A Modern Approach, S. 751.

⁴¹ Russell/Norvig, Artificial Intelligence: A Modern Approach, S. 750 ff.

⁴² Dickson, What are Artificial Neural Networks?, abrufbar unter: <https://bdtechtalks.com/2019/08/05/what-is-artificial-neural-network-ann/> (zuletzt abgerufen am 15.7.2025).

⁴³ Dickson, What are Artificial Neural Networks?, abrufbar unter: <https://bdtechtalks.com/2019/08/05/what-is-artificial-neural-network-ann/> (zuletzt abgerufen am 15.7.2025).

⁴⁴ Krogh, Nature Biotechnology 32 (2008), S. 195 (196 f.).

⁴⁵ Ertel, Grundkurs Künstliche Intelligenz, 2016, S. 299 f.

⁴⁶ Dutt/Chandramouli/Das, Machine Learning, Kap. 10.9; Ertel, Grundkurs Künstliche Intelligenz, 2016, S. 299 f.

Sachregister

- Absolute Eingriffsschranke 154–159,
172, 179–180, 193–194, 271
- Algorithmus 3, 7
- Allgemeine Überwachungspflichten 211–
221, 234–240
 - Abgrenzung zu spezifischen
Überwachungspflichten 212–217,
220–229
 - unionsrechtliche Grundlagen 212–
221, 248
 - Zensur durch 234–240
- Art. 10 EMRK 107, 113, 184
- Art. 11 GRCh 94, 99–100, 105, 132,
151, 208, 230
- Art. 5 GG 91, 154–159
- Audible Magic 32, 37–38, 47, 51–52,
- Audiofilter 16–19, 21
- Ausstrahlwirkung 136, 149, 157–159,
176–183, 197, 206–207, 250, 271

- Bildfilter 19–21
- Blacklisting 23, 55
- Blockhash-Algorithmen 19–20

- Cache 4, 47
- Cheapest Cost Avoider 3, 84
- Chilling Effects 107, 116, 128–132,
241–242
 - Begriffsverständnis 128–129
 - Eingriff durch 129–133
 - Zensur durch 241–242
- Clustering 15, 25
- Code is Law 256
- Code of Conduct on Countering Illegal
Hate Speech 28, 80
- Community Standards 39
- Content Fingerprinting 14–27, 31, 38–
40, 47, 51, 53
 - Begriff 14–16
 - globales und lokales
Fingerprinting 21–22
- Content ID 14–17, 28, 30, 32, 36–38, 47,
51, 78, 84

- Database of Hashs 28, 80,
- Datenbank 3–4, 11–12, 15, 28–29, 38–
40, 80
- Deep Learning 10, 27, 34
- Desinformation *siehe* Fake News
- Digital Services Act 61–65, 70, 78–79,
209, 211, 221, 224, 235, 245
- Digital Single Market Directive (DSM-
RL) 41–61, 125, 186, 216, 221–224,
248
- Direct Effect *siehe* Drittwirkung der
Grundrechte
- Drittwirkung der Grundrechte 136–152
 - im Grundgesetz 136–145
 - im Unionsrecht 145–151
 - mittelbare Drittwirkung 136–137
 - Wandel der Rechtsprechung 137–141
- E-Commerce-Richtlinie (EC-RL) 62–65
- Eingriff
 - durch Abschreckung 129–130
 - durch Chilling Effects 130–1333
 - durch Overblocking 133–135
 - Grundrechtsbindung Privater *siehe*
grundrechtsbindung Privater
 - Zurechenbarkeit 124–134
- Eingriffsbegriffe 124–125

- Fake News 35, 63, 71, 82, 102–108
 - Begriff 63
 - grundrechtlicher Schutz *siehe* Schutz
unwahrer Tatsachenbehauptungen
- Faktische Zensur 169, 180
- Filteralgorithmen 3, 4, 7, 17, 31–32, 35,
37, 40, 65, 72–73, 78, 83–85

- Begriff und Funktionsweise 3, 4, 7
- Entscheidung des Filters 17–18
- Herausforderungen *siehe* Technische Limitationen
- Suchalgorithmus 29–30
- Technische Ausgestaltung 11–26
- Typen 3
- Filterpflichten 45–47, 53, 55–57, 60, 72–77, 84, 87
- Alternativen 48, 53–55
- Ausnahmeregelungen 55–57
- Incentivierende Regelungen 62–72
- nationale Rechtsprechung 72–78
- Uploadfilter als hohe branchenüblicher Standard *siehe* hohe branchenübliche Standards
- Formalbeleidigung 106–109
- Formeller Zensurbegriff 163, 168–169, 180–183, 241, 271

- Grundgesetz 91, 97–100, 1123–150, 153–161
 - Art. 5 GG 91, 97–100, 154–160
 - Grundrechtsbindung 123–150
 - objektive Wertordnung 136
 - Zensurverbot 153–160
- Grundrechtecharta 144–149, 151, 184–201
 - Art. 11 GRCh 90–97, 102, 132, 151, 208, 230
 - Drittwirkung *siehe* Drittwirkung der Grundrechte
 - Verhältnis zum Grundgesetz *siehe* parallele Grundrechtsregime
- Grundrechtlicher Schutz filterrelevanter Inhalte 87–122, *siehe auch* Fake News; Hate Speech
- Grundrechtsverpflichteter 141–149

- Hamming-Wert 16, 25–26, 256, 261
- Hash 13–22, 25
 - Hashing Bedeutung 13–14
 - Verfahren *siehe* kryptografisches Hashing, Content Fingerprinting
- Hate Speech 102–116
 - Begriff 102–105
 - grundrechtlicher Schutz 108–116
 - hohe branchenübliche Standards 45–49, 55
- Information Retrieval 11–12
- Informationsfreiheit 91–92
- Intermediäre 124–132, 135, 210–229, 223–249, 262–264

- Kommunikationsgrundrechte 88–92, 121
- Kryptografisches Hashing 13–14
- Kunstfreiheit 92, 95–96, 114–120
- Künstliche Intelligenz 5–8, 24, 26

- Language Fingerprinting 24
- Lernende Algorithmen 7, *siehe auch* Maschinelles Lernen
- Loi Audiovisuelle 60
- Loi Avia 68, 196

- Machine Learning *siehe* Maschinelles Lernen
- Maschinelles Lernen 7–8, 34, 83
- Materieller Zensurbegriff 168–169, 179–180
- Maximum Margin Separator *siehe* Support Vector Machine
- Medienfreiheiten 93–98
- Meinungsäußerungsfreiheit 87–116, 253
 - Abgrenzung zu Medienfreiheiten 93–95
 - als Abwehrrecht 142, 160, 179
 - als Wertausdruck *siehe* objektive Werteordnung
- Multimediateilen 23, 28, 48
 - Text im gesprochenen Wort 27
 - Text in Bildern 23

- Nachzensur 92, 155, 165–168, 172–174, 204
- Naive-Bayes-Algorithmen 8, 24,
- Natural Language Processing 24, 30
- Netzwerkdurchsetzungsgesetz (NetzDG) 63, 70–72, 134

- neuronale Netze 7–9, 26–27, *siehe auch*
 - Convolutional Neural Networks;
 - Deep Learning
- Notice-and-take-down 46–50, 58–60, 63, 73, 133, 209, 216
- Nutzungsbedingungen 67, 70, 82–84, *siehe auch* Community Standards
- Overblocking 128–135, 240–246
 - Begriff 128–132
 - Eingriff durch Overblocking 128–135
 - Zensur durch Overblocking 240–246
- Parallele Grundrechtsregime 87
- Plattform 1, 42–56, 64, 69–84 97–104, 135, 140, 151–152, 241–246, 255, 264–267
- Präventive Filterung 3–5, 58, 70, 81, 203, 210
 - Begriff 3–5
 - Unterscheidung zur repressiven Filterung 3
 - Zensur durch 203–204, 210, 235
- Privatautonomie Filterung 135–150, 248–250, 263–267
 - Drittwirkung der Grundrechte *siehe* Drittwirkung
 - Verhältnismäßigkeit *siehe* Verhältnismäßigkeitserwägungen
- Proaktive Maßnahmen 41, 66–67, 78–81, *siehe auch* vorbeugende Maßnahmen
- Pufferspeicher *siehe* Cache
- Regulierung 1–3, 36, 41–45, 69–72, 79–84, 125–128, 133–135, 150, 182, 218–221, 250, 254–262
- Reinforcement Learning 8–9
- Robust Perceptual Hashing *siehe* Content Fingerprinting
- Robustheit 15–16, 19, 22, 27
- Schmähkritik 106–109
- Schutz unwahrer Tatsachenbehauptungen 105
- Sinnleichheit 226–227
- Social Plugins 97–98, 117
- Soft Law 79–80
 - Code of Conduct 79
 - Empfehlungen der Kommission zu wirksamen Maßnahmen im Umgang mit illegalen Inhalten 79–80
 - Europäisches Konzept zur Bekämpfung von Desinformation 79–80
- Staatsähnliche Grundrechtsbindung 137–145, 147–150
- Stay-down-Verfahren 44–46, 58–60, 208–209, 216
- Supervised Learning 8, 9, 24, 27, 34
- Support Vector Machine 7–9, 34
- Tatbestandslösung 114–230
- Technische Limitationen 31–32, *siehe auch* False Negatives; False Positives
- Text- und Sprachfilter 16, 23–27, *siehe auch* Language Fingerprinting; Natural Language Processing
- Unsupervised Learning 8, 9, 15, 55
- Upload 3–12, 45–65, 72–84, 87, 116–122
- Uploadfilter
 - als hohe branchenübliche Standards *siehe* hohe branchenübliche Standards
 - Begriff 3–5
 - Einsatz und Alternativen 45–55, 180, 254–257, 262
 - Funktionsweise 7–29
 - gesetzliche Regelungen 41–84
 - im engeren Sinne 3–5
 - im weiteren Sinne 3–5
 - Überwachungspflichten 212–234
 - Zensur durch 203–250
- Urheberdiensteanbietergesetz (UrhDaG) 38, 53–59, 76, 258, 273
- Urheberrechtsverstöße 116–120
- User Generated Content 97–98
- Value Gap 39
- Verfassungsprinzip 154–158, 176, 180

- Verfassungsüberlieferung der Mitgliedstaaten 193–200
- Verhältnismäßigkeit 33–57, 142–150, 251–267
 - privatautonome Filterung 263–264
 - staatlich induzierte Filterung 251–259
- Videofilter 21–22
- Vorbeugende Maßnahmen 78, 186–187, 194, *siehe auch* proaktive Maßnahmen
- Vorratsdatenspeicherung 131, 229–232, 237
- Vorzensur 156, 160, 165–166, 173–179, 186, 190, 194, 197, 200, 203–206
- Watermarking 14, 48, 52
- Wesensgehalt der Äußerungsfreiheiten 157–156, 186–193
- Wirkungsentfaltung 167, 174–179, 204–207
- Wissenschaftsfreiheit 92, 95–96
- Zeitkritikalität 60, 158, 258–262
- Zensur
 - Adressat 164, 170–171
 - Begriff und historische Entwicklung 1–2
 - durch automatisierte Filterung 203–250
 - durch Chilling Effects *siehe* Chilling Effects
 - durch Overblocking *siehe* Overblocking
 - funktionales Äquivalent 169, 240–246
 - Nachzensur *siehe* Nachzensur
 - Qualität 153–160, *siehe auch* Absolute Eingriffsschranke
 - Verfahren 160–162, *siehe auch* Vorbeugende Maßnahmen; Materieller Zensurbegriff
 - Vorzensur *siehe* Vorzensur
- Zensurgleiche Maßnahmen 163–165, 169–170, 181, 233, 241–242