Huawei Wang

Die strafrechtliche Verantwortlichkeit von Internet-Service-Providern

Schriftenreihe des Max-Planck-Instituts für
ausländisches und internationales Strafrecht

Strafrechtliche Forschungsberichte

Herausgegeben von Ulrich Sieber

Band S 163

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Die strafrechtliche Verantwortlichkeit von Internet-Service-Providern

Ein deutsch-chinesischer Rechtsvergleich

Huawei Wang

Duncker & Humblot · Berlin

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Vertrieb in Gemeinschaft mit Duncker & Humblot GmbH, Berlin
http://www.duncker-humblot.de

Umschlagbild: © http://699pic.com/tupian-500729179.html 摄图网
Foto des Autors: Huawei Wang
Druck: Stückle Druck und Verlag, Stückle-Straße 1, 77955 Ettenheim
Printed in Germany
Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ∴

ISSN 1860-0093
ISBN 978-3-86113-781-8 (Max-Planck-Institut)
ISBN 978-3-428-15701-3 (Duncker & Humblot)
DOI https://doi.org/10.30709/978-3-86113-781-8

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2017 von der Rechtswissenschaftlichen Fakultät der Universität Freiburg i. Br. als Dissertation angenommen.

Für meine Doktorarbeit schulde ich vielen Menschen meinen herzlichen Dank. Zunächst möchte ich mich bei meinem Doktorvater Prof. Dr. Dr. h.c. mult. *Ulrich Sieber* für seine kompetente Unterstützung und Betreuung bedanken. Ohne seine wertvollen Hinweise und Vorschläge wäre diese rechtsvergleichende Untersuchung nicht möglich gewesen. Weiter danke ich Prof. Dr. Dr. h.c. mult. *Hans-Jörg Albrecht* für die schnelle und zügige Erstellung des Zweitgutachtens.

Besonders möchte ich meinem chinesischen Doktorvater Prof. Dr. *Genlin Liang* danken, der mein Studium im Ausland unterstützt und gefördert hat. Insoweit danke ich auch Dr. *Zunyou Zhou*, der mir bei meinem Aufenthalt in Deutschland auf verschiedene Weise geholfen hat.

Schließlich gebührt *Ines Hofmann* und *Dorothea Borner-Burger*, die meine Dissertation sorgfältig korrigiert und optimiert haben, Dank.

Peking, im Dezember 2018 *Huawei Wang*

Inhaltsübersicht

Vorwort V

Inhaltsverzeichnis X

Abkürzungsverzeichnis XVI

Einleitung

I. Problemstellung 1

II. Gegenstand der Untersuchung 3

A. Technische Grundlagen der ISP 3

B. Vergleichende Untersuchung der deutschen und der chinesischen Rechtslage 4

C. Auswirkungen des Internets auf die traditionelle Strafrechtslehre 6

D. Balance zwischen Freiheit und Sicherheit 6

III. Ziele der Untersuchung 7

IV. Methode der Untersuchung 7

V. Gang der Untersuchung 8

Erster Teil
Technische Grundlagen

I. Technische Grundlagen des Internets und der Netzwerktechnik 9

A. Entwicklung des Internets und der Netzwerktechnik 9

B. Grundlagen der Netzwerktechnik 11

C. Kriminelle Risiken im Netz 13

II. Technische Grundlagen im Bereich der ISP 15

A. Entstehung und Entwicklung der ISP 15

B. Typen der ISP 15

C. Risiken für die ISP 17

III. Technische Kontrollmöglichkeiten der ISP 18

A. Grundlagen der Kontrollmöglichkeit 18

B. Die technische Entwicklung und ihre Folgen 19

C. Unterschiede zwischen faktischen und normativen Kontrollmöglichkeiten 21

Zweiter Teil
Verantwortlichkeit der ISP in Deutschland

I. Historische Entwicklung, Begriff und Typen der ISP ... 23
A. Historische Entwicklung ... 23
B. Rechtliche Begriffe ... 24
C. Rechtliche Typen der ISP ... 26

II. Allgemeine internetspezifische Verpflichtungen und Privilegien der ISP ... 30
A. Allgemeine Verpflichtungen der ISP nach dem TMG ... 30
B. Allgemeine Privilegierungen der ISP im TMG ... 32
C. Neuregelungen des Netzwerkdurchsetzungsgesetzes 2017 ... 47

III. Allgemeine strafrechtliche Verantwortlichkeit der ISP ... 50
A. Beziehung zwischen StGB und den Verantwortlichkeitsregelungen im TMG ... 50
B. Einschlägige Straftatbestände im Besonderen Teil des StGB ... 53
C. Einordnung der Handlungen der ISP als Tun oder Unterlassen ... 54
D. Strafrechtliche Garantenpflichten der ISP ... 57
E. Vorsatzerfordernisse der strafrechtlichen Verantwortlichkeit ... 68
F. Einordnung der Handlungen als Täterschaft oder Teilnahme ... 71

IV. Gesetzlich nicht geregelte Typen der ISP und ihre Verantwortlichkeit ... 74
A. Peer-to-Peer-Netzwerke ... 74
B. Hyperlinks ... 85

Dritter Teil
Verantwortlichkeit der ISP in China

I. Historische Entwicklung, Begriff und Typen der ISP ... 95
A. Historische Entwicklung ... 95
B. Rechtliche Begriffe der ISP ... 96
C. Rechtliche Typen der ISP ... 97

II. Allgemeine und zivilrechtliche internetspezifische Verpflichtungen und Privilegien der ISP ... 102
A. Grundlegender Rechtsrahmen ... 102
B. Allgemeine Verpflichtungen der ISP ... 105
C. Zivilrechtliche Privilegierungen ... 108

III. Allgemeine strafrechtliche Verantwortlichkeit der ISP ... 114
A. Die Beziehung zwischen dem chStGB und den Verantwortlichkeitsregelungen in anderen Gesetzen ... 114
B. Grundlegender Rechtsrahmen im strafrechtlichen Bereich ... 116
C. Einordnung der Handlung der ISP als Tun oder Unterlassen ... 125

D. Strafrechtliche Garantenpflichten der ISP 129
E. Vorsatzerfordernisse 140
F. Einordnung als Täterschaft oder Teilnahme 146

IV. Gesetzlich nicht geregelte Typen der ISP und ihre Verantwortlichkeit 161
A. Peer-to-Peer-Netzwerke 161
B. Hyperlinks 169

Vierter Teil
Zusammenfassender Vergleich

I. Rechtliche Begriffe der ISP 176
A. Deutschland 176
B. China 176

II. Rechtliche Typen der ISP 177
A. Deutschland 177
B. China 177

III. Internetspezifische Privilegien der ISP 178
A. Deutschland 178
B. China 180

IV. Allgemeine strafrechtliche Verantwortlichkeit der ISP 181
A. Deutschland 181
B. China 182

V. Allgemeine kriminalpolitische Bewertung 185

Literaturverzeichnis 188

Inhaltsverzeichnis

Vorwort V

Inhaltsübersicht VII

Abkürzungsverzeichnis XVI

Einleitung

I. Problemstellung 1

II. Gegenstand der Untersuchung 3

A. Technische Grundlagen der ISP 3

B. Vergleichende Untersuchung der deutschen und der chinesischen Rechtslage 4

C. Auswirkungen des Internets auf die traditionelle Strafrechtslehre 6

D. Balance zwischen Freiheit und Sicherheit 6

III. Ziele der Untersuchung 7

IV. Methode der Untersuchung 7

V. Gang der Untersuchung 8

Erster Teil
Technische Grundlagen

I. Technische Grundlagen des Internets und der Netzwerktechnik 9

A. Entwicklung des Internets und der Netzwerktechnik 9

1. Entstehung des Internets 9

2. Entwicklung des Web 1.0, des Web 2.0 und des Web 3.0 10

B. Grundlagen der Netzwerktechnik 11

1. Grundlegende Struktur des Netzwerks 11

2. Grundlegende Begriffe der Netzwerktechnik 12

a) LAN, MAN und WAN 12

b) ICP/IP 12

C. Kriminelle Risiken im Netz 13

II. Technische Grundlagen im Bereich der ISP 15

A. Entstehung und Entwicklung der ISP 15

B. Typen der ISP ... 15
C. Risiken für die ISP ... 17

III. Technische Kontrollmöglichkeiten der ISP ... 18
A. Grundlagen der Kontrollmöglichkeit ... 18
B. Die technische Entwicklung und ihre Folgen ... 19
C. Unterschiede zwischen faktischen und normativen Kontrollmöglichkeiten ... 21

Zweiter Teil
Verantwortlichkeit der ISP in Deutschland

I. Historische Entwicklung, Begriff und Typen der ISP ... 23
A. Historische Entwicklung ... 23
B. Rechtliche Begriffe ... 24
C. Rechtliche Typen der ISP ... 26
1. Kriterium für die Typisierung ... 26
2. Rechtliche Typen der ISP ... 26
3. Unterscheidung zwischen zwei Zwischenspeicherungen ... 28

II. Allgemeine internetspezifische Verpflichtungen und Privilegien der ISP ... 30
A. Allgemeine Verpflichtungen der ISP nach dem TMG ... 30
1. Umfang der allgemeinen Verpflichtung ... 30
2. TMG und Störerhaftung ... 30
3. Anwendbarkeit im Strafrecht? ... 31
4. Zwischenergebnis ... 32
B. Allgemeine Privilegierungen der ISP im TMG ... 32
1. Verantwortlichkeit von Content Providern ... 32
2. Privilegien von Access Providern ... 33
a) Grundlage der Privilegierung für Access Provider ... 34
b) Konkrete Bedingungen der Privilegierung der Access Provider ... 34
c) Reichweite der Vorschrift ... 36
aa) Gesetzliche Anwendungsfälle ... 36
bb) Gesetzlich nicht geregelte Anwendungsfälle ... 37
3. Privilegien von Caching Providern ... 38
a) Grundlage der Privilegierung für Caching Provider ... 38
b) Konkrete Bedingungen der Privilegierung der Caching Provider ... 39
4. Privilegien von Hosting Providern ... 40
a) Grundlagen der Privilegierung für Hosting Provider ... 40
b) Konkrete Bedingungen der Privilegierung der Hosting Provider ... 41
aa) Vorsatz ... 41
bb) Gegenstand der Kenntnis ... 43
cc) Art der Kenntniserlangung von Informationen ... 46
dd) Unverzügliche Tätigkeit nach Kenntniserlangung ... 46

C. Neuregelungen des Netzwerkdurchsetzungsgesetzes 2017 ... 47
1. Hauptinhalte der Neuregelungen ... 47
2. Bewertung der Neuregelungen ... 47

III. Allgemeine strafrechtliche Verantwortlichkeit der ISP ... 50
A. Beziehung zwischen StGB und den Verantwortlichkeitsregelungen im TMG ... 50
1. „Vorfilterlösung“ ... 50
2. „Integrationslösung“ ... 51
3. Eigene Stellungnahme ... 52
B. Einschlägige Straftatbestände im Besonderen Teil des StGB ... 53
C. Einordnung der Handlungen der ISP als Tun oder Unterlassen ... 54
1. Abgrenzung von Tun und Unterlassen ... 54
2. Einordnung der Handlungen der ISP als Tun oder Unterlassen ... 55
D. Strafrechtliche Garantenpflichten der ISP ... 57
1. Allgemeine strafrechtliche Garantenstellungen ... 57
2. Strafrechtliche Garantenpflichten der ISP ... 57
a) Garantenpflichten aus dem Gesetz? ... 57
b) Garantenpflichten aus Ingerenz? ... 58
c) Garantenpflichten zum Schutz von Rechtsgütern? ... 59
d) Garantenpflichten zur Überwachung von Gefahrenquellen? ... 61
e) Beschränkende Funktion der §§ 7–10 TMG ... 65
E. Vorsatzerfordernisse der strafrechtlichen Verantwortlichkeit ... 68
1. Dominanz von Vorsatzdelikten ... 68
2. Vorsatzformen ... 68
3. Unrechtsbewusstsein und Verbotsirrtum ... 70
F. Einordnung der Handlungen als Täterschaft oder Teilnahme ... 71
1. Abgrenzung von Täterschaft und Teilnahme ... 71
2. Einordnung der ISP als Täter oder Teilnehmer ... 72
a) Kriterien für die Einordnung ... 72
b) Einordnung der Handlung der ISP ... 73
c) Beteiligung durch Unterlassen ... 73

IV. Gesetzlich nicht geregelte Typen der ISP und ihre Verantwortlichkeit ... 74
A. Peer-to-Peer-Netzwerke ... 74
1. Einordnung der Betreiber von Peer-to-Peer-Netzwerken ... 74
2. Privilegien der Betreiber von Peer-to-Peer-Netzwerken ... 78
3. Strafrechtliche Verantwortlichkeit der Betreiber von Peer-to-Peer-Netzwerken ... 81
a) Betreiber zentraler Peer-to-Peer-Netzwerke ... 81
b) Betreiber dezentraler Peer-to-Peer-Netzwerke ... 84
B. Hyperlinks ... 85
1. Einordnung von Hyperlinks ... 85
2. Verantwortlichkeit für Hyperlinks ... 85

a) Auffassung des Gesetzgebers ... 86
b) Keine analoge Anwendung der §§ 7–10 TMG? ... 86
c) Welche analoge Anwendung? ... 88
d) Befürwortung einer differenzierenden Lösung ... 90
3. Strafrechtliche Verantwortlichkeit für Hyperlinks ... 91
a) Einordnung der Handlung als Tun oder Unterlassen ... 91
b) Prüfpflichten der Hyperlinksetzer ... 93
c) Einordnung der Hyperlinksetzer als Täter oder Teilnehmer ... 93

Dritter Teil
Verantwortlichkeit der ISP in China

I. Historische Entwicklung, Begriff und Typen der ISP ... 95
A. Historische Entwicklung ... 95
B. Rechtliche Begriffe der ISP ... 96
C. Rechtliche Typen der ISP ... 97
1. Typen der ISP in der „Vorschrift über die technischen Maßnahmen der Internetsicherheit 2005“ ... 98
2. Typen der ISP im Zivilrecht ... 99
3. Typen der ISP im Strafrecht ... 100

II. Allgemeine und zivilrechtliche internetspezifische Verpflichtungen und Privilegien der ISP ... 102
A. Grundlegender Rechtsrahmen ... 102
1. Zivilrechtliche Normen ... 102
2. Grundtendenz und Einordnung der Rechtsnormen ... 104
B. Allgemeine Verpflichtungen der ISP ... 105
C. Zivilrechtliche Privilegierungen ... 108
1. Verantwortlichkeit der Content Provider ... 108
2. Privilegien der Access Provider ... 108
a) Grundlegende Voraussetzungen der Privilegierung ... 108
b) Unvereinbarkeit zwischen dem Gesetz und der Anordnung ... 109
3. Privilegien der Caching Provider ... 110
4. Privilegien der Hosting Provider ... 110
a) Grundlegende Voraussetzungen der Privilegierung ... 110
b) Kenntnis der Inhalte ... 111
c) Das notice and take down-Verfahren ... 114

III. Allgemeine strafrechtliche Verantwortlichkeit der ISP ... 114
A. Die Beziehung zwischen dem chStGB und den Verantwortlichkeitsregelungen in anderen Gesetzen ... 114
B. Grundlegender Rechtsrahmen im strafrechtlichen Bereich ... 116
1. Vor Inkrafttreten des Strafrechtsänderungsgesetzes (IX) ... 116
2. Nach Inkrafttreten des Strafrechtsänderungsgesetzes (IX) ... 117

a) Inhalte der neuen Tatbestände ... 117
b) Grundlage der neuen Tatbestände ... 118
aa) § 286 Abs. 1 chStGB ... 118
bb) § 287 Abs. 1 chStGB ... 118
cc) § 287 Abs. 2 chStGB ... 119
c) Bewertung der neuen Tatbestände ... 120
C. Einordnung der Handlung der ISP als Tun oder Unterlassen ... 125
1. Allgemeine Abgrenzung von Tun und Unterlassen ... 125
2. Einordnung der Handlung von ISP als Tun oder Unterlassen ... 126
a) Möglichkeit der Einordnung ... 126
b) Kriterium für die Einordnung ... 128
D. Strafrechtliche Garantenpflichten der ISP ... 129
1. Allgemeine strafrechtliche Garantenstellungen ... 129
2. Strafrechtliche Garantenpflichten der ISP ... 130
a) Garantenpflichten aus Gesetz? ... 130
aa) Vor Inkrafttreten des Strafrechtsänderungsgesetzes (IX) ... 131
bb) Nach Inkrafttreten des Strafrechtsänderungsgesetzes (IX) ... 131
b) Garantenpflichten aus Ingerenz? ... 134
c) Garantenpflichten zum Schutz von Rechtsgütern? ... 135
d) Garantenpflichten aus Überwachung der Gefahrenquellen? ... 136
e) Beschränkende Gründe aus anderen Rechtsgebieten ... 136
f) Gleichstellung des Unterlassens mit dem Tun ... 137
E. Vorsatzerfordernisse ... 140
1. Die Möglichkeit der Fahrlässigkeitsdelikte? ... 140
2. Vorsatzformen ... 142
3. Unrechtsbewusstsein und Verbotsirrtum ... 144
F. Einordnung als Täterschaft oder Teilnahme ... 146
1. Abgrenzung von Täterschaft und Teilnahme ... 146
2. Diskussion über die neutrale Handlung ... 146
a) Neutrale Handlung ... 147
aa) Subjektive Theorie ... 148
bb) Objektive Theorie ... 148
cc) Kombinierte Theorie ... 151
b) Berücksichtigung der Lehre von der neutralen Handlung für die Verantwortlichkeit der ISP ... 152
c) Begrenztheit der neutralen Handlung für die Verantwortlichkeit der ISP ... 153
aa) Fehlende Typisierung der ISP ... 153
bb) Abgrenzung der Beteiligung der ISP ... 154
cc) Spezielle Eigenschaften der ISP ... 156
3. Einordnung der Handlung als Täterschaft oder Teilnahme ... 159
a) Vor Inkrafttreten des Strafrechtsänderungsgesetzes (IX) ... 159
b) Nach Inkrafttreten des Strafrechtsänderungsgesetzes (IX) ... 161

IV. Gesetzlich nicht geregelte Typen der ISP und ihre Verantwortlichkeit 161
A. Peer-to-Peer-Netzwerke 161
1. Einordnung der Betreiber von Peer-to-Peer-Netzwerken 161
2. Privilegien der Betreiber von Peer-to-Peer-Netzwerken 162
3. Strafrechtliche Verantwortlichkeit der Betreiber von Peer-to-Peer-Netzwerken 165
a) Strafbarkeit der Betreiber als Gehilfen 166
aa) Anwendung der Theorie der neutralen Handlung 166
bb) Einordnung der Handlung als Tun oder Unterlassen 167
b) Strafbarkeit der Betreiber als Anstifter 168
B. Hyperlinks 169
1. Einordnung von Hyperlinks 169
2. Allgemeine Verantwortlichkeit der Hyperlinksetzer 169
a) Verantwortlichkeit der Anbieter von Surface Links 169
b) Verantwortlichkeit der Anbieter von Deep Links 170
3. Strafrechtliche Verantwortlichkeit von Hyperlinksetzern 172
a) Strafrechtliche Verantwortlichkeit der Anbieter von Surface Hyperlinks 172
b) Strafrechtliche Verantwortlichkeit der Anbieter von Deep Hyperlinks 173

Vierter Teil
Zusammenfassender Vergleich

I. Rechtliche Begriffe der ISP 176
A. Deutschland 176
B. China 176

II. Rechtliche Typen der ISP 177
A. Deutschland 177
B. China 177

III. Internetspezifische Privilegien der ISP 178
A. Deutschland 178
B. China 180

IV. Allgemeine strafrechtliche Verantwortlichkeit der ISP 181
A. Deutschland 181
B. China 182

V. Allgemeine kriminalpolitische Bewertung 185

Literaturverzeichnis 188

Abkürzungsverzeichnis

ABl.	Amtsblatt
Abs.	Absatz
Abschn.	Abschnitt
a.F.	alte Fassung
AfP	Zeitschrift für Medien- und Kommunikationsrecht, Archiv für Presserecht
AG	Amtsgericht
Anm.	Anmerkung
ARPANET	Advanced Research Projects Agency Network
AT	Allgemeiner Teil
Aufl.	Auflage
Bayer. LT-Drs.	Drucksachen des Bayerischen Landtags
Bd.	Band
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BGBl I	Bundesgesetzblatt Teil I
BGHSt	Entscheidungen des Bundesgerichtshofs in Strafsachen
BR-Drs.	Drucksachen des Deutschen Bundesrates
BT-Drs.	Drucksachen des Deutschen Bundestages
CACM	Communications of the ACM
chStGB	chinesisches Strafgesetzbuch
CNKI	National Knowledge Infrastructure
CNNIC	China Internet Network Information Center
CR	Computer und Recht
ders.	derselbe
DFN	Das Deutsche Forschungsnetz
DMCA	Digital Millennium Copyright Act
DoC	United States Department of Commerce

DoD	United States Department of Defense
DRiZ	Deutsche Richterzeitung
ECRL	E-Commerce-Richtlinie (Richtlinie über den elektronischen Geschäftsverkehr)
EGG	Gesetz über den elektronischen Geschäftsverkehr
E-Mail	Electronic mail
f.	folgende
ff.	folgende
FS	Festschrift
GA	Goltdammer´s Archiv für Strafrecht (Zeitschrift)
GmbH	Gesellschaft mit beschränkter Haftung
Hrsg.	Herausgeber
IaaS	Infrastructure as a Service
IDC	Internet-Data-Center
i.d.R.	in der Regel
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organisation for Standardization
ISP	Internet-Service-Provider
IuKDG	Informations-und Kommunikationsdienstegesetz
JA	Juristische Arbeitsblätter
JMStV	Jugendmedienschutz-Staatsvertrag
JR	Juristische Rundschau
JZ	Juristenzeitung
LAN	Local Area Network
LG	Landgericht
MAN	Metropolitan Area Network
MMR	Multimedia und Recht

NAP	Network Access Point
NetzDG	Netzwerkdurchsetzungsgesetz
NIST	National Institute of Standards and Technology
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NSF	National Science Foundation
NSFNET	The National Science Foundation Network
NStZ	Neue Zeitschrift für Strafrecht
OLG	Oberlandesgericht
OSI model	Open System Interconnection Reference Model
OWL	Web Ontology Language
P2P	Peer-to-Peer
PaaS	Platform as a Service
PICS	Platform for Internet Content Selection
RDF	Resource Description Framework
RGSt	Entscheidungen des Reichsgerichts in Strafsachen
Rn.	Randnummer
Rspr.	Rechtsprechung
S.	Seite
SaaS	Software as a Service
SMS	Short Message Service
StGB	Strafgesetzbuch
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft
ZTE	Zhongxing Telecommunication Equipment Corporation
ZUM	Zeitschrift für Urheber- und Medienrecht

Einleitung

I. Problemstellung

In den letzten Jahrzehnten hat sich die Netzwerktechnologie sehr schnell entwickelt. Früher betrachteten wir Computer und Internet nur als Werkzeug für Forschung oder Studium. Heute sind sie ein unentbehrlicher Bestandteil unseres Alltagslebens. Das Internet hat unser Leben gänzlich verändert. Mit der Popularisierung des Internets sind jedoch gleichzeitig immer mehr neue kriminelle Phänomene entstanden. Heute bedroht die sogenannte Cyberkriminalität, die Delikte gegen die Integrität von Computersystemen, Datenschutzdelikte, Urheberrechtsdelikte, Verbreitungsdelikte, Angriffe auf das Vermögen und die Sicherheit des Rechtsverkehrs usw. beinhaltet,[1] die Ordnung und Sicherheit unserer Gesellschaft. Angesichts dieser Situation müssen die Strafrechtswissenschaftler reagieren. Tatsächlich hat die technische Revolution schon gravierende Veränderungen im strafrechtlichen Bereich ausgelöst. So verschwimmen zum Beispiel die nationalen Grenzen im Cyberspace, was eine Herausforderung für den Geltungsbereich des StGB darstellt. Außerdem gestaltet sich die Strafverfolgung oft schwieriger als früher, weil viele Straftaten im Cyberspace mithilfe der Hochtechnologie begangen werden. Ein weiteres Beispiel ist der Einfluss auf die Theorie der Beteiligung im Strafrecht. Die Cyberkriminalität hat sich in einigen Bereichen bereits als eine organisierte Branche etabliert. Die Arbeitsteilung zwischen den Straftätern wird immer ausgefeilter, sodass manchmal kein direkter und bestimmbarer Zusammenhang zwischen den Straftätern besteht. Das bedeutet, dass die traditionelle Theorie der Beteiligung mit mehr Schwierigkeiten im Cyberspace konfrontiert werden könnte.

Neben den oben genannten Herausforderungen hält die Cyberkriminalität eine spezielle Problematik bereit: die Providerverantwortlichkeit.[2] Mit der voranschreitenden Entwicklung der Internetgesellschaft spielen die Internet-Service-Provider (ISP) als *Gatekeeper* eine immer wichtigere Rolle. Bis in die 1990er-Jahre wurde das Internet in der Regel von der Regierung oder offiziellen Institutionen betrieben. Ab 1993 wurde das NSFNET (National Science Foundation Network in den USA) allmählich durch eine Reihe kommerzieller Internet-Backbones ersetzt, und die staatlichen Behörden waren nicht mehr für den Betrieb des Internets verantwortlich, sodass es heute eine große Zahl von Internet-Service-Providern gibt.[3]

---

[1] Vgl. *Sieber*, Straftaten und Strafverfolgung im Internet, C 9 ff.

[2] Vgl. ebenda, C 60.

[3] Vgl. *Xie, Xiren* (Hrsg.), Computer-Netzwerk, S. 4.

ISP spielen eine wichtige Rolle für die Kommunikation zwischen dem Nutzer und dem Internet. Wenn ein Netzwerkbenutzer sich mit dem Internet verbinden will, muss er Kontakt mit ISP haben. Es ist evident, dass ISP im Cyberspace ein sehr wichtiges rechtliches Subjekt geworden sind. Umstritten ist nach wie vor die Frage, inwieweit ein ISP für die rechtswidrigen Inhalte oder die illegalen Handlungen von anderen verantwortlich sein soll. Weil die direkt verantwortlichen Täter aus verschiedenen Gründen oft schwer zu identifizieren sind, rückt die Verantwortlichkeit der ISP in den Mittelpunkt.[4] Obwohl es in Deutschland eine Reihe von Regelungen über die Verantwortlichkeit der ISP gibt, bestehen viele Kontroversen über dieses Thema.

In dem bekannten *CompuServe*-Fall etwa wurde vom AG München entschieden, dass der Angeklagte der Verbreitung pornografischer Schriften nach § 184 Abs. 3 Nr. 2 StGB schuldig war, weil er pornografische Schriften öffentlich zugänglich gemacht hatte.[5] Der Angeklagte war in diesem Fall der Geschäftsführer der deutschen *CompuServe* GmbH, einer Tochtergesellschaft der amerikanischen *CompuServe*. Er bot seinen deutschen Kunden tatsächlich nur einen Zugang zu den Datenspeichern der amerikanischen *CompuServe*. Das heißt, die strafbaren Inhalte wurden nicht bei der deutschen *CompuServe* GmbH gespeichert.[6] Vom LG München wurde der Angeklagte schließlich freigesprochen. Der Richter führte dafür eine Reihe von Gründen an: Erstens konnte die Mittäterschaft des Angeklagten nicht festgestellt werden, weil die deutsche *CompuServe* GmbH der Muttergesellschaft völlig untergeordnet gewesen war. Zweitens konnte das Handeln des Angeklagten auch nicht als Beihilfe betrachtet werden, da das Unterlassen des Angeklagten nicht ursächlich war und eine Garantiepflicht von ihm auch nicht begründet werden konnte. Schließlich fehlte dem Angeklagten der Vorsatz.[7] In diesem Fall wurde die strafrechtliche Verantwortlichkeit der ISP heftig diskutiert. Der damalige Oberstaatsanwalt des Bundesgerichtshofs führte aus, dass die Nichtbefolgung einer Sperrverpflichtung nach § 5 Abs. 4 TDG zu sanktionieren sei.[8] Jedoch wurde das Urteil erster Instanz mehrheitlich nach der allgemeinen strafrechtlichen Grundlage kritisiert, während die Verpflichtung zur Sperrung abgelehnt wurde.[9]

Einen ähnlichen Fall gab es in China. Die Angeklagten waren Geschäftsführer der *Kuaibo* GmbH, die den Nutzern einen kostenlosen Mediaplayer für Videos

---

[4] Vgl. *Sieber*, CR Heft 10, 1997, 581.

[5] Vgl. *Sieber*, MMR Heft 8, 1998, 430 (Urteilsanmerkung AG München, Urteil vom 28.05.1998 – 8340 Ds 465 Js 173158/95).

[6] Vgl. ebenda, 429.

[7] Vgl. Verbreitung pornografischer Inhalte im Internet – Freispruch im *CompuServe*-Prozess, ZUM Heft 3, 2000, 249 ff. (LG München I, Urteil vom 17.11.1999 – 20 Ns 465 Js 173158/95).

[8] Vgl. *Graf*, DRiZ 1999, 286.

[9] Vgl. *Kühne*, NJW Heft 3, 1999, 189 ff.; *ders.,* NJW Heft 14, 2000, 1004; *Sieber*, MMR Heft 8, 1998, 439 ff.

(QVOD Player) bot. Darüber hinaus stellte die *Kuaibo* GmbH den Nutzern eine kostenlose Encoding-Software (QSI) zur Verfügung, mit der jeder Nutzer eigene Video-Ressourcen im Netzwerk freigeben konnte. Zudem versorgte die *Kuaibo* GmbH die Nutzer mit der automatischen und kurzzeitigen Zwischenspeicherung für die abgerufenen Videodateien, um die schnelle Durchleitung der Informationen zu garantieren. Es wurde nicht nur vom Gericht erster Instanz, sondern auch in zweiter Instanz entschieden, dass die Angeklagten der Verbreitung pornografischer Materialien zur Gewinnerzielung nach § 363 Abs. 1 chStGB schuldig waren.[10]

Obwohl das in Kraft getretene Urteil von vielen Rechtswissenschaftlern begrüßt wurde,[11] finden sich auch viele kritische Ansichten.[12] Die gegensätzlichen Kommentare zu diesem konkreten Fall spiegeln den Stand der theoretischen Diskussion über die Verantwortlichkeit der ISP wider und verdeutlichen, dass eine systematische Untersuchung zur Verantwortlichkeit der ISP sowohl in Deutschland als auch in China von großer Bedeutung ist. Im Hinblick auf diese Situation ist es sinnvoll, eine vergleichende Untersuchung zwischen Deutschland und China über dieses Thema zu erarbeiten.

II. Gegenstand der Untersuchung

A. Technische Grundlagen der ISP

Das technische Prinzip der Netzwerke bildet die Grundlage für die Erforschung des Internetstrafrechts. Deshalb ist es unentbehrlich, die technische Basis der ISP aufzuzeigen, bevor wir die Verantwortlichkeit der ISP untersuchen. Erstens werden die allgemeinen Kenntnisse über das Internet und das Netzwerk erläutert. Vor allem ist es notwendig, in die Entstehung und Entwicklung des Internets kurz einzuführen. Dann werden die Struktur und Grundsätze des Netzwerks beschrieben. Mit diesem Grundlagenwissen kann der Betrieb des Netzwerks besser verstanden werden. Dabei werden auch die kriminellen Risiken im Netzwerk diskutiert, damit die neuen Herausforderungen, die sich im Cyberspace ergeben, deutlich erkennbar werden. Zweitens wird die technische Basis für ISP weiter untersucht. Zuerst ist es unerlässlich, die Entstehung und Entwicklung der ISP zu vermitteln. Mit diesem

---

[10] Vgl. Urteil der ersten Instanz zum *Kuaibo*-Fall, abrufbar unter http://bjhdfy.chinacourt.org/public/detail.php?id=4343 [Stand: 15.09.2017]; Urteil der zweiten Instanz zum *Kuaibo*-Fall, Volksgerichtszeitung, 16.12.2016.

[11] Vgl. *Chen Xingliang*, Volksgerichtszeitung, 14.09.2016; *Zhang Mingkai*, Volksgerichtszeitung, A003, 14.09.2016.

[12] Vgl. *Liu Yanhong*, Politik und Recht, Heft 12, 2016, 109 ff.; *Che Hao*, Chinesische Rechtszeitschrift, Heft 1, 2015, 47 ff.; *ders.,* Der neue Kommentar zum *Kuaibo*-Fall, abrufbar unter http://www.law.pku.edu.cn/xwzx/pl/16871.htm [Stand: 15.09.2017]; *Sang Benqian*, Rechtswissenschaft, Heft 1, 2017, 79 ff.

Verständnis ist besser nachzuvollziehen, welche Rolle die ISP in unserer Gesellschaft spielen. Dann wird eine Reihe von konkreten Arten der ISP aufgezählt, die nicht nur die grundlegenden Typen, sondern auch einige gesetzlich nicht geregelte ISP umfasst. Im Anschluss werden die Rechtsrisiken für ISP beschrieben, die den Schwerpunkt der folgenden Untersuchung darstellen werden. Drittens wird sich der Verfasser mit den technischen Kontrollmöglichkeiten der ISP auseinandersetzen. Denn die Beurteilung der technischen Kontrollmöglichkeiten der ISP ist die Basis für die weitere Untersuchung der Verantwortlichkeit der ISP. Zunächst werden jeweils die primären Kontrollmöglichkeiten der verschiedenen ISP analysiert. Dann wird die neue Entwicklung der Technologie weiter erläutert. Damit ist es auch nötig, die möglichen Einflüsse auf die Kontrollmöglichkeiten der ISP zu diskutieren. Schließlich werden Unterschiede zwischen faktischer und normativer Kontrollmöglichkeit aufgezeigt, bei denen neben der physischen Kontrollfähigkeit eine Reihe von anderen normativen Faktoren berücksichtigt wird.

B. Vergleichende Untersuchung der deutschen und der chinesischen Rechtslage

Neben den allgemeinen Grundsätzen in unterschiedlichen Rechtsgebieten gibt es in Deutschland spezifische Verantwortlichkeitsregelungen für ISP. Im Jahr 1997 verabschiedete der Deutsche Bundestag das Teledienstegesetz (TDG), das nicht nur den Begriff des ISP (Diensteanbieter) definiert, sondern auch dessen Arten und die entsprechenden Privilegien beschreibt. Ein Jahr später wurde der *Digital Millennium Copyright Act* (DMCA) in den USA verabschiedet, der die Verantwortlichkeit der ISP für Urheberrechtsverletzungen eindeutig begrenzt. Danach erließ die Europäische Union die Richtlinie über den elektronischen Geschäftsverkehr (*Electronic Commerce Directive*, ECRL) im Jahr 2000, die auch die Definition und die Privilegien der ISP klar festhält. Im Jahr 2007 ersetzte das Telemediengesetz (TMG), das von der Richtlinie über den elektronischen Geschäftsverkehr stark beeinflusst wurde, das Teledienstegesetz, und die Arten und Privilegien der ISP wurden genauer spezifiziert. Das geltende TMG kann in allen Rechtsbereichen angewendet werden.[13] Deshalb bilden die Verantwortlichkeitsregelungen im TMG und die rechtsgebietsspezifischen Regelungen eine zweischichtige Struktur. In China gestaltet sich die Situation gänzlich anders. In der Vergangenheit gab es kein spezifisches Gesetz, das die Verantwortlichkeit der ISP systematisch regulierte. Jedoch existiert eine Reihe von ministerialen Verordnungen und Vorschriften, die auf eine allgemeine Weise vorsehen, dass die ISP keine illegalen Informationen verbreiten dürfen und bestimmte Maßnahmen zur Verhinderung solcher Inhalte ergreifen sollen. Im Jahr 2012 wurde „die Entscheidung über die Verstärkung des Netzwerk-Informationsschutzes“ vom ständigen Ausschuss des Nationalen Volkskongresses

[13] Vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 59, Rn. 185.

verabschiedet. Im Jahr 2016 erließ der ständige Ausschuss des Nationalen Volkskongresses das Gesetz über die Netzwerksicherheit. Beide Normen beziehen sich auch auf die Verpflichtung der ISP. Im Allgemeinen wird diese Verpflichtung nicht konkretisiert; anders als das deutsche Gesetz schreiben sie keine Privilegierung der ISP fest.

In den einzelnen Rechtsgebieten ist die Situation sehr viel komplizierter. Im zivilrechtlichen Bereich wurde der chinesische Rechtsrahmen für ISP stark vom amerikanischen Recht beeinflusst. Deshalb gibt es ähnliche Privilegien für die Verantwortlichkeit der ISP, obwohl viele Unterschiede im Detail bestehen.

Im strafrechtlichen Bereich sind die chinesischen Regelungen sehr speziell. Vor dem Inkrafttreten des Strafrechtsänderungsgesetzes (IX) gab es keinen selbstständigen Paragrafen über die Verantwortlichkeit der ISP. Deshalb wurden die strafbaren ISP früher nach den Tatbeständen der Verbreitungsdelikte oder Äußerungsdelikte geahndet. Zudem wurden vom Obersten Volksgerichtshof und von der Obersten Volksstaatsanwaltschaft der Volksrepublik China in den Jahren 2004 und 2010 zwei einschlägige Interpretationen[14] erlassen. Nach der ersten Interpretation werden die ISP, die durch ihre Internetdienste Hilfe für Straftaten aus dem Bereich der Pornografie zur Verfügung stellen, wegen Teilnahme an der Verbreitung pornografischer Inhalte bestraft. Gemäß der zweiten Interpretation werden die ISP, die Straftätern im Zusammenhang mit Pornografie bestimmte Internetdienste vorsätzlich anbieten, als Täter anstatt als Teilnehmer an der Verbreitung der pornografischen Inhalte bestraft.

Mit dem Inkrafttreten des Strafrechtsänderungsgesetzes (IX) im Jahr 2015 wurden dem chStGB drei neue Tatbestände hinzugefügt, die direkt mit der strafrechtlichen Verantwortlichkeit der ISP zusammenhängen, nämlich

1) § 286 Abs. 1 chStGB: Verweigerung der Sicherheitsverpflichtungen im Informationsnetzwerk;
2) § 287 Abs. 1 chStGB: illegale Nutzung von Informationsnetzen;
3) § 287 Abs. 2 chStGB: Hilfe für Informationen und Cyberkriminalität.

Die neuen Tatbestände im Strafrechtsänderungsgesetz (IX) zeigen deutlich, dass ISP, die gegen das Strafrecht verstoßen, als selbstständige Täter anstatt nur als Teilnehmer an den Straftaten anderer zu bestrafen sind. Es gibt hier einen auffälligen gesetzgeberischen Trend für das Internetstrafrecht in China, dass die tatsächliche Teilnahme als strafrechtliche Täterschaft geahndet wird, nämlich als „Teilnehmer wird Täter“ (共犯正犯化) oder als „Gehilfe wird Täter“ (帮助行为正犯化). Diese Gesetzgebung hat in der Theorie erhebliche Kontroversen ausgelöst. Einige

---

[14] Unter der Interpretation in China versteht man die gerichtliche Erklärung zu relevanten Gesetzen, welche nur von dem Obersten Volksgerichtshof und der Obersten Volksstaatsanwaltschaft der Volksrepublik China erlassen werden dürfen. Die Interpretation ist kein neues Gesetz, sondern nur die konkrete Erläuterung der Gesetze.

Wissenschaftler stehen auf dem Standpunkt, dass die neuen Regelungen nicht explizit seien und den ISP ungerechtfertigt schwere strafrechtliche Verantwortung auferlegten. Dagegen vertreten andere die Meinung, diese Gesetzgebung sei hilfreich, um die immer akuter werdenden Probleme durch Cyberkriminalität zu bekämpfen. Deshalb verdienten die neuen Regelungen für strafrechtliche Verantwortlichkeit der ISP besondere Aufmerksamkeit.

Aus dieser kurzen Beschreibung wird ersichtlich, dass Deutschland und China unterschiedliche Rechtsmodelle für die Verantwortlichkeit der ISP bereithalten. In der vorliegenden Arbeit sollen die verschiedenen Rechtssysteme rechtsvergleichend untersucht werden. In diesem Rahmen sollen grundlegende Definitionen und Typen der ISP, die unterschiedlichen Privilegierungsmodelle und die allgemeinen Probleme der strafrechtlichen Verantwortlichkeit der ISP im Detail diskutiert werden.

C. Auswirkungen des Internets auf die traditionelle Strafrechtslehre

Das Internet hat die traditionellen Strafrechtslehren stark beeinflusst. Wie schon erläutert, zeigt sich dies in vielen Aspekten. Die Bestimmung der strafrechtlichen Verantwortlichkeit der ISP hat auch zu folgender Entwicklung geführt: Wenn die ISP den anderen Straftätern ihre Dienste wissentlich oder unwissentlich zur Verfügung stellen, werden sie unter bestimmten Bedingungen in der Regel wegen Teilnahme bestraft. Jedoch ist der Nachweis der Erfüllung der Voraussetzungen einer Teilnahme in der Praxis oft mit Schwierigkeiten verbunden. Daher wird in der chinesischen Gesetzgebung ein neuer Weg erprobt: Die Täterschaft der ISP wird direkt durch selbstständige Tatbestände bestimmt. In der Theorie wird die Strafbarkeit der ISP von einigen Rechtswissenschaftlern dadurch begründet, dass der Umfang der Täterschaft durch Auslegung erweitert wird. Diese neue Art der Bestimmung der strafrechtlichen Verantwortlichkeit der ISP steht mit den traditionellen Strafrechtslehren möglicherweise nicht im Einklang. Deshalb ist es notwendig, ihre möglichen Auswirkungen auf die traditionellen Strafrechtslehren zu untersuchen.

D. Balance zwischen Freiheit und Sicherheit

Mit der anhaltenden Verschlechterung der Sicherheit im Cyberspace rückt die Bekämpfung der Cyberkriminalität heute in den Vordergrund und viele Maßnahmen werden dagegen ergriffen. Die strafrechtliche Regulierung der ISP gehört zu diesen Maßnahmen. Jedoch dürfen wir niemals vergessen, die Balance zwischen Sicherheit und Freiheit zu wahren. Die Informationsfreiheit ist einer der wichtigsten Werte unserer Gesellschaft. Einerseits gehört die Informationsfreiheit zu den bürgerlichen Grundrechten, die durch die staatliche Verfassung geschützt werden.

Andererseits ist die Informationsfreiheit Voraussetzung für die Entwicklung der Informationsindustrie. Wenn die Informationen im Netzwerk wegen der hohen Rechtsrisiken nicht mehr frei übermittelt würden, wäre die Entwicklung der ganzen Informationsindustrie gefährdet. Deshalb wird dies ein Schwerpunkt dieser Untersuchung sein.

III. Ziele der Untersuchung

Als Grundlage für die weitere Untersuchung muss zunächst die technische Basis der ISP erläutert werden. Es sollen grundlegende Kenntnisse der Funktionsweise des Internets und der ISP vermittelt und die konkreten Kontrollmöglichkeiten der verschiedenen ISP ausführlich diskutiert werden. Im Anschluss daran werden die Ähnlichkeiten und Unterschiede zwischen der Gesetzgebung Deutschlands und Chinas herausgearbeitet und die beiden Rechtssysteme einer Bewertung unterzogen. Diese soll sich nicht nur auf das Ziel und die grundlegende Position der Gesetzgebung beziehen, sondern auch auf deren Form und Struktur. Auf diese Weise können die Vor- und Nachteile der verschiedenen Rechtssysteme festgestellt werden, damit weitere Vorschläge zur Reform gegeben werden können. Zudem werden die theoretischen Diskussionen vorgestellt. Dadurch wird das Problem der Verantwortlichkeit der ISP besser verständlich, sodass eine gerechtere und systematischere theoretische Lösung abgeleitet werden kann. Schließlich versucht diese Untersuchung, für die Rechtspolitik bezüglich der Verantwortlichkeit der ISP ein akzeptables Gleichgewicht zwischen der Informationsfreiheit und der Sicherheit im Cyberspace zu finden. So soll diese Studie einen Beitrag zur Reflexion über die aktuelle Kriminalpolitik leisten und die Verantwortlichkeit der ISP aus einer breiteren Perspektive diskutieren.

IV. Methode der Untersuchung

Vor allem wird die dogmatische Methode in dieser Untersuchung als ein grundlegendes Mittel angewendet. Bezüglich der Verantwortlichkeit der ISP existieren sowohl in Deutschland als auch in China eine Reihe von Rechtsnormen. Diese Regelungen, welche in verschiedenen Formen mit unterschiedlichen Rechtswirkungen vorliegen, bestimmen die rechtliche Verantwortlichkeit der ISP. Deshalb ist es unentbehrlich, zunächst mit einer dogmatischen Methode die Bedeutung der relevanten Rechtsnormen ausführlich zu analysieren. Außerdem wird in dieser Forschungsarbeit eine rechtsvergleichende Betrachtung angewandt. Es wird gezeigt, wie sich die Rechtsquellen und deren Verbindlichkeit in Deutschland und China unterscheiden. Die verschiedenen Systeme der Rechtsquellen und ihre rechtliche Geltung haben zu unterschiedlichen Regulierungsmodellen geführt. Mithilfe der

Rechtsvergleichung kann man die Vor- und Nachteile in Bezug auf das Verantwortungsmodell der ISP in beiden Rechtssystemen deutlich erkennen. Zudem wird auf diese Weise deutlich, welche Rolle die deutsche Rechtswissenschaft in der chinesischen Forschung gespielt hat. Auch aufgrund ihres weltweiten Einflusses wird die deutsche Literatur häufig in den einschlägigen chinesischen Untersuchungen zitiert. Besonders in einigen neuen Themenbereichen wird der Lösungsansatz der deutschen Strafrechtswissenschaft als eine wichtige Referenz betrachtet. Durch eine rechtsvergleichende Methode werden die Einflüsse der deutschen Rechtswissenschaft auf die chinesische Forschung über Verantwortlichkeit der ISP besser verständlich. Schließlich kommt in der Arbeit eine kriminalpolitische Betrachtungsweise zum Einsatz. Als eine völlig neue und aktuelle Problematik ist die Verantwortlichkeit der ISP äußerst umstritten. Ein Konsens über dieses Thema, der in der Welt allgemein anerkannt wäre, existiert bisher nicht. Sogar auf der Ebene des nationalen Rechts befinden sich die Rechtsvorschriften über die Verantwortlichkeit der ISP wegen der schnellen Entwicklung der Cyberkriminalität in einem instabilen Zustand. In dieser Situation reicht eine bloß dogmatische Methode nicht aus. Die Zielsetzung der Rechtsnormen sowie ihre Legitimität sollten auch aus einer rechtspolitischen Sicht weiter berücksichtigt und bewertet werden.

V. Gang der Untersuchung

Die Forschungsarbeit besteht insgesamt aus fünf Teilen. In der Einleitung wird die Problematik im Allgemeinen beschrieben. Der erste Teil behandelt die technischen Grundlagen als Basis für die gesamte Untersuchung. Im zweiten Teil wird die Verantwortlichkeit der ISP nach der deutschen Rechtsordnung erläutert. Im Einzelnen werden die Definition und die Typen der ISP, deren rechtliche Privilegien, die allgemeinen Probleme der strafrechtlichen Verantwortlichkeit der ISP und die Verantwortlichkeit der gesetzlich nicht geregelten ISP detailliert untersucht. Im dritten Teil wird die Regelung der Verantwortlichkeit der ISP in der chinesischen Rechtsordnung herausgearbeitet. Die Struktur folgt hier dem deutschen Teil. Im vierten Teil werden die Verantwortlichkeiten der ISP in Deutschland und China verglichen, wobei die Eigenschaften der beiden Rechtssysteme zusammenfassend dargestellt werden.

Erster Teil

Technische Grundlagen

I. Technische Grundlagen des Internets und der Netzwerktechnik

A. Entwicklung des Internets und der Netzwerktechnik

1. Entstehung des Internets

Das Internet wurde ursprünglich in den USA begründet. Im Jahr 1969 etablierte das US-Verteidigungsministerium (DoD) das ARPANET (*Advanced Research Projects Agency Network*), das aber kein miteinander verbundenes Netzwerk war. Im Jahr 1983 wurde das TCP/IP (*Transmission Control Protocol/Internet Protocol*) als Standardprotokoll festgelegt, sodass Computer durch das gleiche Protokoll verbunden sind und Daten zwischen Computern übermittelt werden konnten. Deshalb gilt das Jahr 1983 als Geburtsstunde des Internets.[1] Im Jahr 1985 errichtete die NSF (*National Science Foundation*) das NSFNET (*National Science Foundation Network*), das der Verbindung der Forschungs- und Bildungseinrichtungen diente. Zu dieser Zeit wurde das Internet nur in einem sehr begrenzten Bereich genutzt. 1991 begann die NSF, den Regierungsbetrieb zu einer gewinnorientierten Organisation umzuwandeln. Danach entstanden viele der heute bekannten Internetunternehmen, die schnell wuchsen.[2] In diesem Stadium wurde das NSFNET allmählich von vielen kommerziellen Internet-Backbones ersetzt, auch die Internet-Service-Provider traten in Erscheinung.[3] Backbone, Providernetzwerk und Kundennetzwerk bilden zusammen das Internet.[4] Im Jahr 1992 konzipierte *Tim Berners-Lee* das World Wide Web (WWW), indem er die entsprechenden URL-Struktur, Hyperlinks und Webbrowser entwarf. Mithilfe der TCP/IP und UDP (*User Datagram Protocol*) wurde das WWW schnell auf der ganzen Welt verbreitet und macht heute einen unentbehrlichen Bestandteil unseres Lebens aus.[5]

---

[1] Vgl. *Xie, Xiren* (Hrsg.), Computer-Netzwerk, S. 3 ff.

[2] Siehe *Rustad*, Internet Law, S. 3–4.

[3] Vgl. *Xie, Xiren* (Hrsg.), Computer-Netzwerk, S. 4.

[4] Vgl. *Forouzan/Mosharraf*, Computer Networks, S. 5.

[5] Siehe *Rustad*, Internet Law, S. 15–16.

2. Entwicklung des Web 1.0, des Web 2.0 und des Web 3.0

Mit der ständigen Verbesserung der Netzwerktechnologie hat das Web sich immer weiterentwickelt. Dabei wird häufig von einem Wechsel von Web 1.0 zu Web 2.0 und sogar zu Web 3.0 gesprochen. Unter Web 1.0 wird das Anfangsstadium der Entwicklung des Internets verstanden. In diesem Stadium konzentrierte sich das Web auf die Verbindung der Informationen und ihre Verfügbarkeit im Netz. Deshalb wurde das Web 1.0 als „Nur-Lese-Web" (*read-only web*) oder „Web der Kognition"[6] bezeichnet. Mit anderen Worten: Das Web 1.0 erlaubte es, die Informationen zu suchen und zu lesen.[7] Deshalb hat das Web 1.0 einen asynchronen Charakter und wird gern mit einem Forum oder Anschlagbrett (*bulletin board*) verglichen.[8]

Im Vergleich zum Web 1.0 hat das Web 2.0 ganz unterschiedliche Erscheinungsweisen hervorgebracht. Das Web 2.0 bemüht sich um die Förderung der Interaktionen zwischen den Nutzern des Webs, die Nutzer können eigene Inhalte ins Netz stellen und diese Inhalte mit anderen austauschen.[9] Das heißt, das Web 2.0 ist nicht mehr ein „Nur-Lese-Web", sondern ein „soziales Web"[10] oder ein „Web der menschlichen Kommunikation".[11] Deshalb hat das Web 2.0 im Gegensatz zum Web 1.0 eine synchrone Eigenschaft.[12] In der Gegenwart beeinflusst das Web 2.0 jede Ebene unserer Gesellschaft. Viele Menschen können sich ein Leben ohne Facebook, Twitter, Wiki oder E-Mail usw. kaum vorstellen. Obwohl es zurzeit keine einheitliche Definition des Web 3.0 gibt, weist es zumindest in die Richtung der künftigen Entwicklung des Internets.

Im Vergleich zum Web 2.0 geht das Web 3.0 weiter, indem viele neue technische Konzepte aufgestellt werden. Ein typisches Beispiel ist das *Semantic Web* von *Tim Berners-Lee*. Dieses Konzept richtet sich durch die Einführung des RDF (*Resource Description Framework*) und der OWL (*Web Ontology Language*) auf ein maschinenlesbares Web.[13] Zudem ist das *Internet of Things* (IoT) ein heiß diskutiertes Thema. Im *Internet of Things* werden zahlreiche Daten von Sachen in der realen Welt gesammelt und bearbeitet, sodass die reale Welt zu einem großen Teil digitalisiert wird. Damit wird die mobile, virtuelle und augenblickliche Verbindung

---

[6] Siehe *Christian Fuchs* u.a., Future Internet, No. 2, 2010, 50 ff.

[7] Siehe *Naik/Shivalingaiah*, Comparative Study of Web 1.0, Web 2.0 and Web 3.0, S. 500.

[8] Siehe *Rustad*, Global Internet Law, S. 20.

[9] Siehe *Naik/Shivalingaiah*, Comparative Study of Web 1.0, Web 2.0 and Web 3.0, S. 500–501.

[10] Siehe *Kamel Boulos* u.a., Health Information and Libraries Journal, Vol. 24, 2007, 2 ff.

[11] Siehe *Christian Fuchs* u.a., Future Internet, No. 2, 2010, 50 ff.

[12] Siehe *Rustad*, Global Internet Law, S. 20.

[13] Siehe *Cardoso*, IEEE Intelligent Systems, Vol. 22, No. 5, 2007, 84.

der ganzen Welt verwirklicht.[14] Auf diese Weise werden auch die Beziehungen zwischen den Menschen immer enger, das Leben und die Arbeit immer bequemer. Deshalb wird das Web 3.0 als „Web der Zusammenarbeit" bezeichnet.[15]

B. Grundlagen der Netzwerktechnik

1. Grundlegende Struktur des Netzwerks

Wenn die äußerst vielfältigen Netzwerke in der Welt vereinheitlicht werden sollen, um alle Computer miteinander zu verbinden und die Daten zwischen diesen Computern fließend austauschen zu können, ist ein allgemein anerkanntes Kriterium für den Aufbau des Netzwerksystems unentbehrlich. Im Jahr 1983 entwickelte die ISO (*International Organization for Standardization*) das OSI-Modell (*Open System Interconnection Reference Model*). Nach diesem OSI-Modell wird das Netzwerksystem in sieben aufeinander aufbauende Schichten unterteilt (von unten nach oben durchnummeriert):

7. Anwendungsschicht (Application Layer)
6. Darstellungsschicht (Presentation Layer)
5. Sitzungsschicht (Session Layer)
4. Transportschicht (Transport Layer)
3. Vermittlungsschicht (Netzwerk Layer)
2. Sicherungsschicht (Data Link Layer)
1. Bitübertragungsschicht (Physical Layer).[16]

Da das OSI-Modell in der Praxis zu kompliziert umzusetzen ist und in diesem Modell einige Überlappungen in unterschiedlichen Schichten bestehen, wird es heute tatsächlich nicht mehr häufig angewendet. Populärer ist das aus der Praxis stammende TCP/IP-Modell, das als der tatsächliche internationale Standard angesehen wird. Es gliedert sich in die folgenden vier Schichten:[17]

4. Anwendungsschicht (entspricht OSI-Modell Schichten 5–7)
3. Transportschicht (entspricht OSI-Modell Schicht 4)
2. Internetschicht (entspricht OSI-Modell Schicht 3)
1. Netzzugangsschicht/Verbindungsschicht (entspricht OSI-Modell Schichten 1–2).

---

[14] Siehe *Rustad*, Global Internet Law, S. 21–22.

[15] Siehe *Christian Fuchs* u.a., Future Internet, No. 2, 2010, 50 ff., 57.

[16] Mehr Erläuterungen vgl. *Sieber*, Verantwortlichkeit im Internet, S. 15, Rn. 26 ff.

[17] Vgl. *Xie, Xiren* (Hrsg.), Computer-Netzwerk, S. 24–25, 27 ff.

Mit diesem Modell können die technischen Prozesse der Kommunikation zwischen Computern und dem Austausch der Daten im Netzwerk deutlich beschrieben werden. Der Sendeprozess beginnt von der Anwendungsschicht nach unten bis in die physikalische Schicht (oder Verbindungsschicht). Nach der Signalübertragung im physischen Medium gehen die Daten im Empfangsprozess von der physikalischen Schicht (oder Verbindungsschicht) nach oben bis in die Anwendungsschicht. OSI-und TCP/IP-Modell bieten uns einen grundlegenden Rahmen, mit dem wir die technische Basis für die Verantwortlichkeit der ISP besser nachvollziehen können.

2. Grundlegende Begriffe der Netzwerktechnik

a) LAN, MAN und WAN

Die Unterscheidung in LAN, MAN und WAN beruht auf dem Ausmaß und Umfang der Netzwerke. Unter dem LAN (*Local Area Network*) wird ein örtliches Netzwerk verstanden, das nur einen lokalen Bereich – beispielsweise innerhalb eines Gebäudes – abdeckt. Das LAN kann weiter in Wireless LAN (drahtloses LAN) und Wired LAN (verdrahtetes LAN) unterteilt werden.[18] Heutzutage ist das LAN fast in jedem Privathaus und an jedem Arbeitsplatz zu finden. Das MAN (*Metropolitan Area Network*) ist ein großes Netzwerk, das den Umfang einer Stadt oder einer ganzen Region umfassen kann. Ein typisches Beispiel für das MAN ist das Kabelfernsehnetz, das den Bürgern nicht nur Fernsehprogramme, sondern auch Internet zur Verfügung stellt.[19] Das WAN (*Wide Area Network*) ist ein riesiges Netzwerk, das ein sehr weites geografisches Gebiet bedient und viele LAN und MAN verbinden kann. Normalerweise besteht das WAN aus zwei getrennten Komponenten, nämlich Übertragungsleitungen (*transmission lines*) und Vermittlungselementen (*switching elements*). Die Übertragungsleitungen übertragen die Bits zwischen Rechnern, während die Vermittlungselemente (spezielle Computer) die Übertragungsleitungen verbinden.[20]

b) ICP/IP

Unter TCP/IP (*Internet Protocol Suite*) wird die Internetprotokollfamilie verstanden, die den Grundstein für die Netzkommunikation legt. IP steht für Internetprotokoll und ist ein grundlegender Vertreter in der Internetprotokollfamilie. Das IP wird in der Internetschicht (oder nach dem OSI-Modell in der Vermittlungsschicht) angewendet, um die Datagramme (IP-Paket) zu übermitteln. Mit dem standardisierten IP können die verschiedenen Rechner miteinander verknüpft werden,

---

[18] Vgl. *Tanenbaum/Wetherall*, Computer Networks, S. 15.

[19] Vgl. ebenda, S. 18.

[20] Vgl. ebenda, S. 18 ff.

sodass ein einheitliches Internet gebaut wird.[21] TCP ist das Übertragungssteuerungsprotokoll (*Transmission Control Protocol*), das ein grundlegendes, aber komplizierteres Protokoll in der Internetprotokollfamilie ist. Das TCP wird in der Transportschicht benutzt, um die Art und Weise des Datenaustauschs zu vereinheitlichen. Im Vergleich zum IP ist das TCP eine Ende-zu-Ende-Verbindung, sodass Daten in beide Richtungen übertragen werden können. Zudem werden die Datenverluste nach TCP erkannt und behoben, damit die Übertragung der Daten garantiert werden kann.[22] Die oben genannten Protokolle bilden die einheitlichen Kriterien, die die schnelle Übertragung und den Austausch der Daten ermöglichen. Sie liegen der Entstehung und Entwicklung eines weltweiten Internets zugrunde.

C. Kriminelle Risiken im Netz

Informationstechnologie und Netzwerk haben nicht nur große Bequemlichkeit gebracht, sondern auch neue kriminelle Risiken. Mit dem Aufkommen der Informationsgesellschaft wird die Cyberkriminalität unvermeidlich zum Problem. Die Formen der kriminellen Risiken im Netzwerk sind breit gefächert. Angriffe gegen die Integrität von Computersystemen, Beeinträchtigung der Privatsphäre der Bürger, Verbreitung illegaler Inhalte sind nur einige Beispiele.[23]

Tatsächlich ist die Cyberkriminalität niemals ein statisches Phänomen. Mit der Entwicklung des Netzwerks von Web 1.0 bis Web 3.0 erscheinen die kriminellen Risiken in immer neuen Ausprägungen. Im Stadium des Web 1.0 wurden das Netzwerk und der Computer hauptsächlich als Gegenstand der Straftat angesehen.[24] Denn in diesem Zeitraum war das Netzwerk nicht synchron und es gab nicht nur relativ begrenzte Ressourcen, sondern auch relativ wenige Nutzer im Netzwerk. Die vorhandenen Tatbestände im StGB, um Cyberkriminalität zu sanktionieren, betrafen etwa das Ausspähen und Abfangen von Daten, Datenveränderung und Computersabotage. Beim Web 2.0 werden das Netzwerk und der Computer überhaupt als Werkzeug für eine Straftat benutzt.[25] In diesem Stadium hat das Netzwerk eine synchrone Eigenschaft, wodurch die Kommunikation zwischen Menschen durch das Web wirksam gefördert wird. Da das Web ein unentbehrlicher Bestandteil der menschlichen Kommunikation geworden ist, wird es auch als Werkzeug oder Medium zur Begehung der traditionellen Straftaten verwendet. Beispielsweise können die traditionellen Straftaten wie Diebstahl, Betrug, Beleidigung und Verleumdung mithilfe des Web im Cyberspace begangen werden.

---

[21] Vgl. *Xie, Xiren* (Hrsg.), Computer-Netzwerk, S. 111.

[22] Vgl. ebenda, S. 187.

[23] Vgl. *Sieber*, Straftaten und Strafverfolgung im Internet, C 9 ff.

[24] Vgl. *Yu Zhigang*, Rechtszeitschrift der Universität Peking Heft 4, 2014, 1047–1048.

[25] Vgl. ebenda, 1048 ff.

Was sind die Formen der Verbrechen im Web 3.0? Diese Frage bleibt zurzeit noch unbeantwortet. Einerseits gibt es noch keine allgemein anerkannte Definition des Web 3.0, andererseits entwickelt sich die Netzwerktechnologie mit jedem Tag weiter. Deshalb bestehen unendliche Möglichkeiten für die Verbindung zwischen Internet und Straftaten. Mit fast jeder Anwendung neuer Netzwerktechnologien gehen entsprechende kriminelle Risiken einher.

Zum Beispiel unterliegt das Eigentum der Bürger aufgrund der schnellen Popularisierung der Online-Bezahldienste wie PayPal oder Ali Pay höheren Risiken als früher. Auch die kriminellen Risiken im übrigen Bereich des elektronischen Handels werden immer höher. In den vergangenen Jahren hat das Internet nicht nur den traditionellen Handel, sondern auch das traditionelle Finanzwesen völlig verändert. Heute weichen die Formen der Investitionen der Menschen zu einem großen Teil von denen der Vergangenheit ab. Die sogenannte Internet-Finanzwirtschaft (*Internet Finance*) hat sich in wenigen Jahren rasant entwickelt. Typische Beispiele für *Internet Finance* sind P2P-Lending und Crowdfunding.[26] Obwohl P2P-Lending und Crowdfunding von der Regierung als positive Formen der neuen Finanz betrachtet werden und sie besonders in China sehr schnell wachsen, tauchen zeitgleich enorme kriminelle Risiken auf. Auf der einen Seite könnten P2P-Lending und Crowdfunding von Straftätern als Werkzeug für Betrug benutzt werden. Auf der anderen Seite besteht die Gefahr, dass sie gegen die staatlichen Verwaltungsvorschriften für das Finanzwesen verstoßen.

Ein weiteres Beispiel ist die Anwendung der *big data*. Das Konzept der b*ig data* hat enorme Veränderungen in unserer Gesellschaft bewirkt. Mit dieser Technik können Daten in der ganzen Welt gesammelt werden.[27] Durch die Analyse und Anwendung der riesigen Datenmengen werden viele Branchen unserer Gesellschaft tief reformiert werden. Damit geht ein deutlich erhöhtes Risiko einher. Der Datenschutz der Bürger wird immer schwieriger, sodass die Privatsphäre der Menschen leichter beeinträchtigt wird.[28] Es kann zusammengefasst werden, dass mit der Entwicklung der Netzwerktechnologie Risiken und Chancen koexistieren. Es ist offensichtlich unvernünftig, aus Angst vor den Risiken die Chancen aufzugeben. Deswegen müssen wir uns mit den neuen Herausforderungen in der Informationsgesellschaft beschäftigen. Hier sind nicht nur entsprechende gesetzgeberische Änderungen, sondern auch veränderte Denkweisen erforderlich.

---

[26] Mehr Erläuterungen vgl. *Yao Wenping*, Die Internet-Finanz, S. 38 ff.

[27] Siehe *Mayer-Schönberger/Cukier*, Big Data, S. 105 ff.

[28] Siehe ebenda.

II. Technische Grundlagen im Bereich der ISP

A. Entstehung und Entwicklung der ISP

Die Internet-Service-Provider bildeten sich im Entwicklungsprozess des Internets heraus. Vor den 1990er-Jahren wurde das Netzwerk hauptsächlich von der NSF (*National Science Foundation*) und anderen Regierungsbehörden betrieben. Um die Anwendung des Netzwerks zu erweitern, wurde dessen Betrieb allmählich von einigen Internet-Backbone-Providern übernommen. Damit traten die ISP erstmals in Erscheinung.[29] Mit der Entwicklung des Internets wird die interne Struktur der ISP immer komplizierter, allmählich entstanden verschiedene Schichten. Deshalb können die ISP weiter in Backbone, regionale und lokale Provider unterteilt werden.[30] Die Backbone-Provider, auch bekannt als Tier-1-ISP, sind in der Regel große internationale Kommunikationsunternehmen, beispielsweise AT&T, Sprint und NTT.[31] Die regionalen Provider, die als Tier-2-ISP bezeichnet werden, sind die Nutzer der Backbone-Provider, während sie den lokalen Providern Internetdienste zur Verfügung stellen. Die lokalen Provider, nämlich die Tier-3-ISP, sind die Nutzer der Tier-2-ISP. Ihre Dienste haben nur eine begrenzte Reichweite. Die Netzwerke in Universitäten, Unternehmen sowie die der einzelnen Bürger sind oft Nutzer der Tier-3-ISP. Diese in unterschiedlichen Schichten liegenden ISP werden durch den NAP (*Network Access Point*) miteinander verbunden.[32]

Heutzutage sind die ISP ein unentbehrlicher Bestandteil unseres Lebens. Wenn die ISP im Netzwerk nicht bestehen würden, hätten wir keinen Zugang zum Internet. Das heißt, die ISP spielen eine verbindende Rolle im Cyberspace. Es ist auch zu beachten, dass der Umfang der ISP tatsächlich sehr groß ist. Denn nach einer breit gefächerten Definition ist der Provider, der den Benutzerzugriff auf das Internet ermöglicht, ein ISP. Mit anderen Worten: Ein Internetnutzer, der mit dem Internet verbunden ist und sich mit anderen Nutzer verbindet, kann somit auch ein ISP sein.[33] Ein solches Verständnis legt die Schlussfolgerung nahe, dass die ISP in unserer Informationsgesellschaft überall bestehen.

B. Typen der ISP

Im Netzwerk erscheinen die ISP in vielen unterschiedlichen Formen. In allgemein anerkanntem Rahmen werden die ISP nach ihren funktionalen Unterschieden in Content Provider, Hosting Provider, Access Provider und Cache Provider unter-

---

[29] Vgl. *Xie, Xiren* (Hrsg.): Computer-Netzwerk, S. 4.

[30] Vgl. *Forouzan/Mosharraf*, Computer Networks, S. 5 f.

[31] Siehe *Kurose/Ross*, Computer Networking, S. 33.

[32] Vgl. *Xie, Xiren* (Hrsg.): Computer-Netzwerk, S. 5.

[33] Vgl. ebenda, S. 6.

teilt. Diese vier Arten der ISP werden nicht nur von Rechtswissenschaftlern akzeptiert, sondern sind auch in das Gesetz aufgenommen worden. Diese Unterscheidung ist von großer Bedeutung, weil sie der Systematisierung der ISP zugrunde liegt. Dies wird nachfolgend weiter auf detaillierte Weise beschrieben. Darüber hinaus gibt es noch eine Reihe von ISP, die nicht im Gesetz verankert werden. Die rechtlichen Einordnungen der folgenden ISP bleiben deshalb noch offen.

a) Betreiber des Peer-to-Peer-Netzwerks

Das Peer-to-Peer-Netzwerk entstand um das Jahr 2000. Seitdem hat sich diese neue Technik sehr schnell entwickelt. Danach war Napster ein bekanntes Peer-to-Peer-Netzwerk, wurde aber schließlich wegen des Rechtsstreits mit Musikfirmen geschlossen. Jedoch hielt dies die Entwicklung der Peer-to-Peer-Technik nicht auf. Sie ist schon in fast allen Anwendungsgebieten im Netzwerk – wie verteiltes Rechnen, Filesharing, Streaming Media, Sprachkommunikation und Online-Spiele – präsent.[34] Heutzutage sind die Datenflüsse im Peer-to-Peer-Netzwerk deutlich höher als im WWW. Hohe Datenmengen, die nicht nur MP3-Dateien, sondern auch Videos und Software umfassen, werden im Peer-to-Peer-Netzwerk ausgetauscht.[35] Obwohl diese Technik große Bequemlichkeiten für die Menschen bringt, werden gleichzeitig die Urheberrechte im Netzwerk ernsthaft bedroht. Deshalb ist es dringend, die Verantwortlichkeit der Betreiber der Peer-to-Peer-Netzwerke zu bestimmen.

b) Hyperlinksetzer

Der Linksetzer ist ein typischer gesetzlich nicht geregelter ISP. Zahlreiche Webseiten werden durch Hyperlinks verbunden, damit das Internet effizienter funktionieren kann. Aber es gibt auch die Möglichkeit, dass illegale Inhalte, wie Urheberrechte verletzende Dateien oder strafbare pornografische Informationen, verlinkt werden. Deswegen ist es auch unvermeidlich, die Verantwortlichkeit der Hyperlinksetzer zu thematisieren. Bis zu einem gewissen Grad ist der Suchmaschinenbetreiber auch ein Hyperlinksetzer. Da die technischen Grundsätze der Suchmaschinen komplizierter als ein bloßer Hyperlink sind, ist eine differenzierende Betrachtung erforderlich, um die Verantwortlichkeit der Suchmaschinenbetreiber zu bestimmen.[36]

c) Cloud-Service-Provider

Mit der raschen Entwicklung der Cloud-Computing-Technologie entstehen Cloud-Service-Provider. Nach der Definition der NIST (*National Institute of Standards and Technology*) von DOC (*United States Department of Commerce*) wird das Cloud Computing als ein Modell verstanden, das einen ubiquitären, bequemen On-Demand-Netzwerkzugang auf einen gemeinsamen Pool von konfigurierbaren Re-

---

[34] Vgl. *Jin Hai/Liao Xiaofei*, ZTE Kommunikationen Heft 6, 2007, 1 ff.

[35] Vgl. *Xie, Xiren* (Hrsg.): Computer-Netzwerk, S. 374.

[36] Vgl. *Sieber/Liesching*, MMR-Beilage Heft 8, 2007, S. 10 ff.

chenressourcen (zum Beispiel Netzwerke, Server, Speicherung, Anwendungssoftware und Service) ermöglicht, die mit minimalem Managementaufwand oder Service-Provider-Interaktion schnell versorgt und freigegeben werden können. Insgesamt werden drei verschiedene Services von der Cloud-Computing-Technologie umfasst: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS).[37] Obwohl nicht alle Cloud-Services bereits ausgereift sind, werden einige Dienste tatsächlich kommerzialisiert. Beispielsweise existieren viele Diensteanbieter, wie Amazon S3, Google Drive oder Alibaba Cloud, die durch Cloud-Computing-Technologie den Nutzern Speicherdienste zur Verfügung stellen. Jedoch gibt es auch große gesetzliche Risiken bei der Offenlegung der Daten oder der Verletzung der Urheberrechte. Dabei bleibt die Verantwortlichkeit der Cloud-Service-Provider noch unbestimmt.[38]

Mit der weiteren Entwicklung der Netzwerktechnologie werden ständig neue Arten der ISP entstehen. Da diese wieder neue rechtliche Herausforderungen bringen werden, ist es absehbar, dass die Verantwortlichkeit der ISP ein stets relevantes Thema bleibt.

C. Risiken für die ISP

Obwohl die ISP in der Regel nur Internetdienste anbieten und Delikte nicht direkt begehen, können sie nicht nur mit zivilrechtlichen, sondern auch mit strafrechtlichen Risiken konfrontiert sein, weil die von ihnen angebotenen Dienste von Dritten missbraucht werden könnten. Die rechtlichen Risiken ergeben sich aus zwei Perspektiven. Einerseits könnten die ISP eine indirekte Haftung übernehmen, weil sie die Delikte von Dritten durch ihre Dienste fördern oder anstiften. Andererseits könnten sie auch eine direkte Haftung tragen, wenn sie, wie von der Allgemeinheit erwartet, eine Verpflichtung zur Überprüfung und Kontrolle der von ihnen gespeicherten Daten und relevanten Handlungen von Dritten übernehmen.

Tatsächlich sind die Handlungen der ISP und die der Dritten relativ getrennt voneinander zu betrachten. In Wirklichkeit haben die ISP nur eine begrenzte Kontrollmöglichkeit, die Informationen und Handlungen von anderen zu verwalten. Darüber hinaus ist die Menge der durch ISP übermittelten oder gespeicherten Informationen ziemlich groß, während der Zustand dieser Informationen sich dauernd verändert. Aus diesen Gründen ist die Frage schwierig zu beantworten,

---

[37] Siehe *Mell/Grance*, The NIST Definition of Cloud Computing, NIST Special Publication 800-145, 2011, S. 2–3. Nach der Definition von NIS Directive (2016) versteht man unter „Cloud-Computing-Dienst" einen digitalen Dienst, der den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht.

[38] Vgl. *Xu Huili*, Technologie und Recht Heft 6, 2013, 1 ff.; *Qi Aimin/Zhu Gaofeng*, Zeitschrift der Chongqing-Universität (Sozialwissenschaftliche Ausgabe) Heft 1, 2017, 103 ff.

inwieweit und welche Verpflichtungen die ISP übernehmen müssen und unter welchen Voraussetzungen sie privilegiert werden können.

III. Technische Kontrollmöglichkeiten der ISP

A. Grundlagen der Kontrollmöglichkeit

Bevor die Verantwortlichkeit der ISP diskutiert wird, ist es unverzichtbar, die technischen Kontrollmöglichkeiten der ISP zu analysieren, weil diese ausschlaggebend für die rechtliche Bewertung der ISP sind. Wenn die ISP in bestimmten Konstellationen nur sehr begrenzte oder gar keine Kontrollmöglichkeit hätten, ihnen aber eine hohe Verpflichtung zur Verwaltung der Informationen oder Handlungen von Dritten obläge, würden die einschlägigen Gesetze ihre Legitimität verlieren. Deshalb muss die Verpflichtung, die die ISP tragen, ihren realen Kontrollmöglichkeiten entsprechen. Eine pauschale Aussage lässt sich dazu allerdings nicht treffen. Hier ist eine differenzierende Betrachtung notwendig.

a) Content Provider

Content Provider haben offensichtlich die vollständige Kontrolle über die Inhalte, weil die Inhalte von ihnen selbst angeboten werden. Diese vollständige Kontrollfähigkeit bedeutet, dass die Content Provider grundsätzlich keine Privilegierung erfahren.

b) Access Provider

Für die bloßen Access Provider sind die Kontrollmöglichkeiten sehr begrenzt. Die Schwierigkeiten für diese Form der Kontrolle wurden von *Sieber* ausführlich erläutert. Auf der einen Seite ist die Identifizierung der rechtswidrigen Inhalte für die Access Provider sehr schwierig. Da die Inhalte nicht auf dem Server der Access Provider gespeichert werden, setzt die Identifizierung der rechtswidrigen Inhalte eine Zulassung von fremden Computern voraus. Neben den eingeschränkten Abfragemöglichkeiten macht die Masse des weltweiten Datenangebots diese Identifizierung noch mühsamer. Deshalb kann man hier nur von Kontrollmaßnahmen zu den als rechtswidrig erkannten Inhalten sprechen.[39] Auf der anderen Seite ist eine Zugangssperre durch die Access Provider mit vielen Hindernissen behaftet. Aus konzeptioneller und rechtlicher Sicht verstößt das Sperren vor allem gegen Fernmeldegeheimnis, Betriebsgeheimnis, Persönlichkeitsrechte sowie die Informationsfreiheit der Nutzer. Zudem gibt es eine Reihe von technischen Schwierigkeiten der Echtzeitkontrolle moderner Massenkommunikation: hierzu gehören Firewall,

---

[39] Vgl. *Sieber*, CR Heft 11, 1997, 658–659.

Schichtenmodell der Computernetze[40] und Verschlüsselung.[41] Deshalb lässt sich zusammenfassend feststellen, dass die bloßen Access Provider im Allgemeinen wenig Kontrollmöglichkeiten haben. Diese Tatsache führt zu einem relativ begrenzten Umfang der Haftung von Access Providern.

c) Caching Provider und Hosting Provider

Für die ISP, die Inhalte auf einem eigenen Server speichern, wird die Situation komplizierter. Sie haben ebenfalls viele Schwierigkeiten, die möglicherweise rechtswidrigen Inhalte zu kontrollieren, da die gespeicherten Daten verschlüsselt werden können und der Speicherzustand der zahlreichen Daten sich sehr schnell verändert. Nachdem die rechtswidrigen Inhalte identifiziert worden sind, ist die Löschung oder Sperrung dieser Inhalte aber in der Regel kein Problem, weil diese Daten schon durch entsprechende Programme bei der Speicherung gezielt verarbeitet worden sind.[42] Mit anderen Worten: Diese ISP (oft die Caching Provider und die Hosting Provider) verfügen über eine bedingte Kontrollmöglichkeit.

B. Die technische Entwicklung und ihre Folgen

Die Frage der Kontrollmöglichkeiten war die Triebfeder für eine Reihe von wichtigen Gesetzen über die Verantwortlichkeit der ISP. Obwohl sie bis heute im Allgemeinen noch zutreffend sind, müssen wir diese Problematik im Hinblick auf die ständige Entwicklung der Netzwerktechnologie erneut berücksichtigen. Vor allem ist der große Fortschritt der Filtertechnologie nicht zu ignorieren. Vor 20 Jahren war es technisch höchst umständlich, rechtswidrige Informationen aus zahlreichen Daten auszuschließen. Damals waren die Identifizierung und Löschung illegaler Inhalte wegen der Begrenztheit der technischen Mittel kostspielig und zeitaufwendig. Jedoch hat sich die Filtertechnologie in den vergangenen zwei Jahrzehnten sehr schnell entwickelt, sodass es sich für die Hosting Provider nicht mehr allzu schwierig gestaltet, die rechtswidrigen Inhalte ohne große Mühen zu filtern. Heutzutage gibt es insgesamt vier Arten von Informationsfilterung *(information filtering)*:

a) die Filterung nach PICS (Platform for Internet Content Selection);

b) die Filterung nach URL (Uniform Resource Locator);

c) die Filterung nach Schlüsselwörtern;

d) die Filterung nach intelligenter Inhaltsanalyse.[43]

---

[40] Vgl. *Sieber*, Verantwortlichkeit im Internet, S. 27, Rn. 51.

[41] Vgl. *Sieber*, CR Heft 11, 1997, 659 ff.

[42] Vgl. *Sieber*, CR Heft 11, 1997, 654 ff.

[43] Vgl. *Sun Yan/Zhou Xueguang*, Informationssicherheit und Vertraulichkeit der Kommunikation Heft 9, 2011, 45.

Die PICS wurde 1995 von W3C (World Wide Web Consortium) etabliert, um die Nutzer vor schädlichen Informationen im Web zu schützen. Diese Plattform liefert uns das Kriterium, um die Inhalte im Web zu markieren und abzustufen, damit die schädlichen Inhalte nach dem vom Nutzer gesetzten Standard gefiltert werden können. Die Filterung nach URL setzt eine Datenbank voraus, in der die IP-Adresse oder URL von verbotenen und zugelassenen Webseiten im Voraus gespeichert werden. Dann können die rechtswidrigen Inhalte nach dieser schwarzen und weißen Liste gefiltert werden. Die Filterung nach Schlüsselwörtern beruht auch auf einer Datenbank, in der Merkmale der Dateien, die mit Schlüsselwörtern beschrieben werden, gespeichert werden. Dann werden die relevanten Dateien nach diesen Schlüsselwörtern ausgeschlossen. Die Filterung mittels intelligenter Inhaltsanalyse wird durch neue Technologien wie Sprachanalyse, Bildverarbeitung, maschinelles Lernen sowie künstliche Intelligenz realisiert, welche die Bedeutung von Text, Bild usw. genau verstehen.[44]

Obwohl aus technischer Sicht die Filterungen nach PICS, URL und Schlüsselwörtern relativ einfach sind, können sie die rechtswidrigen Inhalte bis heute nicht sehr wirksam filtern. Die PICS bietet nur ein grundlegendes Kriterium für die Markierung und Abstufung. Bei der Wirksamkeit der Filterungen kommt es aber tatsächlich auf das Setzen konkreter Standards für die Nutzer an. Die Filterungen nach URL und Schlüsselwörtern sind relativ statische und formelle Überprüfungen, denn in der allgemein zugelassenen URL könnten sich noch illegale Inhalte befinden und die Schlüsselwörter der Dateien nicht ihren eigentlichen Inhalten entsprechen. Deshalb rücken Untersuchung und Anwendung der Filterung nach der intelligenten Inhaltsanalyse allmählich in den Vordergrund.[45]

Inzwischen ist die Inhaltsanalyse-Technologie für Textdateien recht ausgereift. Die Urheberrechte verletzenden Inhalte in Textdateien können genau und ohne Weiteres identifiziert werden. Diese Technologie ist schon von CNKI (*National Knowledge Infrastructure*) aufgenommen und breit angewendet worden.[46] Für Videodateien ist eine Filterung nach intelligenter Inhaltsanalyse dagegen schwieriger. Jedoch ist diese Technik in den letzten Jahren deutlich verbessert worden. Dabei wurde eine Reihe von Schlüsseltechnologien wie videozeitliche Segmentierung, Schlüsselrahmen-Extraktion, Bildinhaltserkennung usw. eingeführt.[47] Inzwischen ist die Fehlerrate der Filterung nach intelligenter Inhaltsanalyse sehr niedrig, obwohl die Geschwindigkeit der Überprüfung erstaunlicherweise hoch ist. Deshalb ist diese Technik schon von einigen bekannten Internetunternehmen wie *YouTube*,

---

[44] Vgl. *Su Shengyong/Liu Hui*, Welt der digitalen Kommunikation Heft 9, 2016, 56 ff.; *Sun Yan/Zhou Xueguang*, Informationssicherheit und Vertraulichkeit der Kommunikation Heft 9, 2011, 45 ff.

[45] Vgl. *Jiang Chengming* u.a., Informationssicherheit und Vertraulichkeit der Kommunikation Heft 2, 2012, 76; *Peng Le* u.a., Ingenieurinformatik und Design Heft 10, 2008, 2587.

[46] Vgl. *Cui Guobin*, Chinesische Rechtswissenschaft Heft 2, 2017, 217.

[47] Vgl. *Peng Le* u.a., Ingenieurinformatik und Design Heft 10, 2008, 2587 ff.

Baidu und *Tencent* angewendet worden.[48] Diese technische Entwicklung bedeutet, dass die Filterung der rechtswidrigen Inhalte für die ISP einfacher wird. Das heißt, die Kontrollmöglichkeiten der ISP werden dank des technischen Fortschritts größer. Aus diesem Grund kann an dem sogenannten s*afe harbor*- sowie dem r*ed flag*-Prinzip gezweifelt werden, das auf einem alten technischen Zustand aus dem Jahr 1998 beruhte.[49]

In unserer Informationsgesellschaft entwickelt sich die Netzwerktechnologie rasch, während unser Rechtssystem hingegen oft stabil bleibt. Dieser Widerspruch könnte zu einem Ungleichgewicht zwischen Rechten und Pflichten führen. Angesichts dieser Situation sollten wir die Verantwortlichkeit der ISP aus einer dynamischen Perspektive überdenken.

C. Unterschiede zwischen faktischen und normativen Kontrollmöglichkeiten

Allerdings ist auch zu beachten, dass die Beurteilung der Kontrollmöglichkeiten der ISP nicht nur eine rein faktische Bewertung ist. Es gibt viele andere Elemente, die in Betracht zu ziehen sind. Es ist notwendig, zwischen faktischer und normativer Kontrollmöglichkeit zu differenzieren. Wenn die ISP die rechtswidrigen Inhalte um jeden Preis überprüfen würden, könnten die illegalen Inhalte natürlich erfolgreich gefiltert werden. Aber auf diese Weise vermag kein ISP die schwere Belastung zur Überprüfung der rechtswidrigen Inhalte zu tragen. Das heißt, neben der faktischen und physikalischen Kontrollfähigkeit müssen berechtigterweise die Betriebskosten der ISP in Erwägung gezogen werden. Jedoch können die Betriebskosten der ISP zur Verhinderung der rechtswidrigen Inhalte unter besonderen Umständen ganz unterschiedlich ausfallen. Deshalb ist eine zutreffende Abwägung hier nicht einfach. Meines Erachtens lässt sich dieses Problem unter Berufung auf den allgemeinen Industriestandard behandeln. Wenn wir zum Beispiel die Verpflichtung eines Betreibers einer Video-Webseite zur Filterung der rechtswidrigen Inhalte nicht bestimmen können, ist es hilfreich zu untersuchen, ob die meisten anderen Betreiber einer Video-Webseite in der gleichen Branche bestimmte Filtrationsmaßnahmen ergriffen haben. Wenn das der Fall ist, kann die Verletzung der Verpflichtung seitens des Betreibers bestimmt werden. Darüber hinaus ist großer Wert auf die Informationsfreiheit und Privatsphäre der Menschen zu legen. Mit der raschen Entwicklung der Informationstechnologie werden die Informationsfreiheit und die Privatsphäre der Menschen ernsthaft bedroht, weil die technischen Angriffe heutzutage in fast allen Lebensbereichen stattfinden. Wenn die Kontrolle der ISP die Bedrohung der Informationsfreiheit oder die Verletzung der Privatsphäre zur Voraus-

---

[48] Vgl. *Cui Guobin*, Chinesische Rechtswissenschaft Heft 2, 2017, 218 ff.

[49] Vgl. ebenda, 220 ff.; *ders.,* Chinesische Rechtszeitschrift Heft 4, 2013, 139 ff.; *Liu Wenjie*, Rechtszeitschrift der Universität Peking Heft 2, 2012, 398 ff.

setzung hat, sollten wir sie außen vor lassen.[50] Außerdem muss die Rechtspolitik, die sich mit der Bekämpfung der Cyberkriminalität beschäftigt, in Erwägung gezogen werden. Für eine wirksame Bekämpfung der Cyberkriminalität ist es erforderlich, dass die Strafverfolgungsbehörden und die ISP eng zusammenarbeiten. Beide Seiten sollten die gegenseitigen Schwierigkeiten und Bedürfnisse verstehen und tolerieren. Nur auf diese Weise kann das Vertrauen zwischen Strafverfolgungsbehörden und ISP begründet werden, um ein Gleichgewicht zwischen Rechten und Pflichten für ISP zu erreichen.[51] Deshalb ist die Bestimmung der endgültigen Kontrollmöglichkeit der ISP auch abhängig von der Arbeitsteilung und von den Kompromissen zwischen zuständigen Behörden und ISP.

Schließlich sollte die Industriepolitik berücksichtigt werden. Wie allgemein bekannt, ist die technische Innovation in unserer Gesellschaft oft mit rechtlichen Risiken verbunden. Manchmal ist dieses Phänomen auf die Opposition der ursprünglichen Interessengruppen zurückzuführen. Beispielsweise wurde Skype von vielen Telekommunikationsunternehmen, die ihren telefonischen Service bedroht sahen, unterdrückt. Heutzutage ist der Anruf mit Skype weltweit üblich. Ein anderes Beispiel ist der SMS-Service: Früher wurde WeChat der Firma *Tencent* von den großen chinesischen Telekommunikationsbetreibern unterdrückt, da der SMS-Service sogar den telefonischen Service dieser Telekommunikationsbetreiber durch den kostenlosen Service von WeChat ersetzte. Jedoch hat WeChat bis 2016 erstaunlicherweise 889 Millionen aktive Nutzer,[52] während hingegen der Marktanteil des SMS-Services ständig gesunken ist.[53] Ein weiteres überzeugendes Beispiel ist die Peer-to-Peer-Technologie. Der bekannte Peer-to-Peer-Netzwerk-Provider *Napster* wurde schließlich wegen Urheberrechtsverletzung geschlossen. Allerdings ist heutzutage die Peer-to-Peer-Technologie in sehr vielen Branchen etabliert. Wenn die Politik damals Druck ausgeübt und bei diesem Service der ISP hart durchgegriffen hätte, würden viele bequeme Internetservices heute nicht mehr bestehen. Deshalb sollte es genug Raum für die Entwicklung der neuen Technologie und Industrie geben, wenn über den Umfang der Verpflichtungen der ISP diskutiert wird.

Zusammenfassend lässt sich feststellen, dass die Beurteilung der Kontrollmöglichkeiten sich nicht nur als eine faktische, sondern auch als eine normative Bewertung darstellt. Die rein faktische Bewertung bildet die Grundlage für die Beurteilung der Kontrollmöglichkeit. Dies ist jedoch nur als eine notwendige, aber nicht hinreichende Bedingung zu betrachten. Daneben soll auch eine Reihe von sozialen, wirtschaftlichen und politischen Elementen in Betracht kommen.

---

[50] Vgl. *Sieber*, CR Heft 11, 1997, 659–660.

[51] Vgl. *Sieber*, MMR Heft 12, 1999, 690.

[52] Vgl. Bericht über die Nutzer von WeChat, abrufbar unter http://www.sohu.com/a/136382735_184641 [Stand: 15.09.2017].

[53] Vgl. Die volle Rezession des SMS-Service, abrufbar unter http://tech.163.com/14/0603/10/9TQC2KRF000915BE.html [Stand: 15.09.2017].

Zweiter Teil

Verantwortlichkeit der ISP in Deutschland

I. Historische Entwicklung, Begriff und Typen der ISP

A. Historische Entwicklung

Die Nutzung von Internetdiensten durch Wissenschaft und Forschung begann in Deutschland mit der Gründung des Vereins zur Förderung eines Deutschen Forschungsnetzes (DFN) im Jahr 1984. Seit Anfang der 90er Jahre bieten immer mehr ISP der Öffentlichkeit ihre Internetdienste an.[1] Das Internet und die Netzwerktechnik haben sich in Deutschland rasch entwickelt. In Juni 2017 betrug die Zahl der deutschen Internetnutzer insgesamt 72.29 Millionen.[2] Der Anteil der Internetnutzer an der deutschen Gesamtbevölkerung erreichte 89.6 %, während der durchschnittliche Anteil weltweit im Jahr 2016 nur 45.9% ausmachte.[3] Außerdem sind die sozialen Netzwerke in Deutschland äußerst populär. Nach der Statistik von Internet World Stats betrug die Zahl der Facebook-Abonnenten 31 Millionen.[4]

Gleichzeitig nimmt auch die Cyberkriminalität immer mehr zu. Nach der Statistik des Bundeskriminalamts ist die Computerkriminalität von 70.068 Fällen im Jahr 2015 auf 107.751 Fälle im Jahr 2016 angestiegen.[5] In den letzten Jahren haben sich Hasskriminalität und andere strafbare Inhalte in den sozialen Netzwerken weit verbreitet. Die Frage, inwieweit die ISP selbst die Verpflichtungen zur Lösung und Sperrung der rechtswidrigen Inhalte übernehmen sollen, ist umstritten und problematisch. Als gesetzliche Reaktion auf diese Entwicklung wurde bereits im Jahr 1997 das Informations- und Kommunikationsdienste-Gesetz (IuKDG) einschließlich des TDG in Deutschland erlassen. Ziel dieses Gesetzes war die Schaffung einer verlässlichen Grundlage für die Gestaltung der sich dynamisch entwickelnden Angebote im Bereich der Informations- und Kommunikationsdienste.[6] Darin wurden vor allem auch die ISP mit Verantwortlichkeitsprivilegien ausgestattet. Die

---

[1] Vgl. *Bleisteiner*, Rechtliche Verantwortlichkeit im Internet, S. 16.

[2] Die Daten stammen von Internet World Stats, abrufbar unter http://www.internetworldstats.com/europa.htm#de [Stand: 15.09.2017].

[3] Die Daten stammen von der Weltbank, abrufbar unter https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2016&start=1990&view=chart [Stand: 15.09.2017].

[4] Die Daten stammen von Internet World Stats, abrufbar unter http://www.internetworldstats.com/europa.htm#de [Stand: 15.09.2017].

[5] Vgl. Bundesministerium des Innern, Bericht zur Polizeilichen Kriminalstatistik 2016, S. 9.

[6] Vgl. BT-Drs. 13/7385, S. 1.

Richtlinie über den elektronischen Geschäftsverkehr (*Electronic Commerce Directive*/ECRL) 2000 des Europäischen Parlaments verlangte dann Modifizierungen dieser Privilegierungen, die der Gesetzgeber schließlich im Telemediengesetz 2007 umgesetzt hat. Aufgrund der zunehmenden Verbreitung von Hasskriminalität und anderen strafbaren Inhalten in sozialen Netzwerken wurden dann die Verpflichtungen zur Löschung und Sperrung der strafbaren Inhalte durch das Netzwerkdurchsetzungsgesetz 2017 präzisiert.[7] Das NetzDG verlangt von Plattformbetreibern daneben auch die Einführung eines Beschwerdemanagementsystems und führt Berichtspflichten für den Umgang mit Beschwerden der Nutzer über illegale Inhalte ein.

B. Rechtliche Begriffe

Die Bestimmung der strafrechtlichen Verantwortlichkeit der ISP hängt zuerst davon ab, wie der Begriff der Internet-Service-Provider definiert wird. Wie schon erläutert, ist der Begriff der ISP im Computerbereich nicht sehr explizit gefasst. Nach der technischen Definition sind ISP ausgesprochen komplex gestaltet. Deshalb muss der Begriff in der Gesetzgebung eingegrenzt und typisiert werden, sonst ist die genaue Bestimmung der strafrechtlichen Verantwortlichkeit der ISP nicht möglich. Nach § 3 Teledienstegesetz (TDG) 1997 waren „Diensteanbieter" (ISP) natürliche oder juristische Personen oder Personenvereinigungen, die eigene oder fremde Teledienste zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln. Der Art 2 (b) der elektronischen Geschäftsverkehrsrichtlinie (ECRL) 2000 des Europäischen Parlaments sieht vor, dass jede natürliche oder juristische Person, die informationsgesellschaftliche Dienste anbietet, ein Service-Provider ist. Nach § 1 (c) der Konvention über Cyberkriminalität 2001 (*Convention on Cybercrime*) ist der Service-Provider:

1) jedes öffentliche oder private Subjekt, das den Nutzern ihres Dienstes die Möglichkeit gibt, mittels eines Computersystems zu kommunizieren;
2) jedes andere Subjekt, das die Computerdaten im Auftrag eines solchen Kommunikationsdienstes oder Nutzers dieser Dienste verarbeitet oder speichert.

Das Telemediengesetz (TMG) 2007, das von den ECRL stark beeinflusst wurde, nahm den Begriff der „Diensteanbieter" aus dem TDG auf. Neben der grundlegenden Definition der ISP sieht das TMG auch vor, dass bei audiovisuellen Mediendiensten auf Abruf jede natürliche oder juristische Person, die die Auswahl und Gestaltung der angebotenen Inhalte wirksam kontrolliert, ein Service-Provider ist.

Jedoch sind diese rechtlichen Begriffe im Allgemeinen immer noch zu weit gefasst. Die oben genannten begrifflichen Beschreibungen wie „Teledienste zur Nutzung bereithalten", „Zugang zur Nutzung vermitteln" usw. können fast alle Hand-

---

[7] Vgl. BT-Drs. 18/12356, S. 11.

lungen bezüglich der informatischen Dienstleistung enthalten. Damit stellt dieser allgemeine Begriff nur eine grundlegende Begrenzung für ISP bereit.

Erstens hat der Begriff „Internet-Service" zahlreiche Bedeutungen, weil es hier keine feste und klare Grenze für die Internetdienste gibt. So galten die Vorschriften in TDG nach § 2 Abs. 1 a.F. TDG für alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bildern oder Tönen bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt. Nach § 1 Abs. 1 TMG gilt dieses Gesetz sogar für alle elektronischen Informations- und Kommunikationsdienste. Zweitens kann die Form der Bereitstellung von Internet-Services sowohl unmittelbar als auch mittelbar erfolgen. Zum Beispiel wird die Vermittlung des Zugangs zur Nutzung nach § 2 TMG zu Service-Providern gerechnet. Darüber hinaus kann die wirksame Kontrolle über die Auswahl und Gestaltung der angebotenen Inhalte nach § 2 Abs. 1 TMG bei audiovisuellen Mediendiensten auf Abruf zu Service-Providern gehören.[8] Drittens können die ISP nicht nur natürliche oder juristische Personen sein, sondern sich weiter in kommerzielle und öffentliche Diensteanbieter gliedern.[9]

Daher bedeutet diese umfassende Eigenschaft des Begriffs, dass Internet-Service-Provider nur „ein Top-Level-Konzept" sind. Wie Kaufmann es ausdrückt: „Begriffe ohne Typen sind leer; Typen ohne Begriffe sind blind".[10] Um die Verantwortlichkeit der ISP genauer zu bestimmen, müssen wir den Begriff weiter typisieren.

Es ist auffällig, dass auch im Telekommunikationsgesetz (TKG) ein Begriff der Telekommunikationsdienste existiert. Nach § 3 Abs. 24 TKG sind die „Telekommunikationsdienste" diejenigen Dienste, die ganz oder überwiegend Signale über Telekommunikationsnetze übertragen, einschließlich der Übertragungsdienste in Rundfunknetzen. Aber im Gegensatz zu den elektronischen Informations- und Kommunikationsdiensten beziehen sich die Telekommunikationsdienste nur auf die rein technischen Aspekte statt auf inhaltliche Gesichtspunkte.[11]

---

[8] Ob es sich um kabelgebundene oder drahtlose Verbindungen handelt, spielt keine Rolle. Siehe dazu Spindler/Schuster-*Hoffmann,* TMG § 8, Rn. 17.

[9] Vgl. ebenda, TMG § 2, Rn. 2.

[10] Vgl. *Kaufmann*, Analogie und „Natur der Sache", S. 43.

[11] Vgl. *Sieber*, Verantwortlichkeit im Internet, S. 132, Rn. 267.

C. Rechtliche Typen der ISP

1. Kriterium für die Typisierung

Bevor der Begriff der ISP typisiert werden kann, muss dazu erst ein Kriterium der ISP bestimmt werden. Da die Netzwerkdienste sowohl ein professionelles als auch ein technisches Merkmal haben, ist die technologiebasierte funktionelle Einteilung zweifellos ein geeignetes Kriterium. Nach der vorherrschenden Meinung soll die typische Einteilung der ISP nicht auf dem personellen und abstrakten Status, sondern auf spezifischen funktionellen Aktivitäten basieren.[12]

Die netzwerktechnische Analyse ist meines Erachtens die Basis der normativen Untersuchung zur strafrechtlichen Verantwortlichkeit der ISP. Wenn wir kein allgemeines Verständnis über das Funktionsprinzip des Internets erarbeiten, wird unsere Untersuchung in die Irre führen, sodass die Schlussfolgerungen nicht der Realität entsprechen. Deshalb ist, um die Verantwortlichkeit der ISP zu beurteilen, zuerst eine Analyse der technischen Aktionsmöglichkeiten der Provider vonnöten. Die technischen Kontrollmöglichkeiten der ISP müssen nach deren Funktionen differenziert werden.[13]

2. Rechtliche Typen der ISP

Das TDG 1997 sieht zwei grundlegende Typen vor, nämlich Diensteanbieter für eigene Inhalte und Diensteanbieter für fremde Inhalte. Diensteanbieter für fremde Inhalte werden weiter in Zugangsvermittler einerseits und Anbieter zur automatischen und kurzzeitigen Vorhaltung fremder Inhalte andererseits aufgeteilt.[14] Die ECRL 2000 der EU bieten eine detailliertere Klassifizierung, nämlich reine Durchleitung (*mere conduit*), Caching und Hosting. Danach nahm das TMG 2007 die Typen der ISP aus TDG und ECRL auf,[15] genauer gesagt: Durchleitung von Informationen, Zwischenspeicherung zur beschleunigten Übermittlung von Informationen sowie Speicherung von Informationen. Nach diesen Regelungen werden theoretische Typen der ISP gebildet, zum Beispiel die Inhaltsanbieter (Content Provider), die Betreiber der Netzwerke (Network Provider), die Zugangsvermittler zum Netz

---

[12] Vgl. *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht, S. 57, Rn. 179; *Kessler*, Zur strafrechtlichen Verantwortlichkeit von Zugangsprovidern, S. 42 ff.; Lackner/Kühl-*Heger,* § 184, Rn. 7.

[13] Vgl. *Sieber*, ZUM Heft 3, 1999, 197.

[14] Das TDG wurde dreimal, Juni 2000, Dezember 2001 und November 2006, vom Bundestag reformiert. Nach der letzten gesetzlichen Änderung wurde das TDG fast gleich wie die ECRL. Vgl. 27. Juni 2000, BGBI. I, S. 907; 14. Dezember 2001, BGBI. I, S. 3721; 10. November 2006, BGBI. I, S. 2585.

[15] Vgl. Spindler/Schuster-*Hoffmann*, TMG § 7, Rn. 5.

(Access Provider) und die Betreiber der Computersysteme, auf denen die Daten gespeichert werden (Host-Service-Provider).[16]

Die Content Provider sind die Diensteanbieter, die eigene Inhalte präsentieren. Unter Access Providern werden die Diensteanbieter verstanden, die nur den Zugang zur Nutzung fremder Inhalte vermitteln. Als Network Provider werden die Diensteanbieter bezeichnet, die fremde Informationen in einem Kommunikationsnetz übermitteln.[17] Die Host-Service-Provider speichern fremde Inhalte auf ihren Servern. Die Differenzierung zwischen Network- und Access Provider hängt davon ab, ob auf den Zugang zu Daten über ein Leitungsnetz, über einen Einwahlknoten oder auf der Ebene der Anwendungsschicht abgestellt wird.[18] Die Access Provider und die Network Provider bieten nur die Durchleitung von Informationen. „Neben den reinen Zugangsanbietern können auch Peer-to-Peer-Systeme, [19] E-Mail-Dienste[20] und W-LANs[21] unter § 8 TMG fallen".[22]

Die oben genannte Einteilung der ISP entspricht den technischen Kontrollmöglichkeiten. Die Content Provider haben volle Kontrolle über ihre Inhalte. Den Host-Service-Providern ist eine Prüfung und gegebenenfalls Sperrung konkret bekannter Daten möglich und zumutbar, wenn sie genaue Kenntnis über illegale Inhalte haben.[23] Den Network- und Access Providern ist eine Kontrolle und Sperrung der im Internet übermittelten Inhalte grundsätzlich nicht möglich.[24]

Diese funktionale Einteilung der ISP, die dem Grad der technischen Kontrollmöglichkeiten entspricht, bildet das Fundament für die Privilegien der ISP.

---

[16] Vgl. *Sieber*, ZUM Heft 3, 1999, 197; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 57–58, Rn. 180; *Malek/Popp*, Strafsachen im Internet, S. 13, Rn. 49; *Matthies*, Providerhaftung für Online-Inhalte, S. 30–31 ff.

[17] Vgl. *Hilgendorf/Valerius*, ebenda, S. 57–58, Rn. 180.

[18] Vgl. *Sieber*, Verantwortlichkeit im Internet, S. 10, Rn. 14, Anm. 26.

[19] Eine detaillierte Erörterung über die Einordnung der Peer-to-Peer-Systeme als Diensteanbieter vgl. *Brinkel*, Filesharing, S. 338 ff.; *Lang*, Filesharing und Strafrecht, S. 114 ff.

[20] Das OLG Karlsruhe, Urteil vom 08.05.2002 – 6 U 197/01, entschied, dass der Access Provider für eine Verletzung der Wettbewerbsordnung durch unzulässige Versendung von Faxwerbung via Internet durch ihre Kunden grundsätzlich nicht haftet.

[21] Vgl. Spindler/Schuster-*Ricke*, TMG § 2, Rn. 2. Das LG Hamburg, Urteil vom 26.07.2006 – Az. 308 O 407/06, entschied, dass die Verwendung einer ungeschützten WLAN-Verbindung für den Zugang zum Internet Prüfungs- und gegebenenfalls Handlungspflichten im Rahmen einer Störerhaftung auslösen, um der Möglichkeit solcher Rechtsverletzungen vorzubeugen.

[22] *Marberth-Kubicki*, Computer- und Internetstrafrecht, S. 180–181, Rn. 368.

[23] Vgl. *Sieber*, ZUM Heft 3, 1999, 198; *ders.,* CR Heft 11, 1997, 654 ff.

[24] Vgl. *Sieber*, ZUM 1999, 197; *ders*, CR Heft 11, 1997, 658 ff.

3. Unterscheidung zwischen zwei Zwischenspeicherungen

Problematisch ist die Position des „Caching". Nach den Regelungen der ECRL und des TMG gibt es zwei unterschiedliche Zwischenspeicherungen. Wenn die automatische, kurzzeitige Zwischenspeicherung nur zur Datenübertragung im Kommunikationsnetz geschieht und die Informationen nicht länger, als es für die Übermittlung üblicherweise erforderlich ist, gespeichert werden, gehört die Zwischenspeicherung gemäß § 8 Abs. 2 TMG zur Durchleitung von Informationen. Sollte die automatische, zeitlich begrenzte Zwischenspeicherung allein dem Zweck dienen, die Übermittlung der Informationen an andere Nutzer auf deren Anfrage effizienter zu gestalten, fällt sie unter § 9 TMG. Offensichtlich ist es schwierig, nach dem Wortlaut des TMG beide Zwischenspeicherungen zu unterscheiden. Deshalb gibt es viele theoretische Versuche, um dieses Problem zu lösen.

Erstens wird behauptet, dass § 9 TMG die Zwischenspeicherung mithilfe von Proxy-Cache-Servern behandele, während § 8 Abs. 2 TMG die Zwischenspeicherung im Rahmen der Zugangsvermittlung regele.[25] Aber dieses Kriterium lässt sich nicht anwenden, um eine klare Grenze zwischen zwei ähnlichen „Cachings" zu ziehen. Zweitens wird die Meinung vertreten, der Nutzer habe keinen Zugang zu der zwischengespeicherten Information bei der unter § 8 Abs. 2 TMG fallenden Zwischenspeicherung.[26] Dies trifft jedoch auf die meisten kurzzeitigen Zwischenspeicherungen zu. Nach diesem Kriterium ist der Umfang der unter § 8 Abs. 2 TMG fallenden Zwischenspeicherung so umfassend, dass § 9 TMG entbehrlich wird. Eine dritte Auffassung befürwortet, dass es sich bei § 9 Abs. 2 a.F. TDG im Unterschied zu § 10 a.F. TDG gerade um ein durch die konkrete Übermittlung veranlasstes Zwischenspeichern handeln müsse, nicht um ein allgemeines Vorhalten der Informationen ohne konkrete Veranlassung durch einen bestimmten Nutzer, um einen erleichterten Zugang zu schaffen.[27] Eine ähnliche Ansicht hält an der These fest, dass die unter § 9 Abs. 2 a.F. TDG fallende automatische, kurzzeitige Zwischenspeicherung in einem technischen Zusammenhang mit dem Routing stehe. Das heißt, bei der Übermittlung von Informationen werden die zu übermittelnden Datenmengen in kleine einzelne Datenpakete aufgeteilt und später auf dem Übertragungsweg wieder zusammengefügt.[28]

Aber diese Auffassungen sind im Ergebnis und in der Begründung zurückzuweisen. Auf der einen Seite werden fast alle automatischen, kurzzeitigen Zwischenspeicherungen durch konkrete Übermittlung der Informationen veranlasst. Außerdem ist der Unterschied zwischen konkreter Übermittlung und allgemeinem Vorhalten der Information nicht klar. Auf der anderen Seite dürften die Service-Provider des

---

[25] Vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 68, Rn. 223.

[26] Vgl. BT-Drs. 14/6098, S. 24; Schönke/Schröder-*Eisele*, § 184, Rn. 88.

[27] Vgl. *Spindler/Schmitz/Geis*, TDG-Kommentar, 2004, § 9, Rn. 8.

[28] Vgl. *Hoffmann*, MMR Heft 5, 2002, 287.

durch konkrete Übermittlung veranlassten Zwischenspeicherns Kontrollmöglichkeiten zu den illegalen Inhalten haben. Deshalb ist es nicht sinnvoll, diese Service-Provider nur als Access Provider zu betrachten.

Die kurze Zeitdauer der Zwischenspeicherung ist nach der herrschenden Meinung und dem legislativen Material ein wichtiges Merkmal. Die unter § 8 Abs. 2 TMG fallende Zwischenspeicherung darf allenfalls nur wenige Stunden andauern, sonst liegt keine reine Durchleitung mehr vor, sondern bereits ein (nicht privilegiertes) Bereithalten von Informationen.[29] Dagegen heißt es, dass diese Zeitbegrenzung der Realität von Proxy-Cache-Speichern in den heutigen Computernetzen nicht gerecht wird: „Denn die Speicherdauer von Daten auf Proxy-Cache-Speichern wird i. d. R. nicht durch feste und vom Betreiber des Servers fixierte Zeitintervalle bestimmt, sondern durch die Kapazität des Servers.“[30]

Die Zeitbegrenzung sollte nicht als maßgebendes Unterscheidungskriterium betrachtet werden, weil die Zeitdauer der Zwischenspeicherung aus technischer Sicht in der Regel nicht von der Kontrolle der ISP, sondern von der Popularität der Inhalte abhängt. Je beliebter die Inhalte bei den Nutzern im Netzwerk sind, desto länger bleiben diese automatisch zwischengespeicherte Informationen.

Deshalb entbehren die oben genannten Lösungen der Überzeugungskraft. Diese Problematik ist bis heute noch umstritten. Meiner Meinung nach gibt es kein festes Kriterium für die Unterscheidung zwischen zwei Zwischenspeicherungen. Angesichts der raschen Entwicklung der Netzwerktechnologie kann ein formales Kriterium die theoretischen Bedürfnisse nicht mehr erfüllen. Es ist praktischer, nach der konkreten Kontrollmöglichkeit der ISP im einzelnen Fall zwischen zwei Zwischenspeicherungen zu differenzieren. Wenn im Hinblick auf alle Voraussetzungen der Service-Provider keine oder wenige Kontrollmöglichkeiten bestehen, fällt die entsprechende Zwischenspeicherung unter die gesetzliche Geltung des § 8 Abs. 2 TMG.

---

[29] Vgl. BT-Drs. 13/7385, S. 20; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 68, Rn. 224; *Malek/Popp*, Strafsachen im Internet, S. 29, Rn. 103; *Spindler/Schmitz/Geis*, TDG-Kommentar, § 9, Rn. 8; *Abel*, Praxiskommentare Telemediengesetz, S. 58; *Pelz*, ZUM Heft 7, 1998, 534.

[30] Vgl. *Sieber*, MMR-Beilage Heft 2, 1999, 24.

II. Allgemeine internetspezifische Verpflichtungen und Privilegien der ISP

A. Allgemeine Verpflichtungen der ISP nach dem TMG

1. Umfang der allgemeinen Verpflichtung

Nach § 7 Abs. 2 Satz 1 TMG sind die ISP *nicht* verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Das heißt, dass die allgemeinen Überwachungs- und Nachforschungspflichten ausgeschlossen werden. Es wird damit eine anlassunabhängige, generelle oder aktive Überwachungspflicht deutlich abgelehnt.[31]

Jedoch wird in § 7 Abs. 2 Satz 2 TMG weiter vorgesehen, dass die Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen auch im Fall der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8–10 unberührt bleiben. Hier ist es wirklich schwierig, die Beziehung zwischen beiden Sätzen zu harmonisieren. Auf der einen Seite werden Überwachungs- und Nachforschungspflichten verneint, aber auf der anderen Seite werden die relativen Entfernungs- oder Sperrungspflichten noch bejaht. Um den Widerspruch zu beseitigen, wird eine einschränkende Auslegung angenommen. Nach dieser Ansicht setzen die Entfernungs- oder Sperrungspflichten nach § 7 Abs. 2 Satz 2 TMG die Kenntnisse der ISP von den Informationen voraus.[32]

Darüber hinaus ist es problematisch, das Verhältnis zwischen den Verpflichtungen nach § 7 Abs. 2 Satz 2 TMG und den Privilegien nach §§ 8–10 TMG zu bestimmen. Denn die ISP können nach §§ 8–10 TMG unter bestimmten Voraussetzungen von der Haftung befreit werden, während die Entfernungs- und Sperrungspflichten nach § 7 Abs. 2 Satz 2 TMG noch unberührt bleiben. Angesichts dieses möglichen Konflikts wird die Auffassung vertreten, dass die Haftungsprivilegierungen der §§ 8–10 TMG auf Unterlassungsansprüche nicht anwendbar seien.[33]

2. TMG und Störerhaftung

Nach den §§ 1004 und 823 BGB kann der Eigentümer von dem Störer die Beseitigung der Beeinträchtigung verlangen und auf Unterlassung klagen, wenn das Eigentum in anderer Weise als durch Entziehung oder Vorenthaltung des Besitzes beeinträchtigt wird. Diese Regelung ist Grundlage der sogenannten Störerhaftung im zivilrechtlichen Bereich.

---

[31] Vgl. Spindler/Schuster-*Hoffmann*, TMG § 7, Rn. 33.

[32] Vgl. Spindler/Schuster-*Hoffmann*, TMG § 7, Rn. 41.

[33] Vgl. Roßnagel-*Jandt*, TMG § 7, Rn. 47.

Die Voraussetzungen für die Störerhaftung sind dabei nicht streng. Jeder kann als Störer betrachtet werden, wenn er „in irgendeiner Weise willentlich und adäquatkausal an der Herbeiführung der rechtswidrigen Beeinträchtigung mitgewirkt hat".[34] Das bedeutet, dass der Umfang der Störerhaftung sehr breit ist. Die ISP, die Durchleitung oder Speicherung von fremden Informationen bieten, könnten grundsätzlich unter die Störerhaftung fallen, sofern sie zu der Beeinträchtigung beitragen. Um die Störerhaftung zu vermeiden, müssen die ISP die von ihnen übermittelten oder gespeicherten Inhalte überwachen, was § 7 Abs. 2 Satz 1 TMG nicht entspricht.[35]

Dieser Widerspruch kann durch eine einschränkende Auslegung des § 7 Abs. 2 Satz 2 TMG aufgehoben werden. Nach einschlägiger Meinung sind die ISP verpflichtet, die Rechtswidrigkeit der Informationen nur zu prüfen, wenn sie Kenntnis von illegalen Inhalten besitzen. Genauer gesagt: In dieser Konstellation haben die ISP die Prüfungs- anstatt die Überwachungspflichten.[36] Es wird in der Literatur ähnlich befürwortet, dass die dem Provider obliegenden Prüfpflichten nach dem Kriterium der Zumutbarkeit eingeschränkt und konkretisiert werden sollten.[37]

3. Anwendbarkeit im Strafrecht?

Wenn § 7 Abs. 2 Satz 2 TMG nur nach seinem Wortlaut interpretiert werden würde, wäre es möglich, dass diese Regelung auch im strafrechtlichen Bereich Anwendung finden könnte. Nach Meinung des Generalbundesanwalts können „die allgemeinen Gesetze" offensichtlich auch das Strafrecht umfassen, deshalb kann § 5 Abs. 4 a.F. TDG (nämlich § 7 Abs. 2 Satz 2 TMG) genutzt werden.[38] Diese Anwendbarkeit des § 7 Abs. 2 Satz 2 TMG im strafrechtlichen Bereich führt dazu, dass ein Access Provider auch für fremde Inhalte verantwortlich sein kann, wenn er Kenntnis von den Informationen und Kontrolle über sie hat.[39]

Jedoch wird diese Meinung mehrheitlich heftig kritisiert. Auf der einen Seite widerspricht sie dem Willen des Gesetzgebers und dem Willen der Regierung. Der Gesetzgeber hat klar dargestellt, dass nur § 5 Abs. 1–3 TDG die strafrechtliche und

---

[34] Vgl. *Spindler/Schmitz/Geis*, TDG-Kommentar, § 8, Rn. 13; Roßnagel-*Jandt*, TMG § 7, Rn. 49; *Hoeren*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 19.

[35] Vgl. *Spindler/Schmitz/Geis*, TDG-Kommentar, § 8, Rn. 18.

[36] Vgl. Spindler/Schuster-*Hoffmann*, TMG § 7, Rn. 41; Gersdorf/Paal-*Paal*, § 7 TMG, Rn. 57; *Spindler/Schmitz/Geis*, TDG-Kommentar, § 8, Rn. 19; *Müller-Broich*, Telemediengesetz, § 7 Rn. 9.

[37] Vgl. Roßnagel-*Jandt*, TMG § 7, Rn. 52; *Hoeren*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 19.

[38] Vgl. Generalbundesanwalt, Haftung eines Access Providers für rechtswidrigen Inhalt, MMR Heft 2, 1998, 95 (Generalbundesanwalt, 26.11.1997 – 2 BJS 104/96-4 – 4, 2 BJS 104/96).

[39] Vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 66, Rn. 217 ff.; *Hilgendorf*, NStZ Heft 10, 2000, 519 ff.

deliktische Verantwortlichkeit der Diensteanbieter regelt.[40] Die Bundesregierung hat auch deutlich gemacht, dass nur verschuldensunabhängige Verpflichtungen zur Sperrung von bestimmten Inhalten von § 5 Abs. 4 TDG (nämlich § 7 Abs. 2 Satz 2 TMG) erfasst werden. Diese Verpflichtungen beziehen sich vor allem auf zivilrechtliche Unterlassungsansprüche und öffentlich-rechtliche Verfügungen anstatt auf strafrechtliche Verantwortlichkeit.[41] Auf der anderen Seite wird in der Literatur die Ansicht vertreten, dass die Zielsetzung und die Systematik der Verantwortlichkeit der ISP bei dieser Argumentation zerstört würden.[42] Daher wird dieser Ansatz als nahezu willkürliche Fehlinterpretation betrachtet.[43] Daraus hat die Mehrheit den Schluss gezogen, dass § 7 Abs. 2 Satz 2 TMG keine Bedeutung für die strafrechtliche Verantwortlichkeit habe.[44]

4. Zwischenergebnis

Als Zwischenergebnis ist damit festzuhalten, dass das für die Verantwortlichkeit der ISP zentrale TMG keine eigenen Haftungsverpflichtungen für die ISP statuiert. Es bezweckt vielmehr eine begrenzte Freistellung der Provider von der Verantwortlichkeit für illegale Inhalte Dritter. Dabei stellt der Gesetzgeber zwar auch fest, dass bestimmte allgemeine Verpflichtungen (insbesondere die Verantwortlichkeit für eigene Inhalte oder die zivilrechtliche Störerhaftung) unberührt bleiben. Solche Begrenzungen der Verantwortlichkeitsfreistellungen sind jedoch keine eigenständigen Verpflichtungen. Das Gleiche gilt auch für die nachfolgend dargestellten Grenzen der im TMG geregelten Privilegien.

B. Allgemeine Privilegierungen der ISP im TMG

1. Verantwortlichkeit von Content Providern

Gemäß § 7 Abs. 1 TMG sind die ISP für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich. Das heißt, für die Content Provider besteht grundsätzlich keine spezifische Privilegierung. Ihre Verantwortlichkeit wird nach den allgemeinen Grundsätzen in spezifischen Rechtsbereichen bestimmt. Heikel ist hierbei allerdings, wie die „eigenen Informationen“ in § 7 Abs. 1 TMG und die „fremden Informationen“ in den §§ 8–10 TMG voneinander zu unterscheiden sind. Unter fremden Informationen werden ausschließlich durch den Nutzer angebotene Informationen verstanden, von denen der

---

[40] Vgl. BR-Drs. 966/96, S. 22–23; BT-Drs. 13/7385, S. 20–21.

[41] Vgl. BR-Drs. 14/1191, S. 10–11.

[42] Vgl. *Sieber*, Verantwortlichkeit im Internet, S. 193, 195, Rn. 390, 392.

[43] Vgl. *Moritz*, MMR Heft 12, 1998, 625.

[44] Vgl. *Sieber*, Verantwortlichkeit im Internet, Rn. 390 ff.; *Kudlich*, JA 2002, 802.

ISP keine Kenntnis hat und über die er auch keine Kontrolle besitzt. In Rechtsprechung und Literatur wurde der Begriff der eigenen Informationen dahingehend erweiternd ausgelegt, dass die zu eigen gemachten Informationen ebenfalls darunter erfasst wurden.[45] Nach dem Willen des Gesetzgebers sind eigene Inhalte auch von Dritten hergestellte Inhalte, die sich der Anbieter zu eigen macht.[46]

Deshalb ist hier nun ein zutreffendes Kriterium für die Unterscheidung der Informationen zu entwickeln. Es gibt viele theoretische Lösungen dafür in der Literatur. Nach einer relativ subjektiven Ansicht liegt das entscheidende Merkmal darin, dass der Anbieter die Inhalte im eigenen Angebotsbereich aufnimmt, ohne sie als von anderen (Dritten) stammend zu kennzeichnen.[47] Nach dieser Meinung ist der Wille des Anbieters der entscheidende Maßstab. Jedoch ist dieses subjektive Kriterium abzulehnen. Die sogenannte Kennzeichnung oder die bloße verbale Distanzierung von Inhalten reichen für eine materiale Unterscheidung zwischen eigenen und fremden Informationen nicht aus.[48] Dies ist lediglich eine Formsache. Der subjektive Zustand ist ohnehin schwer zu beweisen.[49]

Im Gegensatz dazu ist das Kriterium aus dem objektiven Empfängerhorizont eines verständigen Durchschnittsnutzers zu bejahen.[50] Darüber hinaus ist es notwendig, die „zu eigen gemachten Informationen" restriktiv auszulegen. Einerseits müssen die zu eigen gemachten Inhalte mit den selbst hergestellten Inhalten vergleichbar sein, andererseits wird diese Vergleichbarkeit ausgeschlossen, wenn Schwierigkeiten bei der Identifizierung oder der Sperrung der von Dritten erstellten Inhalte existieren.[51] Mit anderen Worten, wenn die Zurechnung der „zu eigen gemachten Informationen" darauf beruht, dass die ISP tatsächlich Kontrollmöglichkeiten über die Informationen besitzen.

2. Privilegien von Access Providern

Die Privilegien von Access Providern werden in § 8 TMG festgelegt. Nach dieser Definition sind die Diensteanbieter, nämlich die Network- und Access Provider, für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie

- die Übermittlung nicht veranlasst,
- den Adressaten der übermittelten Informationen nicht ausgewählt und
- die übermittelten Informationen nicht ausgewählt oder verändert haben.

---

45 Vgl. Spindler/Schuster-*Hoffmann*, TMG § 7, Rn. 15–16.

46 Vgl. BT-Drs. 13/7385, S. 19.

47 Vgl. *Koch*, CR Heft 4, 1997, 197.

48 Vgl. *Malek/Popp*, Strafsachen im Internet, S. 22, Rn. 78.

49 Vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 62–63, Rn. 200.

50 Vgl. Spindler/Schuster-*Hoffmann*, TMG § 7, Rn. 16.

51 Vgl. *Sieber*, Verantwortlichkeit im Internet, Rn. 301.

Diese Regelung gilt jedoch nicht für die ISP, die absichtlich mit einem Nutzer ihres Dienstes zusammenarbeiten, um rechtswidrige Handlungen zu begehen.

a) Grundlage der Privilegierung für Access Provider

In dem nach §§ 7–10 TMG errichteten System der Verantwortlichkeit haben die Access Provider die meisten Privilegien. Nach Meinung des Gesetzgebers liegt diesen Privilegien der technische Charakter der Access Provider zugrunde, denn „die Tätigkeit des Diensteanbieters ist bei der bloßen Durchleitung auf den technischen Vorgang beschränkt ..., ein Kommunikationsnetz zu betreiben und den Zugang zu diesem zu vermitteln".[52]

Dieser Stellungnahme des Gesetzgebers ist zuzustimmen. Auf der einen Seite entspricht sie den technischen Kontrollmöglichkeiten der Access Provider. Zugangssperren im Internet stoßen auf viele grundsätzliche Hindernisse, hierzu zählen die technischen Schwierigkeiten einer Echtzeitkontrolle moderner Massenkommunikationsmittel, die praktischen Probleme von Firewalls, das Schichtenmodell der Computernetze und die Möglichkeit der Verschlüsselung.[53] Die hier aufgeführten technischen Hürden bedeuten, dass die ISP nur sehr begrenzt haften. Auf der anderen Seite entspricht diese Einstellung auch einer rechtspolitisch gerechten Folgerung. Neben der Kontrollmöglichkeit der Access Provider muss die Gefahr beachtet werden, dass massive technische Eingriffe die grundlegenden Rechte der Bürger beeinträchtigen können. Um die Daten von Access Providern umfassend zu kontrollieren, bedarf es einer Gesamtkontrolle und eines Verschlüsselungsverbots, was aber sowohl gegen das Fernmeldegeheimnis verstoßen als auch die rechtsstaatliche Demokratie schädigen würden.[54]

b) Konkrete Bedingungen der Privilegierung der Access Provider

Im Vergleich mit §§ 9–10 TMG stellt die Regelung in § 8 TMG eine Besonderheit dar: Es gibt keine Forderung nach dem subjektiven Zustand der ISP für die Privilegierung und es ist auch keine Pflicht für die ISP vorgesehen, die illegalen Informationen zu entfernen oder den Zugang zu ihnen zu sperren, nachdem sie Kenntnis von illegalen Inhalten erlangt haben. Angesichts dieser Unterschiede wird darüber heftig diskutiert, ob ein Access Provider noch im strafrechtlichen Bereich privilegiert werden kann, wenn er eine bestimmte Adresse trotz der Kenntnis von illegalen oder strafbaren Informationen nicht sperrt.

---

[52] Vgl. BT-Drs. 14/6098, S. 24. Siehe dazu auch *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 61, Rn. 194; *Malek/Popp*, Strafsachen im Internet, S. 24, Rn. 87.

[53] Vgl. *Sieber*, CR Heft 11, 1997, 659 ff.

[54] Vgl. *Sieber*, ZUM Heft 3, 1999, 197.

Nach der herrschenden Ansicht können die Network- und Access Provider nach § 8 Abs. 1 TMG privilegiert werden, auch wenn sie schon die Rechtswidrigkeit der übermittelten Inhalte gekannt haben.[55] Der Autor betont, dass die strafrechtliche Verantwortlichkeit der Access Provider nur bei einer „objektiven Gefahrsteigerung" bestehen könne.[56] Dieser Standpunkt könnte auch vom Gesetzgeber zu bestimmen sein. Nach Ansicht des Gesetzgebers handelt es sich bei der Tätigkeit eines Access Providers normalerweise um einen automatisiert ablaufenden Prozess, deshalb „stellt die Haftungsregelung auch nicht darauf ab, dass der Diensteanbieter keine Kenntnis von der Information hat".[57]

Jedoch gibt es auch gegenteilige Stimmen, die mit der Anwendung des § 7 Abs. 2 Satz 2 TMG argumentieren. Die Regelung des § 7 lautet: Verpflichtungen zur Entfernung oder Sperrung der Nutzer von Informationen nach den allgemeinen Gesetzen bleiben im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10 unberührt. Nach dieser Meinung soll der Access Provider nach Sinn und Zweck des TMG nicht privilegiert werden, wenn er Kenntnis von illegalen Inhalten und die Kontrolle über diese Informationen besitzt. Denn in dieser Situation besteht ausnahmsweise die Sperrverpflichtung für Access Provider nach § 7 Abs. 2 Satz 2 TMG.[58]

Doch dieses Argument stößt auf starke Kritik. Zum einen widerspricht es der Begründung der ECRL.[59] Es wird die Meinung vertreten, dass die ECRL nur eine Ausnahme in Art. 12 Abs. 3 anerkennt, in dem der Access Provider von Gericht oder Verwaltungsbehörde aufgefordert werden kann, eine Rechtsverletzung zu verhindern oder zu verhüten. Diese Ausnahme darf nicht im Strafrecht aufgenommen werden.[60] Zum anderen hängt die Verantwortlichkeit der Access Provider nach der Erläuterung des Gesetzgebers des TDG auch nicht mit der Kenntnis zusammen.[61] Darüber hinaus wird die Ansicht vertreten, dass eine Sperrverpflichtung der Access Provider gegen die Systematik der Verantwortlichkeit nach §§ 7–10 TMG spricht.[62]

Die zweite Meinung scheint auf den ersten Blick plausibel. Der Kontrollmöglichkeit der ISP liegt die Privilegierung der §§ 8–10 TMG zugrunde. Deshalb soll

---

[55] Vgl. *Hörnle*, NJW Heft 14, 2002, 1011; Schönke/Schröder-*Eisele*, § 184, Rn. 89; *Malek/Popp*, Strafsachen im Internet, S. 28, Rn. 102; *Fischer*, Strafgesetzbuch Kommentar, § 184, Rn. 29.

[56] Vgl. *Malek/Popp*, ebenda, S. 28, Rn. 102.

[57] Vgl. BT-Drs. 14/6098, S. 24.

[58] Vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 66, Rn. 217 ff; *Hilgendorf*, NStZ Heft 10, 2000, 519; *Graf*, DRiZ Heft 7, 1999, 286.

[59] Vgl. *Gercke/Brunst*, Praxishandbuch Internetstrafrecht, S. 255, Rn. 616.

[60] Vgl. *Kudlich*, JA 2002, 802.

[61] Vgl. BT-Drs. 14/6098, S. 24; *Gercke/Brunst*, Praxishandbuch Internetstrafrecht, S. 255, Rn. 616.

[62] Vgl. *Moritz*, MMR Heft 12, 1998, 625; *Gercke/Brunst*, Praxishandbuch Internetstrafrecht, S. 255, Rn. 616; *Sieber*, Verantwortlichkeit im Internet, S. 193, Rn. 390.

ein ISP nicht nach dem TMG privilegiert werden, wenn er nicht nur Kenntnis von den rechtswidrigen Informationen, sondern auch Kontrollmöglichkeiten hat. Außerdem wird diese Auffassung in einem gewissen Maß von der weiteren Formulierung des Gesetzgebers unterstützt. Denn es wird gefordert, dass die privilegierte Tätigkeit des Access Providers rein technischer, automatischer und passiver Art sein soll.[63] Jedoch ist diese Stellungnahme bei näherer Betrachtung abzulehnen.

So ist es fraglich, ob ein Access Provider mit Kenntnis der illegalen Inhalte tatsächlich Kontrollmöglichkeiten besitzt. Die Antwort darauf lautet Nein – weil die illegalen Inhalte nicht im Server der Access Provider gespeichert werden, sodass er die Inhalte nicht direkt kontrollieren kann. In dieser Situation ist der Access Provider nur in der Lage, den Zugang zu ihnen zu kontrollieren, was für eine Garantenstellung nicht ausreicht.[64]

Auf der anderen Seite wird die vom Gesetzgeber bewusst begründete Systematik der Verantwortlichkeit der ISP nach dieser Meinung beeinträchtigt. Obwohl der Verfasser der zweiten Meinung die Verantwortlichkeit des Access Providers in dieser Konstellation als „Ausnahme“ bezeichnet, bietet er tatsächlich kein durchführbares Kriterium dafür.

c) Reichweite der Vorschrift

aa) Gesetzliche Anwendungsfälle

Nach § 8 Abs. 1 TMG werden zwei technische Vorgänge erfasst, nämlich die Übermittlung fremder Informationen und die Vermittlung des Zugangs zur Nutzung fremder Informationen. Außerdem wird die automatische, kurzzeitige Zwischenspeicherung fremder Informationen nach § 8 Abs. 2 TMG als Übermittlung dieser Informationen eingeschlossen, sofern dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist.

Es ist auffällig, dass ein WLAN-Anbieter durch das „zweite Gesetz zur Änderung des Telemediengesetzes“ auch als Access Provider betrachtet wird. Nach dieser neuen Regelung gelten § 8 Abs. 1 und 2 auch für Diensteanbieter, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen.

Die gesetzliche Veränderung hat mit der Störerhaftung zu tun. Nach §§ 1004 und 823 BGB könnten ISP in der Regel einer Störerhaftung unterliegen, wenn sie zu einer rechtswidrigen Beeinträchtigung beigetragen haben. Diese gesetzliche Gefahr gilt auch für den WLAN-Anbieter. Wenn ein Betreiber eines Cafés oder eines Re-

---

[63] Vgl. ABl. EG 2000 L 178, 17.7.2000, S. 1(6); *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 67, Rn. 221 ff.

[64] Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 45.

staurants offenen WLAN-Service anbietet und jemand diesen Service missbraucht, dürfte der WLAN-Anbieter eine Störerhaftung tragen. Der BGH hat in einem Urteil aus dem Jahr 2010 beschieden, dass der Inhaber eines WLAN-Anschlusses als Störer auf Unterlassung haftet, wenn er es unterlässt, die marktüblichen Sicherungen ihrem Zweck entsprechend anzuwenden, während der Dritte diesen Anschluss missbraucht.[65] Wegen dieser Rechtsunsicherheit bieten nur wenige Betreiber von Cafés oder Restaurants usw. offenen WLAN-Service (Hotspots) an, während ein solcher Service in anderen Ländern üblich ist.[66] Angesichts dieser Situation wird vorgeschlagen, WLAN-Betreibern die nötige Rechtssicherheit in Haftungsfragen zu verschaffen, um auf diesem Weg eine größere WLAN-Abdeckung in Deutschland zu erreichen.[67]

Jedoch bleibt das zentrale Problem immer noch ungelöst, obwohl das neue Gesetz zur Änderung des Telemediengesetzes am 02.06.2016 vom Bundestag verabschiedet worden ist. Die Frage, ob die Haftungsprivilegierung des § 8 Abs. 1 auch die Unterlassungsansprüche und die Störerhaftung umfasst, ist weiterhin problematisch.[68] Zwar hat der Gesetzgeber klargestellt, dass die Haftungsprivilegierung des Diensteanbieters nach § 8 Abs. 1 und 2 auch die verschuldensunabhängige Haftung im Zivilrecht nach der sogenannten Störerhaftung uneingeschränkt umfasst,[69] es ist aber nicht sicher, ob die frühere Rechtsprechung, die nach § 8 TMG auf Unterlassungsansprüche und Störerhaftung keine Anwendung findet, tatsächlich ungültig ist.[70] Außerdem ist es unbestimmt, ob diese Regelung mit dem europäischen Recht vereinbar ist.[71]

bb) Gesetzlich nicht geregelte Anwendungsfälle

Neben den bereits genannten gesetzlichen Diensteanbietern kann § 8 TMG für die anderen gesetzlich nicht geregelten ISP Anwendung finden. Die gesetzlich nicht geregelten ISP umfassen den Betreiber eines Peer-to-Peer-Systems, den Hyperlinksetzer, den Suchmaschinenbetreiber, den Anbieter eines E-Mail-Dienstes usw. Obwohl diese Services keine typische Durchleitung von Informationen darstellen, kann § 8 TMG begrenzte und analoge Anwendung in bestimmten Konstellationen finden, wie nachfolgend weiter erläutert wird.

---

[65] Vgl. BGH: Haftung des Internetanschlussinhabers mit WLAN – Sommer unseres Lebens, MMR 2010, S. 565 (BGH, Urteil vom 12.05.2010 – I ZR 121/08); *Sesing*, MMR-Aktuell 2016, 378738.

[66] Vgl. Gersdorf/Paal-*Paal*, § 8 TMG, Rn. 43.

[67] Vgl. BT-Drs. 18/8645, S. 7.

[68] Vgl. Gersdorf/Paal-*Paal*, § 8 TMG, Rn. 44.

[69] Vgl. BT-Drs. 18/8645, S. 10.

[70] Vgl. Gersdorf/Paal-*Paal*, § 8 TMG, Rn. 45.

[71] Vgl. ebenda, § 8 TMG, Rn. 45; *Spindler*, CR Heft 1, 2016, 50 ff.

3. Privilegien von Caching Providern

Die Privilegien von Caching Providern werden in § 9 TMG vorgesehen. Danach sind die Diensteanbieter für eine automatische, zeitlich begrenzte Zwischenspeicherung, die allein dem Zweck dient, die Übermittlung fremder Informationen an andere Nutzer auf deren Anfrage hin effizienter zu gestalten, nicht verantwortlich, sofern sie

- die Informationen nicht verändern,
- die Bedingungen für den Zugang zu den Informationen beachten,
- die Regeln für die Aktualisierung der Informationen, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, beachten,
- die erlaubte Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Informationen, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigen und
- unverzüglich handeln, um im Sinne dieser Vorschrift gespeicherte Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald sie Kenntnis davon erhalten haben, dass die Informationen am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt wurden oder der Zugang zu ihnen gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat.

Aber diese Regelung findet keine Anwendung, wenn ISP absichtlich mit einem Nutzer ihres Dienstes zusammenarbeiten, um rechtswidrige Handlungen zu begehen.

a) Grundlage der Privilegierung für Caching Provider

Aus technischer Sicht ist das Caching von der reinen Durchleitung abzugrenzen. Das Caching (Zwischenspeicherung) erfolgt, um Nutzern schnelleren Zugang zu den Informationen zu verschaffen. Es beschränkt sich jedoch lediglich auf den technischen Vorgang, ein Kommunikationsnetz zu betreiben und den Zugang zu diesem zu vermitteln sowie die Übermittlung effizienter zu gestalten.[72]

Die Grundlage der Privilegierung für Caching Provider liegt darin, dass sie auch nur sehr beschränkte Eingriffsoptionen in die Inhalte der zwischengespeicherten Informationen haben. Die Speicherung der Informationen erfolgt automatisch, während die Informationen kurze Zeit gespeichert und danach automatisch gelöscht werden. Mit anderen Worten: Die Caching Provider kümmern sich ausschließlich um die Beschleunigung der Übermittlung von Informationen, nicht um deren Inhalte.

---

[72] Vgl. BT-Drs. 14/6098, S. 24.

b) Konkrete Bedingungen der Privilegierung der Caching Provider

Erstens ist die Privilegierung unabhängig von der Kenntnis der Caching Provider. Obwohl sie in der Regel keine Kenntnis von den gespeicherten Informationen haben, wäre allerdings zu überlegen, ob dies die Basis für die Privilegierung der Caching Provider ist. Nach dem Willen des Gesetzgebers setzt die Haftungsprivilegierung dies nicht voraus, weil bei der automatischen Zwischenspeicherung weder die Caching Provider noch die Access Provider eine eigene Entscheidung treffen.[73] Darüber hinaus wird diese Voraussetzung nach dem Wortlaut des § 9 TMG auch nicht verlangt.[74]

Zweitens dürfen die Caching Provider die Informationen nicht verändern, eine Voraussetzung, die auf die Erhaltung der Integrität der übermittelten Informationen abzielt. Durch diese Bedingung wird gewährleistet, dass die Kopie in jedem Moment dem Original entspricht. Aber die technisch bedingten Veränderungen der Informationen beeinflussen die Haftungsprivilegierung nicht.[75]

Drittens müssen die Caching Provider die Bedingungen für den Zugang zu den Informationen beachten. Es gibt viele Gründe für Zugangskontrollen, etwa Jugendschutz oder Bezahlung von Nutzungsentgelten. Deshalb müssen die Caching Provider garantieren, dass die Zugangsbeschränkungen auch bei ihren Servern eingehalten werden.[76]

Viertens sollen die Caching Provider die Regeln für die Aktualisierung der Informationen, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, beachten. Ähnlich wie die Bedingung in § 9 Abs. 1 Satz 1 TMG richtet sich diese Voraussetzung auf die Identität von Kopie und Original. Mit dieser Bedingung für die Aktualisierung der Informationen kann rechtzeitig erfahren werden, ob die Cache-Kopie dem Original entspricht.[77] Leider bleibt der detaillierte Inhalt der Formulierung „in weithin anerkannten und verwendeten Industriestandards" unklar.[78]

Fünftens dürfen die Caching Provider die erlaubten Anwendungsmöglichkeiten der Technologie, um Daten über die Nutzung der Informationen zu sammeln, die in weithin anerkannten und verwendeten Industriestandards bestimmt sind, nicht beeinträchtigen. Diese Bedingung richtet sich darauf, Zugriffszahlen durch Cache-Kopien zu ermitteln. Aus wirtschaftlichen Gründen werden die Daten des Nutzerverhaltens gespeichert und die Anzahl der Abrufe registriert, damit beispielsweise

---

[73] Vgl. ebenda, S. 24.

[74] Vgl. *Spindler/Schmitz/Geis*, TDG-Kommentar, § 10, Rn. 8.

[75] Vgl. Gersdorf/Paal-*Ott*, TMG § 9, Rn. 14; BT-Drs. 14/6098, S. 25; ebenda, § 10, Rn. 10.

[76] Vgl. BT-Drs. 14/6098, S. 25; *Spindler/Schmitz/Geis*, ebenda, § 10, Rn. 11.

[77] Vgl. BT-Drs. 14/6098, S. 25; *Spindler/Schmitz/Geis*, ebenda, § 10, Rn. 13.

[78] Vgl. Spindler/Schuster-*Hoffmann*, TMG § 9, Rn. 23.

die Höhe von Werbeeinnahmen errechnet werden kann. Deshalb darf die Zwischenspeicherung diese Zählstatistik nicht verändern.[79]

Schließlich sollen die Caching Provider unverzüglich handeln, um die Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald sie Kenntnis davon erhalten haben, dass die Informationen am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt wurden oder der Zugang zu ihnen gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat. Der Grund für diese Bedingung liegt darin, dass manchmal die illegalen Informationen wegen Datenspiegelungen noch abgerufen werden können, obwohl sie beim Ursprungsserver schon gelöscht worden sind.[80] Wenn die Entfernung oder Sperrung aber technisch unmöglich oder unzumutbar wäre, könnte die Kenntniserlangung noch nicht zum Entfall der Haftungsprivilegierung führen.[81]

4. Privilegien von Hosting Providern

Die Privilegien von Hosting Providern werden in § 10 TMG bestimmt. Danach sind die Diensteanbieter für fremde Informationen, die sie für einen Nutzer speichern, nicht verantwortlich, sofern

- sie keine Kenntnis von den rechtswidrigen Handlungen oder der Information haben und ihnen im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, oder
- sie unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie von ihr Kenntnis erlangt haben.

Aber diese Regelung findet keine Anwendung, wenn der Nutzer dem ISP untersteht oder von ihm beaufsichtigt wird.

a) Grundlagen der Privilegierung für Hosting Provider

Die Grundlage der Privilegierung für Hosting Provider liegt darin, dass „die Tätigkeit des ISP auf den technischen Vorgang der Speicherung von Informationen beschränkt ist und auch dem bloßen Vermittlungsvorgang zuzurechnen ist“.[82] Das bedeutet, dass die technische Kontrollmöglichkeit der Hosting Provider noch der Privilegierung für das Hosting zugrunde liegt.

---

[79] Vgl. BT-Drs. 14/6098, S. 25; Spindler/Schuster-*Hoffmann*, TMG § 9, Rn. 29.

[80] Vgl. Spindler/Schuster-*Hoffmann*, TMG § 9, Rn. 33.

[81] Vgl. BT-Drs. 14/6098, S. 25.

[82] Vgl. ebenda, S. 25.

Für die Hosting Provider ist es zum einen nicht einfach, die unbekannten Inhalte auf ihren Servern ausfindig zu machen. Nicht nur die Verschlüsselung von Daten, sondern auch die rasche Veränderung der gespeicherten Daten können die Auffindung der unbestimmten Inhalte verhindern. Zum anderen sind die Hosting Provider in der Lage, die problematischen Inhalte zu sperren oder zu löschen, wenn sie schon Kenntnis von den Inhalten besessen haben.[83]

Deshalb soll die technische Kontrollmöglichkeit immer als ein maßgebendes Kriterium für die Bestimmung der Privilegierung der ISP betrachtet werden. Nach diesem Unterscheidungsmerkmal können die Hosting Provider mit Kenntnis von der rechtswidrigen Handlung oder der Information noch privilegiert werden, wenn die Entfernung oder Sperrung technisch ihnen unmöglich und unzumutbar ist.[84]

b) Konkrete Bedingungen der Privilegierung der Hosting Provider

aa) Vorsatz

Nach § 10 Abs. 1 Nr. 1 TMG tragen die Hosting Provider keine Haftung, sofern sie keine „Kenntnis" von der rechtswidrigen Handlung oder der Information haben. Jedoch gibt es viele Möglichkeiten, die „Kenntnis" unterschiedlich auszulegen. Zuerst ist zu bestimmen, ob die fahrlässige Nichtkenntnis der Inhalte in Betracht kommen kann. Dies kann verneint werden. Aus dem Wortlaut des § 10 Abs. 1 Nr. 1 TMG kann man zum einen nicht den logischen Schluss ziehen, dass den Hosting Providern die Privilegierung wegen der fahrlässigen Nichtkenntnis entzogen werden müsste. Zum anderen haben die Hosting Provider keine Verpflichtung, die von ihnen gespeicherten Informationen zu überwachen.[85] Somit besteht keine Grundlage für eine die Privilegierung einschränkende fahrlässige Nichtkenntnis, also ist eine positive Kenntnis erforderlich. Außerdem wurde die Möglichkeit einer fahrlässigen Nichtkenntnis von der Bundesregierung deutlich abgelehnt. Ihrer Meinung nach setzt die Verantwortlichkeit der Hosting Provider vorsätzliches Handeln voraus.[86]

---

[83] Vgl. *Sieber*, CR Heft 11, 1997, 654 ff.; *ders.*, Verantwortlichkeit im Internet, S. 159–160, Rn. 322.

[84] Vgl. BT-Drs. 14/6098, S. 25; *Vassilaki*, MMR Heft 12, 1998, 634.

[85] Vgl. *Spindler/Schmitz/Geis*, TDG-Kommentar, § 11, Rn. 11; *Spindler*, NJW Heft 48, 1997, 3196; *Malek/Popp*, Strafsachen im Internet, S. 25, Rn. 88; *Marberth-Kubicki*, Computer- und Internetstrafrecht, S. 183, Rn. 374; *Stadler*, Haftung für Informationen im Internet, S. 139–141, Rn. 105; *Bleisteiner*, Rechtliche Verantwortlichkeit im Internet, S. 178; *Pelz*, ZUM Heft 7, 1998, 534; *Engel-Flechsig/Maennel/Tettenborn*, NJW Heft 45, 1997, 2985; *Freytag*, CR Heft 9, 2000, 608.

[86] Vgl. BT-Drs. 13/8153, S. 9.

Weiter ist zu fragen, ob ein bedingter Vorsatz (*dolus eventualis*) für die Voraussetzung der „Kenntnis" ausreicht, da § 10 Abs. 1 Nr. 1 TMG das Willenselement der *mens rea* nicht erwähnt hat.[87]

Nach der Darstellung des Bundestags „setzt die Rechtsordnung im Strafrecht und Ordnungswidrigkeitenrecht für alle Äußerungsdelikte und sonstigen im Bereich der Teledienste durch bestimmte Inhalte begehbare Straftatbestände Vorsatz, also unbedingte oder bedingte Kenntnis der objektiven Tatbestandsverwirklichung voraus".[88] In der Begründung zum Staatsvertrag über Mediendienste wird auch erwähnt, dass „der Begriff sowohl den unbedingten als auch den bedingten Vorsatz umfasst".[89] Deshalb wird in der Literatur die Auffassung vertreten, dass diese Regelung keine weitergehende Einschränkung auf *dolus directus* wolle, weil die Verwendung der „Kenntnis" lediglich der Abgrenzung zur Fahrlässigkeit diene.[90] Eine solche Position ist denkbar, wenn § 10 TMG nur nach dem Wortlaut der „Kenntnis" ausgelegt würde. Jedoch wird diese Meinung in der Literatur kritisiert. Im Schrifttum wird mehrheitlich betont, dass ein bedingter Vorsatz (*dolus eventualis*) für die Verantwortlichkeit der Hosting Provider nicht ausreichend sei.[91]

Vor allem kann die hier skizzierte Sichtweise nicht durch die Auslegung des Wortlauts unterstützt werden, Begriffe wie Vorsatz oder Fahrlässigkeit werden in § 10 TMG gar nicht verwendet. Bei der „Kenntnis" handelt es sich nur um das positive Wissen oder das kognitive Element des Vorsatzes anstelle eines voluntativen Elements.[92] Das bedeutet, dass die „Kenntnis" teleologisch interpretiert werden muss, wenn wir ihre Bedeutung bestimmen möchten. Deshalb ist diese These abzulehnen, weil sie der gesamten Zielsetzung des Gesetzgebers nicht entspricht. Denn der Gesetzgeber will die aktiven Kontrollpflichten der ISP durch die Verantwortlichkeitsregelungen ausschließen, sodass der bedingte Vorsatz (*dolus eventualis*) hier entfällt.[93] Aus dem Wortlaut der „Kenntnis" allein kann keine Schlussfolgerung abgeleitet werden. Außerdem ist diese Überlegung aus der Sicht der Kontrollmöglichkeiten zu kritisieren. Da die gespeicherten Daten wegen der Einschränkung der technischen Gegebenheiten nicht völlig erkannt werden, soll die Rechtssicherheit durch das Erfordernis der positiven und genauen Kenntnis ge-

---

[87] Vgl. *Bleisteiner*, Rechtliche Verantwortlichkeit im Internet, S. 179; *Pelz*, ZUM Heft 7, 1998, 534; *Moritz*, CR Heft 8, 1998, 507.

[88] Vgl. BT-Drs. 13/7385, S. 20. Ähnlich auch vgl. BT-Drs. 13/8153, S. 9.

[89] Vgl. Bayer. LT-Drs. 13/7716, S. 10.

[90] Vgl. *Pätzel/Gravenreuth*, CR Heft 10, 1998, 626.

[91] Vgl. *Malek/Popp*, Strafsachen im Internet, S. 25, Rn. 88; *Bleisteiner*, Rechtliche Verantwortlichkeit im Internet, S. 180; *Sieber*, Verantwortlichkeit im Internet, S. 166–167, Rn. 336; *Moritz*, CR Heft 8, 1998, 507; *Spindler*, NJW Heft 48, 1997, 3196; *Vassilaki*, MMR Heft 12, 1998, 634; Gersdorf/Paal-*Paal*, TMG § 10, Rn. 24; *Müller-Broich*, Telemediengesetz, § 10 Rn. 4.

[92] *Spindler*, NJW Heft 48, 1997, 3196.

[93] Vgl. *Sieber*, Verantwortlichkeit im Internet, S. 166–167, Rn. 336.

schaffen werden.[94] Das heißt, wenn die Hosting Provider nur mit bedingtem Vorsatz (*dolus eventualis*) Kenntnis von den Inhalten besitzen, sind sie überfordert, die Informationen zu entfernen oder den Zugang zu ihnen zu sperren.

Darüber hinaus wird darauf hingewiesen, dass ein direkter Vorsatz (*dolus directus*) regelmäßig bereits vorliege, wenn der Hosting Provider positive Kenntnis von rechtswidrigen Inhalten habe und sie dennoch weiter auf seinem Server bereithalte.[95]

Meines Erachtens bezieht sich die „Kenntnis" nur auf das Erfordernis des kognitiven Elements der Hosting Provider, denn das voluntative Element richtet sich hauptsächlich auf die Täterhandlung oder deren Erfolg, während die Forderung nach der Täterhandlung in § 10 Abs. 1 Nr. 2 TMG aufgenommen ist. Hier ist jedoch ein direkter Vorsatz (*dolus directus*) erforderlich, weil das kognitive Element des direkten Vorsatzes konkreter und genauer als das des bedingten Vorsatzes ist. Mit anderen Worten: Wir brauchen eine konkrete und genaue Kenntnis – die mit einem direkten Vorsatz verbunden ist – von den rechtswidrigen Inhalten,[96] während die voluntative Einstellung der Hosting Provider zu den Inhalten für die Auslegung des § 10 Abs. 1 Nr. 1 TMG unbedeutend ist.

Eben diese Forderung nach konkreter und genauer Kenntnis ist für die strafrechtliche Verantwortlichkeit der ISP besonders von Bedeutung. Beispielsweise ist es nach der Entscheidung des AG München im *CompuServe*-Fall für die Kenntnis erforderlich, dass dem Angeklagten die jeweiligen Beiträge der strafbaren Inhalte im Einzelnen bekannt sind.[97] Gegen die Auslegung des AG München spricht, dass diese nicht nur dem Willen des Gesetzgebers zuwiderläuft, sondern auch den ISP zu viele Pflichten aufbürdet.[98]

bb) Gegenstand der Kenntnis

Die Formulierung – „Kenntnis von der rechtswidrigen Handlung oder der Information" – in § 10 Abs. 1 Nr. 1 TMG (auch § 14 Abs. 1 Nr. a ECRL) ist zweideutig. Nach diesem Wortlaut sind zwei Fallgruppen beim Gegenstand der Kenntnis zu unterscheiden. Zum einen die Fälle, in denen die Information *per se* bereits zu beanstanden ist; zum anderen diejenigen, in denen zwar die Information selbst nicht

---

[94] Vgl. *Pelz*, ZUM Heft 7, 1998, 534; *Sieber*, CR Heft 11, 1997, 654 ff.

[95] Vgl. *Bleisteiner*, Rechtliche Verantwortlichkeit im Internet, S. 180.

[96] Vgl. *Sieber*, Verantwortlichkeit im Internet, S. 167–168, Rn. 338; *Malek/Popp*, Strafsachen im Internet, S. 25, Rn. 88. Nach der Formulierung ist es für die Verantwortlichkeit der Host-Provider erforderlich, dass ihnen der einzelne, konkrete Inhalt bekannt ist. Vgl. BT-Drs. 13/7385, S. 20.

[97] Vgl. AG München, Verbreitung pornografischer Schriften durch Internet-Provider, CR Heft 8, 1998, 504 (AG München, Urteil vom 28.05.1998 – 8340 Ds 465 Js 173158/ 95).

[98] Vgl. *Sieber*, Verantwortlichkeit im Internet, Rn. 339–340; *ders.,* AG München: *CompuServe*-Urteil, MMR Heft 8, 1998, 441 (AG München, Urteil vom 28.05.1998 – 8340 Ds 465 Js 173158/95).

zu beanstanden ist, wohl aber die Verwendung von Informationen ohne Erlaubnis des Rechteinhabers.[99]

Da die „Rechtswidrigkeit" in § 10 Abs. 1 Nr. 1 TMG sich nur auf die „Handlung" und nicht auf die „Information" bezieht, sind die Forderungen der Kenntnis auch unterschiedlich. Auf der einen Seite muss die Rechtswidrigkeit der Handlung, die nicht von dem Rechteinhaber erlaubt wird, der Gegenstand der Kenntnis sein. Auf der anderen Seite ist die Rechtswidrigkeit der Inhalte von der Kenntnis einzuschließen. Nach diesem Verständnis bleibt die Verantwortlichkeit für die Hosting Provider unberührt, obwohl die Hosting Provider im Irrtum über die Rechtswidrigkeit der Inhalte sind.[100]

In der Literatur dagegen wird beteuert, die „Kenntnis" der Rechtswidrigkeit müsse sich nicht nur auf die Handlung, sondern auch auf die Information beziehen.[101] Auffällig oft findet sich diese Beschreibung sowohl in der französischen als auch in der spanischen Fassung der ECRL.[102] Denn der Wortlaut der Regelung in Art. 14 Abs. 1(a) ECRL – „knowledge of illegal activity or information" – ist doppeldeutig: Es könnte als „knowledge of illegal activity or knowledge of information" oder als „knowledge of illegal activity or knowledge of illegal information" ausgelegt werden. Gemeinhin wird in der Literatur die Auffassung vertreten, dass die erste Interpretation falsch sei.[103] Diese Auffassung geht davon aus, dass die oben genannte Unterscheidung zwischen der zu beanstandenden und der nicht zu beanstandenden Information problematisch sei, was zu Unsicherheiten führe.[104] Außerdem können die Hosting Provider nach diesem Verständnis von Kontrollpflichten der Rechtswidrigkeit der Information befreit werden.[105] Letztlich wird auch argumentiert, dass die Kenntnis der Rechtswidrigkeit der Information der Forderung des „Verbotsirrtum"-Grundsatzes entspräche.[106]

Die Rechtswidrigkeit der Information sollte meines Erachtens durch die „Kenntnis" der Hosting Provider abgedeckt werden. Auf der einen Seite ist „Information" in § 10 Abs. 1 Nr. 1 TMG kein wertneutraler Begriff. Es ist schon vom

---

[99] Vgl. BT-Drs. 14/6098, S. 25; *Stadler*, Haftung für Informationen im Internet, S. 136, Rn. 100.

[100] Vgl. *Sieber*, Verantwortlichkeit im Internet, S. 169–170, Rn. 341; *Stadler*, ebenda, S. 136 ff., Rn. 101 ff.

[101] Vgl. *Spindler*, NJW Heft 13, 2002, 924; *Hoffmann*, MMR Heft 5, 2002, 288; *Müller-Broich*, Telemediengesetz, § 10, Rn. 4.

[102] Vgl. *Spindler*, NJW Heft 13, 2002, 924; *Spindler/Schmitz/Geis*, TDG-Kommentar, 2004, § 11, Rn. 19; *Stadler*, Haftung für Informationen im Internet, S. 108, Rn. 103.

[103] Vgl. Gersdorf/Paal-*Paal*, TMG § 10, Rn. 30; Spindler/Schuster-*Hoffmann*, TMG § 10, Rn. 25.

[104] Vgl. *Eck/Ruess*, MMR Heft 6, 2003, 365.

[105] Vgl. ebenda, 365; *Spindler/Schmitz/Geis*, TDG-Kommentar, 2004, § 11, Rn. 20.

[106] Vgl. *Spindler/Schmitz/Geis*, ebenda, § 11, Rn. 20; Gersdorf/Paal-*Paal*, TMG § 10, Rn. 28.

Gesetzgeber deutlich gemacht worden, dass dieser Begriff sich nur auf die Information als solche bezieht, die zu beanstanden ist.[107] Nur wenn die Hosting Provider ganz sicher wissen, dass die Information zu beanstanden ist, könnten sie verpflichtet werden, sie zu entfernen oder den Zugang zu ihr zu sperren. Die negative Wertung, dass die Information zu beanstanden ist, stellt eine Parallele zur „Rechtswidrigkeit" dar. Mit diesem Verständnis kann der Schluss abgeleitet werden, dass die Rechtswidrigkeit der Information auch der Gegenstand der Kenntnis sein soll.

Auf der anderen Seite ist es häufig schwierig für die ISP, die Rechtsnatur der Information im Netzwerk zu bestimmen. Wegen der großen Datenmengen und der raschen Veränderung des Zustands der Speicherung[108] scheint diese Natur oft sehr vage zu sein. Deshalb geschehen nicht selten Irrtümer über die Rechtsnatur. Wenn die Hosting Provider Verantwortlichkeit für die gespeicherten fremden Informationen tragen müssen, obwohl sie die Rechtsnatur der Informationen missverstehen, könnte der Gesetzgeber sein Ziel, das sich auf die Sicherstellung des freien Dienstleistungsverkehrs[109] und auf die Gestaltung der sich dynamisch entwickelnden Angebote im Bereich der Informations- und Kommunikationsdienste[110] richtet, verfehlt haben.

Neben den oben genannten zwei Fallgruppen gibt es einen speziellen Bezugspunkt der Kenntnis für die Schadensersatzansprüche, nämlich die Tatsachen oder Umstände, aus denen die rechtswidrige Handlung oder Information offensichtlich wird. Es ist evident, dass diese Regelung nicht für die strafrechtliche Verantwortlichkeit, sondern nur für die zivilrechtliche Verantwortlichkeit der Hosting Provider gilt.[111]

Eine Minderheit hält daher für den Wegfall der Privilegierung bezüglich der Schadensersatzansprüche einen Vorsatz für erforderlich.[112] Für die herrschende Meinung ist aber eine bewusste, grobe Fahrlässigkeit für diese Verantwortlichkeit der Hosting Provider ausreichend.[113] Außerdem ist es unerlässlich, dass die Hinweise bezüglich der „Tatsachen oder Umstände" so konkret und präzise sein müssen, dass die Identifizierung der rechtswidrigen Information einfach ist.[114] Ein allgemeiner Hinweis reicht für den Wegfall der Privilegierung der Hosting Provider nicht aus.

---

[107] Vgl. BT-Drs. 14/6098, S. 25.

[108] Vgl. *Sieber*, CR Heft 11, 1997, S. 654 ff.

[109] Vgl. BT-Drs. 14/6098, S. 1.

[110] Vgl. BT-Drs. 13/7385, S. 1.

[111] Vgl. BT-Drs. 14/6098, S. 25.

[112] Vgl. Spindler/Schuster-*Hoffmann*, TMG § 10, Rn. 34.

[113] Vgl. *Stadler*, Haftung für Informationen im Internet, S. 139 ff, Rn. 104 ff.; *Spindler/Schmitz/Geis*, TDG-Kommentar, § 11, Rn. 23; *Hoffmann*, MMR 2002, 288; *Freytag*, CR Heft 9, 2000, 608; *Spindler*, NJW 2002, 924.

[114] Vgl. *Spindler/Schmitz/Geis*, ebenda, § 11, Rn. 22; *Stadler*, ebenda, S. 139–141, Rn. 105.

Dies würde auch dem Verbot für die Verpflichtung der allgemeinen Überwachung und Forschung zuwiderlaufen.[115]

cc) Art der Kenntniserlangung von Informationen

Laut herrschender Meinung ist die Art und Weise der Kenntniserlangung der Informationen nicht von Bedeutung.[116] Das heißt, die Art und Weise, wie die Hosting Provider Kenntnis von der rechtswidrigen Handlung oder den rechtswidrigen Informationen bekommen und wie sie im Fall von Schadensersatzansprüchen die Tatsachen oder Umstände kennen, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, ist in der Regel nicht festgelegt.

dd) Unverzügliche Tätigkeit nach Kenntniserlangung

Auch wenn die Hosting Provider Kenntnis von der rechtswidrigen Handlung oder den rechtswidrigen Informationen haben, können sie noch privilegiert werden, sofern sie nach Erlangung der Kenntnis die Informationen sofort löschen oder den Zugang zu ihnen umgehend sperren. Diese Regelung stammt aus dem *notice and take down*-Verfahren im DMCA. Aber in der Literatur gibt es auch die These, dass diese Regelung sich vom tatsächlichen *notice and take down*-Verfahren unterscheide, weil die *notice* nur eine Mitteilung einer angeblichen Urheberrechtsverletzung anstatt der Kenntnis der Rechtswidrigkeit erfordere.[117]

Ausmaß und Aufwand der geforderten Bemühungen für eine Entfernung oder Zugangssperrung der Inhalte waren in § 10 Abs. 2 TMG nicht vorgesehen. Der Grundsatz, dass Entfernung oder Zugangssperrung für den ISP technisch möglich und zumutbar ist, wird demnach in § 10 TMG nicht deutlich genug formuliert – wahrscheinlich deswegen, weil der Gesetzgeber Art. 14 Abs. 1 ECRL wortgetreu umsetzen wollte.[118] Nach dem eigentlichen Willen des Gesetzgebers gilt dieser Grundsatz hier ebenfalls.[119]

Die Tatsache, dass der Zeitpunkt und das Löschverfahren der illegalen Inhalte im TMG nicht geregelt waren, hat sich in der Vergangenheit allerdings als nachteilig erwiesen. In Anbetracht dessen schuf der Gesetzgeber 2017 das Netzwerkdurchsetzungsgesetz, das – anders als das TMG – nicht nur Privilegierungen der Provider für fremde illegale Inhalte enthielt, sondern auch entsprechende Verpflichtungen.

---

115 Vgl. *Spindler/Schmitz/Geis*, ebenda, § 11, Rn. 22.

116 Vgl. *Sieber*, Verantwortlichkeit im Internet, S. 171–172, Rn. 345; *Stadler*, Haftung für Informationen im Internet, S. 141–142, Rn. 105a.

117 Vgl. *Freytag*, CR 2000, 608.

118 Vgl. Spindler/Schuster-*Hoffmann*, TMG § 10, Rn. 44.

119 Vgl. BT-Drs. 14/6098, S. 25.

C. Neuregelungen des Netzwerkdurchsetzungsgesetzes 2017

1. Hauptinhalte der Neuregelungen

Am 1. Oktober 2017 ist das vom Bundestag beschlossene Netzwerkdurchsetzungsgesetz (NetzDG) in Kraft getreten. Das NetzDG legt seinen Schwerpunkt darauf, dass die Betreiber der großen sozialen Netzwerke ihrer Verpflichtung zur Löschung der strafbaren Inhalte besser nachkommen sollen.[120] Es leitet damit einen kriminalpolitischen Wandel von einer Politik der Privilegierung der Provider zu deren strengerer Regulierung ein.

Nach § 3 NetzDG muss der Anbieter eines sozialen Netzwerks ein wirksames und transparentes Verfahren für den Umgang mit Beschwerden über rechtswidrige Inhalte vorhalten. Der Anbieter muss auch Nutzern ein leicht erkennbares, unmittelbar erreichbares und ständig verfügbares Verfahren zur Übermittlung von Beschwerden über rechtswidrige Inhalte zur Verfügung stellen. Das Verfahren muss gewährleisten, dass der Anbieter des sozialen Netzwerks in der Regel einen offensichtlich rechtswidrigen Inhalt innerhalb von 24 Stunden nach Eingang der Beschwerde entfernt oder den Zugang zu ihm sperrt. Die Inhalte, deren Rechtswidrigkeit nicht offensichtlich ist, müssen innerhalb von sieben Tagen nach Eingang der Beschwerde entfernt werden. Gemäß § 2 NetzDG sind die Anbieter sozialer Netzwerke neben dem Beschwerdemanagement auch verpflichtet, vierteljährlich einen deutschsprachigen Bericht über den Umgang mit Beschwerden über rechtswidrige Inhalte auf ihren Plattformen zu erstellen und im Bundesanzeiger sowie auf der eigenen Homepage spätestens einen Monat nach Quartalsende zu veröffentlichen. Darüber hinaus müssen die Anbieter sozialer Netzwerke nach § 5 NetzDG unverzüglich für Zustellungen in Bußgeldverfahren sowie in zivilrechtlichen Verfahren einen inländischen Zustellungsbevollmächtigten gegenüber dem zuständigen Gericht benennen.

2. Bewertung der Neuregelungen

Obwohl durch dieses neue Gesetz die Bedeutung „unverzüglich“ in § 10 TMG konkreter und klarer als früher bestimmt wird, wird dieses Gesetz trotzdem von vielen Parteien, Wissenschaftlern sowie Internetnutzern heftig kritisiert. Sorgen bereitet ihnen vor allem, dass ein so strenges Gesetz die Meinungsfreiheit gefährdet, weil die Anbieter der sozialen Netzwerke wegen der Androhung von Bußgeld viele beanstandete Inhalte sehr schnell löschen würden. Deshalb wird das NetzDG teil-

---

[120] Bundestag beschließt Gesetz gegen strafbare Inhalte im Internet, abrufbar unter https://www.bundestag.de/dokumente/textarchiv/2017/kw26-de-netzwerkdurchsetzungsgesetz/513398 [Stand: 15.09.2017].

weise als verfassungswidrig eingestuft.[121] Außerdem belasteten die neuen Regelungen die Betreiber der sozialen Netzwerke viel mehr, da die Betreiber sehr viel höhere Kosten übernehmen müssten, um die gesetzlichen Anforderungen zu erfüllen. Bedenken bestehen auch, dass auf diese Weise die Abwägungen und Entscheidungen über die strafrechtliche Relevanz der Inhalte – und damit über die Grenzen der Meinungsfreiheit – in die Hände von Privatunternehmen gelegt werden.[122]

Auch die Begründung der neuen Gesetzgebung ist zweifelhaft. Ausgangspunkt der oben genannten Compliance-Pflichten ist die Haftungsregelung für Diensteanbieter nach § 10 TMG, weil nach diesem Paragrafen die Diensteanbieter verpflichtet sind, die gespeicherten Inhalte unverzüglich zu entfernen oder den Zugang zu ihnen zu sperren, wenn sie von den Inhalten Kenntnis genommen haben.[123] Allerdings gehört § 10 TMG nach der überzeugenden Meinung von *Sieber* zu einer Privilegierungs- anstatt zu einer Verpflichtungsregelung:[124] In § 10 TMG werden also keine Verpflichtungen der Hosting Provider begründet. Deshalb ist es unberechtigt, die oben genannten Verpflichtungen aus § 10 TMG abzuleiten. Die entsprechenden Verpflichtungen müssen sich vielmehr aus den allgemeinen strafrechtlichen Regelungen ergeben, die im Folgenden untersucht werden.

Außerdem ist hier eine weitere Frage zu beantworten, ob wegen der Einführung des neuen NetzDG die §§ 7–10 TMG vom Gesetzgeber nicht mehr als Privilegierungsregelungen angesehen werden? Meines Erachtens wird die privilegierende Grundeigenschaft der §§ 7–10 TMG durch die Einführung des NetzDG nicht verändert. So war im alten Gesetzesentwurf schon deutlich gemacht worden, dass diese Paragrafen nur eine verantwortlichkeitseinschränkende Rolle (wie ein Filter) spielen.[125] Offensichtlich kann dieser ausdrücklich geäußerte Wille des Gesetzgebers nicht nachträglich verändert werden. Andererseits dient das neue NetzDG nach der Formulierung im Gesetzgebungsmaterial einer „Verbesserung der Rechtsdurchsetzung".[126] Dies ist so zu verstehen, dass der Gesetzgeber das vorherige Gesetz nur auf diese Weise weiter konkretisieren und ergänzen will, anstatt die grundlegende Natur des TMG wiederaufzubauen.

Allerdings lässt sich nicht leugnen, dass die im NetzDG genannten Verpflichtungen schon deutlich über das TMG hinausgehen. Die Forderung nach einem wirksamen Beschwerdemanagement kann noch theoretisch als eine Konkretisierung der

---

[121] Vgl. 5 Gründe gegen das Netzwerkdurchsetzungsgesetz, abrufbar unter https://www.freiheit.org/NetzDG [Stand: 15.09.2017].

[122] Bundestag beschließt Gesetz gegen strafbare Inhalte im Internet, abrufbar unter https://www.bundestag.de/dokumente/textarchiv/2017/kw26-de-netzwerkdurchsetzungsgesetz/513398 [Stand: 15.09.2017].

[123] Vgl. BT-Drs. 18/12356, S. 12.

[124] Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 15.

[125] BT-Drs. 14/6098, S. 23.

[126] Vgl. BT-Drs. 18/12356, S. 11.

Voraussetzungen in § 10 Abs. 1 Nr. 2 TMG betrachtet werden. Aber auf jeden Fall haben die sogenannte Berichtspflicht, die Verpflichtung zur Erstellung eines wirksamen und transparenten Verfahrens für den Umgang mit Beschwerden über rechtswidrige Inhalte sowie die Verpflichtung zur Benennung eines inländischen Zustellungsbevollmächtigten, welche im TMG nie erwähnt werden, bereits sichtlich erkennbar die Grenze des TMG überschritten. Weil der deutsche Gesetzgeber die Artikel 12–15 ECRL in den §§ 7–10 TMG umgesetzt hat, besteht hier zusätzlich auch das Problem der Vereinbarkeit zwischen NetzDG und ECRL.

Nach den Begründungen im Gesetzesentwurf sind die in den §§ 2, 3, 5 NetzDG vorgesehenen Compliance-Regeln allerdings mit der ECRL vereinbar. Die zentralen Argumente dafür liegen in den offenen Zusätzen, etwa wie Artikel 14 Abs. 3, Erwägungsgründe 46, 48 ECRL.[127] Diese Begründungen vermögen jedoch nicht zu überzeugen, vor allem, weil die Bedeutung dieser offenen Klauseln immer unklar bleibt. Deshalb ist es aus methodischer Sicht zweifelhaft, auf diese Klauseln zurückzugreifen. Darüber hinaus können die oben genannten Verpflichtungen auch inhaltlich nicht treffend durch diese Klauseln begründet werden.

Artikel 14 Abs. 3 ECRL lässt die Möglichkeit unberührt, dass die Mitgliedstaaten Verfahren für die Entfernung einer Information oder die Sperrung des Zugangs zu ihr festlegen. Hier ist jedoch zu beachten, dass nach dem Wortlaut „Verfahren für die Entfernung einer Information oder die Sperrung des Zugangs zu ihr“ nur vom Staat anstatt der ISP herzustellen sind.

Weiterhin lässt die Richtlinie gemäß Erwägungsgrund 46 ECRL die Möglichkeit der Mitgliedstaaten unberührt, spezifische Anforderungen vorzuschreiben, die vor der Entfernung von Informationen oder der Sperrung des Zugangs unverzüglich zu erfüllen sind. Aber diese vor der Entfernung von Informationen zu erfüllenden Anforderungen sind inhaltlich völlig unbestimmt und stellen ohnehin keine solide Unterstützung für die Verpflichtungen im NetzDG dar. Außerdem wird in dem gleichen Erwägungsgrund spezifisch betont, dass im Zusammenhang mit der Entfernung oder der Sperrung des Zugangs der Grundsatz der freien Meinungsäußerung und die hierzu auf einzelstaatlicher Ebene festgelegten Verfahren zu beachten sind. Es ist unzulässig, einen einzelnen Satz aus dem Zusammenhang zu reißen und ihn als Begründung zu nennen.

Nach Erwägungsgrund 48 ECRL lässt die Richtlinie auch die Möglichkeit unangetastet, dass die Mitgliedstaaten von Diensteanbietern, die von Nutzern ihres Dienstes bereitgestellte Informationen speichern, verlangen, die nach vernünftigem Ermessen von ihnen zu erwartende und in innerstaatlichen Rechtsvorschriften niedergelegte Sorgfaltspflicht anzuwenden, um bestimmte Arten rechtswidriger Tätigkeiten aufzudecken und zu verhindern. In gewissem Maß steht Erwägungsgrund 48 selbst mit Artikel 15 ECRL, welcher die allgemeine Überwachungspflicht

---

[127] Vgl. ebenda, S. 13–14.

der ISP verneint, nicht in Einklang, außerdem bleibt auch die Bedeutung dieser sogenannten Sorgfaltspflicht unklar. Deshalb ist es auch problematisch, daraus die oben genannten Verpflichtungen abzuleiten, ganz zu schweigen von ihrer Umsetzung in eine Ordnungswidrigkeit mit einer Geldbuße bis zu fünf Millionen Euro.

Zusammenfassend lässt sich feststellen, dass die Neuregelungen des NetzDG sowohl in ihrer Rechtsgrundlage als auch in ihrer praktischen Wirkung viele Fragen aufwerfen.

III. Allgemeine strafrechtliche Verantwortlichkeit der ISP

Wie oben beschrieben, gibt es zwei entgegengesetzte Auffassungen über das Verhältnis zwischen TMG und Strafgesetz, nämlich die „Vorfilterlösung“ und die „Integrationslösung“. Abgesehen von diesem Gegensatz müssen die Probleme im strafrechtlich allgemeinen Teil neben der Auslegung des TMG berücksichtigt werden.

A. Beziehung zwischen StGB und den Verantwortlichkeitsregelungen im TMG

Die Verantwortlichkeitsregelungen im TMG können alle Rechtsbereiche abdecken. Zur Bestimmung der strafrechtlichen Verantwortlichkeit der ISP kann deshalb auf zwei Kategorien von Regelungen zurückgegriffen werden. Die Frage, wie die Beziehung zwischen den beiden Gesetzen zu handhaben ist, wird in der Literatur vollkommen unterschiedlich gesehen.

1. „Vorfilterlösung“

Die Verantwortlichkeitsregelungen im TMG spielen die Rolle eines „Filters“. Zum einen sind die Regelungen im TMG vor der Anwendung des strafrechtlichen Tatbestands heranzuziehen. Ergibt sich hieraus keine Verantwortlichkeit nach dem TMG, wird eine weitere Prüfung nach dem Strafgesetz unnötig. Wird die allgemeine Verantwortlichkeit nach §§ 7 ff. TMG bestimmt, ist die strafrechtliche Verantwortlichkeit weiter zu prüfen.[128] Zum anderen haben diese Regelungen nur eine einschränkende (nicht begründende) Auswirkung, damit die strafrechtliche Verantwortlichkeit der ISP vorher begrenzt wird.

---

[128] Vgl. *Malek/Popp*, Strafsachen im Internet, S. 21, Rn. 74.

Die „Vorfilterlösung“ wird von vielen Rechtswissenschaftlern unterstützt,[129] schon allein, weil sie dem Willen und Sprachgebrauch des Gesetzgebers entspricht. Der Begriff des Filters wird vom Gesetzgeber selbst verwendet. Seine Äußerung über § 5 TDG a.F. lautet folgendermaßen: „Die Regelungen zur Verantwortlichkeit sind der straf- und zivilrechtlichen Prüfung vorgelagert.“[130] „Die Wirkungsweise der §§ 9 bis 11 TDG lässt sich untechnisch mit der eines Filters vergleichen.“[131] Diese Äußerungen zeigen deutlich, dass die Verantwortlichkeitsregelungen im TDG/TMG vor allem unabhängig vom StGB geprüft werden müssen. Der zweite Grund, warum die Vorfilterlösung unterstützt wird, bezieht sich auf arbeitsökonomische Gesichtspunkte.[132] Nach dieser Meinung wären einige Prüfungen nach dem Strafgesetzbuch nicht notwendig, wenn die Verantwortlichkeit oder die Voraussetzung im TMG nicht erfüllt werden. Von der Gegenmeinung wird kritisiert, dass auf der einen Seite ein rechtsgebietsspezifischer Bezugspunkt für die Auslegung der Tatbestandsmerkmale bei der „Vorfilterlösung“ fehle. Auf der anderen Seite bestünde die Gefahr, die Merkmale mit widersprüchlichem Ergebnis doppelt zu prüfen.[133]

2. „Integrationslösung“

Die „Integrationslösung“ verbindet die §§ 7–10 TMG mit der Auslegung der strafrechtlichen Tatbestände, die Verantwortlichkeitsregelungen im TMG werden also gleichzeitig interpretiert. Zu beachten ist allerdings, wie und auf welche Weise diese Regelungen mit der Auslegung der strafrechtlichen Tatbestände integriert werden können. Es gibt insgesamt drei Interpretationsansätze dafür. So bezieht *Bröhl* die Verantwortlichkeitsregelungen auf die Ebene der Schuld. Die Handlung, die die Voraussetzungen der §§ 8–10 TMG erfülle, sei noch rechtswidrig.[134] Diesem Schluss ist nicht zu folgen, denn eine vom TMG privilegierte Handlung ist gesellschaftlich akzeptiert und sozial üblich.[135]

---

[129] Vgl. *Altenhain*, AfP Heft 29, 1998, 458; *Bleisteiner*, Rechtliche Verantwortlichkeit im Internet, S. 157; *Malek/Popp*, ebenda, S. 21, Rn. 74; *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 14.

[130] BT-Drs. 13/7385, S. 51.

[131] BT-Drs. 14/6098, S. 23.

[132] Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 14; *ders.,* Verantwortlichkeit im Internet, S. 121–122, Rn. 246.

[133] Vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 60, Rn. 190.

[134] Vgl. *Bröhl*, CR Heft 2, 1997, 75; LG München I: Straflosigkeit der reinen Zugangsvermittlung „harter” Pornografie im Internet, NJW Heft 14, 2000, 1051 (LG München I, Urteil vom 17.11.1999 – 20 NS 465 JS 173158/95).

[135] Aus dem gleichen Grund ist die Meinung, welche die Verantwortlichkeitsregelungen als Strafausschließungsgrund betrachtet, abzulehnen. Vgl. *Heghmanns*, ZUM Heft 6, 2000, 465. Eine andere kritische Meinung bei *Popp*, Die strafrechtliche Verantwortung von Internet-Providern, S. 93.

Zweitens wird die Ansicht vertreten, dass die Beschränkung der Handlungs- bzw. Unterlassungspflichten eines Providers auf der Ebene der Rechtswidrigkeit behandelt werden soll.[136] Nach dieser Ansicht beziehen sich die Privilegien in den §§ 8–10 TMG auf eine Abwägung zwischen dem Interesse der ISP und dem Normbefehl. Jedoch ist diese Auffassung noch nicht zutreffend. Nachdem die Merkmale des Tatbestands erfüllt worden sind, besteht normalerweise die formale Rechtswidrigkeit einer Handlung. Obwohl diese Handlung später gerechtfertigt werden kann, brauchen wir noch eine materiale Abwägung zwischen den relevanten Interessen. Aber die Handlung, die nach den §§ 8–10 TMG keine generelle Verantwortlichkeit hat, stellt nicht von vornherein den „Unrechtstyp" dar.

Die dritte Meinung besagt, dass die Integration auf der Ebene des Tatbestands liegen soll. Die Privilegien im TMG werden im Rahmen des Tatbestands bei der Auslegung oder der objektiven Zurechnung geprüft.[137] Deshalb werden die Merkmale des Tatbestands nicht erfüllt und es besteht auch kein typisches Unrecht, wenn die Handlung des ISP nach den §§ 8–10 TMG privilegiert wird. Dieser Lösungsansatz ist auch auf Kritik gestoßen. Zum einen werden die Verantwortlichkeitsregelungen im TMG als einheitliche und eigenständige Rechtsnorm aufgegeben,[138] die Anwendung der Regelungen im TMG ist also von der Auslegung des Tatbestands im StGB absolut abhängig. Dieses Ergebnis verhält sich zum Willen des Gesetzgebers völlig konträr. Zum anderen werden §§ 7–10 TMG nach dieser „Integrationslösung" nicht als tatbestandseinschränkende, sondern als tatbestandsmodifizierende Merkmale betrachtet.[139] Diese Lösung führt dazu, dass einige Voraussetzungen in §§ 7–10 TMG zusätzlich Teil des Tatbestands werden.

3. Eigene Stellungnahme

Die „Vorfilterlösung" ist nach einer vergleichenden Untersuchung zu befürworten. Zuerst ist der klar geäußerte Wille des Gesetzgebers zu respektieren. Wie oben erwähnt, hat der Gesetzgeber deutlich gemacht, dass die Regelungen in den §§ 7–10 TMG vorgelagert werden sollen und eine Filterfunktion übernehmen. Aus dieser Bestimmung resultiert keine Mehrdeutigkeit. Auch der spezielle Wortlaut der §§ 7–10 TMG, wie beispielsweise „Kenntnis" statt „Vorsatz", verdeutlicht die Präferenz des Gesetzgebers.[140] Außerdem stellt der oben genannte Mangel des rechtsgebietsspezifischen Bezugspunkts kein Problem dar, die Anwendung des TMG setzt keine Beziehung mit dem Tatbestand des StGB voraus. Mit anderen Worten, die

---

[136] Vgl. *Popp*, Die strafrechtliche Verantwortung von Internet-Providern, S. 94.

[137] Vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 61, Rn. 192; *Hilgendorf*, NStZ Heft 10, 2000, 519; Schönke/Schröder-*Eisele*, § 184, Rn. 72; Lackner/Kühl-*Heger*, § 184, Rn. 7a; *Hörnle*, NJW 14, 2002, 1011; *Pelz*, wistra Heft 2, 1999, 58.

[138] Vgl. *Bleisteiner*, Rechtliche Verantwortlichkeit im Internet, S. 156 ff.

[139] Vgl. *Sieber*, Verantwortlichkeit im Internet, S. 112–113, 121–122, Rn. 229–230, 246.

[140] Vgl. *Bleisteiner*, Rechtliche Verantwortlichkeit im Internet, S. 154.

§§ 7–10 TMG können unabhängig von der Auswirkung des StGB interpretiert werden, weil das TMG selbstständige Tatbestände kennt. Es gibt im TMG sowohl eine klare Definition des ISP als auch die durchführbaren Regelungen für die Privilegien der ISP, weshalb der sogenannte rechtsgebietsspezifische Bezugspunkt nicht notwendig ist. Darüber hinaus führt die „Vorfilterlösung" nicht dazu, dass die Merkmale mit gegensätzlichem Ergebnis zweimal geprüft werden. Denn die Voraussetzungen in beiden Gesetzen liegen auf unterschiedlichen Ebenen. Die Merkmale im TMG bilden die Grundlage für die Auslegung des Tatbestands. Obwohl die Forderungen in beiden Gesetzen unterschiedlich sind, stellen diese Unterschiede somit keinen Widerspruch dar.

Schließlich kann die mögliche Kollision zwischen den Voraussetzungen des TMG und den Tatbeständen vermieden werden. Da nach der „Integrationslösung" die Privilegien im TMG bei der Auslegung oder Prüfung der objektiven Zurechnung berücksichtigt werden können,[141] ist die Beziehung zwischen den beiden Gesetzen schwierig zu behandeln. Mit dem Eintritt der zusätzlichen Merkmale vom TMG könnte die Stabilität des Strafrechtssystems beschädigt werden. Daraus folgt aber nicht, dass die Privilegierungsregelungen ganz von den Tatbeständen im StGB getrennt werden. Obwohl diese Regelungen im Allgemeinen eine Rolle als Vorfilter spielen, können sie in der Auslegung der konkreten Tatbestände einschränkend wirken. Zum Beispiel kann man sich noch auf die Privilegierungsregelungen im TMG berufen, wenn man die Garantenstellung der ISP bestimmt. Es wird in der Literatur zutreffend konstatiert, dass sie tatsächlich eine außerhalb des eigentlichen Tatbestands liegende Zuordnungsregel bilden.[142]

B. Einschlägige Straftatbestände im Besonderen Teil des StGB

Im deutschen Recht gibt es keine spezifischen Paragrafen über die strafrechtliche Verantwortlichkeit der ISP.[143] Im deutschen StGB wird die strafrechtliche Verantwortlichkeit der ISP auch nicht selbstständig vorgesehen. Jedoch kann die Verantwortlichkeit der ISP durch die allgemeinen Straftatbestände im StGB erfasst werden, insbesondere durch die sogenannten Verbreitungs- und Äußerungsdelikte. Ergo könnten die ISP wegen ihrer Internet-Service-Angebote als Teilnehmer oder sogar als Täter bestraft werden, wenn die Nutzer über die Infrastruktur der ISP strafbare Inhalte verbreiten oder äußern.

Die möglichen, für die strafrechtliche Verantwortlichkeit der ISP in Betracht kommenden Paragrafen des Besonderen Teils des StGBs sind insbesondere: §§ 86, 86a Verbreiten von Propagandamitteln verfassungswidriger Organisationen;

---

141 Vgl. Schönke/Schröder-*Eisele*, § 184, Rn. 72.

142 Vgl. *Pelz*, wistra Heft 2, 1999, 58.

143 Vgl. *Malek/Popp*, Strafsachen im Internet, S. 40, Rn. 147.

Verwenden von Kennzeichen verfassungswidriger Organisationen; § 90 Verunglimpfung des Bundespräsidenten; § 90a Verunglimpfung des Staates und seiner Symbole; § 90b Verfassungsfeindliche Verunglimpfung von Verfassungsorganen; § 91 Anleitung zur Begehung einer schweren staatsgefährdenden Gewalttat; § 130 Volksverhetzung; § 130a Anleitung zu Straftaten; § 131 Gewaltdarstellung; § 184 Verbreitung pornografischer Schriften; § 184a Verbreitung gewalt- oder tierpornografischer Schriften; § 184b Verbreitung, Erwerb und Besitz kinderpornografischer Schriften; § 184c Verbreitung, Erwerb und Besitz jugendpornografischer Schriften; § 184d Zugänglichmachen pornografischer Inhalte mittels Rundfunk oder Telemedien; Abruf kinder- und jugendpornografischer Inhalte mittels Telemedien; § 185 Beleidigung; § 186 Üble Nachrede; § 187 Verleumdung; § 188 Üble Nachrede und Verleumdung gegen Personen des politischen Lebens; § 189 Verunglimpfung des Andenkens Verstorbener; überdies auch die Paragrafen des UrhG: § 106 Unerlaubte Verwertung urheberrechtlich geschützter Werke; § 107 Unzulässiges Anbringen der Urheberbezeichnung; § 108 Unerlaubte Eingriffe in verwandte Schutzrechte; § 108a Gewerbsmäßige unerlaubte Verwertung; § 108b Unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen.

In den oben genannten Paragrafen werden die §§ 184 ff. StGB (Verbreitung pornografischer Schriften) in Literatur und Rechtsprechung für die strafrechtliche Verantwortlichkeit besonders diskutiert. So wurde zum Beispiel dieser Paragraf im berühmten *CompuServe*-Fall angewendet.[144] Da die böswilligen Nutzer oft zur Verbreitung der pornografischen Inhalte die Internetdienste der ISP missbrauchen, werden diese Paragrafen bezüglich der strafbaren pornografischen Schriften häufiger angewendet.

C. Einordnung der Handlungen der ISP als Tun oder Unterlassen

1. Abgrenzung von Tun und Unterlassen

Die Abgrenzung von positivem Tun und Unterlassung ist eine grundlegende Problematik in der strafrechtlichen Theorie und Rechtsprechung. Insgesamt gibt es dazu zwei Theorien. Von der Rechtsprechung[145] wird angeführt, die Abgrenzung sei davon abhängig, wo der Schwerpunkt der Vorwerfbarkeit liegt. In der Literatur

---

[144] Vgl. AG München: *CompuServe*-Urteil, MMR Heft 8, 1998, S. 429 (AG München, Urteil vom 28.05.1998 – 8340 Ds 465 Js 173158/95). Verbreitung pornografischer Inhalte im Internet – Freispruch im *CompuServe*-Prozess, ZUM Heft 3, 2000, 247. Über die Anwendung des § 184c *Waldenberger*, MMR Heft 6, 2008, 400 ff (BGH, Urteil vom 18.10.2007 – I ZR 102/05).

[145] Vgl. BGHSt 6, 59; OLG Karlsruhe GA 1980, 429(431); BGH, NStZ 1999, 607.

neigen viele Autoren zu dieser Ansicht.[146] Zum anderen wird allmählich zunehmend auch die Meinung vertreten, die Abgrenzung von Tun und Unterlassen beruhe auf dem Vorliegen oder Nichtvorliegen einer Begehungskausalität. Hier zielt die Argumentation in der Regel auf den Energieaufwand ab: Wenn ein aktiver Energieaufwand den Erfolg kausal und zurechenbar verursacht, könnte das Tun bestehen, sonst das Unterlassen.[147]

Das zentrale Argument der Vertreter der ersten Meinung ordnet die Abgrenzung zwischen Tun und Unterlassen einer Bewertungsfrage, nicht einer empirischen Frage zu.[148] Dem ist natürlich insoweit zuzustimmen, als dass die äußeren Gestaltungen der Handlungen vielfältig sind, und wir auf Abwege geraten könnten, wenn wir nur eine empirische und naturwissenschaftliche Betrachtungsweise heranziehen. Jedoch birgt diese These viele Unsicherheiten in sich. Das Kriterium der Vorwerfbarkeit wird als Zirkelschluss betrachtet, da diese Meinung keinen konkreten und durchführbaren Maßstab für diese Bewertung gegeben hat.[149]

Aber es ist auch zu anzumerken, dass die zweite Auffassung keine rein naturwissenschaftliche Betrachtungsweise ist.[150] In der Zurechnung verbirgt sich die Bewertung hinter der Kausalität. Deshalb ist der Gegensatz zwischen den oben genannten Auffassungen nicht überzubewerten. In den meisten Fällen gibt es keinen materialen Unterschied in der endgültigen Schlussfolgerung.

2. Einordnung der Handlungen der ISP als Tun oder Unterlassen

Da die Typen der ISP und ihre jeweiligen Funktionen sehr vielfältig sind, existiert keine allgemeingültige Lösung für die Einordnung der Handlung als Tun oder Unterlassen. Dagegen bildet eine differenzierende Ansicht hinsichtlich der unterschiedlichen technischen Eigenschaften der ISP die Wirklichkeit am ehesten ab.

Für die eigene Informationen anbietenden Content Provider besteht grundsätzlich positives Tun nach der herrschenden Meinung.[151] Ohne Zweifel ist die aktive Bereithaltung der eigenen Inhalte der Schwerpunkt der strafgesetzlichen Bewertung. Bei der Verantwortlichkeit für fremde Informationen, die von den ISP übermittelt oder gespeichert werden, wird diese Problematik komplizierter. Theoretisch ist bei-

---

[146] Vgl. *Wessels/Beulke*, AT[38], Rn. 700; Schönke/Schröder-*Stree/Bosch*, Vor §§ 13, Rn. 158a; *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 22; *Malek/Popp*, Strafsachen im Internet, S. 30, Rn. 108.

[147] Vgl. *Roxin*, AT II, § 31 Rn. 78; *Jescheck/Weigend*, AT, § 58 II 2; *Jakobs*, AT, 28/1; *Sieber*, JZ Heft 11/12, 1983, 436.

[148] Vgl. *Mezger* AT[9], S. 76; *Wessels/Beulke*, AT[38], Rn. 700.

[149] Vgl. *Roxin*, AT II, § 31 Rn. 79–80; *Altenhain*, CR Heft 8, 1997, 487.

[150] Die Kritik zur Kausalitätsformel vgl. *Altenhain*, ebenda, 487–488.

[151] Vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 71, Rn. 237; *Malek/Popp*, Strafsachen im Internet, S. 31, Rn. 109.

des jeweils möglich, das aktive Tun wie das Unterlassen.[152] Aber unter normalen Umständen – sofern die ISP nicht absichtlich mit den Nutzern illegal zusammenarbeiten – kommt grundsätzlich nur das Unterlassen in Betracht.[153] Der wichtigste Grund dafür liegt darin, dass die Durchleitung von Informationen, die Zwischenspeicherung zur beschleunigten Übermittlung von Informationen und die Speicherung von Informationen für gewöhnlich rechtmäßige und sozialadäquate Tätigkeiten sind. Die Internet-Services verfügen in der Regel über nützliche Eigenschaften für unsere Gesellschaft.[154] Der sozialadäquate Charakter der Services von ISP führt dazu, dass diese Tätigkeiten keinen Schwerpunkt der strafgesetzlichen Bewertung bilden.

In den meisten Fällen besitzen die ISP, nämlich die Access-, Proxy Cache- und Hosting Provider, keine Kenntnis von den übermittelten oder gespeicherten Informationen. Nach der Regelung des § 7 Abs. 2 TMG sind die ISP auch nicht verpflichtet, diese Informationen zu überwachen. Nur wenn die ISP die strafbaren Informationen schon gekannt haben und sie diese illegalen Inhalte nicht sperren möchten, kann ein Unterlassen der ISP geprüft werden.[155] In einigen Sonderfällen könnte auch aktives Tun vorliegen. Die erste Voraussetzung ist: Die ISP wissen von vornherein, dass die Nutzer durch die Durchleitung oder Speicherung von Informationen bei ISP eine Straftat begehen wollen.[156] Die zweite Voraussetzung ist: Die ISP, die schon Kenntnis von strafbaren Inhalten haben, bieten den Service durch aktive Handlung illegal für dritte Personen.[157]

Neben den im TMG genannten gesetzlichen Typen sind die gesetzlich nicht geregelten ISP, wie die Hyperlinksetzer oder die Betreiber von Suchmaschinen, zu diskutieren. Für die Einordnung der Hyperlinksetzer sind verschiedene Konstellationen zu unterscheiden. Setzt man den Hyperlink mit Kenntnis der strafbaren Inhalte absichtlich, besteht ein positives Tun. Sollte ein rechtmäßiger Link gesetzt worden sein, aber die verlinkten Inhalte wurden verändert und damit strafbar, kommt nur ein Unterlassen in Betracht.[158] Das heißt, für die Einordnung der Hyperlinksetzer können sowohl das Tun als auch das Unterlassen möglich sein. Da die Suchmaschine jedoch eine Reihe von unterschiedlichen Diensten anbietet, ist auch eine differenzierende Betrachtungsweise erforderlich.[159]

---

[152] Vgl. *Conradi/Schlömer*, NStZ Heft 10, 1996, 472 ff.

[153] Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 24; *Hörnle*, NJW Heft 14, 2002, 1012.

[154] Vgl. *Sieber*, ebenda, Rn. 22; *Malek/Popp*, Strafsachen im Internet, S. 31, Rn. 109.

[155] Vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 71, Rn. 239.

[156] Vgl. ebenda, S. 71, Rn. 239.

[157] Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 26; *Conradi/Schlömer*, NStZ Heft 10, 1996, 472.

[158] Vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 71, Rn. 238; *Sieber*, ebenda, Rn. 26; *Hütig*, MMR Heft 1, 1998, 49 (AG Tiergarten, Urteil vom 30.06.1997 – 260 DS 857/96).

[159] Vgl. *Sieber*, MMR-Beilage Heft 8, 2007, 10 ff.

D. Strafrechtliche Garantenpflichten der ISP

1. Allgemeine strafrechtliche Garantenstellungen

Über die strafrechtlichen Garantenpflichten für Unterlassung haben sich in der Literatur zwei grundlegende Auffassungen herausgebildet, nämlich das formale und das materielle Kriterium. Nach dem formalen Kriterium ergibt sich die strafrechtliche Garantenstellung aus Gesetz, Vertrag, enger Lebensgemeinschaft und vorangegangenem Tun. Heutzutage ist dieses formale Kriterium von der herrschenden Meinung aber schon wieder aufgegeben worden, weil tatsächlich nicht bestimmt werden kann, welche Gesetze die Garantenstellungen begründen und wie erschöpfend der Umfang der Garantenpflichten ist.[160]

Zurzeit steht das materielle Kriterium im Fokus. Danach wird die Garantenstellung in zwei Typen, die Beschützergarantenstellung und die Überwachungsgarantenstellung, unterteilt. Bei der Überwachungsgarantenstellung handelt es sich um die Garantenpflicht, eine bestimmte Gefahr zu überwachen und deren Realisierung zu verhindern. Die Beschützergarantenstellung bezieht sich auf die Garantenpflicht, bestimmte Güter vor Gefahr zu bewahren.[161]

2. Strafrechtliche Garantenpflichten der ISP

a) Garantenpflichten aus dem Gesetz?

Bezüglich der strafrechtlichen Garantenpflichten von ISP sind zuerst die Verantwortlichkeitsregelungen im TMG zu diskutieren. Nach § 7 Abs. 2 TMG sind die ISP nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen. Deshalb wird die allgemeine Verpflichtung zur Überwachung der rechtswidrigen Information verneint. In den §§ 8–10 TMG werden die detaillierten Voraussetzungen für die Privilegierung der Access Provider, Caching Provider und Hosting Provider weiter festgelegt. Aber hier ergibt sich auch die Frage, ob diese Voraussetzungen die Garantenpflichten der ISP begründen.[162]

Im alten gesetzgeberischen Material wird darauf verwiesen, dass der ISP, der rechtswidrige Inhalte Dritter in sein Diensteangebot übernimmt und Kenntnis von diesen Inhalten besitzt, eine Garantenstellung für die Verhinderung der Übermittlung hat.[163] Jedoch wird diese Ansicht in der Literatur von der herrschenden Meinung verneint: Da diese Privilegierungsregelungen nur eine die Verantwortlichkeit

---

[160] Vgl. *Rengier*, AT, § 50, Rn. 2; *Roxin*, AT II, § 32 II, Rn. 10 ff.

[161] Vgl. *Kindhäuser*, AT[7], § 36, Rn. 24 ff; *Rengier*, AT, § 50, Rn. 3 ff.; *Roxin*, AT II, § 32 III, Rn. 17 ff.; *Fischer*, Strafgesetzbuch, § 13, Rn. 13 ff.

[162] Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 33.

[163] Vgl. BT-Drs. 13/7385, S. 20.

beschränkende Rolle spielten, sollten sie nicht als Begründung und Unterstützung für die strafrechtlichen Garantenpflichten der ISP interpretiert werden.[164]

Hingegen ist nicht zu übersehen, dass die Privilegierungsregelungen die Bestimmung der Garantenpflichten der ISP sowohl einschränken als auch sinnvoll beeinflussen können, diese Regelungen können also für die Garantenstellung „mittelbare Wirkung" haben.[165] Hier werden die Garantenpflichten der ISP nur nach dem allgemeinen Grundsatz im Strafrecht begründet, die Quelle der Garantenpflichten der ISP beruht demnach auf allgemeinen strafrechtlichen Grundsätzen sowie auf relevanten strafrechtlichen Tatbeständen. Auf dieser Ebene spielen diese Regelungen in den §§ 7–10 TMG keine Rolle. Wenn die theoretisch möglichen Garantenpflichten der ISP weiter kritisch geprüft werden, wird die Bedeutung dieser Regelungen ersichtlich.

Vor allem wird die Typisierung der ISP bei der Anwendung der §§ 7–10 TMG verwirklicht. Die Typisierung der ISP ist eine unentbehrliche Voraussetzung für die Diskussion über die strafrechtliche Verantwortlichkeit der ISP. Wie schon erläutert, gibt es sehr vielfältige Arten von ISP, die jeweils unterschiedlichen Funktionen und Kontrollmöglichkeiten entsprechen. Offensichtlich ist die Diskussion über die strafrechtliche Verantwortlichkeit auf eine allgemeine Weise unpräzise, zumal auch zu beachten ist, dass eine Typisierung der ISP im StGB gar nicht existiert. Diese Problematik kann allein mithilfe der traditionellen dogmatischen Theorie, die überhaupt auf dem Strafgesetzbuch basiert, nicht gelöst werden. Deshalb ist die Bestimmung der strafrechtlichen Verantwortlichkeit der ISP zuerst abhängig von der Anwendung und Auslegung der Regelungen in den §§ 7–10 TMG.

Außerdem hat die Typisierung der ISP die Systematisierung der Garantenpflichten der ISP ermöglicht. Mit der Typisierung der ISP wird dementsprechend ein System für die Privilegierung der ISP festgelegt, aus dem sich ein grundlegender Rahmen für die Garantenpflichten ergibt, denn das System der Privilegierung entspricht im Allgemeinen dem Rahmen der Garantenpflichten.

b) Garantenpflichten aus Ingerenz?

In der Rechtsprechung und der älteren Forschungsliteratur wird die Bestätigung der Garantenstellung aus Ingerenz (gefahrbegründendes Vorverhalten) allgemein anerkannt. Nach dieser Theorie heißt Garantenstellung, wenn man durch sein Verhalten eine Gefahr verursacht, die einen tatbestandsmäßigen Erfolg erzeugen könnte. Deshalb besteht die Garantenpflicht darin, den Erfolg zu verhindern.[166] Für

---

[164] Vgl. *Malek/Popp*, Strafsachen im Internet, S. 32, Rn. 113; *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, 2014, Rn. 33 ff.; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 71–72, Rn. 240.

[165] Vgl. *Sieber*, ebenda, Rn. 35.

[166] Vgl. *Baumann/Weber/Mitsch/Eisele*, AT, § 21, Rn. 70.

die Garantenstellung aus Ingerenz gibt es aber eine wichtige Einschränkung als Voraussetzung, die nicht übersehen werden darf, nämlich die Pflichtwidrigkeit. Ein Verhalten, das pflichtmäßig ist, kann nach der überwiegenden Meinung keine Garantenstellung begründen.[167] Außerdem ist es erforderlich, dass die aus Ingerenz verursachte Gefahr des Eintritts des tatbestandsmäßigen Erfolgs in einem engen zeitlichen Zusammenhang stehen muss.[168] Nach diesem Verständnis sind die ISP, die den Nutzern übliche und nützliche Informationsdienste anbieten, grundsätzlich nicht wegen Ingerenz als Garant zu betrachten. Auf der einen Seite sind die normalen Internetdienste der ISP in der Regel ganz recht- und pflichtmäßig, weil sie die angemessenen Bedürfnisse der Bevölkerung auf sozialadäquate Weise erfüllen. Auf der anderen Seite verursacht dieses sogenannte Vorverhalten keine nahe Gefahr eines tatbestandsmäßigen Erfolgs.[169]

In einer besonderen Konstellation ist es demgegenüber durchaus möglich, dass sich die Garantenstellung der ISP aus Ingerenz ergibt, indem etwa die ISP die notwendigen Maßnahmen zur Verhinderung der rechtswidrigen oder sogar strafbaren Informationen nicht ergreifen, auch wenn diese Maßnahmen für die ISP zumutbar und in einer bestimmten Branche von den meisten ISP allgemein anerkannt worden sind. Wenn die ISP diesen Industriestandard nicht erfüllen, verletzen sie eine Verpflichtung, die den tatbestandsmäßigen Erfolg verursacht.

c) Garantenpflichten zum Schutz von Rechtsgütern?

In der Theorie bestehen die Garantenpflichten zum Schutz von Rechtsgütern aus vielen Teilen, für die es aber keine einheitliche Lösung gibt. Für die Garantenpflichten werden in der Literatur viele höchst unterschiedliche Quellen – wie beispielsweise die Pflichten aus familiärer Verbundenheit und Gemeinschaftsbeziehung, die Übernahme von Schutzfunktionen und Amtspflichten, enge persönliche Lebensbeziehungen, Gefahrengemeinschaft, Vertrag und tatsächliche Übernahme – angenommen.[170] Hier ergibt sich die Frage, ob die ISP wegen ihrer Internetdienste als Beschützergaranten betrachtet werden können.

So wird die Ansicht vertreten, dass für den ISP die Garantenpflichten zum Schutz eines speziellen Rechtsguts in der Regel ausscheiden.[171] Im Allgemeinen ist dieser Ansatz zu bejahen, weil aufgrund einer konkreten Prüfung nach der oben

---

[167] Vgl. BGHSt 25, 218 ff.; BGHSt 34, 82(84); BGHSt 37(117); *Baumann/Weber/Mitsch/Eisele*, ebenda, § 21, Rn. 71 ff; *Rengier*, AT, § 50, Rn. 70; *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, 2014, Rn. 37 ff.; *Malek/Popp*, Strafsachen im Internet, S. 32, Rn. 114; *Fischer*, Strafgesetzbuch, § 13, Rn. 52.

[168] Vgl. *Rengier*, ebenda, § 50, Rn. 72 ff.

[169] Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, 2014, Rn. 38.

[170] Vgl. *Kindhäuser*, AT[7], § 36, Rn. 74 ff.; *Rengier*, AT, § 50, Rn. 11 ff.; *Wessels/Beulke*, AT[38], Rn. 718 ff.

[171] Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 31.

genannten Theorie die Garantenstellung der ISP nicht bestimmt werden kann. Erstens lässt sich keine familiäre Verbundenheit zwischen ISP und den Verletzten konstruieren. Die ISP sollten keineswegs – weder aus Sicht der formalen familienrechtlichen Bande noch aus der der materiellen familiären Verbindung[172] – als „Eltern" betrachtet werden. Zweitens sind die ISP natürlich nicht als Amtsträger tätig. Das Angebot der Internetdienste der ISP unterscheidet sich von der Ausübung der öffentlichen Gewalt. Deshalb haben die ISP keine Verpflichtung, bestimmte Rechtsgüter vor Gefahr zu schützen. Drittens besteht keine sogenannte enge persönliche Lebensbeziehung oder Gefahrengemeinschaft zwischen den ISP und den Verletzten. Auch wenn zunächst zuzugestehen ist, dass im Cyberspace alle ISP und Nutzer zu einer „Gemeinschaft" gehören, in der alle Beteiligten im Netzwerk zusammenarbeiten, reicht dieser Zusammenhang zwischen den ISP und den potenziellen Verletzten für die Konstruktion einer engen persönlichen Lebensbeziehung oder Gefahrengemeinschaft nicht aus, denn dieses Beziehungsgeflecht stammt aus einer allgemeinen, abstrakten und sozial üblichen Zusammenarbeit. Dieser alltägliche Zusammenhang kann noch keine Garantenstellung der ISP erzeugen.

Und schließlich ist es problematisch, die Garantenstellung der ISP aus der vertraglichen Beziehung abzuleiten. Mit einem Vertrag zwischen ISP und Nutzer wird eine Reihe von Rechten und Pflichten seitens des ISP festgelegt. Aber diese Rechte und Pflichten konzentrieren sich auf die Internetdienste. Das Angebot der Internetdienste bildet überhaupt erst den Mittelpunkt des Zusammenhangs zwischen ISP, Nutzern und anderen Beteiligten. Deshalb kann nicht geschlussfolgert werden, dass die ISP die relevanten Rechtsgüter vor Gefahr im Netzwerk beschützen müssen. Da die ISP das Internet nicht organisiert und kontrolliert haben, sind sie auch nicht verpflichtet, ein Internet ohne Delikte zu garantieren.[173] Deswegen kann ein vertragliches Verhältnis allein die Garantenstellung der ISP nicht begründen.

Aber in der Literatur gibt es auch kritische Gegenstimmen, nach denen im Einzelfall eine Beschützergarantenstellung gegenüber Personen vor rechtswidrigen Inhalten bestehen kann.[174] Es wird besonders darauf hingewiesen, dass die Netzbetreiber wegen der faktischen Schutzübernahme eine Garantenstellung hätten. Die Tatbestände des § 184 StGB schützten die Jugendlichen vor Gefahren der Verbreitung pornografischer Schriften. Obwohl hier keine enge persönliche Bindung zwischen den ISP und den Jugendlichen existiere, könne die Garantenstellung der ISP aufgrund des Vertrauens der Jugendlichen und ihrer Eltern und damit der faktischen Schutzübernahme bestimmt werden. Die Eltern der Jugendlichen vertrauten darauf, dass die ISP für ein „sauberes" Netz sorgen.[175]

---

[172] Über die formalen und materiellen Kriterien der familiären Verbundenheit vgl. *Rengier*, AT, § 50, Rn. 11 ff.

[173] Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 31.

[174] Vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 71–72, Rn. 240.

[175] Vgl. *Popp*, Die strafrechtliche Verantwortung von Internet-Providern, S. 130 ff.

Diese Argumente sind nicht überzeugend. Auch wenn die Garantenstellung in der Theorie[176] daraus besteht, dass ein besonderes Vertrauensverhältnis angenommen wird, haben die ISP die Voraussetzungen dafür jedoch in dieser Konstellation nicht erfüllt.

Eigentlich gibt es in der Literatur kein einheitliches und klares Kriterium für die Bestimmung der tatsächlichen Übernahme einer Garantenstellung, sie wird vielmehr durch Einzelfallentscheidungen in der Rechtsprechung festgestellt. Nach vielen Erläuterungen ist ein besonderes Vertrauen, das eine Garantenstellung erzeugt, erforderlich. Wie das besondere Vertrauen zu ermitteln ist, bleibt dabei aber unklar. Durch Beobachtung und Analyse der Fälle in der Rechtsprechung sind für die tatsächliche Übernahme der Garantenstellung zwei Voraussetzungen wichtig: Auf der einen Seite soll der mögliche Garant die tatsächliche Fähigkeit haben, Rechtsgüter vor Gefahren zu beschützen, auf der anderen Seite sollen das Vertrauen und die entsprechende Schutzpflicht zumutbar sein.

Die Garantenstellung der ISP gegenüber Jugendlichen aufgrund der Gefahr der Verbreitung von pornografischen Schriften ist daher zu verneinen. In den meisten Konstellationen sind die ISP, besonders die Access Provider und die Netzwerkprovider, nicht in der Lage, die rechtswidrigen Informationen von Dritten zu überwachen und zu kontrollieren. Wie schon erläutert, sind die Kontrollmöglichkeiten der ISP gegenüber illegalen Inhalten im Netzwerk ohnehin sehr begrenzt. Außerdem ist das sogenannte Vertrauen der Eltern der Jugendlichen in die ISP unhaltbar. Obwohl man erwarten könnte, dass die ISP einige Maßnahmen ergreifen, um gegen rechtswidrige Inhalte im Netzwerk (etwa Filtersoftware) vorzugehen, ist es den ISP nicht zuzumuten, dass sie garantieren sollen, dass keine Gefahr durch die Verbreitung pornografischer Informationen besteht. Im Vergleich zu den ISP spielen die Eltern eine viel wichtigere Rolle, weil die Jugendlichen ja direkt unter der elterlichen Obhut stehen. Tatsächlich bedeutet das sogenannte Vertrauen, dass die ISP eine übermäßige Belastung tragen müssen.

Zusammenfassend lässt sich sagen, dass die ISP im Allgemeinen keine Garantenstellung zur Bewahrung von Rechtsgütern besitzen. Im Einzelfall könnte allerdings die Beschützergarantenstellung eines einzelnen ISP unter bestimmten Voraussetzungen nach der dogmatischen Theorie noch bestehen.

d) Garantenpflichten zur Überwachung von Gefahrenquellen?

Die Überwachungsgarantenstellung bezieht sich auf die Verantwortlichkeit für bestimmte Gefahrenquellen oder Gefahrenherde.[177] In der Literatur gibt es keine einheitliche Lösung für die Quelle dieser Garantenpflichten. Für die Überwachungsga-

---

[176] Vgl. *Kindhäuser*, AT[7], § 36, Rn. 79 ff.; *Rengier*, AT, § 50, Rn. 28 ff.; *Wessels/Beulke*, AT[38], Rn. 720 ff.; *Krey/Esser*, AT[6], Rn. 1141 ff.; *Kühl*, AT, § 18, Rn. 68 ff.

[177] Vgl. *Rengier*, ebenda, § 50, Rn. 42.

rantenstellung wird dabei lediglich eine Reihe von Unterfällen erfasst, beispielsweise Verkehrssicherungspflichten, Pflichten von Wohnungsinhabern, strafrechtliche Produkthaftung, rechtswidriges Verhalten Dritter (Personen als Gefahrenquellen), vorangegangenes gefährdendes Tun oder Übernahme von Sicherungspflichten.[178] Daher ist zu prüfen, bei welchem (Unter-)Fall die ISP einzuordnen sind.

Zuerst ist zu analysieren, ob Personen als Gefahrenquellen betrachtet werden können. Die Nutzer, die die Internetdienste der ISP missbrauchen, könnten theoretisch solche Gefahrenquellen sein. Aber diese Möglichkeit ist auszuschließen, weil aus der Sicht des Zurechnungszusammenhangs die Überwachungsgarantenstellung nur wegen der unmittelbaren Gefahrenquelle anstatt der selbstständigen Handlung Dritter bestehen kann.[179] Darüber hinaus kann im Normalfall nicht zum Schluss gekommen werden, dass jemand für die Straftat Dritter verantwortlich sein soll, weil dies mit dem Prinzip der Eigenverantwortung nicht im Einklang steht. Nur in Ausnahmefällen kann dies in bestimmten Aufsichtsverhältnissen gelten.[180] Da die Nutzer von den ISP unabhängig sind, existiert offensichtlich auch kein Aufsichtsverhältnis zwischen ISP und Nutzern, die Nutzer der Internetdienste können deshalb nicht als Gefahrenquelle verstanden werden.

Zudem wird in der Literatur der Einwand vogebracht, die Datennetze selbst seien die Gefahrenquelle. Demnach „ermöglichen die Datennetze die besonders leichte und besonders schwer kontrollierbare Verbreitung strafbarer Inhalte durch Dritte“, die Beschaffenheit des Datennetzes selbst, nicht der Inhalt der pornografischen Schriften bilde daher die Gefahrenquelle. Nach diesem Verständnis haben „die Netzbetreiber immer eine Garantenstellung für die Verhinderung der Verbreitung oder Zugänglichmachung strafbarer Inhalte in ihrem Datennetz“.[181] Der Generalbundesanwalt vertritt eine ähnliche These, die Besonderheiten des Internets würden das gesteigerte Risiko strukturell in sich tragen, sodass das Netz in einer strafbaren Form der Kommunikation missbraucht werde. Deshalb sei eine Garantenstellung der Netzbetreiber „aus der Überwachung von Gefahrenquellen zu bejahen“.[182]

All diese Auffassungen sollten nicht überschätzt werden, die Schlussfolgerungen sind sehr allgemeiner Natur und übergehen die Unterschiede der vielfältigen ISP. Was ein „Datennetz“ wirklich ist, bleibt unklar; wenn es keine einschränkende Auslegung gibt, kann das „Datennetz“ fast alle Internetdienste umfassen.

---

[178] Vgl. *Kühl*, AT, § 18, Rn. 91 ff.; *Kindhäuser*, AT[7], § 36, Rn. 58 ff.; *Rengier*, ebenda, § 50, Rn. 42 ff.; *Wessels/Beulke*, AT[38], Rn. 722 ff.; *Krey/Esser*, AT[6], Rn. 1162 ff.

[179] Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 58.

[180] Vgl. *Rengier*, AT, § 50, Rn. 62 ff.; *Popp*, Die strafrechtliche Verantwortung von Internet-Providern, S. 134 ff.; *Roxin*, AT II, § 32 A, Rn. 125 ff. Ähnlich vgl. *Finke*, Die strafrechtliche Verantwortung von Internet-Providern, 1998, S. 130.

[181] Vgl. *Popp*, Die strafrechtliche Verantwortung von Internet-Providern, S. 137, 139, 147.

[182] Vgl. Generalbundesanwalt: Haftung eines Access Providers für rechtswidrigen Inhalt, MMR Heft 2, 1998, S. 94 (Generalbundesanwalt, 26.11.1997 – 2 BJS 104/96-4 – 4, 2 BJS 104/96).

Die Funktionen des Datennetzes sowie seine Position in der Gesellschaft werden einseitig interpretiert. Zwar ist es eine Tatsache, dass das Datennetz den böswilligen Nutzern die Möglichkeit eröffnet, eine Straftat zu begehen, aber die hauptsächliche Funktion des Datennetzes wird hier völlig ignoriert. In der heutigen Gesellschaft spielt das Datennetz eine außerordentlich wichtige und positive Rolle. Das Netz verknüpft die ganze Welt miteinander, sodass zahlreiche Daten und Informationen zwischen Menschen schneller, effektiver und bequemer ausgetauscht werden. Es ist zu konstatieren, dass das Datennetz der modernen Informationsgesellschaft zugrunde liegt. Im Vergleich zu der Gefahr, dass das Datennetz vom böswilligen Nutzer missbraucht wird, ist seine allgemeine und grundlegende soziale Nützlichkeit höher zu bewerten. Deshalb sollte die potenzielle Gefahr des Datennetzes nicht überbetont werden, insgesamt ist das Datennetz keineswegs eine Gefahrenquelle für die Gesellschaft.

Ein Werkzeug oder technisches Gerät, das der Allgemeinheit von Nutzen ist, kann möglicherweise auch missbraucht werden, was nicht bedeuten muss, dass es zu den Gefahrenquellen gehört. Eigentlich ist das Datennetz neutral. Ob es eine positive oder negative Rolle spielt, hängt von seinem Gebrauch durch den Nutzer ab. Das bloße Angebot des Datennetzes oder Internets begründet daher keine Überwachungsgarantenstellung der ISP.[183]

Überzeugender ist die Auffassung, die rechtswidrigen Informationen, die unter Kontrolle der ISP stehen, könnten als Gefahrenquelle betrachtet werden.[184] Wenn eine tatsächliche und rechtliche Herrschaft über gefährliche Sachen besteht, könnten sich theoretisch Überwachungsgarantenpflichten daraus ergeben. In diese Kategorie gehören Fälle von „Verkehrssicherungspflichten" und „Wohnungsinhabern", die mit den Konstellationen von ISP vergleichbar sind. So sind etwa Grundstückseigentümer, Kfz-Halter, Tierhalter, Betriebsinhaber usw. für die Sicherheit der gefährlichen Dinge, die unter ihrem Herrschaftsbereich stehen, verantwortlich.[185]

Die Überwachungsgarantenstellung eines Wohnungsinhabers für die üblichen Gefahrenquellen, die von einer Wohnung ausgehen, wird von der herrschenden Meinung anerkannt.[186] Aber ob der Wohnungsinhaber eine Überwachungsgarantenstellung hat, eine Straftat in der von ihm beherrschten Räumlichkeit zu verhindern, bleibt umstritten. In einer alten Entscheidung des BGH wurde diese Überwachungsgarantenstellung des Wohnungsinhabers für die Straftat Dritter angenommen.[187] Da-

---

[183] Vgl. *Finke*, Die strafrechtliche Verantwortung von Internet-Providern, S. 129; *Malek/Popp*, Strafsachen im Internet, S. 32–33, Rn. 116; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 72, Rn. 241 ff.

[184] Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 43 ff.

[185] Vgl. *Rengier*, AT, § 50, Rn. 45 ff.; *Kühl*, AT, § 18, Rn. 106 ff.; *Roxin*, AT II, § 32 A, Rn. 108 ff.

[186] Vgl. *Rengier*, ebenda, § 50, Rn. 54; *Roxin*, ebenda, § 32 A, Rn. 115.

[187] Vgl. BGH NJW 1966, 1763; BGHSt 27, 10.

nach hat der Bundesgerichtshof seine Position geändert, wie er in einem Fall deutlich gemacht hat: Die Überwachungsgarantenstellung des Wohnungsinhabers komme nur in Betracht, „wenn die Wohnung wegen ihrer besonderen Beschaffenheit oder Lage eine Gefahrenquelle darstellt, die er so zu sichern oder zu überwachen hat, dass sie nicht zum Mittel für die leichtere Ausführung von Straftaten gemacht werden kann".[188] Nachfolgende Entscheidungen, in denen die Garantenstellung des Wohnungsinhabers abgelehnt wurde, haben diesen Ansatz aufgenommen.[189] Heute wird gemeinhin die Ansicht vertreten, dass nur die Inhaberschaft einer Wohnung keine Überwachungsgarantenpflicht für die Straftat Dritter erzeugt,[190] wobei die konkrete Bedeutung dieser „besonderen Beschaffenheit oder Lage" offen bleibt.[191]

Wenn die ISP in einer von ihnen kontrollierten und verwalteten Räumlichkeit – ähnlich wie ein Grundstückseigentümer oder Wohnungsinhaber – Informationen von anderen übermitteln oder speichern, könnten sie unter bestimmten Voraussetzungen Garantenpflichten innehaben, um die illegalen Informationen zu sperren oder zu löschen, damit die Sicherheit im Netzwerk garantiert wird. Eine solche Überlegung ignoriert die Unterschiede zwischen den beiden Konstellationen, denn die Herrschaft der ISP über Informationen ist in vielen Aspekten anders als die Kontrolle über ein Grundstück oder eine Wohnung.

Vor allem ist die Menge der Informationen im Netzwerk so riesig, dass die ISP, besonders die Access Provider, mit großen Schwierigkeiten konfrontiert werden, die einzelne illegale Information zu überprüfen, zumal sich der Zustand der übermittelten oder gespeicherten Informationen sehr schnell verändert. Obwohl sich im Allgemeinen diese Informationen in dem von den ISP verwalteten Raum befinden, können sie oft von den Nutzern (Content Provider) verändert oder beeinflusst werden. Außerdem kann eine Reihe technischer Faktoren – etwa wie Firewall, Verschlüsselung –, die Kontrollmöglichkeiten der ISP, wie schon erwähnt, erheblich einschränken.[192] Im Hinblick auf diese technischen Besonderheiten ist die Herrschaft der ISP über fremde Informationen offensichtlich sehr viel schwächer ausgeprägt als die Kontrolle des Wohnungsinhabers über seine Wohnung.[193]

Deshalb besteht höchstens eine strukturelle Ähnlichkeit zwischen dem ISP und dem Wohnungsinhaber bezüglich der Überwachungsgarantenstellung. Die Bestimmung der Garantenstellung von ISP aus der Überwachung von Gefahrenquellen setzt die Typisierung der ISP voraus, weil die verschiedenen Kontrollmöglich-

---

188 Vgl. BGHSt 30, 391(396).

189 Vgl. BGH NJW 1993, 76; BGH NStZ 2010, 221.

190 Vgl. *Roxin*, AT II, § 32 A, Rn. 120; *Rengier*, AT, § 50, Rn. 55.

191 Vgl. *Rengier*, ebenda, § 50, Rn. 57. Nach der Meinung von Sieber ist diese besondere Beschaffenheit mit der gesteigerten Gefährlichkeit verbunden. Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 56.

192 Vgl. *Sieber*, CR Heft 11, 1997, S. 659 ff.

193 Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 56.

keiten der unterschiedlichen ISP berücksichtigt werden müssen. Da Access Provider nur über schwache technische Kontrollmöglichkeiten verfügen, wird die Garantenstellung der Access Provider in der Regel verneint. Im Gegensatz dazu lassen sich unter bestimmten Bedingungen die Garantenstellungen der Caching Provider und Hosting Provider aufgrund ihrer Kontrollmöglichkeiten begründen. Außerdem spielt hier der subjektive Zustand der ISP eine Schlüsselrolle, weil die bestimmten Kenntnisse von rechtswidrigen Handlungen oder Informationen die Kontrollmöglichkeiten der Caching Provider und Hosting Provider erheblich verstärken können. Deswegen sind die Garantenstellungen der Caching Provider und Hosting Provider zu bejahen, wenn sie diese Kenntnisse schon besitzen. Diese Ergebnisse stehen im Allgemeinen mit der einschränkenden Funktion der §§ 7–10 TMG in Einklang, die im Folgenden beschrieben wird.

e) Beschränkende Funktion der §§ 7–10 TMG

So werden nun die Funktionsgrenzen der traditionellen dogmatischen Theorie sichtbar: Sie beruht grundsätzlich auf dem Strafgesetzbuch, in dem allerdings kein spezieller Paragraf für die strafrechtliche Verantwortlichkeit der ISP vorgesehen wird. Außerdem ist der Hauptteil der herrschenden dogmatischen Theorie in einer traditionellen Gesellschaft entstanden und gewachsen, in der sich die komplizierten kriminellen Probleme des Cyberspace noch gar nicht abgezeichnet haben. Deshalb reicht die traditionelle dogmatische Theorie nicht aus, um diese neu auftretenden Probleme zu lösen. Sie bietet nur einen allgemeinen theoretischen Rahmen, der aber durch konkretes und vielfältiges Wissen außerhalb des Strafrechts ergänzt werden muss.

Was die Überwachungsgarantenpflichten der ISP im Netzwerk betrifft, ist es sehr schwierig, nur durch Ableitung oder Analyse der traditionellen dogmatischen Theorie ein zutreffendes Ergebnis zu erzielen. Die Fragen, wann die ISP Maßnahmen zur Sicherung im Netzwerk ergreifen müssen, unter welchen Voraussetzungen die ISP privilegiert werden können, werden schon lange in spezifischen Rechtsbereichen, nicht jedoch im Kernbereich des Strafrechts diskutiert. In dieser Diskussion sind bereits viele Aspekte der Problematik berücksichtigt worden, beispielsweise die Informationsfreiheit, die Sicherheit im Cyberspace, die Kontrollmöglichkeit der ISP, der Zusammenhang zwischen ISP und zuständiger Behörde. Wenn der Umfang der Pflichten von ISP präziser bestimmt werden soll, müssen die spezifischen Gesetze und das entsprechende Wissen über dieses Thema einbezogen werden. Dabei spielt das TMG offensichtlich eine ausschlaggebende Rolle.

Um die Überwachungsgarantenpflichten der ISP mit der Privilegierung der ISP aus dem TMG zu kombinieren, ist eine differenzierte Hypothese zu formulieren. Besonders wichtig ist, dass nach § 7 Abs. 2 TMG die allgemeine Verpflichtung der ISP zur Überwachung der rechtswidrigen Informationen verneint wird. § 7 Abs. 2 TMG lässt den Schluss zu, dass die sogenannte Überwachungsgarantenstellung der ISP für die Gefahrenquelle keineswegs im Allgemeinen bejaht werden soll. Diese

allgemeine Privilegierungsregelung des TMG bedeutet, dass die Garantenpflichten im strafrechtlichen Bereich nur in speziellen Konstellationen mit bestimmten Voraussetzungen ausnahmsweise bestehen könnten.

Wie schon erläutert, soll die Handlung der Content Provider in der Regel als positives Tun betrachtet werden, weil sie bewusst eigene Inhalte anbieten. Die Diskussion über Überwachungsgarantenpflichten der Content Provider ist daher bedeutungslos. Genausowenig kann eine Überwachungsgarantenpflicht für Access Provider grundsätzlich bestimmt werden. Nach § 8 TMG sind Access Provider für die von ihnen übermittelten Informationen nicht verantwortlich, sofern sie die Übermittlung nicht veranlasst, den Adressaten nicht ausgewählt und die übermittelten Informationen nicht ausgesucht oder verändert haben. Unter Berufung auf § 8 TMG kann das Ergebnis lauten, dass Access Provider normalerweise keine Überwachungspflichten haben. Im Gegensatz zu einem Wohnungsinhaber besitzt der Access Provider keine tatsächliche Herrschaft, weil er die Informationen nicht bei sich speichert und ansiedelt. Außerdem sind die übermittelten Informationen so zahlreich, dass die Access Provider gar nicht in der Lage sind, sie zu überprüfen. Der Access Provider bietet dem Nutzer nur einen Zugang zu Informationen, wodurch nicht die Herrschaft über Informationen besteht.

Umstritten ist allerdings, ob die Access Provider mit der Kenntnis von rechtswidrigen Inhalten schon eine Verpflichtung zur Sperrung und Löschung haben. Wie bereits dargestellt, wird die Verpflichtung der Access Provider von der herrschenden Meinung verneint. Aber in Literatur und Rechtsprechung wird auch argumentiert, die Access Provider hätten in einer solchen Konstellation ausnahmsweise eine Sperrverpflichtung.[194] Meines Erachtens basieren die Überwachungsgarantenpflichten hier vor allem auf der objektiven Herrschaft anstatt auf dem subjektiven Willen der Access Provider. Obwohl in dieser Situation die Access Provider die rechtswidrigen Inhalte schon gekannt haben – und damit das subjektive Unrecht bestimmt werden kann –, bleibt die objektiv tatsächliche Kontrollmöglichkeit der Access Provider wegen technischer Gegebenheiten und rechtspolitischer Risiken allerdings sehr begrenzt. Auch wenn die Access Provider in Ausnahmefällen Kontrollmöglichkeiten haben, besitzen sie nur die Herrschaft über den Zugang zu Informationen, nicht über die Gefahrenquelle selbst.[195] Folglich kann eine Überwachungsgarantenstellung hier nicht bejaht werden.

Für die Caching Provider und Hosting Provider könnte die Überwachungsgarantenstellung ausnahmsweise bestehen. Nach §§ 9–10 TMG können Caching Provider und Hosting Provider privilegiert werden, wenn sie keine Kenntnis von den rechtswidrigen Informationen haben oder nach Erlangung dieser Kenntnis die rechtswidrigen Informationen unverzüglich entfernen. Die strafrechtlichen Über-

---

194 Vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 66–67, Rn. 217 ff.

195 Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 45.

wachungsgarantenpflichten der ISP lassen sich hier mithilfe dieser Voraussetzungen für die Privilegierung im TMG strukturieren. Das heißt, nur wenn die ISP konkret Kenntnis von den rechtswidrigen Informationen bekommen haben, könnte die Überwachungsgarantenstellung bestehen.[196] Da die Informationen kurz- oder langzeitig auf den Servern von Caching Providern und Hosting Providern gespeichert werden, haben die Provider eine abstrakte Kontrollmöglichkeit über die Inhalte. Jedoch kann diese noch keine strafrechtliche Überwachungsgarantenstellung erzeugen, da die tatsächliche Herrschaft der Caching Provider und Hosting Provider nicht ausreichend begründet wird.

Zahlreiche Informationen von fremden Nutzern werden in den Servern gespeichert, während der Speicherungszustand dieser Informationen sich sehr schnell verändert, sodass eine Überwachung der gespeicherten Informationen nicht nur zeitaufwendig, sondern auch technisch schwierig ist. Aber wenn die Caching Provider und Hosting Provider konkrete Kenntnis von rechtswidrigen Informationen besitzen, darf vernünftigerweise erwartet werden, dass sie diese illegalen Inhalte unverzüglich sperren oder löschen. Denn in dieser Konstellation ist es technisch nicht schwierig, wirksame Maßnahmen zu ergreifen. Darüber hinaus bürden diese Maßnahmen den Caching Providern und Hosting Providern keine unverhältnismäßigen Belastungen auf, weil der bestimmte Zustand der rechtswidrigen Informationen schon deutlich geworden ist.

Aber die Bedeutung einer unverzüglichen Sperrung oder Löschung ist, wie erwähnt, hier schwierig zu bestimmen. Durch die Einführung des neuen NetzDG wird das Definitionsproblem zu einem großen Teil gelöst. Nach den Neuregelungen des NetzDG müssen die Anbieter sozialer Netzwerke die offensichtlich rechtswidrigen Inhalte innerhalb von 24 Stunden nach Eingang einer Beschwerde entfernen oder den Zugang zu ihnen sperren. Für die anderen rechtswidrigen Inhalte gibt es auch eine Sieben-Tage-Frist. Allerdings gelten diese Regelungen gemäß § 1 NetzDG nur für diejenigen Telemediendiensteanbieter, die mit Gewinnerzielungsabsicht Plattformen (soziale Netzwerke) betreiben und mindestens zwei Millionen Nutzer haben, sie gelten aber nicht automatisch auch für die anderen ISP. Wegen der zunehmenden Verbreitung von Hasskriminalität in sozialen Netzwerken hat der Gesetzgeber mit dem NetzDG strenge Regelungen erlassen. Unverkennbar stellt sich diese verstärkte Regulierung als eine zielgerichtete und selektive Strategie dar. Es wird problematisch sein, diese Regelungen analog auf die anderen ISP anzuwenden.

Zudem ergibt sich eine weitere Fragestellung, nämlich ob die die strafrechtliche Verantwortlichkeit beschränkende Funktion der §§ 7–10 TMG durch die Einführung des NetzDG beeinträchtigt wird. Zunächst ist zu vermerken, dass im NetzDG eine Reihe von neuen Verpflichtungen für die Anbieter sozialer Netzwerke eingeführt wird. Im Allgemeinen sollten die Neuregelungen im NetzDG, welches in vie-

---

[196] Vgl. ebenda, Rn. 49 ff.

lerlei Hinsicht problematisch erscheint, nur als eine Ergänzung oder Konkretisierung für die Verantwortlichkeitsregelungen in TMG angesehen werden.

Die Grundposition des TMG, welche die Verantwortlichkeit der Telemediendiensteanbieter beschränkt, wird nicht dadurch beeinflusst. Außerdem handelt es sich nur um eine Ordnungswidrigkeit, wenn die im NetzDG vorgesehenen Verpflichtungen nicht erfüllt werden. Auf keinen Fall können diese im NetzDG vorgesehenen Verpflichtungen unmittelbar in strafrechtliche Garantenpflichten umgesetzt werden.

E. Vorsatzerfordernisse der strafrechtlichen Verantwortlichkeit

1. Dominanz von Vorsatzdelikten

Aufgrund der Bestimmung von § 15 StGB wird teilweise in der Literatur verneint, dass Fahrlässigkeitsdelikte für die strafrechtliche Verantwortlichkeit der ISP eine erhebliche Relevanz besäßen.[197] Nach § 15 StGB ist vorsätzliches Handeln nur strafbar, wenn nicht das Gesetz fahrlässiges Handeln ausdrücklich mit Strafe bedroht. Wie mehrfach erwähnt, wird die strafrechtliche Verantwortlichkeit der ISP im StGB nicht durch einen selbstständigen Paragrafen spezifisch vorgesehen.

Die Verantwortlichkeit der ISP besteht vor allem für Äußerungs- und Verbreitungsdelikte (zum Beispiel §§ 86 ff., 184 ff. StGB) sowie für Urheberrechtsdelikte (§ 106 ff. UrhG). Aber in diesen Tatbeständen ist Strafbarkeit von Fahrlässigkeit nicht enthalten. Auch die Bestimmungen über Cyberkriminalität im eigentlichen Sinn, etwa §§ 202a, 202b, 202c, 303a, 303b StGB, sehen keine Fahrlässigkeitsdelikte vor. Deshalb kann man feststellen, dass die fahrlässige Handlung der ISP unter normalen Umständen nicht bestraft wird. Einschlägige Fahrlässigkeitsdelikte finden sich allerdings insbesondere im Jugendschutzstrafrecht.[198]

2. Vorsatzformen

In der Rechtstheorie wird der Vorsatz in drei Stufen eingeteilt, nämlich Absicht, direkter Vorsatz (*dolus directus*) und bedingter Vorsatz (*dolus eventualis*). Hier ergibt sich nun die Frage, ob die ISP mit allen drei Vorsatzformen bestraft werden. Unstrittig ist, dass die strafrechtliche Verantwortlichkeit der ISP Absicht und direkten Vorsatz umfassen kann, der bedingte Vorsatz hingegen ist fraglich.

Da die Content Provider im Netzwerk eigene Informationen anbieten, sollen sie nach § 7 TMG für diese Informationen völlig verantwortlich sein. Aus dieser Per-

---

[197] Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 81–82.

[198] Vgl. § 23 JMStV; *Altenhain*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 203.

spektive besteht zwischen ISP und anderen Tätern für die strafrechtliche Verantwortung kein materialer Unterschied, was auch für die Vorsatzformen gilt. Ein bedingter Vorsatz reicht also für die Strafbarkeit der Content Provider aus. Wenn die Content Provider zwar ohne positive Kenntnis sind, aber unter ihren Angeboten mit der Existenz strafbarer Informationen rechnen können und keine entsprechenden Maßnahmen ergreifen, sind sie für dieses Handeln mit bedingtem Vorsatz strafbar.[199]

Für diejenigen ISP, die im Netzwerk keine eigenen Inhalte anbieten und deren Handlungen nur wegen fremder rechtswidriger Inhalte strafbar wären, wird die Sachlage komplizierter. Wie schon erläutert, gilt, dass ein bedingter Vorsatz nicht in der „Kenntnis" der §§ 9–10 TMG subsumiert werden kann.[200] Dies bedeutet, dass die ISP nur mit bedingtem Vorsatz bei rechtswidrigen Inhalten noch nach dem TMG privilegiert werden können. Wenn unter Berufung auf die §§ 9–10 TMG eine einschränkende Auslegung des strafrechtlichen Tatbestands angenommen wird, fällt die Schlussfolgerung, dass ein Eventualvorsatz für die Strafbarkeit der ISP bezüglich der rechtswidrigen Inhalte von Dritten nicht ausreicht, leicht. Im Zusammenhang damit wird eine konkrete Kenntnis vom Zustand der rechtswidrigen Inhalte für die Strafbarkeit der ISP eingefordert,[201] denn aufgrund der riesigen und ständig sich verändernden Datenmenge im Netzwerk ist es für die ISP mit viele Schwierigkeiten verbunden, die strafbaren Informationen zu überprüfen und zu löschen. Die fehlenden Kontrollmöglichkeiten der ISP führen unter normalen Umständen zur Forderung nach einem positiven Vorsatz für die Strafbarkeit der ISP.[202]

Kritischen Meinungen in der Literatur zufolge ist der Umfang des strafrechtlichen Vorsatzes nur von den Merkmalen des objektiven Tatbestandes abhängig. Da in den relevanten Tatbeständen keine detaillierte Beschreibung über den konkreten Zustand der rechtswidrigen Inhalte stehe, solle für den strafrechtlichen Vorsatz eine konkrete Kenntnis über die strafbaren Inhalte unnötig sein. Beispielsweise reiche es für den Vorsatz der Verbreitung kinderpornografischer Schriften aus, dass die ISP mit der Existenz irgendwelcher Speicherungen der Gattung Kinderpornografie gerechnet hätten. Weiter wird die Ansicht vertreten, eine einschränkende Auslegung sei systemwidrig und nicht aus der Privilegierungsregelung im TDG abzuleiten, da die besonderen Schwierigkeiten und Belastungen zur Überprüfung der rechtswidri-

---

[199] Vgl. *Malek/Popp*, Strafsachen im Internet, S. 39, Rn. 141; *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 84.

[200] Vgl. *Malek/Popp*, Strafsachen im Internet, S. 25, Rn. 88; *Bleisteiner*, Rechtliche Verantwortlichkeit im Internet, S. 180; *Sieber*, Verantwortlichkeit im Internet, S. 166–167, Rn. 336; *Spindler*, NJW Heft 48, 1997, 3196; Gersdorf/Paal-*Paal*, § 10 TMG, Rn. 24; *Müller-Broich*, Telemediengesetz, § 10 Rn. 4.

[201] Vgl. *Malek/Popp*, Strafsachen im Internet, S. 39, Rn. 143; *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 84; *Vassilaki*, MMR Heft 12, 1998, 634; *Moritz*, CR Heft 8, 1998, 507; *Pelz*, ZUM Heft 7, 1998, 534.

[202] Vgl. *Pelz*, wistra Heft 2, 1999, 59; *ders.,* ZUM Heft 7, 1998, 534; *Sieber*, CR Heft 11, 1997, S. 654.

gen Informationen zum Erfordernis der objektiven Möglichkeit eines Eingreifens gehörten.[203] Die Berücksichtigung dieser Schwierigkeiten sei somit nicht im Vorsatz auf subjektiver Ebene einzubeziehen.

Meines Erachtens trifft diese Kritik nicht zu. Auch wenn natürlich in den relevanten Tatbeständen keine detaillierte Beschreibung über den Zustand der illegalen Inhalte existiert, kann eine bloß formale Auslegung des Tatbestands auf dieser Grundlage nicht angenommen werden. Der Tatbestand ist ein grundlegender gesetzlicher Rahmen, der durch dogmatische Theorie und materiale Begründung ergänzt werden muss. Mittels der traditionellen dogmatischen Theorie allein können wir keine endgültige Aussage bezüglich der strafrechtlichen Verantwortlichkeit treffen, weil die spezifischen Überlegungen hinsichtlich Technik und Rechtspolitik dabei nicht berücksichtigt werden. Deshalb müssen die Privilegierungsregelungen und die entsprechenden theoretischen Kenntnisse aus dem TMG hier als nützliche Ergänzung einbezogen werden.

Darüber hinaus ist auch keine Systemwidrigkeit zu erkennen. Natürlich stammen die besonderen Schwierigkeiten und Belastungen aus der objektiven Möglichkeit des Eingreifens. Aber diese objektiv begrenzte Möglichkeit hat nicht nur auf die Auslegung der objektiven Merkmale des Tatbestands, sondern auch auf den Vorsatz Auswirkungen. Die besonderen Schwierigkeiten und Belastungen zur Überprüfung der rechtswidrigen Inhalte stehen mit dem bedingten Vorsatz nicht im Einklang. Deshalb soll der Vorsatz der ISP hier restriktiv interpretiert werden.

3. Unrechtsbewusstsein und Verbotsirrtum

Nach § 17 StGB handelt ein Täter ohne Schuld, wenn er kein Unrechtsbewusstsein hat und dieser Irrtum unvermeidbar ist. Interessant ist die Überlegung, ob und inwieweit die ISP wegen fehlenden Unrechtsbewusstseins einem Verbotsirrtum unterliegen. Aus der Literatur lässt sich das Argument entnehmen, dass ein unvermeidbarer Verbotsirrtum der ISP in der Regel deswegen nicht bestehe, weil die ISP Fachkräfte – wie Rechtsanwälte – konsultieren können. Mit dieser Möglichkeit, sich fachlich zu erkundigen, sei der Verbotsirrtum grundsätzlich vermeidbar.[204] Da in der heutigen Informationsgesellschaft der Abruf von Daten und Informationen immer bequemer geworden ist, besteht für ISP auch fast immer eine Gelegenheit, sich über die rechtlichen Risiken sachkundig zu machen und vorzubeugen.

In einem ganz bestimmten Kontext – gemeint sind unterschiedliche Rechtsordnungen verschiedener Länder – könnte unvermeidbarer Verbotsirrtum ausnahmsweise existieren. Wegen der weltweit bestehenden großen Unterschiede in Politik,

---

[203] Vgl. *Popp*, Die strafrechtliche Verantwortung von Internet-Providern, S. 161.

[204] Vgl. *Malek/Popp*, Strafsachen im Internet, S. 39, Rn. 142; *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 86; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 77, Rn. 258.

Wirtschaft, Kultur und sogar Religion ist es oft sehr schwierig für die ISP, fremde, ausländische Rechtsordnungen genau zu kennen. So ist etwa der Spielraum der Meinungsfreiheit in den USA größer als in Deutschland.[205] Oder Sanktionen gegen pornografische Inhalte fallen in China wesentlich schärfer aus als in Deutschland, um ein weiteres Beispiel zu nennen. Die Definition pornografischer Inhalte sowie der Umfang der Bestrafung in China unterscheiden sich stark von der deutschen Rechtslage. Angesichts dieser Unterschiede in den Rechtsordnungen, die für die ISP schwer festzustellen sind, können wir von den ISP nicht allzu viele Pflichten erwarten.

Außerdem wird in der Literatur die Meinung vertreten, bei einigen Delikten könne aufgrund ihres Blankettcharakters ein Verbotsirrtum existieren.[206] Dieser abstrakte Tatbestand muss durch weitere Rechtsordnungen außerhalb des Strafrechts ergänzt werden, sonst wäre die Anwendung dieses Tatbestands unmöglich. Aber diese außerstrafrechtlichen Gesetze, die oft aus uneinheitlichen Quellen stammen, sind manchmal nicht einfach zu finden und zu erfassen. In besonderer Konstellation könnte ein unvermeidbarer Verbotsirrtum noch möglich sein. Im Allgemeinen ist ein Verbotsirrtum hier jedoch allenfalls in Extremfällen anzuerkennen, hauptsächlich geht es ja in der vorliegenden Arbeit um Berufspflichten der Provider. Die in einem bestimmten beruflichen Gebiet tätigen Personen sollten sich mit den entsprechenden Regelungen vertraut machen und auch professionelle Hilfe heranziehen.

F. Einordnung der Handlungen als Täterschaft oder Teilnahme

1. Abgrenzung von Täterschaft und Teilnahme

Es gibt viele unterschiedliche Lösungsansätze für die Abgrenzung von Täterschaft und Teilnahme, in der Literatur existieren zum Beispiel die subjektive Theorie, die formal-objektive Theorie und die materiell-objektive Theorie.

In der Rechtsprechung ist die subjektive Theorie vorherrschend, die subjektive Einstellung der Beteiligten ist das entscheidende Kriterium für die Abgrenzung von Täterschaft und Teilnahme. Jedoch ist anzumerken, dass es in der subjektiven Theorie auch unterschiedliche Ausprägungen gibt. Im *Badewannen*-Fall[207] und im *Staschynskij*-Fall[208] manifestiert sich die sogenannte extrem-subjektive Theorie, nach der die Abgrenzung von Täterschaft und Teilnahme in Abhängigkeit von dem Willen und den Interessen der Beteiligten vorgenommen wird, während nicht berücksichtigt wird, wer den gesetzlichen Tatbestand voll verwirklicht hat. Inzwi-

---

205 Vgl. *Hilgendorf/Valerius*, ebenda, S. 77, Rn. 257.

206 Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 87.

207 Vgl. RGSt 74, 84.

208 Vgl. BGHSt 18, 87.

schen berücksichtigt die Rechtsprechung allerdings zunehmend nicht nur den Willen zur Begehung einer eigenen Tat, sondern – als Reaktion auf die unten genannte Lehre von *Roxin* – auch den Willen zur Tatherrschaft sowie teilweise auch die Tatherrschaft selbst.[209]

Die Schwachstellen der subjektiven Theorie sind so offenkundig, dass sie in der Literatur von den meisten Wissenschaftlern kritisiert werden, zum einen, weil die Abgrenzung von Täterschaft und Teilnahme vom Tatbestand getrennt wird, was den Grundsatz der Gesetzmäßigkeit bedrohen dürfte, zum anderen, weil der Wille der Beteiligten sehr schwer zu bestimmen und festzustellen ist, was zu Rechtsunsicherheit führt.[210] Vor allem die sogenannte formal-objektive Theorie, die besagt, dass der Täter den Tatbestand unmittelbar verwirklicht, während der Teilnehmer den Tatbestand mittelbar verwirklicht, wird deswegen im Schrifttum heute als überholt betrachtet.[211] Offensichtlich steht dieser Ansatz mit der mittelbaren Täterschaft nicht im Einklang.[212] In der Literatur dominiert daher inzwischen die von *Roxin* entwickelte materiell-objektive Theorie oder Tatherrschaftslehre. Demnach ist derjenige der Täter, der durch seinen maßgeblichen Einfluss als Schlüsselfigur oder Zentralgestalt den Tatbestand verwirklicht. Teilnehmer sind denjenigen, die nur als Randfigur die Begehung der Tat fördern oder veranlassen.[213]

2. Einordnung der ISP als Täter oder Teilnehmer

a) Kriterien für die Einordnung

Die Literatur formuliert auf der Grundlage der subjektiven und der objektiven Theorie auch unterschiedliche Kriterien für die Einordnung der Handlung von ISP. Nach der subjektiven Theorie gilt der sogenannte Täterwille als das maßgebliche Kriterium für die Einordnung der Handlung. Die Bestimmung des Täterwillens rückt die Frage in den Mittelpunkt, was der Wille der ISP ist und ob die ISP ein Interesse am Taterfolg besitzen.[214] Diese Auffassung ist jedoch zu kritisieren, denn das Interesse am Taterfolg der ISP kann nicht mit der Inkaufnahme der rechtswidrigen Taten gleichgesetzt werden. Außerdem führt der Wille der ISP allein nicht

---

[209] Vgl. *Wessels/Beulke*, AT[38], Rn. 515; BGHSt 35, 347; BGHSt 40, 218.

[210] Vgl. *Wessels/Beulke*, AT[38], Rn. 517; Laufhütte/Rissing-van Saan/Tiedemann-*Schünemann*, § 25 Rn. 33; *Rengier*, AT, § 41 Rn. 7 ff.

[211] Vgl. *Rengier*, ebenda, § 41 Rn. 7 ff.

[212] Vgl. *Kindhäuser*, AT[7], § 38, Rn. 38; *Wessels/Beulke*, AT[38], Rn. 511.

[213] Vgl. *Wessels/Beulke*, AT[38], Rn. 513; *Roxin*, AT II, § 25, Rn. 27.

[214] Vgl. *Popp*, Die strafrechtliche Verantwortung von Internet-Providern, S. 165–166; Generalbundesanwalt, Haftung eines Access Providers für rechtswidrigen Inhalt, MMR Heft 2, 1998, 94 (Generalbundesanwalt, 26.11.1997 – 2 BJS 104/96-4 – 4, 2 BJS 104/96); AG München: *CompuServe*-Urteil, MMR Heft 8, 1998, 430 (AG München, Urteil vom 28.05.1998 – 8340 Ds 465 Js 173158/95).

direkt zu dem Täter.[215] Offensichtlich kann die subjektive Theorie in diesem speziellen Bereich auch keine Legitimität beanspruchen. Die subjektive Theorie ist für die Einordnung der Handlung von ISP als Täterschaft oder Teilnahme von Nachteil. Deshalb ist eine materiell-objektive Theorie bezüglich dieser Problematik angebracht.

b) Einordnung der Handlung der ISP

Für die Einordnung der Handlung von ISP als Täterschaft oder Teilnahme gibt es keine einheitliche Lösung, die für alle Fälle gilt. Denn die ISP spielen verschiedene Rollen in unterschiedlichen Konstellationen. Es ist unstrittig, dass die Content Provider in der Regel als Täter betrachtet werden sollen, soweit die angebotenen Inhalte strafbar sind.[216] Für die anderen ISP kann die Einordnung nur im Einzelfall bestimmt werden. In der Regel sind die ISP als Teilnehmer zu betrachten, denn das Kriterium für die Tatherrschaft ist schwierig zu erfüllen: Die ISP verwirklichen den Tatbestand nicht als Schlüsselfigur und sie können die strafbaren Inhalte tatsächlich nicht kontrollieren. Da die ISP in den meisten Fällen nur den Nutzern sozial nützliche Internetdienste anbieten, sollen sie grundsätzlich als Gehilfe (Beihelfer) eingestuft werden. Es wird auch darauf hingewiesen, dass die ISP nur Beihilfe leisten können, wenn der Erfolg nicht in tatbestandsspezifischer Weise von den ISP herbeigeführt wird.[217] Aber in speziellen Fällen könnten die ISP auch Täter sein. Wenn sie absichtlich mit anderen Straftätern zusammenarbeiten, um Straftaten zu begehen, und sie den Tatbestand direkt verwirklichen, sind sie als Täter oder Mittäter zu betrachten.

c) Beteiligung durch Unterlassen

Die Beteiligung durch Unterlassen ist ein hoch umstrittenes Thema, weil das zentrale Problem in der Frage liegt, ob beim Unterlassen das allgemeine Kriterium für die Abgrenzung von Täter und Teilnehmer noch gilt.[218] Eine Ansicht stellt darauf ab, dass das allgemeine Kriterium bei Unterlassen ganz entfällt. Da die Möglichkeit zur Erfolgsabwendung der Unterlassung zugrunde liegt, hat der Unterlassende tatsächlich immer die Chance, den Erfolg einer Tat zu verhindern. Mit anderen Worten, der Unterlassende besitzt von vornherein die Tatherrschaft.[219]

---

[215] Vgl. *Malek/Popp*, Strafsachen im Internet, S. 36–37, Rn. 130.

[216] Vgl. ebenda, S. 36, Rn. 129; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 74, Rn. 246.

[217] Vgl. *Popp*, Die strafrechtliche Verantwortung von Internet-Providern, S. 163–164.

[218] Vgl. *Popp*, Die strafrechtliche Verantwortung von Internet-Providern, S. 164 ff.; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 73, Rn. 245 ff.

[219] Vgl. *Roxin*, Täterschaft und Tatherrschaft, S. 459 ff.; *ders.,* AT II, § 31 VII, Rn. 140 ff.; *Stratenwerth/Kuhlen*, AT § 14 Rn. 20.

Laut einer gegenteiligen Auffassung kann der Garant nur Gehilfe statt Täter sein, denn der Unterlassende kann neben dem Täter keine Tatherrschaft haben.[220] Es wird auch vertreten, dass die Tatherrschaftslehre und die subjektive Theorie in dieser Situation keine Anwendung finden, weil die zentrale Rolle und der subjektive Zustand des Straftäters nicht geprüft werden können.[221] Eine dritte Ansicht glaubt, dass die Teilnahme auch durch Unterlassen geleistet werden kann, wenn der Gehilfe eine Garantenpflicht übernehmen soll.[222] Außerdem gibt es auch noch einen Mittelweg, der Beschützergarant soll Täter sein, während der Überwachungsgarant als Gehilfe zu bewerten ist.[223] Bei Unterlassung besteht meines Erachtens noch eine Teilnehmerschaft. Obwohl der Unterlassende die Möglichkeit zur Erfolgsabwendung hat, kann diese Möglichkeit nicht direkt mit der tatsächlichen Tatherrschaft gleichgestellt werden. Denn der Unterlassende hat nur eine mögliche Tatherrschaft, während eine tatsächliche Tatherrschaft für die Täterschaft unentbehrlich ist. Nur wenn diese mögliche Tatherrschaft bei der Unterlassung realistisch verwirklicht wird, besteht die Täterschaft.

IV. Gesetzlich nicht geregelte Typen der ISP und ihre Verantwortlichkeit

A. Peer-to-Peer-Netzwerke

1. Einordnung der Betreiber von Peer-to-Peer-Netzwerken

Ein Peer-to-Peer-Netzwerk ist eine umstrittene Technologie. Sie wird mit dem neuen Netzwerkarchitekturprinzip „Gleichgestellte zu Gleichgestellten" anstatt des traditionellen Client-Server-Prinzips begründet.[224] Das heißt, im Peer-to-Peer-Netzwerk wird nicht unterschieden, wer Service-Provider und wer Service-Nutzer ist. Jeder Teilnehmer eines Peer-to-Peer-Netzwerks ist in der Lage, Daten zu empfangen, zu speichern und auch zu senden.[225] Solange das gleiche Peer-to-Peer-Netzwerk beide, Provider wie Nutzer, verbindet, können sie Daten und Informationen gleichberechtigt teilen und austauschen.[226]

---

220 Vgl. *Kühl*, AT, § 20, Rn. 229 ff.; *Rengier*, AT, § 51, Rn. 15 ff.

221 Vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 73, Rn. 245.

222 Vgl. *Jescheck/Weigend*, AT[5], § 64 III 5; *Wessels/Beulke*, AT[38], Rn. 734; *Kindhäuser*, AT[7], § 42, Rn. 24; *Baumann/Weber/Mitsch/Eisele*, AT, § 26, Rn. 110.

223 Vgl. *Krey/Esser*, AT[6], Rn. 1181 ff.

224 Vgl. *Lang*, Filesharing und Strafrecht, S. 12.

225 *Brinkel*, Filesharing, S. 15; *Schoder/Fischbach*, in: Schoder/Fischbach/Teichmann, Peer-to-Peer, S. 4.

226 *Xie, Xiren* [Hrsg.]: Computer-Netzwerk, S. 10.

Das Peer-to-Peer-Netzwerk ist ausgesprochen populär, weil es keinen zentralen Medienserver erfordert. Es gibt auch keinerlei zentrale Instanz, die die Kommunikation verzögert oder filtert.[227] Das Peer-to-Peer-Netzwerk kann sich selbst einstellen: Je mehr Downloads stattfinden, desto größer ist die Kapazität für Uploads. Deshalb bieten diese Netzwerke immer genug Speichergröße und benötigen keine spezielle Netzwerkinfrastruktur.[228] Alle Informationen und Daten im Peer-to-Peer-Netzwerk werden zwischen normalen Internetnutzern übermittelt. Dies vermittelt den Eindruck, als gäbe es sehr viele (manchmal sogar bis zu Millionen) Medienserver, die Informationen und Daten für andere Nutzer bieten.[229]

Das erste Beispiel für ein Peer-to-Peer-Filesharing tauchte im Dezember 1987 auf. Damals begründete *Wayne Bell* das WWWIVnet. Im Juli 1999 entwarf *Ian Clarke* das Freenet (eine dezentrale und zensur-resistente verteilte Datenspeicherung), um im Peer-to-Peer-Netzwerk die Meinungsfreiheit unter dem Schutz der Anonymität zu gewährleisten.[230] In den folgenden Jahren wurde das Peer-to-Peer-Netzwerk mit der Entstehung der berühmten *Napster*-Software immer attraktiver.[231] Schließlich wurde *Napster* wegen Urheberrechtsverletzungen geschlossen, da circa 500.000 Nutzer Raubkopien von Musikdateien durch *Napster* tauschten.[232]

Es liegt auf der Hand, dass Bereitstellung und Nutzung von Peer-to-Peer-Filesharings im juristischen Bereich äußerst umstritten sind. Seit seiner Entstehung hat sich das Peer-to-Peer-Netzwerk kontinuierlich und schnell weiterentwickelt, die entsprechende Technologie wird heutzutage in vielen Medien und Kommunikationsbereichen angewendet. Zunächst müssen daher die Typen des Peer-to-Peer-Netzwerks weiter unterschieden werden, weil die diversen Peer-to-Peer-Netzwerke im Gesetz unterschiedlich bewertet werden.

Nach der herrschenden Meinung im netzwerktechnischen Bereich lässt sich das Peer-to-Peer-Netzwerk in folgende Typen gliedern:[233]

1. Unstrukturiertes Peer-to-Peer

a) Erste Generation

aa) zentrales Peer-to-Peer (Beispiel Napster): zentrale Entität ist notwendig für Erbringung der Dienste; zentrale Entität ist eine Art von Index/Gruppendatenbank;

bb) reines Peer-to-Peer (Beispiel: Gnutella 0.4/ Freenet): jede Terminalentität kann ohne Verlust der Funktionalität entfernt werden; keine zentrale Entität.

---

227 *Brinkel*, Filesharing, S. 16; *Schoder/Fischbach*, in: Schoder/Fischbach/Teichmann, Peer-to-Peer, S. 4.

228 *Tanenbaum/Wetherall*, Computer Networks, S. 579.

229 *Xie, Xiren* [Hrsg.]: Computer-Netzwerk, S. 373.

230 Siehe *Oram* (ed.), Peer-to-Peer, Preface viii.

231 Siehe *Forouzan/Mosharraf*, Computer Networks, S. 66.

232 Siehe *Tanenbaum/Wetherall*, Computer Networks, S. 578.

233 Siehe *Steinmetz/Wehrle* (ed.), Peer-to-Peer Systems and Applications, S. 36 ff.

b) Zweite Generation hybrides Peer-to-Peer (Beispiel: Gnutella 0.6/ JXTA):
jede Terminalentität kann ohne Verlust der Funktionalität entfernt werden; dynamische zentrale Entität.

2. Strukturiertes Peer-to-Peer: Verteilte Hash-Tabellen (DHT):

jede Terminalentität kann ohne Verlust der Funktionalität entfernt werden; keine zentrale Entität; Verbindungen im Overlay sind „fixiert".

Auch wenn heute dezentrale Peer-to-Peer-Netzwerke Mainstream-Modelle wie Bit Torrent usw. geworden sind, bleibt die Frage nach der Verantwortlichkeit der Betreiber der Peer-to-Peer-Netzwerke in der Rechtslehre immer noch sehr umstritten.[234] Die Verantwortlichkeit hängt vor allem auch vom jeweiligen Typ des Peer-to-Peer-Netzwerkes ab: Bei dezentralen Peer-to-Peer-Netzwerken bieten die Betreiber den Nutzern eine Software, mit der die Nutzer ihre Dateien frei miteinander tauschen. In einem zentralen Peer-to-Peer-Netzwerk dagegen besitzen die Betreiber zusätzlich einen Server, in dem zahlreiche Informationen über die Nutzer und ihre Dateien gespeichert werden. Auf diese Weise werden allerdings auch die Urheberrechte von Werken stark verletzt, weil in einem solchen Netzwerk oft viele Raubkopien verbreitet werden. Manchmal werden auch strafbare Inhalte wie Kinderpornografie durch diesen Netzwerk-Typ verbreitet.

Nach den deutschen Regelungen wird der Betreiber des Peer-to-Peer-Netzwerks in der Literatur als Access Provider eingeordnet. Der Betreiber des zentralen Peer-to-Peer-Netzwerks fällt grundsätzlich unter § 2 Abs. 2 Nr. 3 TDG 2001 a.F., weil er die bereits bestehenden Leitungen des Internets nutzt, um ein vom Internet abgrenzbares virtuelles Netzwerk zu schaffen.[235] Nach der Konvergenz der Medien[236] und Einführung des TMG kann das Peer-to-Peer-Netzwerk durch § 1 Abs. 1 TMG reguliert werden. Aber diese Einordnung ist nicht ganz ohne Tücken, eine reine Zugangsvermittlung des klassischen Access Providers ist nicht als Teledienst im TMG einzustufen, sondern fällt unter § 3 Abs. 24 Telekommunikationsgesetz (TKG).[237] Es ist schwierig, den Unterschied zwischen Telemediendiensten im TMG und Telekommunikationsdiensten im TKG – besonders im Hinblick auf den Access Provider – zu bestimmen. Der herrschenden Meinung einer funktionsbezogenen Abgrenzung ist durchaus zuzustimmen, genauer gesagt, betrifft das TMG die inhaltlichen Aspekte des Datenverkehrs, während das TKG sich mit technischen Fragen beschäftigt.[238] Nach diesem Unterscheidungsmerkmal kann

---

[234] Zum Beispiel sind die Stellungnahmen von Gerichten zu der Verantwortlichkeit der P2P-Betreiber in einer Reihe von berühmten Fällen, etwa wie *Napster*, *KaZaA*, *Grokster* und *Winny*, unterschiedlich. Vgl. *Yang Caixia*, Politik und Recht Heft 3, 2016, 44 ff.

[235] Vgl. *Lang*, Filesharing und Strafrecht, S. 114.

[236] Vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 16, Rn. 53 ff.

[237] Vgl. *Spindler/Schmitz/Geis*, TDG-Kommentar, § 2, Rn. 25.

[238] Vgl. *Sieber*, Verantwortlichkeit im Internet, S. 132–133, Rn. 267; *Spindler/Schmitz/Geis*, ebenda, § 2, Rn. 22; *Gercke/Brunst*, Praxishandbuch Internetstrafrecht, S. 241, Rn. 574.

der Betreiber des Peer-to-Peer-Netzwerks ohne Zweifel als Access Provider angesehen werden, da er sich auf die Inhalte im Netzwerk bezieht. Außerdem „ermöglichen die zentralen P2P-Dienste nicht allein den Zugang zu fremden Diensten, sondern erbringen selbst einen inhaltsbezogenen Service".[239]

Darüber hinaus wird die Auffassung vertreten, dass die Nutzer im Peer-to-Peer-Netzwerk eigene Teledienste nicht dauerhaft anbieten würden. Die dezentralen Peer-to-Peer-Netzwerke wie Gnutella böten weder eigene noch die Nutzung fremder Teledienste, deshalb seien die Betreiber des Peer-to-Peer-Netzwerks nicht als „Diensteanbieter" zu betrachten.[240] Dieser Kritik ist jedoch nicht zu folgen, denn sie nimmt eine zu strenge gesetzliche Auslegung an, sodass der rechtliche Geltungsbereich des TMG zu sehr eingeengt wird. Nach normalem Verständnis können wir sagen, dass der Betreiber des Peer-to-Peer-Netzwerks eigene oder fremde Teledienste zur Nutzung bereithält oder zumindest Zugang zur Nutzung vermittelt.

In der ausländischen Rechtsprechung – etwa im Fall von *Napster* – wurde außerdem die Einstufung des Betreibers von Peer-to-Peer-Netzwerken als Access Provider zurückgewiesen. *Napster* hatte sich einst auf § 512a DMCA berufen, der sich auf die Beschränkung der Verantwortlichkeit von Access Providern bezieht. Der District Court lehnte diese Begründung ab, weil die urheberrechtsrelevanten Daten nicht durch den *Napster*-Server geleitet worden waren.[241] Nach dem Wortlaut des § 512a DMCA ist die Durchleitung von Datenmaterial eine Voraussetzung für die Privilegierung der Access Provider.[242]

Im deutschen Rechtsrahmen besteht dieses Problem nicht. Zwar werden die urheberrechtsrelevanten Daten direkt zwischen den Nutzern anstatt im Kommunikationsnetz des Betreibers ausgetauscht, aber die Handlung von Betreibern kann noch unter § 8 Abs. 1 TMG fallen, da der Betreiber des Peer-to-Peer-Netzwerks den Zugang zur Nutzung dieser Daten vermittelt hat.

Ein Problem, das in der Literatur nicht ausreichend diskutiert wird, betrifft allerdings noch die Frage, ob der Betreiber eines Peer-to-Peer-Netzwerks als eine andere Art der ISP neben Access Providern einzuordnen wäre. Meines Erachtens kann der Betreiber eines dezentralen Peer-to-Peer-Netzwerks wegen seiner Nichteinmischung in den Austausch der Dateien in der Regel nur als Access Provider betrachtet werden. Für den Betreiber eines zentralen Peer-to-Peer-Netzwerks hingegen gibt es weitere Möglichkeiten. Da in einem zentralen Peer-to-Peer-System oft eine Suchfunktion enthalten ist, könnte der Betreiber des zentralen Peer-to-Peer-Netzwerks auch als ein Suchmaschinenbetreiber einzuordnen sein. Im *Napster*-Fall

---

239 *Brinkel*, Filesharing, S. 339.

240 Vgl. *Spindler/Schmitz/Geis*, TDG–Kommentar, § 3, Rn. 15, § 9, Rn. 16.

241 Vgl. *Frey*, ZUM Heft 6, 2001, 473.

242 In diesem Paragraf gibt es die Formulierung von „material through a system or network". Siehe § 512a DMCA 1998.

wurde die Einordnung des Betreibers als sogenanntes *Information Location Tool* anerkannt, obwohl die entsprechende Privilegierung schließlich abgelehnt wurde.[243] Nach § 512d DMCA sind die Betreiber der *Information Location Tools* nicht für ihre Services verantwortlich, sofern

1) sie keine tatsächliche Kenntnis von dem rechtsverletzenden Material oder der Tätigkeit haben;
2) mangels dieser tatsächlichen Kenntnis ihnen keine Tatsache oder Umstände bekannt sind, aus denen die rechtsverletzende Tätigkeit offensichtlich wird, oder
3) sie unverzüglich handeln, um das Material zu entfernen oder den Zugang zu ihm zu sperren, sobald sie diese Kenntnis oder das Bewusstsein erlangt haben.

Dies zeigt deutlich, dass die Voraussetzungen der Privilegierung für den Betreiber des *Information Location Tool* fast denen des Hosting Providers gleichen. Aber im TMG gibt es keine selbstständige Privilegierungsregelung für die Verantwortlichkeit der Betreiber der *Information Location Tools* (nämlich der Suchmaschinenbetreiber). Deshalb ist es auch höchst umstritten, wie die Verantwortlichkeit der Suchmaschinenbetreiber zu bestimmen ist.

Darüber hinaus könnte der Betreiber eines zentralen Peer-to-Peer-Netzwerks im deutschen Rechtsrahmen auch analog als Hosting Provider angesehen werden, weil in einem zentralen Peer-to-Peer-Netzwerk viele Informationen über den Lagerort und das Inhaltsverzeichnis der auszutauschenden Dateien im Server des Betreibers gespeichert werden. Obwohl die Betreiber rechtswidrige Inhalte nicht unmittelbar speichern, hängen die relativen Informationen im zentralen Server des Betreibers eng mit den rechtswidrigen Dateien zusammen. Nur durch die Verbindung mit diesen Informationen im Server des Betreibers können die Nutzer miteinander die zahlreichen Dateien im Peer-to-Peer-Netzwerk flüssig austauschen, weswegen diese relativen Informationen über die Positionen oder die Verzeichnisse der Dateien in bestimmten Situationen auch zur Gefahrenquelle werden könnten. Im Gegensatz zu den Access Providern haben die Betreiber der zentralen Peer-to-Peer-Netzwerke hier vollständige Kontrolle über diese Informationen. Obwohl die Betreiber der zentralen Peer-to-Peer-Netzwerke keine typischen Hosting Provider sind, besitzen sie aber ähnliche Eigenschaften wie Hosting Provider.

2. Privilegien der Betreiber von Peer-to-Peer-Netzwerken

Der Betreiber eines Peer-to-Peer-Netzwerks ist kein gesetzlicher Typ der ISP, kann jedoch als Access Provider betrachtet werden. Aber die Frage, ob ein Betreiber eines Peer-to-Peer-Netzwerks wie beispielsweise *Napster* die Privilegierung von § 8 TMG (sowie § 9 a.F. TDG 2001) in Anspruch nehmen kann, ist äußerst umstritten.

---

[243] Vgl. *Frey*, ZUM Heft 6, 2001, 474.

Erstens muss nach dem Wortlaut des § 8 Abs. 1 Satz 1 Nr. 1–3 TMG diskutiert werden, ob der Betreiber des Peer-to-Peer-Netzwerks die Übermittlung veranlasst, den Adressaten der übermittelten Informationen ausgewählt und die übermittelten Informationen ausgewählt oder verändert hat. Da der Betreiber des Peer-to-Peer-Netzwerks eigentlich nur eine Software für die Nutzer anbietet und das Peer-to-Peer-Netzwerk vielmehr selbstständig von den Nutzern betrieben wird, liegt der Schluss nahe, dass der Betreiber einer Peer-to-Peer-Software (wie *Napster*) offensichtlich weder Adressaten ausgewählt noch die übermittelten Informationen ausgewählt oder verändert hat.[244] Das „Veranlassen" hat viele Bedeutungen, die zu Missverständnissen führen könnten. So liegt eine zu diskutierende Problematik darin, ob auch eine mittelbare Veranlassung unter § 8 Abs. 1 Satz 1 Nr. 1 TMG fällt. In der Literatur wird die Meinung vertreten, dass nur die unmittelbare Veranlassung erfasst werden könne, weil der Übermittlungsvorgang der Informationen vielmehr von den herunterladenden Nutzern selbst initiiert werde.[245]

Zweitens ist das Verhältnis zwischen dem Betreiber des Peer-to-Peer-Netzwerks und den Nutzern detailliert zu analysieren, da die Privilegien von § 8 Abs. 1 Satz 1 TMG keine Anwendung finden, wenn der Betreiber des Peer-to-Peer-Netzwerks absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.

In der Literatur gibt es zwei ganz gegensätzliche Auffassungen hierüber. Die einen sind der Meinung, dass „der Betreiber des Peer-to-Peer-Netzwerks wie Napster sein File-Sharing-Angebot den Usern zum Zwecke des urheberrechtsverletzenden Austauschs von Musikdateien zur Verfügung gestellt hat"[246] und der Betreiber des zentralen Peer-to-Peer-Netzwerks mit seinem zentralen Indexserver als unverzichtbarer Mittler zwischen den einzelnen Teilnehmern fungiere.[247] Daher könne der Betreiber des Peer-to-Peer-Netzwerks offensichtlich nicht privilegiert werden. Die anderen vertreten dagegen den Standpunkt, das aufgrund der umfassenden Haftungsprivilegierung des § 9 a.F. TDG 2001 (nämlich § 8 TMG) grob leichtfertige oder bedingt vorsätzliche Verhalten der ISP reiche für den Ausschluss der Privilegien nicht aus. Wegen des Mangels an ernsthafter Absicht solle deshalb Napster noch privilegiert werden.[248] Eigentlich muss die Diskussion bei der Unterteilung der Betreiber des Peer-to-Peer-Netzwerks in verschiedene Kategorien ansetzen, weil die subjektiven Zustände der Betreiber unterschiedlich sind.

---

[244] Vgl. *Freiwald*, Die private Vervielfältigung im digitalen Kontext am Beispiel des Filesharing, S. 165–166.

[245] Vgl. *Brinkel*, Filesharing, S. 341.

[246] Vgl. *Frey*, ZUM Heft 6, 2001, S. 476.

[247] Vgl. *Freiwald*, Die private Vervielfältigung im digitalen Kontext am Beispiel des Filesharing, S. 166.

[248] Vgl. *Brinkel*, Filesharing, S. 342.

In einem zentralen Peer-to-Peer-Netzwerk ist eine absichtliche Zusammenarbeit zwischen Betreiber und Nutzern vorstellbar: Obwohl die Dateien nur zwischen den Nutzern übermittelt werden, ist ein zentraler Server für diesen Vorgang unentbehrlich. Wenn ein Nutzer sich im Peer-to-Peer-Netzwerk einloggen will, muss er sich zuerst am zentralen Server, der der Verbindung zwischen den anfordernden und den anbietenden Knoten dient, registrieren.[249] Durch die Registrierung des Nutzers kann der Betreiber des zentralen Peer-to-Peer-Netzwerks normalerweise erfahren, dass es illegale Inhalte im Peer-to-Peer-Netzwerk gibt. Wenn der Betreiber solche erkennt und er diesen Service weiter für die Nutzer bereitstellt, kann man daraus ableiten, dass er absichtlich mit einem rechtswidrige Handlungen begehenden Nutzer zusammengearbeitet hat. Deshalb kann der Betreiber des zentralen Peer-to-Peer-Netzwerks nicht nach § 8 Abs. 1 Satz 1 TMG privilegiert werden.

Betrachtet man die Betreiber der zentralen Peer-to-Peer-Netzwerke wegen ihrer Kontrolle des zentralen Servers sowie der dabei gespeicherten Informationen analog als Hosting Provider, sind die Betreiber nach § 9 TMG für den rechtswidrigen Austausch der Dateien nicht verantwortlich, sofern sie bestimmte Voraussetzungen für die Privilegierung erfüllen. In einem dezentralen Peer-to-Peer-Netzwerk verhält es sich ganz anders, dort gibt es natürlich keinen zentralen Server. Demnach werden die Inhalte ohne Kontrolle und Hilfe vonseiten des Betreibers direkt zwischen den Nutzern übermittelt. In dieser Konstellation hat der Betreiber in der Regel keine Kenntnis von illegalen Informationen, deshalb soll er nach dem § 8 Abs. 1 Satz 1 TMG privilegiert werden.

Drittens muss der Aspekt der Kontrollmöglichkeit des Peer-to-Peer-Netzwerk-Betreibers in die Betrachtung einbezogen werden. Zwar hat der Betreiber die Voraussetzungen des § 8 TMG erfüllt, aber verfügt er tatsächlich über Kontrollmöglichkeiten der übermittelten Inhalte wie beispielsweise bei Schul-PCs oder bei Betreibern von Internet-Cafés? Für diese Situation muss eine teleologische Reduktion zum TMG vertreten werden. Der Grund für die teleologische Reduktion liegt darin, dass die Privilegien sich eigentlich auf die Unmöglichkeit der Datenkontrolle richten.[250]

Es erhebt sich daher die Frage, ob ein Betreiber des Peer-to-Peer-Netzwerks faktische Kontrollmöglichkeiten hat. Wenn die Frage zu bejahen ist, müssen wir uns weiter entscheiden, ob die Privilegien des Betreibers nach § 8 TMG entfallen. So wird die Meinung vertreten, dass § 9 a.F. TDG 2001 (§ 8 TMG) bewusst solche Kontrollmöglichkeiten ausklammere und die teleologische Reduktion zu Privilegien des Betreibers den Tatbestand des § 9 a.F. TDG 2001 „ausfransen“ ließe.[251] Diese Ausführung klingt zunächst ziemlich einleuchtend, weil nach dem Wortlaut

---

[249] Siehe *Steinmetz/Wehrle* (ed.), Peer-to-Peer Systems and Applications, S. 38.

[250] Vgl. *Spindler/Schmitz/Geis*, TDG-Kommentar, § 9, Rn. 11.

[251] Vgl. *Brinkel*, Filesharing, S. 343.

von § 8 TMG keine – wie oben genannte – materiale Überlegung zur Kontrollmöglichkeit gefordert wird, bei näherem Hinsehen scheint sie jedoch lückenhaft. Denn diese formale Auffassung lässt das normative Ziel des Gesetzes außer Acht, sodass das eigentliche Kriterium für die Auslegung verloren geht. Aus kriminalpolitischer Sicht könnte diese Auffassung sogar dazu führen, dass böswillige Betreiber die vom Gesetz bestimmte Haftung durch eine spezielle technische Konstruktion umgehen. Die Kontrollmöglichkeit bildet nicht nur die Grundlage der Gesetzgebung, sondern auch ein maßgebendes Prinzip für die Auslegung des TMG. Deshalb ist die formale Auslegung hier zu verneinen.

3. Strafrechtliche Verantwortlichkeit der Betreiber von Peer-to-Peer-Netzwerken

In der Praxis geht es sich auch um die strafrechtliche Verantwortlichkeit der Betreiber der Peer-to-Peer-Netzwerke. Wenn zwischen den Nutzern strafbare Informationen durch das Peer-to-Peer-Netzwerk ausgetauscht werden, könnten nicht nur die böswilligen, Informationen hoch- oder herunterladenden Nutzer, sondern auch die Betreiber der Peer-to-Peer-Netzwerke strafbar sein.

In diesem Zusammenhang sind die Tatbestände der sogenannten Verbreitungsdelikte (wie § 184 StGB Verbreitung pornografischer Schriften) und der Äußerungsdelikte (wie § 185 StGB) von Bedeutung. Am meisten diskutiert wird § 106 UrhG, nämlich die unerlaubte Verwertung urheberrechtlich geschützter Werke, weil zahlreiche im Peer-to-Peer-Netzwerk ausgetauschte Dateien das Urheberrecht des Berechtigten verletzt haben.

Die Diskussion über die strafrechtliche Verantwortlichkeit der Betreiber der Peer-to-Peer-Netzwerke ist wegen der technischen Komplexität nicht einfach. Wie bereits erwähnt, gibt es viele unterschiedliche Typen von Peer-to-Peer-Netzwerken, die verschiedene Funktionen und interne Strukturen aufweisen. Deshalb setzt die Forschung hier die Unterscheidung der Peer-to-Peer-Netzwerke voraus. Im Allgemeinen ist die Unterscheidung zwischen zentralem und dezentralem Peer-to-Peer-Netzwerk sinnvoll, da die Kontrollmöglichkeiten der Betreiber in beiden Systemen deutlich verschieden sind.

a) Betreiber zentraler Peer-to-Peer-Netzwerke

In einem zentralen Peer-to-Peer-Netzwerk gibt es einen zentralen Server, in dem ein Katalog über den Peer-Knoten und die angebotenen Inhalte existiert. In dieser Konstellation haben die Betreiber eine starke Kontrollmöglichkeit, deshalb ist das strafrechtliche Risiko für sie auch relativ hoch. Die herrschende Meinung sieht die Strafbarkeit der Betreiber der zentralen Peer-to-Peer-Netzwerke in der Rolle des Gehilfen anstatt des Täters. In der Regel scheidet die Möglichkeit der Einordnung

der Betreiber als Täter aus.[252] Der wichtigste Grund liegt darin, dass der Tatbestand der Verletzung der Urheberrechte nicht von den Betreibern beherrscht wird. Nur in sehr speziellen Ausnahmefällen könnte die Strafbarkeit der Betreiber als Täter dennoch bestehen: Wenn die Betreiber eine besondere Verpflichtung zur Kontrolle der rechtswidrigen Informationen haben, könnten sie wegen der Verletzung der Verpflichtung als Täter bestraft werden.

In der Literatur wird die Handlung von Betreibern zentraler Peer-to-Peer-Netzwerke in zwei Typen unterteilt, nämlich in die Bereitstellung der benötigten Software und in den Betrieb zentraler Server sowie darauf eingerichteter Suchmaschinen oder Peer-Cache-Speicher.[253] In einem zentralen Peer-to-Peer-Netzwerk werden die beiden Services normalerweise von dem gleichen ISP betrieben. Die bloße Bereitstellung der Software wird von Rechtswissenschaftlern als neutrale Handlung betrachtet.[254] Denn obwohl die Bereitstellung der Software die Verletzung von Urheberrechten objektiv fördern kann, steht auf der anderen Seite der alltägliche, neutrale und sozial nützliche Charakter dieser Handlung im Vordergrund.

Außerdem ergibt sich diese Schlussfolgerung von allein, wenn man sich auf die Privilegierungsregelung bezieht. Da die Software Nutzern den Zugang zum Peer-to-Peer-Netzwerk anbietet, sollen die Anbieter der Software als Access Provider angesehen werden. Nach § 8 TMG sind die Access Provider für fremde Informationen nicht verantwortlich, sofern sie eine bestimmte Übermittlung nicht veranlasst, den Adressaten der übermittelten Informationen nicht ausgewählt und die übermittelten Informationen nicht ausgewählt oder verändert haben. Die bloße Bereitstellung der Software für das Peer-to-Peer-Netzwerk greift nicht in die Durchleitung der Informationen ein, weshalb diese Handlung die Voraussetzungen für die Privilegierung erfüllen kann.

Die Bestimmung der strafrechtlichen Verantwortlichkeit der Betreiber der zentralen Server sowie relevanter Suchmaschinen und Peer-Cache-Speichern ist andererseits sehr umstritten. *Heghmanns* meint, die Betreiber hätten objektiv kausale Beihilfehandlungen zu den Straftaten der anbietenden Peers geleistet, während ihnen die Förderung einer fremden Straftat auch genau bewusst gewesen sei. Für die Bejahung des Beihilfevorsatzes sei es nicht nötig, dass die Betreiber die Personen oder die Einzelheiten der Taten kennten, weil sie hier nur so viel wie die Forderung einer abstrakten Subsumtion des § 106 UrhG zu wissen bräuchten. Zudem reiche der bedingte Vorsatz hier aus.[255]

---

[252] Vgl. *Lang*, Filesharing und Strafrecht, S. 111; *Heghmanns*, MMR Heft 1, 2004, 15; vgl. Wissenschaftliche Dienste des Bundestags, Rechtliche Reaktionsmöglichkeiten auf „Internetpiraterie", WD 10 – 3000/094-12, S. 20.

[253] Vgl. *Heghmanns*, MMR Heft 1, 2004, 16.

[254] Vgl. ebenda, 17.

[255] Vgl. ebenda, 16 ff.

Diese Position erweist sich allerdings als unzutreffend. Auf der einen Seite wird in der Literatur kritisch angemerkt, dass der Betrieb des Servers – ähnlich wie die Bereitstellung der Software – die gleiche Möglichkeit für eine sozial nützliche Anwendung eröffnet.[256] Mit anderen Worten: Die Betreiber des Servers sind nicht unbedingt wegen seiner technischen Besonderheiten strafbar.

Auf der anderen Seite ist die Einschränkung der Verantwortlichkeit von ISP nach dem TMG vernachlässigt worden.[257] Nach der herrschenden Meinung bezieht das Problem sich hier auf die Privilegierungsregelung für die Access Provider.[258] Aber meines Erachtens sind die Betreiber des zentralen Servers, wie oben erläutert, einem Hosting Provider vergleichbar, weil die relevanten Informationen über die von Peers angebotenen Dateien auch zentral gespeichert werden. Deshalb muss die Möglichkeit der Anwendung von § 10 TMG sorgfältig geprüft werden.

Wie schon erläutert, kann ein bedingter Vorsatz von der rechtswidrigen Handlung oder Information die Verantwortlichkeit der Hosting Provider für fremde Informationen nach herrschender Meinung noch nicht ausreichend begründen. Da das TMG nach dem Willen des Gesetzgebers für alle Rechtsgebiete gilt, soll die zuvor genannte Schlussfolgerung über die Beschränkung der Verantwortlichkeit der Hosting Provider auch in der Auslegung des strafrechtlichen Tatbestands aufgenommen werden.

In einem zentralen Peer-to-Peer-Netzwerk gibt es zahlreiche Nutzer, die vielfältige Dateien miteinander austauschen. Natürlich besteht die Möglichkeit, dass in dem riesigen Datenfluss einige rechtswidrige Dateien existieren; dieses abstrakte Wissen oder eine Vermutung allein vermag die Strafbarkeit der Betreiber noch nicht begründen, weil die Betreiber der Peer-to-Peer-Netzwerke bezüglich ihrer strafrechtlichen Verantwortlichkeit nicht überfordert werden sollen. Hier bezieht die Verantwortlichkeit der ISP sich nicht nur auf eine abstrakte Subsumtion des Tatbestands. Die technischen Schwierigkeiten der Betreiber, die vernünftige Berücksichtigung der Betriebskosten sowie die Balance zwischen Rechten und Pflichten von Betreibern sollen auch in der einschränkenden Auslegung des Tatbestands in Betracht gezogen werden.

Unter Berufung auf die Privilegierungsregelung im TMG ist folglich festzustellen, dass die Betreiber der Peer-to-Peer-Netzwerke nur, wenn sie schon bestimmte und konkrete Kenntnis von der rechtswidrigen Handlung oder den Informationen besessen haben, aufgrund ihrer Dienstleistungen zur Unterstützung der Urheberrechtsverletzung als Beihelfer bestraft werden können.[259]

---

[256] Vgl. *Lang*, Filesharing und Strafrecht, S. 113.

[257] Vgl. Wissenschaftliche Dienste des Bundestags, Rechtliche Reaktionsmöglichkeiten auf „Internetpiraterie", WD 10 – 3000/094-12, S. 21.

[258] Nach einer Mindermeinung handelt es sich jedoch um die Privilegierungsregelungen für die Caching Provider. Vgl. *Heghmanns*, MMR Heft 1, 2004, 15.

[259] Vgl. *Lang*, Filesharing und Strafrecht, S. 113.

b) Betreiber dezentraler Peer-to-Peer-Netzwerke

Obwohl es viele Varianten von dezentralen Peer-to-Peer-Netzwerken gibt,[260] haben sie alle die Gemeinsamkeit, dass in der Regel kein zentraler Server im Netzwerk besteht, sodass sich die Handlung der Betreiber überhaupt als bloße Softwarelieferung darstellt. Theoretisch könnte der Betreiber als Gehilfe strafbar sein, weil er objektiv gesehen Unterstützung für die Rechtsverletzung bietet. Doch die Strafbarkeit des Betreibers kann aus mehreren Gründen verneint werden:

Erstens kann die Theorie der neutralen Handlung – wie zuvor beschrieben – hier Anwendung finden.[261] Im Allgemeinen dient die Software dem berechtigten Austausch der Dateien, das heißt, die Bereitstellung der Software für ein Peer-to-Peer-Netzwerk hat einen neutralen und sozial nützlichen Charakter. Sofern die Software nicht absichtlich zur Unterstützung einer Urheberrechtsverletzung entwickelt wird, bleibt die Handlung des Betreibers neutral. Zweitens ist die Strafbarkeit des Betreibers auch dann zu verneinen, wenn wir uns auf die Privilegierungsregelung im TMG beziehen. Der Anbieter der Software stellt Nutzern nur den Zugang zu einem Peer-to-Peer-Netzwerk zur Verfügung. Mit anderen Worten, bei den Betreibern der dezentralen Peer-to-Peer-Netzwerke werden keine Inhalte gespeichert. Deshalb soll der bloße Anbieter einer Software für Peer-to-Peer-Netzwerke als Access Provider angesehen werden. Entsprechend kommt die Privilegierungsregelung für Access Provider, nämlich § 8 TMG, hier zum Zuge. Drittens haben die Betreiber der dezentralen Peer-to-Peer-Netzwerke eben gerade wegen ihrer dezentralen Struktur grundsätzlich keine ausreichende Kontrollmöglichkeit über die zahlreichen und sich schnell verändernden Daten.[262] Deswegen soll die Strafbarkeit der Betreiber der dezentralen Peer-to-Peer-Netzwerke aus einer materialen Perspektive abgelehnt werden.

Die Strafbarkeit der Betreiber der dezentralen Peer-to-Peer-Netzwerke besteht allenfalls, wenn die Beweise ausreichend belegen können, dass die Betreiber absichtlich mit den Nutzern zusammenarbeiten, um rechtswidrige Handlungen zu begehen. In der Literatur wird behauptet, dass die Strafbarkeit der Beihilfe begründet werden kann, wenn die Funktion der angebotenen Software zum Tausch der urheberrechtlich geschützten Dateien besonders herausgestellt wird.[263]

---

[260] Siehe *Steinmetz/Wehrle* (ed.), Peer-to-Peer Systems and Applications, S. 36 ff.

[261] Vgl. *Heghmanns*, MMR Heft 1, 2004, 17; Wissenschaftliche Dienste des Bundestags, Rechtliche Reaktionsmöglichkeiten auf „Internetpiraterie", WD 10 – 3000/094-12, S. 22.

[262] Vgl. *Frey*, ZUM Heft 6, 2001, 466.

[263] Vgl. *Heghmanns*, MMR Heft 1, 2004, 17; Wissenschaftliche Dienste des Bundestags, Rechtliche Reaktionsmöglichkeiten auf „Internetpiraterie", WD 10 – 3000/094-12, S. 22.

B. Hyperlinks

1. Einordnung von Hyperlinks

Das Web besteht aus einer immensen Anzahl von Inhalten, die weltweit verteilt werden und in Form von Webseiten existieren. Auf jeder Webseite können Hyperlinks, die wiederum auf andere Webseiten hinweisen, gesetzt werden. Durch die Hyperlinks werden die weltweit verteilten Webseiten miteinander verknüpft.[264] Mit der Entwicklung der Netzwerktechnik haben sich unterschiedliche Arten von Hyperlinks herausgebildet. Deshalb ist es notwendig, zuerst eine konkrete Differenzierung vorzunehmen: Aus technischer Sicht lassen sich in der Regel drei verschiedene Arten von Hyperlinks unterscheiden, nämlich „Surface Links", „Deep Links" und „Inline-Links". Die „Surface Links" verweisen auf eine Homepage (Eingangsseite), während die „Deep Links" direkt auf bestimmte Dateien auf einer Unterseite verweisen. Unter einem „Inline-Link" wird ein Einbetten von fremden Dokumenten, die man oft nicht erkennen kann, verstanden.[265]

Darüber hinaus wird in der Literatur eine Unterscheidung nach den einzelnen Linkebenen vertreten. Die Links können in Links auf erster Ebene und Links auf tieferer Ebene aufgeteilt werden.[266]

Die rechtliche Einordnung von Hyperlinks ist schwierig und umstritten. Erstens hält der Service-Provider keine eigenen Informationen bereit, weswegen das bloße Setzen eines Hyperlinks nicht unter § 7 Abs. 1 TMG fallen kann. Zweitens können die §§ 9–10 TMG keine Anwendung finden, weil der Setzer eines Hyperlinks keine Inhalte für andere gespeichert oder zwischengespeichert hat und der Hyperlink selbst nur auf Inhalte hinweist. Drittens entspricht die Setzung eines Hyperlinks nicht ganz dem Prinzip einer Durchleitung von Informationen, denn „ein Teledienstanbieter, der bewusst und gewollt einen Hyperlink auf eine fremde Webseite setzt, tut jedoch erheblich mehr, als lediglich den Zugang zur Nutzung eines Angebots zu vermitteln".[267] Deswegen kann der Setzer auch nicht durch § 8 TMG privilegiert werden. Diese Einordnungsschwierigkeiten von Hyperlinks sind ein wichtiger Grund für den heftigen Streit um die Verantwortlichkeit für Hyperlinks.

2. Verantwortlichkeit für Hyperlinks

Die Verantwortlichkeit für Hyperlinks wird seit langer Zeit äußerst kontrovers diskutiert. Das erste Problem liegt darin, dass nach der herrschenden theoretischen Meinung und dem Willen des Gesetzgebers die Privilegien in den §§ 8–10 TMG

---

264 Vgl. *Tanenbaum/Wetherall*, Computer Networks, S. 500.

265 Vgl. *Ernst/Vassilaki/Wiebe*, Hyperlinks, S. 2 f., Rn. 4–6; *Boese*, Strafrechtliche Verantwortlichkeit für Verweisungen durch Links im Internet, S. 40 ff.

266 Vgl. *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht, S. 91–92, Rn. 334.

267 *Waldenberger*, MMR Heft 3, 1998, 128.

für Hyperlinks nicht anwendbar sind.[268] Diese Problematik ist aus einem gesetzgebenden und aus einem theoretischen Blickwinkel zu betrachten.

a) Auffassung des Gesetzgebers

Im Entstehungsprozess der ECRL wurde heftig darüber debattiert, ob eine entsprechende Regelung für Hyperlinks in die Richtlinie aufgenommen werden sollte, die EU-Kommission verzichtete aber auf diesen Vorschlag.[269] Nach § 21 Abs. 2 ECRL wurde das Problem der Verantwortlichkeit für Hyperlinks ausgespart.[270] Im Gesetzgebungsverfahren zur neuen Fassung des TDG 2001 wurde auch ein entsprechender Vorschlag erhoben, um einen ausgeglichenen Haftungsmaßstab zu schaffen.[271] Schließlich wurde dieser Entwurf ebenfalls abgelehnt. Nach Ansicht der Bundesregierung sei die damit verbundene Frage so komplex, dass es besser wäre, „zunächst die weitere Entwicklung in Wissenschaft und Rechtsprechung zu verfolgen und eine generelle Regelung möglichst auf europäischer Ebene anzustreben".[272] Offensichtlich ist die Positionierung des Gesetzgebers zur neuen Regelung für die Verantwortlichkeit der Hyperlinks als zurückhaltend zu bezeichnen. Jedoch sind die Auffassungen in Literatur und Rechtsprechung völlig gegensätzlich.

b) Keine analoge Anwendung der §§ 7–10 TMG?

Die einen sind der Meinung, dass bei der Behandlung des Problems der Hyperlinks der Gesetzgeber seine verneinende Position deutlich formuliert hat. Genauer gesagt, habe der Gesetzgeber deutlich gemacht, dass „es ohne spezielle Beschränkungen der zivil- oder strafrechtlichen Verantwortlichkeit für Hyperlinks bei der Haftung nach allgemeinen Vorschriften bleibe".[273] Die Analogie zu den §§ 7–10 TMG sei deshalb nicht berechtigt.[274] Dagegen sind die anderen der Auffassung, dass trotz der Abwesenheit einer speziellen Regelung für Hyperlinks eine Analogie zu den §§ 7–10 TMG (§§ 8–11 a.F. TDG 2001, § 5 a.F. TDG 1997) angewendet werden könne.[275] Es gebe eine erhebliche Regelungslücke im § 5 a.F. TDG 1997,

---

[268] Vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 69–70, Rn. 232.

[269] Vgl. *Spindler/Schmitz/Geis*, TDG-Kommentar, Vor § 8, Rn. 32; *Spindler*, MMR Heft 4, 1999, 204.

[270] Vgl. BGH: Zugang pornografischer Internetangebote über ein unzureichendes AVS – ueber18.de, MMR Heft 6, 2008, 402 (BGH, Urteil vom 18.10.2007 – I ZR 102/05).

[271] Vgl. BT-Drs. 14/7370, S. 3; BT-Drs. 14/6098, S. 34; *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht, S. 91, Rn. 332. Nach dem TMG gab es auch einen ähnlichen gesetzlichen Entwurf. Vgl. BT-Drs. 16/11173, S. 3.

[272] Vgl. BT-Drs. 14/6098, S. 37.

[273] Vgl. BT-Drs. 14/6098, S. 37.

[274] Vgl. *Spindler/Schmitz/Geis*, TDG-Kommentar, Vor § 8, Rn. 33.

[275] Vgl. *Waldenberger*, MMR Heft 3, 1998, 128; über die strafrechtliche Verantwortlichkeit vgl. *Koch*, MMR Heft 12, 1999, 707.

denn „der § 5 a.F. TDG 1997 will die Verantwortlichkeit der Teledienstanbieter im Rahmen des Möglichen umfassend bestimmen“, während diese Regelungen keine direkte Anwendung für die Setzung der Hyperlinks fänden.[276] Es wird auch die Ansicht vertreten, die Möglichkeit einer analogen Anwendung zu den §§ 7–10 TMG sei durch die ECRL und EGG nicht negativ vorentschieden, denn „eine bewusste Lücke kann, gemessen an den der Gesamtregelung zugrundeliegenden Wertungen, planwidrig sein“.[277] Das heißt, obwohl der Gesetzgeber bewusst (sogar absichtlich) keine speziellen Regelungen für Hyperlinks erlassen hat, gibt es noch eine Regelungslücke.

Die erste, formale Begründung gibt meines Erachtens Anlass zu Bedenken. Denn dass der Gesetzgeber damals keine spezielle Regelung für Hyperlinks erlassen hat, lag an dem Umstand, dass er noch keine eindeutige und zutreffende Lösung für die Verantwortlichkeit für Hyperlinks angesichts der Komplexität der Problematik gefunden hatte, weniger daran, dass der Setzer des Hyperlinks in geeigneter Konstellation nicht privilegiert werden sollte. Deshalb ist der Wille des Gesetzgebers in dieser Situation auf das Ziel des Gesetzes in einer materialen Weise zurückzuführen. In einem Entwurf wurde richtigerweise vorgeschlagen, dass verhindert werden sollte, dass die „Diensteanbieter aus Sorge um einen unangemessen hohen Haftungsmaßstab auf das Angebot von Hyperlinks verzichten“.[278] Da außerdem der Setzer einen mit der Webseite verbundenen Netzwerkservice bietet, spielt er eine ganz ähnliche Rolle wie ein normaler Diensteanbieter. In Anbetracht dessen führt es tatsächlich zu einer wesentlichen Ungleichheit, wenn der Setzer des Hyperlinks nicht durch eine analoge Anwendung zu den §§ 7–10 TMG privilegiert werden darf.

Aus der Perspektive der Auslegungsmethode ist die oben genannte formale Auffassung zu verneinen. In Literatur und Rechtsprechung gibt es seit Langem einen Streit zwischen der subjektiven Auslegungstheorie, die auf dem Willen des Gesetzgebers beruht, und der objektiven Auslegungstheorie, die von der objektiven und sich wandelnden Bedeutung des Gesetzes abhängt. Gesetzeslücken zu schließen ist von der objektiven Theorie aus leichter zu bewerkstelligen, deswegen hat sich diese allmählich durchgesetzt.[279] Umgekehrt bedeutet das aber nicht, dass der subjektive Wille des Gesetzgebers nicht mehr wichtig ist. Es wäre besser, einen Kompromiss oder eine Synthese zwischen subjektiver und objektiver Auslegungstheorie zu finden.[280] Heutzutage ist der Hyperlink ein üblicher und umfassender Netzwerkservice und seine technische Anwendung ist ausgereift.

---

[276] Vgl. *Waldenberger*, ebenda, 128.

[277] *Sieber/Höfinger*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 100–101; *Sieber/Liesching*, MMR-Beilage Heft 8, 2007, S. 10.

[278] Vgl. BT-Drs. 14/7370, S. 3.

[279] Vgl. *Jescheck/Weigend*, AT[5], § 17 IV 2.

[280] Vgl. *Jescheck/Weigend*, AT[5], § 17 IV 2; *Roxin*, AT[4], § 5 E Rn. 32; *Jakobs*, AT[2], 4. Abschn. 22.

In dieser Situation sollten die Setzer der Hyperlinks genauso wie die anderen Service-Provider privilegiert werden, wenn sie die entsprechenden Voraussetzungen erfüllen. Sie haben einen Anspruch darauf, rechtlich gleich behandelt zu werden. Dieses objektive Verständnis ist gegenüber der formalen subjektiven Auslegung zu bevorzugen. Die materiale Auslegung gerät zudem nicht mit der subjektiven Auslegung in Konflikt, weil der Gesetzgeber nicht gegen diese materiale Ansicht ist.

c) Welche analoge Anwendung?

Nachdem schon die Legitimität der analogen Anwendung zum TMG begründet worden ist, bleibt die Frage, welcher Paragraf des TMG angewendet werden kann, weiterhin klärungsbedürftig. Bevor man dieses Problem weiter erforscht, müssen zunächst verschiedene Arten von Hyperlinks differenziert werden. Technisch gesehen sind die automatisch erzeugten Hyperlinks von den manuell gesetzten Hyperlinks abzugrenzen,[281] was zu unterschiedlichen gesetzlichen Bewertungen führt. Grundsätzlich ist die analoge Anwendung zum TMG für die manuell gesetzten Hyperlinks zu diskutieren.

Für diese Problematik gibt es viele gegensätzliche Auffassungen in der Literatur. Die erste Ansicht besagt, dass nur die automatisch erzeugten Hyperlinks durch die analoge Anwendung privilegiert werden könnten, während die Haftung der manuell gesetzten Hyperlinks nach allgemeinen Haftungsgrundsätzen bestimmt werde.[282] Eine solche Differenzierung stellt übermäßige Anforderungen an die analoge Anwendung, obwohl der Verfasser die Unterscheidung zwischen dem Setzer und den normalen ISP befürwortet.

Der zweite Ansatz betont, dass der Setzer eines Links auf seinem System keine Inhalte bereithalte, sondern nur einen Zugang zu Inhalten für andere vermittele.[283] Deshalb solle der Betreiber ähnlich wie ein Access Provider betrachtet werden. Diese Auffassung wirkt auf den ersten Blick plausibel, denn aus technischer Perspektive verknüpft der Setzer eines Links die Nutzer nur mit dem Content Provider und bietet keine eigenen Inhalte an. Bei näherer Betrachtung erweist sie sich als unzutreffend, weil deren Vertreter übersehen haben, dass der Betreiber die verlinkten Inhalte bewusst oder absichtlich ausgewählt hat.[284] Das bedeutet, dass der Hyperlinksetzer offensichtlich eine größere Kontrollmöglichkeit über sein Angebot als der Access Provider besitzt. Eine analoge Anwendung des § 8 TMG würde auch

---

[281] Vgl. *Sieber/Höfinger*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 102.

[282] Vgl. ebenda, Rn. 102, 106.

[283] Vgl. *Pelz*, ZUM Heft 7, 1998, 533; *Koch*, CR Heft 4, 1997, 198.

[284] Vgl. *Flechsig/Gabel*, CR Heft 6, 1998, 354; *Sieber/Höfinger*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 103; *Spindler/Schmitz/Geis*, TDG-Kommentar, Vor § 8, Rn. 37; *Koch*, MMR Heft 12, 1999, 707; *Spindler*, NJW Heft 13, 2002, 924; *Bettinger/Freytag*, CR Heft 9, 1998, 549; Spindler, NJW Heft 48, 1997, 3198; *Ernst/Vassilaki/Wiebe*, Hyperlinks, Rn. 136 ff; Joecks/Miebach-*Hörnle*, § 184, Rn. 48.

dazu führen, dass die Hyperlinks wegen der übermäßigen Privilegien von kriminellen ISP missbraucht werden.

Die dritte Meinung argumentiert, dass „der Link zum Teil des eigenen Angebots wird", wenn „der Betreiber den Hyperlink willentlich und gezielt in die Homepage-Gestaltung miteinbezieht";[285] § 7 Abs. 1 TMG könne analoge Anwendung finden. Diese Auffassung ist jedoch zu verneinen, da das Setzen eines Hyperlinks nicht ohne Weiteres mit dem Anbieten eigener Inhalte gleichgestellt werden kann.[286] Die Links weisen grundsätzlich nur auf die von Dritten angebotenen Inhalte hin, halten aber keine eigenen Inhalte bereit. Nach dieser Ansicht wird der Hyperlinksetzer in Bezug auf die gesetzliche Haftung überfordert.

Die vierte These hält bei der Verwendung von Hyperlinks eine analoge Anwendung von TMG-Paragrafen für die Verantwortlichkeit des Hosting Providers für gerechtfertigt.[287] Laut dieser Auffassung kann der Hyperlinksetzer somit analog als ein Hosting Provider betrachtet und nach § 10 TMG privilegiert werden. Die Kritik an dieser Meinung wiederum konzentriert sich überhaupt auf den Unterschied zwischen Hyperlinks und Host-Service. Auf der einen Seite wird Inhalt auf einem Server nicht über einen längeren Zeitraum vorgehalten, deshalb liegt kein Bereithalten bei der Hyperlinksetzung vor.[288] Auf der anderen Seite wählt der Linksetzer die Inhalte aus, weshalb er in der Regel Kenntnis über die Inhalte hat. Der Hosting Provider hingegen weiß grundsätzlich nicht, welche Inhalte auf seinem Server gespeichert werden.[289] Darüber hinaus wird auch argumentiert, dass der Linksetzer die Inhalte nicht beeinflussen bzw. wie ein Hosting Provider löschen könne.[290]

Die fünfte Anschauung neigt zu einer differenzierenden Lösung. Es wird danach unterschieden, ob ein Bereithalten eigener oder fremder Informationen bei einer Verweisung auf erster Ebene vorliegt, während es eine Zugangsvermittlung zu fremden Informationen grundsätzlich nur auf den tieferen Ebenen gibt.[291] Begründet wird dies damit, dass „die Inhalte auf den tieferen Link-Ebenen regelmäßig außerhalb des Herrschaftsbereichs des Anbieters liegen und von diesem nicht gezielt gelöscht oder unterdrückt werden können".[292] Außerdem können eigene Inhalte beim Einrichten von Links vorliegen, wenn „sich jemand beim Setzen eines Links die Inhalte fremder Seiten dadurch zu eigen macht, dass er sich mit diesen

---

285 Vgl. *Flechsig/Gabel*, CR Heft 6, 1998, 354.

286 Vgl. *Spindler/Schmitz/Geis*, TDG-Kommentar, Vor § 8, Rn. 37.

287 Vgl. *Waldenberger*, MMR Heft 3, 1998, 129; *Koch*, MMR Heft 12, 1999, 707; *Sieber*, Verantwortlichkeit im Internet, S. 161, Rn. 326.

288 Vgl. *Pelz*, ZUM Heft 7, 1998, 533.

289 Vgl. *Spindler/Schmitz/Geis*, TDG-Kommentar, Vor § 8, Rn. 37.

290 Vgl. ebenda, S. 147; *Spindler*, CR Heft 12, 1998, 752.

291 Vgl. *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht, S. 91–92, Rn. 334.

292 Vgl. *Sieber*, Verantwortlichkeit im Internet, S. 163–164, Rn. 330.

Inhalten identifiziert und dafür Verantwortung übernehmen will".[293] Meines Erachtens ist diese differenzierende Meinung zu bejahen, da der Verfasser den großen Unterschieden zwischen Hyperlinks Rechnung trägt. Angesichts dieser Heterogenität ist es unmöglich, einen für alle Konstellationen allgemeingültigen Schluss zu ziehen.

d) Befürwortung einer differenzierenden Lösung

Eine fundierte Unterscheidung zwischen Hyperlinks nach objektiven und subjektiven Aspekten legt den Grundstein für eine gerechte Behandlung der Verantwortlichkeit für Hyperlinks. Unter objektiven Gesichtspunkten haben einige Hyperlinksetzer unmittelbare Kontrolle über das Bereithalten der Inhalte, während andere Betreiber nur indirekt und begrenzt Einfluss auf Inhalte nehmen. Aus subjektivem Blickwinkel werden einige Hyperlinks auf Webseiten deswegen errichtet, damit sich der Hyperlinksetzer die verlinkten Inhalte zu eigen machen kann. Hingegen richten andere Hyperlinksetzer die Hyperlinks nur ein, um die fremden Inhalte zu vermitteln. Auf keinen Fall dürfen diese Unterschiede übersehen werden. Daraus folgt für die oben genannten Hyperlinks im gesetzlichen Bereich eine differenzierende Bewertung, sonst wäre die Verantwortlichkeit für Hyperlinks unpräzise.

Darüber hinaus sollte die Kontrollmöglichkeit oder die Beherrschung des einzelnen gespeicherten Inhalts als das maßgebende Kriterium für die Unterscheidung und die Einordnung der Hyperlinks betrachtet werden.[294] Natürlich unterscheidet sich die Setzung eines Hyperlinks sowohl von der Durchleitung als auch von der Speicherung oder Zwischenspeicherung von Informationen, aber genau aus diesem Grund suchen wir eine analoge Anwendung zu den §§ 7–10 TMG. Deshalb ist nicht der formale Unterschied, sondern die materiale Beherrschung der einzelnen Inhalte das entscheidende Kriterium dafür, ob die §§ 7–10 TMG Anwendung finden können.

Über Hyperlinks, die auf die erste Ebene verweisen, besitzt der Hyperlinksetzer in der Regel eine starke Kontrolle. Obwohl er die verlinkten Inhalte nicht löschen kann – während ein Hosting Provider dazu in der Lage ist –, ist der Hyperlinksetzer fähig, die Hyperlinks zu sperren oder aufzuheben. Für den Nutzer entsteht in diesem Moment der Eindruck, die Inhalte seien nicht mehr aufrufbar. Außerdem hat bestimmt nicht jeder Hyperlinksetzer Kenntnis von den verlinkten rechtswidrigen Informationen. Zusammenfassend kann festgehalten werden, dass diese Hyperlinksetzer überhaupt eine ähnliche Kontrolle über die einzelnen Inhalte ausüben wie Hosting Provider. Schließlich ist auch darauf hinzuweisen, dass es in der Rechtslogik gerechtfertigt ist, § 10 TMG analog anzuwenden, wenn die Kontrollmöglichkeit des Hyperlinksetzers schwächer als die des Hosting Providers ist.

---

[293] Vgl. ebenda, Rn. 308. ff.

[294] Vgl. *Sieber*, Verantwortlichkeit im Internet, S. 161–162, Rn. 326; *Spindler*, CR Heft 12, 1998, 752.

Wenn ein Service-Provider mit hoher Kontrollmöglichkeit nach § 10 TMG privilegiert werden soll, kann natürlich auch ein vergleichbarer Service-Provider mit weniger Kontrollmöglichkeit nach § 10 TMG privilegiert werden.

Über Hyperlinks, die auf tiefere Ebenen verweisen, besitzt der Hyperlinksetzer eine sehr geringe Kontrolle. Die Nutzer können durch die Hyperlinks die Inhalte nicht unmittelbar erreichen; diese Hyperlinks vermitteln nur einen Übergang zu fremden Informationen. Die Hyperlinksetzer können die verlinkten Inhalte gar nicht beeinflussen. Diejenigen Hyperlinksetzer, die sich bei der Hyperlinksetzung fremde Inhalte zu eigen machen, können als Content Provider betrachtet werden.[295] Denn wenn die Hyperlinksetzer sich durch eine technische Einbindung mit den fremden Inhalten identifizieren, gewinnt der Nutzer den Eindruck, diese Inhalte seien von den Hyperlinksetzern ursprünglich erstellt worden.[296] Darüber hinaus haben diese Hyperlinksetzer in der Regel eine bestimmte und konkrete Kenntnis von den Inhalten. Insgesamt jedoch bleibt das Kriterium dafür, inwieweit das Hyperlinksetzen fremde Informationen zu eigenen machen kann, noch unklar.[297]

3. Strafrechtliche Verantwortlichkeit für Hyperlinks

Wenn es sich bei verlinkten Inhalten um illegale oder strafbare Informationen handelt, rückt die strafrechtliche Verantwortlichkeit für Hyperlinks in den Mittelpunkt der Betrachtung. Dieses Thema bezieht sich vor allem auf die Verbreitungsdelikte, etwa §§ 86, 86a, 130a, 184 StGB, und die Äußerungsdelikte wie §§ 90a, 103, 111, 185 StGB.[298]

a) Einordnung der Handlung als Tun oder Unterlassen

Da die dogmatische Grundlage und das theoretische System von positivem Tun und Unterlassen unterschiedlich sind, ist zuerst zu bestimmen, ob das Setzen von Hyperlinks als positives Tun oder als Unterlassung zu werten ist. In der Regel wird das Verhalten der ISP als Unterlassen eingeordnet (herrschende Meinung),[299] Hyperlinksetzer bilden aber eine Ausnahme. Grundsätzlich soll das Setzen von Hyperlinks als positives Tun betrachtet werden, weil der Hyperlinksetzer normalerweise gewisse Kenntnisse über die zu verlinkenden Inhalte hat. Er hat die Inhalte bewusst ausgewählt und dann die Links aktiv gesetzt, das heißt, „die Hyperlinks, die den Nutzer beim Anklicken automatisch auf eine andere Seite führen, bedeuten eine

---

[295] Vgl. BGH: Zugang pornografischer Internetangebote über ein unzureichendes AVS – ueber18.de, MMR Heft 6, 2008, 402 (BGH, Urteil vom 18.10.2007 – I ZR 102/05).

[296] Vgl. *Sieber*, Verantwortlichkeit im Internet, S. 154–155, Rn. 309–310; *Pelz*, ZUM Heft 7, 1998, 532.

[297] Vgl. *Malek/Popp*, Strafsachen im Internet, S. 23, Rn. 83.

[298] Vgl. *Ernst/Vassilaki/Wiebe*, Hyperlinks, S. 169 f., Rn. 305.

[299] Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 24.

direkte Einladung an die Nutzer".[300] Bei dieser Definition können die §§ 8–10 TMG schwer analoge Anwendung finden, denn die Kenntnis über die verlinkten Inhalte ist oft mit positivem Tun verbunden, während die Privilegien von §§ 8–10 TMG die Unkenntnis der ISP voraussetzen.[301]

In speziellen Ausnahmefällen kann Hyperlinksetzern eine Unterlassung angelastet werden. In der Literatur werden zwei mögliche Sachverhalte erwähnt:[302] Zum einen könnte sich für den Hyperlinksetzer eine Garantenpflicht zur Löschung des Hyperlinks aus vorangegangenem Tun ergeben. Denkbar sind Konstellationen, in denen der Hyperlinksetzer die rechtswidrigen und damit strafbaren Links nicht frühzeitig erkannt hat. Sobald er Kenntnis darüber hat, muss er diese illegalen Links löschen.[303] Zum anderen könnte eine Garantenpflicht aufgrund von Sachherrschaft oder wegen Eröffnung einer Gefahrenquelle bestehen.[304] Wenn zum Beispiel das Setzen eines Links rechtmäßig war, der Link aber später als rechtswidrig eingestuft wurde, könnte sich in dieser Situation eine Garantenpflicht bilden. In der Literatur wird der praktische Fall genannt, dass „Angela Marquardt auf ihrer Homepage auf eine rechtmäßige Ausgabe einer Zeitschrift verlinkte und nicht bemerkte, dass ihr Link sich später um einen strafbaren Artikel handelte".[305] Dem Urteil zufolge kann eine Strafbarkeit nicht begründet werden, wenn die Angeklagte den Link ohne Kenntnis der strafbaren Inhalte weiterhin aufrecht erhält.[306]

Das Setzen legaler Links ist eine rechtmäßige und sozial übliche Handlung. Deshalb kann es kein rechtswidriges Vorverhalten sein.[307] Wird der Link jedoch ausschließlich von der Setzerin kontrolliert, erwartet deswegen das Publikum, dass der strafbare Link gelöscht wird. Hätte die Hyperlinksetzerin in diesem Fall Kenntnis von den strafbaren Inhalten, wäre sie verpflichtet, den illegalen Link zu entfernen.[308] In dieser Situation können die §§ 8–10 TMG eine begrenzte analoge Anwendung finden. Vor allem ist es notwendig, eine differenzierende Lösung anzustreben. Wie oben erwähnt, sind die gesetzlichen Bewertungen zu Hyperlinks recht unterschiedlich.

---

[300] Joecks/Miebach-*Hörnle*, § 184, Rn. 48; auch *Sieber*, ebenda, Rn. 26.

[301] Die Privilegien für Access Provider sind eine Ausnahme.

[302] Vgl. *Malek/Popp*, Strafsachen im Internet, S. 31, Rn. 110.

[303] Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 41.

[304] *Vassilaki*, CR Heft 2, 1998, 112. Zur entgegengesetzten Auffassung vgl. *Malek/Popp*, Strafsachen im Internet, S. 34 ff., Rn. 121 ff.

[305] Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 41, 50; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 71, Rn. 238.

[306] Vgl. *Hütig*, AG Tiergarten, Link auf eine Homepage mit rechtswidrigem Inhalt, MMR Heft 1, 1998, 49 (AG Tiergarten, Urteil vom 30.06.1997 – 260 DS 857/96).

[307] Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 37, 41. Dagegen vgl. Joecks/Miebach-*Freund*, 2017, § 13, Rn. 164.

[308] Vgl. *Vassilaki*, CR Heft 2, 1998, 111 ff.; *ders.,* CR Heft 2, 1999, 88 ff.

b) Prüfpflichten der Hyperlinksetzer

Neben den Garantenpflichten des Hyperlinksetzers ist auch festzulegen, ob der Hyperlinksetzer aktive Prüfpflichten zur Ermittlung von strafbaren Inhalten hat und ob er regelmäßig oder nur sporadisch die gelinkten Inhalte prüfen muss. In dem oben geschilderten Fall (AG Tiergarten) ist auch fraglich, in welchen Zeitabständen die Überprüfung des Links vorzunehmen wäre.[309] Nach § 7 TMG sind ISP im Sinne der §§ 8–10 TMG nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Jedoch wird in Literatur und Rechtsprechung verbreitet gesagt, dass für die Bestimmung der Prüfpflichten der Hyperlinksetzer die §§ 7–10 TMG weder unmittelbare noch analoge Anwendung finden könnten.[310]

Auch wenn es keine generelle Lösung für diese Problematik gibt und die Anforderungen für die Hyperlinksetzer unterschiedlich sind, stellen der potenzielle Gefährdungsgrad der verlinkten Inhalte und die Kontrolle über die Inhalte zwei wichtige Kriterien dar, um die Prüfpflichten zu bestimmen. Bei einem manuell gesetzten Link wird vorausgesetzt, dass die zu verlinkenden Inhalte zuvor überprüft werden. Die „Prüftiefe" auf weitere Links einer zweiten oder dritten Ebene ist vom potenziellen Gefährdungsgrad der Inhalte abhängig.[311] Beim Aufrechterhalten eines Links hat der Hyperlinksetzer eine relativ geringe Herrschaft über die verlinkten Inhalte, deshalb wird auch eine nicht so umfangreiche Prüfpflicht von ihm erwartet. Verändern sich die verlinkten Inhalte, hat der Hyperlinksetzer in der Regel keine Garantenpflicht, es sei denn, dass es Anhaltspunkte für die Änderung gegeben hat oder dass von den verlinkten Inhalten eine gesteigerte Gefahr ausgeht.[312]

c) Einordnung der Hyperlinksetzer als Täter oder Teilnehmer

Die Einordnung der strafbaren Hyperlinksetzer als Täter oder Teilnehmer ist eine sehr umstrittene Problematik. In der Literatur gibt es viele unterschiedliche Auffassungen dazu. Einige Rechtswissenschaftler schließen die Täterschaft der Hyperlinksetzer in der Regel aus, weil die Hyperlinksetzer nur auf die strafbaren Inhalte Hyperlinks schalten, aber diese Inhalte nicht unmittelbar beeinflussen und kontrollieren können. Mit anderen Worten, bei den Hyperlinksetzern fehlt die die Täter-

---

309 Vgl. *Hütig*, AG Tiergarten, Link auf eine Homepage mit rechtswidrigem Inhalt, MMR Heft 1, 1998, 49 (AG Tiergarten, Urteil vom 30.06.1997 – 260 DS 857/96); *Vassilaki*, CR Heft 2, 1998, 111.

310 Vgl. Joecks/Miebach-*Freund*, 2017, § 13, Rn. 165; BGH: Zugang pornografischer Internetangebote über ein unzureichendes AVS – ueber18.de, MMR Heft 6, 2008, 402 (BGH, Urteil vom 18.10.2007 – I ZR 102/05).

311 Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 53.

312 Zum Beispiel, wenn es sich um einen strafrechtlich besonders stark betroffenen Bereich handelt. Vgl. *Sieber*, ebenda, Rn. 53; Joecks/Miebach-*Freund*, 2017, § 13, Rn. 165.

schaft begründende Herrschaft.[313] Obwohl diese Argumentation zunächst einleuchtend klingt, ist dieses Problem allerdings komplexer als gedacht. Wenn alle Umstände, wie Hyperlinks gesetzt werden, in die Überlegung einbezogen werden, ergibt sich der Schluss, dass die Hyperlinksetzer in unterschiedlichen Konstellationen nicht nur als Täter, sondern auch als Teilnehmer, vor allem als Gehilfen eingeordnet werden könnten. Natürlich sind Fälle denkbar, in denen die Hyperlinksetzer den Tätern durch ihre Dienste Hilfe leisten, denn die strafbaren Informationen liefern die Content Provider, die zuerst als Täter zu betrachten sind, wobei die Hyperlinksetzer nur eine fördernde Nebenrolle spielen dürften. Tatsächlich ist die Begründung einer Gehilfenstrafbarkeit manchmal schwieriger als die einer Täterschaft, weil bei Beihilfe der sogenannte doppelte Vorsatz erforderlich ist: Die Hyperlinksetzer müssen nicht nur die strafbaren Informationen kennen, sondern auch wissentlich und willentlich die Haupttat fördern.[314]

Es ist zudem nicht zu vernachlässigen, dass die Verwirklichung mancher strafrechtlichen Tatbestände nicht unbedingt auf unmittelbarer Einflussnahme auf und tatsächlicher Kontrolle über die strafbaren ursprünglichen Inhalte beruht. In dieser Hinsicht steht die Tatsache, dass die Hyperlinksetzer die verlinkten Inhalte nicht direkt steuern können, mit der möglichen Täterschaft der Hyperlinksetzer nicht im Widerspruch. Besonders ist dies bei den sogenannten Verbreitungsdelikten der Fall. Denn im Kern bedeutet „Verbreitung", die Informationen von Dritten anderen Personen zugänglich zu machen oder sie weiterzugeben. Offensichtlich erfüllen Hyperlinks diese Forderung aus den Tatbeständen der Verbreitungsdelikte.[315] Deshalb wird in der Literatur beschrieben, dass bei der Einrichtung eines Hyperlinks auf strafbare Inhalte Dritter die Strafbarkeit der Hyperlinksetzer als Täter überhaupt nur in Betracht kommt, sofern es sich auf die Verbreitungsdelikte bezieht.[316] Darüber hinaus kann die Täterschaft der Hyperlinksetzer grundsätzlich festgestellt werden, wenn sie fremde Informationen durch Setzen von Hyperlinks zu eigenen machen. In dieser Tatbestandsvariante sind die Hyperlinksetzer als Content Provider zu betrachten, bei denen die Täterschaft ohne Zweifel bestimmt werden kann.

Zusammenfassend lässt sich feststellen, dass keine allgemeine Schlussfolgerung zu der Einordnung der strafbaren Hyperlinksetzer als Täter oder Teilnehmer besteht. Es ist hier sinnvoller, eine differenzierte Position, die die konkreten Umstände berücksichtigt, einzunehmen.[317]

---

313 Vgl. *Vassilaki*, CR Heft 2, 1999, 90; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, S. 74, Rn. 246.

314 Vgl. *Flechsig/Gabel*, CR Heft 6, 1998, 356.

315 Vgl. *Flechsig/Gabel*, ebenda, 355.

316 Vgl. *Boese*, Strafrechtliche Verantwortlichkeit für Verweisungen durch Links im Internet, S. 128 ff.

317 Vgl. *Malek/Popp*, Strafsachen im Internet, S. 38, Rn. 138.

Dritter Teil

Verantwortlichkeit der ISP in China

I. Historische Entwicklung, Begriff und Typen der ISP

A. Historische Entwicklung

Aus historischen Gründen kam die Entwicklung des Internets und der Netzwerktechnik in China relativ spät in Gang. Am 25. August 1986 verschickte *Wu Weimin* vom Institut für Hochenergiephysik der Chinesischen Akademie der Wissenschaften die erste E-Mail in China an *Jack Steinberger* in Genf. Im September 1987 gründeten Professor *Wang Yunfeng* und Dr. *Li Chengjiong* den ersten E-Mail-Knoten mithilfe von Professor *Werner Zorn* von der Universität Karlsruhe. Sie schickten erfolgreich eine E-Mail nach Deutschland, deren Inhalt lautete: „Über die große Mauer können wir jede Ecke der Welt erreichen".[1] Laut dem ersten statistischen Bericht über Chinas Internetentwicklung 1997 betrug die Anzahl der Computer, die Verbindung mit dem Internet hatten, nur 299.000, während sich die Anzahl der Internetnutzer auf 620.000 belief.[2]

Mit der Reform- und Öffnungspolitik von *Deng Xiaoping* begann die Marktwirtschaft in China zu blühen. Vor diesem Hintergrund entwickelte sich das Internet in China rasant. In den letzten zwei Jahrzehnten hat China einen enormen Ausbau der Netzwerktechnologie, die inzwischen in fast allen Lebens- und Arbeitsbereichen weit verbreitet ist, erlebt.

Nach den von CNNIC (China Internet Network Information Center) veröffentlichten Daten betrug die Zahl der chinesischen Internetnutzer im Juni 2017 insgesamt 751 Millionen,[3] was etwa der Gesamtbevölkerung von Europa entspricht. Der Anteil aller chinesischen Internetnutzer erreichte bis Juni 2017 54.3 %. Dieser Wert liegt mehr als 10 % über dem durchschnittlichen Wert (43.998 %) von 2015.[4] Obwohl dieser Anteil noch geringer als der in westlichen Industrieländern[5] ist, ist der

---

[1] Vgl. CNNIC, Internet Meilensteine 1986–1993, abrufbar unter http://www.cnnic.net.cn/hlwfzyj/hlwdsj/201206/t20120612_27414.htm [Stand: 15.09.2017].

[2] CNNIC, Der statistische Bericht über Chinas Internet-Entwicklung 1997, S. 1.

[3] CNNIC, Der statistische Bericht über Chinas Internet-Entwicklung 2017, S. 13.

[4] Die Daten stammen von der Weltbank. Vgl. http://data.worldbank.org/indicator/IT.NET.USER.P2 [Stand: 15.09.2017].

[5] Zum Beispiel betrug der Anteil der Internetnutzer 2015 in USA 74.5%, in Großbritannien 92%, in Deutschland 87.6%, in Frankreich 84.7%. Vgl. http://data.worldbank.org/indicator/IT.NET.USER.P2 [Stand: 15.09.2017].

absolute Wert in China allerdings schon sehr groß. Zudem ist auffällig, dass die Zahl der chinesischen Internetnutzer, die online einkaufen, insgesamt 514 Millionen beträgt.[6] Darüber hinaus ist das mobile Bezahlen (*mobile payment*) sehr populär. Nach den Daten von CNNIC beläuft sich die Zahl der Internetnutzer, die mobil bezahlen, auf 502 Millionen.[7] Interessanterweise wird die Anwendung der Netzwerktechnologie immer von der chinesischen Regierung stark unterstützt und aktiv gefördert. Im August 2017 wurde in Hangzhou der erste Internet-Gerichtshof begründet. Unter die Zuständigkeit dieses Gerichtshofs fallen nur Rechtsangelegenheiten, die einen Bezug zum Internet haben. Alle Gerichtsverfahren werden online durchgeführt.[8] Allerdings geht mit dieser Entwicklung auch eine von Jahr zu Jahr ansteigende Cyberkriminalität in China einher. Gleichzeitig ist die Problematik der Verantwortlichkeit der ISP in China dringend zu diskutieren, weil immer vielfältigere Internetdienste angeboten werden, während die einschlägige rechtliche Haftung der ISP unklar bleibt. Deshalb ist eine ausführliche und systematische Untersuchung zu diesem Thema von großer Bedeutung.

B. Rechtliche Begriffe der ISP

Seit den 1990er-Jahren hat die chinesische Regierung eine Reihe von Gesetzen, Verordnungen und Vorschriften über die Rechte und Pflichten im Internet erlassen.[9] Hier eine Auswahl:

- im Jahr 2000 verabschiedete der Staatsrat die „Verordnung über die Internet-Informationsservices";
- im Jahr 2004 verabschiedete das Hauptamt für Rundfunk, Film und Fernsehen die „Vorschrift über die audiovisuelle Sendung durch Internet und andere Informationsnetzwerke";
- im Jahr 2005 erließ das Ministerium für öffentliche Sicherheit die „Vorschrift über die technischen Maßnahmen der Internetsicherheit";
- im Jahr 2005 erließen das Hauptamt für Rundfunk, Film und Fernsehen und das Ministerium für Informationsindustrie die „Vorschrift über die audiovisuellen Sendungsservices durch Internet";
- im Jahr 2006 verabschiedete der Staatsrat die „Verordnung über den Schutz des Informationsnetz-Übertragungsrechts";[10]

---

[6] Vgl. CNNIC, 40th China Statistical Report on Internet Development, 2017, S. 13, 34.

[7] Vgl. ebenda, S. 40.

[8] Vgl. Der erste Internet-Gerichtshof in China wird begründet, abrufbar unter http://news.china.com/news100/11038989/20170818/31127149.html [Stand: 15.09.2017].

[9] In China haben die verschiedenen Normen (Gesetz, Verordnung und Vorschrift) unterschiedliche Rechtswirkungen. Gesetze werden vom nationalen Volkskongress oder seinem ständigen Komitee, Verordnungen vom Staatsrat, Vorschriften von den Ministerien und den auf der gleichen Ebene stehenden Ämtern erlassen.

– im Jahr 2009 verabschiedete der Ständige Ausschuss des Nationalen Volkskongresses das „Deliktsgesetz“;
– im Jahr 2011 erließ das Ministerium für Kultur die „provisorische Vorschrift über die Kultur im Internet“;
– im Jahr 2012 verabschiedete der Ständige Ausschuss des Nationalen Volkskongresses die „Entscheidung über die Verstärkung des Netzwerk-Informationsschutzes“;
– im Jahr 2015 verabschiedete der Ständige Ausschuss des Nationalen Volkskongresses das „Strafrechtsänderungsgesetz (IX)“, das sich teilweise auf das Internetstrafrecht, besonders aber auf die strafrechtliche Verantwortlichkeit der ISP bezieht;
– im Jahr 2016 verabschiedete der Ständige Ausschuss des Nationalen Volkskongresses das „Gesetz über die Netzwerksicherheit“.

In den oben genannten Gesetzen, Vorschriften und Verordnungen wird der Begriff der ISP ausdrücklich erwähnt, ohne jedoch die ISP direkt und klar zu definieren. Die Bedeutung des Begriffs erschließt sich nur indirekt aus der Typologie der ISP. So sieht § 18 der „Vorschrift über die technischen Maßnahmen der Internetsicherheit 2005“ des Ministeriums für öffentliche Sicherheit zum Beispiel vor: Unter Internet-Service-Providern versteht man die Organisation (单位),[11] die den Nutzern Internet-Access-Service, Internet-Datacenter-Service, Internet-Informationsservices und Internetzugangsservice anbieten. In diesem Paragrafen wird die Definition des Begriffs durch die Aufzählung der Typen der ISP ersetzt. Ebenso wenig gibt es in der „Verordnung über den Schutz des Informationsnetz-Übertragungsrechts 2006“ eine direkte Definition der ISP, dafür aber klar strukturierte Typen der ISP. In § 36 des Deliktsgesetzes werden nicht nur der Begriff der ISP, sondern auch die Regelungen von *notice and take down* deutlich hervorgehoben. Allerdings fehlt es noch an einer konkreten und unmittelbaren Definition der ISP, ein Mangel, der zu Rechtsunsicherheiten führen wird, weil die Abgrenzung der ISP völlig offenbleibt.

C. Rechtliche Typen der ISP

Im Gegensatz zu Deutschland werden die Typen der ISP in China in unterschiedlichen Rechtsbereichen genannt. Die Kriterien für die Typisierung der ISP in den verschiedenen Normen sind dabei teilweise unvereinbar.

---

[10] Diese Verordnung wurde im Jahr 2013 vom Staatsrat modifiziert, aber die Paragrafen über die Verantwortlichkeit der ISP blieben unverändert.

[11] Dies ist ein besonderer Begriff in chinesischen Gesetzen. Er umfasst sowohl die Staatsorgane als auch die Privat- und Staatsunternehmen und die öffentlichen Einrichtungen. Vgl. § 30 des chinesischen Strafgesetzbuchs.

1. Typen der ISP in der „Vorschrift über die technischen Maßnahmen der Internetsicherheit 2005“

Nach § 18 der „Vorschrift über die technischen Maßnahmen der Internetsicherheit 2005“ werden vier unterschiedliche Arten von Internetdiensten für die ISP skizziert:

a) Internet-Access-Service

In der Anordnung des Ministeriums für öffentliche Sicherheit wird der Internet-Access-Service nicht weiter definiert, einige Hinweise dazu lassen sich jedoch aus anderen Vorschriften entnehmen. Im Jahr 2013 verabschiedete das Ministerium für Industrie und Informationstechnologie die „Internet-Access-Spezifikation“. In dieser Spezifikation beziehen sich Internet-Access-Dienste nur auf technische und physische Dienste, die mit den übermittelten Inhalten nichts zu tun haben. Mit anderen Worten, diese Dienste werden in den niedrigen Schichten des ISO/OSI-Schichtenmodells (besonders in der physikalischen Schicht) angeboten.

b) Internet-Datacenter-Service (IDC)

Nach § 18 Abs. 3 der Vorschrift des Ministeriums für öffentliche Sicherheit wird der Internet-Datacenter-Service als ein Dienst bezeichnet, der Colocation, Dedicated-Hosting-Service und Vermietung des Cyberspace umfasst. Mit der Colocation wird der Server im Internet Datacenter (IDC) untergebracht und von dem ISP im Auftrag des Eigners des Servers betrieben, der Eigner kann seinen Server durch Fernsteuerung kontrollieren. Der Dedicated-Hosting-Service bedeutet, dass der Nutzer ausschließlich einen Server von IDC mietet.

c) Internet-Informationsservices

Die Bedeutung dieser Dienste ist unklar, eine weitere Klärung dieses Begriffs nicht vorhanden. Nach § 2 der „Verordnung über die Internet-Informationsservices“ des Staatsrats werden diejenigen Dienste als Internet-Informationsservices bezeichnet, die den Internetnutzern Informationen durch das Internet anbieten. Jedoch ist diese Definition so umfassend, dass es an Rechtssicherheit fehlt.

d) Internetzugangsservice

Der Umfang dieses Services ist auch nicht eindeutig zu beschreiben. Aber nach § 2 der „Verordnung über die Verwaltung der Internetzugangsservices in Geschäftsstandorten“ kann aus dem Wortlaut abgeleitet werden, dass der Internetzugangsservice sich auf die von Internetcafés angebotenen Internet-Access-Services bezieht.

Es kann zusammengefasst werden, dass die in der „Anordnung über die technischen Maßnahmen der Internetsicherheit“ genannten Typen der ISP rechtlich nicht zutreffend charakterisiert sind. Erstens fehlt die Rechtssicherheit bei allen vier Arten der unterschiedlichen Dienste. Wie oben erläutert, bleibt der Angebotsumfang jedes Dienstes der ISP unklar. Zweitens stellen die Typen dieser Dienste keine Systematik dar. Die Umfänge der unterschiedlichen Dienste dürften mit sich selbst ko-

inzidieren, vermutlich, weil diese Typen der Dienste nicht nach einem einheitlichen Kriterium eingeteilt werden. Drittens beziehen sich einige Dienste auf die übermittelten oder gespeicherten Inhalte in den oberen Schichten des ISO/OSI-Schichtenmodells (besonders in der Anwendungsschicht), während andere Dienste sich mit technischen und physischen Services in den niedrigen Schichten beschäftigen. Viertens werden einige Dienste nach der Art der angebotenen Services, nicht nach der Funktion der ISP typisiert, was im Widerspruch zu ihrer ursprünglichen Verantwortlichkeit stehen könnte. Schließlich beschränken sich die ISP nach dieser Typisierung nur auf die Organisation. Das würde bedeuten, dass ein menschliches Individuum kein ISP sein kann. Obwohl die Internetdienste in den meisten Fällen von Unternehmen oder Organisationen betrieben werden, ist es durchaus möglich, dass diese Dienste auch von Einzelpersonen initiiert werden. Im Hinblick auf diese Nachteile ist eine Typisierung der ISP in der gerichtlichen Praxis schwierig anzuwenden.

2. Typen der ISP im Zivilrecht

In der „Verordnung über den Schutz des Informationsnetz-Übertragungsrechts 2006“ des Staatsrats findet sich weder eine direkte Definition zu ISP noch eine direkte Beschreibung der Internetdienste. Jedoch können wir die Typen von Internetdiensten mittelbar eruieren, denn in den §§ 20–23 dieser Verordnung wird eine Reihe von Regelungen über die Verantwortlichkeit der unterschiedlichen ISP vorgestellt. In diesen Regelungen werden der Access Service, der Caching Service, der Hosting Service und Search- sowie Link-Services beschrieben. Diese Services bilden die Grundstruktur der Typen der ISP.

In dieser Verordnung ist auffällig, dass Search- und Link-Services selbstständig vorgesehen werden, was jedoch von dem Gesetzgeber in Deutschland abgelehnt wird. An diesem Punkt übernimmt der chinesische Gesetzgeber offensichtlich die Erfahrungen aus dem *Digital Millennium Copyright Act* der USA.[12] Denn die Privilegierung für das *Information Location Tool*, welches sich auf das Verzeichnis, den Index, die Referenz, den Zeiger oder Hypertextlink bezieht, wird in 17 U.S. Code § 512 (d) selbstständig vorgesehen.[13]

In der Literatur werden diese rechtlichen Typen der ISP im zivilrechtlichen Bereich von der herrschenden Meinung aufgenommen.[14] Auf dieser Grundlage wer-

---

[12] Vgl. *Xu Wei*, Moderne Rechtswissenschaft Heft 1, 2013, 64; *Wang Qian*, Rechtswissenschaft Heft 6, 2010, 133.

[13] Siehe 17 U.S. Code § 512(d).

[14] Vgl. *Lu Chunya*, Politik und Recht Heft 4, 2011, 117 ff.; *Wu Handong*, Die Haftung der Urheberrechtsverletzung von ISP, Chinesische Rechtswissenschaft Heft 2, 2011, 38; *ders.*, Studium des Rechts und der Wirtschaft Heft 6, 2010, 28; *Wang Liming* (Hrsg.), Erläuterungen zum chinesischen Deliktsgesetz, S. 158; *Wang Shengming* (Hrsg.), Erklärungen zum chinesischen Deliktsgesetz, S. 180; *Zhang Xinbao/Ren Hongyan*, Zeitschrift der

den die zivilrechtlichen Haftungen der Access Provider, Caching Provider, Hosting Provider und Search- und Link-Services-Provider jeweils im Einzelnen analysiert.

Im zivilrechtlichen Bereich ist die Typisierung der ISP zutreffend und steht auch mit der zivilrechtlichen Haftung im Einklang. Denn die Typisierung der ISP wird nicht nur durch das systematische Gesetz, sondern auch durch die tiefgründigen theoretischen Erklärungen unterstützt. Jedoch ist bemerkenswert, dass die „Verordnung über den Schutz des Informationsnetz-Übertragungsrechts" überhaupt im zivilrechtlichen (besonders im urheberrechtlichen) Bereich gilt. Ob und wie diese Verordnung auch im strafrechtlichen Bereich angewendet werden kann, wird jetzt noch nicht weiter diskutiert. Bis heute beziehen sich nur wenige Untersuchungen im strafrechtlichen Bereich auf dieses Thema.

3. Typen der ISP im Strafrecht

Vor dem Erlass des „Strafrechtsänderungsgesetzes (IX)" im Jahr 2015 gab es im chStGB keinen Begriff – und damit auch keine Typen – der ISP. Aber aus der richterlichen Auslegung des Obersten Volksgerichtshofs und der Obersten Volksstaatsanwaltschaft konnten die Typen der ISP mittelbar abgeleitet werden: In § 7 der „Interpretation I" (2004)[15] werden „Internet-Access-Service", „Colocation", „Netzwerkspeicherung", und „Kommunikationsübermittlung" erwähnt. In § 5 der „Interpretation (II)" (2010)[16] werden die gleichen Begriffe sowie „Internet Information Service Provider" angeführt. Am 29. August 2015 wurde von dem Ständigen Ausschuss des Nationalen Volkskongresses das „Strafrechtsänderungsgesetz (IX)" erlassen, in dem sich drei Paragrafen mit der strafrechtlichen Verantwortlichkeit der ISP befassen.

§ 286 Abs. 1 chStGB bezieht sich auf die strafrechtliche Verantwortlichkeit der ISP, wenn sie sich weigern, die Sicherheitsverpflichtungen in Gesetzen oder Anordnungen zu erfüllen. Der Tatbestand dieses Paragrafen beschreibt Sonderdelikte für ISP. In diesem Paragrafen wird der Begriff Internet-Service-Provider deutlich formuliert, während leider weder eine klare Definition noch konkrete Typen zu ihm existieren.

Universität Renmin Heft 4, 2010, 18–19; *Liu Deliang*, Studium des Rechts und der Wirtschaft Heft 5, 2001, 111–112.

[15] "Interpretation of the Supreme People's Court and the Supreme People's Procuratorate of Several Issues on the Specific Application of Law in the Handling of Criminal Cases about Producing, Reproducing, Publishing, Selling and Disseminating Pornografic Electronic Information via the Internet, Mobile Communication Terminals and Sound Message Stations"(2004).

[16] "Interpretation (II) of the Supreme People's Court and the Supreme People's Procuratorate of Several Issues on the Specific Application of Law in the handling of Criminal Cases about Producing, Reproducing, Publishing, Selling and Disseminating Pornografic Electronic Information via the Internet, Mobile Communication Terminals and Sound Message Stations" (2010).

§ 287 Abs. 2 chStGB bezieht sich auf die strafrechtliche Verantwortlichkeit des Straftäters, der Dritten, die durch das Informationsnetzwerk Straftaten begehen, hilft. In diesem Paragrafen werden auch „Internet-Access-Service", „Colocation", „Netzwerkspeicherung" und „Kommunikationsübermittlung" erwähnt.[17] Jedoch werden diese unterschiedlichen Dienste gesetzlich gleich behandelt. Das heißt, obwohl der Begriff der ISP und ihre entsprechenden Typen im chStGB existieren, ist diese Unterscheidung lediglich eine Formsache.

Darüber hinaus wird diese Problematik in der Theorie nicht ausreichend berücksichtigt. In vielen einflussreichen rechtswissenschaftlichen Arbeiten wird die strafrechtliche Verantwortlichkeit der ISP auf eine allgemeine Weise analysiert, ohne dass diese Verantwortlichkeit die oben genannte Typisierung der Internetdienste zur Voraussetzung hat.[18] Den meisten Wissenschaftlern ist in diesem Bereich nicht bewusst, dass die Typisierung der ISP und ihrer Dienste der systematischen Privilegierung zugrunde liegen. Dies ist wirklich ein Mangel, denn wenn die Funktionstypen der ISP vor der Analyse der strafrechtlichen Verantwortlichkeit nicht bestimmt werden, kann auch das Ergebnis dieser Analyse nicht präzise sein.

In der strafrechtlichen Literatur liegen schon einige vorbereitende Untersuchungen über die Typisierung der ISP vor, die jedoch unbefriedigend sind. Zum Beispiel wird behauptet, dass die ISP in Internet Access Provider und Internet Content Provider aufgeteilt werden können.[19] In der Erläuterung zu § 286 Abs. 1 chStGB wird diese Unterscheidung vom Gesetzgeber ebenfalls angenommen.[20] Obwohl diese Differenzierung sinnvoll ist, werden die Diensteanbieter für Zwischenspeicherung und Speicherung von Informationen nicht in ihr berücksichtigt. Hier gibt es offensichtlich eine Gesetzeslücke. Heutzutage spielen Hosting Provider und Caching Provider eine immer wichtigere Rolle in der Informationsgesellschaft. Viele Wissenschaftler haben darauf hingewiesen, dass die Netzwerkspeicherung die dritte Welle der Informationstechnologie anführen wird.[21] Deshalb kann gesagt werden, dass Hosting Provider und Caching Provider unverzichtbare Typen der ISP sind.

---

[17] Inhaltlich folgt dieser Paragraf der oben genannten „Interpretation I" (2004) und „Interpretation (II)" (2010).

[18] Vgl. *Zhou Guangquan*, China Law Review Heft 2, 2015, 177; *Che Hao*, China Law Review Heft 1, 2015, 49 ff.; *Zhao Yuan*, Die strafrechtliche Verantwortlichkeit der ISP in der Cyberkriminalität, Legal Daily, A 011, 23.07.2014.

[19] Vgl. *Peng Wenhua*, Zeitschrift der Universität Foshan (Sozialwissenschaftliche Ausgabe) Heft 3, 2004, 55; *Ye Qi*, Zeitschrift der Shanghaier Akademie für öffentliche Sicherheit Heft 4, 2005, 77.

[20] Vgl. *Zang Tiewei* (Hrsg.), Erklärungen über das „Strafrechtsänderungsgesetz (IX)", 2015, S. 191.

[21] *Chen Kai/Bai Yingcai*, Acta Electronica Sinica Heft 12A, 2012, 1928; *Han Dezhi*, Forschung zur Anwendung von Computern Heft 7, 2005, 5.

Darüber hinaus wird in der Literatur argumentiert, dass die ISP in Internet-Access-Provider, Internet-Content-Provider und Internet-Platform-Provider zu gliedern seien.[22] In dieser Konzeption fehlen auch wieder Caching Provider und Hosting Provider. Der Internet-Platform-Provider ist gar nicht geeignet, um als grundlegende Kategorie der ISP betrachtet zu werden, der Umfang einer Plattform ist so breit, dass viel zu viele Internetdienste in dieser Definition berücksichtigt werden müssten. Der Plattformservice kann sowohl den Access Service als auch den Hosting Service darstellen, was die Systematik der Typen von ISP beeinträchtigt.

II. Allgemeine und zivilrechtliche internetspezifische Verpflichtungen und Privilegien der ISP

A. Grundlegender Rechtsrahmen

1. Zivilrechtliche Normen

Im Gegensatz zu Deutschland gibt es kein dem TMG vergleichbares, einheitliches Gesetz über die Verantwortlichkeit der ISP in China, das alle rechtlichen Bereiche von Zivilrecht, Verwaltungsrecht, Strafrecht usw. umfasst. Im Vergleich zu anderen Rechtsbereichen ist der Rechtsrahmen im zivilrechtlichen Sektor über die Verantwortlichkeit der ISP relativ weit gesteckt und eindeutig.

Im Jahr 2000 verabschiedete der Oberste Volksgerichtshof eine Interpretation über das Urheberrecht im Computernetzwerk.[23] Nach § 5 dieser Interpretation trägt der Inhalte anbietende ISP mit dem Nutzer die gemeinsame Deliktshaftung, wenn

(1) der ISP weiß, dass der Nutzer durch das Netzwerk das Urheberrecht des Dritten verletzt, oder der ISP von dem Urheberrechtsinhaber mit einem Beweis gewarnt wird und

(2) der ISP keine Maßnahmen ergreift, die verletzenden Inhalte zu löschen.

Obwohl diese Interpretation des Obersten Volksgerichtshofs kein Gesetz ist, spielt sie tatsächlich eine dem Gesetz vergleichbare Rolle.

Im Jahr 2006 wurde eine Reihe von Regelungen über die Privilegierung der ISP bezüglich des Übertragungsrechts durch „die Anordnung über den Schutz des Informationsnetz-Übertragungsrechts“ (§§ 20–23) vom Staatsrat festgelegt. In dieser

---

[22] Vgl. *Yang Caixia*, Der Sucher Heft 2, 2007, 96–97; *Chen Hongbing*, Zeitschrift der Nordöstlichen Universität (Sozialwissenschaftliche Ausgabe) Heft 3, 2009, 258; *Pi Yong*, Die strafrechtliche Verantwortlichkeit der ISP, Guang Ming Daily, 28.06.2005.

[23] Vgl. die Interpretation über die Anwendung der Gesetze bezüglich des Streits des Urheberrechts im Computernetzwerk (2000). Diese Interpretation wurde im Jahr 2003 und 2006 zweimal modifiziert und durch die Interpretation (2012) des Obersten Volksgerichtshofs ersetzt.

Anordnung werden die Privilegien von Access Service Providern, Caching Service Providern, Hosting Service Providern und Search- und Link-Service-Providern jeweils in detaillierter Weise vorgesehen. Die Geltung dieser Anordnung beschränkt sich aber nur auf das Übertragungsrecht im Informationsnetzwerk.

Im Jahr 2009 wurden diese Regelungen im breiteren Umfang durch § 36 des Deliktsgesetzes bestätigt, der vorsieht:

(1) Der Nutzer und der ISP sollen Deliktshaftung tragen, wenn sie die Zivilrechte von Dritten durch das Netzwerk verletzen.

(2) Wenn der Nutzer die Zivilrechte von Dritten durch Netzwerkservices verletzt, kann der Verletzte den ISP auffordern, die notwendigen Maßnahmen, etwa Löschung, Sperrung der illegalen Inhalte und Abbruch der Hyperlinks, zu ergreifen. Wenn der ISP nach dieser Mitteilung nicht unverzüglich notwendige Maßnahmen einleitet, soll der ISP mit dem Nutzer für den vergrößerten Anteil der Beschädigung die gesamtschuldnerische Haftung übernehmen.

(3) Wenn der ISP weiß, dass der Nutzer die Zivilrechte von Dritten durch seine Netzwerkdienste verletzt, und er keine notwendigen Maßnahmen ergreift, soll er mit dem Nutzer die gesamtschuldnerische Haftung übernehmen.

In der Literatur wird § 36 des Deliktsgesetzes von der herrschenden Meinung als eine erweiternde Übernahme und Bestätigung der Prinzipien s*afe harbor* und *notice and take down* verstanden. Diese Prinzipien werden auf eine allgemeine Weise vorgesehen, ohne dass die konkreten Typen der ISP in diesem Paragrafen beschrieben werden. Das bedeutet, dass die Privilegierung der ISP nach dem *safe harbor*-Prinzip sich nicht nur auf das Informationsnetz-Übertragungsrecht beschränkt, sondern sich auf alle Deliktshaftungen bezieht. Nach der „Anordnung über den Schutz des Informationsnetz-Übertragungsrechts“ gilt das *notice and take down*-Prinzip nur für den Caching Provider, den Hosting Provider, den Search- und Link-Provider, aber nicht für den Access Provider. Dieses Verständnis steht mit der umfassenden Geltung des *notice and take down*-Prinzips nach § 36 des Deliktsgesetzes nicht im Einklang. Diese Problematik wird nachstehend weiter diskutiert.

Außerdem wurden die Regelungen – ähnlich wie die in § 36 des Deliktsgesetzes – von der nationalen Urheberrechtsverwaltung auch in den „Entwurf der dritten Veränderung des Urheberrechtsgesetzes“ im März 2012 aufgenommen.[24] Wenn dieser Entwurf schließlich vom Gesetzgeber verabschiedet werden würde, könnte man zu dem Schluss kommen, dass das *notice and take down*-Prinzip sowie seine entsprechenden Privilegien im ganzen urheberrechtlichen Bereich akzeptiert werden.

Im November 2012 erließ das Oberste Volksgericht „die Interpretation über die Anwendung der Gesetze zu dem Zivilstreit bezüglich des Informationsnetz-Übertragungsrechts“.

---

[24] Vgl. § 69 des „Entwurfs der dritten Veränderung des Urheberrechtsgesetzes“ (2012).

§ 7 dieser Interpretation sieht Ähnliches vor:

(1) Wenn der ISP einem Nutzer zu dessen Verletzung des Informationsnetz-Übertragungsrechts von Dritten Hilfe leistet oder der ISP einen Nutzer dazu anstiftet, soll der ISP eine Deliktshaftung übernehmen.

(2) Wenn der ISP einen Nutzer durch Rede, technische Unterstützung für Förderung oder Belohnungspunkte usw. ermutigt oder belehrt, das Informationsnetz-Übertragungsrecht von Dritten zu verletzen, soll der ISP als Anstifter zu dem Delikt betrachtet werden.

(3) Wenn der ISP weiß oder wissen sollte, dass der Nutzer durch die Netzwerkdienste das Informationsnetz-Übertragungsrecht verletzt, und der ISP keine notwendigen Maßnahmen wie Löschung oder Sperrung der illegalen Inhalte ergreift, oder der ISP dem Nutzer Hilfe wie technische Unterstützung leistet, soll er als Gehilfe zu dem Delikt betrachtet werden.

Diese Interpretation konkretisiert die Verantwortlichkeit der ISP bezüglich des Informationsnetz-Übertragungsrechts weiter. Damit werden die Voraussetzungen für einen Anstifter und einen Gehilfen zu dem rechtsverletzenden Delikt auf detaillierte Weise beschrieben.

2. Grundtendenz und Einordnung der Rechtsnormen

Es ist auffällig, dass sich der Wortlaut und die sprachliche Logik der Paragrafen über die Verantwortlichkeit der ISP in chinesischen Gesetzen, Anordnungen oder Interpretationen stark von der ECRL der EU, dem TMG aus Deutschland oder dem DMCA der USA unterscheiden.

Zum Beispiel lautet die Formulierung der §§ 8–10 des deutschen TMG: „Diensteanbieter sind ... nicht verantwortlich, sofern sie ...“. Dahingegen heißt die Formulierung des § 36 des Deliktsgesetzes oder die des § 7 der Interpretation des Informationsnetz-Übertragungsrechts des chinesischen Obersten Volksgerichtshofs: „Wenn der ISP..., soll er ... Haftung übernehmen.“

In der Literatur wird gesagt, dass die Regelungen im TMG usw. zu einem Privilegierungsmodell gehören, während die Regelungen in den oben genannten chinesischen Gesetzen zu einem Zurechnungsmodell zählen. Dieses Zurechnungsmodell steht mit den Regelungen aus der „Anordnung über den Schutz des Informationsnetz-Übertragungsrechts“ des Staatsrats, die als Privilegierungsmodell betrachtet wird, nicht im Einklang.[25]

Nach der herrschenden Meinung sind die Regelungen in chinesischen Gesetzen und deren Interpretation als Privilegierungsmodell zu verstehen, weil sie über das *safe harbor*-Prinzip oder das *notice and take down*-Verfahren darauf ausgerichtet sind, dem ISP zusätzliche Verteidigung anzubieten. Mit anderen Worten, der ISP

---

[25] Vgl. *Lu Chunya*, Zeitschrift der Universität Henan für Wirtschaft und Recht Heft 5, 2012, 59 ff.

kann keine Haftung übernehmen, obwohl er die Voraussetzungen der Privilegierungsregelungen nicht erfüllt.[26]

Meines Erachtens sollten die Gesetze in China ebenso als Privilegierungsmodell wie in Deutschland und den USA verstanden werden, obwohl natürlich der Wortlaut und die sprachliche Logik der chinesischen Regelungen anders als die der amerikanischen und deutschen sind. Diesen Schluss kann man durch eine teleologische Auslegung ziehen. Außerdem ist die Position des Gesetzgebers oder des Obersten Volksgerichtshofs klar, dass die Verantwortlichkeit der ISP für fremde Inhalte beschränkt werden soll.[27]

B. Allgemeine Verpflichtungen der ISP

Im chinesischen Rechtsrahmen gibt es eine Reihe von Gesetzen, Verordnungen und Vorschriften,[28] die sich auf die Pflichten der ISP beziehen. Es wird in diesen Anordnungen und Vorschriften vorgesehen, dass die ISP die Informationen zur Verbreitung von Pornografie, Glücksspiel, Gewalt, Mord, Terrorismus oder Anstiftung eines Verbrechens nicht herstellen, vervielfältigen, veröffentlichen und verbreiten dürfen. Nach diesen Normen sollen die ISP eine allgemeine und aktive Verpflichtung übernehmen. Beispielsweise wurde in § 13 der „Verordnung über die Internet-Informationsservices" des Staatsrats im Jahr 2000 vorgesehen, dass die ISP den Nutzern gute Services anbieten und die Gesetzmäßigkeit der angebotenen Informationen garantieren sollen.

§ 5 der „Entscheidung über die Verstärkung des Netzwerkinformationsschutzes" des Ständigen Ausschusses des Nationalen Volkskongresses im Jahr 2012 lautet:

> Die ISP sollen die Verwaltung der von ihren Nutzern veröffentlichten Informationen verstärken. Wenn sie illegale Informationen gefunden haben, sollen sie die Durchleitung dieser Informationen unverzüglich stoppen, die rechtswidrigen Informationen löschen, die entsprechenden Dateien speichern und an die zuständigen Behörden melden.

---

[26] Vgl. *Liu Jiarui*, Geistiges Eigentum Heft 2, 2009, 14 ff.; *Lu Chunya*, Politik und Recht Heft 4, 2011, 125; *Lu Chunya*, ebenda, 66 ff.; *Xie Guanbin/Shi Xueqing*, Geistiges Eigentum Heft 1, 2008, 85; *Shi Xueqing/Wang Yong*, Geistiges Eigentum Heft 3, 2009, 25 ff.; *Cui Guobin*, Chinesische Rechtszeitschrift Heft 4, 2013, 153. Zur Kritik vgl. *Xu Wei*, Moderne Rechtswissenschaft Heft 1, 2013, 58 ff.; *Wang Qian*, Rechtswissenschaft Heft 6, 2010, 136 ff.

[27] „Das Oberste Volksgericht spricht von der Interpretation über das Informationsnetz-Übertragungsrecht", vgl. http://news.xinhuanet.com/zgjx/2012-12/27/c_132065681.htm [Stand: 15.09.2017].

[28] Zum Beispiel § 15(7) der „Verordnung über die Internet-Informationsservices" des Staatsrats; § 19(7) der „Vorschrift über die audiovisuelle Sendung durch Internet und andere Informationsnetzwerke" des Hauptamts für Rundfunk, Film und Fernsehen; § 16(7) „die Vorschrift über die audiovisuelle Sendung durch Internet" des Hauptamts für Rundfunk, Film und Fernsehen und Ministerium für Informationsindustrie; § 16(7) „die provisorische Vorschrift über die Kultur im Internet" des Ministeriums für Kultur.

Diese Formulierung über die Verpflichtung der ISP wurde später vom „Gesetz über die Netzwerksicherheit“ im Jahr 2016 angenommen. In § 47 des „Gesetzes über die Netzwerksicherheit“ gibt es den gleichen Paragrafen.[29]

§ 21 des „Gesetzes über die Netzwerksicherheit“ beschreibt grundlegend die Verpflichtung der Betreiber eines Netzwerks, die seiner Definition[30] nach auch die ISP umfasst. Dieser Paragraf besagt:

> Das Schutzsystem für Netzwerksicherheit mit unterschiedlichen Niveaus wird vom Staat geschaffen. Die Betreiber des Netzwerks sollen nach der Forderung dieses Schutzsystems die vorliegenden Sicherheitsverpflichtungen erfüllen, das Netzwerk vor Störung, Zerstörung, unbefugtem Zugriff schützen und ein Datenleck, das Abfangen von Daten sowie Datenveränderung verhindern:
>
> (1) interne Sicherheitsmanagementsysteme und Betriebsverfahren aufstellen, die verantwortliche Person für Netzwerksicherheit bestimmen, die Verantwortung für Netzwerksicherheit konkretisieren;
>
> (2) Maßnahmen gegen die Netzwerksicherheit gefährdende Handlungen wie Computerviren, Netzwerkangriffe, unbefugte Zugriffe ergreifen;
>
> (3) technische Maßnahmen ergreifen, den Betriebszustand des Netzwerks und die Netzwerksicherheit überprüfen und protokollieren und die entsprechenden Webprotokolle mindestens sechs Monate erhalten;
>
> (4) technische Maßnahmen ergreifen, um die Daten zu sortieren, die wichtigen Daten zu sichern und zu verschlüsseln usw.;
>
> (5) die anderen Verpflichtungen aus Gesetzen und Anordnungen beachten.

Aus dieser Perspektive ist festzustellen, dass die Verpflichtung der ISP zur Verwaltung der rechtswidrigen Informationen einseitig betont wird, während die Privilegierung der ISP vom Gesetzgeber übersehen wird. Die Inhalte dieser Normen sind unklar. Die Verpflichtung der ISP wird nur auf eine allgemeine Weise formuliert. Die konkreten Forderungen und ihre Grenzen bleiben offen. Außerdem fehlt diesen Normen die Einheitlichkeit. Die Verpflichtungsregelungen liegen in unterschiedlichen Gesetzen, Anordnungen und Vorschriften vor, die von verschiedenen Behörden erlassen werden.

Jedoch vertritt die herrschende Meinung in der Literatur die These, die ISP sollten keine allgemeine Verpflichtung zur Überwachung und Forschung nach illegalen Inhalten übernehmen, mit der Begründung, die große Menge der Informationen im Internet mache die allgemeine und aktive Überwachung und Erforschung unmöglich.[31] Nach den Regelungen aus § 36 des Deliktsgesetzes hat der ISP nur dann

---

[29] Die Zusammenfassung über diese Verpflichtungsregelung bei *Chen Xingliang*, Rechtszeitschrift der Universität Peking Heft 1, 2017, 15 ff.; *Fan Jun*, Rechtszeitschrift der Universität Peking Heft 1, 2017, 30; *Qin Tianning/Zhang Mingxun*, Strafrechtliche Wissenschaft Heft 9, 2009, 43; *Zang Tiewei* (Hrsg.), Erläuterungen über das „Strafrechtsänderungsgesetz (IX)“, 2015, S. 192 ff.

[30] Vgl. § 76 Abs. 3 des Gesetzes über die Netzwerksicherheit der Volksrepublik China.

[31] Vgl. *Zhang Xinbao/Ren Hongyan*, Zeitschrift der Universität Renmin Heft 4, 2010, 24; *Yang Lixin*, Zeitschrift des nationalen Staatsanwalts-Instituts Heft 2, 2010, 5; *Liu Jiarui*, Geistiges Eigentum Heft 2, 2009, 21; *Wang Shengming* (Hrsg.), Erklärungen zum chi-

Verpflichtungen zur Sperrung und Löschung von Daten, wenn er Kenntnis von illegalen Inhalten bekommt. Aus diesem Verständnis heraus kann auch logisch abgeleitet werden, dass vom ISP nicht erwartet wird, die aktive und allgemeine Verpflichtung zu übernehmen.[32]

Es ist auch bemerkenswert, dass die Verneinung der allgemeinen Verpflichtung schon in dem „Entwurf der dritten Veränderung des Urheberrechtsgesetzes" im Jahr 2012 von der Nationalen Urheberrechtsverwaltung deutlich gemacht worden ist.[33] Außerdem wird in § 8 Abs. 2 der Interpretation von 2012 des Obersten Volksgerichts vorgesehen: Wenn die ISP die Delikte von Netzwerknutzern bezüglich des Informationsnetz-Übertragungsrechts nicht aktiv überprüfen, dürfen sie vom Volksgerichtshof nur aufgrund dieser Tatsache nicht als schuldig betrachtet werden. Diese Regelung weist indirekt darauf hin, dass die ISP keine aktive Verpflichtung zur Überprüfung und Überwachung der rechtswidrigen Informationen übernehmen sollen.

Allerdings bedeutet die Verneinung der allgemeinen und aktiven Verpflichtung der ISP nicht, dass sie ganz frei von Verpflichtungen sind. In der Literatur werden die Störerhaftung des TMG und die Sorgfaltspflicht (*duty of care*) der ECRL[34] und des DMCA auf rechtsvergleichende Weise diskutiert.[35] Es wird postuliert, dass die Verkehrspflichten im Zivilrecht in gewissem Maß auch für die ISP gelten sollten, weil die ISP im 21. Jahrhundert eine einem Veranstalter oder einem Manager vergleichbare Rolle spielten.[36] In dieser Meinung wird das *safe harbor*-Prinzip kritisch berücksichtigt, während die Verkehrspflichten der ISP nach dem allgemeinen Prinzip des gemeinschaftlichen Delikts betont werden.[37] Es wird auch darüber diskutiert, dass der ISP nur, wenn er die illegalen Inhalte kennt, die Sorgfaltspflicht trägt.[38] Insgesamt ist der Umfang dieser Verpflichtung noch nicht klar und diese Thematik bleibt umstritten.

---

nesischen Deliktsgesetz, 2010, S. 196; *Wang Liming*, Nördliche Rechtswissenschaft Heft 2, 2014, 36; *Liu Ying/Huang Qiong*, Zeitschrift der Universität Jinan (Sozialwissenschaftliche Ausgabe) Heft 3, 2010, 57; *Chen Jinchuan*, Geistiges Eigentum Heft 2, 2011, 59.

[32] Vgl. *Yang Lixin*, Zeitschrift des nationalen Staatsanwalts-Instituts Heft 2, 2010, 6.

[33] Vgl. § 69 Abs. 1 des „Entwurfs der dritten Veränderung des Urheberrechtsgesetzes" (2012).

[34] Vgl. Erwägungsgründe Nr. 47–48 der ECRL.

[35] Vgl. *Liu Jiarui*, Geistiges Eigentum Heft 2, 2009, 21; *Liu Wenjie*, Rechtszeitschrift der Universität Peking Heft 2, 2012, 400 ff.

[36] Vgl. *Liu Wenjie*, Rechtszeitschrift der Universität Peking Heft 2, 2012, 395 ff.; *Wu Weiguang*, Internet-Rechtszeitschrift Heft 1, 2011, 17 ff.; *Feng Shujie*, Chinesische Rechtswissenschaft Heft 4, 2016, 190 ff.

[37] Vgl. *Cui Guobin*, Chinesische Rechtszeitschrift Heft 4, 2013, 154 ff.

[38] Vgl. *Liu Jiarui*, Geistiges Eigentum Heft 2, 2009, 21.

C. Zivilrechtliche Privilegierungen

1. Verantwortlichkeit der Content Provider

In den chinesischen Gesetzen ist die Verantwortlichkeit von Content Providern nicht parallel zu anderen ISP wie Access Providern oder Hosting Providern eindeutig vorgesehen. Jedoch ist es sowohl in der Literatur als auch in der Rechtsprechung völlig unstrittig, dass der Content Provider für eigene Inhalte nach den allgemeinen Gesetzen und Prinzipien verantwortlich sein soll.[39] Darüber hinaus wird auch von Wissenschaftlern die Meinung vertreten, dass § 36 Abs. 1 des Deliktsgesetzes als Haftungsregelung für Content Provider interpretiert werden kann.[40]

2. Privilegien der Access Provider

a) Grundlegende Voraussetzungen der Privilegierung

Die Voraussetzungen für die Privilegierung des Access Providers werden eindeutig in § 20 der „Anordnung über den Schutz des Informationsnetz-Übertragungsrechts" genannt:

> Wenn die ISP auf Abruf von Nutzern automatische Zugangsdienste zur Verfügung stellen oder sie für Werk, Aufführung, Audio- und Videoprodukte von Nutzern automatische Durchleitungsdienste anbieten, tragen sie keine Entschädigungshaftung, sofern sie
>
> (1) die übermittelten Werke, Aufführungen, Audio- und Videoprodukte nicht ausgewählt und verändert,
>
> (2) dem bestimmten Nutzer diese Werke, Aufführungen, Audio- und Videoprodukte anbieten und verhindern, dass andere Nutzer sie bekommen.

Diese Privilegierung berücksichtigt, dass die gesetzliche Gefahr und der Aufwand der ISP für das Dienstleistungsangebot durch das Informationsnetzwerk beschränkt und reduziert werden sollen, um die Entwicklung der Internetindustrie zu fördern. Sowohl der Staatsrat, der diese Anordnung verabschiedet hat, als auch die meisten Wissenschaftler haben sich entschieden für diese Berücksichtigung ausgesprochen.[41]

Nach diesem Paragrafen gibt es zwei Arten von Access Providern, nämlich den Network Provider und den Access Provider. Die erste Voraussetzung der Privilegierung ähnelt der Formulierung in TMG, ECRL oder DMCA. Jedoch ist die zweite Voraussetzung anders als die oben genannten ausländischen Regelungen, weil diese Anordnung sich speziell auf das Informationsnetz-Übertragungsrecht bezieht.

---

[39] Vgl. *Lu Chunya*, Zeitschrift der Universität Henan für Wirtschaft und Recht Heft 5, 2012, 61; *Liu Ying/Huang Qiong*, Zeitschrift der Universität Jinan (Sozialwissenschaftliche Ausgabe) Heft 3, 2010, 57.

[40] *Lu Chunya*, Politik und Recht Heft 4, 2011, 125.

[41] Vgl. *Wu Handong*, Geistiges Eigentum Heft 5, 2012, 17.

b) Unvereinbarkeit zwischen dem Gesetz und der Anordnung

Die Privilegierung der Access Provider wird von § 36 des Deliktsgesetzes ausführlich beschrieben. Allerdings sind das Deliktsgesetz und die „Anordnung über den Schutz des Informationsnetz-Übertragungsrechts" in diesem Punkt unvereinbar.

Wie schon erwähnt, fehlt es den chinesischen Regelungen für die Verantwortlichkeit der ISP an einer Typisierung. In § 36 des Deliktsgesetzes werden das *safe harbor*-Prinzip und das entsprechende *red flag*-Prinzip für die Verantwortlichkeit der ISP auf allgemeine Weise vorgesehen. Deshalb kann man aus dem Wortlaut des § 36 des Deliktsgesetzes logisch ableiten, dass das *safe harbor*- und das *red flag*-Prinzip für alle Arten der ISP einschließlich der Access Provider gelten. Daraus ist zu folgern: Wenn die Access Provider Kenntnis von rechtswidrigen Inhalten haben und keine notwendigen Maßnahmen wie Sperrung oder Löschung der Inhalte ergreifen, sollen sie Haftung übernehmen. Aber nach § 20 der Anordnung gilt das *red flag*-Prinzip gerade nicht für die Access Provider. Dort gehört das Erfordernis der subjektiven Kenntnis von Access Providern nicht zu den Voraussetzungen der Privilegierung.

Das gleiche Problem besteht auch, wenn man die Beziehung zwischen § 36 des Deliktsgesetzes und § 7 Abs. 3 der „Interpretation über die Anwendung der Gesetze zu dem Zivilstreit bezüglich des Informationsnetz-Übertragungsrechts" des Obersten Volksgerichts analysiert, denn es fehlt der Interpretation auch an der Typisierung der ISP. Deshalb kann hieraus geschlussfolgert werden: Wenn die Access Provider die Delikte von Nutzern bezüglich des Informationsnetz-Übertragungsrechts kennen oder davon wissen sollten und sie keine notwendigen Maßnahmen ergreifen oder dem Nutzer Hilfe, wie technische Unterstützung, anbieten, sollen sie als Gehilfe (Beihelfer) Deliktshaftung übernehmen. Dieser Schluss steht auch wieder in Konflikt mit § 20 der Anordnung. Darüber hinaus existiert diese Problematik auch in § 69 des „Entwurfs der dritten Veränderung des Urheberrechtsgesetzes", in dem die Typisierung der ISP gleichermaßen fehlt.

Angesichts dieser Konflikte und Gesetzeslücken behaupten viele chinesische Wissenschaftler, dass das *red flag*-Prinzip für die Access Provider nicht gelte.[42] Das heißt, es ist notwendig, eine teleologisch einschränkende Auslegung zu § 36 des Deliktsgesetzes und § 7 Abs. 3 der Interpretation zu erarbeiten. Diese einschränkende Auslegung ist zu bejahen, da die Access Provider aus technischen Gründen nur eine sehr begrenzte Kontrollmöglichkeit für die rechtswidrigen Informationen besitzen.

---

[42] Vgl. *Lu Chunya*, Zeitschrift der Universität Henan für Wirtschaft und Recht Heft 5, 2012, 60; *Wu Handong*, Chinesische Rechtswissenschaft Heft 2, 2011, 44; *Zhang Xinbao/Ren Hongyan*, Zeitschrift der Universität Renmin Heft 4, 2010, 19. Es wird auch behauptet, dass das „sollten wissen" in § 36 Abs. 3 des Deliktsgesetzes für die Access Provider einschränkender interpretiert werden soll. Vgl. *Chen Jinchuan*, Geistiges Eigentum Heft 2, 2011, 60 ff.

Darüber hinaus wird von Wissenschaftlern vorgeschlagen, dass die Regelungen in § 36 des Deliktsgesetzes nach den unterschiedlichen Typen der ISP jeweils konkretisiert werden sollten.[43] Meines Erachtens kommt eine rechtsvergleichende Untersuchung der Anwendung und Auslegung des Gesetzes in China zugute. Obwohl es dem grundlegenden Rechtsrahmen bezüglich der Verantwortlichkeit der ISP an Systematik und Typisierung fehlt, können diese abstrakten Regelungen mithilfe der Erfahrungen anderer Länder weiter konkretisiert und bestimmt werden.

3. Privilegien der Caching Provider

Die Voraussetzungen für die Privilegierung des Caching Provider sind in § 21 der Anordnung über das Informationsnetz-Übertragungsrechts enthalten. Dieser Paragraf besagt:

> Wenn die ISP die Werke, Aufführungen, Audio- und Videoprodukte von anderen ISP automatisch speichern, um die Effizienz der Übermittlung der Informationen zu verbessern, und sie diese Services dem Nutzer nach dem technischen Verfahren automatisch anbieten, tragen sie keine Entschädigungshaftung, sofern sie
>
> (1) die automatisch gespeicherten Werke, Aufführungen, Audio- und Videoprodukte nicht verändern und
>
> (2) keinen Einfluss darauf haben, dass der ursprüngliche ISP, die Werke, Aufführungen, Audio- und Videoprodukte anbietet; sie wissen, wie der Nutzer Werke, Aufführungen, Audio- und Videoprodukte erhält;
>
> (3) die Informationen nach dem technischen Verfahren automatisch korrigieren, löschen oder sperren, wenn der ursprüngliche ISP die Werke, Aufführungen, Audio- und Videoprodukte korrigiert, löscht oder sperrt.

In der Literatur gibt es kaum spezifische Diskussionen über die Verantwortlichkeit der Caching Provider, wahrscheinlich deswegen, weil in der Praxis selten ein Rechtsstreit über das bloße Angebot der Caching Services besteht. Aber es ist auffällig, dass im Vergleich zu § 9 TMG in Deutschland die Bedingungen der Privilegierung für Caching Provider in China relativ einfach gehalten sind.

4. Privilegien der Hosting Provider

a) Grundlegende Voraussetzungen der Privilegierung

Die Voraussetzungen für die Privilegierung der Hosting Provider werden deutlich in § 22 der Verordnung über das Informationsnetz-Übertragungsrechts vorgesehen. Dieser Paragraf lautet:

> Wenn die ISP dem Nutzer eine Speicherung zur Verfügung stellen, damit er der Öffentlichkeit die Werke, Aufführungen, Audio- und Videoprodukte anbieten kann, tragen die ISP keine Entschädigungshaftung, sofern sie

---

[43] Vgl. *Liu Ying/Huang Qiong*, Zeitschrift der Universität Jinan Heft 3, 2010, 58.

(1) deutlich machen, dass der Speicherraum für den Nutzer angeboten wird, und Name, Ansprechperson, Netzwerkadresse der ISP bekannt machen,
(2) Werk, Aufführung, Audio- und Videoprodukt vom Nutzer nicht verändern,
(3) nicht kennen und auch nicht kennen müssen, dass Werk, Aufführung, Audio- und Videoprodukt von Nutzern die Rechte verletzen,
(4) nicht vom Werk, von der Aufführung oder dem Audio- und Videoprodukt des Nutzers direkt profitieren,
(5) das rechtsverletzende Werk, die Aufführung oder das Audio- und Videoprodukt nach Erhalt der Mitteilung der Rechteinhaber nach dieser Anordnung löschen.

b) Kenntnis der Inhalte

In den USA wurde zunächst eine verschuldensunabhängige Haftung der ISP bestimmt. Diese strenge Stellungnahme wurde von amerikanischen Gerichten durch eine Reihe von wichtigen Entscheidungen verändert. Der berühmte DMCA wurde vor diesem Hintergrund verabschiedet, damit die verschuldensunabhängige Haftung für ISP aufgehoben wird.[44] Wie schon erwähnt, werden die chinesischen Regelungen über die Verantwortlichkeit der ISP offensichtlich vom DMCA beeinflusst. Der oben genannte Kontext der Entstehung des DMCA ist in der Literatur in China schon von vielen Wissenschaftlern bemerkt worden. Deshalb wird von der herrschenden Meinung argumentiert, dass die Feststellung der Haftung der ISP verschuldensabhängig sei.[45]

Jedoch werden die subjektiven Erfordernisse in chinesischen Gesetzen und Anordnungen nicht einheitlich formuliert. In § 36 Abs. 3 des Deliktsgesetzes steht „Wissen“ (知道), während nicht nur „Kennen“ (明知), sondern auch „Kennenmüssen“ (应知) in den §§ 22–23 der Anordnung des Staatsrats 2006, in § 7 der Interpretation des Obersten Gerichtshofs 2012 und auch in § 69 des Entwurfs der Nationalen Urheberrechtsverwaltung 2012 existieren. Diesbezüglich sind Gesetz, Anordnung und Entwurf unvereinbar. Deshalb ist es umstritten, wie das „Kennen“ im Deliktsgesetz zu interpretieren ist.

In der Literatur gibt es zwei gegensätzliche Auffassungen. Nach der herrschenden Meinung bedeutet „Wissen“ (知道) sowohl „Kennen“ (明知) als auch „Kennenmüssen“ (应知).[46] Erstens kann nach dem Wortlaut (aus dem Chinesischen) des „Wissens“ zu diesem Schluss gekommen werden. Der Bedeutungsspielraum des

---

[44] Vgl. *Wang Qian*, Rechtswissenschaft Heft 6, 2010, 129 ff.; *Liu Deliang*, Studium des Rechts und der Wirtschaft Heft 5, 2001, 113 ff.

[45] *Wu Handong*, Chinesische Rechtswissenschaft Heft 2, 2011, 42 ff.; *Wang Liming*, Nördliche Rechtswissenschaft Heft 2, 2014, 37 ff.; *Xue Hong*, Technik und Recht Heft 1, 2000, 55 ff.; *Liu Deliang*, Studium des Rechts und der Wirtschaft Heft 5, 2001, 117 ff.; *Zhang Xinbao/Ren Hongyan*, Zeitschrift der Universität Renmin Heft 4, 2010, 20 ff.

[46] *Wu Handong*, Chinesische Rechtswissenschaft Heft 2, 2011, 43 ff.; *Chen Jinchuan*, Geistiges Eigentum Heft 2, 2011, 57; *Wang Qian*, Studium des Rechts und der Wirtschaft Heft 4, 2008, 52.

Begriffs lässt diese Auslegung zu. Zweitens wird diese Ansicht von Regierung und Rechtsprechung indirekt unterstützt. Die Interpretation des Obersten Gerichtshofs und der Entwurf der Nationalen Urheberrechtsverwaltung zeigen deutlich eine gesetzliche Tendenz, dass die subjektiv einschränkenden Voraussetzungen der Privilegierung der ISP das „Kennen" und das „Kennenmüssen" umfassen sollen. Diese Auffassung haben die Gerichte schon in viele Rechtsentscheidungen übernommen.[47] Außerdem wurde von dem ehemaligen Vizepräsidenten des Obersten Volksgerichts *Xi Xiaoming* geäußert, dass das „Wissen" in § 36 Abs. 3 Deliktsgesetz das „Kennen" und das „Kennenmüssen" einschließe und die subjektiven Erfordernisse des § 36 Abs. 3 Deliktsgesetz denen der §§ 22–23 der Anordnung des Staatsrats gleich seien.[48]

Jedoch ist diese Ansicht auf starke Kritik gestoßen. Es wird von vielen Rechtswissenschaftlern argumentiert, das „Kennenmüssen" sollte in der Interpretation des „Wissens" in § 36 Abs. 3 Deliktsgesetz nicht in Betracht kommen. Diese Position wird zunächst von der Entstehungsgeschichte des Deliktsgesetzes untermauert. Der erste und der zweite Entwurf des Deliktsgesetzes sahen das „Kennen" anstatt des „Kennenmüssens" oder des „Wissens" vor. Deshalb wird von einigen Wissenschaftlern die Meinung vertreten, dass man die einschränkende Auffassung des Gesetzgebers daraus erschließen könne.[49] In einem einflussreichen Buch, das von Gesetzgebern herausgegeben worden ist, wird auch argumentiert, dass das „Wissen" in § 36 Abs. 3 des Deliktsgesetzes die oben genannten Begrifflichkeiten umfasse.[50]

Zweitens wird auch der Aspekt der Auslegung nach dem Wortlaut des „Wissens" kritisiert, denn „Wissen" stehe für einen realen subjektiven Umstand von Kenntnis, während „Kennenmüssen" sich in der Regel auf Fahrlässigkeit beziehe und eine reale Kenntnis fehle. Deshalb sei es von der Logik her problematisch, das „Kennenmüssen" vom „Wissen" abzuleiten.[51]

Drittens verträgt sich die erste Meinung nicht mit der Verneinung der allgemeinen und aktiven Verpflichtung zur Überwachung und Überprüfung der ISP, das „Kennenmüssen" erfordert oft, dass die ISP einige e*x-ante*-Verpflichtungen übernehmen.[52] Auf der einen Seite führt die Aufnahme des „Kennenmüssens" in die Verantwortlichkeit der ISP dazu, dass sie eine schwere Haftung für fremde Infor-

---

[47] Vgl. *Xu Wei*, Wissenschaft des Rechts Heft 2, 2014, 164.

[48] Vgl. *Feng Shujie*, Chinesische Rechtswissenschaft Heft 4, 2016, 185; *Chen Jinchuan*, Geistiges Eigentum Heft 2, 2011, 57.

[49] Vgl. *Yang Lixin*, Das Verständnis und die Interpretation der Deliktshaftung im Netzwerk im Deliktsgesetz, Zeitschrift des nationalen Staatsanwalts-Instituts Heft 2, 2010, 8 ff.; *Zhang Xinbao/Ren Hongyan*, Zeitschrift der Universität Renmin Heft 4, 2010, 23; *Feng Shujie*, Chinesische Rechtswissenschaft Heft 4, 2016, 186.

[50] Vgl. *Wang Shengming* (Hrsg.), Erklärungen zum chinesischen Deliktsgesetz, 2010, S. 159.

[51] Vgl. *Feng Shujie*, Chinesische Rechtswissenschaft Heft 4, 2016, 186.

[52] Vgl. *Xu Wei*, Wissenschaft des Rechts Heft 2, 2014, 166.

mationen tragen.[53] Auf der anderen Seite ist es schwierig, ein klares und durchführbares Kriterium für die Bestimmung des „Kennenmüssens" zu finden.[54]

Neben den oben genannten gegensätzlichen Auffassungen gibt es auch eine einen Kompromiss suchende Meinung, der zufolge das „Wissen" in § 36 Deliktsgesetz grundsätzlich nur „Kennen" bedeute. Aber in einigen speziellen Konstellationen könne das „Wissen" auch als „Kennenmüssen" interpretiert werden.[55] Darüber hinaus wird in der Literatur angeführt, dass die Theorien, die das „Wissen" in der Richtung von „Kennen" und „Kennenmüssen" interpretieren, irren. Das „Wissen" lasse sich in zwei Fälle teilen, nämlich in das reale „Kennen" und in das „Grund haben, zu kennen". Dieses Verständnis könne den subjektiven Erfordernissen des *safe harbor*-Prinzips der USA entsprechen.[56]

Der ersten Meinung ist meines Erachtens zuzustimmen, vor allem im Hinblick auf die mögliche Bedeutung des „Wissens" kann man zu diesem Schluss kommen. Die Bedeutung des „Wissens" beschränkt sich nicht unbedingt nur auf das reale „Kennen". Außerdem steht das „Kennenmüssen" auch der Verneinung der allgemeinen und aktiven Verpflichtung zur Überwachung und Überprüfung der ISP nicht entgegen. Denn wie schon erwähnt, bedeutet die Verneinung der allgemeinen und aktiven Verpflichtung der ISP nicht, dass sie ganz verpflichtungsfrei sind. Wenn die ISP mit einigen Tatsachen oder Umständen konfrontiert sind, aus denen die rechtswidrige Handlung oder die Information erkennbar wird, kann im zivilrechtlichen Bereich berechtigterweise die Folgerung abgeleitet werden, dass die ISP schon das „Wissen" vom Delikt der Nutzer besitzen. Darüber hinaus ist diese Meinung aus rechtsvergleichender Sicht zu bejahen. Diese Einstellung wird schon sowohl im deutschen TMG als auch im US-amerikanischen DMCA eingenommen.

Schließlich sollte die Problembehandlung die ständige Weiterentwicklung der Netzwerktechnologie berücksichtigen. Die Privilegien der ISP, die aus ECRL, TMG oder DMCA stammen, beruhen auf technischen Einschränkungen der ISP für die Kontrolle der rechtswidrigen Informationen. Jedoch ist zu bemerken, dass diese Situation sich innerhalb eines bestimmten Bereichs in gewissem Maße verändert, wie beispielsweise die Anwendung des digitalen Wasserzeichens und des digitalen Fingerabdrucks schon in der Praxis zeigen, zwei Technologien, die die rechtswidrigen Informationen im Netzwerk wirksam filtern können, ohne dass die ISP schwer damit belastet werden.[57] Deshalb kann die Öffentlichkeit erwarten, dass die ISP all diese notwendigen und angemessenen Maßnahmen ergreifen.

---

[53] Vgl. *Yang Lixin*, Zeitschrift des nationalen Staatsanwalts-Instituts Heft 2, 2010, 9.

[54] Vgl. *Zhang Xinbao/Ren Hongyan*, Zeitschrift der Universität Renmin Heft 4, 2010, 23.

[55] Vgl. *Wang Liming*, Die Untersuchung des Deliktsgesetzes II, 2011, S. 142 ff.

[56] Vgl. *Yang Ming*, Zeitschrift der östlichen Universität in China für Politik- und Rechtswissenschaft Heft 3, 2010, 125.

[57] Vgl. *Wang Qian*, Studium des Rechts und der Wirtschaft Heft 4, 2008, 49.

c) Das notice and take down-Verfahren

Das *notice and take down*-Verfahren stammt aus den Privilegierungsregelungen im DMCA. Die §§ 22–23 der Anordnung des Staatsrats und § 36 Abs. 2–3 Deliktsgesetz haben das *notice and take down*-Verfahren übernommen. Zum einen können die Urheber den ISP die Tatsache einer Rechtsverletzung mitteilen und einfordern, dass die ISP die rechtsverletzenden Informationen löschen oder den Zugang zu ihnen sperren. Zum anderen können die ISP von der Deliktshaftung befreit werden, sofern sie die rechtswidrigen Inhalte nach der Erlangung der Kenntnis unverzüglich löschen oder sperren.

Die Aufnahme des *notice and take down*-Verfahrens durch die Gesetzgebung trifft allgemein auf Zustimmung: Mit diesem Verfahren könne eine Rechtsverletzung effektiver im Internet gefunden werden, weil die Urheber dazu bessere technische Möglichkeiten und eine stärkere Motivation hätten. Darüber hinaus werde eine programmierte Methode für die Privilegierung durch dieses Verfahren geschaffen, sodass eine Balance zwischen Rechten und Pflichten der ISP erreicht werde.[58]

Die detaillierten Schritte des *notice and take down*-Verfahrens und des entsprechenden *counter notification*-Verfahrens werden in den §§ 14–17 der Anordnung des Staatsrats formuliert. Obwohl das *counter notification*-Verfahren in § 36 Deliktsgesetz nicht genau beschrieben wird, vertreten allerdings Rechtswissenschaftler die Auffassung, dieses Verfahren könne von diesem Paragrafen logisch abgeleitet werden.[59]

III. Allgemeine strafrechtliche Verantwortlichkeit der ISP

A. Die Beziehung zwischen dem chStGB und den Verantwortlichkeitsregelungen in anderen Gesetzen

Im chinesischen Rechtssystem gibt es viele unterschiedliche Gesetze, Verordnungen und Vorschriften für die Verantwortlichkeit der ISP, denen aber Systematik und Vereinbarkeit fehlen. Im Gegensatz zu Deutschland existiert kein einheitliches Gesetz wie das TMG oder die ECRL über die Privilegierung der ISP in China. Die Verhältnisse zwischen Gesetz, Verordnung und Interpretation im zivilrechtlichen Bereich sind recht chaotisch, ganz zu schweigen von den Beziehungen zwischen chStGB und Verantwortlichkeitsregelungen in anderen rechtlichen Bereichen.

---

[58] Vgl. *Wang Liming*, Nördliche Rechtswissenschaft Heft 2, 2014, 36–37.

[59] Vgl. *Yang Lixin/Li Jialun*, Wissenschaft des Rechts Heft 2, 2012, 158; *Wang Liming*, ebenda, 41.

Bis heute wird dieses Thema nicht ausführlich und systematisch in der Wissenschaft diskutiert. Obwohl der Begriff und die Typen der ISP schon in der strafrechtlichen Literatur erwähnt werden, gerät die Frage, wie die Privilegierungen im zivilrechtlichen Bereich auf die strafrechtlichen Theorien übertragen werden können, nicht in den Fokus.

Unter dem Aspekt der Einheit der Rechtsordnung ist diese Trennung und Spaltung zwischen der strafrechtlichen und der zivilrechtlichen Bewertung zu kritisieren. Die erforderliche Einheit der Rechtsordnung wurde zuerst von *Engisch* in der Literatur diskutiert.[60] Obwohl seine Ausführungen auf Kritik gestoßen sind, ist es inzwischen Konsens, dass die rechtmäßige Handlung im zivilrechtlichen Bereich auch im strafrechtlichen Bereich erlaubt werden soll, weil der Wertungswiderspruch zwischen Zivilrecht und Strafrecht untragbar ist.[61] Nach diesem Verständnis ist es nicht akzeptabel, dass die ISP die strafrechtliche Verantwortlichkeit übernehmen sollen, während sie nach den zivilrechtlichen Regelungen gerechtfertigt werden können.

Deshalb sollen die Privilegierungen der ISP nach den zivilrechtlichen Regelungen vor der strafrechtlichen Verantwortlichkeit geprüft werden. Wenn die ISP nach den Privilegierungsregelungen im zivilrechtlichen Bereich nicht haften sollen, wird die Prüfung der strafrechtlichen Verantwortlichkeit aus arbeitsökonomischem Grund unnötig. Das Problem der Verantwortlichkeit von ISP hängt eng mit der Entwicklung des Internets und der Netzwerktechnologie zusammen. Das heißt, dies ist ein neu entstandenes Problemfeld, das mit den traditionellen strafrechtlichen Dogmatiken allein nicht gelöst werden kann. International sind wir in gewissem Maße zu einem grundlegenden Konsens über die Privilegierung der ISP gelangt, der aber nicht nur von dem zivilrechtlichen oder strafrechtlichen System abgeleitet wird. Dagegen beruht dieser Konsens auf technischen Kontrollmöglichkeiten der ISP, während der Ausgleich zwischen der Förderung zur Entwicklung der Informationsindustrie und der Ordnung und Sicherheit im Cyberspace insbesondere berücksichtigt wird.

Die Bestimmung der strafrechtlichen Verantwortlichkeit von ISP ist heutzutage zunehmend abhängig von dem Wissen außerhalb des traditionellen theoretischen Rechtssystems. Wenn wir uns auf ein geschlossenes strafrechtliches System beschränken würden, könnten die daraus abgeleiteten Ergebnisse nicht mit der Entwicklung der Gesellschaft in Einklang gebracht werden. Obwohl im chinesischen Rechtsrahmen die Systematik und Vereinbarkeit für die Beziehung zwischen StGB und Verantwortlichkeitsregelungen in anderen Gesetzen fehlen, können wir diese Schwäche in der Theorie wettmachen.

---

[60] Vgl. *Engisch*, Die Einheit der Rechtsordnung, 1935, S. 43 ff.; *ders.*, Einführung in das juristische Denken, 2005, S. 211 ff.

[61] Vgl. *Roxin*, AT I[4], § 14 E, Rn. 32; *Jakobs*, AT[2], 11. Abschn. 2, Rn. 4 ff.; *Krey/Esser*, AT[6], Rn. 449 ff.; *Günther*, Strafrechtswidrigkeit und Strafunrechtsausschluss, 1983, S. 90 ff.

B. Grundlegender Rechtsrahmen im strafrechtlichen Bereich

1. Vor Inkrafttreten des Strafrechtsänderungsgesetzes (IX)

Vor dem Inkrafttreten des Strafrechtsänderungsgesetzes gab es keinen spezifischen Paragrafen für die strafrechtliche Verantwortlichkeit der ISP im chStGB. Die Bestimmung der strafrechtlichen Verantwortlichkeit der ISP hing mit der Anwendung folgender Paragrafen zusammen: chStGB § 217 Verletzung des Urheberrechts (侵犯著作权罪); § 221 Verletzung des kommerziellen Rufs (损害商业信誉，商品声誉罪); § 246 Beleidigung und Verleumdung (侮辱罪、诽谤罪); § 250 Veröffentlichung der Werke zum Diskriminierung und Beleidigung der nationalen Minderheiten (出版歧视、侮辱少数民族作品罪); § 295 Vermittlung krimineller Methoden (传授犯罪方法罪); § 363 Abs. 1 Vervielfältigung, Veröffentlichung, Verbreitung pornografischer Materialien zur Gewinnerzielung (复制、出版、传播淫秽物品牟利罪); § 364 Abs. 1 Verbreitung pornografischer Materialien (传播淫秽物品罪). Ähnlich wie in Deutschland steht die strafrechtliche Verantwortlichkeit der ISP in China in einer sehr engen Beziehung mit der Verbreitung pornografischer Materialien. So verabschiedeten der Oberste Volksgerichtshof und die Oberste Volksstaatsanwaltschaft zwei wichtige Interpretationen über die Behandlung pornografischer Informationen im Internet.

§ 7 der ersten Interpretation über Pornografie im Netzwerk (2004)[62] lautet:

> Wer erkennt, dass andere pornografische Informationen herstellen, vervielfältigen, veröffentlichen, verkaufen oder verbreiten und ihnen Hilfe durch Internet Access, Server Hosting, Netzwerkspeicherung, Kommunikationskanäle, Ausgabenabrechnung usw. zur Verfügung stellt, wird als Teilnehmer bestraft.

§ 4 der zweiten Interpretation über Pornografie im Netzwerk (2010)[63] besagt:

> Wenn der Gründer oder direkt zuständige Manager einer Website weiß, dass andere pornografische Informationen herstellen, vervielfältigen, veröffentlichen, verkaufen oder verbreiten, und er die Veröffentlichung solcher Informationen auf seiner Website zur Gewinnerzielung zulässt oder unterlässt, wird er nach § 363 Abs. 1 chStGB (Verbreitung pornografischer Materialien zur Gewinnerzielung) verurteilt und bestraft.

§ 5 der zweiten Interpretation über Pornografie im Netzwerk (2010) lautet:

> Wenn der Gründer oder direkt zuständige Manager einer Website weiß, dass andere pornografische Informationen herstellen, vervielfältigen, veröffentlichen, verkaufen oder ver-

---

[62] "Interpretation of the Supreme People's Court and the Supreme People's Procuratorate of Several Issues on the Specific Application of Law in the Handling of Criminal Cases about Producing, Reproducing, Publishing, Selling and Disseminating Pornografic Electronic Information via the Internet, Mobile Communication Terminals and Sound Message Stations" (2004).

[63] "Interpretation (II) of the Supreme People's Court and the Supreme People's Procuratorate of Several Issues on the Specific Application of Law in the Handling of Criminal Cases about Producing, Reproducing, Publishing, Selling and Disseminating Pornografic Electronic Information via the Internet, Mobile Communication Terminals and Sound Message Stations" (2010).

breiten, und er die Veröffentlichung solcher Informationen auf seiner Website zulässt oder unterlässt, wird er nach § 364 Abs. 1 chStGB (Verbreitung pornografischer Materialien) verurteilt und bestraft.

§ 6 der zweiten Interpretation über Pornografie im Netzwerk (2010) sagt aus:

Wenn die Telekommunikationsbetreiber oder Internet-Service-Provider Kenntnis von einer pornografischen Website haben und ihr Internet Access, Server Hosting, Netzwerkspeicherung, Kommunikationskanäle, Ausgabenabrechnung usw. kostenpflichtig zur Verfügung stellen, wird die direkt zuständige Person nach § 363 Abs. 1 chStGB (Verbreitung pornografischer Materialien zur Gewinnerzielung) verurteilt und bestraft.

In der ersten Interpretation neigen der Oberste Gerichtshof und die Oberste Staatsanwaltschaft offensichtlich dazu, die ISP als Teilnehmer zu bestrafen, wie der Wortlaut nahelegt. Jedoch scheint die Formulierung in der zweiten Interpretation zweideutig: In der Literatur wird gefordert, dass die ISP nach dieser Interpretation als Täter bestraft werden sollen.[64] Aber es gibt auch kritische Stimmen, die die Handlungen der ISP in der Regel noch als Teilnahme behandelt haben wollen.[65]

2. Nach Inkrafttreten des Strafrechtsänderungsgesetzes (IX)

a) Inhalte der neuen Tatbestände

Angesichts der steigenden Cyberkriminalität hat der Gesetzgeber im Jahr 2015 im Strafrechtsänderungsgesetz (IX) drei neue Paragrafen angelegt, die sich mittelbar oder unmittelbar auf die strafrechtliche Verantwortlichkeit der ISP beziehen.

§ 286 Abs. 1 chStGB (Verweigerung der Erfüllung der Sicherheitsverpflichtungen im Informationsnetzwerk) lautet:

Wenn die Internet-Service-Provider die Erfüllung der Sicherheitsverpflichtungen im Informationsnetzwerk aus Gesetzen und Anordnungen verweigern und nach dem Erfordernis der Korrekturmaßnahmen von Regulierungsbehörden nicht korrigieren, werden sie mit Freiheitsstrafe bis zu drei Jahren, Gewahrsam (拘役), Überwachung (管制) oder Geldstrafe bestraft, sofern die Handlungen von Internet-Service-Providern

(1) die weite Verbreitung der rechtswidrigen Informationen verursachen oder
(2) die Offenlegung der Benutzerinformationen und schwere Folgen verursachen oder
(3) in besonders schweren Fällen den Verlust der Beweise in Strafsachen verursachen oder
(4) besonders schwere Fälle sind.

§ 287 Abs. 1 chStGB (illegale Nutzung von Informationsnetzwerken) besagt:

Wer durch das Informationsnetzwerk in besonders schweren Fällen eine der folgenden Handlungen begeht, wird mit Freiheitsstrafe bis zu drei Jahren oder Gewahrsam bestraft, zugleich oder in selbstständiger Weise wird er mit einer Geldstrafe belegt:

---

[64] Vgl. *Yu Zhigang*, Die Untersuchung zur Entfremdung der traditionellen Straftaten im Netzwerk, 2010, S. 371.

[65] Vgl. *Chen Xingliang*, Rechtszeitschrift der Universität Peking Heft 1, 2017, 27; ähnlich *Che Hao*, China Law Review Heft 1, 2015, 48.

(1) bei Gründung einer Webseite, die zur Nutzung von Betrug, Vermittlung krimineller Methoden, Herstellung und Verkauf von rechtswidrigen oder staatlich kontrollierten Sachen usw. dient;
(2) bei Verbreitung strafbarer Informationen bezüglich der Herstellung oder des Verkaufs von Drogen, Waffen, Pornografie usw.;
(3) bei Verbreitung von Informationen, um andere Verbrechen wie Betrug zu begehen.

§ 287 Abs. 2 chStGB (Hilfe für Informationen und Cyberkriminalität) legt fest:

Wer weiß, dass andere durch die Informationsnetzwerke Verbrechen begehen, und ihnen Internet Access, Server Hosting, Netzwerkspeicherung, Kommunikationskanäle, Werbung, Ausgabenabrechnung usw. zur Verfügung stellt, wird mit Freiheitsstrafe bis zu drei Jahren oder Gewahrsam bestraft, zugleich oder in selbstständiger Weise wird er mit einer Geldstrafe belegt.

b) Grundlage der neuen Tatbestände

aa) § 286 Abs. 1 chStGB

§ 286 Abs. 1 chStGB bezieht sich speziell auf die strafrechtliche Verantwortlichkeit der ISP, gehört also zu den Sonderdelikten. In der Vergangenheit konnten die Handlungen der ISP, die ihre Sicherheitsverpflichtungen nicht erfüllten, in der Theorie nach den relevanten Paragrafen nicht nur als Tat, sondern als Teilnahme bewertet werden. Nach der Änderung des chStGB werden die Straftäter nach § 286 Abs. 1 in der Regel nun als Täter betrachtet.

Nach der Meinung des Gesetzgebers ist das Phänomen, dass die ISP die Verpflichtungen von Gesetzen oder Vorschriften nicht erfüllen und dies manchmal schwere Folgen hat, in der Praxis weit verbreitet. Diese Unterlassung ist unter folgenden Gesichtspunkten schädlich: Erstens wird die Voraussetzung für Verbrechen im Netzwerk geschaffen; zweitens werden die Untersuchung und Bekämpfung der Cyberkriminalität gestört; drittens wird die Sicherheit persönlicher Daten von Bürgern beeinträchtigt. Auf der Grundlage dieser Überlegungen hat der Gesetzgeber diesen neuen Tatbestand vorgesehen.[66]

bb) § 287 Abs. 1 chStGB

Darüber hinaus hat § 287 Abs. 1 chStGB die strafrechtliche Verantwortlichkeit beeinflusst. Nach der traditionellen Theorie sind die in § 287 Abs. 1 chStGB beschriebenen Handlungen tatsächlich Vorbereitungen von Verbrechen im Netzwerk. Jedoch müssen die vorbereitenden Handlungen nach der neuen Regel als Vollendung behandelt werden. Das bedeutet, dass die Bestrafung der Cyberkriminalität deutlich vorverlagert wird und der Eingriff des Strafrechts früher stattfindet. Natürlich beeinflusst die Veränderung der Bestrafung der Täter wegen Cyberkriminalität

---

[66] Vgl. *Zang Tiewei* (Hrsg.), Erläuterungen über das Strafrechtsänderungsgesetz (IX), 2015, 190 ff.

auch die strafrechtliche Verantwortlichkeit der ISP, die den Tätern Internetdienste anbieten. Dieser neue Tatbestand zeigt eine umstrittene gesetzgeberische Tendenz, dass bereits die Vorbereitung einer Straftat als deren Vollendung interpretiert wird.[67]

Im Internet kann ein Straftäter in kurzer Zeit viele Menschen dazu bringen, zusammen eine Straftat zu begehen. Es ist auch einfach, eine Straftat gegen eine große Menge von Menschen im Internet zu richten. In vielen Fällen können nur die Aktivitäten der Organisation festgestellt werden, während die sozialschädlichen Handlungen von anderen Straftätern, die an verschiedenen Orten operieren, nicht detailliert identifiziert werden können. Außerdem ist es nicht einfach, die Umstände der Opfer festzustellen. Die oben genannten Schwierigkeiten könnten dazu führen, dass die Straftäter letztlich nicht bestraft werden. Angesichts dessen erließ der Gesetzgeber den neuen Tatbestand für die strafrechtliche Verantwortlichkeit der Täter, die durch Gründung einer Website oder Verbreitung relevanter Informationen für die nachfolgenden Straftaten vorbereitend agieren.[68]

cc) § 287 Abs. 2 chStGB

Aus dem gesetzlichen Wortlaut lässt sich nicht unmittelbar ablesen, dass der Tatbestand des § 287 Abs. 2 zum Bereich der Sonderdelikte gehört. Jedoch geht es bei den meisten Handlungen in diesem Paragrafen um Internetdienste. Deshalb wird die strafrechtliche Verantwortlichkeit der ISP durch diesen Paragrafen stark beeinflusst. In der Vergangenheit wurden ISP grundsätzlich als Teilnehmer bestraft, wenn sie Straftätern Infrastruktur im Netz zur Verfügung stellten. Nach diesem neuen Paragrafen muss der eigentliche Beihelfer als Täter bestraft werden.

Die Entwicklung der Netzwerktechnologie hat viele Veränderungen für die Gesellschaft mit sich gebracht und auch das Verständnis von Rechtsfragen wie die traditionelle Theorie der Beteiligung beeinflusst. Im Netzwerk spielt die Beihilfe für das Begehen der Straftat eine zunehmend größere Rolle als in der realen Welt. Die Beihilfe im Cyberspace kennzeichnet eine hohe Sozialschädlichkeit, die manchmal sogar stärker als die des Täters ist. Außerdem gibt es oft eine detaillierte und systematische Arbeitsteilung zwischen den Straftätern, die häufig keinen direkten Kontakt miteinander haben und den jeweils eigenen Teil der „Arbeit" relativ selbstständig erledigen. Diese Arbeitsteilung beruht nicht auf der konkreten Kommunikation zwischen den Straftätern, sondern auf dem üblichen Arbeitsablauf der kriminellen „Industrie". Dies führt dazu, dass die Bestimmung der Beteiligung nach der traditionellen Dogmatik sehr schwierig wird. Im Hinblick auf diese Über-

---

[67] Vgl. *Che Hao*, Rechtswissenschaft Heft 10, 2015, 11 ff.

[68] Vgl. *Zang Tiewei* (Hrsg.), Erläuterungen über das Strafrechtsänderungsgesetz (IX), 2015, S. 200 ff.

legungen wurde der neue Tatbestand erlassen, damit die Rechtsgüter der Bürger und der Gesellschaft besser geschützt werden können.[69]

c) Bewertung der neuen Tatbestände

Seit dem Erlass des Entwurfs des Strafrechtsänderungsgesetzes (IX) wird heftig diskutiert, ob die neuen Tatbestände vernünftig und gerechtfertigt sind. In dieser Diskussion ist § 287 Abs. 2 chStGB (Hilfe für Informationen und Cyberkriminalität) besonders umstritten. Bezüglich dieses Tatbestands nennen die Rechtswissenschaftler oft die Phänomene „Teilnehmer zum Täter" (共犯正犯化) oder „Gehilfe zum Täter" (帮助犯正犯化). In diesem neuen Paragrafen wird der ursprüngliche Teilnehmer (Gehilfe) durch einen eigenständigen Tatbestand als Täter bestraft. Zu dieser Gesetzgebung gibt es in der Literatur ganz gegensätzliche Auffassungen. Die Befürworter argumentieren mit folgenden Begründungen:

Erstens werde durch den neuen Tatbestand die Unverhältnismäßigkeit zwischen Unrecht und Strafe für die Teilnahme beseitigt. Wie schon erwähnt, stellt die Beihilfe im Netzwerk häufig – wegen der Besonderheiten der Beteiligung – einen höheren Grad der Rechtswidrigkeit und gesellschaftlichen Schädlichkeit als die Täterschaft selbst dar. Aber nach dem traditionellen Tatbestand und der Akzessorietät der Teilnahme wurde bislang der Gehilfe in der Cyberkriminalität grundsätzlich milder als der Täter bestraft. Ein eigenständiger Tatbestand für den ursprünglichen Gehilfen könne dieses Missverhältnis korrigieren.[70] Zweitens sei es möglich, dass die Teilnahme eine hohe gesellschaftliche Schädlichkeit oder Rechtsverletzung darstelle, während die Voraussetzungen für die Teilnahme nach der Theorie der Beteiligung nicht erfüllt seien. Wie schon erläutert, kommunizieren die Beteiligten wegen der Arbeitsteilung in der Cyberkriminalität häufig nicht miteinander und haben damit keinen gemeinsamen Vorsatz, der einer strafrechtlichen Verantwortlichkeit zugrunde liegt. Ohne Vorsatz dürften die das Rechtsgut massiv verletzenden Beteiligten schließlich nicht vom Strafrecht reguliert werden.[71] Drittens sei eine Vorverlagerung des Schutzes durch das Strafrecht gegen besonders schwere Straftaten erforderlich.[72] Das Verhalten im Netzwerk sei deutlich anders als in der realen Welt. Die Sozialschädlichkeit könne durch das Internet in kurzer Zeit mit wenig Aufwand schnell verbreitet, vervielfacht und vergrößert werden. Wegen der

---

[69] Vgl. ebenda, S. 206 ff.

[70] Vgl. *Yu Zhigang*, Sozialwissenschaften in China Heft 3, 2010, 125 ff.; *Zang Tiewei* (Hrsg.), Erläuterungen über das Strafrechtsänderungsgesetz (IX), 2015, S. 206 ff.; *Wang Aixian*, Zeitschrift der Universität Henan (Sozialwissenschaftliche Ausgabe) Heft 2, 2017, 40 ff.; *Yu Chong*, Kriminalwissenschaft Heft 1, 2017, 88; *Zhang Xiaona*, Erklärungen des nationalen Volkskongresses zum Strafrechtsänderungsgesetz (IX), Zeitung für Demokratie und Recht, 15.11.2015.

[71] Vgl. *Zang Tiewei* (Hrsg.), ebenda, S. 206 ff.; *Chen Yijian*, Rechtszeitschrift der Universität Zhongshan Heft 2, 2010, 301.

[72] *Zang Tiewei* (Hrsg.), ebenda, S. 206 ff.

Besonderheiten der Cyberkriminalität solle der Eingriff des Strafrechts durch das Konzept „Teilnehmer zum Täter" vorverlagert werden.[73] Schließlich wird die Ansicht vertreten, dass das Prinzip „Teilnehmer zum Täter" die Generalprävention des Strafrechts betone.[74] In der Literatur haben sich einige Rechtswissenschaftler auf die positive Generalprävention nach *Jakobs* berufen.[75]

Dagegen haben die Kritiker des neuen Tatbestands aus § 287 Abs. 2 chStGB folgende Argumente zusammengetragen: Erstens gebe es gar keine sogenannte Unverhältnismäßigkeit zwischen Unrecht und Strafe aufgrund der Besonderheit des chinesischen Beteiligungssystems. Wegen der Akzessorietät der Teilnahme wird der Teilnehmer, besonders der Beihelfer in Deutschland, in der Regel milder als der Täter bestraft. Das heißt, der Grad der Strafe ist zu einem großen Teil mit der Beteiligungsform des Straftäters verbunden. In diesem Kontext könnte die Unverhältnismäßigkeit zwischen Unrecht und Strafe wirklich bestehen.

Jedoch gibt es im chStGB das sogenannte duale Beteiligungssystem.[76] Auf der einen Seite existiert ein Beteiligungssystem, das auf den unterschiedlichen Rollen der Beteiligten beruht. Ähnlich wie in Deutschland gibt es in diesem System den Täter, den Anstifter, den Gehilfen und den Organisator.[77] Auf der anderen Seite besteht ein Beteiligungssystem, das auf der Wirkung der Beteiligten basiert. In diesem System gibt es den Hauptbeteiligten, der die Hauptwirkung in der Beteiligung hat, den Nebenbeteiligten, der nur eine nebensächliche Wirkung besitzt, und den unfreiwilligen Nebenbeteiligten, der von anderen gezwungen wird, sich an der Straftat zu beteiligen.

Im chStGB sind die beiden Beteiligungssysteme eng miteinander verzahnt. Wegen der Zusammenwirkung der beiden Beteiligungssysteme könnte die folgende Situation entstehen: Wenn der Täter, der den Tatbestand unmittelbar verwirklicht, nur eine nebensächliche Wirkung im Fall hat, wird er als Nebenbeteiligter bezeichnet. Wenn der Teilnehmer, der zur Verwirklichung des Tatbestands mittelbar beiträgt, eine Hauptwirkung hat, wird er auch als Hauptbeteiligter betrachtet. Nach den §§ 27–28 des chStGB sollen die Nebenbeteiligten und unfreiwilligen Nebenbeteiligten milder bestraft werden. Deshalb ist es nach diesen Regelungen durchaus möglich, dass die als Hauptbeteiligte betrachteten Teilnehmer schwerer als die als

---

[73] Vgl. *Yu Zhigang*, Sozialwissenschaften in China Heft 3, 2010, 118 ff.

[74] *Wang Aixian*, Zeitschrift der Universität Henan (Sozialwissenschaftliche Ausgabe) Heft 2, 2017, 42.

[75] Vgl. *Chen Yijian*, Rechtszeitschrift der Universität Zhongshan Heft 2, 2010, 307; *Li Can*, Zeitschrift der südöstlichen Universität (Sozialwissenschaftliche Ausgabe) Beilage Heft 18, 2016, 77.

[76] Vgl. *Qian Yeliu*, Chinesische Rechtszeitschrift Heft 1, 2012, 126 ff.

[77] Der Organisator ist eine spezielle Beteiligungsform, die auf das sowjetische Strafrecht zurückzuführen ist.

Nebenbeteiligte betrachteten Täter bestraft werden. Dann kann nicht von einer Unverhältnismäßigkeit zwischen Unrecht und Strafe gesprochen werden.[78]

Dem wird entgegengehalten, dass im Allgemeinen der Täter wesentlich gesellschaftsschädlicher als der Teilnehmer sei, weswegen der Teilnehmer natürlich milder als der Täter bestraft werden sollte. Gerade wenn der Gesetzgeber einen eigenständigen Tatbestand für den Teilnehmer vorsehe, bilde sich eine echte Unverhältnismäßigkeit zwischen Unrecht und Strafe.[79] Zweitens wird der Tatbestand in § 287 Abs. 2 chStGB kritisiert, weil die neue Gesetzgebung gegen die übliche Behandlung der neutralen Handlung verstoße. Das Anbieten der Internetdienste von ISP gehöre zur sogenannten neutralen Handlung, die wegen ihrer Alltäglichkeit und Neutralität nach der strafrechtlichen Dogmatik nicht bestraft werden soll. Durch diese neue Gesetzgebung mache der Gesetzgeber die neutrale Handlung strafbar.[80] Somit dürfte diese Gesetzgebung die gesunde Entwicklung der Informationsindustrie behindern. Drittens ist die Begründung der positiven Generalprävention unhaltbar, in der Literatur ist sie auf starke Kritik gestoßen. Die positive Generalprävention basiert auf dem Utilitarismus und steht nicht im Einklang mit dem grundlegenden Kant'schen Prinzip, dass der Mensch zum Zweck anstatt zum bloßen Mittel gehört.[81] Deshalb kann die positive Generalprävention die Gesetzgebung vom „Teilnehmer zum Täter" unterstützen.[82] Schließlich wird argumentiert, dass die Beteiligungstheorie nach dem allgemeinen Teil des chStGB schon ausreichend sei, um dieses Problem zu lösen, die gesetzgeberische Veränderung also unnötig. In der Literatur gibt es sogar eine spezielle Ansicht, die § 287 Abs. 2 chStGB nicht als neuen Tatbestand, sondern als eine Strafzumessungsregel einstuft.[83]

Ob der neue Tatbestand sowie das Prinzip „Teilnehmer zum Täter" gut oder schlecht ist, kann in dieser Arbeit nicht eindeutig bewertet werden. Dieser gesetzgeberische Modus ist ein zweischneidiges Schwert, das sowohl Vor- als auch Nachteile hat. Ein realistischer Vorschlag wäre, aus der dogmatischen Sicht im erweiternden Rechtsrahmen eine restriktive Auslegung abzuleiten.

Im Netzwerk existieren wirklich einige Besonderheiten von kriminellen Handlungen, die nicht übersehen werden dürfen. In vielen Konstellationen bewirkt der

---

[78] Vgl. *Wang Lin*, Politik und Recht Heft 9, 2016, 34 ff.

[79] Vgl. *Chen Yijian*, Rechtszeitschrift der Universität Zhongshan Heft 2, 2010, 298.

[80] Vgl. *Liu Yanhong*, Studium des Rechts und der Wirtschaft Heft 3, 2016, 18 ff., *ders.,* Law Review Heft 5, 2016, 40 ff.; *Xiong Yawen/Huang Yazhu*, Volksjustiz Heft 31, 2016, 75 ff.; *Li Can*, Zeitschrift der südöstlichen Universität (Sozialwissenschaftliche Ausgabe) Beilage Heft 18, 2016, 77 ff.

[81] Vgl. *Wang Bingbing*, Zeitschrift der Universität Suzhou (Rechtswissenschaftliche Ausgabe) Heft 1, 2017, 103.

[82] Vgl. *Yan Erpeng*, Sozialwissenschaftliche Zeitschrift Heft 4, 2016, 77.

[83] Vgl. *Zhang Mingkai*, Politik und Recht Heft 2, 2016, 2 ff.

ursprüngliche Teilnehmer tatsächlich eine größere gesellschaftliche Schädlichkeit als der Täter. Dies ist auf die spezielle Struktur des Netzwerks zurückzuführen. Zunächst hat sich der Zusammenhang zwischen Teilnehmern und Tätern verändert. Die traditionelle Beziehung in der realen Welt ist zumeist „eins zu eins", während das Verhältnis im Cyberspace oft „einer zu vielen" ist.[84] Im traditionellen Verhältnis bildet der Täter den Schwerpunkt, weil er als Schlüsselfigur den Tatbestand unmittelbar verwirklicht. Im neuen virtuellen Verhältnis hingegen handelt der Teilnehmer oft gleichzeitig mit vielen Tätern. Der ISP bietet zum Beispiel seine Internetdienste zahlreichen Nutzern zugleich an. In diesem Netzverhältnis sind die Teilnehmer als Knotenpunkt tätig, sodass der Schwerpunkt dieses Handlungszusammenhangs häufig vom Täter zum Teilnehmer verlagert wird.

Wenn sich der Fokus nur auf den unmittelbaren Zusammenhang zwischen Täter und Teilnehmer richtet, ergibt sich der Schluss, dass der Grad der Rechtswidrigkeit des Täters höher als der des Teilnehmers ist. Jedoch kehrt sich dieses Ergebnis um, wenn die Aufmerksamkeit auf das ganze System erweitert wird, das aus zahlreichen Tätern und Teilnehmern besteht. Obwohl der einzelne Täter den gegebenen Tatbestand direkt verwirklicht, hat er im ganzen System nur begrenzte Wirkung. Dagegen hat der Teilnehmer in vielen Konstellationen eine riesige Wirkung, obgleich er nur indirekt zur Verwirklichung des gegebenen Tatbestands beiträgt. Denn im „eins zu vielen"-System hat die Teilnahme auf erstaunliche Weise eine multiplikatorische Wirkung. Dementsprechend wirkt die Verletzung des Rechtsguts oder die gesellschaftliche Schädlichkeit auch stärker.

Darüber hinaus kommt der Teilnahme im Netzwerk eine verbindende Rolle zu, denn ohne den Teilnehmer in diesem System würden sich die zahlreichen, an völlig verschiedenen Orten ansässigen Täter nicht kennen. Mit der Verbindungsfunktion des Teilnehmers aber bilden alle Beteiligten ein System, in dem alle Täter durch eine systematische Arbeitsteilung zusammenarbeiten, obwohl der inzwischen von der strafrechtlichen Theorie geforderte gemeinsame Vorsatz nicht existiert. Da in diesem System der Teilnehmer, nicht der Täter, unentbehrlich ist, verwandelt das vom Teilnehmer organisierte System das einzelne Risiko in ein systematisches Risiko. Deshalb ist es in einigen Situationen notwendig, dass der Teilnehmer strenger als der Täter bestraft wird, weil im Vergleich zum einzelnen das systematische Risiko einer schwereren Strafe entspricht.

Jedoch ist die strengere Strafe keine vernünftige Begründung für den neuen Tatbestand. Denn wie schon erwähnt, kann der Teilnehmer im chinesischen dualen Beteiligungssystem schwerer als der Täter bestraft werden. Für die Höhe der Strafe allein sind der neue Tatbestand sowie das Prinzip „Teilnehmer zum Täter" also überflüssig. Außerdem führt der neue Paragraf zu einer unnötigen Konkurrenz zwischen unterschiedlichen Tatbeständen.

---

[84] Vgl. *Yu Zhigang*, Sozialwissenschaften in China Heft 3, 2010, 110, 119 ff.

Meines Erachtens erlaubt der neue Tatbestand eine mildere anstatt eine schwerere Strafe für die Straftäter. Denn nach § 287 Abs. 2 chStGB ist die Obergrenze der Strafe nur eine dreijährige Freiheitsstrafe, während die Obergrenze der Strafe in anderen relevanten Paragrafen viel höher sein dürfte. Zum Beispiel wird der Straftäter, der den Tatbestand nach § 363 Abs. 1 (Verbreitung pornografischer Materialien zur Gewinnerzielung) verwirklicht, im besonders schweren Fall mit Freiheitsstrafe ab zehn Jahren oder lebenslanger Freiheitsstrafe bestraft. Obwohl der Straftäter wegen der gesetzlichen Milderungsgründe milder bestraft werden kann, dürfte die endgültige Strafe viel schwerer als die dreijährige Freiheitsstrafe ausfallen.[85]

Die eigentliche Begründung für § 287 Abs. 2 chStGB sowie des Prinzips „Teilnehmer zum Täter" liegt in einer umfassenderen, aber milderen Kriminalisierung: Wegen der Besonderheiten des Netzwerks können die Voraussetzungen für die Teilnahme häufig nicht erfüllt werden, nach dem allgemein anerkannten Grundsatz der limitierten Akzessorietät kann die Teilnahme nur strafbar sein, wenn die Tatbestandsmäßigkeit und die Rechtswidrigkeit des Täters bestimmt worden sind.[86] Jedoch sind diese Erfordernisse des Täters im Cyberspace oft schwierig zu erfüllen, insbesondere, weil es im chStGB zahlreiche quantitative Elemente (Grad der Straftat) gibt, die als Voraussetzung der Strafbarkeit in der Form des „Schadensumfangs", „schwerer Folgen" und „besonders schwerer Fälle" vorgesehen werden.[87] Diese quantitativen Elemente bedeuten, dass der Grad der Rechtswidrigkeit der Strafbarkeit des Täters zugrunde liegt. Deshalb haben diese quantitativen Elemente tatsächlich eine interne Beziehung zur Lehre der strafwürdigen Rechtswidrigkeit in Japan[88] sowie zur Lehre der Strafrechtswidrigkeit von *Günther*.[89]

Im Netzwerk spielt ein einzelner Täter, der oft als böswilliger Nutzer erscheint, eine sehr geringe Rolle. Die schwerwiegende Verletzung der Rechtsgüter oder die schwere gesellschaftliche Schädlichkeit, die schon die Schwelle der strafrechtlichen Bewertung erreicht hat, besteht aus zahlreichen Bagatellschäden. Aber jeder Bagatellschaden, der von einem einzelnen Täter verursacht wird, kann die Voraussetzung der „quantitativen Elemente" nicht erfüllen. Deshalb dürfte ein einzelner Täter in diesem System die Strafbarkeit des gegebenen Tatbestands nicht haben. Dementsprechend wird die Strafbarkeit der Teilnahme nach dem Grundsatz der Akzessorietät verneint.

Darüber hinaus könnte die subjektive Voraussetzung für eine Beteiligung auch nicht erfüllt werden. Denn der Teilnehmer betreibt das ganze System und ist mit zahlreichen Nutzern gleichzeitig konfrontiert, sodass er in der Regel nicht in der

---

[85] Vgl. *Zhang Mingkai*, Politik und Recht Heft 2, 2016, 15.

[86] Vgl. *Rengier*, AT, § 45, Rn. 13; *Wessels/Beulke*, AT[38], Rn. 553.

[87] Vgl. *Liang Genlin*, ZStW 126, Heft 3, 2014, 773 ff.

[88] Vgl. *Asada*, ZStW 97, Heft 2, 1985, 194 ff.

[89] Vgl. *Günther*, Strafrechtswidrigkeit und Strafunrechtsausschluss, 1983, S. 394; *ders.*, Festschrift für Günter Spendel, S. 190.

Lage ist, mit den von unterschiedlichen Orten aus operierenden Tätern direkt zu kommunizieren.

Jedoch können diese Schwierigkeiten mit dem neuen Tatbestand sowie dem Prinzip „Teilnehmer zum Täter" leicht überwunden werden. Wenn für die ursprüngliche Teilnahme ein eigenständiger Tatbestand eingeführt wird, kommt die Akzessorietät zwischen Täter und Teilnehmer nicht mehr in Betracht. Einige Teilnehmer, die früher wegen der Akzessorietät nicht bestraft werden konnten, aber tatsächlich Rechtsgüter massiv verletzt haben, können nun durch den neuen Tatbestand auch zur Rechenschaft gezogen werden. Gleichzeitig werden Teilnehmer, die schon die Voraussetzungen der Beteiligung nach dem alten Tatbestand erfüllt haben, nach dem neuen Tatbestand vergleichsweise milder bestraft.

Schließlich sind die kritischen Argumente bezüglich der neutralen Handlung zu verneinen. Der neue Tatbestand in § 287 Abs. 2 chStGB bedeutet nicht, dass der Gesetzgeber die neutrale Handlung im Allgemeinen strafbar gemacht hat. Die in § 287 Abs. 2 chStGB beschriebenen Straftaten können mit der neutralen Handlung überhaupt nicht gleichgesetzt werden. Dementsprechend soll die Handlung der ISP wegen ihrer speziellen Eigenschaften nicht mit der neutralen Handlung gleichgestellt werden, wie noch weiter zu erläutern sein wird.

C. Einordnung der Handlung der ISP als Tun oder Unterlassen

1. Allgemeine Abgrenzung von Tun und Unterlassen

Im chinesischen strafrechtlichen System ist die Abgrenzung zwischen Tun und Unterlassen die Basis für die Prüfung einer kriminellen Handlung. In der Literatur werden viele Theorien, beispielsweise aus Deutschland oder Japan, mittels der Rechtsvergleichung analysiert: Zum Beispiel werden die Kriterien, wie etwa der Schwerpunkt der Vorwerfbarkeit des strafrechtlichen Handelns, die Begehungskausalität, der aktive Energieaufwand, der Zustand des Rechtsguts, die gesellschaftliche Bedeutung, schon ausführlich beschrieben.[90]

Obwohl viele strafrechtliche Untersuchungen zu diesem Thema durchgeführt worden sind, bleibt die Abgrenzung zwischen Tun und Unterlassen weiterhin unklar. Nach der herrschenden Meinung spielt die Verpflichtung eine wichtige Rolle. Unter dem Tun versteht man die gegen das strafrechtliche Verbot gerichtete Handlung, die durch aktive körperliche Bewegung (Energieeinsatz) begangen wird. Als Unterlassen wird die Untätigkeit zur Verpflichtung bezeichnet, die zu dem Täter

---

[90] Vgl. *Zhang Mingkai*, Strafrechtliche Wissenschaft, 2011, S. 148 ff.; *Li Hong*, Die Untersuchung des Unterlassungsdelikts, S. 17 ff.; *Ma Kechang*, Die Grundsätze des Strafrechts in der Rechtsvergleichung, S. 179 ff.

gehört und von dem Täter erfüllt werden kann.[91] Jedoch ist dieses Kriterium nicht anwendbar, weil die oben genannte Definition von Tun und Unterlassen nur eine nachträgliche Beschreibung darstellt.

In der Literatur wird sogar die These vertreten, dass die kriminelle Handlung in einer ganz speziellen Konstellation gleichzeitig sowohl ein Tun als auch ein Unterlassen sein kann. Steuerverweigerung zum Beispiel wird in § 202 des chStGB als eine Kombination von Tun und Unterlassen betrachtet. Darin heißt es: „Wer mit Gewalt oder mit Drohungen die Steuer verweigert, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Haft und mit Geldstrafe bestraft". Das Mittel der Gewalt oder Drohungen beziehen sich auf aktives Tun, während die Verweigerung zum Unterlassen zählt.[92] Diese Meinung wird jedoch von anderen mit der Begründung kritisiert, das Tun beziehe sich auf das Verbot im Strafrecht, während es sich beim Unterlassen um das Gebot im Strafrecht handele. Das Tun sei dem Unterlassen genau entgegengesetzt, deshalb könne eine Straftat nicht gleichzeitig sowohl Tun als auch Unterlassen sein.[93]

Die Auffassung, nach der ein Tun und ein Unterlassen in einer Straftat gleichzeitig bestehen können, ist zu verneinen, denn die Abgrenzung zwischen Tun und Unterlassen ist keine reine faktische Bewertung, sondern eine normative Beurteilung. Da das Mittel der Gewalt oder Drohungen in § 202 des chStGB zur Verweigerung der Steuer dienen, liegt der Schwerpunkt der strafrechtlichen Bewertung in der Verweigerung. Deshalb soll die Straftat soweit als Unterlassen betrachtet werden.

2. Einordnung der Handlung von ISP als Tun oder Unterlassen

a) Möglichkeit der Einordnung

Früher wurde in der Literatur diskutiert, ob die Handlungen der ISP sowohl Tun als auch Unterlassen sein können. Nach einer – wenn auch unzutreffenden – Ansicht kann Cyberkriminalität sich nur als Tun, nicht als Unterlassen manifestieren.[94] Jedoch ist es Konsens, dass kriminelle Handlungen im Netzwerk nicht nur im

---

[91] Vgl. *Li Hong*, ebenda, S. 27; *Zhang Mingkai*, ebenda, S. 148; *Zhou Guangquan*, Strafrecht Allgemeiner Teil, 2011, S. 85; *Chen Xingliang*, Die normative strafrechtliche Wissenschaft I, S. 119 ff.; *ders.*, Die ontologische strafrechtliche Wissenschaft, S. 245 ff.; *Gao Mingxuan* (Hrsg.), Die strafrechtlichen Grundsätze I, 1993, S. 530 ff.

[92] Vgl. *Zhang Mingkai*, ebenda, S. 149 ff.; *Gao Mingxuan* (Hrsg.), Die chinesische strafrechtliche Wissenschaft, 1989, S. 99.

[93] Vgl. *Chen Xingliang*, Die ontologische strafrechtliche Wissenschaft, S. 259 ff.; *Lin Shantian*, Strafrecht Allgemeiner Teil I, 2000, S. 146.

[94] Vgl. *Guo Chuntao*, Info-Netzwerk Sicherheit Heft 10, 2005, 47.

aktiven Tun, sondern auch im Unterlassen bestehen können.[95] Dieses Verständnis gilt natürlich auch für die Handlungen der ISP.[96]

Weiterhin offen ist in der Literatur die Frage, ob die strafbare Handlung aller ISP sowohl Tun als auch Unterlassen sein kann. Es wird von einigen Wissenschaftlern gefordert, dass die Handlungen der Access Provider nicht als Unterlassen bestraft werden dürften, weil Access Provider wegen der enormen Menge der Informationen im Internet nur über sehr begrenzte Fähigkeiten verfügen, die rechtswidrigen Inhalte zu löschen oder zu sperren, weswegen sie die Verpflichtung, die illegalen Informationen zu beseitigen, nicht übernehmen sollten.[97] Außerdem würde die Verantwortlichkeit der ISP durch Unterlassung dazu führen, dass die Entwicklung der Informationsindustrie beeinträchtigt wird. Schließlich ähnelten die Services von Access Providern denen der Telekommunikationsunternehmen, die niemals für fremde Inhalte oder Handlungen verantwortlich sind.[98]

Diese Ausführungen klingen zunächst sehr einleuchtend. Auf der einen Seite haben die Access Provider im Vergleich zu anderen ISP, wie etwa Hosting Provider oder Caching Provider, gar keine Kontrolle über die übermittelten Informationen. Sie übermitteln Informationen oder vermitteln den Zugang zu diesen Informationen auf neutrale Weise. Auf der anderen Seite werden keine Verpflichtungen von Access Providern in den Privilegierungsregelungen vorgesehen. Weder im TMG, in den ECRL oder im DMCA außerhalb Chinas noch in den Gesetzen, Anordnungen oder Vorschriften in China werden die Access Provider aufgefordert, bestimmte Verpflichtungen zu erfüllen. Zum Beispiel gilt das *red flag*-Prinzip, wie schon erwähnt, auch nicht für die Access Provider.

Die oben genannte Auffassung, nach der die Handlung von Access Providern kein Unterlassen sein kann, erweist sich bei näherer Betrachtung jedoch als unzutreffend. Zum einen gibt es auch Ausnahmen für die Privilegierung der Access Provider. So gelten die Privilegien in § 8 Abs. 1 TMG beispielsweise nicht für Access Provider, wenn sie absichtlich mit dem Nutzer ihres Dienstes zusammenarbeiten, um rechtswidrige Handlungen zu begehen.

Zum anderen ist es auch in der Theorie durchaus möglich, dass Access Provider eine Straftat durch Unterlassung begehen, denn Access Provider sind nicht ganz verpflichtungsfrei, obwohl die allgemeine Verpflichtung zur Überwachung und Überprüfung der rechtswidrigen Inhalte und die Sperrungs- und Löschungsverpflichtung nach dem *red flag*-Prinzip von Access Providern schon von der herr-

---

[95] Vgl. *Du Jing*, Sozialwissenschaftliche Zeitschrift der Jiamusi-Universität Heft 4, 2005, 30; *Yang Caixia*, Der Sucher Heft 2, 2007, 96–97.

[96] Vgl. *Qin Tianning/Zhang Mingxun*, Strafrechtliche Wissenschaft Heft 9, 2009, 42 ff.

[97] Vgl. *Peng Wenhua*, Zeitschrift der Universität Foshan (Sozialwissenschaftliche Ausgabe) Heft 3, 2004, 56 ff.; *Meng Chuanxiang*, Zeitschrift der Universität Chongqing für Post und Telekommunikation (Sozialwissenschaftliche Ausgabe) Heft 6, 2012, 28.

[98] Vgl. *Pi Yong*, Law Review Heft 3, 2002, 145.

schenden Meinung verneint werden. Wenn einige Verpflichtungen, die üblich und zumutbar sind und den Access Providern keinen übermäßigen Aufwand verursachen, nicht von den Access Providern erfüllt werden, könnten sie als Unterlassungsdelikte betrachtet werden. Wenn die Straftat durch ein Tun begangen werden kann, ist es auch in der Theorie möglich, dass diese Straftat durch ein unechtes Unterlassen stattfinden könnte.

Zusammenfassend lässt sich feststellen, dass die kriminellen Handlungen aller ISP sowohl als aktives Tun wie auch als Unterlassen existieren können.

b) Kriterium für die Einordnung

In der chinesischen strafrechtlichen Literatur ist das Kriterium für die Einordnung der Handlung von ISP als Tun oder Unterlassen nicht eindeutig. Es gibt einige Stimmen, die die Services der ISP oft als aktives Tun betrachten. Diese Auffassung kann in der Diskussion über die strafrechtliche Verantwortlichkeit der ISP im *Kuaibo*-Fall exemplarisch nachvollzogen werden. In diesem Fall bot die Firma *Kuaibo* eine QVOD-Player-Software und eine entsprechende QSI-Encoding-Software an, mit denen die Nutzer Videodateien mit speziellem Format abspielen konnten. Gleichzeitig stellte *Kuaibo* dem Netzwerksystem durch ihre eigenen Server die unterstützende Zwischenspeicherung zur Verfügung, um die Videodateien schneller zu übermitteln.[99]

Einige Wissenschaftler ordnen die Zwischenspeicherung der Firma *Kuaibo* als aktives Tun ein, weil *Kuaibo* die populären Videodateien, die von den Nutzern mehrmals abgerufen werden, aktiv auf eigene Server gezogen hat. Genau mit dieser technischen Unterstützung von *Kuaibo* können die Nutzer mit der QVOD-Player-Software pornografische Videodateien lesen. Deshalb hat die Firma tatsächlich durch diese Handlung pornografische Videos gespeichert und ausgestellt.[100] Wenn der zentrale Server von *Kuaibo* bei der Übermittlung der Informationen erkennt, dass die Nutzer wegen der begrenzten Geschwindigkeit beim Download die Videodateien nicht schnell lesen können, gibt er sofort einen Befehl, dass der nahe liegende Caching Server den Nutzern die Videodateien anbietet. Diese aktive technische Unterstützung gehört daher zum Tun.[101]

In der Literatur wird auch angeführt, dass die Handlungen von *Kuaibo* eine Kombination von Tun und Unterlassen darstellen. Wenn die Firma *Kuaibo* die pornografischen Videodateien auf eigene Server zieht, bestehe schon ein aktives Tun.

---

[99] Vgl. Urteil der ersten Instanz zum *Kuaibo*-Fall, http://bjhdfy.chinacourt.org/public/detail.php?id=4343 [Stand: 15.09.2017].

[100] Vgl. *Zhou Guangquan*, Rechtszeitschrift der Universität Peking Heft 1, 2017, 53 ff.

[101] Vgl. *Fan Jun*, Rechtszeitschrift der Universität Peking Heft 1, 2017, 36 ff.

Danach habe sie wegen der Zwischenspeicherung die Pflicht, die rechtswidrigen Inhalte zu sperren oder zu löschen. Biete jedoch das Unternehmen den Nutzern durch seinen Caching Server die pornografischen Videodateien weiterhin an, ergebe sich deshalb dennoch ein Unterlassen.[102]

Jedoch sind die oben genannten Meinungen meines Erachtens zu verneinen. Auf der einen Seite wird die technische Grundlage der Zwischenspeicherung von diesen Wissenschaftlern falsch verstanden. Die Zwischenspeicherung ist heute schon im Netzwerk nicht nur als eine notwendige, sondern auch als eine übliche Netzwerktechnologie weltweit akzeptiert. Normalerweise läuft die Zwischenspeicherung automatisch, um die Informationen störungsfreier zu übermitteln. Wenn die übermittelten Dateien nicht durchgängig überspielt werden können, werden sie automatisch und kurzzeitig in bestimmten Servern zwischengespeichert, damit die Nutzer die benötigten Dateien nicht von den ursprünglichen Content Providern abrufen müssen. Das heißt, die pornografischen Videodateien werden nach dem allgemein anerkannten technischen Standard von den Servern automatisch gespeichert und nicht von *Kuaibo* aktiv angeboten. Die Beschreibung der Handlung von *Kuaibo*, dass sie die pornografischen Videodateien aktiv auf eigene Server zieht, stimmt in diesem Fall nicht mit den Tatsachen überein. Es existiert somit kein aktives Tun der Firma *Kuaibo*. Die oben genannten Meinungen sind deswegen unzutreffend, weil die technische Grundlage der Zwischenspeicherung nicht richtig verstanden worden ist.

Auf der anderen Seite wird die Natur des Anbietens der Zwischenspeicherung einseitig interpretiert. Das Anbieten der Zwischenspeicherung ist vor allem eine sozial nützliche Handlung, mit der die Nutzer berechtigterweise bessere Netzwerkdienste bekommen können. Deshalb sind diese Services nicht nur in hohem Maße erwünscht, sondern werden auch teilweise staatlich gefördert.[103] Es kann nicht verneint werden, dass das Anbieten der Zwischenspeicherung zur gerechten Nutzung der Netzwerkdienste dient. Der echte Schwerpunkt der strafrechtlichen Bewertung liegt nicht in dem Anbieten der Zwischenspeicherung, sondern in dem Unterlassen der *Kuaibo*-Firma, nachdem sie die pornografischen Videodateien schon gekannt hat.

D. Strafrechtliche Garantenpflichten der ISP

1. Allgemeine strafrechtliche Garantenstellungen

Nach der chinesischen traditionellen Theorie gibt es vier Arten von Quellen für die Garantenpflichten der Unterlassung, nämlich Gesetz, Amt oder Berufsarbeit,

---

[102] Vgl. *Zhang Mingkai*, Eine kurze Analyse des Urteils des *Kuaibo*-Falls, Volksgerichtszeitung, A 003, 14.09.2016.

[103] Vgl. *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, Rn. 22.

Rechtsgeschäft und vorangegangenes Tun.[104] Diese etablierte Ansicht gehört zu einer formalen Lehre, die jedoch – ähnlich wie in Deutschland – auf starke Kritik stößt. Die traditionelle Lehre kann kein wirksames Kriterium für die Garantenpflichten der Unterlassung nennen.[105]

Heute wird von immer mehr Wissenschaftlern die materiale Theorie vertreten.[106] Die Unterscheidung zwischen Beschützergarantenstellung und Überwachungsgarantenstellung, wie sie in Deutschland besteht, ist schon in vielen chinesischen strafrechtlichen Aufsätzen und Lehrbüchern akzeptiert worden. Aber bis in die Gegenwart gibt es für die Bestimmung der Garantenpflichten kein einheitliches und systematisches Kriterium, das allgemein von allen akzeptiert wird. In der Literatur existieren zu diesem Thema vielfältige Lösungsansätze, nach denen unterschiedliche Systeme von strafrechtlichen Garantenpflichten konstruiert werden.[107]

In Rechtspraxis und Rechtsprechung ist die formale Lehre leider noch dominant. Deshalb besteht immer die Gefahr, dass der Umfang der strafrechtlichen Garantenpflichten zu weit gefasst ist. In der Literatur wird eine Beschränkung der Garantenpflichten als eine grundlegende Tendenz dargestellt.

2. Strafrechtliche Garantenpflichten der ISP

Da der Umfang der strafrechtlichen Garantenpflichten der ISP weiterhin umstritten ist, ist es sinnvoll, alle zu diesem Thema vorhandenen Thesen zu beschreiben und zu analysieren.

a) Garantenpflichten aus Gesetz?

Bezüglich der strafrechtlichen Verantwortlichkeit werden die Garantenpflichten der ISP aus dem Gesetz diskutiert. In der ersten Instanz des berühmten *Kuaibo*-Falls hat der Richter sich auch auf die Garantenpflichten aus relevanten Gesetzen

---

[104] Vgl. *Gao Mingxuan/Ma Kechang* (Hrsg.), Strafrechtliche Wissenschaft, S. 67 ff.; *Zhou Guangquan*, Strafrecht Allgemeiner Teil, 2016, S. 109 ff.

[105] Vgl. *Zhang Mingkai*, Strafrechtliche Wissenschaft, 2011, S. 154 ff.; *Li Hong*, Die Untersuchung des Unterlassungsdelikts, 1997, S. 126 ff.

[106] Vgl. *Xie Shaohua*, Forum der Politikwissenschaft und des Rechts Heft 2, 2008, 133 ff.

[107] Zum Beispiel meint *Zhou Guangquan*, dass das vorangegangene Tun die einzige Quelle der strafrechtlichen Garantenpflichten ist. Vgl. *Zhou Guangquan*, Strafrecht Allgemeiner Teil, 2016, S. 113 ff. Andere Garantenpflichten einschränkende Meinungen vgl. *Zhang Mingkai*, Chinesische Rechtszeitschrift Heft 6, 2011, 136 ff.; *Li Hong*, Rechtszeitschrift der Universität Peking Heft 6, 2014, 1573 ff.; *Wang Ying*, Rechtszeitschrift der Universität Peking Heft 2, 2013, 325 ff.; *ders.*, Der Jurist Heft 2, 2013, 119 ff.; *Mao Lingling*, Orientalisches Recht Heft 3, 2014, 23 ff.; *Liu Xiaoshan/Sun Baomin*, Kriminalwissenschaft Heft 4, 2008, 33 ff.

bezogen.[108] Jedoch wird dieses Problem wegen des neuen selbstständigen Tatbestands für die strafrechtliche Verantwortlichkeit komplizierter.

aa) Vor Inkrafttreten des Strafrechtsänderungsgesetzes (IX)

Vor dem Inkrafttreten des Strafrechtsänderungsgesetzes (IX) war die Bestimmung der strafrechtlichen Verantwortlichkeit von der Anwendung der traditionellen Tatbestände im chStGB abhängig, etwa wie § 363 Abs. 1 Vervielfältigung, Veröffentlichung, Verbreitung pornografischer Materialien zur Gewinnerzielung, § 364 Abs. 1 Verbreitung pornografischer Materialien. Offensichtlich gehören diese Tatbestände zum aktiven Tun. Da die rechtswidrigen Informationen im Netzwerk in der Regel nicht direkt von den ISP, sondern von ihren Nutzern angeboten werden, sind die Handlungen der ISP schwer als aktives Tun bei den Verbreitungsdelikten einzuordnen. Aus diesem Grund hat sich die theoretische Diskussion auf die unechte Unterlassung konzentriert.

Wie schon erläutert, gibt es im chinesischen Rechtsrahmen eine Reihe von Gesetzen, Verordnungen und Vorschriften, die die Verpflichtung der ISP vorsehen. In diesen Normen wird die allgemeine und aktive Verpflichtung der ISP festgestellt, während der Inhalt dieser Verpflichtung weiterhin nicht konkretisiert wird. In Anbetracht dessen ist ein formales Kriterium für die Bestimmung der Garantenpflichten in diesem breiten Rechtsrahmen nicht zu bejahen. Nach einer formalen Lehre kann der Umfang der Garantenpflichten der ISP sehr weit bemessen sein, weil es leicht ist, eine Rechtsgrundlage für die Quelle der Verpflichtung zu finden. Die vorhandenen Gesetze, Verordnungen und Vorschriften formulieren für die ISP nur die allgemeinen Forderungen. Sie sind allerdings nicht direkt als Quelle für die strafrechtlichen Garantenpflichten der ISP zu betrachten.

bb) Nach Inkrafttreten des Strafrechtsänderungsgesetzes (IX)

Nach dem Inkrafttreten des Strafrechtsänderungsgesetzes (IX) wird die Unterlassung der ISP im chStGB bestimmt. Wenn die ISP die Sicherheitsverpflichtungen im Informationsnetzwerk aus Gesetzen und Anordnungen nicht erfüllen und die erforderlichen Korrekturmaßnahmen nicht umsetzen, werden sie nach § 286 Abs. 1 chStGB bestraft.

In der Literatur wird § 286 Abs. 1 chStGB von der herrschenden Meinung als echte Unterlassung betrachtet,[109] während die Mindermeinung § 286 Abs. 1 chStGB als

---

[108] Vgl. Urteil der ersten Instanz über *Kuaibo*-Fall, http://bjhdfy.chinacourt.org/public/detail.php?id=4343 [Stand: 15.09.2017].

[109] Vgl. *Xie Wangyuan*, Chinesische Rechtswissenschaft Heft 2, 2017, 241; *Liang Genlin*, Rechtswissenschaft Heft 2, 2017, 10.

unechte Unterlassung interpretiert haben will.[110] § 286 Abs. 1 chStGB ist meines Erachtens natürlich nur als echte Unterlassung zu verstehen, weil die Formulierung des Tatbestands deutlich gemacht hat, dass dieses Delikt nur durch Unterlassung begangen wird. Die Unterlassungsstrafbarkeit der Garantenstellung ist schon im Straftatbestand geregelt.[111]

Jedoch ist die Bedeutung der „Sicherheitsverpflichtungen im Informationsnetzwerk aus Gesetzen und Verordnungen" völlig unklar. Auf der einen Seite sind die Inhalte der „Sicherheitsverpflichtungen" sehr umfangreich. Es gibt zu viele Faktoren, die die Sicherheit des Netzwerks gefährden. Allerdings können die ISP nicht alle diese Faktoren kontrollieren. Vor dem Inkrafttreten des Strafrechtsänderungsgesetzes (IX) war der Entwurf des § 286 Abs. 1 chStGB schon wegen der Unbestimmtheit der „Sicherheitsverpflichtungen" kritisiert worden.[112] Im Gesetzgebungsverfahren konzentrierte sich dann die Diskussion über § 286 Abs. 1 chStGB auf zwei Aspekte: Erstens gebe es zu viele Verbote. Würden die ISP alle Forderungen aus diesen Normen umsetzen, wären sie nicht imstande, ihre Dienste zu betreiben. Außerdem überschritten die Aufsichtsbehörden oft die Grenze der Berechtigung von ISP. Die ISP seien zweitens häufig nicht in der Lage, die Rechtswidrigkeit der Informationen festzustellen.[113] Deshalb müssten die Inhalte der „Sicherheitsverpflichtungen" in der Auslegung des Tatbestands konkreter präzisiert werden.

Auf der anderen Seite ist der Umfang der „Gesetze und Verordnungen" ebenfalls unbestimmt. Die Gesetze, Verordnungen und Vorschriften werden von unterschiedlichen Behörden erlassen, sodass sie verschiedene Rechtswirksamkeiten haben. Deshalb ist zu diskutieren, welche Normen die Quelle der strafrechtlichen Verpflichtung in § 286 Abs. 1 chStGB sein können.

Darum haben die chinesischen Rechtswissenschaftler viele Lösungen vorgeschlagen, um die „Sicherheitsverpflichtungen im Informationsnetzwerk aus Gesetzen und Verordnungen" teleologisch beschränkend auszulegen.[114] Zu Recht wird festgestellt, dass die Auslegung des Tatbestands des § 286 Abs. 1 chStGB sich nicht nur auf die logische und systematische Ableitung beschränken soll. Die technische Innovation in der Informationsgesellschaft, die Entwicklung der Industrie im Informationszeitalter und die durch die chinesische Verfassung garantierte Meinungsfreiheit sollen ebenfalls in Betracht kommen.[115]

---

110 Vgl. *Jing Lijia*, Politik und Recht Heft 1, 2017, 63.

111 Vgl. *Rengier*, AT, § 48, Rn. 7.

112 Vgl. *Liu Renwen/Zhang Hui*, Vorschläge zur Verbesserung der Verfolgung von Cyberkriminalität im Entwurf des Strafrechtsänderungsgesetzes (IX), Volksgerichtszeitung, 12.08.2015.

113 Vgl. *Zhou Guangquan*, Rechtswissenschaftliche Zeitschrift Heft 5, 2015, 80.

114 Vgl. *Wang Wenhua*, Volksstaatsanwaltschaft Heft 6, 2016, 24.

115 Vgl. *Liang Genlin*, Rechtswissenschaft Heft 2, 2017, 11 ff.

Die Inhalte der „Sicherheitsverpflichtung“ müssen konkreter erläutert werden. Es wird in der Literatur argumentiert, dass die „Sicherheitsverpflichtung“ sich hauptsächlich auf die Sicherheit der Inhalte der Informationen und die Sicherheit des Informationssystems beziehe.[116]

Dem ist entgegenzuhalten, dass der Umfang der „Sicherheitsverpflichtung“ weitreichender als der der Sicherheit der Informationsinhalte ist. Die Kernbedeutung der „Sicherheitsverpflichtung“ ist die Verwaltung der Verbreitung der Informationen. Nach diesem Verständnis wird die Bedeutung der „Sicherheitsverpflichtung“ erweitert, sodass die Plattformprovider und die Betreiber der kritischen Infrastrukturen eine aktive Überprüfungsverpflichtung übernehmen müssen.[117]

Aber dieser Meinung ist nicht zu folgen. Das Problem, das hier diskutiert wird, sollte sich auf die strafrechtliche Verantwortlichkeit der ISP wegen der unterlassenen Kontrolle über die rechtswidrigen Informationen von Dritten konzentrieren. Von den ISP wird nicht erwartet, dass sie die Verbreitung der Informationen verwalten; dazu sind sie ja gar nicht in der Lage. Außerdem trifft der Begriff der „Plattformprovider“, wie schon erwähnt, nicht zu; die Bedeutung der Plattform ist diffus, sodass viele ISP mit unterschiedlichen Funktionen darunter eingeordnet werden. Eine Plattform ist im Netzwerk ein übliches Konzept, wenn aber die strafrechtliche Verantwortlichkeit der Betreiber einer Plattform geprüft wird, muss nach der konkreten Funktion der einzelnen ISP entschieden werden.

Darüber hinaus ist eine aktive Überprüfungsverpflichtung der ISP zu verneinen. Es herrscht Konsens, dass die ISP einschließlich der Plattformprovider keine allgemeine und aktive Überprüfungsverpflichtung übernehmen sollen. Diesbezüglich bleibt die grundlegende Meinung unverändert, obwohl sich in den letzten Jahren die Technologie der Netzwerksicherheit sehr schnell entwickelt hat. Außerdem kann die Forderung an ISP, die nötigen Sicherungsmaßnahmen zu ergreifen, auch nicht direkt mit der strafrechtlichen Verpflichtung gleichgesetzt werden.[118]

Trotz der oben genannten teleologischen Beschränkungen bleiben die Inhalte der „Sicherheitsverpflichtung“ noch zu umfangreich. In § 21 des „Gesetzes über die Netzwerksicherheit“ werden die Verpflichtungen der Betreiber der Netzwerke einschließlich ISP ausführlich dargestellt. Dieser Paragraf wird in der Literatur als die Quelle für die allgemeinen Sicherheitsverpflichtungen der ISP betrachtet.[119] Offen-

---

[116] Vgl. *Wang Wenhua*, Volksstaatsanwaltschaft Heft 6, 2016, 25.

[117] Vgl. *Jing Lijia*, Politik und Recht Heft 1, 2017, 58 ff.

[118] Ähnliche Meinung *Che Hao*, Der neue Kommentar zum *Kuaibo*-Fall, abrufbar unter http://www.law.pku.edu.cn/xwzx/pl/16871.htm [Stand: 15.09.2017].

[119] Vgl. *Xie Wangyuan*, Chinesische Rechtswissenschaft Heft 2, 2017, 242. Mehr Mehr Zusammenfassungen der Inhalte der „Sicherheitspflichten“ der ISP siehe *Ouyang Benqi/Wang Qian*, Zeitschrift des Jiangsu Verwaltungsinstituts Heft 4, 2016, 126; *Peng Yuyong*, Zeitschrift der Universität Jinan (Sozialwissenschaftliche Ausgabe) Heft 12, 2014, 76 ff.

sichtlich umfasst er so viele Verpflichtungen der ISP, dass die Auslegung des Tatbestands in § 286 Abs. 1 chStGB nach den besonderen Umständen in einzelnen Fällen weiter beschränkt werden soll.

Außerdem wird der Umfang der „Gesetze und Anordnungen" von vielen Rechtswissenschaftlern beschränkend interpretiert. Nach der herrschenden Meinung fokussieren sich die „Gesetze und Anordnungen" in § 286 Abs. 1 chStGB nur auf die vom Nationalen Volkskongress oder dem Ständigen Ausschuss des Nationalen Volkskongresses erlassenen Gesetze und vom Staatsrat verabschiedeten Vorschriften.[120] Das heißt, ministeriale Anordnungen und örtliche Vorschriften dürfen nicht zur Quelle der strafrechtlichen Verpflichtung werden.[121]

Schließlich ist zu beachten, dass es nach dem Inkrafttreten des Strafrechtsänderungsgesetzes (IX) zwei Möglichkeiten für die Bestimmung der strafrechtlichen Verantwortlichkeit der ISP – jeweils nach § 286 Abs. 1 chStGB und den anderen relevanten traditionellen Tatbeständen – gibt. Bei Bezugnahme auf die traditionellen Tatbestände werden die Handlungen der ISP oft als unechte Unterlassungsdelikte betrachtet. Die traditionellen Tatbestände kennen keine direkte Formulierung eines Tatbestands über die Verpflichtung der ISP. Eine materiale Ansicht ist hier unentbehrlich, um die Garantenpflichten der ISP endgültig zu bestimmen. Bezieht man sich jedoch auf § 286 Abs. 1 chStGB, sind die ISP nur als echte Unterlassungsdelikte anzusehen. Allerdings ist es schwierig, die konkreten Inhalte der Verpflichtung der ISP nur durch die Auslegung des Blanketttatbestands in § 286 Abs. 1 chStGB zu bestimmen. Um die Sicherheitspflichten zu beschränken, ist eine materiale Position notwendig.

b) Garantenpflichten aus Ingerenz?

Obwohl viele chinesische Rechtswissenschaftler anmerken, wie wichtig es sei, die Verpflichtungen der ISP zu beschränken, gibt es kaum Untersuchungen, die sich auf das materiale Kriterium konzentrieren, um die Quelle und den Umfang der Verpflichtungen von ISP zu bestimmen. Deshalb wird die Möglichkeit, dass die Garantenpflichten der ISP aus Ingerenz stammen, nicht sehr ausführlich diskutiert.

Allerdings existieren zwei gegensätzliche Auffassungen über dieses Problem. Nach Meinung eines Richters, der unmittelbar mit dem Urteil des *Kuaibo*-Falls befasst war, gehört das Anbieten der Zwischenspeicherung von *Kuaibo* zu dem vorangegangenen Tun, aus dem sich die Garantenverpflichtung ableitet, denn die Zwischenspeicherung von *Kuaibo*, die mit den Handlungen von Content Providern

---

[120] Vgl. §§ 62, 67, 89 der Verfassung der Volksrepublik China; §§ 7, 56 des Gesetzgebungsgesetzes der Volksrepublik China.

[121] Vgl. *Xie Wangyuan*, Chinesische Rechtswissenschaft Heft 2, 2017, 241; *Wang Wenhua*, Volksstaatsanwaltschaft Heft 6, 2016, 25; *Li Bencan*, Juristisches Forum Heft 3, 2017, 145.

zusammenwirkt, führt zu der beschleunigten Verbreitung der pornografischen Informationen.[122] Ein anderer wissenschaftlicher Kommentar zum *Kuaibo*-Fall verneint diese Sichtweise, denn der Kausalverlauf zwischen dem Anbieten der Zwischenspeicherung und der Verbreitung pornografischer Informationen unterscheide sich vom Regelfall über die Garantenstellung aus vorangegangenen Handlungen.[123] Zwischen dem Anbieten der Plattform von *Kuaibo* und der erfolgreichen Verbreitung der pornografischen Informationen existierten zusätzlich die Handlungen der Nutzer, die die pornografischen Videodateien veröffentlichen, herunterladen und abspielen. Diese unterbrächen die Kausalitätskette zwischen dem Anbieten der Plattform und den schädlichen Folgen.[124]

Dem Kommentar ist zuzustimmen. Wenn die Verbreitung der pornografischen Informationen unmittelbar von den rechtswidrigen Handlungen der Nutzer abhängig ist, wird die tatsächliche Tatherrschaft der ISP deutlich geschwächt. Die schwache Kontrolle der ISP steht mit der Garantenstellung nicht im Einklang, was aber nicht heißt, dass das Anbieten der Zwischenspeicherung nicht zu der Garantenstellung führen kann, weil neben den Einflüssen der Nutzer die selbstständige Herrschaft der ISP über die Gefahrenquellen weiter beachtet werden muss.

Die richterliche Auffassung hingegen ignoriert eine wichtige Voraussetzung für das vorangegangene Tun, nämlich dass ein rechtmäßiges oder verkehrsgerechtes Vorverhalten keine Garantenstellung begründen kann,[125] und ist daher abzulehnen. Für die Garantenverpflichtung ist es außerdem erforderlich, dass das Vorverhalten eine nahe Gefahr des Eintritts des tatbestandsmäßigen Erfolges herbeigeführt hat.[126] Ein bloßes Anbieten der Zwischenspeicherung kann diese Voraussetzungen offensichtlich nicht erfüllen. Die Zwischenspeicherung ist ein üblicher und sozial nützlicher Netzwerkservice, sodass sie nicht als ein vorangegangenes Tun betrachtet werden sollte.

c) Garantenpflichten zum Schutz von Rechtsgütern?

Die Garantenpflichten der ISP zum Schutz von speziellen Rechtsgütern zu bestimmen, ist schwierig. Im Kommentar zum *Kuaibo*-Fall wird angeführt, die ISP hätten keine pflegende Position inne, wie etwa Eltern gegenüber ihren Kindern. Bezüglich der Verbreitung pornografischer Informationen seien die ISP nicht zu-

---

122 Vgl. *Fan Jun*, Rechtszeitschrift der Universität Peking Heft 1, 2017, 37.

123 Zum Beispiel: Ein Autofahrer fährt einen Fußgänger an und lässt ihn verletzt liegen. Vgl. *Rengier*, AT, § 50, Rn. 74; *Wessels/Beulke*, AT[38], Rn. 725.

124 Vgl. *Che Hao*, Der neue Kommentar zum *Kuaibo*-Fall, abrufbar unter http://www.law.pku.edu.cn/xwzx/pl/16871.htm [Stand: 15.09.2017].

125 Vgl. *Wessels/Beulke*, AT[38], Rn. 726.

126 Vgl. *Rengier*, AT, § 50, Rn. 96.

ständig für die Ordnung des kulturellen Marktes und die guten sozialen Sitten.[127] Dieser Ansicht ist zuzustimmen. Die ISP sind zuerst Marktteilnehmer, keine Aufsichtsbeamten. Deshalb sind sie nicht beauftragt, die relevanten Rechtsgüter zugunsten der Sauberkeit des Netzwerks zu beschützen.

d) Garantenpflichten aus Überwachung der Gefahrenquellen?

In der chinesischen Literatur gibt es nur wenige Aufsätze, die die Garantenpflichten aus Überwachung der Gefahrenquellen von einer materialen Ansicht her diskutieren. Einer Auffassung zufolge bestehe keine Gefahrenquelle im *Kuaibo*-Fall, denn die Nutzer könnten schließlich nicht als Gefahrenquelle angesehen werden. Es könne nicht unterstellt werden, dass alle Nutzer von *Kuaibo* mit dem entsprechenden Abspielgerät pornografische Videodateien zwangsläufig suchen und abspielen. Zudem weiche das Verhältnis zwischen *Kuaibo* und den Nutzern auch von dem Regelbeispiel für die Garantenpflichten aus Überwachung der Gefahrenquellen ab.[128] Mit anderen Worten: Die ISP seien keine Aufseher für die Nutzer.

Eine andere Ansicht besagt, dass die von ISP übermittelten und gespeicherten rechtswidrigen Informationen eine Gefahrenquelle darstellen könnten. Da die ISP, sobald sie Kenntnis von rechtswidrigen Informationen haben, über die Möglichkeit verfügen, die illegalen Inhalte zu löschen oder den Zugang zu ihnen zu sperren, könne die Garantenstellung der ISP aus Überwachung der Gefahrenquellen begründet werden.[129]

Diese Auffassung trifft den Kern der Problematik. Der theoretische Ansatz, die Gefahrenquelle auf die Nutzer zurückzuführen, ist nicht richtig, weil die Nutzer von den ISP unabhängig sind und im Hinblick auf die durch die Verfassung geschützten Rechte der Bürger auch nicht von den ISP überwacht werden dürfen. Aber die rechtswidrigen Informationen, die schon von ISP erkannt und tatsächlich kontrolliert worden sind, sollen in bestimmten Konstellationen als Gefahrenquelle von den ISP überwacht werden. In dieser Situation kann die Garantenstellung der ISP mit voller Berechtigung bestimmt werden.

e) Beschränkende Gründe aus anderen Rechtsgebieten

Wie schon erwähnt, gibt es in China kein einheitliches Gesetz wie das TMG, das die Verantwortlichkeit der ISP systematisch beschränkt und für alle Rechtsbereiche gilt. Im zivilrechtlichen Bereich wurde immerhin eine Reihe von Privilegierungsregelungen über die Verantwortlichkeit der ISP in Gesetzen, Anordnungen und Inter-

---

[127] Vgl. *Che Hao*, Der neue Kommentar zum *Kuaibo*-Fall, abrufbar unter http://www.law.pku.edu.cn/xwzx/pl/16871.htm [Stand: 15.09.2017].

[128] Vgl. ebenda [Stand: 15.09.2017].

[129] Vgl. *Liang Genlin*, Rechtswissenschaft Heft 2, 2017, 12.

pretationen kontinuierlich erlassen, beispielsweise §§ 20–23 „Anordnung über den Schutz des Informationsnetz-Übertragungsrechts", § 36 des Deliktsgesetzes usw. Deshalb haben die chinesischen Rechtswissenschaftler die zivilrechtliche Verantwortlichkeit der ISP durch Einführung des s*afe harbor*- und des *red flag*-Prinzips im Allgemeinen beschränkend bestimmt, obwohl im Detail noch theoretische Streitpunkte über die Auslegung der Privilegierungsregelungen bestehen. Ob und wie die zivilrechtlichen Privilegierungsregelungen auch im strafrechtlichen Bereich eingeführt und aufgenommen werden können, wird allerdings nicht ausreichend diskutiert.

In der aktuellen Literatur gibt es vereinzelte Beiträge, die sich in der Frage der strafrechtlichen Verantwortlichkeit der ISP auf die zivilrechtlichen Privilegierungsregelungen beziehen. Nach einer rechtsvergleichenden Untersuchung propagiert ein Wissenschaftler, dass die ISP keine aktive Überprüfungsverpflichtung zu rechtswidrigen Inhalten übernehmen sollten, sonst werde deren Geschäftsentwicklung wegen Überlastung beeinträchtigt.[130] Unter Berufung auf die Untersuchungen zu diesem Thema in Deutschland wird die Ansicht vertreten, dass die Access Provider wegen der fehlenden Kontrollmöglichkeiten über die vermittelten Informationen keine Garantenstellung besäßen, während die Caching Provider und Hosting Provider nach Kenntnis rechtswidriger Informationen Garantenpflichten haben könnten.[131]

Offenkundig wächst das Verständnis für die Bedeutung dieses Themas allmählich dadurch, dass die ausländischen Erfahrungen als Ressourcen der Rechtsvergleichung rezipiert werden. Obwohl im chinesischen Gesetzesrahmen kein spezielles Gesetz für die Privilegierung der strafrechtlichen Verantwortlichkeit von ISP besteht, können allgemein anerkannte Schlussfolgerungen in die Theorie einbezogen werden. Wenn die zivilrechtliche Verantwortlichkeit der ISP nach den Privilegierungsregelungen verneint wird, soll die strafrechtliche Verantwortlichkeit der ISP aus der Forderung der Einheitlichkeit der Rechtsordnungen abgelehnt werden. Dementsprechend können diese Privilegierungsregelungen in der materialen Prüfung der Garantenpflichten der ISP natürlich eine wichtige Rolle spielen.

f) Gleichstellung des Unterlassens mit dem Tun

Da vor dem Inkrafttreten des Strafrechtsänderungsgesetzes (IX) kein selbstständiger Tatbestand für die strafrechtliche Verantwortlichkeit der ISP bestanden hatte, beruhte die Bestimmung der Verantwortlichkeit auf der Auslegung der relevanten Tatbestände, die jedoch ursprünglich für aktives Begehen vorgesehen worden waren. Damit erschienen die Tätigkeiten der ISP oft als unechte Unterlassungsdelikte.

---

[130] Vgl. *Tu Longke*, Law Review Heft 3, 2016, 67 ff.

[131] Vgl. *Liang Genlin*, Rechtswissenschaft Heft 2, 2017, 12 ff.; *Yang Caixia*, Der Sucher Heft 2, 2007, 98. Ferner ähnliche Behauptung bei *Tu Longke*, Law Review Heft 3, 2016, 71 ff.

Die Gleichstellung des Unterlassens mit dem Tun führte folglich unvermeidlich zu Problemen.

Unter unechten Unterlassungsdelikten werden diejenigen Unterlassungen verstanden, die den gesetzlichen Tatbestand durch ein aktives Tun verwirklichen. In § 13 des deutschen Strafgesetzbuchs sind die Bedingungen einer unechten Unterlassung deutlich vorgesehen. Im Vergleich zu Deutschland gibt es jedoch im chinesischen Strafgesetzbuch keinen speziellen Paragrafen zu diesem Problemkreis. Deshalb ist die rechtsvergleichende Untersuchung in der Theorie von großer Bedeutung.

In Bezug auf die strafrechtliche Verantwortlichkeit der ISP wird von Rechtswissenschaftlern kritisch eingewendet, dass die Verbreitung pornografischer Informationen im Netzwerk durch ISP nicht als unechtes Unterlassungsdelikt bestraft werden sollte, weil das Unterlassen der Sicherheitspflichten im Netzwerk durch ISP nicht mit dem aktiven Tun der Verbreitung pornografischer Materialien zur Gewinnerzielung in § 363 chStGB gleichgesetzt werden könne. Nach dieser Logik wird die Garantiefunktion des Tatbestands im Namen des Schutzes der Rechtsgüter beeinträchtigt, sodass der Bereich der unechten Unterlassung erweitert wird und das Gesetzlichkeitsprinzip zerstört werden könnte.[132] Da in Deutschland spezielle Regeln über das Begehen durch Unterlassen im StGB bestehen, ist dieses Problem schon in angemessener Form gelöst worden. Aber nach dem chStGB verstoße die Bestrafung der unechten Unterlassung gegen das Gesetzlichkeitsprinzip.[133]

Diese Rechtswissenschaftler haben die Gleichstellung von Unterlassen und Tun missverstanden. In der Prüfung der Gleichstellung ist eine Gesamtbewertung unnötig. Es muss nicht eruiert werden, ob das Unterlassen in der Unrechtsbewertung mit dem aktiven Tun äquivalent ist, sonst wird die Rechtssicherheit durch diese Auslegung beeinträchtigt.[134]

Heute ist die herrschende Meinung die Lehre von der „Modalitätenäquivalenz", die auf die Erläuterungen von *Galas* über die „Handlungsmodalitäten" zurückzuführen ist.[135] Nach der Argumentation von *Galas* in der zweiten Lesung des Entwurfs im Jahr 1959 muss eine Gleichwertigkeit des Unterlassens mit dem Tun auch in Bezug auf die im Tatbestand vorausgesetzten besonderen Handlungsmodalitäten bestehen, wenn der Straftatbestand auch die Art und Weise beschreibt, mit der der Erfolg herbeigeführt werden muss. Zum Beispiel muss ein Vermögensschaden bei Betrug durch Täuschung verursacht werden.[136]

---

132 Vgl. *Gao Yandong*, Rechtszeitschrift der Universität Peking Heft 1, 2017, 68 ff.

133 Vgl. ebenda, 79 ff.

134 Vgl. Schönke/Schröder-*Stree/Bosch*, § 13, Rn. 4.

135 Vgl. *Roxin*, AT II, § 32, Rn. 225.

136 Vgl. *Roxin*, AT II, § 32, Rn. 219 ff.

Nach der herrschenden Meinung ist dieses Problem auf eine differenzierte Weise zu diskutieren. Bei den reinen Erfolgsdelikten wie Totschlag oder Körperverletzung spielt die Entsprechungsklausel keine selbstständige Rolle, weil die Gleichwertigkeit des Unterlassens mit dem aktiven Tun in dieser Situation schon durch eine Garantenstellung begründet worden ist. Aber bei den verhaltensgebundenen Delikten wie Betrug oder Nötigung kann die Gleichwertigkeit allein durch Garantenstellung nicht bestimmt werden, der Unrechtsgehalt dieses Handelns beruht nicht nur auf der Herbeiführung des Erfolgs, sondern auch auf dem speziellen Handlungsunwert.[137] Damit sind die „Handlungsmodalitäten" in dieser Konstellation in der Auslegung des Tatbestands detailliert zu prüfen.[138]

Zusammenfassend lässt sich feststellen, dass eine zusätzliche Prüfung über die Gleichstellung des Unterlassens mit dem Tun hauptsächlich von der unentbehrlichen Handlungsmodalität im Tatbestand abhängig ist. Es ist allgemein anerkannt, dass Unrecht eine Kombination von Handlungs- und Erfolgsunwert ist.[139] Die Gleichstellung des Unterlassens mit dem Tun dient hier dazu, dass der im Tatbestand vorausgesetzte Handlungswert in unechter Unterlassung auch mit Sicherheit verwirklicht werden kann.

Wenn die Gleichstellung des Unterlassens der Sicherheitspflichten von ISP mit dem aktiven Tun der Verbreitung pornografischer Materialien zur Gewinnerzielung in § 363 chStGB geprüft wird, ist zuerst die Struktur dieses Tatbestands zu analysieren. Es gibt keine speziellen Erfordernisse an die Art und Weise, in der der Erfolg des § 363 chStGB herbeigeführt werden muss. Nach der Beschreibung des Tatbestands können die pornografischen Inhalte in beliebiger Weise verbreitet werden. Solange die Handlung des Straftäters den Erfolg der Verbreitung der pornografischen Inhalte zur Gewinnerzielung zurechenbar herbeigeführt hat, wird der Tatbestand des § 363 chStGB verwirklicht. Wenn der ISP die Verpflichtungen zur Löschung pornografischer Informationen oder zur Sperrung des Zugangs hat, er sie aber absichtlich nicht erfüllt, damit die pornografischen Inhalte im Netzwerk weiterverbreitet werden, kann dieses Unterlassen des ISP mit einem aktiven Tun zur gewerbsmäßigen Verbreitung der pornografischen Inhalte gleichgesetzt werden.

---

137 Vgl. Kindhäuser/Neumann/Paeffgen-*Wohlers/Gaede*, § 13, Rn. 19.

138 Vgl. *Roxin*, AT II, § 32, Rn. 225; *Kindhäuser*, AT[7], § 36, Rn. 3.

139 Vgl. *Roxin*, AT I[4], § 10, Rn. 88.

E. Vorsatzerfordernisse

1. Die Möglichkeit der Fahrlässigkeitsdelikte?

Im chinesischen Rechtsrahmen gibt es in der Regel keine Möglichkeit für Fahrlässigkeitsdelikte von ISP. Ähnlich wie in Deutschland wird in § 15 chStGB vorgesehen: Die Fahrlässigkeitsdelikte sind nur mit positiver Bestimmung im StGB strafbar.

Bei allen vorhandenen Straftatbeständen im chStGB, die mittelbar oder unmittelbar im Zusammenhang mit der strafrechtlichen Verantwortlichkeit der ISP stehen, handelt es sich nur um vorsätzliche Begehungsdelikte. In den Tatbeständen für die sogenannten Verbreitungs- und Äußerungsdelikte, etwa § 246 chStGB (Beleidigung und Verleumdung), § 364 Abs. 1 chStGB (Verbreitung pornografischer Materialien), gibt es keine Fahrlässigkeit. Die neu erlassenen Straftatbestände wie § 286 Abs. 1 chStGB (Verweigerung der Erfüllung der Sicherheitsverpflichtungen im Informationsnetzwerk) und § 287 Abs. 2 chStGB (Hilfe für Informationen und Cyberkriminalität), die die strafrechtliche Verantwortlichkeit spezifisch direkt vorschreiben, beinhalten ebenfalls keine Fahrlässigkeitsdelikte.

In der Diskussion über die Einordnung des § 286 Abs. 1 chStGB als Fahrlässigkeits- oder vorsätzliche Begehungsdelikte gibt es aber auch einige wenige gegensätzliche Meinungen. Wie schon erläutert, schreibt § 286 Abs. 1 chStGB die strafrechtliche Verantwortung der ISP eigenständig vor. Deshalb spielt dessen Einordnung auf subjektiver Ebene eine wichtige Rolle für die Bestimmung der strafrechtlichen Verantwortlichkeit der ISP. Nach autoritativer Meinung gehört § 286 Abs. 1 chStGB zu den vorsätzlichen Begehungsdelikten.[140] Dagegen wenden Kritiker ein, diese Interpretation führe zur Überlappung von § 286 Abs. 1 chStGB und § 287 Abs. 2 chStGB. Wenn die ISP die Sicherheitspflichten im Informationsnetzwerk vorsätzlich nicht erfüllen, haben sie schon den Tatbestand der Hilfe für Informationen und Cyberkriminalität verwirklicht. Nach dieser Meinung gehört § 286 Abs. 1 chStGB im Hinblick auf die Koordinierung mit § 287 Abs. 2 chStGB zu den Fahrlässigkeitsdelikten.[141] Wenn die ISP davon ausgehen, dass die Straftat von Dritten durch ihre technischen Maßnahmen vermieden werden können, sie die Sicherheitsverpflichtungen im Informationsnetzwerk aber verweigern, sei ihr Verhalten als Fahrlässigkeitsdelikt einzuordnen. Aus der Verweigerung der Erfüllung der Sicherheitsverpflichtungen könne nicht unbedingt auf Vorsatz geschlossen werden.[142]

Darüber hinaus wird die Auffassung vertreten, dass die Grundlage der Strafbarkeit von § 286 Abs. 1 chStGB auf die Lehre der Aufsichtsfahrlässigkeit in Japan

---

[140] Vgl. *Zhang Mingkai*, Strafrechtliche Wissenschaft, 2016, S. 1050; *Xie Wangyuan*, Chinesische Rechtswissenschaft Heft 2, 2017, 247.

[141] Vgl. *Yu Zhigang*, Chinesische Rechtswissenschaft Heft 2, 2016, 23.

[142] Vgl. *Li Bencan*, Juristisches Forum Heft 3, 2017, 141 ff.

zurückzuführen sei.[143] Nach diesem Verständnis liegt der Grund für die Einführung der Fahrlässigkeitsschuld darin, dass der Gesetzgeber die Verantwortlichkeit der Internetplattformprovider durch den neuen Straftatbestand verstärken will. Hier wird die innere Struktur dieses Tatbestands weiter analysiert. Es wird auch gesagt, dass die unterschiedlichen Tatbestandsmerkmale in § 286 Abs. 1 chStGB verschiedenen Formen der *mens rea* entsprächen. Deshalb stelle der § 286 Abs. 1 chStGB eine Vorsatz-Fahrlässigkeit-Kombination dar.[144]

Die obigen Meinungen sind meines Erachtens nicht haltbar. Erstens führt die Einordnung des § 286 Abs. 1 chStGB als vorsätzliches Begehungsdelikt nicht zu einer vollständigen Überlappung von § 286 Abs. 1 chStGB und § 287 Abs. 2 chStGB. Der Schwerpunkt der strafrechtlichen Bewertung des § 286 Abs. 1 StGB liegt in der Verweigerung, Sicherheitsverpflichtungen im Informationsnetzwerk zu erfüllen, während § 287 Abs. 2 chStGB sich auf die Regulierung der Hilfe für Informationen und Cyberkriminalität konzentriert. Es muss bedacht werden, dass das Unterlassen der ISP nach § 286 Abs. 1 chStGB manchmal mit der Beihilfe von § 287 Abs. 2 chStGB koinzidieren könnte. Jedoch sind die Inhalte der Unterlassung der Sicherheitsverpflichtungen offensichtlich umfangreicher als die Hilfe für Informationen und Cyberkriminalität. Die Unterlassung der Sicherheitsverpflichtungen hängt nicht unbedingt von den kriminellen Handlungen anderer im Cyberspace ab. Außerdem gehört § 286 Abs. 1 chStGB zu den echten Unterlassungsdelikten, während in § 287 Abs. 2 chStGB ein normaler Tatbestand besteht, das heißt, die Strukturen beider Tatbestände können nicht einander gleichgestellt werden. Zudem ist Gesetzeskonkurrenz aus der Perspektive der gesetzgeberischen Technik üblich. Deshalb sind die obigen Ansichten von diesem Standpunkt aus nicht überzeugend.

Zweitens ist der Lehre einer Vorsatz-Fahrlässigkeit-Kombination nicht zu folgen. Die Umstände der Vorsatz-Fahrlässigkeit-Kombination und ihre Behandlung in Deutschland und China sind unterschiedlich. In § 11 Abs. 2 des deutschen StGB wird deutlich vorgesehen: Vorsätzlich im Sinne dieses Gesetzes ist eine Tat auch dann, wenn sie einen gesetzlichen Tatbestand verwirklicht, der hinsichtlich der Handlung Vorsatz voraussetzt, hinsichtlich einer dadurch verursachten besonderen Folge jedoch Fahrlässigkeit ausreichen lässt. Dieses strafgesetzliche Phänomen wird von den Rechtswissenschaftlern Vorsatz-Fahrlässigkeit-Kombination genannt.[145] Trotz der bestehenden Kontroverse ist dieses Problem im Allgemeinen schon durch eine selbständige Gesetzgebung gelöst worden.

---

[143] Vgl. *Lu Xu*, Untersuchung der Rechtsstaatlichkeit Heft 6, 2015, 62 ff.

[144] Vgl. *Yu Zhigang*, Chinesische Rechtswissenschaft Heft 2, 2016, 23 ff. Zu den Vorsatz-Fahrlässigkeit-Kombinationen im chinesischen StGB siehe *Chu Huaizhi/Yang Shuwen*, Chinesische Rechtszeitschrift Heft 1, 1999, 55 ff.; *diess.*, Zeitschrift für Strafrecht Heft 7, 2000, 447 ff.; *Yang Shuwen*, Der Grundriss der Vorsatz-Fahrlässigkeit-Kombination, 2004.

[145] Vgl. Kindhäuser/Neumann/Paeffgen-*Saliger*, § 11, Rn. 70; Schönke/Schröder-*Eser/Hecker*, § 11, Rn. 63; Lackner/Kühl-*Heger*, § 11, Rn. 23; Joecks/Miebach-*Radtke*, 2. Aufl. 2011, § 11, Rn. 134.

Im chStGB gibt es aber keine spezielle Regel zu diesem gesetzlichen Phänomen. Obwohl viele gegensätzliche Auffassungen[146] in der Theorie existieren, bleibt dieses Problem sehr umstritten, nicht zuletzt wird die Lehre der sogenannten Vorsatz-Fahrlässigkeit-Kombination heftig kritisiert. Denn in der Bestimmung der strafrechtlichen Verantwortlichkeit muss endgültig entschieden werden, ob die *mens rea* des Straftäters zur Fahrlässigkeit oder zum Vorsatz gehört. Viele andere Beurteilungen im chinesischen Strafrechtssystem, beispielsweise Versuch und Beteiligung, setzen die Bestimmung der Form der *mens rea* voraus. Obwohl die unterschiedlichen Tatbestandsmerkmale in einigen Delikten verschiedenen Formen der *mens rea* entsprechen könnten, ist es wichtig, eine normative Entscheidung über die Form der *mens rea* zu treffen. Die Vorsatz-Fahrlässigkeit-Kombination bedeutet, dass die Form der *mens rea* sowohl Vorsatz als auch Fahrlässigkeit sein könnte. Dieses Verständnis kann mit dem Prinzip der Verhältnismäßigkeit[147] und dem *ultima-ratio*-Prinzip[148] unvereinbar sein.

Schließlich hat der Gesetzgeber durch den Wortlaut der „Verweigerung" in § 286 Abs. 1 chStGB schon darauf hingewiesen, dass die Form der *mens rea* Vorsatz sein soll. Die Formulierung „Verweigerung" bedeutet, dass die ISP ihre Sicherheitsverpflichtungen schon gekannt haben, aber absichtlich nicht erfüllen.[149] Auf der anderen Seite kann die Fahrlässigkeit aus der Formulierung des § 286 Abs. 1 chStGB nicht abgeleitet werden. Deshalb ist die Möglichkeit der Fahrlässigkeit hier nach der Forderung von § 15 chStGB auszuschließen.

2. Vorsatzformen

Nach der herrschenden Meinung in Deutschland ist die Möglichkeit des bedingten Vorsatzes für die Verantwortlichkeit der ISP (ausgenommen Content Provider) verneint worden. Nach § 14 chStGB wird der Vorsatz in eine direkte und in eine bedingte Form unterteilt. Die meisten Straftatbestände im chStGB können sowohl mit direktem Vorsatz als auch mit bedingtem Vorsatz verwirklicht werden. Aber wegen der technischen Begrenztheit soll die strafrechtliche Verantwortlichkeit der ISP auch im subjektiven Aspekt beschränkt werden.

---

[146] Vgl. *Chu Huaizhi/Yang Shuwen*, Chinesische Rechtszeitschrift Heft 1, 1999; *Li Wenyan/Deng Zibing*, Chinesische Rechtswissenschaft Heft 5, 1999; *Zhang Mingkai*, Chinesische Rechtszeitschrift Heft 3, 1999; *Chen Xingliang*, Die normative strafrechtliche Wissenschaft I, 2008, S. 194; *Zhou Guangquan*, Moderne Rechtswissenschaft Heft 2, 2007.

[147] Vgl. *Zhou Guangquan*, ebenda, 40; *Ou Jinxiong*, Zeitschrift der Guangxi-Verwaltung und des Kader-Instituts für Politik und Recht Heft 4, 2005, 4.

[148] Vgl. *Xiang Chaoyang/Yue Yang*, Law Review Heft 3, 2005, 58 ff.; *Lao Dongyan*, Zeitschrift der Rechtsvergleichung Heft 1, 2009, 49; *Li Lanying*, Moderne Rechtswissenschaft Heft 4, 2005, 75 ff.

[149] Vgl. *Xie Wangyuan*, Chinesische Rechtswissenschaft Heft 2, 2017, 247.

In der chinesischen Literatur haben die Rechtswissenschaftler dieses Problem noch nicht eingehend untersucht, möglicherweise deswegen, weil im chinesischen Rechtsrahmen keine speziellen Privilegierungsregelungen – etwa wie im deutschen TMG – für ISP bestehen, die sich nicht nur auf den objektiven Aspekt, sondern auch auf den subjektiven Aspekt beziehen. Darüber hinaus werden die rechtswissenschaftlichen Ergebnisse über die Beschränkung der Verantwortlichkeit der ISP im zivilrechtlichen Bereich leider nicht in den strafrechtlichen Bereich einbezogen. Deshalb gibt es nur wenige Untersuchungen, die sich teilweise der beschränkenden Auslegung der subjektiven Elemente widmen.

Hier sind die Diskussionen über § 287 Abs. 2 chStGB spezifisch zu besprechen. Obwohl § 287 Abs. 2 chStGB nicht zu den Sonderdelikten von ISP gehört, kann aus der Beschreibung des Tatbestands festgestellt werden, dass § 287 Abs. 2 chStGB eng mit der strafrechtlichen Verantwortlichkeit der ISP verbunden ist. Es lässt sich sogar vorhersagen, dass die unter diesen Paragrafen fallenden Straftäter hauptsächlich ISP sein dürften. Deshalb bezieht sich die Art des Vorsatzes des § 287 Abs. 2 chStGB unmittelbar auf den subjektiven Aspekt der strafrechtlichen Verantwortlichkeit der ISP.

Eine umstrittene Frage liegt darin, ob das „Kennen“ (明知) in § 287 Abs. 2 chStGB auch das „Kennenmüssen“ (应知) umfassen kann. In der Literatur gibt es viele kontroverse Auffassungen zu der Auslegung des „Kennens“ im StGB. Eine Ansicht ist, dass das „Kennen“ im besonderen Teil des StGB auch das „Kennenmüssen“ umfasst. Das „Kennenmüssen“ bezieht sich auf die Fahrlässigkeit, vor allem auf die unbewusste Fahrlässigkeit.[150] Dem ist kritisch entgegenzuhalten, dass „Kennen“ nicht mit „Kennenmüssen“ gleichgesetzt werden kann. Das „Kennen“ bedeutet, dass der Täter tatsächliche Kenntnis haben soll, sonst wird der Vorsatz mit der Fahrlässigkeit verwechselt.[151]

Nach der herrschenden Meinung kann das „Kennenmüssen“ auch unter das „Kennen“ fallen. Diese Ansicht wird deutlich vom Obersten Gerichtshof in einigen wichtigen Interpretationen aufgenommen.[152] Aber hier handelt es sich beim „Kennenmüssen“ nicht um die Fahrlässigkeit, sondern um den Vorsatz, der aus den objektiven Tatsachen abgeleitet werden kann.[153]

---

[150] Vgl. *Dang Jianjun* (Hrsg.), Die Straftaten gegen das Urheberrecht, 1999, S. 184. Eine relevante Meinung in der gleichen Richtung ist, dass das „Kennen“ im besonderen Teil des StGB nicht unbedingt zu Vorsatz führt. Vgl. *Zou Bingjian*, Rechtszeitschrift der Universität Peking Heft 5, 2015, 1349 ff.

[151] Vgl. *Zhang Mingkai*, Strafrechtliche Wissenschaft, 2011, S. 246.

[152] Vgl. § 9 der Interpretation der gesetzlichen Anwendung über die Straftaten gegen das Urheberrecht 2004; § 1 der Interpretation der gesetzlichen Anwendung über die Geldwäsche 2009.

[153] Vgl. *Chen Xingliang*, Der Jurist Heft 3, 2013, 94 ff.

In Bezug auf die strafrechtliche Verantwortlichkeit der ISP gibt es auch ähnliche Diskussionen über die Auslegung des „Kennens“ in § 287 Abs. 2 chStGB. Das „Kennenmüssen“ solle von dem Umfang der Bedeutung des „Kennens“ ausgeschlossen werden, weil diese Möglichkeit im zivilrechtlichen Bereich schon verneint worden ist. Es ist allgemein bekannt, dass es für die strafrechtliche Verantwortlichkeit einen strengeren Bewertungsmaßstab gibt als für die zivilrechtliche Haftung. Deshalb sei die Möglichkeit für das „Kennenmüssen“ im strafrechtlichen Bereich offensichtlich zu verneinen.[154] In ähnlicher Weise heißt es, dass die Bedeutung des „Kennens“ sich nur auf die konkrete Kenntnis beschränke, damit das normale Geschäftsverhalten nicht bestraft wird.[155]

Darüber hinaus ist zu beachten, dass in den Straftatbeständen mit „Kennen“ (明知) der bedingte Vorsatz normalerweise auch für möglich gehalten wird.[156] Wenn wir diese Auslegung des § 287 Abs. 2 chStGB nach wie vor vertreten, kann ein Eventualvorsatz für die Strafbarkeit der ISP wegen der rechtswidrigen Inhalte von Dritten ausreichen.

Meines Erachtens sind beide, das „Kennenmüssen“ und der bedingte Vorsatz, zu verneinen. Nach dem Wortlaut des „Kennens“ gibt es viele Auslegungsmöglichkeiten. Aber das „Kennen“ bezieht sich hier nicht nur auf eine Interpretation nach dem bloßen Wortlaut des Tatbestands, sondern auch auf eine teleologisch beschränkende Auslegung. Auf der einen Seite sind die Inhalte und die Bedeutung des „Kennenmüssens“ unbestimmt. Dies könnte mit dem Gesetzlichkeitsprinzip nicht im Einklang stehen. Auf der anderen Seite stammt die Strafbarkeit der ISP in den meisten Konstellationen aus der Unterlassung der Kontrolle der rechtswidrigen Inhalte oder aus Delikten von Dritten. Wie schon erläutert, ist diese Kontrolle aus vielen technischen und kriminalpolitischen Gründen nicht einfach. Wenn das „Kennenmüssen“ und der bedingte Vorsatz in der Auslegung bejaht werden, könnten den ISP zu viele strafrechtliche Risiken auferlegt werden. Das bedeutet, dass die ISP aktivere Maßnahmen zur Prävention und Verhinderung der möglichen rechtswidrigen Inhalte oder Delikte ergreifen müssen.

3. Unrechtsbewusstsein und Verbotsirrtum

Nach § 17 StGB handelt ein Täter ohne Schuld, wenn er kein Unrechtsbewusstsein hat und diesen Irrtum nicht vermeiden konnte. Interessant ist, ob und inwieweit die ISP wegen des fehlenden Unrechtsbewusstseins einem Verbotsirrtum unterliegen.

---

[154] Vgl. *Ouyang Benqi/Wang Qian*, Zeitschrift des Jiangsu Verwaltungsinstituts Heft 4, 2016, 128.

[155] Vgl. *Yu Haisong*, Zeitschrift der Rechtsanwendung Heft 9, 2016, 9.

[156] Vgl. *Chen Xingliang*, Der Jurist Heft 3, 2013, 94 ff.; *Zhang Mingkai*, Strafrechtliche Wissenschaft, 2011, S. 246.

Im Vergleich zu Deutschland gibt es im chStGB keinen Paragrafen über den Verbotsirrtum. In der früheren Literatur und Rechtsprechung wurde der Verbotsirrtum im Allgemeinen verneint, weil das Prinzip *ignorantia juris non excusat* in China anerkannt wird. Außerdem, so die weit verbreitete Meinung könne dies dazu führen, dass der Angeklagte sich oft mit dieser Begründung der strafrechtlichen Verantwortlichkeit entzieht.[157]

Jedoch wird diese traditionelle Ansicht von vielen Rechtswissenschaftlern zunehmend kritisiert, weil eine vollständige Verneinung des Verbotsirrtums mit dem modernen Schuldprinzip nicht vereinbar sei.[158] Heute haben die meisten Rechtswissenschaftler den Verbotsirrtum im Strafrechtssystem angenommen. Für die systematische Einordnung des Verbotsirrtums gibt es insgesamt zwei theoretische Lösungen. Zum einen wird der Verbotsirrtum als Bestandteil in die Prüfung des Vorsatzes einbezogen, die Kenntnis der Rechtswidrigkeit wird damit als ein unentbehrlicher Teil des Vorsatzes betrachtet. Zum anderen wird der Verbotsirrtum als ein selbstständiger Schuldausschließungsgrund bestimmt. In der aktuellen Literatur ist die zweite Lösung dominant.[159]

Bei den ISP besteht auch die Möglichkeit, dass sie die Rechtswidrigkeit ihrer Handlungen nicht kennen. Die ISP wissen zum Beispiel manchmal nicht, ob die teils sehr kritischen Informationen zu einigen nationalen Politikern in dem von ihnen betriebenen Netzwerk rechtswidrig sind. Nach Konsultation eines Rechtsprofessors glauben die ISP, dass diese Informationen durch die chinesische Verfassung geschützt werden. In dieser Konstellation sollten die ISP nicht bestraft werden, weil hier die Kenntnis der Rechtswidrigkeit fehle.[160]

Diese Überlegung ist besonders im chinesischen Gesetzesrahmen zu bejahen, denn in einigen speziellen Situationen kann der Verbotsirrtum unvermeidbar sein. Auf der einen Seite steht er mit der offenen Struktur des § 286 Abs. 1 chStGB im Zusammenhang. Wie schon dargelegt, bleiben die „Sicherheitspflichten im Netzwerk“ und der Umfang der Formulierung von „Gesetzen und Anordnungen“ in § 286 Abs. 1 chStGB noch unklar; dies ist selbst für Fachkräfte schwierig zu erklären. Für die ISP ist die genaue Bedeutung der „Sicherheitspflichten im Netzwerk nach den Gesetzen und Anordnungen“ noch schwieriger zu erfassen.

Auf der anderen Seite sind die rechtswidrigen Informationen nicht einfach zu definieren. So können etwa „pornografische Inhalte“ unterschiedlich verstanden werden. In China gibt es keine gesetzliche Klassifikation dazu, die Grenze, ab der por-

---

[157] Vgl. *Yang Chunxi/Yang Dunxian* (Hrsg.), Chinesische Strafrechtswissenschaft, 1998, S. 108; *Gao Mingxuan/Ma Kechang*, Strafrechtliche Wissenschaft, 2010, S. 133. Ferner vgl. *Zhang Mingkai*, Erläuterungen über strafrechtliche Prinzipien, 1999, S. 207 ff.

[158] Vgl. *Chen Xingliang*, Die normative strafrechtliche Wissenschaft I, 2008, S. 183 ff.

[159] Vgl. *Zhang Mingkai*, Strafrechtliche Wissenschaft, 2011, S. 300; *Chen Xingliang*, ebenda, S. 185.

[160] Vgl. *Xie Wangyuan*, Chinesische Rechtswissenschaft Heft 2, 2017, S. 249 ff.

nografische Inhalte strafbar sind, ist daher unbestimmt. Ein weiteres Beispiel sind die Grenzen der Meinungsfreiheit. In Rechtspraxis und Rechtsprechung wird die Meinungsfreiheit von vielen gesetzlichen oder gesetzlich nicht geregelten Faktoren beeinflusst, sodass der Umfang der die Meinungsfreiheit überschreitenden Äußerungen ebenfalls unbestimmt bleibt. Diese Ungewissheiten könnten zu Verbotsirrtum der ISP führen. In diesen Konstellationen ist die Bestrafung der ISP, weil sie es unterlassen haben, sogenannte rechtswidrige Inhalte von Dritten zu kontrollieren, nicht berechtigt.

F. Einordnung als Täterschaft oder Teilnahme

1. Abgrenzung von Täterschaft und Teilnahme

Im chStGB gibt es nur Paragrafen über die Beteiligung an einer Tat, aber keine selbstständige Regelung über die Täterschaft. Trotzdem wird das theoretische System von Täter und Teilnehmer in der Wissenschaft weithin akzeptiert.

Aus der Sicht der Rechtsvergleichung wird eine Reihe von Lehren über die Abgrenzung von Täterschaft und Teilnahme ausführlich diskutiert. Die subjektive Theorie, die formal-objektive Theorie, die materiell-objektive Theorie sowie die Tatherrschaftslehre werden von Rechtswissenschaftlern in Monografien oder Strafrechtslehrbüchern eingeführt.

Ähnlich wie in Deutschland haben auch chinesische Rechtswissenschaftler die subjektive Theorie zunächst abgelehnt, weil der den Tatbestand unmittelbar verwirklichende Straftäter wegen der fehlenden subjektiven Interessen nicht als Täter betrachtet werden kann. Zudem ist das sogenannte subjektive Kriterium oft unbestimmt. Die formal-objektive Theorie stieß ebenfalls auf Kritik; ihr größtes Problem ist die schwere Begründbarkeit der mittelbaren Täterschaft. Nach dem Rechtsvergleich wird die Tatherrschaftslehre im heutigen China immer populärer. Diese Lehre ist als ein Kompromiss zwischen subjektiven und objektiven, formalen und materialen Abgrenzungstheorien zu verstehen.[161] Die Tatherrschaftslehre kann somit die Nachteile von subjektiven und formal-objektiven Lehren umgehen.

2. Diskussion über die neutrale Handlung

Die strafrechtliche Verantwortlichkeit der ISP ist ein relativ neues Thema in China. In der chinesischen Diskussion darüber spielt die Theorie der neutralen Handlung eine erhebliche Rolle. Viele chinesische Strafrechtswissenschaftler glauben, dass die Tätigkeiten der Internetdienste der ISP neutrale Handlungen seien und

---

[161] Vgl. *Zhou Guangquan*, Strafrecht Allgemeiner Teil, 2011, S. 210 ff.; *Zhang Mingkai*, Strafrechtliche Wissenschaft, 2016, S. 390 ff.

die Handlungen der ISP deswegen grundsätzlich straflos bleiben sollten, auch wenn die Provider rechtswidrige Informationen und Handlungen von Dritten kennen. Diese Auffassung, die auf der Theorie der neutralen Handlung beruht, erscheint allerdings unzutreffend. Es ist deswegen notwendig, die im chinesischen Recht diskutierte Theorie der neutralen Handlung hier ausführlich zu erläutern, damit die Anwendbarkeit dieser Theorie zur Bestimmung der strafrechtlichen Verantwortlichkeit der ISP genau geprüft werden kann. Wenn dabei auch intensiv deutsche Strafrechtsliteratur zitiert wird, so beruht dies darauf, dass diese in der entsprechenden chinesischen Diskussion eine wesentliche Rolle spielt.

a) Neutrale Handlung

Die neutrale Handlung geht auf die deutschen strafrechtlichen Theorien zurück. Unter diesem Begriff wird eine Handlung, „welche die traditionellen Voraussetzungen des Unrechts der Beihilfe erfüllt, am Ende aber kein objektives Beihilfeunrecht ist“, verstanden. Nach dieser Definition besitzt die neutrale Handlung einen alltäglichen, normalen und sozialen Charakter.[162]

Die Definition ist allerdings so weit gefasst, dass sie viele sogenannte neutrale Handlungen umschließt, wie nachfolgende Beispiele zeigen: Ein Taxifahrer bringt einen Fahrgast zum Zielort, obwohl er zufällig weiß, dass der Fahrgast dort einen Einbruch begehen möchte. Zu den berufstypischen Handlungen gehört auch das Beispiel der Arbeitnehmer, die eng mit dem Eigentümer eines Unternehmens zusammenarbeiten, obwohl die Arbeitnehmer wissen, dass der Eigentümer Steuern hinterzieht.[163] Ein als Verkaufsleiter in einem Industrieunternehmen angestellter Mitarbeiter weiß, dass die Unternehmensleitung gegen Umweltschutzvorschriften verstößt.[164] Als Beispiel einer alltäglichen Handlung wäre der Naturfreund zu nennen, der weiß, dass seine selbst gezüchtete Blumen von einem Heiratsschwindler als Präsent zur Betrügerei verwenden werden.[165]

Nach einer allgemeinen Definition werden die oben genannten Beispiele als neutrale Handlung betrachtet, sodass alle Teilnehmer in diesen Konstellationen nicht strafbar sind. Jedoch ist noch unklar, wie der sogenannte alltägliche, normale und soziale Charakter der neutralen Handlung zu prüfen und zu bestimmen ist. Wegen der Unsicherheit der Definition ist diese Theorie in der Literatur höchst umstritten. Insgesamt gibt es drei Lösungsansätze zur Unterscheidung zwischen

---

162 Vgl. *Hassemer*, wistra Heft 2, 1995, S. 42.

163 Vgl. *Wohlleben*, Beihilfe durch äußerlich neutrale Handlungen, S. 3.

164 Vgl. *Meyer-Arndt*, wistra Heft 8, 1989, 281.

165 Vgl. *Jakobs*, AT^2, S. 24, Rn. 13. Mehr Beispiele vgl. BGHSt, 46, 2001, S. 107 ff.; *Roxin*, AT II, § 26, Rn. 218, 247 ff.; *Wessels/Beulke*, AT^{38}, Rn. 582a; *Schild Trappe*, Harmlose Gehilfenschaft?, S. 4 ff.; *Rackow*, Neutrale Handlungen als Problem des Strafrechts, 2007, S. 281 ff.

den neutralen Handlungen und den strafbaren Beihilfen, nämlich die subjektive Theorie, die objektive Theorie und die kombinierte Theorie.[166]

aa) Subjektive Theorie

Die subjektive Theorie beruht auf dem subjektiven Kriterium, die neutrale Handlung von der strafbaren Beihilfe abzugrenzen. Der Gehilfe muss den Vorsatz haben, sich mit einem Täter im Hinblick auf eben diese Straftat erfolgreich zu solidarisieren, während der Täter dies auch erkennt und akzeptiert.[167]

Die subjektive Theorie ist starker Kritik ausgesetzt, vor allem steht diese Meinung im Widerspruch zum Tatstrafrecht, weil die Unterscheidung zwischen den neutralen Handlungen und den strafbaren Beihilfen hauptsächlich von den subjektiven Zuständen der Straftäter abhängig ist. Das Tatstrafrecht fordert, dass der Ansatz und der Schwerpunkt der Zurechnung grundsätzlich im objektiven Aspekt liegen, denn sonst besteht die Gefahr eines Gesinnungsstrafrechts.[168] Darüber hinaus ist die Bedeutung der „Solidarisierung" unklar. Bei den neutralen Handlungen haben die Gehilfen oft Kenntnisse über die Straftaten der Täter. Dem subjektiven Kriterium zufolge dürfte der Kreis der strafbaren Gehilfen sehr groß sein. Zudem ist dieser Gehilfenvorsatz in der Praxis äußerst schwierig nachzuweisen, sodass die Entscheidung der Richter mit vielen Unsicherheiten behaftet ist.[169]

bb) Objektive Theorie

Im Vergleich zur subjektiven Lehre bezieht sich die objektive Theorie auf die objektiven Eigenschaften der Handlungen von Gehilfen. Unter den Anhängern der objektiven Lehre gibt es viele Rechtswissenschaftler, die eigene Lösungswege zur Unterscheidung zwischen neutraler Handlung und strafbarer Beihilfe einschlagen.

Lehre von der professionellen Adäquanz

Diese Lehre wurde von *Hassemer* vertreten. Zunächst kritisierte *Hassemer* die früher vertretene subjektive Konzeption. Er schlug vor, dass die neutrale Handlung vor allem in dem objektiven Aspekt von der strafbaren Beihilfe unterschieden werden soll. Nach seiner Meinung sei die Verneinung der Strafbarkeit der neutralen Handlung auf die professionelle Adäquanz (sowie die soziale Adäquanz) zurückzuführen. Die Konzeption zur Neutralität von Verhalten liege an der Grenze zwischen sozialen und strafrechtlichen Normen. Die strafrechtliche Norm sei unrechtskonstitu-

---

[166] Vgl. Schönke/Schröder-*Heine/Weiße*, § 27, Rn. 12; *Chen Hongbing*, Die neutralen Handlungen, S. 73 ff.

[167] Vgl. *Schild Trappe*, Harmlose Gehilfenschaft?, S. 161 ff.

[168] Vgl. *Hassemer*, wistra Heft 2, 1995, S. 43; *Weigend*, in: Eser (Hrsg.), Festschrift für Haruo Nishihara, S. 199 ff.

[169] Vgl. *Hassemer*, ebenda, 43.

ierend, während die außerstrafrechtliche Norm unrechtsausschließend sei. Deshalb sei das Verhältnis zwischen diesen unterschiedlichen Normen zu harmonisieren.[170] Jedoch stellen einige Rechtswissenschaftler diese Auffassung infrage: Ähnlich wie bei der sozialen Adäquanz bleibe der Inhalt der sogenannten professionellen Adäquanz unklar. Hier gebe es noch kein einheitliches Kriterium für die Bestimmung der neutralen Handlungen.[171]

Lehre von der Solidarisierung mit fremdem Unrecht

Diese Lehre wurde von *Schumann* aufgestellt, der Strafgrund der Teilnahme liegt in der Solidarisierung mit fremdem Unrecht. Die Verneinung der Strafbarkeit der neutralen Handlung kann damit ebenfalls begründet werden, denn das Unrecht der Beihilfe besteht nicht allein in dem vorsätzlichen Beitrag der Gehilfen, sondern auch in der gemeinsamen Solidarisierung mit der Tat anderer.[172] *Schumanns* These wird wegen ihrer allgemeinen Bewertung von Unrecht kritisiert: Der Akzent des Unrechts werde vom Erfolgsunrecht zu weit zum Handlungsunrecht hin verschoben. Nur die sogenannte Solidarisierung reiche für die Strafbarkeit der Teilnahme nicht aus, da man nicht auf das Erfordernis der Kausalität zwischen der Teilnahmehandlung und dem Taterfolg verzichten sollte.[173] Das heißt, diese Lehre wird stark vom Standpunkt des Handlungsunwerts geprägt. Es wird in der Literatur sogar eingewendet, dass dies zu einem Fehler von Schumanns grundlegender Auffassung von Unrecht gehöre.[174] Aus diesem Grund könnte der Umfang der strafbaren Beihilfe noch zu weit gefasst sein.

Lehre des Regressverbots

Diese Lehre wurde von *Jakobs* vertreten. Nach Jakobs könnte eine „Distanzierung" eines Beteiligten im Bereich des Regressverbots bestehen, wenn dessen Verhalten nicht davon abhängt, dass die Handlung des Täters überhaupt nachfolgt. Das heißt, das Verhalten hat ohne die Handlung des Täters auch einen selbstständigen Sinn. Hier hat der Beteiligte eine Situation geschaffen, in der andere Personen den Tatbestand weitgehend verwirklichen könnten. Diese Situation kann von der Tatbestandsverwirklichung nicht rückwirkend beeinflusst werden.[175] Obwohl der Beteiligte zusammen mit dem Täter handelt, kann die Verantwortlichkeit des Beteiligten noch verneint werden, solange sich der soziale Kontakt auf die Leistung des

---

[170] Vgl. *Hassemer*, ebenda, 42 ff.

[171] Vgl. *Pilz*, Beihilfe zur Steuerhinterziehung durch neutrale Handlungen von Bankmitarbeitern, S. 79; *Otto*, „Vorgeleistete Strafvereitelung" durch berufstypische oder alltägliche Verhaltensweisen als Beihilfe, in: Eser/Schittenhelm/Schumann (Hrsg.), Festschrift für Theodor Lenckner, S. 203; *Roxin*, AT II, § 26, Rn. 233.

[172] Vgl. *Schumann*, Strafrechtliches Handlungsunrecht und das Prinzip der Selbstverantwortung der Anderen, S. 50, 57 ff.

[173] Vgl. *Niedermair*, ZStW 107, Heft 3, 1995, 513.

[174] Vgl. *Chen Hongbing*, Die neutralen Handlungen, 2010, S. 95.

[175] Vgl. *Jakobs*, AT^2, 24/15.

Gegenstands und die Realisierung des Ziels der Sache beschränkt. Denn nur bei Isolierung der Zweckverfolgung und jeweiligem Handlungssinn kann der „reibungslose Informations- und Warenaustausch" verwirklicht werden.[176] Mehrere Wissenschaftler übten Kritik an dieser Interpretation. Wenn der Gehilfe schon erkannt hat, dass bald eine Straftat (Risikoerhöhung) geschehen wird, aber dennoch dem Täter Hilfe leistet, könnten die objektive Förderung und der Förderungsvorsatz des Gehilfen nicht verneint werden. Deshalb könne die Abgrenzung der neutralen Handlung mit dieser These nicht ausreichend begründet werden.[177]

Lehre von Puppe

Darüber hinaus hängt das Umreißen der neutralen Handlung nach der Meinung von *Puppe* davon ab, in welcher Phase die Handlung des Täters liegt.[178] Wenn die Ausführungshandlung des Täters nicht unmittelbar bevorsteht, kann die Beihilfe nicht bestraft werden, solange der Täter die nötige Hilfe anderweitig bekommen kann. Wenn die Ausführungshandlung des Täters jedoch kurz vor der Umsetzung ist, ist diese Beihilfe nicht erlaubt, weil der Gehilfe die hohe Wahrscheinlichkeit, dass eine Straftat begangen wird, in diesem Moment erkennen kann.[179] Aber diese Überlegung trifft nach der kritischen Meinung von *Roxin* auch nicht zu: So könne der Täter immer selbst entscheiden, ob er seine Straftat beende. Außerdem werde nicht ausreichend begründet, warum die Beihilfe im Vorbereitungsstadium straflos sein soll.[180]

Lehre von der objektiven Zurechnung

Neben den oben genannten Lösungen gibt es noch viele andere Ansichten in Bezug auf die objektive Zurechnung. Nach *Löwe-Krahl* liegt der Grund für die Straflosigkeit der neutralen Handlung nicht in der Neutralität der Bestätigung der Normen, sondern in den hypothetischen Kausalverläufen im Rahmen der objektiven Zurechnung. Bei der neutralen Handlung hat der Gehilfe keine rechtlich missbilligte Gefahr geschaffen.[181] *Frisch* führt das Problem auf die Risikoerhöhung zurück. Wenn der Gehilfe keine spezifischen Bedingungen zur Begehung der Straftat geschaffen oder die Möglichkeit, die Straftat zu begehen, nicht verbessert habe, bestehe keine missbilligte Risikoerhöhung.[182] Allerdings scheint dieses Argument auch nicht haltbar zu sein. Denn Beiträge zum Verbrechen könnten von vielen an-

---

[176] Vgl. ebenda, 24/17.

[177] Vgl. *Niedermair*, ZStW 107, Heft 3, 1995, 511 ff.; *Roxin*, AT II, § 26, Rn. 228; *Pilz*, Beihilfe zur Steuerhinterziehung durch neutrale Handlungen von Bankmitarbeitern, 2001, S. 116 ff.

[178] Vgl. *Rackow*, Neutrale Handlungen als Problem des Strafrechts, 2007, S. 158 ff.

[179] Vgl. Kindhäuser/Neumann/Paeffgen-*Puppe*, Vorbemerkungen zu § 13, Rn. 173 ff.

[180] Vgl. *Roxin*, AT II, § 26, Rn. 238.

[181] Vgl. *Löwe-Krahl*, wistra Heft 6, 1995, 205.

[182] Vgl. *Frisch*, Tatbestandsmäßiges Verhalten und Zurechnung des Erfolgs, S. 294.

deren Tätern oder Helfern geleistet werden, sodass dies zu einer Aushöhlung der Strafbarkeit führe.[183] Es wird auch kritisch angeführt, dass diese Einbeziehung der hypothetischen Kausalverläufe in letzter Konsequenz auf reinen Utilitarismus bezüglich der Bedürfnisdeckung der Täter und Gehilfen hinauszulaufen drohe, ohne die verletzten Rechtsgüter zu berücksichtigen.[184]

cc) Kombinierte Theorie

Die kombinierte Theorie wird repräsentativ von *Roxin* vertreten. Auf der objektiven Seite wird die Beihilfe als eine für den tatbestandsmäßigen Erfolg kausale und missbilligte Risikosteigerung verstanden.[185] Auf der subjektiven Seite bezieht sich diese Auffassung auf den Vertrauensgrundsatz, um den Umfang der strafbaren Beihilfe zu beschränken. Nach dem Vertrauensgrundsatz kann darauf vertraut werden, dass andere keine vorsätzlichen Straftaten begehen. Die Zurechnung zum objektiven Tatbestand ist wegen des durch den Vertrauensgrundsatz begründeten erlaubten Risikos ausgeschlossen. Deshalb soll ein Gehilfe mit nur *dolus eventualis* nicht bestraft werden.[186] Jedoch wird diese Auffassung in der Literatur kritisch bewertet. Die kombinierte Theorie beruht im Grundsatz auf der Unterscheidung von *dolus directus* und *dolus eventualis*, um die neutrale Handlung abzugrenzen. Dies könnte nach den Kritikern der kombinierten Theorie zu einem Gesinnungsstrafrecht führen.[187] Ferner löst der Vertrauensgrundsatz eine Diskussion darüber aus, inwieweit auf die Lauterkeit von anderen Personen vertraut werden darf. Das Kriterium der erkennbaren Tatgeneigtheit kann allerdings schwer aus einem allgemeinen Vertrauensgrundsatz abgeleitet werden.[188]

Die oben genannte Kritik an der kombinierten Theorie ist jedoch nicht zutreffend. Die kombinierte Theorie hat meines Erachtens insbesondere nichts mit dem Gesinnungsstrafrecht zu tun, sie hat zuerst einmal eine objektive Basis. Die objektiven Voraussetzungen garantieren bereits, dass dieser Denkansatz nicht zum sogenannten Gesinnungsstrafrecht führt. Das subjektive Kriterium dient in diesem Zusammenhang hauptsächlich dazu, die strafrechtliche Verantwortung einzuschränken. Auch können die subjektiven Elemente in dieser Theorie nicht direkt mit dem Gesinnungsstrafrecht gleichgestellt werden. Der Charakter einer Handlung wird auch sonst häufig durch ihren Zweck bestimmt, weil ohne diesen Zweck die meisten Beihilfehandlungen neutral sind. So kann etwa das Tragen einer Leiter auch als ein alltagsüb-

---

[183] Vgl. *Pilz*, Beihilfe zur Steuerhinterziehung durch neutrale Handlungen von Bankmitarbeitern, S. 146 ff.

[184] Vgl. *Rackow*, Neutrale Handlungen als Problem des Strafrechts, S. 200.

[185] Vgl. *Roxin*, AT II, § 26, Rn. 183 ff.

[186] Vgl. ebenda, § 26, Rn. 241 ff.

[187] Vgl. *Tag*, JR Heft 2, 1997, 51.

[188] Vgl. *Rackow*, Neutrale Handlungen als Problem des Strafrechts, S. 200.

licher Vorgang betrachtet werden, wenn das subjektive Element der Beihilfe – die Leiter wird für einen (Einbruch-)Diebstahl verwendet – nicht berücksichtigt wird.[189]

Außerdem kann die Einschränkung der strafrechtlichen Verantwortlichkeit durch den Vertrauensgrundsatz zutreffend begründet werden. Im beruflichen Umfeld kann der ISP grundsätzlich darauf vertrauen, dass seine Kunden oder Mitarbeiter normalerweise in einem gesetzlich zulässigen Rahmen mit ihm zusammenarbeiten würden, sonst wäre der Aufwand der sozialen Zusammenarbeit zu hoch. Deswegen braucht der ISP im Normalfall nicht zu überprüfen, ob seine beruflichen Services die Begehung der Straftat von anderen unterstützt haben, es sei denn, man hat bestimmte Kenntnis von den strafbaren Handlungen Dritter erhalten.

Die deutsche Rechtsprechung stimmt dieser Wirkung des subjektiven Tatbestands zur Abgrenzung der neutralen Handlung deswegen auch zu Recht zu. Nach einer Reihe von Entscheidungen des deutschen BGH wird die Strafbarkeit des Gehilfen ausgeschlossen, wenn der Hilfeleistende nicht weiß oder es nur für möglich hält (*dolus eventualis*), dass seine neutrale und insbesondere berufstypische Handlung (zum Beispiel im Beruf als Bankkaufmann, Notar, Anwalt) zur Begehung einer Straftat genutzt wird.[190] Im Gegensatz zu den abstrakten Kriterien der geschilderten objektiven Theorien (professionelle Adäquanz, Solidarisierung mit fremdem Unrecht) ist diese Auffassung des BGH in der Praxis auch besser durchsetzbar.

Im Übrigen steht diese Interpretation auch mit dem aus § 10 TMG abgeleiteten Ergebnis in Einklang. Wie schon erläutert, kann nach § 10 TMG ein bedingter Vorsatz für die Verantwortlichkeit der Hosting Provider nicht ausreichend sein, sonst würden die Hosting Provider unverhältnismäßig hohe Belastungen für ihren Betrieb in Kauf nehmen. Deshalb ist die oben genannte kombinierte Theorie eine relativ überzeugende Lösung.

b) Berücksichtigung der Lehre von der neutralen Handlung für die Verantwortlichkeit der ISP

Bezüglich der strafrechtlichen Verantwortlichkeit der ISP wird die Theorie der neutralen Handlung von vielen chinesischen Wissenschaftlern aufgenommen und angewendet.[191] Beispielsweise wird angeführt, dass die strafrechtliche Verantwortlichkeit der Firma *Kuaibo* sich auf die neutrale Handlung bezieht.[192] Der neu erlassene § 287 II[193] des chStGB wird kritisiert, weil es sich bei der in diesem Paragrafen beschriebenen Straftat um die neutrale Handlung handele und die Bestrafung

---

189 Vgl. *Roxin*, AT II, § 26, Rn. 231.

190 Vgl. BGHSt 46, 107, 112; BGH, Urteil vom 26.10.1998 – 5 StR 746–97, NStZ-RR 1999, 184; BGH, Beschluß vom 20.09.1999 – 5 StR 729/98, NStZ 2000, 34.

191 Vgl. *Chen Hongbing*, Rechtszeitschrift der Universität Peking Heft 6, 2008, 931.

192 Vgl. *Che Hao*, Chinesische Rechtszeitschrift Heft 1, 2015, 49.

193 Der Titel dieses Paragrafen lautet „Hilfe für Informationen und Cyberkriminalität“.

dieser Handlung mit der Entwicklung der Gesellschaft nicht einhergehe.[194] Demnach seien die ISP nicht strafbar, obwohl sie die Voraussetzungen der strafbaren Beihilfen erfüllt haben, weil die Internetdienste der ISP neutral, sozial nützlich und alltäglich sind.[195]

Dieser Ansatz ist zumindest teilweise zu bejahen, da er den großen Umfang der strafrechtlichen Verantwortlichkeit der ISP in China einschränken kann. Wie schon oben erwähnt, gibt es viele Gesetze, Anordnungen und Vorschriften in China, die sich auf die Verantwortlichkeit der ISP beziehen und ihnen allgemeine Verpflichtungen zusprechen. Deshalb können in den Gesetzen die entsprechenden Verpflichtungen für die ISP, aus denen sich die strafrechtliche Verantwortlichkeit der ISP herleitet, leicht eruiert werden. Aufgrund dieser umfassenden und aktiven Verpflichtungen für ISP und des die Schuld erweiternden Paragrafen im chStGB kann ein Richter mühelos zu dem Schluss kommen, dass die ISP für fremde Inhalte die strafrechtliche Verantwortlichkeit übernehmen sollen.

Das Ziel der neutralen Handlungstheorie liegt in der Einschränkung der umfassenden strafrechtlichen Verantwortlichkeit der strafbaren Beihilfe. Mit anderen Worten: Sie dient dazu, die alltäglichen und sozial adäquaten Tätigkeiten von den strafbaren Handlungen zu unterscheiden. Mit diesem Verständnis wird sichtbar, dass das Konzept der neutralen Handlung in gewissem Maße mit dem Erfordernis der Einschränkung der strafrechtlichen Verantwortung übereinstimmt. In diesem Sinn kann konstatiert werden, dass die Theorie der neutralen Handlung nützlich ist, um die strafrechtliche Verantwortlichkeit der ISP zu bestimmen.

c) Begrenztheit der neutralen Handlung für die Verantwortlichkeit der ISP

Obwohl die neutrale Handlung der Einschränkung der strafrechtlichen Verantwortlichkeit der ISP zugutekommt, ist ihre begrenzte Wirkung nicht zu ignorieren.

aa) Fehlende Typisierung der ISP

Vor allem ist zu beachten, dass die Typisierung der ISP der Anwendung der neutralen Handlungstheorie zugrunde liegt. Da die vielfältigen ISP unterschiedliche Funktionen haben und je nach Situation verschiedene Rollen spielen, ist ihre Typisierung entscheidend. Manche Rechtswissenschaftler legen keinen großen Wert auf diese Problematik. So wird zum Beispiel behauptet, dass die Handlungen der ISP, die den Nutzern trotz Kenntnis von rechtswidrigen Inhalten oder illegaler Nutzung der Internetdienste Access Services oder Peer-to-Peer-System-Services anbieten, in

---

[194] Vgl. *Che Hao*, Rechtswissenschaft Heft 10, 2015, 13; *Zhou Guangquan*, Chinesische Rechtszeitschrift Heft 2, 2015, 175 ff.

[195] Vgl. *Chen Hongbing*, Zeitschrift der Nordöstlichen Universität (Sozialwissenschaftliche Ausgabe) Heft 3, 2009, 262 ff.

der deutschen oder japanischen Literatur zu den typisch neutralen Handlungen gehören.[196] Sowohl der Access Service und das Anbieten der Netzwerkplattform als auch der Peer-to-Peer-Service werden der neutralen Handlung zugerechnet. Diese Handlungen sollen nicht als Beihilfen bestraft werden.[197]

Diese Argumentation ist nicht stichhaltig. Auf der einen Seite gibt es in Deutschland nur wenige Untersuchungen,[198] die sich speziell auf die neutrale Handlung berufen, um die strafrechtliche Verantwortlichkeit der ISP zu erörtern. Außerdem gehören die Tätigkeiten der ISP in der Literatur nicht zu den typischen Beispielen der neutralen Beihilfe. In der Rechtsprechung wird diese Theorie sehr selten angewendet; zum Beispiel hat sich der Richter im *Compuserve*-Fall nicht direkt auf die neutrale Handlungstheorie berufen.

Auf der anderen Seite sollte die rechtliche Behandlung der verschiedenen ISP differenziert werden. Zur Bestimmung der Verantwortlichkeit der Access Provider könnte es sinnvoll sein, auf das Modell der neutralen Handlung zurückzugreifen, weil Access Provider wegen ihrer technischen Begrenztheit nur geringe Kontrollmöglichkeiten über Inhalte haben und sie grundsätzlich auch dann noch privilegiert werden, wenn sie zuvor schon Kenntnis von rechtswidrigen Inhalten besessen haben. In dieser speziellen Konstellation könnte die neutrale Handlungstheorie analog Anwendung finden. Aber um die Verantwortlichkeit der Caching Provider oder Hosting Provider zu bestimmen, ist die Anwendung dieser Theorie offensichtlich problematisch, da nach den allgemein anerkannten Grundsätzen Caching Provider und Hosting Provider rechtswidrige Informationen unverzüglich entfernen oder den Zugang zu ihnen sperren sollen, nachdem sie Kenntnis von den illegalen Informationen haben. Das heißt also, in dieser Situation spielen die ISP keine neutrale Rolle, damit gibt es hier auch keine Basis für die Anwendung der neutralen Handlungstheorie.

Zusammenfassend lässt sich feststellen, dass die vorgelagerte Typisierung der ISP eine Voraussetzung für die mögliche Anwendung der neutralen Handlungstheorie ist. Die allgemeine Diskussion der neutralen Handlung ist zu verneinen.

bb) Abgrenzung der Beteiligung der ISP

Das Internet und die Netzwerktechnologie haben das Leben erheblich verändert und damit auch die traditionellen strafrechtlichen Theorien stark beeinflusst. Be-

---

196 Vgl. *Chen Hongbing*, Rechtszeitschrift der Universität Peking Heft 6, 2008, 931.

197 Vgl. *Chen Hongbing*, Zeitschrift der Nordöstlichen Universität (Sozialwissenschaftliche Ausgabe) Heft 3, 2009, 262 ff.

198 Zu Untersuchungen aus der Sicht der neutralen Handlung siehe *Bode*, ZStW 127, Heft 4, 2015. Ferner vgl. *Heliosch*, Verfassungsrechtliche Anforderungen an Sperrmaßnahmen von kinderpornografischen Inhalten im Internet, S. 123; *Eichhorn*, Internetrecht, S. 82; *Kudlich*, Die Unterstützung fremder Straftaten durch berufsbedingtes Verhalten, 2004, S. 502.

sonders in dem Bereich der Beteiligung hat dieses Phänomen bereits Spuren hinterlassen.

Erstens ist es im Cyberspace schwieriger, eine Grenze zwischen Täterschaft und Teilnahme zu ziehen. Der innere Mechanismus der Verbreitung pornografischer Videodateien im Peer-to-Peer-Netzwerk verhält sich anders als im realen Raum. Im Peer-to-Peer-Netzwerk gibt es normalerweise keinen zentralen Server, der die vermittelten Inhalte speichert. Stattdessen kann jeder Nutzer als ein kleiner Server betrachtet werden. Das heißt, alle Dateien werden direkt zwischen den Nutzern ausgetauscht, ohne dass die vermittelten Dateien von einem zentralen Server einheitlich kontrolliert und verwaltet werden. Der Betreiber des Peer-to-Peer-Netzwerks bietet nur eine Plattform an, auf der die Informationen tatsächlich von zahlreichen Nutzern verwendet werden. Im Peer-to-Peer-Netzwerk arbeiten alle Nutzer indirekt zusammen. Wenn nur wenige Nutzer den *sharing mode* öffnen, kann das Peer-to-Peer-Netzwerk nicht dynamisch funktionieren. Deshalb ist die Verbreitung pornografischer Videodateien von der Zusammenarbeit der zahlreichen Nutzer abhängig. In dieser Konstellation ist es höchst problematisch, festzulegen, wer als Täter und wer als Teilnehmer betrachtet werden soll.

Außerdem sind im chStGB die quantitativen Elemente für Kriminalität[199] weit verbreitet. So kann etwa ein Diebstahl nur von der Staatsanwaltschaft angeklagt werden, wenn der Wert des gestohlenen Gegenstands 1.000 bis 3.000 Yuan erreicht.[200] Bei Verbreitung pornografischer Videodateien kann ein Verdächtiger von der Staatsanwaltschaft angeklagt werden, wenn die Menge der verbreiteten pornografischen Videodateien mindestens 40 Stück beträgt.[201] Nicht nur der Staatsanwalt, sondern auch der Richter muss mit diesem quantitativen Standard umgehen. Die Bestrafung der rechtswidrigen Handlung unterliegt aufgrund des quantitativen Standards großen Schwierigkeiten: Auf der einen Seite ist die Menge der verbreiteten pornografischen Videodateien schwierig zu ermitteln, weil die Form der Verbreitung von Informationen im Internet sehr vielfältig ist. Auf der anderen Seite erreicht die Menge der pornografischen Videodateien von einzelnen Nutzern oft nicht den quantitativen Standard.

Daher ist es denkbar, dass niemand nach dem chStGB bestraft werden kann, obwohl strafbare pornografische Videodateien im Netzwerk weit verbreitet werden. Da die Bestrafung der Teilnehmer auf der Strafbarkeit des Täters beruht und letztere nicht bestimmt wird, können die ISP, die als Teilnehmer zur Verbreitung porno-

---

[199] Für eine detaillierte Beschreibung der quantitativen Elemente im chinesischen StGB siehe *Wang Yu*, Qualitative und quantitative Instrumente zur Einschränkung der Strafverfolgung bei fehlendem Strafbedürfnis, 2014.

[200] Vgl. § 1 der Interpretation über die gesetzliche Anwendung des Diebstahls 2013 des Obersten Volksgerichtshofs und der Obersten Staatsanwaltschaft.

[201] Vgl. §§ 1–3 der ersten Interpretation über die Pornografie im Netzwerk (2004).

grafischer Videodateien betrachtet werden, nach der Akzessorietät der Teilnahme nicht bestraft werden.

Darüber hinaus besteht ein Unterschied zwischen den Handlungen der ISP und den neutralen Handlungen im subjektiven Sinne. In den Konstellationen mit neutralen Handlungen haben die Beihelfer normalerweise Kenntnis von rechtswidrigen Inhalten. Weiterhin haben sie in dieser Situation oft schon alle formalen Voraussetzungen für die Beihilfe erfüllt. Dagegen haben die ISP keine konkrete Kenntnis von den rechtswidrigen Informationen, weil die Menge der übermittelten Informationen im Netzwerk zu groß ist. Zum einen sind die ISP nicht in der Lage, den konkreten Umstand aller Informationen zu erfahren. Zum anderen sind die ISP nach den allgemein anerkannten Grundsätzen nicht verpflichtet, die rechtswidrigen Informationen im Netzwerk aktiv zu überwachen und zu überprüfen. Außerdem muss der Vorsatz der Teilnahme die Unterstützung und Hilfeleistung erfassen. Das heißt, der Teilnehmer muss Kenntnis von der konkreten Haupttat haben.[202] Jedoch können die ISP in den meisten Fällen diese Voraussetzung gar nicht erfüllen. Da sie in der Regel ihre Internetdienste vielen anonymen Nutzern gleichzeitig anbieten, können sie selten die genauen Tätigkeiten ihrer Nutzer nachvollziehen.

Zusammenfassend ist festzuhalten, dass die Handlungen der ISP die grundlegenden Voraussetzungen für Gehilfen (Teilnehmer) oft nicht erfüllen können. Deshalb lässt sich die Theorie der neutralen Handlung nur schwer anwenden.

cc) Spezielle Eigenschaften der ISP

Neben den Unterschieden im Bereich der Beteiligung führen die speziellen Eigenschaften der ISP auch zur Begrenztheit der neutralen Handlung für deren Verantwortlichkeit der ISP. Ähnliche wie ein Taxifahrer, ein Angestellter oder ein Arbeitnehmer besitzen auch die ISP berufsbedingt einen alltäglichen, normalen und sozialen Charakter, aufgrund dessen die Handlungen der ISP von der Gesellschaft allgemein akzeptiert werden. Andererseits sind die ISP nicht gänzlich verpflichtungsfrei, und ihre Handlung ist nicht komplett neutral.

Bestimmte ISP besitzen in besonderen Konstellationen einige Pflichten. Obwohl die ISP nach allgemein anerkanntem Grundsatz keine allgemeine und aktive Verpflichtung zur Überwachung rechtswidriger Informationen haben, müssen sie wirksame Maßnahmen ergreifen, die nach dem Industriestandard zumutbar sind und keine unverhältnismäßig schweren Belastungen bedeuten. Beispielsweise ist es in einigen Bereichen inzwischen üblich, dass eine Filtersoftware, die zur Löschung der illegalen Informationen dient, installiert wird.

Hingegen sind manche ISP – etwa Hosting Provider – nach der Kenntniserlangung der konkreten rechtswidrigen Informationen verpflichtet, die illegalen Inhalte

---

[202] Vgl. *Wessels/Beulke*, AT[38], Rn. 584.

zu löschen und zu sperren. Diese Regelung ist nicht nur im TMG, ECRL und DMCA, sondern auch im chinesischen Gesetz deutlich vorgesehen. Das bedeutet, dass diese ISP nach der Kenntniserlangung der rechtswidrigen Inhalte die neutrale Eigenschaft verlieren. Ab diesem Zeitpunkt gilt die neutrale Handlungstheorie nicht mehr. Es gibt viele Gründe, die dieses Ergebnis stützen: Erstens haben die ISP in gewissem Maße eine Kontrollmöglichkeit über die Informationen. Normalerweise beherrschen die ISP mit einem professionellen Team die fortschrittliche Netzwerktechnologie. Besonders die Hosting Provider sind nach der konkreten Kenntnis durchaus in der Lage, die strafrechtlich relevanten Inhalte zu kontrollieren.

Zweitens ist aus Sicht der Kriminalpolitik zu verneinen, dass die ISP in Bezug auf die Sicherheit des Cyberspace ganz neutral sind. Im Cyberspace spielen Funktion und Position der ISP eine immer wichtigere Rolle. Ohne die Zusammenarbeit der ISP mit den Strafverfolgungsbehörden bei der Bekämpfung der Cyberkriminalität könnten strafbare Handlungen im Netzwerk nicht verhindert oder ihnen vorgebeugt werden. Die Kooperation der ISP mit den Strafverfolgungsbehörden ist die Voraussetzung für eine wirksame Bekämpfung der Internetkriminalität.[203]

Drittens stellt die rasche Entwicklung der Netzwerktechnologie mehr Anforderungen an die Netzwerksicherheit. Zum Beispiel sind in den letzten Jahren mit der ständigen Entwicklung der Cloud-Computing-Technologie auch immer mehr Cloud-Service-Provider entstanden. Dabei wächst der Anspruch an die Netzwerksicherheit, weil das Cloud-System besonders anfällig für Störungen und Eingriffe ist.[204] In dem Entwicklungsprozess der Cloud-Computing-Technologie spielt die Sicherheit eine Schlüsselrolle, weil der normale Betrieb des Cloud-Service-Systems von den Sicherheitsmaßnahmen des Cloud-Service-Providers abhängig ist.[205] Deshalb ist es für diese Provider unentbehrlich, wirksame Maßnahmen zu ergreifen, damit Vertraulichkeit, Integrität und Verfügbarkeit der Speicherungsdienste garantiert werden können.[206] Es wird erkennbar, dass der neue technische Wandel die Position der ISP in der Gesellschaft stark beeinflusst hat. In einigen Bereichen wird die beschützende Intervention der ISP unvermeidlich.

Obwohl eine allgemeine Verpflichtung der ISP zur Überwachung der rechtswidrigen Inhalte verneint wird, sollen sie schließlich doch für bestimmte Inhalte mehr Pflichten übernehmen. Zum Beispiel haben die ISP in den USA nach § 604 des Gesetzes zum Schutz vor sexuellen Übergriffen auf Kinder von 1998 eine aktive Berichtspflicht über Kinderpornografie. Nach dieser Regelung sollen die ISP den zuständigen Behörden unverzüglich mitteilen, wenn sie Kenntnis von rechtswidrigen Inhalten haben, sonst werden sie bei der ersten Unterlassung mit bis zu 50.000

---

203 Vgl. *Sieber*, MMR Heft 12, 1999, 690.

204 Siehe *Subashini/Kavitha*, Journal of Network and Computer, 2011, 9.

205 Siehe *Armbrust*, etc., CACM, Vol. 53, Issue 4, 2010, 55.

206 Siehe *Kaufman*, IEEE Security & Privacy, Vol. 7, Issue 4, 2009, 62.

Dollar, bei der zweiten Unterlassung mit bis zu 100.000 Dollar bestraft.[207] Dies bedeutet, dass die Verpflichtung der ISP zumindest in den USA teilweise geändert worden ist. Der Grund dafür liegt in der Besonderheit der Kinderpornografie und im besonderen Schutz der Kinder.

Insgesamt ist zu sagen, dass die Anforderungen an die Netzsicherheit und die daraus resultierenden Pflichten der ISP in einigen speziellen Konstellationen wesentlich höher als im Normalbetrieb sind. Den ISP eine allgemeine neutrale Eigenschaft zuzugestehen, wird dadurch unmöglich. Inzwischen haben immer mehr Rechtswissenschaftler die Begrenztheit der neutralen Handlung für die Bestimmung der strafrechtlichen Verantwortlichkeit der ISP erkannt.

Im Kommentar zum *Kuaibo*-Fall wird festgestellt, dass die Angeklagten (die ISP) das strafrechtliche Risiko durch ihre Internetdienste erheblich erhöht haben. Deshalb solle die Theorie von der neutralen Handlung für *Kuaibo* nicht in Betracht kommen. Außerdem hätten die Angeklagten die Sicherheitspflichten im Netzwerk nicht erfüllt. Dies sei als Pflichtdelikt, nicht als Beihilfe einzustufen.[208] Der für den *Kuaibo*-Fall zuständige Richter wies auch darauf hin, dass das Prinzip der technischen Neutralität nur für den Anbieter der Technik, nicht für deren Benutzer gelte. Da die Angeklagten nicht zu den bloßen Benutzern der Technik gehörten, sei das Prinzip der technischen Neutralität hier nicht anzuwenden.[209]

Zudem wird mit Berufung auf die Meinung von *Roxin* argumentiert, dass die Strafbarkeit der sogenannten neutralen Gehilfen nicht verneint werden kann, wenn der Gehilfe die zu begehende Straftat des Täters schon erkannt hat. Außerdem seien die Sicherheitspflichten im chStGB schon vorgesehen. Aus diesem Grund habe die Theorie der neutralen Handlung ihre Anwendungsgrundlage verloren.[210]

Darüber hinaus gibt es viele unterschiedliche theoretische Ansichten zu der neutralen Handlung. Bis heute existiert kein maßgebendes Kriterium dafür. Deshalb ist die Durchführbarkeit dieser Theorie problematisch. Eine so allgemeine Theorie kann der Typisierung der Handlungen von ISP nicht entsprechen, was wiederum ihre Anwendbarkeit beeinträchtigt.[211]

Schließlich wird konstatiert, dass die Position der ISP in der Informationsgesellschaft nicht immer neutral sei. Im derzeitigen Rechtsrahmen gebe es schon viele

---

[207] Siehe Protection of Children from Sexual Predators Act of 1998, Article 604.

[208] Vgl. *Zhou Guangquan*, Rechtszeitschrift der Universität Peking Heft 1, 2017, 61; ähnliche Meinung vgl. *Chen Xingliang*, Rechtszeitschrift der Universität Peking Heft 1, 2017, 13.

[209] Vgl. *Fan Jun*, Rechtszeitschrift der Universität Peking Heft 1, 2017, 40. Diese Stellungnahme wird auch in dem Urteil des *Kuaibo*-Falls dargestellt. Vgl. Urteil der ersten Instanz zum *Kuaibo*-Fall, abrufbar unter http://bjhdfy.chinacourt.org/public/detail.php?id=4343 [Stand: 15.09.2017].

[210] Vgl. *Xie Wangyuan*, Chinesische Rechtswissenschaft Heft 2, 2017, 253 ff.

[211] Vgl. *Tu Longke*, Law Review Heft 3, 2016, 70.

Regelungen, die sich auf die Sicherheitspflichten im Netzwerk beziehen. In bestimmen Situationen seien die ISP nach den einschlägigen Normen zu bestrafen, anstatt nach der Theorie der neutralen Handlung privilegiert zu werden.[212]

Zusammenfassend lässt sich feststellen, dass die Theorie der neutralen Handlung nur in begrenztem Umfang zur Bestimmung der strafrechtlichen Verantwortlichkeit der ISP angewendet werden kann. Die Handlungen der ISP sollten nicht leichtfertig mit der neutralen Handlung gleichgesetzt werden.

3. Einordnung der Handlung als Täterschaft oder Teilnahme

Da die Diskussion über die strafrechtliche Verantwortlichkeit der ISP ein relativ neues Thema in China ist, gibt es bislang keine systematische Untersuchung, die sich mit der Einordnung der Handlungen der ISP als Täter oder Teilnehmer befasst. Eine solche Einordnung wird normalerweise anhand von Einzelfallanalysen vorgenommen, sie beruht also auf dem allgemeinen Grundsatz für die Abgrenzung von Täter und Teilnehmer.

a) Vor Inkrafttreten des Strafrechtsänderungsgesetzes (IX)

Vor dem Inkrafttreten des Strafrechtsänderungsgesetzes (IX) 2015 existierten keine spezifischen Paragrafen über die strafrechtliche Verantwortlichkeit der ISP. In diesem Rechtsrahmen gab es zwei Möglichkeiten für die Einordnung der ISP als Teilnehmer oder Täter.

Da die ISP grundsätzlich keine eigenen Inhalte anbieten und eine relativ untergeordnete Rolle spielen, sind sie der Einfachheit halber als Teilnehmer zu betrachten. In den meisten Fällen stellen die ISP den Nutzern nur die Internetdienste zur Verfügung und haben daher in der Regel keine Tatherrschaft. Um ein Beispiel zu nennen: Das Angebot der Internetdienste von ISP könnte die Verbreitung strafbarer Inhalte fördern, die ISP sind aber gar nicht in der Lage, diese zu kontrollieren. Theoretisch gesehen gibt es deshalb vor allem die Möglichkeiten, die ISP als Gehilfen anstatt als Täter zu bestrafen.[213]

Die Einordnung der ISP als Teilnehmer ist in der Praxis mit vielen Schwierigkeiten konfrontiert. Das Hauptproblem liegt darin, dass die Täter aus vielen Gründen oft nicht direkt bestraft werden können. Etliche Content Provider, die wegen ihrer unmittelbaren Nutzungsangebote rechtswidriger Inhalte als Täter zu betrachten sind, befinden sich im Ausland. Diese eigentlichen Täter sind aufgrund der gesetzlichen Unterschiede im ausländischen Rechtsrahmen meist nicht strafbar. Manchmal kön-

---

[212] Vgl. *Liang Genlin*, Rechtswissenschaft Heft 2, 2017, 10 ff.

[213] Vgl. *Qin Tianning/Zhang Mingxun*, Strafrechtliche Wissenschaft Heft 9, 2009, 43.

nen sie auch nicht bestraft werden, weil es Konflikte über die Zuständigkeit oder Schwierigkeiten bei der Rechtshilfe gibt.

Außerdem gibt es im chStGB zahlreiche quantitative Elemente, die den Grad des Unrechts bestimmen und dazu führen, dass die Täter in vielen Fällen die quantitative Schwelle, ab der eine Straftat strafwürdig ist, nicht erreichen. Dies ist wiederum auf die spezielle Struktur der Beteiligung im Netzwerk zurückzuführen: Im Vergleich zu der realen Welt spielen gerade die Teilnehmer oft eine zentrale Rolle beim Verbrechen, während die Täter umgekehrt relativ wenige Beiträge leisten. Deshalb können die Täter den Standard der einschlägigen quantitativen Elemente nicht erreichen. Aufgrund der Forderung der Akzessorietät wird die Bestrafung der ISP entsprechend stark eingeschränkt. Darüber hinaus wird die subjektive Beziehung zwischen den Straftätern im Netzwerk wegen der komplexen Arbeitsteilung in der Cyberkriminalität immer schwächer. Deshalb kann die subjektive Voraussetzung für eine Beteiligung im Netzwerk häufig nicht erfüllt werden.

Angesichts dieses Dilemmas kommt die Möglichkeit in Betracht, dass die ISP wegen ihrer Verletzung bestimmter Pflichten direkt als Täter einzustufen sind. Auf diese Weise ist die strafrechtliche Verantwortlichkeit der ISP nicht mehr von der Strafbarkeit des eigentlichen Täters abhängig, und das Problem der Akzessorietät zwischen Täter und Teilnehmer kann dadurch gelöst werden.

Aus dieser Perspektive liegt die zentrale Frage in der Bestimmung der einschlägigen strafrechtlichen Garantenstellung der ISP. Wenn die ISP beispielsweise als Täter für die Verbreitung pornografischer Inhalte betrachtet werden sollen, ist zuerst festzustellen, ob sie in einer bestimmten Konstellation die Verpflichtung besitzen, eine derartige Verbreitung zu verhindern. In der Praxis trat diese Lösung in den Vordergrund. Im *Kuaibo*-Verfahren konzentrierte sich der Staatsanwalt auf die Verletzung der Sicherheitsverpflichtung der ISP. Die Verdächtigen wurden vom Staatsanwalt direkt als Täter angeklagt. Auffällig ist, dass die Verteidigung unter Berufung auf die Theorie der neutralen Handlung deutlich vom Gericht in erster Instanz zurückgewiesen wurde.[214] Schließlich wurde die Anklage im Allgemeinen vom Gericht in zweiter Instanz anerkannt.[215] Nach dem *Kuaibo*-Fall nahmen die Rechtswissenschaftler in der Theorie zunehmend die Untersuchung der Einordnung der ISP als Täter in den Blick.

Insgesamt sind die oben genannten zwei Lösungen unter bestimmten Bedingungen haltbar. Da die Einordnung der ISP als Teilnehmer oft auf Schwierigkeiten stößt, wird ihre Klassifizierung als Täter wegen der Verletzung ihrer Verpflichtung nun häufiger diskutiert. Jedoch ist zu beachten, dass bei diesem Ansatz die straf-

---

[214] Vgl. Urteil der ersten Instanz zum *Kuaibo*-Fall, http://bjhdfy.chinacourt.org/public/detail.php?id=4343 [Stand: 15.09.2017].

[215] Vgl. Urteil der zweiten Instanz zum *Kuaibo*-Fall, Volksgerichtszeitung, 16.12.2016.

rechtliche Verpflichtung der ISP ausreichend begründet werden muss, sonst wird die strafrechtliche Verantwortlichkeit der ISP auf ungeeignete Weise erweitert.

b) Nach Inkrafttreten des Strafrechtsänderungsgesetzes (IX)

Nach Inkrafttreten des Strafrechtsänderungsgesetzes (IX) hat sich die Situation verändert. In § 286 Abs. 1 chStGB wird die strafrechtliche Verantwortlichkeit der ISP selbstständig vorgesehen. Wenn die ISP die in den Gesetzen und Anordnungen formulierten Sicherheitsverpflichtungen nicht erfüllen, werden sie direkt als Täter, nicht als Teilnehmer bestraft. Stellen sie anderen Straftätern im Netzwerk Hilfe durch Internetdienste zur Verfügung, sollen sie nach § 287 Abs. 2 chStGB ebenso als Täter bestraft werden. Die Bestimmung der strafrechtlichen Verantwortlichkeit der ISP ist jetzt nicht mehr von den allgemeinen Grundsätzen der Beteiligung abhängig. Auffällig ist das Problem der Gesetzeskonkurrenz nach Inkrafttreten des Strafrechtsänderungsgesetzes (IX). Denn neben den neuen selbstständigen Tatbeständen bezüglich der strafrechtlichen Verantwortlichkeit können die ISP weiterhin von den traditionellen Tatbeständen als Teilnehmer oder sogar als Täter erfasst werden. Wenn die ISP beispielsweise wussten, dass die Nutzer durch die Internetdienste Straftaten begehen, aber ihnen die Dienste weiter zur Verfügung gestellt haben, können nicht nur § 286 Abs. 1 chStGB, § 287 Abs. 2 chStGB, sondern auch § 363 Abs. 1 und § 364 Abs. 2 Anwendung finden. Bei Gesetzeskonkurrenz haben die spezielleren Vorschriften (§§ 286 Abs. 1, 287 Abs. 2 chStGB) allerdings grundsätzlich Vorrang.

IV. Gesetzlich nicht geregelte Typen der ISP und ihre Verantwortlichkeit

A. Peer-to-Peer-Netzwerke

1. Einordnung der Betreiber von Peer-to-Peer-Netzwerken

In China hat sich die Peer-to-Peer-Technologie sehr schnell entwickelt, seit dem Jahr 2000 etwa wird sie in der Praxis angewendet. Das Problem der Urheberrechtsverletzung, das sich nicht nur im zivilrechtlichen, sondern auch im strafrechtlichen Bereich als ein ganz neues Thema darstellt, ist in einigen Peer-to-Peer-Netzwerken besonders verbreitet. Im Allgemeinen werden die Peer-to-Peer-Netzwerke in China auch in eine zentrale und dezentrale Struktur unterteilt.[216] Diese Unterscheidung

[216] Vgl. *Yang Caixia*, Politik und Recht Heft 3, 2016, 43 ff. In der Literatur wird auch die Auffassung vertreten, dass drei Generationen in der Geschichte der Entwicklung der P2P-Netzwerke bestehen, nämlich das P2P-Netzwerk mit zentralem Server, das P2P-Netz-

wird ebenso als eine grundlegende Voraussetzung für die Diskussion der Verantwortlichkeit der Betreiber der Peer-to-Peer-Netzwerke betrachtet.

Im chinesischen Rechtsrahmen gibt es fünf Arten von ISP, nämlich Content Provider, Access Provider, Caching Provider, Hosting Provider und Suchmaschinenbetreiber. Die gesetzliche Typisierung der ISP wurde von den amerikanischen Gesetzen, besonders dem DMCA, deutlich beeinflusst, dementsprechend ist die systematische Einordnung der Betreiber der Peer-to-Peer-Netzwerke in China ähnlich wie in den USA. In den Vereinigten Staaten wird die Verantwortlichkeit der Betreiber von Peer-to-Peer-Netzwerken nicht mit dem Privilegierungssystem im DMCA verknüpft, weil bei Ausarbeitung des DMCA die Peer-to-Peer-Technologie noch kaum bekannt war. Die Gesetzgeber haben daher die Eigenschaften von Peer-to-Peer-Netzwerken beim Entwerfen des DMCA gar nicht in Erwägung gezogen. Deshalb wurde in der amerikanischen Rechtsprechung die Forderung, die Verantwortung der P2P-Betreiber gemäß DMCA zu privilegieren, abgelehnt.[217]

Die chinesischen Rechtswissenschaftler haben die Auffassung der USA übernommen und ordnen die Betreiber von Peer-to-Peer-Netzwerken nicht mehr in das Privilegierungssystem der ISP ein. Im Gegenteil, die Verantwortlichkeit der P2P-Betreiber wird nach dem traditionellen Prinzip für die gemeinschaftlich begangene unerlaubte Handlung beurteilt, die Position der Betreiber der Peer-to-Peer-Netzwerke als selbstständig angesehen. Deshalb ist der Vergleich zwischen den Betreibern der Peer-to-Peer-Netzwerke und den gesetzlichen ISP nicht der Schwerpunkt der vorliegenden Untersuchung.

2. Privilegien der Betreiber von Peer-to-Peer-Netzwerken

Da die meisten chinesischen Rechtswissenschaftler urheberrechtlich die Theorie von der gemeinschaftlich begangenen unerlaubten Handlung von den USA übernommen haben, wird die Verantwortlichkeit der Betreiber der Peer-to-Peer-Netzwerke in China auch von der amerikanischen Lehre stark geprägt. In der einschlägigen Literatur wird die US-amerikanische Lösung und ihre Entwicklungsgeschichte oft ausführlich erklärt. Nach amerikanischem Recht gibt es zwei Arten von Urheberrechtsverletzungen, nämlich die direkte Verletzung (*direct infringement*) und die indirekte Verletzung (*indirect infringement*). Die indirekte Verletzung kann weiter in mitwirkende Ver letzung (*contributory infringement*) und stellvertretende Verletzung (*vicarious in fringement*) unterschieden werden. Danach wurde die Haf-

---

werk mit Client-Server, das P2P-Netzwerk mit verteiltem Server. Vgl. *Cui Lihong/Hao Lei*, Juristisches Forum Heft 2, 2006, 90 ff.

[217] Vgl. *Zhang Lingling*, Geistiges Eigentum Heft 4, 2012, 41; *Jiang Shuai*, Elektronisches geistiges Eigentum Heft 8, 2015, S. 78; *Weng Mingjiang/Wu Lei*, Recht und soziale Entwicklung Heft 2, 2002, 153; *Frey*, ZUM Heft 6, 2001, 473 ff.

tungsregel der sogenannten „substanziellen nicht-verletzenden Nutzung“ (*substantial non-infringing use*) im bekannten *Sony*-Fall begründet: Die mitwirkende Verletzung kann nicht festgestellt werden, wenn das angebotene Produkt überwiegend einer legalen und unstrittigen Verwendung dient oder – mit anderen Worten – eine „substanzielle nicht-verletzende Nutzung“ hat, obwohl die Anbieter der Produkte wissen, dass die Produkte von Dritten zur Rechtsverletzung angewendet werden könnten.[218]

Dieses aus dem *Sony*-Fall abgeleitete Merkmal hat die indirekte Deliktshaftung beschränkt.[219] Mit der Entwicklung der Peer-to-Peer-Netzwerk-Technologie wurde es aber zunehmend problematisch, denn obwohl die Forderung der „substanziellen nicht-verletzenden Nutzung“ erfüllt werden kann, tauschen Nutzer immer noch zahlreiche urheberrechtlich geschützte Werke in Peer-to-Peer-Netzwerken aus.

Im *Napster*-Fall hatte der Richter schließlich die Verantwortung des Betreibers aus indirekter Rechtsverletzung festgestellt,[220] weil der Betreiber den rechtsverletzenden Nutzern durch Bereitstellung des zentralen Servers materiale Hilfe leistete.[221] Aber mit fortschreitender technischer Entwicklung ist ein zentraler Server im Peer-to-Peer-Netzwerk nicht mehr unentbehrlich. In einer dezentralen technischen Struktur können schwere Urheberrechtsverletzungen begangen werden, während die durch den zentralen Server begründete Kontrolle des Betreibers nicht mehr besteht. Gemäß der „substanziellen nicht-verletzenden Nutzung“ werden diese Betreiber jedoch privilegiert. Deswegen ist zu beachten, dass das Kriterium der „substanziellen nicht-verletzenden Nutzung“ bezüglich der Verantwortlichkeit der Betreiber der Peer-to-Peer-Netzwerke mit Herausforderungen konfrontiert ist.[222]

Besonders im *Grokster*-Fall zeigte sich dessen Schwäche. In den Entscheidungen erster und zweiter Instanz hafteten die Betreiber unter Berufung auf die „substanzielle nicht-verletzende Nutzung“ nicht für die indirekte Urheberrechtsverletzung. Diese Urteile wurden als ungerecht bewertet, weil die Urheberrechte der geschützten Werke im dezentralen Peer-to-Peer-Netzwerk fortlaufend verletzt werden.[223] Angesicht dieser möglichen ungerechten Ergebnisse hat der Supreme Court in den USA eine gegenteilige Entscheidung getroffen. Demnach hafteten die *Grokster*-Betreiber wegen mitwirkender Verletzung, weil sie die Rechtsverletzung angeleitet und angestiftet haben. Daher wurde das Kriterium der sogenannten induzierenden

---

218 Vgl. *Wang Qian*, Zeitschrift für Wissenschaft, Technologie und Recht Heft 4, 2004, 62.

219 Vgl. *Xiong Qi*, Geistiges Eigentum Heft 6, 2009, 67 ff.

220 In diesem Fall wird die Haftung nicht nur bei mitwirkender Verletzung, sondern auch bei stellvertretender Verletzung vom Gericht bejaht. Vgl. *Weng Mingjiang/Wu Lei*, Recht und soziale Entwicklung Heft 2, 2002, 147 ff.

221 Vgl. *Cui Lihong/Hao Lei*, Juristisches Forum Heft 2, 2006, 93; *Wang Qian*, Elektronisches geistiges Eigentum Heft 11, 2004, 31.

222 Vgl. *Wang Qian*, Zeitschrift für Wissenschaft, Technologie und Recht Heft 4, 2004, 67.

223 Vgl. *Wang Qian*, Elektronisches geistiges Eigentum Heft 11, 2004, 31 ff.

Verletzung (*inducing infringement*) begründet, indem die „substanzielle nichtverletzende Nutzung“ beschränkt wird.[224]

Im chinesischen Rechtsrahmen gibt es nur einige allgemeine Regelungen über die Deliktshaftung bei gemeinschaftlicher Rechtsverletzung. § 9 des chinesischen Deliktsgesetzes lautet: Wer einen anderen zu dessen Rechtsverletzung bestimmt oder Hilfe geleistet hat, soll mit dem Handelnden die gesamtschuldnerische Haftung übernehmen. § 7 Abs. 1 der „Interpretation über die Anwendung der Gesetze zu dem Zivilstreit bezüglich des Informationsnetz-Übertragungsrechts“ 2012 des Obersten Volksgerichts besagt: Wenn der ISP einem Nutzer zu dessen Verletzung des Informationsnetz-Übertragungsrechts von Dritten Hilfe leistet oder der ISP einen Nutzer dazu anstiftet, soll der ISP eine Deliktshaftung übernehmen. Diese Regelungen bilden einen grundlegenden Rechtsrahmen für die gemeinschaftliche Deliktshaftung. Zudem werden die US-amerikanischen Kriterien über die indirekte Rechtsverletzung in der chinesischen Literatur als ergänzende Inhalte weiter aufgenommen. In der Praxis war die Haftung bei indirekter Urheberrechtsverletzung schon in einer Reihe von Fällen – etwa im *Kuro*-Fall[225] und im *POCO*-Fall[226] – festgestellt worden.

Jedoch ist es auffällig, dass im Gegensatz zu den USA das *safe harbor*- und das entsprechende *red flag*-Prinzip in der Bestimmung der gemeinschaftlichen Deliktshaftung der Betreiber von Peer-to-Peer-Netzwerken in China noch eine wichtige Rolle spielen. Einigen Rechtswissenschaftlern zufolge tragen die Betreiber nur dann eine gemeinschaftliche Deliktshaftung mit den rechtsverletzenden Nutzern, wenn sie die Rechtsverletzung von Dritten kennen oder kennen sollten, was sich offensichtlich aus den beiden genannten Prinzipien herleitet.[227] Diese Auffassung, die sich auch im *Kuro*-Fall zeigte,[228] ist meines Erachtens zu bejahen, weil sie dem chinesischen Rechtsrahmen über die Verantwortlichkeit der gemeinschaftlichen Deliktshaftung entspricht.

Auf der einen Seite sind das *safe harbor*- und das *red flag*-Prinzip aus dem DMCA – wie oben erläutert – schon durch § 36 des Deliktsgesetzes und andere Anordnung und Interpretation auf eine allgemeine Weise in den chinesischen Rechtsrahmen aufgenommen worden. Das heißt, grundsätzlich können alle ISP unter die Privilegierungsregelungen fallen. Aus dieser Perspektive gibt es die Möglichkeit, diese Regelungen für die Verantwortlichkeit der Betreiber der Peer-to-Peer-Netzwerke anzuwenden, auch wenn in den USA eine andere Ausgangslage herrscht. Tatsächlich wurden beide Prinzipien in der amerikanischen Rechtsprechung

---

[224] Vgl. *Wang Qian*, Elektronisches geistiges Eigentum Heft 9, 2005, 54 ff.; *Yang Hui/Ma Ning*, Elektronisches geistiges Eigentum Heft 8, 2005, 50 ff.

[225] Vgl. *Feng Gang*, Geistiges Eigentum Heft 3, 2008, 47 ff.

[226] Vgl. *Zhu Jianjun/Tan Minghua*, Geistiges Eigentum Heft 1, 2009, 45 ff.

[227] Vgl. ebenda, 48 ff.; *Feng Gang*, Geistiges Eigentum Heft 3, 2008, 48 ff.

[228] Vgl. *Zhang Lingling*, Geistiges Eigentum Heft 4, 2012, 45.

nicht absolut verneint. Im *Napster*-Fall wurde von dem Berufungsgericht argumentiert, dass die Möglichkeit der Haftung bei indirekter Urheberrechtsverletzung die Anwendbarkeit des DMCA nicht ausschließt. Außerdem solle der Kläger nach dem Urteil verpflichtet sein, über die Existenz der rechtsverletzenden Dateien zu berichten, während der Angeklagte nur im Rahmen seiner Kontrollmöglichkeit die Verpflichtung habe, die Rechtsverletzung zu beobachten.[229] Dies zeigt, dass der Kern des *safe harbor*-Prinzips noch mittelbar vom amerikanischen Gericht akzeptiert wird. Auf der anderen Seite sind die Regeln über die gemeinschaftliche Deliktshaftung im chinesischen Rechtsrahmen relativ generell gehalten. Obwohl die Haftung bei helfender und anstiftender Verletzung in chinesischen Gesetzen vorgesehen wird, bleiben die konkreten Voraussetzungen für diese Deliktshaftung noch unklar. Deshalb kann die Auslegung der chinesischen Regelungen unter Berufung auf die amerikanischen Haftungsregelungen bei indirekter Verletzung bereichert und verbessert werden.[230]

Die Einführung der *safe harbor*- und *red flag*-Prinzipien in China und die in einer Reihe von Entscheidungen begründeten amerikanischen Kriterien über die Haftung bei indirekter Rechtsverletzung können meines Erachtens kombiniert werden, die beiden Systeme widersprechen sich nicht.

3. Strafrechtliche Verantwortlichkeit der Betreiber von Peer-to-Peer-Netzwerken

Über die strafrechtliche Verantwortlichkeit der Betreiber von Peer-to-Peer-Netzwerken herrscht kein breiter Konsens, zum einen, weil dies ein völlig neues Problem darstellt, dem die meisten Rechtswissenschaftler noch keinen großen Wert beimessen, zum anderen, weil sich die Peer-to-Peer-Technologie schnell entwickelt hat und sich ständig verändert. Deswegen ist eine zutreffende strafrechtliche Bewertung nicht einfach.

In der älteren Literatur findet die Typisierung der Peer-to-Peer-Netzwerke nicht ausreichend Beachtung. Folglich existieren nur einige allgemeine Aussagen über die strafrechtliche Verantwortlichkeit der Betreiber von Peer-to-Peer-Netzwerken, beispielsweise, dass sie in der Regel nicht strafbar sein sollen.[231] Offensichtlich wird die Problematik auf diese Weise unangemessen vereinfacht.

Das Problem der Typisierung der Peer-to-Peer-Netzwerke tritt erst in der aktuellen Literatur in den Vordergrund. Es wird darauf hingewiesen, dass der Unterschied zwischen einem zentralen und einem dezentralen Peer-to-Peer-Netzwerk die Bewertung der strafrechtlichen Verantwortlichkeit deutlich beeinflusst. Eine Unter-

---

[229] Vgl. *Jiang Shuai*, Elektronisches geistiges Eigentum Heft 8, 2015, 78.

[230] Vgl. *Xiong Qi*, Geistiges Eigentum Heft 6, 2009, 73.

[231] Vgl. *Chen Hongbing*, Zeitschrift der Nordöstlichen Universität (Sozialwissenschaftliche Ausgabe) Heft 3, 2009, 260.

suchung zeigt, dass im Vergleich zu den dezentralen Peer-to-Peer-Netzwerken die Betreiber der zentralen Peer-to-Peer-Netzwerke anfällig für die strafrechtlichen Risiken sind.[232] Rein formal können die Betreiber der Peer-to-Peer-Netzwerke bei einer Rechtsverletzung sowohl Täter als auch Teilnehmer werden.[233] Allerdings gilt allgemein, dass die Betreiber der Peer-to-Peer-Netzwerke in der Regel nur als Teilnehmer zu bestrafen sind. Da die P2P-Betreiber nicht zu den Content Providern gehören und Urheberrechte nicht direkt verletzen, wird die Strafbarkeit der Betreiber hier hauptsächlich als Anstifter oder Gehilfe diskutiert.[234] Im *Kuro*-Fall in Taiwan wurde die Mittäterschaft des Betreibers des Peer-to-Peer-Netzwerks vom Gericht bestimmt. Aber diese Ansicht ist in der Theorie auf Kritik gestoßen.[235]

a) Strafbarkeit der Betreiber als Gehilfen

aa) Anwendung der Theorie der neutralen Handlung

Wenn die Betreiber den rechtsverletzenden Nutzern absichtlich durch ihre Dienste Hilfe leisten, können sie als strafbare Gehilfen angesehen werden.[236] Rein kausal gesehen können die böswilligen Nutzer ohne die Dienste der Betreiber überhaupt keine Straftaten begehen. Da aber von vielen Rechtswissenschaftlern eine normative Beschränkung der Strafbarkeit der Gehilfen als nötig erachtet wird, verdient hier die Theorie der neutralen Handlung besondere Beachtung.

Im *erPeer*-Fall in Taiwan hatte der Richter die strafrechtliche Verantwortlichkeit der Betreiber des Peer-to-Peer-Netzwerks unter Berufung auf die Theorie der neutralen Handlung ausdrücklich ausgeschlossen. Nach Meinung des Gerichts gehört die Bereitstellung der „erPeer“ zu einer neutralen Verhaltensweise, weil die Internetdienste des Betreibers für alle Mitglieder zugänglich sind und sie dem Austausch von Dateien der Nutzer und nicht speziell zu Straftaten dienen. Zur Abgrenzung zwischen der neutralen Handlung und der strafbaren Beihilfe hatte das Gericht die subjektive Ansicht aus der Entscheidung des deutschen BGH übernommen.[237] Laut dem taiwanesischen Urteil sollen die Betreiber der Peer-to-Peer-Netzwerke nicht als Gehilfen bestraft werden, wenn sie keine oder nur bedingte Kenntnisse von den Straftaten haben.[238]

---

232 Vgl. *Yang Caixia*, Politik und Recht Heft 3, 2016, 47.

233 Vgl. *Cai Huifang*, Soochow Rechtszeitschrift Heft 1, 2006, S. 62.

234 Vgl. *Yang Caixia*, Politik und Recht Heft 3, 2016, 48 ff.

235 Vgl. *Cai Huifang*, Rechtszeitschrift für Technologie Heft 1, 49 ff.

236 Vgl. *Tan Shaomu/Wu Weibing*, Volksjustiz Heft 10, 2006, 67.

237 Vgl. BGHSt 46, 107, 112.

238 Vgl. das strafrechtliche Urteil des Amtsgerichts Taiwan Shilin 2003, Nr. 728 (台湾士林地方法院刑事判决 2003 年诉字第 728 号).

In der Literatur zeichnet sich diese Tendenz ebenfalls ab. Es wird von Rechtswissenschaftlern die These vertreten, dass die Dienste der Betreiber von Peer-to-Peer-Netzwerken zur neutralen Handlung anstatt zur strafbaren Beihilfe zu rechnen sind, obwohl die Betreiber den Tätern wirklich kausale Hilfe geleistet haben. Zum Kriterium der neutralen Handlung gibt es zwei entgegengesetzte Auffassungen: Eine wohl durch die Lehre von *Roxin* beeinflusste Ansicht konzentriert sich auf den subjektiven Zustand der Betreiber.[239] Im Gegensatz dazu vertreten andere die Meinung, dass die Besonderheit der neutralen Handlung nicht in dem subjektiven, sondern in dem objektiven Aspekt liege. Da die neutrale Handlung keine rechtlich missbilligte Gefahr geschafft habe, sei sie nicht strafbar.[240]

Die positive Bedeutung und die Begrenztheit der Theorie der neutralen Handlung für die Verantwortlichkeit der ISP sind schon zuvor erläutert worden. Meines Erachtens kann diese Theorie nicht ohne die Typisierung der ISP als einer unentbehrlichen Voraussetzung auf eine allgemeine Weise auf die strafrechtliche Verantwortlichkeit der ISP angewendet werden.[241] Das heißt, dass die Theorie der neutralen Handlung nur für einen bestimmten Teil der ISP anwendbar ist, was gleichfalls für die Betreiber von Peer-to-Peer-Netzwerken gilt.

In den unterschiedlichen Peer-to-Peer-Netzwerken gibt es verschiedene technische Strukturen, sodass die Kontrollmöglichkeit der Betreiber jeweils sehr detailliert und konkret analysiert werden muss. In einem zentralen Peer-to-Peer-Netzwerk werden die Informationen über ein Inhaltsverzeichnis und den Speicherort der ausgetauschten Dateien auf dem Server des Betreibers registriert und gespeichert. Der Lauf des Netzwerks für den Dateienaustausch steht also bis zu einem gewissen Grad unter der Kontrolle der Betreiber. In dieser Situation hat der Betreiber die Verpflichtung, relevante Informationen zu löschen, wenn konkrete Kenntnisse über Straftaten vorliegen. In einem dezentralen Peer-to-Peer-Netzwerk gestalten sich die Verhältnisse anders. Dessen Betreiber hat wegen der spezifischen technischen Struktur in der Regel keine wirksame Kontrolle über das Handeln seiner Mitglieder. Vorausgesetzt, dass der Betreiber diese Dienste nicht speziell für das illegale Handeln konstruiert, gibt es heir die Möglichkeit, die Theorie der neutralen Handlung anzuwenden.

bb) Einordnung der Handlung als Tun oder Unterlassen

Im Allgemeinen können die Betreiber der Peer-to-Peer-Netzwerke nicht nur für positives Tun, sondern auch für Unterlassen bestraft werden. In der Praxis erscheinen die Handlungen der Betreiber in den meisten Fällen wegen ihrer Pflichtverlet-

---

239 Vgl. *Cai Huifang*, Soochow Rechtszeitschrift Heft 1, 2006, 73 ff.

240 Vgl. *Chen Hongbing*, Zeitschrift der Nordöstlichen Universität (Sozialwissenschaftliche Ausgabe) Heft 3, 2009, 262.

241 Vgl. *Chen Hongbing*, Chinesische Rechtswissenschaft Heft 1, 2017, 203.

zung als Unterlassungen.[242] Deswegen bildet die Quelle der Verpflichtung zur Kontrolle rechtswidriger Informationen den Schwerpunkt der Diskussion.

So wird die Forderung erhoben, dass die Betreiber der Peer-to-Peer-Netzwerke sich verpflichten sollten, die Gesetzmäßigkeit der Informationen für das Urheberrecht zu kontrollieren, bevor Dateien ins Netz gestellt werden.[243] Im Gegensatz dazu wird argumentiert, dass die Unterlassung wegen Pflichtverletzung bei Betreibern von Peer-to-Peer-Netzwerken schwer begründet werden könne, weil über die vorherige Verpflichtung keine klare Regelung existiere. Zudem hätten die Betreiber nicht nur der dezentralen, sondern auch der zentralen Peer-to-Peer-Netzwerke nur eine sehr geringe Kontrollfähigkeit über den rechtsverletzenden Dateienaustausch.[244] Deshalb wird die vorherige Verpflichtung der P2P-Betreiber zur Überprüfung rechtswidriger Informationen von den meisten Rechtswissenschaftlern verneint. Nur wenn die Betreiber Kenntnisse von den Straftaten Dritter erlangt oder eine Mitteilung über diese Rechtsverletzung erhalten hätten, sei der Verpflichtung der P2P-Betreiber zuzustimmen.[245]

b) Strafbarkeit der Betreiber als Anstifter

In der Literatur wird auch diskutiert, ob die Betreiber der Peer-to-Peer-Netzwerke als Anstifter bestraft werden können. Im urheberrechtlichen Bereich wird die Haftung der P2P-Betreiber bei induzierender (anstiftender) Verletzung – wie zuvor beschrieben – in einigen Entscheidungen bejaht. Jedoch wird die Strafbarkeit der Betreiber als Anstifter im strafrechtlichen Bereich grundsätzlich verneint. Auf der einen Seite haben die Betreiber oft nur bedingte Kenntnisse von dem Handeln der Nutzer. Auf der anderen Seite ist noch weiter zu überprüfen, ob die Betreiber durch ihre Dienste ihre Nutzer zu Straftaten angestiftet haben, obwohl sie schon konkrete Kenntnisse von Straftaten Dritter besessen haben. Allerdings ist es schwierig zu beweisen, dass das Motiv zur Straftat sich erst durch das Angebot der Dienste entwickelt hat.[246]

---

242 Vgl. *Tan Shaomu/Wu Weibing*, Volksjustiz Heft 10, 2006, 67.

243 Vgl. *You Chunliang*, Die vorherige Verpflichtung zur Überprüfung soll den ISP gegeben werden, Legal Daily 005, 27.10.2008.

244 Vgl. *Yang Caixia*, Politik und Recht Heft 3, 2016, 52.

245 Vgl. *Chen Zhigang/Li Shanhe*, Kriminalwissenschaft Heft 4, 2014, 51 ff.

246 Vgl. *Yang Caixia*, Politik und Recht Heft 3, 2016, 49 ff.

B. Hyperlinks

1. Einordnung von Hyperlinks

Die Hyperlink-Technologie ist im chinesischen Netzwerk weit verbreitet. Insgesamt werden die Hyperlinks in zwei Typen unterteilt, nämlich normale Hyperlinks (*Surface Links*) und tiefe Hyperlinks (*Deep Links*). Der zentrale Unterschied liegt in der Entfernung zwischen den Hyperlinks und den verlinkten Dateien. Bei Deep Links werden die verlinkten Dateien direkt, nicht über die Homepage der Webseite, durch Hyperlinks erreicht. Für die tiefen Hyperlinks unterscheidet man weitere Formen, zum Beispiel Framed Links, Embedded Links und Inline Links.[247] Im Gegensatz zu der Gesetzgebung in Deutschland wird die Verantwortlichkeit der Hyperlinksetzer in Gesetzen, Verordnungen und Interpretationen des Obersten Volksgerichts als selbstständig angesehen, der Regelung von § 512 Abs. d DMCA in den USA vergleichbar.

Jedoch ist die rechtliche Einordnung von Hyperlinksetzern wegen der technischen Komplexität und Vielfalt der Hyperlinks noch nicht eindeutig geregelt. Die gesetzlichen Verantwortlichkeitsregelungen können nicht für jeden Hyperlinksetzer Anwendung finden. Hier ist die Unterscheidung zwischen Surface Links und Deep Links der Schlüssel, weil die beiden Hyperlinksetzer ganz unterschiedliche Kontrollmöglichkeiten über die verlinkten Inhalte haben.[248] In der Regel kann die Verantwortlichkeit der Anbieter der Surface Links nach der selbstständigen Privilegierung in Gesetz und Interpretation vom Obersten Gerichtshof bestimmt werden. Offen bleibt aber die rechtliche Behandlung der Anbieter der Deep Links, wie weiter auszuführen sein wird.

2. Allgemeine Verantwortlichkeit der Hyperlinksetzer

a) Verantwortlichkeit der Anbieter von Surface Links

Im chinesischen Rechtsrahmen gibt es Privilegierungsregelungen für die Hyperlinksetzer. Obwohl in § 36 Deliktsgesetz der Hyperlinksetzer nicht unmittelbar genannt wird, hat der Gesetzgeber hier schon von dem „Abbruch der Hyperlinks“ gesprochen. Dies trifft auch auf § 7 Abs. 3 der „Interpretation über die Anwendung der Gesetze zu dem Zivilstreit bezüglich des Informationsnetz-Übertragungsrechts“ des Obersten Volksgerichts zu. Zudem wird die Privilegierung der Hyperlinksetzer in § 23 der „Anordnung über den Schutz des Informationsnetz-Übertragungsrechts“ deutlich beschrieben. Dieser Paragraf lautet:

> Wenn der ISP, der den Nutzern Dienste von Suchmaschinen und Hyperlinks bietet, Mitteilung einer Rechtsverletzung von Rechteinhabern erhält, und dann die Hyperlinks der

---

247 Vgl. *Cui Guobin*, Politik und Recht Heft 5, 2014, 74.

248 Vgl. *Yang Yong*, Chinesisches Urheberrecht Heft 1, 2015, 54 ff.

rechtsverletzenden Werke, Aufführungen, Audio- und Videoprodukte abbricht, trägt er keine Entschädigungshaftung. Wenn der ISP die Rechtsverletzung der verlinkten Werke, Aufführungen, Audio- und Videoprodukte kennt oder kennen sollte, soll er die gemeinschaftliche Deliktshaftung tragen.

Für gewöhnlich kann die Verantwortlichkeit der Anbieter der Surface Links nach diesen Regelungen bestimmt werden, diese Hyperlinksetzer sind hiernach grundsätzlich für die verlinkten Inhalte nur verantwortlich, wenn sie schon Kenntnisse von den rechtsverletzenden Informationen besessen haben. In der Literatur wird die Position vertreten, dass die Hyperlinksetzer eine indirekte gemeinschaftliche Deliktshaftung übernehmen könnten, wenn sie nach Kenntniserlangung rechtsverletzender Inhalte noch Hyperlinks setzen.[249]

b) Verantwortlichkeit der Anbieter von Deep Links

Die Verantwortlichkeit der Anbieter der Deep Links ist sehr umstritten. Durch die Deep Links werden die verlinkten Dateien unmittelbar erreicht, während der Nutzer noch auf der vom Hyperlinksetzer angebotenen Webseite bleibt. Bei einigen spezifischen Deep Links ist für die Nutzer nicht erkennbar, dass die verlinkten Inhalte tatsächlich von den ursprünglichen Urhebern stammen.[250] Dabei könnten die Nutzer irrtümlicherweise denken, dass diese Werke von den Hyperlinksetzern angeboten werden. Die zentrale Kontroverse dreht sich um die Frage, ob das Setzen der Deep Links besonders im urheberrechtlichen Bereich zu einer indirekten oder einer direkten Rechtsverletzung gehört. Zu dieser Problematik gibt es zwei kontroverse Kriterien, nämlich das „Serverkriterium“ und das „Nutzerkriterium“.

Nach dem „Serverkriterium“ besteht die Deliktshaftung einer direkten Rechtsverletzung nur, wenn die rechtsverletzenden Dateien auf dem Server der Hyperlinksetzer gespeichert werden. Nach diesem Standard gibt es grundsätzlich nur die Haftung bei indirekter Rechtsverletzung für die Hyperlinksetzer der Deep Links, weil in den meisten Fällen keine verlinkten Dateien auf dem Server der Hyperlinksetzer gespeichert werden, obwohl diese Hyperlinks unmittelbar auf Dateien verweisen. Dieses Kriterium wird gemeinhin akzeptiert.

Erstens stammen die verlinkten Werke von den eigentlichen Urhebern. Vor der Hyperlinksetzung können sie auch durch andere Zugänge erreicht werden. Zudem sind die Hyperlinksetzer nicht in der Lage zu verhindern, dass die Urheber die verlinkten Werke löschen oder ihre Server abschalten. Die Anbieter der Hyperlinks können die verlinkten Inhalte damit nicht steuern.[251] Zweitens entspricht das „Serverkriterium“ dem Willen des Gesetzgebers. Das im chinesischen Urheberrechtsgesetz genannte Übertragungsrecht ins Informationsnetz stammt ursprünglich aus

---

249 Vgl. *Cui Guobin*, Politik und Recht Heft 5, 2014, 75.

250 Vgl. *Rui Yansong*, China Patent & Marke Heft 4, 2009, 81.

251 Vgl. *Wang Qian*, China Invention & Patent Heft 7, 2007, 14 ff.

dem WIPO Copyright Treaty (WCT). Die Formulierung „Angebot des Werks" in beiden Gesetzen bedeutet, dass die Werke noch einmal für die Öffentlichkeit zugänglich gemacht werden müssen. Jedoch wird dieses Ziel durch das bloße Setzen von Deep Links nicht erreicht.[252] Drittens kann eine Interessenabwägung zwischen Hyperlinksetzer und Urheber verwirklicht werden. Weltweit wurde dieses Kriterium von vielen Ländern, in denen es keine subjektive Forderung für die Haftung der direkten Rechtsverletzung gibt, übernommen. Wenn das „Serverkriterium" nicht angewendet werden würde, müssten die meisten Hyperlinksetzer die Haftung bei direkter Rechtsverletzung übernehmen, sodass die Entwicklung der Suchmaschinentechnologie ernsthaft behindert werden würde.[253]

Im Gegensatz dazu besteht eine Deliktshaftung bei direkter Rechtsverletzung nach dem „Serverkriterium", wenn die Nutzer wegen der Existenz der Deep Links glauben, dass die Werke direkt von den Hyperlinksetzern angeboten werden. Auf der einen Seite bedeutet die Formulierung „Angebot des Werks" nicht, dass die Verbreitung oder Übertragung der Werke im Netzwerk eine Kopie und ein Hochladen der Dateien voraussetzt. Durch die Deep Links können die Nutzer die urheberrechtlich geschützten Werke unmittelbar aufrufen. Auf der anderen Seite kann die Urheberrechtsrechtsverletzung mit diesem „Nutzerkriterium" wirksamer verhindert werden, damit die Urheberrechte besser geschützt werden können.[254]

Insgesamt ist das „Serverkriterium" zutreffender und findet mehr Zustimmung. Von vielen Rechtswissenschaftlern wird die Meinung vertreten, das „Serverkriterium" könne als grundlegendes Prinzip für die Unterscheidung zwischen direkter und indirekter Rechtsverletzung herangezogen werden, während es in einigen besonderen Konstellationen bis zu einem gewissen Grad auch modifiziert werden sollte.[255] Darüber hinaus wurde das „Serverkriterium" in dem berühmten *Baidu*-Fall sowie im *Yahoo*-Fall akzeptiert.[256]

Deshalb kann geschlussfolgert werden, dass in der Regel nur eine urheberrechtliche Haftung bei indirekter Rechtsverletzung für die Anbieter der Deep Links besteht. Bei der Haftung bei indirekter Rechtsverletzung können das *safe harbor*-Prinzip und das entsprechende *red flag*-Prinzip noch Anwendung finden.[257] Dieses

---

[252] Vgl. *Wang Qian*, Orientalisches Recht Heft 2, 2009, 13 ff.; *Xie Lanfang/Fu Qiang*, Geistiges Eigentum Heft 11, 2016, 42.

[253] Vgl. *Wang Qian*, ebenda, 15 ff.

[254] Vgl. *Rui Yansong*, China Patent & Marke Heft 4, 2009, 83 ff.; *Cui Guobin*, Politik und Recht Heft 5, 2014, 90.

[255] Vgl. *Xie Lanfang/Fu Qiang*, Geistiges Eigentum Heft 11, 2016, 43 ff.; *Feng Xiaoqing/Han Tingting*, Elektronisches geistiges Eigentum Heft 6, 2016, 46.

[256] Vgl. *Long Jingrong*, Rechtswissenschaftliche Zeitschrift Heft 12, 2014, 131; *Wang Qian*, China Invention & Patent Heft 7, 2007, 15; *ders.*, Orientalisches Recht Heft 2, 2009, 19 ff.

[257] Vgl. *Wang Qian*, Geistiges Eigentum Heft 1, 2006, 17; *ders.*, Geistiges Eigentum Heft 4, 2007, 9 ff.

Verständnis bezieht sich hier deswegen auch auf die Privilegierungsregelungen in § 23 chStGB der „Anordnung über den Schutz des Informationsnetz-Übertragungsrechts“ und § 7 Abs. 3 der „Interpretation über die Anwendung der Gesetze zu dem Zivilstreit bezüglich des Informationsnetz-Übertragungsrechts“. Auf diese Weise kann das Verhältnis zwischen dem Urheberrechtsschutz und der Entwicklung der Technologie von Hyperlinks vernünftig behandelt werden.

3. Strafrechtliche Verantwortlichkeit von Hyperlinksetzern

Die Hyperlinksetzung könnte strafbar sein, wenn die Hyperlinks sich auf rechtswidrige Informationen beziehen. In der Praxis handelt es sich hauptsächlich um Urheberrechtsverletzungen und die Verbreitung pornografischer Inhalte.

a) Strafrechtliche Verantwortlichkeit der Anbieter von Surface Hyperlinks

In der Literatur existieren nur wenige Diskussionen über die strafrechtliche Verantwortlichkeit der Anbieter von Surface Hyperlinks. Zudem gibt es kaum Rechtsprechung, die den ISP wegen Setzen von Surface Hyperlinks auf rechtswidrige Inhalte bestraft.

Obwohl die strafrechtliche Verantwortlichkeit der Hyperlinksetzer im chStGB nicht unmittelbar beschrieben wird, wird sie in einigen Interpretationen des Obersten Volksgerichtshofs miteinbezogen. § 4 der ersten Interpretation über Pornografie im Netzwerk (2004) lautet:

> Wenn man Kenntnis von pornografischen Informationen hat, und direkte Hyperlinks zu diesen Informationen auf der von ihm besessenen, verwalteten oder benutzten Webseite bietet, wird das quantitative Kriterium nach dem Typ der verlinkten pornografischen Informationen bestimmt.

Darüber hinaus wird die strafrechtliche Verantwortlichkeit der ISP auf allgemeine Weise in § 7 der ersten Interpretation über Pornografie im Netzwerk (2004) und § 6 der zweiten Interpretation über Pornografie im Netzwerk (2010) und nach Inkrafttreten des Strafrechtsänderungsgesetzes (IX) auch in den §§ 286 Abs. 1 und 287 Abs. 2 chStGB vorgesehen. Die Hyperlinksetzung kann ohne Zweifel als eine Handlung der Verbreitung gemäß § 384[258] und Vervielfältigung und Veröffentlichung (复制和发行) gemäß § 217[259] betrachtet werden, wenn eine weit gefasste Auslegung angenommen wird, obwohl das Anbieten der Hyperlinks sich von der traditionellen Handlung der Verbreitung pornografischer Inhalte und urheberrechtlichen Rechtsverletzung unterscheidet.[260] Nach dieser Meinung kann die Handlung der Hyperlinksetzer selbstständig als täterschaftliches Handeln verstanden werden.

---

[258] § 384 chStGB: Verbreitung der pornografischen Inhalte.

[259] § 217 chStGB: urheberrechtliche Verletzung.

[260] Vgl. *Yu Zhigang*, Volksstaatsanwaltschaft Heft 12, 2010, 10.

Dagegen wird die Auffassung vertreten, dass das Anbieten indirekter Hyperlinks nicht strafbar sei. Auf der einen Seite komme hier nur die Strafbarkeit der Hyperlinksetzer als Gehilfen in Betracht, weil die Anbieter der Hyperlinks die verlinkten Inhalte nicht kontrollieren. Deswegen könne höchstens von einer Beihilfe gesprochen werden. Auf der anderen Seite könne das Setzen direkter anstatt indirekter Hyperlinks nach § 4 der ersten Interpretation über die Pornografie im Netzwerk (2004) bestraft werden. Folglich sei das bloße Anbieten indirekter Hyperlinks (*Surface Hyperlinks*) nicht strafbar.[261]

Beide Ansichten treffen nicht zu. Nicht alle Anbieter von Surface Links können zu Tätern für die relevanten Tatbestände gemacht werden, weil sie in vielen Konstellationen nicht als die Zentralgestalt des Verbrechens anzusehen sind. Außerdem wäre es auch vorschnell, den Schluss abzuleiten, dass alle Anbieter indirekter Hyperlinks überhaupt nicht bestraft werden dürfen, da einige Hyperlinksetzungen die Voraussetzungen der relevanten Tatbestände eigentlich erfüllen. Hier wäre es besser, eine differenzierte Position einzunehmen: Je nachdem, welche Rolle die Anbieter der Surface Links in ihrer Beteiligung bei den einschlägigen Delikten spielen, können sie sowohl zum Täter als auch zum Teilnehmer werden.

b) Strafrechtliche Verantwortlichkeit der Anbieter von Deep Hyperlinks

In der Literatur gibt es keinen Konsens über die strafrechtliche Verantwortlichkeit der Anbieter der Deep Links. Die theoretische Diskussion konzentriert sich hauptsächlich auf die Rechtsverletzung und die entsprechende strafrechtliche Verantwortung, weil die Deep Links-Technologie im Netz häufig angewendet wird und die Urheberrechte ernsthaft bedroht.

§ 217 chStGB bezieht sich auf die strafrechtliche Verantwortlichkeit bei schwerer Urheberrechtsverletzung. Die Straftat, die die Urheberrechte durch Hyperlinksetzung verletzt, wird zwar nicht unmittelbar in diesem Paragrafen behandelt, aber in einer Interpretation des Obersten Volksgerichtshofs und der Obersten Volksstaatsanwaltschaft konkretisiert. § 11 Abs. 3 der „Interpretation über die Probleme der gesetzlichen Anwendung bezüglich der urheberrechtlichen Verletzung“ lautet: Die Handlung, die durch ein Informationsnetzwerk der Öffentlichkeit Schriftwerke, Musik, Film, Fernsehen, Video, Software und andere Werke zugänglich macht, soll als „Vervielfältigung und Verbreitung“ nach § 217 chStGB angesehen werden.

Bezüglich der strafrechtlichen Verantwortlichkeit der Anbieter der Deep Links existieren jedoch ganz unterschiedliche Deutungen in der Theorie. Kritisch betrachtet, ist die oben angeführte Interpretation verfehlt, denn „Vervielfältigung und Verbreitung“ haben eine spezifische Bedeutung im urheberrechtlichen Bereich. Es handelt sich hier um das Informationsnetz-Übertragungsrecht. Die Verletzung die-

---

[261] Vgl. *Pi Yong*, Volksstaatsanwaltschaft Heft 6, 2005, 21 ff.

ses Rechts setzt ein „Anbieten von Werken" voraus, was nach dem herrschenden „Serverkriterium" beim Setzen von Deep Links besteht.[262] Wie zuvor beschrieben, gibt es in der rechtswissenschaftlichen Theorie und in der Rechtsprechung schon lange den Streit zwischen „Serverkriterium" und „Nutzerkriterium". Wenn die Verantwortlichkeit der Anbieter der Deep Links im zivilrechtlichen Bereich noch umstritten bleibt, sollte im strafrechtlichen Bereich aufgrund des *ultima-ratio*-Prinzips nicht zu weit gegangen werden.[263]

Nach anderer Auffassung können die Verbreitung der rechtswidrigen Inhalte durch Deep Links und die „Vervielfältigung und Verbreitung" in § 217 chStGB trotz ihrer technischen Unterschiede gleichgesetzt werden, weil sie eine gleiche Strafwürdigkeit haben. Durch die Deep Links erreichen die Nutzer die Werke gleichfalls unmittelbar, während deren Urheberrechte ebenfalls schwer verletzt werden.[264] Obwohl die Anbieter der Deep Links den Nutzern nur die Zugänge zu Werken, aber nicht deren Kopien im Internet zur Verfügung stellen, gehört diese Handlung tatsächlich zu der direkten Rechtsverletzung.[265] Deshalb ist diese Interpretation zutreffend und kann auch für das rechtsverletzende Setzen der Deep Links Anwendung finden. Die Einheitlichkeit der Bedeutung der Formulierung „Vervielfältigung und Verbreitung" im urheberrechtlichen und strafrechtlichen Bereich muss beachtet werden. Aufgrund der Forderung, eine Einheit in der Rechtsordnung zu schaffen, muss zunächst geprüft werden, ob das Setzen der Deep Links zur direkten oder indirekten Urheberrechtsverletzung gehört, bevor die strafrechtliche Verantwortlichkeit der Hyperlinksetzer bestimmt werden kann. Wie schon erläutert, ist das „Serverkriterium" für die Unterscheidung zwischen direkter und indirekter Urheberrechtsverletzung im Allgemeinen zutreffender, das Setzen der Deep Links kann in der Regel nur als indirekte Rechtsverletzung betrachtet werden. Deshalb ist nicht sofort unter Berufung auf § 11 Abs. 3 der oben genannten Interpretation zum Schluss zu kommen, dass das Setzen der Deep Links mit der „Vervielfältigung und Verbreitung" in § 217 chStGB gleichgestellt werden kann.[266]

Die Schlussfolgerung, dass das Setzen der Deep Links zu einer indirekten Rechtsverletzung gehört, könnte grundsätzlich nur zu der Strafbarkeit der Beihilfe führen. In der Literatur wird von einigen Rechtswissenschaftlern argumentiert, dass wegen des spezifisch technischen Charakters der Hyperlinks die Teilnehmer hier

---

[262] Vgl. *Wang Yufei*, Urheberrecht in China Heft 4, 2014, 49 ff.

[263] Vgl. *Lin Qinghong/ Zhou Zhou*, Rechtswissenschaft Heft 9, 2013, 157 ff.; *Luo Qiong*, Zeitschrift des Technischen Colleges in Wuhan für Kommunikation Heft 3, 2014, 37 ff.; *Yang Caixia*, Zeitschrift der Nordöstlichen Universität (Sozialwissenschaftliche Ausgabe) Heft 3, 2017, 295 ff.

[264] Vgl. *Wang Guan*, Rechtswissenschaft Heft 9, 2013, 144; *Yan Erpeng/Mei Teng*, Jianghai akademische Zeitschrift Heft 4, 2015, 132.

[265] Vgl. *Xu Songlin*, Geistiges Eigentum Heft 11, 2014, 28 ff.

[266] Vgl. *Yang Caixia*, Zeitschrift der Nordöstlichen Universität (Sozialwissenschaftliche Ausgabe) Heft 3, 2017, 295 ff.

durch juristische Auslegung oder sogar Gesetzgebung als Täter betrachtet werden sollten.[267] Die Vor- und Nachteile des gesetzgeberischen Phänomens der „Teilnehmer zum Täter" (共犯正犯化) sind bereits diskutiert worden. Aber das Prinzip „Teilnehmer zum Täter", das durch eine erweiterte Auslegung des Tatbestands verwirklicht wird, ist nicht haltbar. Obwohl das Setzen von Deep Links die Urheberrechte im Netzwerk eigentlich schwer verletzen könnte, ist dies kein überzeugender und maßgebender Grund für diese Annahme.

Es ist allerdings auch zu berücksichtigen, dass es kein allgemeines Schema für alle Anbieter von Deep Links gibt, es kommt immer auf den konkreten Kontext und die spezifischen Eigenschaften der einzelnen Tatbestände an. Die Täterschaft von Anbietern von Deep Links käme beispielsweise in denjenigen Fällen in Betracht, in denen sie durch ihre Hyperlinks pornografische Informationen verbreiten. Der Grund liegt darin, dass im Gegensatz zu einer Urheberrechtsverletzung die Bedeutung von „Verbreitung pornografischer Inhalte" in § 364 chStGB von der spezifischen Bedeutung dieses Begriffs im urheberrechtlichen Bereich nicht abhängig ist. Die Kernaussage der „Verbreitung pornografischer Inhalte" bedeutet, dass man die pornografischen Inhalte durch die Handlung der Verbreiter erreichen kann. Mit diesem Verständnis kann der Anbieter von Deep Links natürlich auch ein Täter sein.

---

[267] Vgl. *Wang Guan*, Rechtswissenschaft Heft 9, 2013, 147 ff.; *Xu Songlin*, Geistiges Eigentum Heft 11, 2014, 29 ff.; *Yu Zhigang*, Volksstaatsanwaltschaft Heft 12, 2010, 10.

Vierter Teil

Zusammenfassender Vergleich

I. Rechtliche Begriffe der ISP

A. Deutschland

Das deutsche Recht kennt den Begriff der ISP: Nicht nur im TDG, sondern auch im TMG wird eine entsprechende Definition vorgesehen. Obwohl die Definition der ISP (Diensteanbieter) im Gesetz klar dargestellt wird, ist der Umfang der ISP nicht einfach zu bestimmen, weil die Definition zu viele Anbieter miteinschließt. Unter normalen Umständen kann nach dieser Definition entschieden werden, ob der Anbieter zu den ISP gehört und ob das TMG dafür anzuwenden ist. Aber in einigen speziellen Konstellationen muss die Möglichkeit der (analogen) Einordnung weiter analysiert werden. Insgesamt sind der Begriff und die entsprechende Definition der ISP zutreffend, da ein gewisses Maß an Unklarheit in fast jeder Definition existiert. In der Semantik gibt es gar keine Definitionen, die völlig klar und eindeutig sind. Außerdem sind der Begriff und die entsprechende Definition der ISP unter dem Aspekt einer einheitlichen Rechtsordnung zu bejahen, denn sie gelten für alle Rechtsbereiche. Sowohl die zivilrechtliche Haftung als auch die strafrechtliche Verantwortlichkeit der ISP beruhen also auf dem grundlegenden Begriff und der Definition im TMG. Mit dieser Systematik kann der mögliche Wertungswiderspruch zwischen unterschiedlichen Rechtsbereichen vermieden werden.

B. China

Im chinesischen Recht gibt es zwar den Begriff der ISP, aber die entsprechende direkte Definition fehlt. Die Konnotation des Begriffs wird durch die Typen der ISP mittelbar gezeigt. Das erzeugt einige Probleme für dieses Modell: Vor allem ist die Grenze der ISP nach diesem Begriff sehr schwierig zu bestimmen, weil keine direkte Definition für ISP besteht. Wenn ein Provider nicht von den gesetzlichen Typen der ISP erfasst wird, ergibt sich ein theoretischer Streit über seine Einordnung als ISP. Die fehlende Definition führt dazu, dass die Bedeutung der ISP in verschiedenen Rechtsbereichen wie Zivilrecht und Strafrecht unterschiedlich ist. Die mögliche Unvereinbarkeit der Begriffe und Definitionen der ISP könnte in unterschiedlichen Rechtsbereichen widersprüchliche Bewertungen der Verantwortlichkeit der ISP verursachen.

II. Rechtliche Typen der ISP

A. Deutschland

Die Typen der ISP werden in Deutschland im TMG aufgeführt. Nach den §§ 7–10 TMG werden die ISP in vier Typen aufgeteilt, nämlich in Content Provider, Access Provider, Caching Provider und Hosting Provider. Außerdem werden diese Typen durch entsprechende Definitionen in den §§ 7–10 TMG weiter konkretisiert. Die Typisierung wird auch einheitlich und systematisch gestaltet, weil die Regelungen im TMG eine alle Rechtsgebiete umfassende Geltung haben. Darüber hinaus ist festzustellen, dass die Typen der ISP in verschiedenen Schichten des ISO/OSI-Schichtenmodells unterschiedliche Bedeutungen haben. Die Typen der ISP im TMG beziehen sich auf die Dienste, die in den oberen Schichten – etwa der Anwendungsschicht – angeboten werden und sich mit den inhaltlichen, nicht mit den technischen Aspekten befassen. Die Telekommunikationsdienste, die sich hingegen auf den technischen Aspekt konzentrieren, fallen unter das TKG.

Jedoch bestehen noch einige Unklarheiten für die Typisierung der ISP, beispielsweise ist die Frage, wie die unter § 8 TMG fallende Zwischenspeicherung und die von § 9 TMG berührte Zwischenspeicherung voneinander zu unterscheiden sind, bis heute umstritten. Obwohl es in der Literatur viele Lösungsvorschläge dazu gibt, scheint keiner ganz zutreffend zu sein. Außerdem bleibt im deutschen Recht noch offen, wie die gesetzlich nicht geregelten ISP einzuordnen sind. Anders als der DMCA in den USA erfasst das TMG die Suchmaschinenbetreiber und die Hyperlinksetzer nicht, obwohl gerade sie im Cyberspace eine so wichtige Rolle spielen, dass ihre Verantwortlichkeit zu einem der zentralen Probleme der ISP gehört. In Literatur und Rechtsprechung wird heftig diskutiert, ob die Privilegierungsregelungen für ISP im TMG analog für die Verantwortlichkeit der Suchmaschinenbetreiber und Hyperlinksetzer angewendet werden können. Obwohl es viele plausible theoretische Lösungen gibt, lässt sich die Unsicherheit der Einordnung, die durch die Gesetzeslücke verursacht wird, nicht übersehen.

B. China

Die Typen der ISP werden auch in den chinesischen Gesetzen deutlich ausformuliert. Es gibt detaillierte Beschreibungen für Content Provider, Access Provider, Caching Provider sowie Hosting Provider. Im Gegensatz zum TMG sind die Suchmaschinenbetreiber und Hyperlinksetzer neben den genannten Typen im chinesischen Gesetz als selbstständige Kategorien festgelegt. Im Allgemeinen ist diese Typisierung aber auch nicht zufriedenstellend.

Vor allem sind die Typen der ISP in den unterschiedlichen Gesetzen miteinander nicht vereinbar. Wie schon erläutert, existieren viele Gesetze, Verordnungen und Vorschriften in China, die diese Typen der ISP beschreiben, während ein einheit-

liches Kriterium bei dieser Problematik fehlt. Zum Beispiel stimmen die Typen der ISP in der „Anordnung über die technischen Maßnahmen der Internetsicherheit“ des Ministeriums für öffentliche Sicherheit nicht mit denen in der „Anordnung über den Schutz des Informationsnetz-Übertragungsrechts“ des Staatsrats überein. Im Deliktsgesetz und im Strafgesetzbuch gibt es den Begriff der ISP und Regelungen für ihre Verantwortlichkeit, aber die Typisierung der ISP fehlt in beiden.

Darüber hinaus wird im chinesischen Rechtswesen nicht erkannt, dass nicht alle Typen der ISP in unterschiedlichen Schichten des ISO/OSI-Schichtenmodells Anwendung finden können. So werden die Access Provider, die sich nur auf technische und physische Internetdienste in den niedrigen Schichten beziehen, auch in der „Anordnung über die technischen Maßnahmen der Internetsicherheit“ berücksichtigt. Schließlich haben die Wissenschaftler in der Theorie auf die Typisierung der ISP keinen großen Wert gelegt. Besonders im strafrechtlichen Bereich wird dieses Problem offensichtlich. Die Einführung der bislang im chStGB fehlenden Typisierung der ISP in die Rechtstheorie würde dieses Defizit abdecken. Leider wird dieses Thema aber in der Literatur nicht ausreichend diskutiert.

III. Internetspezifische Privilegien der ISP

A. Deutschland

In Deutschland werden die Privilegien der ISP in den §§ 7–10 TMG verdeutlicht, unter bestimmten Voraussetzungen sind Access Provider, Caching Provider und Hosting Provider für fremde Informationen nicht verantwortlich. Da das TMG fast alle Rechtsgebiete abdeckt, haben die Privilegien der ISP im TMG eine allgemeine Geltung. Deshalb besteht ein zweistufiges Modell in der Auslegung der spezifischen Gesetze. In der Literatur gibt es unterschiedliche Lösungsansätze für die Auslegung dieser gesetzlichen Struktur, nämlich die „Vorfilterlösung“ und die „Integrationslösung“. Dieses Modell hat zwei grundlegende Funktionen. Zum einen hat die vorgelagerte Prüfung von Privilegien des TMG die Typisierung der ISP, die der Verantwortlichkeit der ISP in anderen spezifischen Gesetzen zugrunde liegt, vorher realisiert. Zum anderen spielt das vorgelagerte TMG eine einschränkende Rolle. Mit dem zweistufigen Modell kann die Haftung der ISP innerhalb einer angemessenen Grenze bestimmt werden.

Im Allgemeinen ist zu schlussfolgern, dass das System der Privilegien von ISP in Deutschland eine die Verantwortlichkeit beschränkende Tendenz aufweist, die schon in dem oben genannten zweistufigen Modell angedeutet wird. Auch § 7 TMG verdeutlicht sie, indem die ISP keine allgemeine Verpflichtung zur Überwachung und Überprüfung der übermittelten oder gespeicherten Informationen übernehmen. Das

zugrunde liegende Ziel dieses Konstrukts liegt in der Balance zwischen der Förderung der Entwicklung der Dienste im Internet und der Wahrung der Sicherheit im Cyberspace. Trotzdem existieren in diesem System der Privilegierung auch einige Unklarheiten. So bleibt etwa die Verpflichtung der ISP zur Entfernung oder Sperrung von Informationen nach den allgemeinen Gesetzen unberührt, obwohl die allgemeine Verpflichtung zur Überwachung und Überprüfung der Informationen verneint wird. In welchem Umfang die ISP dazu verpflichtet sind, bleibt nach den allgemeinen Gesetzen unbestimmt, sodass die Grenze der sogenannten Störerhaftung der ISP auch in Literatur und Rechtsprechung heftig diskutiert wird.

Im Übrigen hat die Ungewissheit in der subjektiven Voraussetzung für die Privilegien der ISP viele Kontroversen verursacht. Über die Frage, ob die Privilegierung der Access Provider beeinflusst wird, wenn sie schon Kenntnis von rechtswidrigen Informationen haben und nicht unverzüglich entsprechende Maßnahmen ergreifen, wird auch in der Literatur ausführlich debattiert. Das konkrete Verständnis der Kenntnis der Hosting Provider über rechtswidrige Handlungen oder Informationen ist ebenfalls ein sehr umstrittenes Thema. Daneben gibt es auch keine einheitliche Lösung für die analoge Anwendung des TMG bezüglich der Privilegien der gesetzlich nicht geregelten ISP (etwa Peer-to-Peer-Netzwerktreiber und Hyperlinksetzer).

Außerdem hat der Gesetzgeber die Verantwortlichkeit der gesetzlich nicht geregelten ISP nicht vorgesehen, weil die relevante Technologie sich immer schneller entwickelt. Obendrein gibt es oft viele unterschiedliche Arten von Internetservices, sodass eine allgemeine und einheitliche Bewertung unmöglich ist. Aus diesen Gründen bleibt diese Problematik bis heute nicht nur in der Praxis, sondern auch in der Theorie umstritten. Allerdings sind Internetdienste wie Peer-to-Peer-Technologie und Hyperlinks im Cyberspace schon so weit verbreitet, dass sie unentbehrliche Bestandteile des alltäglichen Lebens sind. Deswegen wäre es besser, die nicht geregelten ISP in die Gesetzgebung aufzunehmen.

Schließlich hat auch das stark kritisierte NetzDG die Frage nach der Verantwortlichkeit der ISP aufgeworfen. Nach dem neu erlassenen Gesetz müssen die Anbieter der großen sozialen Netzwerke eine Reihe von Verpflichtungen übernehmen, welche allerdings im TMG so nicht vorgesehen werden. Wenn diese Verpflichtungen nicht erfüllt werden, müssen Telemediendiensteanbieter mit einer Geldbuße von bis zu fünf Millionen Euro rechnen. Obwohl der grundlegende Standpunkt des TMG zur Einschränkung der Verantwortlichkeit von ISP durch die Einführung des neuen NetzDG nicht verändert wurde, ist zuzugeben, dass die konkreten Verpflichtungen sowie die Haftung der ISP offensichtlich verschärft worden sind. Deshalb steht das NetzDG bezüglich der Verantwortlichkeit der ISP in gewissem Maß mit dem TMG sowie den ECRL nicht in Einklang. Folglich sind die Aussichten für die Verantwortlichkeit der ISP nicht mehr klar. Die Konsequenzen dieses neuen Gesetzes bleiben abzuwarten.

B. China

In China hat der Gesetzgeber die Privilegien der ISP in den Gesetzen vorgesehen. Durch eine vergleichende Analyse kann festgestellt werden, dass die Privilegierungsregelungen in China vom US-amerikanischen DMCA stark beeinflusst wurden, weshalb sich die Privilegien nicht nur auf Access Provider, Caching Provider und Hosting Provider, sondern auch auf Suchmaschinenbetreiber und Hyperlinksetzer beziehen. Allgemein gesagt, dienen die Privilegierungsregelungen dazu, die Verantwortlichkeit der ISP einzuschränken, um die Entwicklung der Informationsindustrie nicht zu behindern. Dieses Prinzip wird durch eine Reihe von Gesetzen, Verordnungen und Interpretationen verkörpert.

Der chinesische Rechtsrahmen weist aber auch einige Mängel auf. Das erste Problem liegt in der fehlenden Systematik und Einheitlichkeit der unterschiedlichen Normen bezüglich der Verpflichtung und Privilegierung der ISP. In den zivilrechtlichen Gesetzen gibt es viele Unvereinbarkeiten. Auf der einen Seite stimmen die Privilegierungsregelungen der ISP in der „Verordnung über den Schutz des Informationsnetz-Übertragungsrechts“ (§§ 20–23) nicht mit den Regelungen im Deliktsgesetz (§ 36) überein. Die Privilegien der §§ 20–23 der Verordnung setzen die Typisierung der ISP voraus, das heißt, die Privilegien der Access Provider, Caching Provider, Hosting Provider werden jeweilig bestimmt. Im Gegensatz dazu werden die Regelungen des § 36 Deliktsgesetz auf eine allgemeine Weise dargestellt.

Dieses Modell hat viele Rechtsunsicherheiten zur Folge, weil die verschiedenen ISP unterschiedliche Bedingungen für die Privilegierung haben. Auf der anderen Seite gelten die ersteren nur für das Informationsnetz-Übertragungsrecht. Sie haben im Zivilrecht keinen umfassenden Geltungsbereich. Allerdings haben die letzteren eine allgemeine Geltung für die ganze Rechtsverletzung im zivilrechtlichen Bereich. Dies führt zu Unklarheiten über die Harmonisierung zwischen den beiden Privilegierungsregelungen.

Neben den Privilegierungsregelungen gibt es auch viele andere Paragrafen, die eine allgemeine und aktive Verpflichtung für die ISP vorsehen. Diese Paragrafen zeigen, dass der Gesetzgeber eine relativ strenge Position gegenüber den ISP vertritt. Jedoch steht dies bis zu einem gewissen Grad der allgemein anerkannten Privilegierung der ISP entgegen, denn es wird weithin akzeptiert, dass die ISP aus vielen Gründen nur eine beschränkte Haftung für die Inhalte von Dritten übernehmen sollen. Die chinesischen Regelungen scheinen allerdings eine Tendenz zu einer erweiterten Verpflichtung zu reflektieren. Wenn man sich bei der Bestimmung der strafrechtlichen Garantenstellung auf diese Paragrafen beruft, fällt der Umfang der strafrechtlichen Verantwortlichkeit der ISP auch sehr weit aus.

Des Weiteren gibt es noch viele Unbestimmtheiten über die konkreten Voraussetzungen für die Privilegien der ISP. Ein typisches Beispiel ist die Auslegung des „Wissens“ in § 36 des Deliktsgesetzes. Es ist äußerst umstritten, ob das „Kennen-

müssen“ im „Wissens“-Begriff inkludiert ist. Unterschiedliche Auslegungen dazu würden zu einer ganz anderen Verantwortlichkeit der ISP führen. Deshalb ist es notwendig, dieses Problem durch die Gesetzgebung zu lösen.

Schließlich beschränken sich die chinesischen Privilegierungsregelungen nur auf den zivilrechtlichen Bereich. Im strafrechtlichen Sektor wird die Möglichkeit der Aufnahme dieser Privilegien nicht ausreichend diskutiert, was dazu führen könnte, dass die strafrechtliche Verantwortlichkeit der ISP unangemessen erweitert wird.

IV. Allgemeine strafrechtliche Verantwortlichkeit der ISP

A. Deutschland

Im deutschen Rechtsrahmen spielt das TMG eine sehr wichtige Rolle für die Bestimmung der strafrechtlichen Verantwortlichkeit der ISP. Nach Meinung des Gesetzgebers funktionieren die Haftungsregelungen wie ein Vorfilter, was aber in der Literatur auch auf Kritik stößt. Obwohl es unterschiedliche Ansichten zu der Beziehung zwischen den strafrechtlichen Tatbeständen und den Privilegierungsregelungen im TMG gibt, wird immerhin allgemein anerkannt, dass eine Prüfung nach den Privilegierungsregelungen im TMG die Voraussetzung für die Bestimmung der strafrechtlichen Verantwortlichkeit der ISP ist.

Außerdem werden die Haftungsregelungen des TMG in der Auslegung der konkreten Tatbestände tatsächlich auch als beschränkende Gründe zitiert. Da beispielsweise die allgemeine Verpflichtung der ISP zur Überwachung und Nachforschung nach § 7 TMG ausgeschlossen wird, kann die strafrechtliche Garantenstellung der ISP nur ausnahmsweise begründet werden, wenn die ISP konkrete Kenntnis von rechtswidrigen Informationen haben und tatsächlich über technische Kontrollmöglichkeiten verfügen. Aus dem gleichen Grund wird der bedingte Vorsatz für die Begründung der strafrechtlichen Verantwortlichkeit auch verneint.

In Deutschland gibt es keinen speziellen Paragrafen für die strafrechtliche Verantwortlichkeit der ISP. Deshalb ist die Bestimmung ihrer strafrechtrechtlichen Verantwortlichkeit von der Anwendung der traditionellen Straftatbestände, besonders der sogenannten Äußerungs- und Verbreitungsdelikte, abhängig. In diesem Rahmen wird die strafrechtliche Verantwortlichkeit der ISP auch nach den traditionellen allgemeinen Verbrechenslehren – etwa der Theorie von Unterlassung oder Beteiligung – ermittelt.

Es ist besonders bemerkenswert, dass in der Literatur der sozial nützliche Charakter der Internetdienste der ISP in der strafrechtlichen Bewertung Beachtung findet, obwohl deren Handlungen von Nutzern zur Begehung von Verbrechen missbraucht werden können. Die Handlungen der ISP werden aus diesem Grund in der

Regel als Unterlassen und nicht als aktives Tun interpretiert. Außerdem werden die technischen Eigenschaften der ISP bei der Prüfung der strafrechtlichen Verantwortung auch in Betracht gezogen: Beispielsweise sind die ISP grundsätzlich nur als Teilnehmer einzustufen, weil sie die rechtswidrigen Inhalte wegen ihrer technisch beschränkten Möglichkeiten nicht zu kontrollieren vermögen. Die Auslegung zur strafrechtlichen Verantwortung der ISP beschränkt sich nicht nur auf die wörtliche Interpretation der Straftatbestände. Im Gegensatz zum Wortlaut werden viele normative Elemente hier in Erwägung gezogen.

Grundsätzlich ist festzuhalten, dass der gesetzliche Rahmen für die strafrechtliche Verantwortlichkeit der ISP in Deutschland zu Einschränkungen tendiert. Obwohl es viele gegensätzliche Auffassungen in der theoretischen Diskussion über dieses Thema gibt, wird von der herrschenden Meinung eine die Haftung der ISP beschränkende Ansicht vertreten.

B. China

Im Gegensatz zu Deutschland gibt es in China kein einheitliches Gesetz wie das TMG, das sich auf die Verantwortlichkeit der ISP spezialisiert und einen umfassenden Geltungsbereich hat. Die Privilegierungsregelungen der ISP stammen hauptsächlich aus den zivilrechtlichen Normen. Ob und wie diese Privilegierungsregelungen im strafrechtlichen Bereich angewendet werden können, wird in der Literatur nicht ausreichend diskutiert.

Folglich fehlt es der strafrechtlichen Verantwortlichkeit an Privilegierung. Einerseits könnte die strafrechtliche Verantwortlichkeit der ISP dadurch unverhältnismäßig erweitert werden, was für die Entwicklung der Informationsindustrie einer Katastrophe gleichkäme. Andererseits steht die erweiterte strafrechtliche Verantwortlichkeit der ISP mit der Forderung nach der Einheit der Rechtsordnung nicht im Einklang, was zu der widersprüchlichen Folgerung führen könnte, dass eine Handlung der ISP im zivilrechtlichen Bereich privilegiert, aber im strafrechtlichen Bereich bestraft wird. Obwohl dieser Widerspruch durch eine theoretische Lösung aufgehoben werden kann, ist es unbedingt erforderlich, dieses strukturelle Problem auch durch die Gesetzgebung zu lösen.

Es fällt auf, dass im Gegensatz zum deutschen Rechtsrahmen im chStGB spezielle Paragrafen für die strafrechtliche Verantwortlichkeit der ISP vorgesehen werden. Vor dem Inkrafttreten des Strafrechtsänderungsgesetzes (IX) 2015 bestanden schon zwei Interpretationen, in denen die ISP nach den §§ 363 Abs. 1 und 364 Abs. 1 chStGB als Teilnehmer oder sogar Täter bestraft wurden, wenn sie bestimmten Straftätern im Cyberspace Internetdienste als Hilfsmittel zur Verfügung stellten. Danach erließ der Gesetzgeber durch das Strafrechtsänderungsgesetz eine Reihe von neuen Straftatbeständen, die sich direkt oder indirekt auf die strafrechtliche Verantwortlichkeit der ISP beziehen, nämlich § 286 Abs. 1 chStGB (Verweige-

rung der Erfüllung der Sicherheitsverpflichtungen im Informationsnetzwerk), § 287 Abs. 1 chStGB (illegale Nutzung von Informationsnetzwerken) und § 287 Abs. 2 chStGB (Hilfe für Informationen und Cyberkriminalität).

Die oben genannten Regelungen zeigen eine gesetzgeberische Tendenz, die sich von der deutschen unterscheidet. Auf der einen Seite ist noch nicht erkennbar, dass die Privilegien der ISP von den weltweit anerkannten Grundsätzen in den neuen Straftatbeständen Berücksichtigung finden.[1] Deshalb bleibt die Frage nach wie vor offen, wie die allgemeinen Privilegien der ISP mit der strafrechtlichen Verantwortlichkeit der ISP kombiniert werden können. Im Gegensatz dazu werden die Sicherheitsverpflichtungen im Informationsnetzwerk ausdrücklich in § 286 Abs. 1 chStGB angesprochen. Allerdings sind die Inhalte dieser Sicherheitsverpflichtungen so vage, dass es viele theoretische Streitpunkte sowie Kritik daran in der Literatur gibt. Dies könnte nicht nur zu Rechtsunsicherheit, sondern auch zu einer erweiterten Haftung für die ISP führen.

Auf der anderen Seite sollen die ISP nach den neuen speziellen Tatbeständen (§§ 286 Abs. 1, 287 Abs. 2 chStGB) als Täter und nicht als Teilnehmer behandelt werden. Im Allgemeinen bedeutet diese gesetzliche Veränderung eine schwerere strafrechtliche Bewertung für die Handlung der ISP, weil der Täter sich im Vergleich zum Teilnehmer in höherem Maße sozialschädlich verhält.[2]

Außerdem können die Voraussetzungen für die Strafbarkeit der ISP mit dieser gesetzlichen Veränderung leichter erfüllt werden. Vor dem Strafrechtsänderungsgesetz (IX) wurden die ISP oft als Teilnehmer bestraft, da sie in den meisten Fällen den unmittelbaren Straftätern mit Internetdiensten halfen, anstatt die Straftatbestände direkt zu verwirklichen. In dieser Situation war die Strafbarkeit der ISP von derjenigen der Täter abhängig, während viele Voraussetzungen für die Beteiligung nach dem chinesischen StGB – wie etwa der gemeinschaftliche Vorsatz[3] und die gemeinschaftliche Handlung – erfüllt werden mussten.

Wie schon erläutert, waren diese Voraussetzungen im Netzwerk wegen der Entfremdung der Beteiligung der ISP oft schwierig nachzuweisen. Nach dem Inkrafttreten des Strafrechtsänderungsgesetzes (IX) gibt es spezielle Straftatbestände für die strafrechtliche Verantwortlichkeit der ISP. Das heißt, der Gesetzgeber hat die

---

[1] Aber wenn man diese Paragrafen sorgfältig liest, kann man auch einige mittelbare Spuren für diese Privilegierung finden. Zum Beispiel setzt die Strafbarkeit der ISP nach § 286 Abs. 1 chStGB das Erfordernis der Korrekturmaßnahmen von Regulierungsbehörden voraus. Nach § 287 Abs. 2 chStGB wird die Kenntnis des Angeklagten als eine Voraussetzung für die Strafbarkeit betrachtet.

[2] Vgl. *Kern*, ZStW 64, 1952, 281 ff.

[3] Nach § 25 des chinesischen StGB setzt die Begründung der Beteiligung einen gemeinschaftlichen Vorsatz der Beteiligten voraus. Nach dem deutschen StGB muss der Haupttäter von der Hilfeleistung keine Kenntnis haben. Das heißt, eine heimliche Beihilfe ist auch möglich. Vgl. *Rengier*, AT, § 45, Rn. 83.

Akzessorietät der Teilnahme von Hindernissen befreit, damit die Bestrafung der ISP in Theorie und Praxis reibungsloser erfolgen kann.

Mit der umfassenden Entwicklung der Informationsgesellschaft wird die traditionelle Beteiligungstheorie mit vielen Herausforderungen konfrontiert. Wenn Cyberkriminalität fast industriell betrieben wird, wird auch die Arbeitsteilung der Straftäter perfektioniert und immer detaillierter. Verbrechen im Netz zu begehen ist aufgrund dieser Veränderung nicht mehr so von der engen Zusammenarbeit und direkten Kommunikation der Straftäter untereinander abhängig. Indem jeder Straftäter sich nur mit einem Segment eines Verbrechens selbstständig befasst und mit anderen Teilnehmern nicht unmittelbar kommuniziert, kann in der Summe ein Verbrechen begangen werden, sodass die grundlegenden Rechtsgüter der Gesellschaft schwer verletzt werden.

Natürlich können die selbstständigen Straftatbestände in diesem Sinne eine positive Rolle zur Behandlung der oben genannten Schwierigkeiten spielen. Jedoch ist die Legitimität dieser Straftatbestände in der Literatur umstritten, weil das dazu führen könnte, dass die ISP zu viele strafrechtliche Risiken auf sich nehmen. Bei einem so hohen Risiko wird die normale Entwicklung der Informationsindustrie behindert und die Informationsfreiheit der Bürger beeinträchtigt.

Diese Gefahr lässt sich meines Erachtens durch eine einschränkende theoretische Struktur reduzieren. Obwohl der gesamte strafrechtliche Rechtsrahmen erweitert zu sein scheint, ist es durchaus möglich, die strafrechtliche Verantwortlichkeit der ISP durch eine dogmatische Theorie einzuschränken. Dies ist auch genau die Aufgabe des Rechtswissenschaftlers. Vor allem müssen die allgemeinen Privilegien der ISP in den strafrechtlichen Bereich aufgenommen werden. Im zivilrechtlichen Bereich haben die Rechtswissenschaftler die Privilegierung der ISP wirklich ausführlich diskutiert, sodass eine relativ haftungseinschränkende Position schon zum grundlegenden Konsens geworden ist. Da in dem strafrechtlichen Bereich noch kein großer Wert auf diese Ergebnisse gelegt wird, ist es notwendig, diese Resultate in Übereinstimmung mit den besonderen Anforderungen des Strafrechts umzusetzen. Darüber hinaus ist eine teleologisch beschränkende Auslegung für die neuen Straftatbestände unentbehrlich: Beispielsweise sollten die „Sicherheitsverpflichtungen im Informationsnetzwerk“ in § 286 Abs. 1 StGB nicht nur nach dem Wortlaut interpretiert werden. Die Hilfeleistung im § 287 Abs. 2 StGB darf ebensowenig nur formal ausgelegt werden. Zu diesen Straftatbeständen braucht es eine materiale Auslegung, um die strafrechtliche Haftung der ISP zu beschränken.

Neben der speziellen Gesetzgebung ist die theoretische Diskussion über die Verantwortlichkeit der ISP in China bemerkenswert. In der Literatur wird der sozial nützliche Charakter der Internetdienste der ISP respektiert, viele Rechtswissenschaftler haben deshalb großen Wert auf die Theorie der neutralen Handlung, die eine wichtige Rolle für die Beschränkung der Haftung spielt, gelegt. Natürlich ist diese Theorie in dem chinesischen Kontext für die Beschränkung der Verantwort-

lichkeit der ISP von Bedeutung, weil der chinesische Rechtsrahmen im Allgemeinen zur erweiterten Haftung der ISP tendiert. Jedoch ist auch zu beachten, dass die neutrale Handlung für die Bestimmung der Verantwortlichkeit der ISP nicht missbraucht werden darf, denn in bestimmten Konstellationen haben die ISP tatsächlich keine sogenannte neutrale Eigenschaft. Wenn zum Beispiel die Hosting Provider schon konkrete Kenntnis von rechtswidrigen Inhalten besitzen, sind sie nach dem allgemein anerkannten Grundsatz verpflichtet, die illegalen Inhalte zu löschen. Die Theorie der neutralen Handlung kann folglich nicht auf eine allgemeine Weise für die Bestimmung der strafrechtlichen Verantwortlichkeit der ISP angewendet werden.

Ein weiteres Problem liegt darin, dass die technischen Eigenschaften der ISP nicht ausführlich analysiert werden, der innere technische Mechanismus der ISP sowie der Informationstechnologie wird nicht genug verdeutlicht. Manchmal entstehen sogar Missverständnisse aus dieser Problematik, wie dies schon bei der Unterscheidung zwischen aktivem Tun und Unterlassen bezüglich des Angebots der Zwischenspeicherung veranschaulicht worden ist.

Alles in allem ist das chinesische Strafrecht von der Tendenz, die Haftung der ISP zu erweitern, geprägt, während viele Rechtswissenschaftler hingegen sich bemühen, die strafrechtliche Verantwortlichkeit der ISP durch theoretische Auslegung der Tatbestände zu beschränken.

V. Allgemeine kriminalpolitische Bewertung

Die Verantwortlichkeit der ISP stellt die Wissenschaftler vor ein Dilemma. Einerseits ist es angesichts der stark steigenden Cyberkriminalität dringend geboten, wirksame rechtliche Maßnahmen zu ergreifen. Im Cyberspace spielen die ISP eine sehr wichtige Rolle, weil das Internet ohne ihre Dienste nicht funktionieren kann. Aufgrund ihrer entscheidenden Position werden die ISP damit oft als *Gatekeeper* betrachtet,[4] ein sicherer Cyberspace ist demnach ohne die Zusammenarbeit der ISP unmöglich.

Dies erfordert, dass sie unter bestimmten Bedingungen Verpflichtungen sowie Haftung übernehmen. Außerdem ist es aus der Perspektive des Gesetzgebers praktischer, die ISP anstelle der Internetnutzer gesetzlich zu regulieren, weil die zahlreichen Internetnutzer über die ganze Welt verteilt und damit schwierig zu verfolgen sind. Andererseits brauchen die ISP auch ausreichende Freiheiten, um ihre Geschäfte zu betreiben. Wenn die ISP sich aktiv an der Überprüfung der Inhalte der übermittelten Informationen ihrer Nutzer beteiligen müssten, würden sie unverhältnismäßig schwer belastet. Die Weiterentwicklung der Informationsindustrie würde ohne diese Freiheiten behindert werden, weil die Motivation zur technischen Inno-

---

[4] Vgl. *Sieber*, Straftaten und Strafverfolgung im Internet, C 61.

vation dadurch beeinträchtigt wäre. Darüber hinaus könnten Eingriffe in die Informationsfreiheit sowie in die Privatsphäre die Folge sein. Angesichts dieses Dilemmas sollte man sich bemühen, ein akzeptables Gleichgewicht zwischen der Informationsfreiheit und der Sicherheit im Cyberspace herzustellen. Diese Arbeit hat dargelegt, dass sich die Ausführungen zur Verantwortlichkeit der ISP im chinesischen und im deutschen Rechtsrahmen deutlich unterscheiden.

Im deutschen Rechtskontext wird die Privilegierung der ISP betont. Trotz einiger bestehender Unklarheiten wird die Freiheit der ISP im Allgemeinen ernst genommen. Jedoch gibt es auch bei diesem Modell die Möglichkeit, dass bestimmte Konstellationen der Cyberkriminalität durch rechtliche Mittel nicht wirksam bekämpft werden. Ein Beispiel dafür ist die zunehmende Verbreitung von Hasskriminalität und anderen strafbaren Inhalten im Internet. In Anbetracht dessen wurde vom Gesetzgeber das umstrittene NetzDG verabschiedet, um die Hasskriminalität effektiver zu bekämpfen. Allerdings wird das NetzDG von vielen Juristen sowie Internetnutzern stark kritisiert, weil es eine Reihe von Problemen – etwa die Beeinträchtigung der Meinungsfreiheit – dadurch verursacht, dass die Anbieter der sozialen Netzwerke mehrere Verpflichtungen zusätzlich übernehmen müssen. Obwohl die neue gesetzgeberische Tendenz einige Unsicherheiten zur Folge hat, bleibt allerdings die im TMG (sowie TDG a.F.) festgestellte Rechtspolitik, dass zugunsten der dynamischen Entwicklung der Informations- und Kommunikationsdienste die Verantwortlichkeit der ISP durch ein abgestuftes System eingeschränkt werden sollte,[5] im Allgemeinen unverändert.

Im Gegensatz zu Deutschland fehlen den Haftungsregelungen der ISP im chinesischen Rechtsrahmen vor allem Einheitlichkeit und Systematik. Außerdem wird die Privilegierung der ISP im strafrechtlichen Bereich wegen der speziellen Beachtung der Sicherheit im Internet nicht ausreichend akzentuiert, obwohl die Verantwortlichkeit der ISP im chinesischen Zivilrecht ähnlich wie im deutschen geregelt ist. Ein direkter Grund für diese gesetzgeberische Veränderung liegt darin, dass die Cyberkriminalität in China immer mehr zunimmt. Nach einer Aussage des ehemaligen Ministers für öffentliche Sicherheit macht der Anteil der Cyberkriminalität in China heutzutage fast ein Drittel aller Verbrechen aus. Die Cyberkriminalitätsrate ist um rund 30 % pro Jahr gestiegen.[6] Diese dramatische Entwicklung führt zu einer sogenannten aktiven strafrechtlichen Gesetzgebung. In der Literatur wird dies so eingeschätzt, dass die neuen Straftatbestände über die Verantwortlichkeit der ISP einer notwendigen Vorverlagerung der Bestrafung entsprechen.[7]

---

[5] Vgl. BT-Drs. 13/7385, S. 1; BT-Drs. 14/6098, S. 22.

[6] Die zunehmende Cyberkriminalität in China, abrufbar unter http://www.thepaper.cn/newsDetail_forward_1547385 [Stand: 15.09.2017].

[7] Vgl. *Zhou Guangquan*, Chinesische Rechtszeitschrift Heft 4, 2016, 30.

In Deutschland stimmt die Situation der Cyberkriminalität auch nicht optimistisch. Nach einer Statistik des Bundeskriminalamts ist die Computerkriminalität von 70.068 Fällen im Jahr 2015 auf 107.751 Fälle im Jahr 2016 gestiegen. Es wird besonders darauf hingewiesen, dass bezüglich der Kriminalität im Bereich der Informations- und Kommunikationstechnik (IuK-Kriminalität) im engeren Sinne insgesamt 82.649 Fälle im Jahr 2016 registriert wurden, während es nur 45.793 registrierte Fälle im Jahr 2015 gab. Es ist auch auffällig, dass die Aufklärungsquote für Computer- und IuK-Kriminalität sehr niedrig ist (jeweils mit 33.8 % und 32.8 %).[8] Diese Zahlen belegen, dass die Netzwerksicherheit sich auch in Deutschland drastisch verschlechtert hat.

Angesichts dieser ernsten Lage hat der chinesische Gesetzgeber im Vergleich zu dem deutschen eine wesentlich aktivere Rolle eingenommen, obwohl ein neues, die Verpflichtung der ISP verstärkendes Gesetz auch in Deutschland erlassen worden ist. Wie effektiv diese Paragrafen im chStGB sind und welche weiteren Auswirkungen sie in Zukunft haben werden, bleibt abzuwarten. Jedoch sollte auch nicht vergessen werden, dass ein erweiterter strafrechtlicher Rahmen im Einzelfall nicht unbedingt zu strengerer Haftung führt, denn in dem Rechtsrahmen kann die teleologische Auslegung in der gesetzlichen Anwendung eine wichtige Rolle spielen. In diesem Sinn ist eine vergleichende Untersuchung zwischen Deutschland und China von großer Bedeutung: Das deutsche Modell bietet chinesischen Juristen ein Muster, wie ein systematisches und einheitliches Privilegierungssystem für die ISP zu konstruieren ist, wohingegen das chinesische Modell deutschen Juristen eine neue Möglichkeit aufzeigt, wie die grassierende Cyberkriminalität mit einer relativ aktiven Gesetzgebung zu bekämpfen ist.

---

[8] Vgl. Bericht zur Polizeilichen Kriminalstatistik 2016, S. 9, 15.

Literaturverzeichnis

Abel, Horst G., Praxiskommentare Telemediengesetz, Telekommunikationsgesetz und Telekommunikations-Überwachungsverordnung. Kissing 2007.

Altenhain, Karsten, Die gebilligte Verbreitung mißbilligter Inhalte – Auslegung und Kritik des § 5 TDG. AfP Heft 29, 1998, 457–464.

– Die strafrechtliche Verantwortung für die Verbreitung missbilligter Inhalte in Computernetzen. CR Heft 8, 1997, 485–496.

– Jugendschutz (Teil 20), in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, 2014.

Armbrust, Michael etc., A View of Cloud Computing. CACM Vol. 53, Issue 4, 2010, 50–58.

Asada, Kazushige, Strafwürdigkeit als strafrechtliche Systemkategorie. ZStW 97 Heft 2, 1985, 193–207.

Baumann, Jürgen/Weber, Ulrich/Mitsch, Wolfgang/Eisele, Jörg, Strafrecht. Allgemeiner Teil. Lehrbuch. 12. Aufl. Bielefeld 2016.

Bericht über die Nutzer der WeChat, abrufbar unter http://www.sohu.com/a/136382735_184641 [Stand: 15.09.2017].

Bettinger Torsten/Freytag Stefan, Privatrechtliche Verantwortlichkeit für Links, zugleich Anmerkung zum Urteil des LG Hamburg vom 12.05.1998. CR Heft 9, 1998, 545–556.

Bleisteiner, Stephan, Rechtliche Verantwortlichkeit im Internet, unter besonderer Berücksichtigung des Teledienstegesetzes und des Mediendienste-Staatsvertrags. Köln 1999.

Bode, Thomas, Das Providerprivileg aus §§ 7, 10 TMG als gesetzliche Regelung der Beihilfe durch „neutrale" Handlungen. ZStW 127, Heft 4, 2015, 937–990.

Boese, Oliver, Strafrechtliche Verantwortlichkeit für Verweisungen durch Links im Internet. Frankfurt am Main 2000.

Boulos, Maged N. Kamel/Wheeler, Steve, The emerging Web 2.0 social software: an enabling suite of sociable technologies in health and health care education. Health Information and Libraries Journal Vol. 24, Issue 1, 2007, 2–23.

Brinkel, Guido, Filesharing: Verantwortlichkeit in Peer-to-Peer-Tauschplattformen. Tübingen 2006.

Bröhl, Georg M., Rechtliche Rahmenbedingungen für neue Informations- und Kommunikationsdienste. CR Heft 2, 1997, 73–79.

Bundesministerium des Innern, Bericht zur Polizeilichen Kriminalstatistik, 2016.

Cai, Huifang, Die strafrechtliche Verantwortlichkeit der P2P-Netzwerkbetreiber als Beihilfe durch neutrale Handlung. Soochow Rechtszeitschrift (东吴法律学报) Heft 1, 2006, 61–90.

Cai, Huifang, Die Möglichkeit der Mittäterschaft der P2P-Netzwerkbetreiber und ihren Mitgliedern. Rechtszeitschrift für Technologie (科技法学评论) Heft 1, 2006, 45–73.

Cardoso, Jorge, The Semantic Web Vision: Where Are We? IEEE Intelligent Systems Vol. 22, No. 5, 2007, 84–88.

Che, Hao, Der neue Kommentar zum *Kuaibo*-Fall, abrufbar unter http://www.law.pku.edu.cn/xwzx/pl/16871.htm [Stand: 15.09.2017].

– Die dogmatischen Reflexionen über die strafrechtliche Gesetzgebung. Eine Analyse des Strafrechtsänderungsgesetzes (IX). Rechtswissenschaft (法学) Heft 10, 2015, 3–16.

– Wer soll für die neutrale Handlung im Internet-Zeitalter verantwortlich sein? China Law Review (中国法律评论) Heft 1, 2015, 47–50.

Chen, Hongbing, Die neutralen Handlungen. Peking 2010.

– Die neutralen Handlungen. Rechtszeitschrift der Universität Peking (中外法学) Heft 6, 2008, 931–957.

– Die Grenze der Strafbarkeit der neutralen Handlung. Chinesische Rechtswissenschaft (中国法学) Heft 1, 2017, 189–208.

– Die Strafbarkeit der neutralen Handlung im Netzwerk: Die Analyse der Handlung der P2P-Netzwerkbetreiber. Zeitschrift der Nordöstlichen Universität (Sozialwissenschaftliche Ausgabe) (东北大学学报-社会科学版) Heft 3, 2009, 258–263.

Chen, Jinchuan, Die Untersuchung der subjektiven Schuld von ISP. Geistiges Eigentum (知识产权) Heft 2, 2011, 56–62.

Chen, Kai/Bai, Yingcai, Die Technologie der Netzwerkspeicherung und ihr Trend. Acta Electronica Sinica (电子学报) Heft 12A, 2012, 1928–1932.

Chen, Xingliang, Die strafrechtlich dogmatische Bewertung zum Urteil der ersten Instanz des *Kuaibo*-Falls. Rechtszeitschrift der Universität Peking (中外法学) Heft 1, 2017, 7–28.

– Zwischen Technik und Recht: Die strafrechtlich dogmatische Bewertung zum Urteil der ersten Instanz des *Kuaibo*-Falls. Volksgerichtszeitung (人民法院报), 14.09.2016.

– Über das „Kennen" im besonderen Teil des StGB – Basierend auf der Erläuterung der Ausdrucksdelikte. Der Jurist (法学家) Heft 3, 2013, 79–97.

– Die normative strafrechtliche Wissenschaft I (规范刑法学). Beijing 2008.

– Die ontologische strafrechtliche Wissenschaft (本体刑法学). Beijing 2001.

Chen, Yijian, Eine Bewertung zur Legitimität der „Teilnahme zum Täter". Rechtszeitschrift der Universität Zhongshan (中山大学法律评论) Heft 2, 2010, 297–307.

Chen, Zhigang/Li, Shanhe, Die strafrechtliche Analyse und die Behandlung des Downloads durch P2P Software. Kriminalwissenschaft (中国刑事法杂志) Heft 4, 2014, 48–54.

China Internet Network Information Center (CNNIC), Internet Meilensteine 1986–1993, abrufbar unter http://www.cnnic.net.cn/hlwfzyj/hlwdsj/201206/t20120612_27414.htm. [Stand: 15.09.2017].

– Der statistische Bericht über die Entwicklung des Internets in China 1997, abrufbar unter http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/200905/P020120709345374625930.pdf [Stand: 15.09.2017].

China Internet Network Information Center (CNNIC), Der statistische Bericht über die Entwicklung des Internets in China 2017, abrufbar unter http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201708/P020170807351923262153.pdf [Stand: 15.09.2017].

Chu, Huaizhi/Yang, Shuwen, Eine Diskussion über die Vorsatz-Fahrlässigkeit-Kombination und über die Anwendung einer verschwommenen Erkenntnistheorie. Zeitschrift für Strafrecht (刑事法评论) Heft 7, 2000, 410–456.

– Die Untersuchung zur Vorsatz-Fahrlässigkeit-Kombination. Eine theoretische Erläuterung des neuen gesetzlichen Phänomens im StGB. Chinesische Rechtszeitschrift (法学研究) Heft 1, 1999, 50–57.

Conradi, Ulrich/Schlömer, Uwe, Die Strafbarkeit der Internet-Provider. NStZ Heft 8, 1996, 366–369, Heft 10, 1996, 472–477.

Cui Guobin, Die Verpflichtung zur Filterung der Inhalte der ISP. Chinesische Rechtswissenschaft (中国法学). Heft 2, 2017, 215–237.

– Die urheberrechtliche Regulierung der Framed Links. Politik und Recht (政治与法律) Heft 5, 2014, 74–93.

– Die Umgestaltung des Systems für eine gemeinschaftliche Verletzung der ISP. Chinesische Rechtszeitschrift (法学研究) Heft 4, 2013, 138–159.

Cui, Lihong/Hao, Lei, Die Untersuchung zu der Urheberrechtsverletzung der P2P-Technologie. Juristisches Forum (法学论坛) Heft 2, 2006, 90–95.

Dang, Jianjun (Hrsg.), Die Straftaten gegen das Urheberrecht (侵犯知识产权罪). Peking 1999.

Du, Jing, Cyberkriminalität und ihre Gegenmaßnahmen. Sozialwissenschaftliche Zeitschrift der Jiamusi-Universität (佳木斯大学社会科学学报) Heft 4, 2005, 29–31.

Die zunehmende Cyberkriminalität in China, abrufbar unter http://www.thepaper.cn/newsDetail_forward_1547385. [Stand: 15.09.2017].

Eck, Stefan/Ruess, Peter, Haftungsprivilegierung der Provider nach der E-Commerce-Richtlinie – Umsetzungsprobleme dargestellt am Beispiel der Kenntnis nach § 11 Satz 1 Ziff. 1 TDG. MMR Heft 6, 2003, 363–366.

Eichhorn, Bert, Internetrecht. Ein Wegweiser für Nutzer und Web-Verantwortliche. Berlin 2007.

Engel-Flechsig, Stefan/Maennel, Frithjof A./Tettenborn, Alexander, Das neue Informations und Kommunikationsdienste-Gesetz. NJW Heft 45, 1997, 2981–2992.

Engisch, Karl, Einführung in das juristische Denken. 10. Aufl. Stuttgart 2005.

– Die Einheit der Rechtsordnung. Heidelberg 1935.

Erklärung der „Verordnung über den Schutz des Informationsnetz-Übertragungsrechts“ des Staatsrats, abrufbar unter http://news.xinhuanet.com/it/2006-05/30/content_4620272_1.htm [Stand: 15.09.2017].

Ernst, Stefan/Vassilaki, Irini E./Wiebe, Andreas, Hyperlinks: Rechtsschutz, Haftung, Gestaltung. Köln 2002.

Der erste Internet-Gerichtshof in China wird begründet, abrufbar unter http://news.china.com/news100/11038989/20170818/31127149.html. [Stand: 15.09.2017].

Fan, Jun, Die Strafbarkeit im *Kuaibo*-Fall und die relevanten Probleme in der Urteilsbegründung im Rahmen einer technischen Bewertung. Rechtszeitschrift der Universität Peking (中外法学) Heft 1, 2017, 29–50.

Feng, Gang, Die Deliktshaftung der Betreiber der P2P Software. Eine Analyse des ersten P2P-Rechtsverletzungsfalls. Geistiges Eigentum (知识产权) Heft 3, 2008, 47–52.

Feng, Shujie, Die Formen der Schuld der indirekten Deliktshaftung von ISP. Chinesische Rechtswissenschaft (中国法学) Heft 4, 2016, 179–197.

Feng, Xiaoqing/Han, Tingting, Die Diskussion über die Anwendung und Verbesserung des „Serverkriteriums" im Streit über Urheberrecht im Netzwerk. Elektronisches geistiges Eigentum (电子知识产权) Heft 6, 2016, 41–53.

Finke, Thorsten, Die strafrechtliche Verantwortung von Internet-Providern. Tübingen 1998.

Fischer, Thomas, Strafgesetzbuch und Nebengesetze. Kommentar. 61. Aufl. München 2014.

Flechsig Norbert P./Gabel, Detlev, Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks. CR Heft 6, 1998, 351–358.

Forouzan, Behrouz/Mosharraf, Firouz, Computer Networks: A Top-Down Approach (计算机网络教程:自顶向下方法), übersetzt von *Zhang Jianzhong* u.a. Peking 2012.

Frey, Dieter, Peer-To-Peer File-Sharing, das Urheberrecht und die Verantwortlichkeit von Diensteanbietern am Beispiel Napster, Inc. im Lichte des US-amerikanischen und des EG-Rechts. ZUM Heft 6, 2001, 466–478.

Freytag, Stefan, Providerhaftung im Binnenmarkt, Verantwortlichkeit für rechtswidrige Inhalte nach der E-Commerce-Richtlinie. CR Heft 9, 2000, 600–609.

Freiwald, Sven, Die private Vervielfältigung im digitalen Kontext am Beispiel des Filesharing. Baden-Baden 2004.

Frisch, Wolfgang, Tatbestandsmäßiges Verhalten und Zurechnung des Erfolgs. Heidelberg 2012.

Fuchs, Christian, u.a., Theoretical Foundations of the Web: Cognition, Communication, and Co-Operation, Towards an Understanding of Web 1.0, 2.0, 3.0. Future Internet, No. 2, 2010, S. 41–59.

Gao, Mingxuan/Ma, Kechang (Hrsg.), Strafrechtliche Wissenschaft (刑法学). 6. Aufl. Peking 2014.

– Strafrechtliche Wissenschaft (刑法学). 4. Aufl. Peking 2010.

Gao, Mingxuan (Hrsg.), Die strafrechtlichen Grundsätze I (刑法学原理). Peking 1993.

– Die chinesische strafrechtliche Wissenschaft (中国刑法学). Peking 1989.

Gao, Yandong, Das Schicksal der unechten Unterlassungsdelikte in China, Kommentar zum *Kuaibo*-Fall. Rechtszeitschrift der Peking Universität (中外法学) Heft 1, 2017, 68–88.

Gercke, Marco/Brunst, Phillip W., Praxishandbuch Internetstrafrecht. Stuttgart 2009.

Gersdorf, Hubertus/Paal, Boris P.(Hrsg.), Beck'scher Online-Kommentar Informations- und Medienrecht. 17. Aufl. 2017 (zit. Gersdorf/ Paal-*Bearbeiter*).

Graf, Jürgen Peter, Internet: Straftaten und Strafverfolgung. DRiZ Heft 7, 1999, 281–286.

Guo, Chuntao, Die Definition der Cyberkriminalität und ihre Gesetzgebung. Info-Netzwerk Sicherheit (信息网络安全) Heft 10, 2005, 46–48.

Günther, Hans-Ludwig, Klassifikation der Rechtfertigungsgründe im Strafrecht. In: Manfred Seebode (Hrsg.), Festschrift für Günter Spendel zum 70. Geburtstag. Berlin 1992, S. 189–202.

– Strafrechtswidrigkeit und Strafunrechtsausschluss, Studien zur Rechtswidrigkeit als Straftatmerkmal und zur Funktion der Rechtfertigungsgründe im Strafrecht. Köln 1983.

Han, Dezhi, Die Technologie der Netzwerkspeicherung und ihre Entwicklung. Forschung zur Anwendung von Computern (计算机应用研究) Heft 7, 2005, 5–8.

Hassemer, Winfried, Professionelle Adäquanz, bankentypisches Verhalten und Beihilfe zur Steuerhinterziehung. Zeitschrift für Wirtschaft, Steuer, Strafrecht Heft 2, 1995, 41–46.

Heghmanns, Michael, Musiktauschbörsen im Internet aus strafrechtlicher Sicht. MMR Heft 1, 2004, 14–18.

– Anmerkung zum Urteil des Landgerichts München I vom 17. November 1999 – 20 Ns 465 Js 173158/95 – CompuServe. ZUM Heft 6, 2000, 462–466.

Heliosch, Alexandra, Verfassungsrechtliche Anforderungen an Sperrmaßnahmen von kinderpornographischen Inhalten im Internet, unter besonderer Berücksichtigung des Zugangserschwerungsgesetzes. Göttingen 2012.

Hilgendorf, Eric, Zur Anwendbarkeit des § 5 TDG auf das Strafrecht. NStZ Heft 10, 2000, 518–522.

Hilgendorf, Eric/Valerius, Brian, Computer- und Internetstrafrecht. 2. Aufl. Berlin 2012.

Hilgendorf, Eric/Frank, Thomas/Valerius, Brian, Computer- und Internetstrafrecht. Berlin 2005.

Hoeren, Thomas, Zivilrechtliche Haftung im Online-Bereich (Teil 18.2). In: Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.), Handbuch Multimedia-Recht. München 2014, Rn. 1–163.

– Urteilsanmerkung, Generalbundesanwalt, Haftung eines Access Providers für rechtswidrigen Inhalt. MMR Heft 2, 1998, 93–98.

Hoffmann, Helmut, Zivilrechtliche Haftung im Internet. MMR Heft 5, 2002, 284–289.

Hörnle, Tatjana, Pornographische Schriften im Internet: Die Verbotsnormen im deutschen Strafrecht und ihre Reichweite. NJW Heft 14, 2002, 1008–1013.

Hütig, Stefan, Urteilsanmerkung, AG Tiergarten, Link auf eine Homepage mit rechtswidrigem Inhalt. MMR Heft 1, 1998, 49–52.

Jakobs, Günter, Strafrecht. Allgemeiner Teil. Die Grundlagen und die Zurechnungslehre. 2. Aufl. Berlin 1993.

Jescheck, Hans-Heinrich/Weigend Thomas, Lehrbuch des Strafrechts. Allgemeiner Teil. 5. Aufl. Berlin 1996.

Jiang, Chengming/Jiang, Xinghao/Sun, Tanfeng, Die auf Multimodal-Features basierende Filtermethode für die Sicherheit des Video-Content. Informationssicherheit und Vertraulichkeit der Kommunikation (信息安全与通讯保密) Heft 3, 2012, 76–77.

Jin, Hai/Liao, Xiaofei, Die Grundsätze und Anwendungen der P2P-Technik. ZTE Kommunikationen (中兴通讯技术) Heft 6, 2007, 1–5.

Jing, Lijia, Über die „Verweigerung der Erfüllung der Sicherheitsverpflichtungen im Informationsnetzwerk", Diskussion über die strafrechtliche Verantwortlichkeit der ISP. Politik und Recht (政治与法律) Heft 1, 2017, 50–65.

Jiang, Shuai, Die Untersuchung zu der Deliktshaftung der Anbieter der P2P-Software in den USA. Elektronisches geistiges Eigentum (电子知识产权) Heft 8, 2015, 75–81.

Joecks, Wolfgang/Miebach, Klaus (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Band 3, 2. Aufl. München 2012 (zit. Joecks/Miebach-*Bearbeiter*).

Joecks, Wolfgang/Miebach, Klaus (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Band 1, 2. Aufl. München 2017 (zit. Joecks/Miebach-*Bearbeiter*).

Kaufmann, Arthur, Analogie und „Natur der Sache", zugleich ein Beitrag zur Lehre vom Typus, übersetzt von Wu Congzhou. Taipei 1999.

Kaufman, Lori M., Data Security in the World of Cloud Computing. IEEE Security & Privacy, Vol. 7, Issue 4, 2009, pp.61–64.

Kern, Eduard, Grade der Rechtswidrigkeit. ZStW Band 64, 1952, 255–291.

Kessler, Clemens, Zur strafrechtlichen Verantwortlichkeit von Zugangsprovidern in Deutschland und der Umsetzung der E-Commerce-Richtlinie in Europa. Berlin 2003.

Kindhäuser, Urs, Strafrecht. Allgemeiner Teil. 7. Aufl. Baden-Baden 2015.

Kindhäuser, Urs/Neumann, Ulfrid/Paeffgen, Hans-Ullrich, Strafgesetzbuch. Nomos Kommentar. 4. Aufl. Baden-Baden 2013 (zit. Kindhäuser/Neumann/Paeffgen-*Bearbeiter*).

Koch, Alexander, Strafrechtliche Verantwortlichkeit beim Setzen von Hyperlinks auf mißbilligte Inhalte. MMR Heft 12, 1999, 704–710.

Koch, Frank A., Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen. CR Heft 4, 1997, 193–203.

Krey, Volker/Esser, Robert, Deutsches Strafrecht. Allgemeiner Teil. 6. Aufl. Stuttgart 2016.

Kudlich, Hans, Die Unterstützung fremder Straftaten durch berufsbedingtes Verhalten. Berlin 2004.

– Die Neuregelung der strafrechtlichen Verantwortung von Internetprovidern. JA 2002, 798–803.

Kurose, James F./Ross, Keith W., Computer Networking, A Top-Down Approach. 6th edition Boston 2013.

Kühl, Kristian, Strafrecht. Allgemeiner Teil. 8. Aufl. München 2016.

Kühne, Hans-Heiner, Urteilsanmerkung, LG München I: Straflosigkeit der reinen Zugangsvermittlung „harter" Pornografie im Internet. NJW Heft 14, 2000, 1051–1052.

– Nochmals: Die Strafbarkeit der Zugangsvermittlung von pornographischen Informationen im Internet. NJW Heft 14, 2000, 1003–1004.

– Strafbarkeit der Zugangsvermittlung von pornographischen Informationen im Internet. Die *CompuServe*-Entscheidung des AG München. NJW Heft 3, 1999, 188–190.

Lackner/Kühl, Strafgesetzbuch Kommentar. Kristian Kühl/Martin Heger (Hrsg.), 28. Aufl. München 2014 (zit. Lackner/Kühl-*Bearbeiter*).

Lang, Alexander, Filesharing und Strafrecht. Berlin 2009.

Lao, Dongyan, Die Elementaranalyse des Vorsatzes. Zeitschrift der Rechtsvergleichung (比较法研究) Heft 1, 2009, 45–68.

Laufhütte, Heinrich Wilhelm/ Rissing-van Saan, Ruth/Tiedemann, Klaus (Hrsg.), Strafgesetzbuch. Leipziger Kommentar. Erster Band. 12. Aufl. Berlin 2007 (zit. Laufhütte/ Rissing-van Saan/Tiedemann-*Bearbeiter*).

Liang, Genlin, Die traditionellen Delikte im Netzwerk: Zurechnungsprobleme, strafrechtliche Reaktionen und ihre dogmatischen Beschränkungen. Rechtswissenschaft (法学) Heft 2, 2017, 3–13.

– Die Entwicklung der chinesischen Verbrechenslehre, Überblick und Stellungnahme. ZStW 126, Heft 3, 2014, 743–774.

Li, Bencan, Die zweiseitige Erläuterung des § 286 I StGB. Juristisches Forum (法学论坛) Heft 3, 2017, 138–145.

Li, Can, Die Forschung zur Strafbarkeit der neutralen Handlung im Rahmen der Risikogesellschaft – Basierend auf der vergleichenden Untersuchung zwischen deutscher und japanischer Theorie. Zeitschrift der südöstlichen Universität (Sozialwissenschaftliche Ausgabe) (东南大学学报-哲学社会科学版) Beilage Heft 18, 2016, 77–81.

Li, Hong, Die Errichtung der exklusiven Herrschaft, Schwierigkeiten und Lösungen der unechten Unterlassung. Rechtszeitschrift der Universität Peking (中外法学) Heft 6, 2014, 1573–1595.

– Die Untersuchung des Unterlassungsdelikts. Wuhan 1997.

Li, Lanying, Die weitere Besprechung der Vorsatz-Fahrlässigkeit-Kombination. Moderne Rechtswissenschaft (现代法学) Heft 4, 2005, 74–78.

Lin, Qinghong/Zhou, Zhou, Die zurückhaltende Bestrafung der Deep Links. Rechtswissenschaft (法学) Heft 9, 2013, 152–159.

Lin, Shantian, Strafrecht Allgemeiner Teil I (刑法通论 上册). 8. Aufl. Taipei 2000.

Liu, Deliang, Der Status und die Haftung der ISP im Deliktsrecht. Studium des Rechts und der Wirtschaft (法商研究) Heft 5, 2001, 111–119.

Liu, Jiarui, Die Bewertung zur *safe harbor*-Regelung der ISP. Anmerkung zum Yahoo-Fall. Geistiges Eigentum (知识产权) Heft 2, 2009, 13–22.

Liu, Renwen/Zhang, Hui, Vorschläge zur Verbesserung der Verfolgung von Cyberkriminalität im Entwurf des Strafrechtsänderungsgesetzes (IX). Volksgerichtszeitung (人民法院报), 12.08.2015.

Liu, Wenjie, Die Verkehrspflichten der ISP. Rechtszeitschrift der Universität Peking (中外法学) Heft 2, 2012, 395–410.

Liu, Xiaoshan/Sun, Baomin, Eine Reflexion über den Wiederaufbau der ursprünglichen Pflichten von unechter Unterlassung. Kriminalwissenschaft (中国刑事法杂志) Heft 4, 2008, 33–39.

Liu, Yanhong, Die straflose *Kuaibo* und die Kritik an dem *Kuaibo*-Urteil. Politik und Recht (政治与法律) Heft 12, 2016, 104–112.

– Die kritische Beleuchtung der Geschichte der Strafbarkeit der neutralen Beihilfe im Netzwerk – Eine vergleichende Untersuchung der deutschen und japanischen Theorie und Praxis. Law Review (法学评论) Heft 5, 2016, 40–49.

– Kritik an der gesetzgeberischen Veränderung „Gehilfe zu Täter“ (帮助犯正犯化) im Rahmen der Cyberkriminalität. Studium des Rechts und der Wirtschaft (法商研究) Heft 3, 2016, 18–22.

Liu, Ying/Huang, Qiong, Die Haftung der ISP im „Deliktsrecht“. Zeitschrift der Universität Jinan (Sozialwissenschaftliche Ausgabe) (暨南学报-哲学社会科学版) Heft 3, 2010, 52–59.

Li, Wenyan/Deng, Zibing, Über die strenge Verantwortung im chinesischen StGB. Chinesische Rechtswissenschaft (中国法学) Heft 5, 1999, 90–95.

Long, Jingrong, Analyse der neuen Entwicklungslinien im Rahmen der urheberrechtlichen Haftung von Hyperlinksetzung in der EU und Großbritannien, Kommentar zu der chinesischen urheberrechtlichen Praxis. Rechtswissenschaftliche Zeitschrift (法学杂志) Heft 12, 2014, 125–132.

Lu, Chunya, Die Deliktshaftung der ISP. Zeitschrift der Universität Henan für Wirtschaft und Recht (河南财经政法大学学报) Heft 5, 2012, 58–68.

– Die Typisierung der Deliktshaftung von ISP. Politik und Recht (政治与法律) Heft 4, 2011, 117–127.

Lu, Xu, Erläuterungen der strafrechtlichen Verantwortlichkeit von ISP. Kommentar zu den einschlägigen Paragraphen. Untersuchung der Rechtsstaatlichkeit (法治研究) Heft 6, 2015, 61–67.

Luo, Qiong, Die zurückhaltende Bestrafung für das Setzen von Deep Links. Kommentar zum ersten Rechtsverletzungsfall aufgrund des Setzens von Deep Links. Zeitschrift des Technischen Colleges in Wuhan für Kommunikation (武汉交通职业学院学报) Heft 3, 2014, 35–40.

Löwe-Krahl, Oliver, Beteiligung von Bankangestellten an Steuerhinterziehungen ihrer Kunden. Die Tatbestandsmäßigkeit berufstypischer Handlungen. wistra Heft 6, 1995, 201–206.

Naik, Umesha/Shivalingaiah D, Comparative Study of Web 1.0, Web 2.0 and Web 3.0. 6th International CALIBER 2008, S. 499–507.

Niedermair, Harald, Beihilfe durch neutrale Handlungen? ZStW 107, Heft 3, 1995, 507–544.

Ma, Kechang, Die Grundsätze des Strafrechts in der Rechtsvergleichung (比较刑法原理). Wuhan 2002.

Malek, Klaus/Popp, Andreas, Strafsachen im Internet. 2. Aufl. Heidelberg 2015.

Mantz, Reto, Urteilsanmerkung, BGH: Haftung des Internetanschlussinhabers mit WLAN – Sommer unseres Lebens. MMR Heft 8, 2010, 565–570.

Mao, Lingling, Ein bedingt materielles Differenzierungskriterium für die Bestimmung der Unterlassungspflichten. Orientalisches Recht (东方法学) Heft 3, 2014, 23–33.

Marberth-Kubicki, Annette, Computer- und Internetstrafrecht. 2. Aufl. München 2010.

Matthies, Ulf, Providerhaftung für Online-Inhalte, eine vergleichende Untersuchung zur Rechtslage in Deutschland, Österreich und England. Baden-Baden 2004.

Mayer-Schönberger, Viktor/Cukier, Kenneth, Big Data: A Revolution That Will Transform How We Live, Work, and Think, translated by Sheng Yangyan, Zhou Tao. Hangzhou 2013.

Mell, Peter/Grance, Timothy, The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800–145, 2011.

Meng, Chuanxiang, Die Untersuchung der Unterlassungshandlungen im Kontext von ISP. Zeitschrift der Universität Chongqing für Post und Telekommunikation (Sozialwissenschaftliche Ausgabe) (重庆邮电大学学报-社会科学版) Heft 6, 2012, 26–30.

Meyer-Arndt, Lüder, Beihilfe durch neutrale Handlungen? Zeitschrift für Wirtschaft, Steuer, Strafrecht Heft 8, 1989, 281–287.

Mezger, Edmund, Strafrecht. Allgemeiner Teil. 9. Aufl. München 1960.

Moritz, Hans-Werner, § 5 TDG im deutschen Recht – die wissenschaftliche Diskussion ist eröffnet. MMR Heft 12, 1998, 625–626.

– Urteilsanmerkung, Amtsgericht München, Verbreitung pornographischer Schriften durch Internet-Provider. CR Heft 8, 1998, 500–510.

Müller-Broich, Jan D., Telemediengesetz, Nomos-Kommentar, Baden-Baden 2012.

Das Oberste Volksgericht spricht von der Interpretation über das Informationsnetz-Übertragungsrecht, abrufbar unter http://news.xinhuanet.com/zgjx/2012-12/27/c_132065681.htm. [Stand: 11.05.2017].

Oram, Andy (ed.), Peer-to-Peer. Harnessing the Benefits of Disruptive Technologies. Sebastopol 2001.

Otto, Harro, „Vorgeleistete Strafvereitelung" durch berufstypische oder alltägliche Verhaltensweisen als Beihilfe. In: Albin Eser/Ulrike Schittenhelm/Heribert Schumann (Hrsg.), Festschrift für Theodor Lenckner zum 70. Geburtstag. München 1998, 193–225.

Ou, Jinxiong, Die Verneinung der Vorsatz-Fahrlässigkeit-Kombination. Die Feststellung der Mens Rea von Delikten mit doppelten Erfolgen. Zeitschrift der Guangxi-Verwaltung und des Kader-Instituts für Politik und Recht (广西政法管理干部学院学报) Heft 4, 2005, 3–8, 17.

Ouyang, Benqi/Wang, Qian, Die gesetzliche Anwendung der neu erlassenen Regeln über die Cyberkriminalität im Strafrechtsänderungsgesetz (IX). Zeitschrift des Jiangsu-Verwaltungsinstituts (江苏行政学院学报) Heft 4, 2016, 124–130.

Pätzel, Claus/Gravenreuth, Günter, Frhr. v., Urteilsanmerkung, AG München, Verbreitung pornographischer Schriften durch Internet-Provider. CR Heft 10, 1998, 624–629.

Pelz, Christian, Die Strafbarkeit von Online-Anbietern. Zugleich eine Besprechung von AG München. wistra Heft 2, 1999, 53–59.

– Die strafrechtliche Verantwortlichkeit von Internet-Providern. ZUM Heft 7, 1998, 530–534.

Peng, Le/Xue, Yibo/Wang, Chunlu, Die zusammenfassende Untersuchung zur Identifizierung und Filterung des Video-Content im Netzwerk. Ingenieurinformatik und Design (计算机工程与设计) Heft 10, 2008, 2587–2590, 2634.

Peng, Wenhua, Die Untersuchung der strafrechtlichen Verantwortlichkeit von ISP. Zeitschrift der Universität Foshan (Sozialwissenschaftliche Ausgabe) (佛山科学技术学院学报-社会科学版) Heft 3, 2004, 55–59.

Peng, Yuyong, Über die Rechte und Pflichten der ISP. Zeitschrift der Universität Jinan (Sozialwissenschaftliche Ausgabe) (暨南学报-哲学社会科学版) Heft 12, 2014, 67–82.

Pilz, Klaus, Beihilfe zur Steuerhinterziehung durch neutrale Handlungen von Bankmitarbeitern. Frankfurt am Main 2001.

Pi, Yong, Die Analyse strafrechtlicher Verfolgungsprobleme von pornographischen Informationen im Netzwerk. Volksstaatsanwaltschaft (人民检察) Heft 6, 2005, 20–23.

– Die strafrechtliche Verantwortlichkeit der ISP. Guang Ming Daily (光明日报) 28.06.2005.

– Probleme der Kriminalitätsbekämpfung bezüglich pornografischer Informationen im Internet. Law Review (法学评论) Heft 3, 2002, 144–149.

Popp, Martin, Die strafrechtliche Verantwortung von Internet-Providern. Berlin 2002.

Qi, Aimin/Zhu, Gaofeng, Rechtsschutz der Datensicherheit in der Cloud-Speicherung. Zeitschrift der Chongqing-Universität (Sozialwissenschaftliche Ausgabe) (重庆大学学报-社会科学版) Heft 1, 2017, 101–108.

Qian, Yeliu, Die Abgrenzung von Täterschaft und Teilnahme im Kontext des Dual-Beteiligungssystems. Chinesische Rechtszeitschrift (法学研究) Heft 1, 2012, 126–143.

Qin, Tianning/Zhang, Mingxun, Eine auf den „technischen Maßnahmen" basierende Untersuchung der Elemente von Unterlassungsdelikten von ISP. Strafrechtliche Wissenschaft (中国刑事法杂志) Heft 9, 2009, 42–47.

Rackow, Peter, Neutrale Handlungen als Problem des Strafrechts. Frankfurt am Main 2007.

Rengier, Rudolf, Strafrecht. Allgemeiner Teil. 9. Aufl. München 2017.

Rui, Yansong, Die Bestimmung der direkten Deliktshaftung von Deep Links. Das Nutzer-Kriterium als Regelbestimmung, Das technische Kriterium als die Ausnahme. China Patent & Marke (中国专利与商标) Heft 4, 2009, 81–91.

Roßnagel, Alexander (Hrsg.), Beck'scher Kommentar zum Recht der Telemediendienste. München 2013 (zit. Roßnagel-*Bearbeiter*).

Roxin, Claus, Täterschaft und Tatherrschaft. 8. Aufl. Berlin 2006.

– Strafrecht. Allgemeiner Teil. Band I. Grundlagen. Der Aufbau der Verbrechenslehre. 4. Aufl. München 2006.

– Strafrecht. Allgemeiner Teil. Band II. Grundlagen. Besondere Erscheinungsformen der Straftat. München 2003.

Rustad, Michael L., Global Internet Law in a Nutshell. 3rd. edition St. Paul, Minn. 2016.

– Internet Law in a Nutshell. St. Paul, Minn., 2009.

Sang, Benqian, Die Internet-Pornografie, technische Neutralität, und nationale Wettbewerbsfähigkeit. Die politische Ökonomie hinter dem *Kuaibo*-Fall. Rechtswissenschaft (法学) Heft 1, 2017, 79–94.

Schild Trappe, Grace Marie Luise, Harmlose Gehilfenschaft? Eine Studie über Grund und Grenzen der Gehilfenschaft. Bern 1995.

Schoder, Detlef/Fischbach, Kai/Teichmann René (Hrsg.), Peer-to-Peer, ökonomische, technologische und juristische Perspektiven. Berlin 2002.

Schönke/Schröder, Kommentar zum Strafgesetzbuch. Gesamtredaktion: Albin Eser. 29. Aufl. München 2014 (zit. Schönke/Schröder-*Bearbeiter*).

Schumann, Heribert, Strafrechtliches Handlungsunrecht und das Prinzip der Selbstverantwortung der Anderen (sic). Tübingen 1986.

Sesing, Andreas, Neuerungen im TMG für mehr freies WLAN. MMR-Aktuell, Ausgabe 11, 2016, 378738.

Shi, Xueqing/Wang, Yong, Die Erläuterung zu § 23 der „Verordnung über den Schutz des Informationsnetz-Übertragungsrechts". Geistiges Eigentum (知识产权) Heft 3, 2009, 23–29.

Sieber, Ulrich, Allgemeine Probleme des Internetstrafrechts (Teil 19.1). In: Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.), Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs. München 2014, Rn. 1–93.

– Straftaten und Strafverfolgung im Internet, Gutachten C zum 69. Deutschen Juristentag. München 2012.

– Aufbruch in das neue Jahrtausend, für eine neue Kultur der Verantwortlichkeit im Internet. MMR Heft 12, 1999, 689–690.

– Die Verantwortlichkeit von Internet-Providern im Rechtsvergleich. ZUM Heft 3, 1999, 196–213.

– Die rechtliche Verantwortlichkeit im Internet – Grundlagen, Ziele und Auslegung von § 5 TDG und § 5 MDStV. MMR-Beilage Heft 2, 1999, 1–32.

– Verantwortlichkeit im Internet: Technische Kontrollmöglichkeiten und multimediarechtliche Regelungen. Zugleich eine Kommentierung von § 5 TDG und § 5 MDStV. München 1999.

– Urteilsanmerkung, AG München: *CompuServe*-Urteil. MMR Heft 8, 1998, 429–448.

– Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II), CR, Heft 11, 1997, 653–669.

– Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (I), CR, Heft 10, 1997, 581–598.

– Die Abgrenzung von Tun und Unterlassen bei der „passiven" Gesprächsteilnahme. JZ Heft 11/12, 1983, 431–437.

Sieber, Ulrich/Höfinger, Frank Michael, Allgemeine Grundsätze der Haftung (Teil 18.1). In: Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.), Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs. München 2014, Rn. 1–134.

Sieber, Ulrich/Liesching, Marc, Die Verantwortlichkeit der Suchmaschinenbetreiber nach dem TMG. MMR Beilage Heft 8, 2007, 1–30.

Spindler, Gerald, Die geplante Reform der Providerhaftung im TMG und ihre Vereinbarkeit mit Europäischem Recht. Warum die beabsichtigte Reform ihr Ziel verfehlen wird. CR Heft 1, 2016, 48–56.

Spindler, Gerald/Schuster, Fabian, Recht der elektronischen Medien. Kommentar. 3. Aufl. München 2015 (zit. Spindler/Schuster-*Bearbeiter*).

Spindler, Gerald/Schmitz, Peter/Geis, Ivo, TDG, Teledienstegesetz, Teledienstedatenschutzgesetz, Signaturgesetz. Kommentar. München 2004 (zit. Spindler/Schmitz/Geis-*Bearbeiter*).

– Das Gesetz zum elektronischen Geschäftsverkehr – Verantwortlichkeit der Diensteanbieter und Herkunftslandprinzip. NJW Heft 13, 2002, 921–927.

– Verantwortlichkeit von Diensteanbietern nach dem Vorschlag einer E-Commerce-Richtlinie. MMR Heft 4, 1999, 199–207.

– Die Haftung von Online-Diensteanbietern im Konzern. CR Heft 12, 1998, 745–757.

– Haftungsrechtliche Grundprobleme der neuen Medien. NJW Heft 48, 1997, 3193–3199.

Stadler, Thomas, Haftung für Informationen im Internet. 2. Aufl. Berlin 2005.

Steinmetz, Ralf/Wehrle, Klaus (ed.), Peer-to-Peer Systems and Applications. Heidelberg, 2005.

Stratenwerth, Günter/Kuhlen, Lothar, Strafrecht. Allgemeiner Teil. 6. Aufl. München 2011.

Subashini S./Kavitha V., A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications Vol. 34, Issue 1, 2011, 1–11.

Sun, Yan/Zhou, Xueguang, Der Forschungsfortschritt zur Informationsfilterung, Informationssicherheit und Vertraulichkeit der Kommunikation (信息安全与通讯保密) Heft 9, 2011, 45–49.

Su, Shengyong/Liu, Hui, Die Filtertechnologie und ihre Anwendung. Welt der digitalen Kommunikation (数字通信世界) Heft 9, 2016, 56–57.

Tag, Brigitte, Beihilfe durch neutrales Verhalten. JR Heft 2, 1997, 49–57.

Tanenbaum, Andrew S./Wetherall, David J., Computer Networks, übersetzt von Yan Wie/Pan Aiming. 5. Aufl. Beijing 2011.

Tan, Shaomu/Wu, Weibing, Die Analyse der strafrechtlichen Verantwortlichkeit der Herunterladung durch BT Software. Volksjustiz (人民司法) Heft 10, 2006, 66–68.

Tu, Longke, Die Verpflichtung zur Verwaltung der Netzwerkinhalte und die strafrechtliche Verantwortlichkeit der ISP. Law Review (法学评论) Heft 3, 2016, 66–73.

Urteil der ersten Instanz zum *Kuaibo*-Fall, abrufbar unter http://bjhdfy.chinacourt.org/public/detail.php?id=4343 [Stand: 11.05.2017].

Urteil der zweiten Instanz zum *Kuaibo*-Fall. Volksgerichtszeitung (人民法院报), 16.12.2016.

Vassilaki, Irini E., Strafrechtliche Verantwortlichkeit durch Einrichten und Aufrechterhalten von elektronischen Verweisen (Hyperlinks), Anwendbarkeit der allgemeinen Strafrechtsdogmatik auf neue Verhaltensformen. CR Heft 2, 1999, 85–93.

– Strafrechtliche Verantwortlichkeit der Diensteanbieter nach dem TDG. Eine Untersuchung unter besonderer Berücksichtigung der Einordnung des § 5 TDG im Strafrechtssystem. MMR Heft 12, 1998, 630–638.

– Urteilsbemerkung, AG Berlin-Tiergarten: Strafbarkeit beim Setzen von Links. CR Heft 2, 1998, 111–112.

Die volle Rezession des SMS-Service, abrufbar unter http://tech.163.com/14/0603/10/9TQC2KRF000915BE.html. [Stand: 15.09.2017].

Waldenberger, Arthur, Urteilsanmerkung, BGH: Zugang pornografischer Internetangebote über ein unzureichendes AVS – ueber18.de. MMR Heft 6, 2008, 400–408.

– Teledienste, Mediendienste und die „Verantwortlichkeit" ihrer Anbieter. MMR Heft 3, 1998, 124–129.

Wang, Aixian, Die Untersuchung zu § 287 II StGB aus der Sicht von „Gehilfe zu Täter"(帮助行为正犯化). Zeitschrift der Universität Henan (Sozialwissenschaftliche Ausgabe) (河南大学学报-社会科学版) Heft 2, 2017, 39–47.

Wang, Bingbing, Die Kritik an dem „Teilnehmer zum Täter". Kommentar zu § 287 Abs. 2 StGB. Zeitschrift der Universität Suzhou (Rechtswissenschaftliche Ausgabe) (苏州大学学报-法学版) Heft 1, 2017, 98–106.

Wang, Guan, Die finale Lösung zum Problem der Kriminalität durch Deep Links. Rechtswissenschaft (法学) Heft 9, 2013, 142–151.

Wang, Lin, Die dogmatische Gestaltung der strafrechtlichen Verantwortlichkeit von Beteiligung in der Cyberkriminalität. Ein wiederkehrender Zurechnungsmodus im Rahmen der Beteiligung. Politik und Recht (政治与法律) Heft 9, 2016, 30–42.

Wang, Liming, Das *notice and take down*-Prinzip für die Rechtsverletzung im Netzwerk. Nördliche Rechtswissenschaft (北方法学) Heft 2, 2014, 34–44.

– Die Untersuchung des Deliktsrechts II (侵权责任法研究-下). Peking 2011.

Wang, Liming (Hrsg.), Erläuterungen zum chinesischen Deliktsrecht (中华人民共和国侵权责任法释义). Peking 2010.

Wang, Qian, Die Geltung des *safe harbor*-Prinzips in der „Verordnung über den Schutz des Informationsnetz-Übertragungsrechts". Rechtswissenschaft (法学) Heft 6, 2010, 128–140.

– Die Bestimmung der direkten Urheberrechtsverletzung im Netzwerk. Orientalisches Recht (东方法学), Heft 2, 2009, 12–21.

– Untersuchung zur Urheberrechtsverletzung einer Video-Sharing Website. Studium des Rechts und der Wirtschaft (法商研究), Heft 4, 2008, 42–53.

– Die Hyperlinksetzung und die mitwirkende Rechtsverletzung, Kommentar zum Urteil der ersten Instanz des *Yahoo*-Falls. China Invention & Patent (中国发明与专利) Heft 7, 2007, 14–15.

– Untersuchung zur Bestimmung der indirekten Rechtsverletzung des Anbieters von Informations- und Lokalisationswerkzeugen. Ein Vergleich zwischen den Urteilen des *Baidu*-Falls und des *Yahoo*-Falls. Geistiges Eigentum (知识产权) Heft 4, 2007, 3–11.

– Die Bestimmung der indirekten Rechtsverletzung des Anbieters von Informations- und Lokalisationswerkzeugen. Geistiges Eigentum (知识产权) Heft 1, 2006, 11–18.

– Die Haftung der mitwirkenden Verletzung von Betreibern der P2P-Software. Elektronisches geistiges Eigentum (电子知识产权) Heft 9, 2005, 52–56.

– Die Herausforderungen von neuer P2P-Technologie im Kontext der traditionellen Theorie von indirekter Urheberrechtsverletzung. Elektronisches geistiges Eigentum (电子知识产权) Heft 11, 2004, 30–33, 48.

Wang, Qian, Rückblick, Reflexionen und Lehren des *Sony*-Falls. Zeitschrift für Wissenschaft, Technologie und Recht (科技与法律) Heft 4, 2004, 59–68.

Wang, Shengming (Hrsg.), Erklärungen zum chinesischen Deliktsrecht (中华人民共和国侵权责任法释义). Peking 2010.

Wang, Wenhua, Analyse der Anwendung des § 286 Abs. 1 StGB „Verweigerung der Erfüllung der Sicherheitsverpflichtungen im Informationsnetzwerk". Volksstaatsanwaltschaft (人民检察) Heft 6, 2016, 24–27.

Wang, Ying, Die Einordnung des theoretischen Systems der Garantenpflichten bei vorangegangenem Tun. Rechtszeitschrift der Universität Peking (中外法学) Heft 2, 2013, 325–346.

– Über die Garantenstellung aus Ingerenz. Der Jurist (法学家) Heft 2, 2013, 119–129.

Wang, Yu, Qualitative und quantitative Instrumente zur Einschränkung der Strafverfolgung bei fehlendem Strafbedürfnis, Ein deutsch-chinesischer Rechtsvergleich. Berlin 2014.

Wang, Yufei, Die Abgrenzung zwischen Strafrecht und Zivilrecht bei Deep Links. Urheberrecht in China (中国版权) Heft 4, 2014, 48–52.

Weigend, Thomas, Grenzen strafbarer Beihilfe. In: Albin Eser (Hrsg.), Festschrift für Haruo Nishihara zum 70. Geburtstag. Baden-Baden 1998, 197–214.

Weng, Mingjiang/Wu, Lei, Der Napster-Fall und seine Einflüsse auf das amerikanische Urheberrechtsgesetz. Recht und soziale Entwicklung (法制与社会发展) Heft 2, 2002, 144–156.

Wessels, Johannes/Beulke, Werner, Strafrecht. Allgemeiner Teil. Die Straftat und ihr Aufbau. 38. Aufl. Heidelberg 2008.

Wissenschaftliche Dienste des Bundestags, Rechtliche Reaktionsmöglichkeiten auf „Internetpiraterie", Darstellung der Instrumente im Hinblick auf Nutzer und Betreiber von Anwendungen, welche zum Austausch urheberrechtlich geschützten Materials genutzt werden können, WD 10 – 3000/094-12, 2012.

Wohlleben, Marcus, Beihilfe durch äußerlich neutrale Handlungen. München 1996.

Wu, Handong, Das Gesetzgebungsprogramm und der Inhalt des Entwurfs der dritten Veränderung des Urheberrechtsgesetzes. Geistiges Eigentum (知识产权) Heft 5, 2012, 13–18.

– Die Haftung der Urheberrechtsverletzung von ISP. Chinesische Rechtswissenschaft (中国法学) Heft 2, 2011, 38–47.

– Die Analyse der Deliktshaftung im Netzwerk aus dem Deliktsrecht. Studium des Rechts und der Wirtschaft (法商研究) Heft 6, 2010, 28–31.

Wu, Weiguang, Die Verantwortlichkeit der ISP für die Rechtsverletzung seines Nutzers. Die unveränderte Institution des *Gatekeepers* und das veränderte Sorgfaltspflichtkriterium. Internet-Rechtszeitschrift (网络法律评论) Heft 1, 2011, 17–32.

Xiang, Chaoyang/Yue, Yang, Die Skepsis gegenüber der Legitimität der Vorsatz-Fahrlässigkeit-Kombination. Law Review (法学评论) Heft 3, 2005, 53–59.

Xie, Guanbin/Shi, Xueqing, Die Haftungsbestimmungen der Suchmaschinenbetreiber, Kommentar zu den Urteilen erster Instanz des *Yahoo*-Falls und des *Baidu*-Falls. Geistiges Eigentum (知识产权) Heft 1, 2008, 81–86.

Xie, Lanfang/Fu, Qiang, Die Diskussion über die Kriterien der Rechtsverletzung von Deep Links. Geistiges Eigentum (知识产权) Heft 11, 2016, 41–45.

Xie, Shaohua, Die Materialisierung des Ursprungs der Garantenpflichten. Forum der Politikwissenschaft und des Rechts (政法论坛) Heft 2, 2008, 133–141.

Xie, Wangyuan, Die Untersuchung zum § 286 Abs. 1 StGB – „Verweigerung der Erfüllung der Sicherheitsverpflichtungen im Informationsnetzwerk". Chinesische Rechtswissenschaft (中国法学) Heft 2, 2017, 238–255.

Xie, Xiren (Hrsg.): Computer-Netzwerk. 5th edition Peking 2008.

Xiong, Qi, Die Erweiterung und Einschränkung der indirekten Verantwortung des Urheberrechts. Geistiges Eigentum (知识产权) Heft 6, 2009, 66–73.

Xiong, Yawen/Huang, Yazhu, Die gerichtliche Anwendung des § 287 Abs. 2 StGB. Volksjustiz (人民司法) Heft 31, 2016, 75–79.

Xu, Huili, Die Rechtsrisiken im Kontext des Cloud-Computing aus der Perspektive der Datensicherheit. Technologie und Recht (科技与法律) Heft 6, 2013, 1–9.

Xu, Songlin, Die strafrechtliche Regulierung von Deep Links in Video Search Websites. Geistiges Eigentum (知识产权) Heft 11, 2014, 26–31.

Xu, Wei, Die neue Auslegung des „Wissens" von ISP. Kritik an der Lehre vom „Kennenmüssen". Wissenschaft des Rechts (法律科学) Heft 2, 2014, 163–173.

– Das neue Verständnis für das *notice and take down*-Verfahren. Moderne Rechtswissenschaft (现代法学) Heft 1, 2013, 58–70.

Xue, Hong, Die Haftung der Urheberrechtsverletzung der ISP. Technik und Recht (科技与法律) Heft 1, 2000, 49–57.

Yan, Erpeng, Reflexion auf den „Gehilfe zum Täter"-Ansatz (帮助犯正犯化) aus dogmatischer Sicht, Kommentar zu dem Strafrechtsänderungsgesetz (IX). Sozialwissenschaftliche Zeitschrift (社会科学辑刊) Heft 4, 2016, 73–79.

Yan, Erpeng/Mei, Teng, Die Untersuchung der Kriminalität der Deep Links aus Sicht einer gemeinschaftlichen Handlungslehre. Jianghai akademische Zeitschrift (江海学刊) Heft 4, 2015, 131–137.

Yang, Caixia, Die strafrechtliche Regulierung der Deep Links von Suchmaschinen aus der Perspektive von Sollen und Sein. Zeitschrift der Nordöstlichen Universität (Sozialwissenschaftliche Ausgabe) (东北大学学报-社会科学版) Heft 3, 2017, 292–304.

– Die Untersuchung der strafrechtlichen Verantwortlichkeit für Urheberrechtsverletzung der Betreiber von P2P-Netzwerken – Basierend auf der technischen Struktur der P2P-Netzwerke. Politik und Recht (政治与法律) Heft 3, 2016, S .42–53.

– Neue Forschung zur Unterlassung der Cyberkriminalität. Der Sucher (求索) Heft 2, 2007, 96–98.

Yang, Chunxi/Yang, Dunxian (Hrsg.), Chinesische Strafrechtswissenschaft (中国刑法论). 2. Aufl. Peking 1998.

Yang, Hui/Ma, Ning, Die Regel der positiven Verleitung, Das neue Kriterium der Rechtsverletzung der P2P-Betreiber aus dem *Grokster*-Fall. Elektronisches geistiges Eigentum (电子知识产权) Heft 8, 2005, 49–52.

Yang, Lixin/Li, Jialun, Das *counter notification*-Verfahren und seine Wirkung für die Rechtsverletzung im Netzwerk. Wissenschaft des Rechts (法律科学), Heft 2, 2012, 157–164.

Yang, Lixin, Das Verständnis und die Interpretation der Deliktshaftung im Netzwerk im Rahmen des Deliktsrechts. Zeitschrift des nationalen Staatsanwalts-Instituts (国家检察官学院学报), Heft 2, 2010, 3–10.

Yang, Ming, Die Erläuterung des § 36 Deliktsgesetz. Zeitschrift der östlichen Universität in China für Politik- und Rechtswissenschaft (华东政法大学学报), Heft 3, 2010, 123–132.

Yang, Shuwen, Der Grundriss der Vorsatz-Fahrlässigkeit-Kombination. Peking 2004.

Yang, Yong, Die Untersuchung zu einer rechtlichen Regulierung der Deep Links. Chinesisches Urheberrecht (中国版权), Heft 1, 2015, 53–59.

Yao, Wenping, Die Internet-Finanz, die kommende neue Epoche der Finanz. Peking 2014.

Ye, Qi, Die strafrechtliche Verantwortlichkeit des Unterlassens von Internet Content Providern. Eine Analyse der Straftat durch BBS. Zeitschrift der Shanghaier Akademie für öffentliche Sicherheit (上海公安高等专科学校学报), Heft 4, 2005, 77–79, 96.

You, Chunliang, Die vorherige Verpflichtung zur Überprüfung soll den ISP gegeben werden. Legal Daily (法制日报), 005, 27.10.2008.

Yu, Chong, Die normative Erläuterung und theoretische Reflexion des „Gehilfens zum Täter" (帮助犯正犯化) in der Cyberkriminalität. Kriminalwissenschaft (中国刑事法杂志), Heft 1, 2017, 80–93.

Yu, Haisong, Die gesetzgeberische Erweiterung und gerichtliche Praxis zur Bekämpfung der Cyberkriminalität. Zeitschrift der Rechtsanwendung (法律适用), Heft 9, 2016, 2–10.

Yu, Zhigang, Das Sanktionssystem der Beihilfe im Cyberspace und seine Reform. Chinesische Rechtswissenschaft (中国法学), Heft 2, 2016, 5–24.

– Die Evolution des Netzwerk- und Sanktionsdenkens in der Cyberkriminalität. Rechtszeitschrift der Universität Peking (中外法学), Heft 4, 2014, 1045–1058.

– Die Untersuchung zur Entfremdung der traditionellen Straftaten im Netzwerk (传统犯罪的网络异化研究). Peking 2010.

– Die strafrechtliche Bewertung der böswilligen Hyperlinks von Suchmaschinen. Volksstaatsanwaltschaft (人民检察), Heft 12, 2010, 6–10.

– Die Cyberkriminalität und die Behandlung des chinesischen Strafrechts. Sozialwissenschaften in China (中国社会科学), Heft 3, 2010, 109–126.

Zang, Tiewei (Hrsg.), Erläuterungen über das Strafrechtsänderungsgesetz (IX) (中华人民共和国刑法修正案九解读). Peking 2015.

Zhang, Lingling, Die Untersuchung zur Deliktshaftung von Betreibern der P2P-Netzwerke. Geistiges Eigentum (知识产权), Heft 4, 2012, 39–45.

Zhang, Mingkai, Strafrechtliche Wissenschaft (刑法学). 5. Aufl. Peking 2016.

– Die Untersuchung des § 287 II StGB. Politik und Recht (政治与法律), Heft 2, 2016, 2–16.

– Eine kurze Analyse des Urteils des *Kuaibo*-Falls. Volksgerichtszeitung (人民法院报), A003, 14.09.2016.

– Das vorangegangene Tun im Unterlassungsdelikt. Chinesische Rechtszeitschrift (法学研究), Heft 6, 2011, 136–154.

– Strafrechtliche Wissenschaft (刑法学). 4. Aufl. Peking 2011.

– Befürwortung des Begriffs von „überschießenden objektiven Merkmalen". Chinesische Rechtszeitschrift (法学研究), Heft 3, 1999, 22–31.

– Erläuterungen über strafrechtliche Prinzipien (刑法格言的展开). Peking 1999.

Zhang, Xiaona, Erklärungen des nationalen Volkskongresses zum Strafrechtsänderungsgesetz (IX). Zeitung für Demokratie und Recht (民主与法制时报), 15.11.2015.

Zhang, Xinbao/Ren, Hongyan, Die Deliktshaftung im Internet, Erläuterungen zum § 36 des Deliktsgesetzes. Zeitschrift der Universität Renmin (中国人民大学学报), Heft 4, 2010, 17–25.

Zhao, Yuan, Die strafrechtliche Verantwortlichkeit der ISP in der Cyberkriminalität. Legal Daily (法制日报), A011, 23.07.2014.

Zhou, Guangquan, Tatherrschaft oder Pflichtverletzung? Die Untersuchung zu den Gründen des Urteils vom *Kuaibo*-Fall. Rechtszeitschrift der Universität Peking (中外法学), Heft 1, 2017, 51–67.

– Die Begründung der aktiven strafrechtlichen Gesetzgebung in China. Chinesische Rechtszeitschrift (法学研究), Heft 4, 2016, 23–40.

– Strafrecht Allgemeiner Teil. 3. Aufl. Peking 2016.

– Einige strittige Fragen im Entwurf des Strafrechtsänderungsgesetzes (IX). Rechtswissenschaftliche Zeitschrift (法学杂志), Heft 5, 2015, 77–84.

– Der Umfang der strafrechtlichen Verantwortlichkeit von ISP. China Law Review (中国法律评论), Heft 2, 2015, 175–178.

– Strafrecht Allgemeiner Teil. 2. Aufl. Peking 2011.

– Über die „hauptsächliche *mens rea*". Moderne Rechtswissenschaft (现代法学), Heft 2, 2007, 38–48.

Zhu, Jianjun/Tan, Minghua, Haftungsbestimmungen der indirekten Rechtsverletzung von Betreibern der P2P-Netzwerke. Geistiges Eigentum (知识产权), Heft 1, 2009, 45–49.

Zou, Bingjian, „Kennen" bedeutet nicht unbedingt Vorsatz. Diskussion über das „Kennen" im StGB. Rechtszeitschrift der Universität Peking (中外法学), Heft 5, 2015, 1349–1375.

Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht

Die zentralen Veröffentlichungen des Max-Planck-Instituts für ausländisches und internationales Strafrecht werden in Zusammenarbeit mit dem Verlag Duncker & Humblot in den folgenden sechs Unterreihen der „Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht“ vertrieben:

- „Strafrechtliche Forschungsberichte“
- „Kriminologische Forschungsberichte“
- „Interdisziplinäre Forschungen aus Strafrecht und Kriminologie“
- „Publications of the Max Planck Partner Group for Balkan Criminology“
- „Series of the Max Planck Institute for Foreign and International Criminal Law and Bahçeşehir University Joint Research Group“
- „Sammlung ausländischer Strafgesetzbücher in Übersetzung“

Diese Publikationen können direkt über das Max-Planck-Institut unter <www.mpicc.de> oder über den Verlag Duncker & Humblot unter <www.duncker-humblot.de> erworben werden. Darüber hinaus erscheinen in der Unterreihe „research in brief“ zusammenfassende Kurzbeschreibungen von Forschungsergebnissen und in der Unterreihe „Arbeitsberichte“ Veröffentlichungen vorläufiger Forschungsergebnisse. Diese Veröffentlichungen können über das Max-Planck-Institut bezogen werden.

Detaillierte Informationen zu den einzelnen Publikationen des Max-Planck-Instituts für ausländisches und internationales Strafrecht sind unter <www.mpicc.de> abrufbar.

The main research activities of the Max Planck Institute for Foreign and International Criminal Law are published in the following six subseries of the “Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht” (Research Series of the Max Planck Institute for Foreign and International Criminal Law), which are distributed in cooperation with the publisher Duncker & Humblot:

- “Strafrechtliche Forschungsberichte” (Reports on Research in Criminal Law)
- “Kriminologische Forschungsberichte” (Reports on Research in Criminology)
- “Interdisziplinäre Forschungen aus Strafrecht und Kriminologie” (Reports on Interdisciplinary Research in Criminal Law and Criminology)
- “Publications of the Max Planck Partner Group for Balkan Criminology”
- “Series of the Max Planck Institute for Foreign and International Criminal Law and Bahçeşehir University Joint Research Group”
- “Sammlung ausländischer Strafgesetzbücher in Übersetzung” (Collection of Foreign Criminal Laws in Translation)

These publications can be ordered from the Max Planck Institute at <www.mpicc.de> or from Duncker & Humblot at <www.duncker-humblot.de>. Two additional subseries are published: “research in brief” contains short reports on results of research activities, and “Arbeitsberichte” (working materials) present preliminary results of research projects. These publications are available at the Max Planck Institute.

Detailed information on all publications of the Max Planck Institute for Foreign and International Criminal Law can be found at <www.mpicc.de>.

Max-Planck-Institut für ausländisches
und internationales Strafrecht

G 126 **Strafgesetzbuch der Tschechischen Republik – Trestní zákonik České republiky**
Deutsche Übersetzung von Susanne Altmann
Einführung von Helena Valková, Josef Kuchta, Petr Bohata
Zweisprachige Ausgabe
2017 • 430 Seiten • ISBN 978-3-86113-789-4 € 50,00

G 125 **Die türkische Strafprozessordnung – Ceza Muhakemesi Kanunu**
Deutsche Übersetzung und Einführung von Mehmet Arslan
Zweisprachige Ausgabe
2017 • 289 Seiten • ISBN 978-3-86113-792-4 € 48,00

Auswahl aus dem strafrechtlichen Forschungsprogramm:

S **128.1.1** *Ulrich Sieber / Konstanze Jarvers / Emily Silverman* (eds.)
National Criminal Law in a Comparative Legal Context
Volume 1.1: Introduction to National Systems
2013 • 314 Seiten • ISBN 978-3-86113-822-8 € 40,00

S 128.1.2 Volume 1.2: Introduction to National Systems
2013 • 363 Seiten • ISBN 978-3-86113-826-6 € 43,00

S 128.1.3 Volume 1.3: Introduction to National Systems
2014 • 297 Seiten • ISBN 978-3-86113-818-1 € 40,00

S 128.1.4 Volume 1.4: Introduction to National Systems
2014 • 391 Seiten • ISBN 978-3-86113-810-5 € 43,00

S **128.2.1** *Ulrich Sieber / Susanne Forster / Konstanze Jarvers* (eds.)
National Criminal Law in a Comparative Legal Context
Volume 2.1: General limitations on the application of criminal law
2011 • 399 Seiten • ISBN 978-3-86113-834-1 € 43,00

S 128.2.2 *Ulrich Sieber / Konstanze Jarvers / Emily Silverman* (eds.)
National Criminal Law in a Comparative Legal Context
Volume 2.2: General limitations on the application of criminal law
2017 • 272 Seiten • ISBN 978-3-86113-798-6 € 35,00

S **128.3.1** *Ulrich Sieber / Susanne Forster / Konstanze Jarvers* (eds.)
National Criminal Law in a Comparative Legal Context
Volume 3.1: Defining criminal conduct
2011 • 519 Seiten • ISBN 978-3-86113-833-4 € 46,00

S 128.3.2 *Ulrich Sieber / Konstanze Jarvers / Emily Silverman* (eds.)
National Criminal Law in a Comparative Legal Context
Volume 3.2: Defining criminal conduct
2017 • 370 Seiten • ISBN 978-3-86113-790-0 € 43,00