Die Regulierung rechtswidriger Informationen im Internet unter besonderer Berücksichtigung von Sperrmaßnahmen gegen Access-Provider

–

Vergleich zwischen Deutschland und China

Zha Yunfei • 查云飞

Universität Münster

7. August 2019

Erster Berichterstatter: Prof. Dr. Bernd Holznagel

Zweiter Berichterstatter: Prof. Dr. Hartmut Bauer

Dekan/in: Prof. Dr. Klaus Boers

Tag der mündlichen Prüfung: 10.12.2019

Inhaltsübersicht

Inhaltsverzeichnis

1. Kapitel EINLEITUNG

A. Herausforderung des globalen Internet und Regulierung der Online-Informationen

Das Internet ist vom Moment seiner Erfindung an global und nach dem Entstehungskonzept von der Billigkeit, Interaktivität, Offenheit, Anti-Kontrolle, Anonymität und Allgegenwärtigkeit geprägt.[1] Euphorisch wird es oft als „revolutionäre Technologie“[2], oder „ein neues kollektives Phänomen“[3] bezeichnet. Der Cyberraum ist gleichzeitig aber auch – zugespitzt formuliert – ein Paradies für Gesetzesbrecher. Die Schattenseite des Internet gewinnt nicht nur durch Cyberangriffe von Staaten, Terrorismus oder grenzüberschreitender organisierter Kriminalität an Relevanz, sondern auch durch alltägliche, weniger schwere (Cyber-)Delikte, die sich gegen Rechtsgüter von öffentlichen und privaten Akteuren richten.[4] Auch darf nicht außer Acht gelassen werden, dass nun fast sämtliche kritische Infrastrukturen, wie Anlagen der Energie, Telekommunikation, des öffentlichen Verkehrs, des Finanz- und Gesundheitswesens usw. an das Internet angeschlossen sind. Sie können – wofür sich bereits in der Vergangenheit Empirie findet – aufgrund von gegen sie ausgerichteten Cyberangriffen versagen.[5] Das Internet darf demnach heutzutage kein digitaler Freiraum mehr bleiben.[6]

---

1 *Boehme-Neßler*, ZÖR 2009, 145 (149 ff.); *Herrera*, 67 (69); *Hornig*, ZUM 2001, 846 (847); *Christiansen*, MMR 2000, 123 (123 f.); *Engel*, 3 ff.; *Thiel*, in: Der Begriff der Souveränität in der transnationalen Konstellation, 215 (217 f.); *Perritt*, 5:2 Ind. J. Global Legal Stud. 423 (426); *Goldsmith/Wu*, 23; *Greve*, 29.

2 *Post*, 5 Ind. J. Global Legal Stud. 521 (522).

3 *Ladeur*, ZUM 1997, 372 (376).

4 *Germann*, 38 ff.; *Schulze*, 24 ff.; *Cornils*, in: VVDStRL (76), 416 ff.; *Herrera*, 67 (72 ff.); *Grewlich*, 18; *Engel*, 41 f.; *Hoffmann-Riem*, in: Neue Macht- und Verantwortungsstrukturen in der digitalen Welt, 27 (31 f.); die Situation in China, siehe *CNCERT*, 15 ff., abrufbar unter <http://www.cert.org.cn/publish/main/upload/File/2015annualreport.pdf> [Stand: 7.8.2019].

5 *Schulze*, 20 f.; Hoffmann-Riem, in: Neue Macht- und Verantwortungsstrukturen in der digitalen Welt, 27 (32); *Yu Zhigang*, Legal Forum 2014/6, 5 (8); die Situation in China, siehe *CNCERT*, 26 ff., abrufbar unter <http://www.cert.org.cn/publish/main/upload/File/2015annualreport.pdf> [Stand: 7.8.2019].

6 *Thiel*, in: Der Begriff der Souveränität in der transnationalen Konstellation, 215 (215); *Herrera*, in: Power and security in the information age, 67 (76 ff.); *Cornils*, in: VVDStRL (76), 397 ff.; *Christiansen*, MMR 2000, 123 (127 ff.); *Greve*, 37 ff.

Besonders betroffen sind auch die im Cyberspace kursierenden Informationen, die im Duktus der Internetgemeinde teilweise als Rohstoff, Wirtschaftsgut oder Währung bezeichnet werden.[7]

Sie können einerseits mithilfe vielfältiger Kommunikationsangebote zur Willensbildung des Gemeinwesens beitragen. Im Zeitalter von Web. 2.0 führt das sog. self-media dazu, dass sowohl massive interpersonelle Vernetzung sowie die Publikation eigenen Wissens auf sozialen Medien, als auch ein Austausch mitanderen Netizens – Net Citizens – stattfindet.[8] Damit wird der Netznutzer ein Informationshersteller, der sich Informationen aus allen möglichen Quellen beschafft, verarbeitet und letztlich auch selbst zur Verfügung stellen kann. Folglich ist im Netz eine Informationsfreizügigkeit entstanden, die einen Informationsaustausch zwischen Bürgerinnen und Bürgern ermöglicht und gleichzeitig die Informationsmonopolisierung und Informationskontrolle vorzubeugen sucht.[9]

Andererseits können die Bereitstellungen, respektive das Teilen von Online-Informationen allerdings auch in der Form von Propagandamitteln, Kinder- und Tierpornographie, extremen Gewaltdarstellungen, Beleidigungen und sonstiger strafbewehrter Handlungsweisen rechtswidrig sein, sodass die öffentliche Gewalt dem Informationsfluss nicht völlig freien Lauf lassen darf.

B. Netz- und Inhaltsregulierung vor dem Hintergrund der Ent- und Reterritorialisierung

Kein anderes Thema ist wie das Internet und das sog. Internetrecht so eng mit dem Aspekt der Ent- und Reterritorialisierung verbunden.[10] Strukturell stammt das Internet aus dem ARPANET, das ursprünglich in den 1960er in den US für militärische Zwecke geschaffen und verwendet wurde. Anfang der 1980er Jahre wurde das ARPANET teilweise privatisiert und war danach im Rahmen der TCP/IP Pro-

---

7 *Schoch*, FS Stern, 1491 (1501); *Grewlich*, 18; Rossi, in: Informationen der öffentlichen Hand - Zugang und Nutzung, 145 (160 f.).

8 *Roßnagel*, in: Zur Reichweite der staatlichen Verantwortung für Teilhabe in der digitalen Zeit, 74; zur Web 2.0 und Demokratie, Kersten, Schwarmdemokratie, 20 ff.; Christiansen, MMR 2000, 123 (128).

9 *Grewlich*,18; *Roßnagel*, in: Zur Reichweite der staatlichen Verantwortung für Teilhabe in der digitalen Zeit, 81; *Hobe*, 286; *Greve*, 30.

10 *Engel*, 34; *Thiel*, 22; *Hobe*, 381 ff.

tokoll weltweit anschlussfähig, sodass andere Länder nach dem Vorbild des amerikanischen ARPANET eigene Netzwerke aufbauten, die ihrerseits an das ARPANET angeschlossen wurden.[11]

I. Die Rolle des ICANN

Als Netzwerk der Netzwerke gilt das Internet anders als das nationale Telekommunikationsnetz strukturell von Anfang an grenzenlos und transnational.[12] Als Beispiel sei die Internet Corporation for Assigned Names and Numbers (ICANN), welche für die weltweite Verteilung von Domainnamen und IP-Adressblöcken zuständig ist, genannt. Bei dieser 1988 privatrechtlich gegründeten Gesellschaft sollte die Selbstregulierung und der „Multistakeholderism" als Grundsatz gelten.[13] Hierbei wird allerdings zum einen kritisiert, dass die ICANN-Struktur die Souveränität der Nationalstaaten nicht beachte und daher nicht legitimiert sei, und zum anderen ist fraglich, ob die ICANN tatsächlich von einem souveränen Staat unabhängig ist, da sie doch in den USA registriert ist. Sie wird hauptsächlich aus amerikanischen Organisationen und Unternehmen gebildet und ist, so wird vermutet, massiv von den Interessen der US-amerikanischen Internetindustrie und Administration abhängig.[14] Angesichts der National Security Agency-Affäre (NSA-Affäre) verliert schließlich die US-geführte Administration des Internets mehr und mehr das Vertrauen anderer Länder und der allgemeinen Nutzerschaft.[15]

Durch das wirtschaftliche Aufschließen der sog. „Schwellenländer" zu den sog. „Industrieländern" stellt sich die geopolitische Situation als fundamental divergierend zu der der 60er Jahre des vergangenen Jahrhunderts dar. Mittlerweile wird vermehrt Hoffnung auf eine effektive Netzregulierung durch die Nationalstaaten gesetzt. Im Rahmen des „World Summit on Internet Governance" (WSIG), dessen

---

11 *Fang*, Einleitung 2; *Huang*, 196; *Liu Han*, Peking University Law Journal 2016/2, 518 (525); *Cornils*, in: VVDStRL (76), 391 (413); Greve, 27 f.

12 Im Gegenteil wurde das Telekommunikationsnetz zuerst vom Nationalstaat aufgebaut und sich später durch Verträge miteinander angeschlossen, wobei die internationale Organisation -International Telecommunication Union (ITU) - eine wichtige Rolle spielt, Fang, Einleitung 1 f.

13 *Cornils*, in: VVDStRL (76), 391 (413); Huang, 198; kritisiert von Fang, 113.

14 *Fang*, Einleitung 2; *Cornils*, in: VVDStRL (76), 391 (414 f.); *Huang*, 222; *Mueller*, 61 f.; *Yu Zhigang*, Legal Forum 2014/6, 5 (14).

15 Baldwin/Cave/Lodge (ed.), § 21 Rn. 524; *Heidrich/Wegener*, MMR 2015, 487 (487); *Taeger*, NJW 2013, 3698 (3698); *Kühling*, NJW 2014, 681 (683); *Ewer/Thienel*, NJW 2014, 30 (30 f.).

Vorläufer der „World Summit on Information Society" war, fand ein gleichberechtigter Diskurs über Netzthemen zwischen Nationalstaaten statt. Dabei wurden die Bestrebungen einiger Schwellenländer offenkundig, das einpolige System des Internet-Governance hin zu einem mehrpoligen *Multistakeholderism* umzuwandeln.[16] Anders als der Multistakeholderism des ICANN, der private Organisationen und Industrieunternehmen als Regulierungssubjekt hat, bezieht sich der Multistakeholderism hierbei auf Nationalstaaten. Des Weiteren haben die bestehenden globalen Organisationen wie ICANN, Internet Engineering Task Force (IETF), The Internet Society (ISOC), Internet Architecture Board (IAB) und das World Wide Web Consortium (W3C) sowie die fünf regionalen Internet-Register (ANIC, ARIN, APNIC, LACNIC und RIPE NCC) auf die Enthüllung der vom US-amerikanischen NSA geführten PRISM reagiert und zusammen am 7.10.2013 in Uruguay das „Montevideo Statement on the Future of Internet Cooperation" abgegeben, in dem ebenfalls zur *gemeinsamen* Regulierung des Cyberspace aufgerufen wurde.[17] Hier wird auch die Erforderlichkeit der Zusammenarbeit der Nationalstaaten betont, mit der Folge, dass die Netzregulierung von der Entterritorialisierung zur Reterritorialisierung zurückkehrt – die fundamentale Voraussetzung einer wie auch immer gearteten internationalen Kooperation.

II. Multinationale Sachverhalte

Die gleiche Frage nach Machtmonopolisierung oder -diversifizierung könnte auch in Bezug auf die Inhaltsregulierung im Netz gestellt werden. Handelt es sich in Internet-Multi-State-Fällen um die Regulierung von Inhalten, ist die stets Frage nach der Jurisdiktion entscheidend. Einer der bekanntesten Fälle ist im Jahr 2000 durch das Tribunal de grande instance de Paris zwischen einem jüdischen Studentenverband (L'Uejf), einem internationalen Verein für Antirassismus und gegen Antisemitismus (La Licra) und der Firma Yahoo (sowohl Yahoo! Inc. als auch Yahoo.fr) entschieden worden. L'Uejf und La Licra forderten zuerst Yahoo! Inc. auf, die in den USA online durchgeführte Auktion über Nazi-Devotionalien zu

---

16 Zur „Tunis Agenda For The Information Society, abrufbar unter <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html> [Stand: 7.8.2019]; *Liu Han*, Peking University Law Journal 2016/2, 518 (531 ff.); Internet Governance wurde 1998 von „International Telecommunication Union (ITU)" zuerst herausgebracht, *Brousseau/Marzouki*, 369.

17 Zur „Montevideo Statement on the Future of Internet Cooperation", abrufbar unter <https://www.icann.org/news/announcement-2013-10-07-en> [Stand: 7.8.2019] .

unterlassen und forderten gleichzeitig Yahoo.fr auf, den Link zur betroffenen Auktion zu entfernen.[18] Das Kernproblem hierbei war kompetenzieller Natur: Warum sollte ein französisches Gericht Jurisdiktion über einen Rechtsstreit einer in den USA stattgefundenen (und dort legalen Auktion) und deren Vereinbarkeit mit französischem Recht ausüben können?. Relevant wird in diesem Zusammenhang etwa die sog. „long-arm-jurisdiction"-Regel.[19] Im Yahoo-Fall hat das französische Gericht die eigene Zuständigkeit bejaht, da Yahoo.fr den Nutzern in Frankreich die Möglichkeit anbot, dass sie durch den Link zur Auktion in den USA die Webseite besuchen konnten. Noch im Jahr 2000 hat das Gericht dann das Urteil ausgesprochen, dass Yahoo! Inc. jede mögliche technische Maßnahme treffen muss, um das Aufsuchen der betroffenen Website durch französische Nutzer zu verhindern.[20] In einem weiteren Schritt der Eskalation erhob Yahoo! Inc. gegen dieses Urteil Klage; diesmal vor dem Bezirksgericht in Nordkalifornien.[21] Richter Jeremy Fogel entschied im Sinne der Yahoo! Inc., dass eine Gerichtsentscheidung eines französischen Gerichts in den USA keine Geltung beanspruche, es sei nicht

---

18 Hierzu die Zusammenfassung des Urteils des Tribunal de grande instance de Paris, abrufbar unter: <https://www.dalloz.fr/documentation/Document?id=TGI_LIEUVIDE_2000-05-22_XTGIP220500X&ctxt=0_YSR0MT1UcmlidW5hbCBkZSBncmFuZGUgaW5zdGFuY2UgUGFyaXPCp3gkc2Y9c2ltcGxlLXNlYXJjaA==&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PcKncyRzbE5iUGFnPTIwwqdzJGlzYWJvPVRydWXCp3MkcGFnaW5nPVRydWXCp3Mkb25nbGV0PcKncyRmcmVlc2NvcGU9RmFsc2XCp3Mkd29JUz1GYWxzZcKncyRicT3Cp3Mkej1EQVRFLzIwMDBgMjAwMC8wNQ==&nrf=0_TGlzdGVEZVJlc3VsdGF0R2xvYmFs> [Stand: 7.8.2019]; Tribunal de grande instance de Paris, 11 août 2000, UEJF-LICRA c/ Yahoo ! Inc. et Yahoo France, abrufbar unter: <https://www.dalloz.fr/documentation/Document?id=A56180&ctxt=0_YSR0MT1UcmlidW5hbCBkZSBncmFuZGUgaW5zdGFuY2UgUGFyaXPCp3gkc2Y9c2ltcGxlLXNlYXJjaA==&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1UcnVlwqdzJHNvcnQ9wqdzJHNsTmJQYWc9MjDCp3MkaXNhYm89VHJ1ZcKncyRwYWdpbmc9VHJ1ZcKncyRvbmdsZXQ9wqdzJGZyZWVzY29wZT1GYWxzZcKncyR3b0lTPUZhbHNlwqdzJGJxPcKncyR6PTBEQkZDOERCLzE4RTA2NjQzL0ZGOTFGNjM2fERBVEUvMjAwMGAyMDAwLzA4&nrf=0_TGlzdGVEZVJlc3VsdGF0R2xvYmFs> [Stand: 7.8.2019].

19 Zur „long-arm-jurisdiction", *Liu Yanhong*, China Legal Science 2018/3, 89 (96ff.); Guo/Gan, Journal of Comparative Law 2000/3, 266 (266 ff.); *Guo/Xiang*, China Legal Science 2002/6, 156 (156 ff.); *Yu Zhigang*, Legal Forum 2014/6, 5 (19).

20 *Fang*, 104 f.; *Goldsmith/Wu*, 1 ff.; *Engel*, MMR-Beil. 4/2003, 1 (8); *Hoeren*, ZfWG 2008, 311 (314).

21 LICRA, 15 mai 2000: La LICRA contre Yahoo, in: archives.licra, abrufbar unter: <http://archives.licra.org/15-mai-2000-licra-contre-yahoo> [Stand: 7.8.2019].

mit dem amerikanischen Verständnis von Meinungsfreiheit unter dem ersten Verfassungszusatz vereinbar.[22] Die hiergegen eingelegte Berufung beim Curt of Appeals gab wiederum den Rechtsstreitgegnern Recht: Das Gericht führte aus, das bei einer wirtschaftlichen Tätigkeit auf fremdem Territorium auch die Regeln des jeweiligen Staates zu beachten seien.[23]

III. Gemeinsames Vorgehen der Staaten oder individuelle Regelungen in den verschiedenen Staaten („Reterritorialisierung")

Anders als die Netz- oder Strukturregulierung (z.B. Domain- und IP-Adressvergabe) ist die Inhalteregulierung demnach v.a. an die Gesetze und Regeln der Territorialstaaten gebunden, sodass die Diskussion über das Phänomen der Reterritorialisierung hierzu weniger virulent ist.[24] Das bedeutet allerdings nicht, dass in Bezug auf Inhalteregulierung im Netz nationale Lösung allein ausreichen. Angesichts des Phänomens der neuen Many-to-Many Kommunikation, durch die Informationen im Netz explosionsartig verbreitet werden können, ist eine rechtliche Regulierung durch den Staat *allein* nicht zu schaffen, da das Vollzugsdefizit aufgrund von technischen Mängeln und verschiedenen Wertordnungen zwischen Staaten nur schwierig überwunden werden kann.[25] Auch aufgrund knapper personeller sowie finanzieller Ressourcen kann zudem das nationale Recht nur begrenzt erfolgreich durchgesetzt werden.[26] Eine internationale Regulierung des Cyberspace könnte ferner Vorteile mit sich bringen, wenn die Nationalstaaten Abkommen abschließen oder sich auf ein gemeinsames Ziel, zumindest auf der Basis geteilter Grundwerte, verständigen. Internationale und transnationale Regulierung *kann* die

---

22 Federal District Court of Northern California, No. 00-21275 JF, YAHOO! INC., v. LA LIGUE CONTRE LE RACISME ET, L'ANTISEMITISME, et al., abrufbar unter: <http://www.lapres.net/usjurju.html> [Stand: 7.8.2019].

23 US Court of Appeals, 9th Circuit. - 433 F.3d 1199, Yahoo! Inc. v. LICRA and UEJF, abrufbar unter: <https://law.justia.com/cases/federal/appellate-courts/F3/433/1199/546158/> [Stand: 7.8.2019]; LICRA, 15 mai 2000: La LICRA contre Yahoo, in: archives.licra, abrufbar unter: <http://archives.licra.org/15-mai-2000-licra-contre-yahoo> [Stand: 7.8.2019].

24 *Holznagel/Kussel*, MMR 2001, 347 (347 ff.); *Bremer*, MMR 2002, 147 (147); *Grewlich*, 53 f.; *Tang*, 19; Baldwin/Cave/Lodge (ed.), § 21 Rn. 534; *Goldsmith/Wu*, 149 f.

25 *Holznagel/Kussel*, MMR 2001, 347 (350); *Dietlein/Heinemann*, in: Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2003, 395 (396); *Sieber/Nolde*, 2; *Fang*, 114; *Goldsmith/Wu*, 150 ; *Engel*, 4/2003, 1 (7); *Lang*, AöR 2018, 220 (223); *Engel*, 4/2003, 1 (7); *Bremer*, MMR 2002, 147 (148), Kritik dazu *ders*, 147 (149 f.)

26 *Holznagel/Kussel*, MMR 2001, 347 (350); *Schaar*, digma 2015, 40 (41); *Hobe*, 293.

Beschränkungen nationalen Rechts überwinden.[27] Für einen modernen Rechtsstaat muss es das Ziel sein, die internationalen und transnationalen Regelungen anzunehmen ohne gleichzeitig die Selbstständigkeit des eigenen staatlichen Handelns aufgeben zu müssen.

C. Möglichkeit der Inhaltsregulierung des souveränen Staats

I. Die Entwicklung des Internet zum Steuerungsinstrument

Nichtsdestotrotz kann zum heutigen Zeitpunkt internationale und transnationale Inhaltsregulierung im Netz nur im subsidiären Sinne Hilfe leisten kann. Dies führt dazu, dass, wie bereits oben eingehend erörtert, die Staaten die Regulierungsverantwortung zu großen Teilen schultern. Als sich die Informations- und Kommunikationsinfrastrukturen noch in der Anfangsphase befanden, waren die Reaktionsmöglichkeiten der nationalstaatlichen öffentlichen Gewalt wegen begrenzter technischer Steuerressourcen und geringerem Regelungsbedarf begrenzt.[28] Es scheint nicht allzu lange her, dass *Nicholas Negroponte* der ganzen Welt stolz erklärte, wie ein Stück Information in mehreren Datenpaketen in den Kommunikationsnetzen von A nach B übermittelt wird.[29] In den Fokus rückt nun jedoch der Grundsatz der Netzneutralität, unter dem man versteht, dass Daten bei der Übertragung gleichbehandelt und der Zugang zum Internet ohne Diskriminierung ermöglicht werden muss.[30] Dies setzt aber voraus, dass nach jetzigem technischen Stand die Zugangs- und Netzwerkanbieter die „Paketautobahn" sowie darauf gelieferte Datenpakete manipulieren können.

---

27 *Goldsmith*, 5 Ind. J. Global Legal Stud. 475 (478) (1997); *Goldsmith/Wu*, 25 f.; *Perritt*, 5:2 Ind. J. Global Legal Stud. 423 (433 ff.) (1998); *Pichler*, 79 ff.; internationale Kooperation spielt bei der Inhaltsregulierung nur begrenzte Rolle, siehe *Cornils*, in: VVDStRL (76), 391 (427).

28 *Lawrence*, 3; *Christiansen*, MMR 2000,123 (123 f.); *Goldsmith/Wu*, 25.

29 *Negroponte*, 274.

30 *Holznagel/Ricke*, DuD 2011, 611 (611 f.); Greve, in: Netzneutralität in der Informationsgesellschaft, 13 (13); *Tang Zicai/Liang Xiongjian*, 4; *Dong Yuanyuan*, Universität des Journalismus 2011, 57 (57); *Spies/Ufer*, MMR 2015, 91 (91 ff.).

Seitdem der souveräne Staat zur Kontrolle dieser kontroversen virtuellen Welt technische Ansätze entdeckt, traditionale Kontrollmaßnahmen „reterritorialisiert“ [31] hat und „alle Machtstrategien moderner Staatlichkeit [darin] kulminier(t)“[32] sind, ist diese anfängliche staatsfreie Utopia schrittweise zerbrochen.[33] Mit der explosionsartigen Weiterentwicklung der Informations- und Kommunikationstechnik werden sich auch Hoheitsträger des Steuerungspotenzials bewusst; das globale Netz ist heute völlig kontrollierbar.[34] Ein souveräner Staat kann mithilfe der Technik das „arms race“ gegen private Organisationen im Cyberspace gewinnen. Das Internet kann so nach dem Wunsch vor allem autoritärer Staaten der Gewährleistung der vorhandenen Staatsform und der Erhaltung des status quo dienen.[35]

II. Das Internet in autoritären Staaten

Das Internet ist in autoritären Staaten, in denen Grundrechte – allen voran die Meinungsfreiheit – offline kaum entfaltet werden können, ein idealer Raum für die Entfaltung von Freiheit.[36] Auf Internetplattformen frei vermittelte und sekündlich explodierende Datenströme können jederzeit ein autoritäres Regime stürzen, was bereits in der arabischen Welt geschehen ist.[37] Danach können Meinungsäußerungen von Internetnutzern von großer Wirkkraft sein. So wird eine Revolution nicht durch einen Wortführer, sondern zahlreiche Unbekannte organisiert und dann durchgeführt.[38] Ein in der früheren Geschichte nicht vorkommendes Szenario, in dem Bürger oder auch Bürgerinnen furchtlos Kritik gegen die Autorität äußern, eigene Rechte und Interesse verteidigen oder Gerechtigkeit für andere einfordern,

---

31 *Herrera*, in: Power and security in the information age, 67 (75); *Cornils*, in: VVDStRL (76), 397 ff.; *Thiel*, in: Der Begriff der Souveränität in der transnationalen Konstellation, 215 (225); Christiansen, MMR 2000, 123 (127 ff.).

32 *Thiel*, in: Der Begriff der Souveränität in der transnationalen Konstellation, 215 (215).

33 Ebd., 215 (215 ff.); Post., 5 Ind. J. Global Legal Stud. 521 (522); *Franzese*, 64 A. F. L. Rev. 1, 11(11 ff.).

34 *Li Yonggang*, 69 ff; Vergleichbares ist auch bei herkömmlichen Medien geschehen, *He*, Media control in China, 8, 143; *Holznagel/Ricke*, DuD 2011, 611 (611).

35 *Herrera*, in: Power and security in the information age, 67 (76 ff.); *Goldsmith/Wu*, 67; *Grewlich*, 18; *Pichler*, 85.

36 *Li Yonggang*, 149; *Thiel*, in: Der Begriff der Souveränität in der transnationalen Konstellation, 215 (221); *Herrera*, in: Power and security in the information age, 67 (71); *Greve*, 31 ff.

37 *Herrera*, in: Power and security in the information age, 67 (71); *Pelinka*, 40 ff.; *Kersten*, JuS 2017, 193 (193); *Brinkmann*, ZUM 2013, 193 (198).

38 *Wang Yi*, China Newsweek 2004/3, 64 (64); von einer Organisation diffuser Minderheiten spricht *Engel*, 21; weitere zur Menschenschwärme im Internet, siehe *Kersten*, Schwarmdemokratie, 1 ff.

ist dank des Internet möglich. Ein solches Szenario wünscht sich ein autoritäres Regime freilich nicht. Mit Aufbietung aller Kräfte versucht es, die Informationsbeschaffung im Netz zu kontrollieren, den Informationsfluss zu lenken und unerwünschte Inhalte z.B. durch Internetsperren zu verbieten.[39] Ist die Inhaltsregulierung nicht einer verfassungsmäßigen Rechtsordnung unterworfen, bedeutet dies demnach nicht nur den Anfang vom Ende des Internet wie man es in der Anfangszeit kannte,[40] sondern es ist auch sehr wahrscheinlich, dass die Entwicklung hin zu einem freien und demokratischen Staat verhindert wird.[41]

III. Die Entwicklung des Internet in China

Überschaubarer ist der Entwicklungsvorgang des Internet in der Volksrepublik China. Nachdem am 14.9.1987 die erste Email aus China an ein deutsches akademisches Institut gesendet wurde, mussten chinesische Bürger noch sieben Jahren warten, bis sie ihr Zugang zum Internet erhielten. Zunächst wurden fast keine wirkungsvollen Gesetze für das Internet erlassen, weil es auf der einen Seite aufgrund der hohen Kosten sehr wenige Internetznutzer gab und auf der anderen Seite der Staat das Internet noch nicht als Bedrohung für die politische Stabilität ansah. Nach diesen goldenen freien Jahren hörte der Jubel in China über die Erreichung aller Ecken der Welt jäh auf. Bis heute sind tausende von der zentralen Regierung Pekings erlassene Verwaltungsnormen und Verwaltungsregeln in Kraft getreten, die als Internet- oder Informationsrechtsnormen bezeichnet werden.

D. Internetsperren zur Inhaltsregulierung und ihre Funktionsweise – Maßnahmen gegen Access-Provider

Im Mittelpunkt der deutschen und chinesischen Diskussion zur Internetüberwachung stehen Begriffe wie Vorratsdatenspeicherung, Cyberwar, Cyberangriff oder

---

39 *Pichler*, 85; *Grewlich*, 18; *Pelinka*, Jahrbuch Menschenrechte 2010, 30 (46); *Schliesky*, in: Zur Reichweite der staatlichen Verantwortung für Teilhabe in der digitalen Zeit, 97 (106); *Habermas*, in: Ach, Europa, Frankfurt, 138 (138).

40 *Holznagel*, The Huffington Post v. 25.4.2014.

41 *Lawrence*, 5; *Thiel*, in: Der Begriff der Souveränität in der transnationalen Konstellation, 215 (215); *Grewlich*, 18; *Hoffmann-Riem*, in: Neue Macht- und Verantwortungsstrukturen in der digitalen Welt, 27 (32); *Schliesky*: in: Neue Macht- und Verantwortungsstrukturen in der digitalen Welt, 97 (103 ff.).

Cyber-Spionage. Dazu gehören auch sog. Internetsperren, wodurch die Kenntnisnahme der Informationen im Netz erschwert wird.[42] Internetsperren können als geeignetes und effektives Mittel zur Regulierung der Online-Informationen angesehen werden.

Bevor auf die jeweilige rechtliche Analyse eingegangen wird, ist zunächst ein Überblick über die verschiedenen technischen Ansätze zu geben. Das Internet durchbricht die Grenze zwischen souveränen Staaten und stellt demnach enorme Herausforderungen an die Bekämpfung von Cyber-Delikten. Es werden täglich zahlreiche grenzüberschreitende Verbrechen und andere Delikte aufgrund des Verstoßes gegen inhaltliche Gebote und Verbote im Cyberspace begangen. Obwohl im Ausland generierte illegale Inhalte vom nationalen Strafrecht unter bestimmten Umständen erfasst sein können, liegt jedoch ein enormes Vollzugsdefizit vor. Die Effektivität der Bekämpfung hängt im hohen Maße von der internationalen Kooperation und Rechtsangleichung ab. Die Listen von rechtswidrigen Informationen bzw. überhaupt das Verständnis von rechtswidrigen Informationen sind je nach Land sehr unterschiedlich. Im Weiteren liegen die Probleme hier sowohl im juristischen als auch im technischen Bereich.

I. Schlüsselwörter filtern

Proxy-Server, Firewalls oder Deep Packet Inspection (DPI) bieten Möglichkeiten die Kommunikation und das Surfverhalten einzelner Nutzer unmittelbar zu lenken. Anhand eines vorher festgelegten Regelwerks können sensible Inhalte oder URLs in den Datenströmen von der Weiterleitung ausgeschlossen werden, indem ein Reset zwischen den Servern gefälscht wird.[43] Aus Sicht des Kommunikationssenders handelt es sich um eine Ablehnung von der Empfangsseite. Der Besuch einer bestimmten Website wird so unterbunden. Umgehungsmöglichkeiten seitens des

---

42 Zur Balancierung der Interessen Erschwerung des Zugangs und freies Internet, OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 911; *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (2); *Dietlein/Heinemann*, in: Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2003, 395 (395); grundlegend *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (1 ff.); zu Internetsperren in der Schweiz siehe *Schwarzenegger*, in: Arter/Jörg (Hrsg.), Internet-Recht und electronic Commerce Law, 3. Tagungsband, 249 (250 ff.); zu Internetsperren in den USA siehe *ders*, 249 (254 ff.).

43 *Sieber*, 77, 80; OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, Rn. 939; *Tang*, 93 f.; *Yuan*, 5 ff.

Nutzers bestehen im Einsatz von Verschlüsselungen (z.B. SSL[44]) oder Pseudonymisierungen. Beim Filtern der Schlüsselwörter mithilfe von Proxy-Servern wird der Inhaltskontext berücksichtigt, so dass die „positiven" und „negativen" Inhalte ohne weitere Unterscheidung betroffen wären.[45] Eine Sperrung der Zieladresse (URL), wobei jede einzelne Webseite nach der Veröffentlichung rechtswidriger Angebote und nach jeder Einzelentscheidung gesperrt werden muss, wird in der Regel geringere Kollateralschäden herbeiführen.

II. Blockade von IP-Adressen

Eine IP-Adresse (Internet Protocol Address) ist vergleichbar mit einer Telefonnummer. Durch sie kann jedes Gerät einem Internetnutzer zugeordnet werden. Sie ist von einem hierarchisch organisierten Netzwerk (ICANN[46]) vorgegeben und besteht als Binärzahl aus 32 Bit (IPv4) oder aus 128 Bit (IPv6). Erst mit der IP-Adresse erfolgt die Kommunikation zwischen zwei oder mehreren Rechnern. Im Fall einer Blockade von IP-Adressen werden am Router des Access-Providers die Nutzeranfragen an eine bestimmte Adresse nicht weitergeleitet, sodass rechtswidrige Inhalte nicht mehr aufgerufen werden können.[47] Durch einen Wechsel der IP-Adresse, durch einen Wechsel des Access-Providers oder durch die Nutzung von Proxy-Servern ist diese Methode leicht zu umgehen.[48] Die Blockade von IP-Adressen kann dennoch ein Overblocking zur Folge, weil hinter einer einzigen IP-Adresse oftmals zahlreiche Domains gehostet sind.[49]

III. Eingriff am DNS-Server

Da eine IP-Adresse als eine Reihe von Zahlen (z.B. IPv4 Adresse: xxx.xxx.xxx.xxx) dargestellt wird, gibt man als Nutzer aus dem praktischen Grund

---

44 SSL ist die Abkürzung von Secure Sockets Layer und ein Netzwerkprotokoll zur sicheren Übertragung von Daten, siehe *Degen/Emmert*, Elektronischer Rechtsverkehr, § 8 Rn. 412 ff.

45 *Zhou*, Journal of Intelligence 2004/6, 25; *Sieber*, JZ 2009, 653 (657).

46 Internet Corporation for Assigned Names and Numbers, siehe hierzu oben Kapitel 1. B.

47 *Schnabel*, K&R 2008, 26 (28); *Sieber*, 84; *Schöttle*, K&R 2007, 366 (367); OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 938; *Sieber/Nolde*, Sperrverfügung im Internet, 2008, S. 50.

48 *Billmeier*, 206; *Schöttle*, K&R 2007, 366 (368); *Hoeren*, ZfWG 2008, 311 (312 ff.); *Sieber*, Verantwortlichkeit im Internet, 84.

49 *Frey/Rudolph*, Stellungnahme zur öffentlichen Expertenanhörung des Rechtsausschusses des Deutschen Bundestages am 10.11.2010, 4 ff.

in den Browser den sog. Domain-Namen anstelle der IP-Adresse ein. Der eingegebene Domain-Name wird auf dem Domain Name Service (DNS) in die ihr zugeordnete IP-*Adresse* umgewandelt. Wenn man dort einen bestimmten Domainnamen blockiert, wird die Umwandlung verhindert, der Nutzer wird zu einer ungültigen oder einer falschen Webseite weitergeleitet. Allerdings ist diese Maßnahme besonders leicht zu umgehen, beispielweise durch Eingabe der IP-Adresse statt des Domain-Namens, durch einen Wechsel des DNS-Servers von Seiten des Content-Providers oder einfach durch Nutzung einer Suchmaschine.[50] Eine DNS-Sperre könnte zur Sperrung legaler Angebote führen, da sich zahlreiche Zieladressen unter einem Domain-Namen verbergen.[51]

IV. Hybride Sperrtechniken – Die Great Fire Wall

Hybride Sperrtechniken werden beispielweise bei der mittlerweile wohl weltbekannten chinesischen Great Fire Wall (GFW) verwendet, die zum einen eine effektive Inhaltskontrolle, zum anderen auch die Verhinderung von Umgehungsmöglichkeiten zum Ziel hat.[52] Das Computernetz besteht im Gebiet der VR China gemäß § 3 der vorläufigen Bestimmungen der VR China zur Lenkung des Internet aus drei Schichten, und zwar Zugangsnetz, Verbindungsnetz (oder Backbone-Netz) und WWW-Net.[53] Nur mit Hilfe der Zugangsnetzes sind Nutzer über das von Verbindungsnetzeinheiten angebotene Verbindungsnetz mit dem WWW-Netz verbunden (§§ 8 I und 10 Vorläufige Bestimmungen der VR China zur Lenkung des Internet).

Aus der Perspektive der Nutzer ist das Zugangsnetz das erste Netz, das aus verschiedenen lokalen Netzwerken besteht und im Ganzen als Metropolitan Area Network (MAN) bezeichnet wird. Bei lokalen Netzwerken handelt es sich um einen kleinen Kreis einiger Computer, deren Träger sowohl privat oder kommerziell als

---

50 *Sieber*, Verantwortlichkeit im Internet, 84; Stadler, MMR 2002, 343 (345); *Schöttle*, K&R 2007, 366 (367); *Schnabel*, K&R 2008, 26 (28 f.); OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 936；*Sieber/Nolde*, Sperrverfügung im Internet, 50.

51 *Fei*, 4; *Frey/Rudolph*, Stellungnahme zur öffentlichen Expertenanhörung des Rechtsausschusses des Deutschen Bundestages am 10.11.2010, 4 ff.

52 *Sieber*, 44 ff., 78 ff.; *Germann*, 299 ff.; 92; *Schöttle*, K&R 2007, 366 (368); *Fei*, 1 ff.; mit Hilfe von amerikanischen Unternehmen Cisco und Microsoft wurde GFW aufgebaut, siehe *Goldsmith/Wu*, 93 ff.

53 Vorläufige Bestimmungen der VR China zur Lenkung des Internet (计算机信息网络国际联网管理暂行规定) vom 1.2.1996.

auch öffentlich sein können. Bei Verbindungsnetzen oder Backbone-Netzen besitzen die drei staatlichen Telekommunikationsunternehmen zusammen die Monopolstellung. Da alle sechs gewerblich genutzten Backbone-Netze komplett unter staatlicher Kontrolle stellen, ist der Informationsfluss in diesem Teil absolut vom Staat manipulierbar. Zwischen dem Verbindungsnetz und WWW-Netz sind außerdem die sog. internationalen Datenzugangskanäle eingerichtet, über die eine wechselseitige Verbindung von Computernetzen der VR China mit ausländischen Netzen erst möglich ist. Die Lizenz der Einheiten, welche die internationalen Datenzugangskanäle zur Verfügung stellen, ist ausschließlich von (drei) staatlichen Telekommunikationsunternehmen zu erwerben. Die Kanäle können erst mit Genehmigung der zuständigen Behörde (das Ministerium für Industrialisierung und Information) errichtet werden (§§ 4-5 Verwaltungsmethode für internationale Datenzugangskanäle). Die Datenzugangskanäle verteilen sich auf die drei Metropolen Beijing, Shanghai und Guangzhou. Nach einer dynamisch geänderten IP-Liste, auf der einige Proxy-Server und vorläufig zu sperrende Webseiten aufgelistet sind, und einer stabilen Liste, die *ständig gesperrte* Internetseiten beinhaltet, kontrollieren die drei Datenzugangskanäle effektiv den Informationsaustausch zwischen China und dem Ausland.[54]

Chinesische Nutzer kommen letztlich über drei „Gateways" – Zugangsnetz, Verbindungsnetz und WWW-Netz – ins Internet und können dementsprechend von diesen drei „Gatekeepern" der Kontrolle der GFW ausgesetzt werden. Die GFW gilt als Synthese aller Sperrmöglichkeiten, die mindestens auch die in Deutschland verwendeten Maßnahmen der DNS-Sperre, Blockade von IP-Adressen, DPI (Deep Packet Inspection) und Filterung von Schlüsselwörtern durch den Einsatz von Proxy-Servern bereithält. Mit DPI ist es möglich, in den internationalen Datenzugangskanälen Informationen zu analysieren, Schlüsselwörter herauszufinden, sie intelligent zu erkennen und dann filtern. Fallen die sensitiven Schlüsselwörter oder chinesischen Schriftzeichen unter die Verbote, wird der Proxy-Server dem Nutzer ein Datenpaket zurücksenden. Als Ergebnis kann der Nutzer die gezielte Internetseite nicht mehr erfolgreich abrufen, sondern erreicht nur eine Webseite, in der es heißt „The Page cannot be displayed" oder „404 Not Found".

---

54 *Li Yonggang*, 131; *Xu*, China Information Industry Policy & Decision making 1997/6, 12 (12 f.); *Chen Peng*, Radio & TV Broadcast Engineering 1996/4, 69 (69).

E. Zielsetzung dieser Arbeit

I. Gegenstand und Ziel der Arbeit

Online-Informationen werden sowohl in Deutschland als auch in China zur Bekämpfung von Rechtsverletzungen gesperrt. Die Inhalteregulierung ist in der Literatur ein viel diskutiertes Thema in den letzten Jahren. Die vorliegende Arbeit stellt nicht so sehr die Inhalte in den Vordergrund. Im Mittelpunkt der Darstellung dieser Arbeit geht es um zeitlich vorangehende Mechanismen zur Sicherstellung eines Internets, das frei von schädlichen oder rechtswidrigen Inhalten ist. Hierbei spielen Lizenzen eine Rolle. Von Bedeutung ist auch die Besetzung von Schlüsselpositionen in Redaktionen oder Online-Medienunternehmen, ebenso wie die Löschung von Inhalten auf Online-Plattformen. Dies alles soll Erwähnung finden. Der Fokus der Arbeit soll aber auf die Sperrmaßnahmen von Access-Provider gerückt werden, ob und ggf. Sperrmaßnahmen gegen Access-Provider erlaubt sind. Sperrmaßnahmen gegen Access-Provider schränken die Bewegungsfähigkeit im Internet ungleich stärker ein als Löschungen von Inhalten. Hier werden rechtsstaatliche Grundsätze herausgefordert. Wenn für Nutzer eine Internetseite gar nicht erreichbar ist, stellt dies einen schweren Eingriff in die Informationsmöglichkeiten des Netznutzers dar. Maßnahmen gegen Access-Provider können „als Einstieg in eine durch die Provider einzurichtende *Sperrinfrastruktur* erheblich sein."[55]

Es stellt sich daher die Frage, wie beide Länder solche Sperrmaßnahmen gesetzlich ausgestalten, welche Ansätze sich dahinter verbergen, welchen Grundsätzen das Sperren von Inhalten bzw. das Sperren des Zugangs zu den Inhalten unterliegt, welche Rechtsschutzmöglichkeiten den Betroffenen zustehen und welche Hindernisse zum Rechtsschutz bestehen. Auf dieses Thema wird in China wegen der Meinungskontrolle selten wissenschaftlich eingegangen. In nur sehr geringem Umfang liegen juristische Beiträge vor und der große Teil davon rechtfertigt die Internetsperren.[56] Traditionell orientiert sich China bei der Einführung von Rechtsvorschriften oft an Deutschland. Im Zivilrecht ist dies zu beobachten. Im

---

55 *Heidrich/Heymann*, MMR 2016, 370 (370), Hervorhebung durch Verfasser.

56 *Hu Ling*, in: Fu, Hualing/Zhu, Guobin, Grundrecht und Konstitutionalismus, 411; *Li Dayong*, Law Science 2014/1, 100; *Li Yonggang*, Journal of Nanjing Tech University 2007, 44; *Liu Han*, Peking University Law Journal 2016/2, 518; *Liu Hao/Wang Kai*, Journal of Capital Normal University (Social Sciences Edition), 2015/5, 56; *Wei*, Cass Journal of Foreign Law 2011/1, 69; *Yin*, Polical Science and Law 2015/1, 102.

öffentlichen Recht bestehen derart enge Verbindungen zwischen beiden Ländern nicht. Dennoch gibt die traditionelle Verbundenheit beider Länder den Anstoß für die vorliegende Arbeit. Die Arbeit verfolgt auch das Ziel den Dialog zwischen Deutschland und China zu fördern. Vor allem das deutsche Fachpublikum soll über die Rechtslage in China informiert werden.

II. Fragestellung

Im Mittelpunkt dieser Arbeit steht die Frage der Regulierung schädlicher Informationen. Für beide Länder, China und Deutschland, wird dargestellt, wie sie versuchen, das Internet frei von rechtswidrigen bzw. schädlichen Informationen zu halten. Da in China Sperrmaßnahmen gegen bzw. durch Access-Provider eine große Rolle spielen, soll der Fokus im „deutschen" Teil dieser Arbeit auf diese Art von Sperrmaßnahmen gelegt werden. Für diese Art von Maßnahmen herrschen in Deutschland hohe Anforderungen. Access-Provider sind relativ weit vom Inhalt entfernt. Ein Vorgehen gegen sie ist begründungsbedürftig. Speziell gilt es die Frage zu beantworten: Inwiefern sind in China und in Deutschland Sperrmaßnahmen gegenüber Zugangsanbieter wegen rechtswidriger Inhalte möglich? Sind hierfür in beiden Ländern besondere Anforderungen zu beachten? Ausgehend von den Ergebnissen soll rechtsvergleichend erarbeitet werden, welche Verbesserungsmöglichkeiten in beiden Ländern – vor allem in China – bestehen.

III. Gang der Untersuchung

Das vorliegende Forschungsvorhaben basiert auf einem funktionalen Rechtsvergleich zwischen China und Deutschland. Nach dieser Rechtsvergleichsmethode ist zunächst ein Ausgangspunkt festzulegen, durch den das gemeinsame Problem dargestellt wird.[57] In diesem Fall ist es die gemeinsame Herausforderung der Bekämpfung rechtswidriger Informationen online sowohl für Deutschland als auch für China. Möchte jeder souveräne Staat, wie China und Deutschland, dass Internetsperren die Einhaltung von Rechtsvorschriften gewährleisten, ist die allgemeine Frage nach Souveränität von Staaten im Internet aufzuwerfen. Diese kann vor dem Hintergrund des Internet unter neuen Vorzeichen diskutiert werden

---

[57] Für einen „Mikrovergleich", also einen Vergleich mit klar umrissenem Untersuchungsgegenstand, im öffentlichen Recht, siehe *Krüger*, in: FS Kriele, 1393 (1405); *Schmidt-Aßmann*, ZaöRV 2018, 807 (838); *Hasse*, JA 2005, 232 (235 f.).

(2. Kapitel). Das Internet schafft eine Vernetzung und unmittelbare Verbindung zwischen den Staaten. Es soll hierbei kurz der Begriff der „Internetsouveränität“ erklärt werden. Dieser Begriff ist für die vorliegende Arbeit vor allem deshalb so wichtig, weil die chinesische Regierung hiermit ihre Internetpolitik rechtfertigt. Die Frage nach der Souveränität ist vor allem deshalb wichtig, da sich Internetsperren, also Maßnahmen gegen Access-Provider, häufig auf ausländische Inhalte beziehen. Im Anschluss daran soll das Vorgehen der chinesischen Regierung in Bezug auf das Sperren von Online-Inhalten näher dargestellt werden, wobei die deutsche Fachöffentlichkeit nicht nur über die chinesische Netzpolitik informiert werden soll, sondern es soll auch ein Überblick zu den chinesischen Rechtsgrundlagen gegeben werden (3. Kapitel). Auf dieser Basis kann die chinesische Netzpolitik sowie die chinesische Rechtspraxis besser nachvollzogen werden und danach abgewogen werden, ob die Vor- oder die Nachteile überwiegen. In China spielen Sperrmaßnahmen gegenüber und durch Access-Provider eine bedeutende Rolle. Es werden aber auch andere Mechanismen vorgestellt, die im Ergebnis dafür sorgen, dass praktisch ein lückenloses und effektives Internetsperrensystem besteht. Andererseits kann China, das sich teilweise am deutschen Recht orientiert, durch einen Rechtsvergleich die eigene Entwicklung zum Rechtsstaat ebenfalls vorantreiben. Dazu wird die Rechtslage in Deutschland dargestellt (4. Kapitel). Abschließend wird anhand der gefundenen Ergebnisse eine Bewertung des chinesischen Systems zur Bekämpfung von illegalen Inhalten online vorgenommen, wobei im Ansatz auch überlegt wird, wie das deutsche System verbessert werden kann (5. Kapitel).

Bei der Befassung mit chinesischem Recht soll nicht nur auf die Beschreibung der Rechtssätze eingegangen werden, sondern es soll eine dogmatische Analyse folgen, an der es bislang bei der Untersuchung über chinesisches Internetsperren zur Bekämpfung der Online-Inhalte sowohl in der westlichen Welt als auch in China fehlt. Die rechtsdogmatische Analyse beleuchtet insbesondere die Perspektive des Rechtsschutzes. Im Hinblick auf die fehlende Verfassungsgerichtsbarkeit in China wird dies im Folgenden überwiegend auf der chinesischen einfachgesetzlichen Ebene analysiert. Hierzu werden einerseits theoretische und praktische Standpunkte ausgewertet. Andererseits wird der noch nicht sehr umfangreiche Forschungsstand des chinesischen Rechts, das chinesische Politiksystem sowie die chinesische Kultur besonders berücksichtigt.

2. Kapitel „INTERNET-SOUVERÄNITÄT“

Um im Netz aufgetauchte rechtswidrige Informationen zu bekämpfen, hat ein Staat zur Aufrechterhaltung des Rechtssystems die entsprechenden Maßnahmen zu ergreifen, die ihm dafür erforderlich und angemessen erscheinen. Das erscheint nicht selbstverständlich, weil der Cyberspace in der Anfangsphase einen rechtsfreien und danach teilweise selbstregierten Raum darstellte. Mittlerweile wird er allerdings neben dem Hoheitsgebiet, Luftraum, Hoheitsgewässer und Weltraum als ein sog. „fünfter Raum“ im politischen Sinne betrachtet.[58] Hierbei spielt die sog. Internet-Souveränität eine entscheidende Rolle. Wäre Internet-Souveränität juristisch gerechtfertigt, würde dies bedeuten, dass der souveräne Staat auch im Internet die Hoheitsgewalt ausübt und die Staatsaufgaben dementsprechend zu erfüllen hat. Die politische Behauptung sowie die Interpretation der Internet-Souveränität könnte allerdings zur unbegrenzten Internetregulierung führen. In Bezug auf die Regulierung von Informationen im Internet mittels Sperren beruft sich China hauptsächlich auf seine Internet-Souveränität.

In diesem Kapitel soll der Frage nachgegangen werden, ob einem Staat aus Souveränitätsgründen bei der Regulierung des Internets Grenzen gesetzt werden. Oder besitzt der Staat hier volle Regelungskompetenz?

A. Die These der Souveränität des Cyberspace

Bevor näher auf die Internet-Souveränität eingegangen wird, ist sie von der mit ihr leicht zu verwechselnden These der Souveränität des Cyberspace oder Cyberspace als Souverän abzugrenzen. Regierungen haben im Cyberspace keine Souveränität, so *John Perry Barlow* im Jahre 1996.[59] Der Cyberspace galt damals als selbstständiges freies Gebiet und im Vergleich zur realen Welt als ein virtueller Ort.[60] Die dort vertretenen Menschen begegneten sich auf Augenhöhe. Sie standen nicht in

---

58 *Mayer*, NJW 1996, 1782 (1782); *Sieber*, 1.

59 *Barlow*, A Declaration of the Independence of Cyberspace, abrufbar unter <https://www.eff.org/cyberspace-independence> [Stand: 7.8.2019]; auch Baldwin/Cave/Lodge (ed.), § 21 Rn. 523; zu Barlow, *Goldsmith/Wu*, 17 ff.; *Greve*, 96.

60 *Roßnagel*, MMR 2002, 67 (68); *Eichensehr*, 103 Geo. L. J., 317 (326); *Thiel*, in: Der Begriff der Souveränität in der transnationalen Konstellation, 215 (215 ff.); *Post*, 5 Ind. J. Global Legal Stud. 521 (522); *Franzese*, 64 A. F. L. Rev. 1, 11(11 ff.); *Goldsmith/ Wu*, 6.

einem Über- und Unterordnungsverhältnis zueinander. Die sog. Netizen charakterisierten sich als Schöpfer oder Nutzer der Netztechnik, teilten gleiche Verhaltenskodizes, Kultur und Werteordnungen, sahen sie als liberal und antiautoritär.[61] Vor diesem Hintergrund wurde das Internet als ein „rechtsfreier Raum“[62], ein „anarchischer Raum”[63], ein „öffentlicher oder sozialer Raum neuen Typs“[64] oder als „neue, selbstständige und mit Gleichheit und Freiheit ausgerüstete Gemeinschaft”[65] angesehen.

Die Netizen, vor allem die Internet-Techniker,[66] versuchten stets, den Staat sowie die Staatsgewalt möglichst vom Cyberspace auszuschließen.[67] Die 1986 gegründete und für die Feststellung der technischen Standards des Internet zuständige Organisation – Internet Engineering Task Force (IETF) – zielte genau darauf ab, dass durch Technik das traditionelle hierarchische Regulierungsmodell in souveränen Staaten abzuschaffen sei und gleichzeitig ein wirklich demokratischer Diskurs und eine Selbstregulierung der Gesellschaft zu entwickeln sei.[68] Klarer drückte dies der Internet-Pionier *David Clark* aus: „We reject: kings, presidents, and voting. We believe in: rough consensus and running code.“[69] Als Folge wurde die These der sog. Souveränität des Cyberspace, die als Kernbegriff Mitte der 90er Jahre in den USA entstanden ist, aufgestellt.[70]

Unter dem Konzept der Souveränität des Cyberspace muss man jedoch in diesem Zusammenhang verstehen, dass dessen Vertreter nur ein globales, anonymes, kostgünstiges und schnelles Kommunikationsnetz vor Augen hatten.[71] Cyberspace

---

61 *Engel*, AfP 2002, 119 (119 ff.); *Liu Han*, Peking University Law Journal 2016/2, 518 (520); *Pichler*, 12 f.

62 *Mayer*, NJW 1996, 1782 (1789).

63 *Hobe*, in: HStR, Bd. XI, § 231 Rn. 13; zur anarchistischen Mentalität der Internetnutzer siehe *Hornig*, ZUM 2001, 846 (848); dagegen, *Johnson/Post*, 5 Stanford Law Review 1367 (1389).

64 *Mayer*, NJW 1996, 1782 (1783).

65 *Liu Han*, Peking University Law Journal 2016/2, 518 (520 ff.); dazu noch *Greve*, 95, 112; *Trute*, VVDStRL 57, 216 (245 f.).

66 Nennenswert sind z.B. Larry Roberts, Robert Kahn, Vint Cerf, John Postel und David Clark, dazu *Goldsmith/Wu*, 22 f.

67 *Thiel*, in: Der Begriff der Souveränität in der transnationalen Konstellation, 215 (219 ff.); *Pichler*, 17; *Goldsmith/Wu*, 23.

68 *Goldsmith/Wu*, 24.

69 Ebd.

70 *Eichensehr*, 103 Geo. L. J., 317 (326); *Johnson/Post*, 5 Stanford Law Review 1367 (1367 ff.); ausführlich zur Theorie von Johnson und Post, siehe *Pichler*, 19 ff.; *Wu*, 10 Harv. JL & Tech. 648 (648 ff.); Zur Unterschied zwischen „Internet Sovereignty” und „Sovereignty of the Internet” siehe *Liu Han*, Peking University Law Journal 2016/2, 518 (519).

71 *Johnson/Post*, 5 Stanford Law Review 1367 (1370 ff.); *Thiel*, in: Der Begriff der Souveränität in der transnationalen Konstellation, 215 (226); *Pichler*, 19.

wurde dann kontrovers entweder als „no place“[72] und „placelessness“[73] im negativen Sinne oder als „a supraterritorial phenomenon“[74] im positiven Sinne gesehen. Danach besteht keine Gebietsgrenze im Cyberspace, sondern nur die Grenze zwischen realer und virtueller Welt. Überspringt man den Bildschirm und tritt ins dahinerstehende Cyberspace ein, gelten sofort die von Netizen selber festgelegten Regeln. Die Trennung zwischen dem Cyberspace und der realen Welt wird unter anderem auch im antiautoritären Technikrahmen gerechtfertigt, weil die Legitimität allein auf dem gemeinsamen Willen aller Netizen im Sinne von einem gesellschaftlichen Vertag zurückzuführen ist.[75] Der Cyberspace ist „eine eigenständige Jurisdiktion ”[76], ein „eigener Rechtsraum“[77] oder „self-contained Regime”[78], wo Netizen sich selbst regulieren,[79].

In den USA gewann dieses Konzept der Souveränität des Cyberspace nicht nur im theoretischen Sinne Unterstützung, sondern auch durch die Rechtspraxis. 1996 wurde dort das erste Internet-Gesetz – „The Communications Decency Act“ erlassen, gegen das später eine Verfassungsklage erhoben wurde. Im bekannten Fall *American Civil Liberty Union v. Reno* stellte der Supreme Court fest: „these tools constitute a unique medium – known to its users as ‘cyberspace’ – located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet.”[80] Und: „The electronic world is fundamentally different. Because it is no more than the interconnection of electronic pathways, cyberspace allows speakers and listeners to mask their identities.”[81] Angesichts der Unabhängigkeit des Cyberspace verstößt, gemäß den Ausführungen des Supreme Court der „Communications Decency Act“ gegen „the freedom of speech” nach dem First Amendment.[82]

---

72 *Herrera*, in: Power and security in the information age, 67 (67); *Greve*, 28.
73 *Herrera*, in: Power and security in the information age, 67 (68).
74 *Trachtman*, 5 Ind. J. Global Legal Stud. 561 (568).
75 *Christiansen*, MMR 2000, 123 (124); *Pichler*, 50 f.
76 *Mayer*, NJW 1996, 1782 (1790).
77 *Pichler*, 19.
78 *Hobe*, in: HStR, Bd. XI, § 231 Rn. 15; *Johnson/Post*, 5 Stanford Law Review 1367 (1388).
79 *Hornig*, ZUM 2001, 846 (850); *Christiansen*, MMR 2000, 123 (123 ff.); *Engel*, 45 ff.; *Mayer*, NJW 1996, 1782 (1790); *Johnson/Post*, 5 Stanford Law Review 1367 (1391); *Pichler*, 21 ff.
80 *American Civil Liberty Union v. Reno*, 521 U.S. 844 (851).
81 Ebd., 844 (889 f.)
82 Ebd., 844 (851); dazu auch *Grewlich*, 40; *Goldsmith/Wu*, 21; *Holznagel*, Die Verwaltung-Beil. 4/2001, 83 (88 f.).

Ob die oben dargestellten technischen und davon abhängigen theoretischen sowie rechtspraktischen Ansätze in den USA Wirklichkeit hätten werden können, scheint zweifelhaft, da eine liberale, offene und antiautoritäre Internetstruktur nicht unbedingt mit einer liberalen, offenen und antiautoritären *Nutzung* der Internetstruktur gleichgesetzt werden kann.[83] In der Tat blieb der rechtsfreie oder selbstregulierende Zustand nur in der Anfangsphase – von der reinen wissenschaftlichen Forschung und militärischen Nutzung des Internet bis zur deren Kommerzialisierung – unverändert[84], weil der Staat aufgrund von geringen Außenwirkungen des Cyberspace damals keinen Grund für einen Eingriff sowie kein Interesse daran hatte. Der Cyberspace hatte somit keine Gefährdungen oder Bedrohungen für das reale Leben. Mit der weiteren Kommerzialisierung und Popularität des globalen Netzes schwindet der egalitäre Charakter des Internet. Mit vielfältigen Werteordnungen und Verhaltenskodizes, die von den verschiedenen Akteuren ins Netz gebracht wurden, sind die unabhängige Stellung des Internet gegenüber der Politik, Wirtschaft und Gesellschaft nicht mehr vorhanden. Der These des „rechtsfreien Raums" ist somit nicht mehr zu folgen und eine neue Periode der Internet-Regulierung wurde eingeläutet.[85]

B. Souveränität des Staates und ihre Existenz im Cyberspace

Über die These der „Souveränität des Cyberspace" wurde in den USA, wie angedeutet, heftig diskutiert. Problematisch ist vor allem aus der Sicht der Staatslehre, wie ein virtueller Ort, der über kein physisches Territorium verfügt, das Eindringen von einem mit Souveränität ausgestatteten Staat verhindern soll. Völkerrechtlich ist nur ein souveräner Staat unabhängig und grenzt sich somit von anderen souveränen Staaten ab. Erlangt der Cyberspace eigene Souveränität oder erstreckt sich die Souveränität des Staates eben auf den Cyberspace? Um dies zu klären, ist auf den Begriff der Souveränität sowie die dazugehörige Staatslehre zurückzugreifen. Zwei wichtige Fragen sind schließlich zu beantworten: ob der Cyberspace einen Staat ausmacht und falls es kein Staat ist, ob er doch souverän sein könnte.

---

83 *Cornils*, in: VVDStRL (76), 392, 400; *Greve*, 112; Dagegen, *Herrera*, in: Power and security in the information age, 67 (70).

84 *Mayer*, NJW 1996, 1782 (1782); *Sassen*, 5 Ind. J. Global Legal Stud. 545 (547 f.); *Naughton*, 85.

85 *Thiel*, in: Der Begriff der Souveränität in der transnationalen Konstellation, 215 (225); *Christiansen*, MMR 2000, 123 (127 ff.); *Cornils*, in: VVDStRL (76), 397 ff.; *Herrera*, in: Power and security in the information age, 67 (76 ff.).

I. Staat ohne (physisches) Gebiet?

Die Auseinandersetzung mit dem Staatsbegriff hat sowohl in der Politikwissenschaft als auch in der Rechtswissenschaft eine lange Tradition. Wie *Schulze-Gävernitz* beschreibt, seien die Erklärungen zum Staat zahllos und fast jeder Gelehrter habe dazu eigene und originelle Definitionen beigetragen.[86] Nach *Isensee* liegt das Dilemma der Staatsbegriffe darin, „dass ihnen ihr Objekt immer wieder entgleitet."[87] Zudem sind philosophische und methodische Streitereien unvermeidbar. Abgesehen von verschiedenen Theorien wird von allen angenommen, dass der Staat auch „eine Zweckschöpfung der politischen Vernunft"[88] ist. Beim Begriffsverständnis über Staaten wird heute gemeinhin von der sog. Drei-Elementen-Lehre von *Jellinek* ausgegangen. Hiernach ist ein Staat im formellen Sinne durch drei Merkmalen gekennzeichnet, das Staatsvolk, das Staatsgebiet und die Staatsgewalt.[89]

Nach *Jellinek* soll der Staat als ein Organismus versubjektiviert werden, indem er die Herrschaftsgewalt über Personen ausübt, die in einem bestimmten Gebiet sesshaft sind.[90] Staatsgebiet ist danach nicht nur physisch ein abgegrenzter Teil der Erdoberfläche, der sämtliche territorialen Bereiche mit Festland, Hoheitsgewässer und Luftraum umfasst, sondern beinhaltet auch einen Herrschaftsbereich.[91] Die Frage ist, ob ein Raum ohne physisches Hoheitsgebiet einen Staat ausmachen kann. Zunächst stellt eine Volksansammlung ohne territorialen Bereich keinen Staat

---

86 *Schulze-Gävernitz*, 15; dazu siehe auch *Schöbener/Knauff*, 71; ferner *Baldus*, Der Staat 1997, 381 (381); *Schliesky*, 8 ff.; Isensee, in: HStR, Bd. I, § 13 Rn. 26; Böckenförde, Die Entstehung des Staates als Vorgang der Säkularisation, in: ders., Recht, Staat, Freiheit, 92 (112); zur Staatslehren des 19. Jahrhunderts in Deutschland, Hobe, 54 ff; zur Staatsidee der Bundesrepublik Deutschland, Schliesky, 53.

87 *Isensee*, in: HStR, Bd. II, § 15 Rn. 46.

88 *Isensee*, in: HStR, Bd. II, § 15 Rn. 79; *Schliesky*, 120; *Koppensteiner*, 33 ff., 48 ff.

89 *Jellinek*, 394 ff.; ausführlich siehe Schliesky, 25 ff.; ferner, *Hobe*, 61 ff.; *Maurer*, Staatsrecht, § 1 Rn. 5 ff; *Isensee*, in: HStR, Bd. II, § 15 Rn. 50; *Kersten*, Georg Jellinek und die klassische Staatslehre, 262 ff., 280 ff., 306 ff.; die Kritik *Smend*, Verfassung und Verfassungsrecht, 169.

90 *Jellinek*, 395 ff.; *Schliesky*, 28 ff.; *Zippelius*, 87.

91 Nach *Jellinek* bezeichnet das Staatsgebiet „seiner rechtlichen Seite nach den Raum, auf dem die Staatsgewalt ihre spezifische Tätigkeit, die des Herschens, entfalten kann." Jellinek, 394; ferner Isensee, in: HStR, Bd. I, § 13 Rn. 28 f.; *Isensee*, in: HStR, Bd. II, § 15 Rn. 51; *Schöbener/Knauff*, 87; *Badura*, A3; *Maurer*, § 1 Rn. 5 ff.; *Gornig*, in: Gornig/Horn, Territoriale Souveränität und Gebietshoheit, 35 (35 f.); *Menthe*, 4. Mich. Telecom, & Tech. L. Rev. 69 (88 ff.); *Li Huizong*, 13; Kritik zu Jellineks Drei-Elementen-Lehre, *Smend*, in: Staatsrechtliche Abhandlungen und andere Aufsätze, 119 (168 ff.); *Quaritsch*, Souveränität, 22 ff.; Krüger, 146.

dar,[92] entsprechend der historischen Entwicklung kann eine Volksansammlung zum Territorialstaat werden.[93] Diese Entwicklung kann auf das Ende des Mittelalters zurückgeführt werden, seitdem die Staatskonzeption von den personalen Herrschaftsgewalten langsam zu Territorialgewalten überging.[94] Ferner ist der Begriff des Staatsgebietes eng und untrennbar mit der Staatsgewalt verbunden. Nach *Jellinek* äußert sich das Staatsgebiet im rechtlichen Sinne in zwei Funktionen: Die negative Funktion bewirkt, „dass jeder anderen, dem Staat nicht unterworfenen Macht es untersagt ist, ohne ausdrückliche Erlaubnis von Seiten des Staates Herrschaft zu üben."[95] Im heutigen Völkerrecht wird diese negative Funktion auch „territoriale Souveränität" genannt.[96] Die positive Funktion besteht darin, "dass alle auf dem Gebiete befindlichen Person der Staatsherrschaft unterworfen sind."[97] Die zweite Funktion wird nach dem allgemeinen Verständnis als „Gebietshoheit" bezeichnet.[98] Nur auf dem Staatsgebiet kann sich die staatliche Herrschaft entfalten. Demnach setzt die Existenz eines Staates ein Staatsgebiet voraus.

Ob der Cyberspace als virtueller Ort ein Staatsgebiet darstellt und daher selber einen Staat bildet, ist hier zu diskutieren.[99] Zwar sammeln sich Netizen im Cyberspace an und es zeigt sich im Internet eine gewisse Gewalt, die z.B. von der Online-Community geschaffen wird. Der Cyberspace verfügt jedoch über kein physisches Hoheitsgebiet. Die globale Netzinfrastruktur verhindert allerdings nicht, dass souveräne Staaten hier das Internet lokalisieren (z.B. mit Geolokation, Internet der Dinge, GPS oder RFID) und nicht-anonym machen,[100] weil letztlich sämtliche physischen Anlagen (Server, Netzstruktur, Endgeräte, Kabel usw.) vom physischen Raum abhängen.[101] Selbst wenn der Cyberspace ein gewisses virtuelles

---

92 *Horn*, in: Gornig/Horn, Territoriale Souveränität und Gebietshoheit, 21 (21 ff.); *Gornig*, in: Gornig/Horn, Territoriale Souveränität und Gebietshoheit, 35 (35); *Pichler*, 34 ff.; *Menzel*, 110; zum Begriff des Staatsvolks, *Jellinek*, 406 ff.; *Schliesky*, 30 ff., 67.

93 *Hobe*, in: HStR, Bd. XI, § 231 Rn. 6; *Boehme-Neßler*, ZÖR 2009, 145 (151 ff.); *Grimm*, 77 f.; *Horn*, in: Gornig/Horn, Territoriale Souveränität und Gebietshoheit, 21 (22); *Menzel*, 95 ff.; *Schliesky*, 67; *Kimminich*, 111; *Kriele*, 83.

94 *Schliesky*, 67, 71; *Stern*, in: Staatsrecht V, 73 ff.; *Schmidt*, Geschichte des Alten Reiches, 9 ff.

95 *Jellinek*, 394.

96 *Randelzhofer*, in: HStR, Bd. II, § 17 Rn. 28; *Schliesky*, 26.

97 *Jellinek*, 394.

98 *Schliesky*, 27; *Isensee*, in: HStR, Bd. II, § 15 Rn. 51.

99 *Christiansen*, MMR 2000, 123 (124); *Pichler*, 50 f.; *Hornig*, ZUM 2001, 846 (850); *Engel*, 45 ff.

100 *Thiel*, in: Der Begriff der Souveränität in der transnationalen Konstellation, 215 (227); *Herrera*, in: Power and security in the information age, 67 (76); *Engel*, 33; dagegen, *Johnson/Post*, 5 Stanford Law Review 1367 (1372 ff.).

101 *Hobe*, in: HStR, Bd. XI, § 231 Rn. 44; *Hobe*, 289; *Thiel*, in: Der Begriff der Souveränität in der transnationalen Konstellation, 215 (227); *Goldsmith*, 5 Ind. J. Global Legal Stud.

Territorium besitzt, werden souveräne Staaten den Cyberspace okkupieren, bevor die Netizen einen Gesamtwillen formulieren .[102] Als Folge koexistieren die weltweiten Kommunikationsverbindungen des Internet neben den territorial begrenzten souveränen Staaten. Der Cyberspace ist kein von den physischen Gebieten getrennter Raum, sondern nur ein Teil der realen Welt.[103] Als Folge entsteht im Cyberspace kein neuer Staat, da dort es am Merkmal des Staatsgebiets fehlt.

II. Souveränität ohne Staat?

Die zweite Frage besteht darin, ob der Cyberspace als ein nichtstaatlicher „öffentlicher oder sozialer Raum neuen Typs“[104] auch souverän sein könnte. Um dies zu erklären, muss man sich mit dem Kernbegriff der Souveränität auseinandersetzen. Der Begriff der Souveränität ist mit seinen zeitlichen und räumlichen Wandlungen sehr vieldeutig.[105] Souveränität ist immer vor seinem historischen Hintergrund zu definieren und zu beschreiben.[106]

1. Theoretischer Hintergrund

Das Souveränitätskonzept ist vor allem von *Bodin* geprägt worden, der vor dem Hintergrund der konfessionellen Bürgerkriege eine neue säkularisierte Herrschaft gestalten wollte, die über den konfliktgeneigten Glaubensgruppen steht,[107] wobei dieses absolute und dauernde Herrschaftsrecht nach *Bodin* aber nicht unbedingt

---

475 (476); *Roßnagel*, MMR 2002, 67 (68); *Engel*, AfP 2002, 119 (127); *Herrera*, in: Power and security in the information age, 67 (85 ff.); *Schaar*, digma 2015, 40 (41); *Trachtman*, 5 Ind. J. Global Legal Stud. 561 (568); *Jensen*, 50 Tex. Int'l L. J. 275 (296).

102 *Pichler*, 66; *Christiansen*, MMR 2000, 123 (124); *Hornig*, ZUM 2001, 846 (850); *Engel*, 45 ff.; *Post*, 5 Ind. J. Global Legal Stud. 521 (537 ff.).

103 *Li Yonggang*, Journal of Nanjing Tech University 2007, 44 (46); *Liu Han*, Peking University Law Journal 2016/2, 518 (524); *Cornils*, in: VVDStRL (76), 392.

104 *Mayer*, NJW 1996, 1782 (1783).

105 *Dreier*, in: ders./Hoffmann (Hrsg.), Parlamentarische Souveränität und technische Entwicklung, 11 (16); Zum Streit über die Entstehung der Souveränität als einen Begriff siehe *Randelzhofer*, in: HStR, Bd. II, § 17 Rn. 13 ff.; *Grimm*, 16; zum Überblick über Entwicklung der Souveränität siehe Jellinek, 435 ff.; *Häberle*, AöR 1967, 259 (265 ff.); *Grimm*, 9; *Dreier*, in: ders., Idee und Gestalt des freiheitlichen Verfassungsstaates, 111 (112 ff.); *Schliesky*, 59 ff.; zur Eliminierung des Souveränitätsbegriffs siehe *Baldus*, Der Staat 1997, 381 (381 ff.).

106 *Grimm*, 13; *Häberle*, AöR 1967, 259 (265); *Menzel*, 124.

107 *Grimm*, 21 f.; *Dennert*, 59, 70 ff; *Schliesky*, 73; zum religiösen Hintergrund der Souveränität siehe *Haltern*, 24 ff. ; siehe auch *Schliesky*, 52, 72 ff.; *Di Fabio*, 16 f.; *Quaritsch*, Staat und Souveränität, 39; *Böckenförde*, Die Entstehung des Staates als Vorgang der Säkularisation, in: ders., Recht, Staat, Freiheit, 92 (104 f.); *Starck*, JZ 2000, 1 (4).

einem Monarchen zufallen soll.[108] Jedenfalls erstreckt sich die Herrschaft nach *Bodin* auf sämtliche innere Gegenstände, insbesondere auch auf das Gesetzgebungsmonopol, soweit es dem inneren Frieden dient.[109] Vor dem konfessionellen Bürgerkrieg veröffentlichte auch *Hobbes* seine These. Er ging vom inneren Frieden und der Sicherheit der Individuen aus und stellte sich damit einen Naturzustand vor, in dem die Einzelnen ihre Naturrechte „vollständig und bedingungslos"[110] dem Staat abtreten.[111] Die Souveränität wird nach *Hobbes* vom Staat („Leviathan") als künstliche juristische Person besetzt und vom Herrscher (Monarch) ausgeübt.[112] Dagegen überträgt das Individuum nach *Locke* – anders als *Hobbes* – dem Staat nur einen Teil seines Naturrechts, um seine eigene Freiheit zu schützen, wobei der Souveränitätsbegriff nicht bei Locke auftaucht, er spricht vom „supreme".[113] Über die ausführliche Entwicklung des Souveränitätsbegriffs soll hier nicht weiter und vertieft diskutiert werden. Die These der Volkssouveränität wird aber dank der Aufklärung weltweit von vielen Ländern übernommen. Sie wurde nach der amerikanischen Unabhängigkeitsrevolution durch die im Jahre 1787 verkündete Verfassung und nach der französischen Revolution im Zuge der Verfassungsgebung umgesetzt.[114] In der Bundesrepublik Deutschland bleibt das Staatsvolk auch souverän, was insbesondere in der Präambel und in Art. 146 GG festgehalten ist. Dieses Konzept wurde ebenfalls von der VR China rezeptiert. Die Konzeption der Volkssouveränität ist mit der Frage der Legitimation verbunden und gestaltet auch die Basis der sog. Souveränität des Cyberspace, worüber näher zu diskutieren ist.

Die Souveränität wurde nicht von *Bodin* zuerst entdeckt, sondern von ihm systematisiert und begründet. Er bietet ein wertneutrales Begriffsverständnis an, worin jeder seinen eigenen Wille umsetzen kann.[115] Die Frage ist, ob dieser wertneutrale Begriff der Souveränität, wonach sich diese einerseits aus dem Innehaben der

---

108 *Bodin*, 429 ff.; *Grimm* 24; *Dennert*, 58; *Quaritsch*, Staat und Souveränität, 243 ff.; *Hobe*, 42 f.; *Zippelius*, 58 ff.; zu Bodins Beitrag des Begriffs der Souveränität, *Schliesky*, 52, 59.; *Kondylis*, Der Staat 1995, 351 (352); *Niedhart*, in: ders. (Hrsg.), Jean Bodin - über den Staat, 132; *Imboden*, Johannes Bodinus und die Souveränitätslehre, 5 f.; *Dennert*, 72; *Jellinek*, 453; die Definition von „absolut" und „dauernd", *Schliesky*, 74.

109 *Bodin*, I. Buch, 10. Kap., 221; *Grimm,* 24; *Dennert*, 60; *Schliesky* 68, 75, 77; *Di Fabio*, 35; *Quaritsch*, Staat und Souveränität, 260; *Schliesky*, 75.

110 *Grimm*, 32.

111 *Hobbes*, 83 ff.; *Grimm*, 31 f.; *Dennert*, 80 ff.

112 *Hobbes*, 86 ff.

113 *Locke*, 248; *Grimm*, 33.

114 Ausführlich *Grimm*, 35 ff.

115 *Bodin*, Über den Staat, I 8, 126; *Schliesky*, 75; *Jellinek*, 458.

höchsten Gewalten im Staate (innere Souveränität) und andererseits aus der Unabhängigkeit des Staates (äußere Souveränität) zusammensetzt,[116] im Cyberspace weiterhin Anwendung finden kann.

2. Souveränität des Cyberspace?

Die Souveränität des Cyberspace ist stark von der Volkssouveränität geprägt, in dessen Mittelpunkt der auf der Basis von Gesamtwillen begründete Gesellschaftsvertrag steht.[117] Die Souveränität des Cyberspace haben danach die Netizen, die sich selber für Ausübungsorgane entscheiden.[118] Problematisch ist allerdings, ob dabei der Gesamtwille sowie die Gesellschaftsvertragstheorie nicht überschätzt werden. Abgesehen davon, ob die virtuelle Welt tatsächlich von der realen Welt unterschieden werden kann, wäre das Postulat eines völlig selbstständigen Cyberspace in sich widersprüchlich, weil es die Vereinbarung aller Netizen, die im Vorbehalt eigener Staatsangehörigkeit abstimmen, voraussetzt.[119] Eine von Netizen gewählte weltweite Internet-Community ist folglich kaum vorstellbar.

Im Cyberspace ist zwar die Ausübung der Staatsgewalt sowohl für demokratische Verfassungsstaaten als auch für autoritäre Staaten maßgeblich eingeschränkt,[120] jedoch wird das Innehaben der Staatsgewalt und damit das Fundament des Staates nicht ausgehöhlt.[121] Im Gegenteil erstrecken sich die drei Elemente eines souveränen Staates auch auf den Cyberspace, d.h. der Cyberspace gehört zum Staatsgebiet, Netizen zum Staatsvolk und er führt nur zur Erschwerung aber nicht zur Aushöhlung der Staatsgewalt.[122] Wer die anfängliche Motivation vergisst, mit der die

---

116 *Isensee*, in: HStR, Bd. II, § 15 Rn. 53; *Schliesky*, 57 f.; *Randelzhofer*, in: HStR, Bd. II, § 17 Rn. 23, 25 ff.; *Zippelius*, 66 f.

117 *Post*, 5 Ind. J. Global Legal Stud. 521 (537 ff.); *Pichler*, 66; *Christiansen*, MMR 2000, 123 (124); *Hornig*, ZUM 2001, 846 (850); *Engel*, 45 ff.

118 *Post*, 5 Ind. J. Global Legal Stud. 521 (539); *Mayer*, NJW 1996, 1782 (1790); *Engel*, 45.

119 *Mayer*, NJW 1996, 1782 (1790); *Greve*, 108; *Roßnagel*, MMR 2002, 67 (69); *Mankowski*, AfP 1999, 138 (140); Bei der Resultate ist zwischen Selbstregulierung auf Internet-weiter und netzinterner Ebene zu unterscheiden, dazu *Christiansen*, MMR 2000, 123 (125 ff.); *Pichler*, 52 ff.; *Goldsmith/Wu*, 150.

120 *Perritt*, 5:2 Ind. J. Global Legal Stud. 423 (427 ff.); *Hobe*, in: HStR, Bd. XI, § 231 Rn. 8 f.; *Pichler*, 77 ff.

121 *Perritt*, 5:2 Ind. J. Global Legal Stud. 423 (432); *Pichler*, 65 ff.

122 *Schliesky*, ZRP 2015, 56 (57); *Boehme-Neßler*, ZÖR 2009, 145 (161 f.); Engel, 37; *Sunstein*, 132.

USA zur Vermeidung der potenzialen Angriffe im kalten Krieg das Internet dezentral konstruierten,[123] kommt leicht zur Annahme, dass das Internet ein autogenes Wesen sei.[124] Wie *Milton L. Mueller* formuliert: „In short, those who have been bold enough to question the status of the nation-state in the age of global communications were simply not up to the task. They had only the most superficial understanding of their enemy. They taunted states with the claim that the Internet rendered them powerless, and were quickly proved wrong."[125] Die These der Souveränität des Cyberspace ist somit nicht begründet.

III. Zusammenfassung

Die in den USA diskutierte These der „Souveränität des Cyberspace" widerspricht der Drei-Elementen-Lehre von *Jellinek*, wonach ein Staat durch Staatsvolk, Staatsgebiet und Staatsgewalt begründet ist. Netizen sammeln sich zwar im Cyberspace und begründen zahlreiche Online-Communities. Sie geben ihre eigene Staatsangehörigkeit in der realen Welt aber nicht auf. Das Staatsgebiet ist ein physisch ein abgegrenzter Teil der Erdoberfläche. Der Cyberspace hängt von den physischen Anlagen im physischen Raum ab und ist somit nicht von den physischen Gebieten getrennt. Die Erschwerung der Ausübung der Staatsgewalt im Cyberspace führt nicht zur Aushöhlung der Staatsgewalt. Die These der Volkssouveränität kann nicht zur Begründung der Souveränität des Cyberspace beitragen. Der Cyberspace macht somit keinen Staat aus und ist selber nicht souverän. Die Souveränität des Staates erstreckt sich auf den Cyberspace.

C. Internet-Souveränität und die Begrenzung ihrer Entfaltung

Die konzeptionell abgelehnte Souveränität des Cyberspace stärkt gleichzeitig die Rolle des Staates im Cyberspace. Er beansprucht Souveränität auch an diesen „vir-

---

123 *Naughton*, 85; *Mayer*, NJW 1996, 1782 (1782); *Sassen*, 5 Ind. J. Global Legal Stud. 545 (547 f.).

124 *Liu Han*, Peking University Law Journal 2016/2, 518 (523); *Mayer*, NJW 1996, 1782 (1789); Hobe, in: HStR, Bd. XI, § 231 Rn. 13.

125 *Mueller*, 3.

tuellen“ Orten. Die „Souveränität im Cyberspace“ oder die sog. Internet-Souveränität übernimmt Inhalte des traditionalen Souveränitätsbegriffs, der sich aus der inneren Souveränität und der äußeren Souveränität zusammensetzt. [126]

I. Kritik am Zuhöchstsein der Souveränität

Selbst, wenn die Internet-Souveränität theoretisch begründet werden kann, ist die Aussage, dass der souveräne Staat absolut unabhängig auf völkerrechtlicher Ebene sei und im Staate die höchste Gewalt ohne Einschränkungen liege – das sog. Zuhöchstsein[127] – abzulehnen.[128] Es besteht immer die Gefahr, dass Souveränität als Begriff missbraucht wird. Er ist in gewisser Weise „ideologiegefährdet“[129]. In der Zeit des Absolutismus wurde beispielweise ein souveräner Staat mit unbegrenzter Macht des Monarchen gleichgestellt, was in Deutschland in der ersten Hälfte des 20. Jahrhunderts gleichfalls geschehen war, damit der Staat nicht an völkerrechtliche Verträge gebunden zu sein braucht.[130]

Bereits nach *Bodin* ist Souveränität keine unbegrenzte Macht. Als Bespiel wird bei ihm die Gesetzgebung angeführt, die sowohl dem göttlichen Gebot als auch dem Naturrecht unterworfen ist.[131] Schlagwortartig: „*Bodins* Souverän steht über dem Gesetz, nicht über dem Recht.“[132] Die naturrechtlichen Staatsvertragstheorien des späteren 18. Jahrhunderts sprechen mehr gegen uneingeschränkte Souve-

---

126 *Isensee*, in: HStR, Bd. II, § 15 Rn. 53; *Eichensehr*, 103 Geo. L. J., 317 (327 ff.); *Hillgruber*, JZ 2002, 1072 (1074); *Yu Zhigang*, Legal Forum 2014/6, 5 (14); Souveränität im Cyberspace ist zudem ein gesetzlicher Begriff im chinesischen Recht geworden, dazu § 25 Staatssicherheitsgesetz (国家安全法) vom 1.7.2015 und § 1 Cybersicherheitsgesetz (网络安全法) vom 7.11.2016.

127 *Heller*, Staatslehre, 246; *ders*., Die Souveränität, 161 ff.; *Krüger*, Zum Problem der Souveränität, 1; *Koppensteiner*, 27.

128 *Grimm*, 101; *Baldus*, Der Staat 1997, 381 (388 ff.); *Schliesky*, 138; 144; Zur Kollision zwischen der Souveränität und Gleichheit der Staaten als einen Grundsatz des Völkerrechts siehe *Nelson*, 53 f.; *Koppensteiner*, 31 f.

129 *Häberle*, AöR 1967, 259 (262), Fn. 19.

130 *Randelzhofer*, in: HStR, Bd. II, § 17 Rn. 5.

131 *Bodin*, Über den Staat, I 8, 128 ff., 156; I 10, 214.

132 *Bodin*, Über den Staat I 8, 129, 131, 156; *Grimm*, 25; ferner *Dennert*, 65; *Schliesky*, 78; *Quaritsch*, Staat und Souveränität, 264.

ränität, da der Einzelne nicht nur zur eigenen Sicherheit, sondern auch zur „Sicherheit der freien Gesellschaft“ seine Naturrechte dem Staat abtritt.[133] Ein demokratischer Staat verfügt zwar über sämtliche Hoheitsrechte, ist jedoch durch die Volkssouveränität legitimiert und begrenzt.[134]

Wenn ein Staat nach außen auf Wert auf Souveränität legt, soll er auf seine Unabhängigkeit gegenüber jeglicher Fremdherrschaft ausgerichtet sein, um sich gegen fremde Eingriffe zu verteidigen, internationale Kooperation zu ermöglichen und seine Friedenspflicht zu erfüllen.[135] Keinesfalls darf Souveränität auf die Entlastung von völkerrechtlichen Pflichten abzielen, sodass die Rechtsordnung des Völkerrechts dadurch nicht aufrechterhalten wird. Dementsprechend darf ein souveräner Staat im Innern nicht mit einem unbeschränkten „Leviathan“ gleichgestellt werden und muss zumindest an die Menschen- bzw. Grundrechte gebunden sein.[136]

II. Kein Bedürfnis für die Betonung der Internet-Souveränität

Bislang bezieht sich die Behauptung der Internet-Souveränität vor allem auf die Abwehr von Cyberattacken (z.B. ausländische Überwachung) oder Cyberdelikten aus dem Ausland und eine unabhängige Netzinfrastruktur.[137] Sofern es sich darum handelt, bestehen Zweifel, ob das World Wide Web die Ausübung der Staatsgewalt in diesem Bereich auf im Territorium ansässige Subjekte und Objekte aushöhlt. Dieser Zweifel trifft wie oben erörtert nicht ganz zu, da der Staat einerseits die Effektivität der Kontrolle des Cyberspace tatsächlich teilweise verliert, andererseits waren ähnliche Hindernisse auch schon vor der Internetzeit zu überwinden.

Auf völkerrechtlicher Ebene darf die Souveränität eines Staates zwar nicht beeinträchtigt werden. Dadurch kann jedoch nicht verhindert werden, dass andere Staaten im Internet Gegenmaßnahmen in Bezug auf unerwünschte Veröffentlichungen, Beleidigungen, Kriegspropaganda oder Gewaltdarstellungen treffen.[138] Daraus ist

---

133 *Grimm*, 33 f.

134 *Grimm*, 70, 116; *Schliesky* 51,141; *Zippelius*, Geschichte der Staatsideen, 105 ff.; *Kielmansegg*, 242.

135 *Grimm*, 78; Engel, 38 ff.; *Schliesky*, 75.

136 *Hobe*, in: HStR, Bd. XI, § 231 Rn. 30; *Schliesky*, 138; *Di Fabio*, 34; *Isensee*, in: HStR, Bd. II, § 15 Rn.102.

137 *Schaar*, digma 2015, 40 (41).

138 *Engel*, 41 f.; *Cornils*, in: VVDStRL (76), 416 ff.; *Grewlich*, 18; *Herrera*, in: Power and security in the information age, 67 (72 ff.); *Schulze*, 24 ff.; *Hoffmann-Riem*, in: Neue Macht- und Verantwortungsstrukturen in der digitalen Welt, 27 (31 f.).

zu schließen, dass Rechtsstreite über querstaatliche Inhaltsregulierung auch in der digitalen Zeit wie zuvor im völkerrechtlichen Rechtsrahmen gelöst werden können. Hieraus folgt, dass die Unabhängigkeit eines Staates sowie seine Außensouveränität nur angegriffen sind, wenn z.B. nachrichtendienstliche Spionage über völkerrechtlich gebotene Grenzen hinausgehen. Nicht anzunehmen ist außerdem, dass innerhalb eines Staates der Cyberspace außerhalb der Kontrolle von Legislative, Exekutive und Judikative liegen.

Mit der Behauptung der Internet-Souveränität zielt man vordergründig auf die „räumliche Zuteilung von Zuständigkeiten“[139] der souveränen Staaten ab. Tatsächlich geht es aber um Machtverteilung im politischen Sinne.[140]

III. Internet-Souveränität als Hauptmotiv des chinesischen Internetrechts

In China begannen offizielle Stellen zunächst im Jahre 2009 aufgrund des Austritts von Google aus dem chinesischen Markt, Internet-Souveränität als Begriff zu verwenden.[141] Seitdem wirbt China weiterhin für dieses Konzept und erreichte in der zweiten und dritten internationalen Internet-Tagung, die seit 2014 jährlich von der chinesischen Regierung organisiert wird und in Wuzhen stattfindet, einen kleinen Fortschritt in Bezug auf die Akzeptanz der Internet-Souveränität durch die beteiligten Länder, internationalen Organisationen und Internetkonzerne. Ein verbindliches Abkommen wurde aufgrund fehlenden Konsenses allerdings nicht angenommen. Unter dem Titel „Zum Schutz des Friedens und der Sicherheit im Internet” der sog. Wuzhen-Initiative 2015 enthielt das vorgelegte Dokument die Formulierung: „die Souveränität des Staates im Cyberspace respektieren…“ Ebenso ging es darum, grundlegende Menschenrechte im Internet zu respektieren.[142]

---

139 *Thiel*, in: Der Begriff der Souveränität in der transnationalen Konstellation, 215 (225).

140 *Zhi*, Law and Social Development 2017/1, 91 (102).

141 So betont der Staatspräsident *Xi Jinping*, dass mit dem Internet nicht in die Souveränität der anderen Staaten eingegriffen und damit nicht auf Kosten der Sicherheit der anderen Staaten entwickelt werden darf, *Xi*, abrufbar <http://news.xinhuanet.com/world/2014-07/17/c_1111656037.htm> [Stand: 7.8.2019]; Cyber-Sicherheit und Internet-Souveränität als wesentliche Konzeptionen der Staatsstrategie, *Yu Zhigang*, Legal Forum 2014/6, 5 (7); Souveränität als ein striktes Verständnis in China, siehe *Hobe*, 174.

142 Wuzhen Initiative 2015, abrufbar <http://www.cac.gov.cn/2015-12/18/c_1117511999.htm> [Stand: 7.8.2019]; Im Wuzhen-Bericht 2016 wurde die Respektierung der Internet-Souveränität nochmals unterstrichen und wollte diesmal die Respektierung des Völkerrechts hinzugefügt werden, Wuzhen Bericht 2016, abrufbar <http://www.wuzhenwic.org/2016-11/18/c_61834.htm [Stand: 7.8.2019].

Anders als die Wuzhen-Iniviative 2015 und der Wuzhen-Bericht 2016, die weder als Rechtsnorm noch als internationaler Vertrag rechtlich verbindlich sind, regelt China im Jahr 2015 für sich selbst die Internet-Souveränität (oder Souveränität im Cyberspace) ausdrücklich im neu erlassenen Staatssicherheitsgesetz (SSG) und Cybersicherheitsgesetz (CSG).[143] Im SSG wird ferner festgestellt, dass zum Schutz der Souveränität, Sicherheit und Entwicklungsinteressen im Cyberspace auch die Verbreitung illegaler Informationen zu unterbinden ist (§ 25 Staatssicherheitsgesetz).

China steht, wie die meisten Staaten, aufgrund erhöhter Cyberdelikte und fehlender Kontrolle über die gesamte internationale Infrastruktur des Internets vor großen Bedrohungen. Deshalb beruft sich China zur Bekämpfung dieser Bedrohungen auf den politisch und ideologisch gefärbten Begriff der „Internet-Souveränität". Handelt es sich um die Online-*Inhalte*, liegt ein weiterer wichtiger Grund zur Regulierung darin, dass China als ein mit dem Marxismus-Leninismus lebender Staat die im Westen geltende Werteordnung, im Speziellen Menschen- und Grundrechte, nicht übernommen hat. Da, wie oben dargestellt, der Cyberspace kein rechtsfreier oder vollständig selbstregierender Raum ist und vielmehr unter der Kontrolle von den jeweiligen souveränen Staaten liegt, werden Rechtsnormen zur Bekämpfung illegaler Inhalte erlassen. In China wurde dazu bereits eine große Zahl von Gesetzen erlassen. Dies wird dogmatisch unter die Netzwerk- und Informationssicherheit, die wiederum der Staatssicherheit unterliegt, eingeordnet.

D. Zwischenergebnis

Der Cyberspace ist kein regelungsloser Raum. Mit der These der „Souveränität des Cyberspace" wurde in den USA versucht, den Ausschluss der Hoheitsgewalt aus diesem Raum zu begründen. Diese These ist abzulehnen. Gemäß der Definition aus der allgemeinen Staatslehre stellt der nur aus Netizen gebildete virtuelle Raum keinen Staat dar, da er über kein physisches Hoheitsgebiet verfügt. Eine von Netizen gewählte, weltweite Internet-Community ist auch kaum vorstellbar. Vielmehr ist es so, dass sich die Souveränität der Nationalstaaten auch auf das Cyberspace erstreckt. Die Erstreckung der traditionellen Souveränität eines Staates auf

---

143 Staatssicherheitsgesetz (**国家安全法**) vom 1.7.2015; Cybersicherheitsgesetz (**网**络安全法) vom 1.6.2017.

den Cyberspace begründet daher die *Internet-Souveränität*. Die Internet-Souveränität übernimmt Inhalte des traditionellen Souveränitätsbegriffs, der sich aus der inneren und äußeren Souveränität zusammensetzt ist. Internet-Souveränität gilt als Hauptmotiv des chinesischen Internetrechts. Eine Überbetonung dieses Begriffs ist allerdings abzulehnen. Da das Internet die Souveränität des Staates weder auf der völkerrechtlichen Ebene beeinträchtigt, noch auf der nationalen Ebene den Staat wesentlich herausfordert, darf der Staat den Cyberspace rechtlich in seinem Zuständigkeitsbereich regulieren.

3. Kapitel EIN LÜCKENLOSES UND EFFEKTIVES INTERNETSPERRENSYSTEM GEGEN SCHÄDLICHE ONLINE-INHALTE IN DER VR CHINA

A. Grundlagen

I. Die Bedeutung eines Kontrollsystems

Die rapide ansteigende Anzahl an Internetnutzern, Domainnamen und Webseiten in China lässt den Schluss zu, dass die Internetbranche in wirtschaftlicher Hinsicht von großer Bedeutung ist.[144] Dieser Bedeutungszuwachs geht aber auch mit der Zunahme der davon ausgehenden Gefahren einher. Das Kernziel der chinesischen Netzpolitik besteht in der Bekämpfung der Kriminalität und der Etablierung eines strengen Kontrollsystems in Bezug auf Meinungsäußerungen. Dies wird an den in den letzten Jahren erlassenen Gesetzen deutlich. Anknüpfend an diese Entwicklung wird ebenfalls vorgebracht, dass die Kommunikation zwischen Individuen mithilfe des Internet durch das vorhandene Politiksystem beschränkt wird und seiner Kontrolle unterliegt. Für einen sich noch zum Rechtsstaat entwickelnden Staat wie China sind die modernen Kommunikationsinfrastrukturen deswegen keine regelungsfreie Welt.

II. Der Belang der Staatssicherheit im Rahmen der Inhaltsregulierung

Bei der Online-Inhaltsregulierung nimmt vor allem die *Staatssicherheit* in chinesischen Gesetzen einen wichtigen Platz ein.[145] Dieser vage Begriff ist nicht nur auf den militärischen sowie den territorialen Bereich begrenzt, sondern umfasst nach chinesischem Verständnis auch die Sicherheit der Wirtschaft, der Kultur, der Umwelt, der Technik, der Netzwerke und der Informationstechnologie.[146] Unter diesem umfangreichen Dach verfügt die chinesische öffentliche Gewalt über einen

---

144 China Internet Network Information Center, Statistik des gegenwärtigen Standes über chinesisches Internet v. 7.2018, abrufbar unter < http://www.cac.gov.cn/2018-08/20/c_1123296882.htm > [Stand: 7.8.2019].

145 *Post*, 5 Ind. J. Global Legal Stud. 521 (539); *Li Zhu*, 6; *Zhou/Cao*, Law and Social Development, 2018/3, 40 (45 ff.).

146 *Wu*, China Legal Science 2006/4, 62 (66); *Wang Dongguang*, Peking University Law Journal 2016/5, 1289 (1291); *Li Zhu*, 60 ff.; kritisch hierzu *He Yilun*, Cass Journal of Political Science 2004/3, 117 (117); ohne Netzwerk- und Informationssicherheit gibt es keine Staatssicherheit, siehe *Yu Zhigang*, Legal Forum 2014/6, 5 (15).

praktisch unbegrenzten Ausgestaltungsspielraum. Dass hierbei in verfassungsrechtlich geschützte Grundrechte eingegriffen wird, versteht sich von selbst. Im Jahr 2000 wurde in diesem Bereich ein wichtiger Beschluss vom Ständigen Ausschuss des Nationalen Volkskongresses[147] erlassen, bei dem noch zwischen Netzwerksicherheit und der Bekämpfung illegaler Inhalte unterschieden wurde. Später wurde die Strategie der chinesischen Netzwerk- und Informationssicherheit in *einem* vom Staatsrat herausgebrachten Dokument[148], das in diesem Bereich als grundlegende Leitlinie bezeichnet werden kann, systematisch festgelegt. Dazu gehören auch Ansätze gegen die sog. schädlichen Informationen. Seitdem sind *alle* Regelungen über die illegalen Inhalte im Netz in den Bereich der Netzwerk- oder Informationssicherheit integriert.[149] Im Laufe dieser Arbeit wird sich noch herausstellen, inwiefern diese Verortung der Inhaltsregulierung zu kritisieren ist.[150]

III. Rechtsquellen

Es sei zunächst darauf hingewiesen, dass es in China eine Fülle von Arten von Rechtsvorschriften gibt, anders als in Deutschland, wo in erster Linie Gesetze, Verordnungen und Satzungen von Bedeutung sind. In China tragen die Vorschriften verschiedene Bezeichnungen wie Gesetz (法), Verordnung, (条例), Methode (办法), Regel (规定), Bestimmung (规范), Ausführungsbestimmung (细则) oder Beschluss (决定). Hiermit sind nicht unbedingt Rangfolgen verbunden. Die meisten der in dieser Arbeit relevanten Vorschriften betreffen sehr konkrete Gegenstände. Diese sind meistens von Verwaltungsorganen erlassen. Sie entfalten wie Gesetze Bindungswirkung. Daneben gibt es auch Verlautbarungen von politischen Entscheidern, die keinen Rechtscharakter aufweisen, aber doch in der Praxis von großer Bedeutung sind. Diese tragen, je nachdem, von wem sie erlassen wurden

147 Beschluss des Ständigen Ausschusses des Nationalen Volkskongresses zur Sicherung der Cyber-Sicherheit (**全国人民代表大会常**务委员会关于维护互联网安全的决定) vom 28.12.2000.

148 Ansichten der Leitungsgruppe der staatlichen Digitalisierung zur Verstärkung der Gewährung der Informationssicherheit (**国家信息化**领导小组关于加强信息安全保障工作的意见) vom 26.8.2003, in China wird dies wegen ihres Aktenzeichens in Kürze als das 27. Dokument genannt.

149 *Xie Zhiyong/Yu Peng*, Einleitung 3; *Yu Zhigang*, Legal Forum 2014/6, 5 (7); *Wang Shiwei*, Journal of Library Science in China 2015/2, 72 (75 ff.).

150 Siehe hierzu Kapitel 5.D.I.

und was sie beinhalten, Bezeichnungen wie Mitteilung (通知), Ansicht (意见), Auslegung (解释) oder Antwort (批复).

Im Bereich der chinesischen Online-Inhaltsregulierung ist vor allem der 2004 festgelegte und bis heute noch geltende politische Beschluss[151] maßgeblich, der ein vierdimensionales Kontrollsystem für Online-Inhalte vorgibt. Das heißt, dass sich das Erlassen der Rechtsnormen (1), der Vollzug der exekutiven Gewalt (2), die Selbstregulierung der Internetbranche (3) und die technische Ausgestaltung (4) zusammen auf die Kontrolle der Online-Inhalte auswirken. Danach wurden zahlreiche Rechtsvorschriften von den Verwaltungsbehörden erlassen, die die Ermächtigungsgrundlage für eine strenge Kontrolle des Internet geschaffen haben. Darüber hinaus werden alle am Markt beteiligten Telekommunikations- und Telemedienanbieter durch Konventionen zur Selbstdisziplinierung von der chinesischen Vereinigung des Internet organisiert. Nicht zuletzt spielen die traditionellen Governance-Ansätze auf den Internetplattformen ebenfalls eine zentrale Rolle.

B. Die umfangreiche Liste der schädlichen Informationen

Zunächst soll ein Überblick über die Informationen gegeben werden, die als schädlich eingestuft werden. Es sind im Ergebnis diese Informationen, die aus dem Internet ferngehalten werden sollen. Internetsperren beziehen sich stets auf diese Informationen. Die Freiheit, die für die Bürger im Internet gegeben ist, hängt in großem Maße davon ab, welche Informationen hiervon erfasst sind und in welchem Umfang Inhalte als schädlich eingestuft werden.

I. Schädliche Informationen anstatt rechtswidriger Informationen

Es ist im Wesentlichen auf den Zweck der Verwischung der Abgrenzung von Datensicherheit und Inhaltesicherheit zurückzuführen, dass Inhaltsregulierung dem Bereich der Netzwerk- und Informationssicherheit angehört. Die von der Staatssicherheit abgeleitete Netzwerk- und Informationssicherheit soll nur Datensicherheit und keine sog. Inhaltesicherheit umfassen. Die Netzwerk- und Informationssicherheit erfordert vor allem die Gewährleistung der Integrität, Nutzbarkeit, Ver-

---

151 Beschluss des Zentralkomitees der KP zur Verstärkung des Aufbaus der Regierungskompetenz (关于加强党执政能力建设的决定) vom 19.9.2004.

traulichkeit, Kontrollierbarkeit und Unveränderlichkeit des informationstechnischen Systems sowie der Daten selbst.[152] Datensicherheit stellt daher nur einen Teil der Netzwerk- und Informationssicherheit dar. Zu unterscheiden ist sie von der Inhaltesicherheit. Es ist außerdem sehr fragwürdig, ob Inhalt und Sicherheit im semantischen Sinne kombiniert werden können.

Information als eine Art natürlicher Ressourcen erlangt durch gesamtsubjektive Erkenntnis einen objektiven Inhalt, der für diese Subjekte ein gewisses Interesse repräsentiert.[153] Man unterscheidet zwischen Datum und Information nicht streng und vermischt in der Alltagssprache häufig beide Begriffe. Datum ist als verkörperte Information zu verstehen.[154] Ist das informationstechnische System defekt, wird das Datum ohne Verkörperung nicht existieren. Wird auf das System illegal oder ohne Gestattung zugegriffen und dann eine Datei gestohlen oder preisgegeben, ist die Sicherheit der Datei betroffen. Was hier nicht relevant ist, ist die Frage, ob eine Information politisch, wirtschaftlich, rechtmäßig oder rechtswidrig ist. Handelt es sich um Inhalte der Datei, wurden zunächst nur Viren, Schadsoftware oder Spam-Emails von der Netzwerk- und Informationssicherheit gedeckt. Seit Beginn der Internetregulierung werden sie wegen ihrer Störung des Informationssystems gesetzlich reguliert.

Es ist nun verständlich, warum in China gesetzgeberisch die *schädlichen* anstelle der *rechtswidrigen* Online-Informationen bevorzugt reguliert werden. Die illegalen Inhalte im Netz werden als Viren oder Schadsoftware angesehen, die von vorneherein nicht in irgendeinem Informationsgerät existieren sollen. Aufgrund dieser Denkweise werden illegale Inhalte im chinesischen Recht auch als schädliche Informationen benannt. Dies wird von der chinesischen Rechtslage, die im Folgenden ausführlich dargestellt wird, mehrfach bestätigt.[155]

---

152 Gesetzliche Definition der Netzwerks- und Informationssicherheit siehe § 76 Cybersicherheitsgesetz; ferner siehe *Ma*, Zum Informationssicherheitsrecht, 2 ff.; *Xie/Yu*, 220; *Pi*, Einleitung 7; *Holznagel*, 11 ff.

153 *Rossi*, 19; *Roßnagel*, in: Neue Macht- und Verantwortungsstrukturen in der digitalen Welt, 73 (74); *Gao Jiawei*, Administrative Law Review 2005/3, 1 (9); *Qi Aimin*, 51.

154 *Abel*, Geschichte des Datenschutzes, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 194 (199); *Simitis*, NJW 1971, 673 (673); *Albers*, 88.

155 Siehe hierzu Kapitel 3.D.-F.

II. Schädliche Information als unbestimmter Rechtsbegriff

Die sog. schädlichen Informationen als unerwünschte Inhalte wurden zunächst in § 15 der Verordnung zur Sicherheit des informationstechnischen Systems[156] geregelt, wo sie ohne weitere Definition erstmals gesetzlich den Computerviren gleichgestellt wurden. Zur Beseitigung der Unbestimmtheit dieses Begriffs erklärte das Ministerium für öffentliche Sicherheit einige Zeit später (in der sog. Antwort von 1994[157]), dass „schädliche Informationen" die im informationstechnischen System oder dessen Speichermedium gespeicherte und in Form von Computerprogrammen, Bildern, Texten, Audios etc. aufgetauchte Informationen seien, die (1) die Staatssicherheit beschädigen, vor allem die volksdemokratische Diktatur, den Sozialismus, Leitungspersonal von Partei und Staat und die nationale Solidarität angreifen; (2) die soziale Ordnung stören, vor allem Aberglauben, Obszönität oder Pornographie, Mord oder Totschlag, Anstiftung zu Straftaten; (3) die Funktionalität des informationstechnischen Systems und die Integrität sowie Vertraulichkeit der Daten gefährden.[158]

Abgesehen von diesen diffusen Begriffen steht gemäß der amtlichen Antwort jedoch fest, dass die Bedeutung der schädlichen Informationen in China deutlich über IT- und Datensicherheit im ursprünglichen Sinne hinausgeht und auch auf den Inhalt der Informationen ausgerichtet ist. Im Mittelpunkt des chinesischen IT-Rechts steht im Namen des Schutzes der IT-Sicherheit die Staatssicherheit und die soziale Ordnung an erster Stelle und nicht die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationssystemen. Dies führt dazu, dass die Bekämpfung von illegalen Inhalten in China als Unterdisziplin dem Informationsrecht, genauer gesagt, dem IT-Sicherheitsrecht zugeordnet ist und mit der Rechtsfigur „Sicherheit" zukünftig alle Lebensbereiche des Staates, der Gesellschaft sowie des Individuums ohne Abwägung zwischen Sicherheit und Freiheit erfasst werden können.

---

156 Verordnung zur Sicherheit des informationstechnischen Systems (计算机信息系统安全保护条例) vom 18.2.1994.

157 Antwort des Ministeriums für öffentliche Sicherheit für die Frage, wie man unter „schädliche Informationen" in der „Verordnung zur Sicherheit des informationstechnischen Systems" (1994) versteht (**公安部《关于**<计算机信息系统安全保护条例>**中涉及的"有害数据"**问题的批复》) vom 9.5.1996.

158 Dazu siehe auch *Ma*, Grundkurs der Informationssicherheit im Internet, 28; *Yu Zhigang*, Legal Forum 2014/6, 5 (6 f.).

Im Cyberspace galt die 1997 vom Ministerium für öffentliche Sicherheit erlassene „Bestimmungen zur Steuerung des Internet“[159] als die zweite Rechtsnorm über Inhaltsregulierung im Netz, gefolgt von der vom Staatsrat erlassenen grundlegenden Verwaltungsnorm „Methode für Internet-Informationsdienste“.[160] In § 5 der „Bestimmung“ und dem § 15 der „Methode“ wurde ein Muster der sog. schädlichen Online-Informationen bestimmt.[161] Zur klaren Analyse solcher illegalen Online-Inhalte sollen sie drei Kategorien zugeordnet werden, und zwar gibt es politische, soziale und private schädliche Informationen.[162] Dies geht einerseits auf den von der Antwort 1994 bestimmten Regelungsrahmen zurück. Andererseits entspricht dies der Rechtsprechung, in der ein Volksgericht die schädlichen Informationen definiert hat: und zwar als solche Informationen, die das rechtliche Interesse des Staats, der Gesellschaft sowie des Privaten gefährden oder beeinträchtigen.[163]

III. Auf Politik bezogene schädliche Informationen

Politische schädliche Informationen sind solche Online-Inhalte, die (1) gegen verfassungsrechtliche Grundprinzipien verstoßen, (2) die Staatssicherheit gefährden, Staatsgeheimnisse preisgeben, die Souveränität unterminieren oder die nationale Einheit gefährden und (3) die nationale Würde und Staatsinteressen beschädigen.[164] Alle Informationen hierzu sind mit dem zentralen unbestimmten Rechtsbegriff der „Staatssicherheit“ eng verbunden und es wird in der Praxis immer wieder wegen Verstößen dagegen bestraft. Es stellt sich deshalb die Frage, wie dieser zentrale Begriff der „Staatssicherheit“ definiert wird.

Gesetzlich definiert ist die Staatssicherheit als ein stabiler Zustand, in dem Staatsmacht, Souveränität, Einheit des Staates, Volkswohl, nachhaltige Entwicklung der Wirtschaft und Gesellschaft oder ein anderes starkes Interesse des Staates nicht gefährdet wird (§ 2 SSG).[165] Dies ist die erste gesetzliche Bestimmung über

---

159 Bestimmungen zur Steuerung des Internet 计算机信息网络国际联网安全保护管理办法 vom 30.12.1997.

160 Methode für Internet-Informationsdienst (互联网信息服务管理办法) vom 25.9.2000.

161 Zur ausführlichen Darstellung diese Muster der sog. schädlichen Online-Informationen siehe Becker, 104.

162 *Yin Jianguo*, Politcal Science and Law, 2015/1, 102 (107 ff.); *Wang Shiwei*, Journal of Library Science in China 2015/2, 72 (78); *Xie/Ji*, Journal of Chinese Academy of Governance 2010/5, 94 (95); *Hu Ling*, in: Grundrecht und Konstitutionalismus, 411 (412).

163 *Wang Jianjun*, Legal Daily (法制日报) v. 12.9.2006.

164 Zur ausführlichen Darstellung siehe *Becker*, 104.

165 *Wang Zuofu*, 1; *Zhang Jun*, 12; *Zhang Mingkai*, 593; *Wang Dongguang*, Peking University Law Journal 2016/5, 1289 (1291).

Staatssicherheit in China. Der Begriff ist gemäß § 3 SSG sehr weit zu fassen, so dass die politische, wirtschaftliche, militärische, kulturelle und soziale Sicherheit sowie die Volkssicherheit inkludiert sind.

Nach hier vertretener Ansicht ist es jedoch nicht sinnvoll, die Staatssicherheit als Kernbegriff in einem derart weiten Sinne zu begreifen, da so die Gefahr besteht, dass sozialen und wirtschaftlichen Unruhen schlicht mit der Berufung auf die Staatssicherheit begegnet werden könnte.[166] Deshalb sollte der Begriff auf die Staatsicherheit im politischen Sinne beschränkt werden. In der alten Fassung des SSG waren einige politische Fallkonstellationen aufgelistet (§ 4 SSG a.F.), die allerdings dem Umfang des Strafgesetzbuchs Chinas nicht ganz entsprachen.[167] Die politischen Fallkonstellationen umfassen gemäß § 4 SSG a.F. solche Taten, die den Umsturz der Regierung betreffen, den Staat spalten oder den Sozialismus stürzen (1), an einer Spionageorganisation teilnehmen oder Aufträge von Seiten einer Spionageorganisation und ihrer Agenten entgegennehmen (2), Staatsgeheimnisse stehlen, ankaufen oder rechtswidrig liefern (3) und Beamte zum Amtsmissbrauch verleiten oder bestechen (4). Zwar entsprachen die gesetzlichen Fallkonstellationen über Staatssicherheit den Bestimmungen im chinesischen Strafgesetzbuch (chStGB)[168] nicht ganz. Ihre Auflistung kann aber dennoch bei der teleologischen Auslegung des unbestimmten Rechtsbegriffs der Staatssicherheit helfen. In der aktuellen Fassung findet sich ein Verweis auf die Vorschriften des chStGB nicht mehr.

Zur Auseinandersetzung mit dem unbestimmten Begriff der Staatssicherheit ist es angezeigt ins Detail zu gehen. Ansonsten verliert man sich in der stark von Ideologie geprägten chinesischen Gesetzgebung, insbesondere in den verfassungsrechtlichen Grundprinzipien, in der nationalen Würde oder im Staatsinteresse. Im Folgenden kommen daher nur die für die politische Staatssicherheit gefährlichen Informationen im Cyberspace in Betracht, wobei die zur Preisgabe von Staatsgeheimnissen oder Untergrabung der Staatsgewalt führenden Informationen juristisch analysierbar sind und in der Gerichtspraxis tatsächlich behandelt werden.

---

166 *He Yilun*, in: Cass Journal of Political Science 2004/3, 117 (117); *He/Wang*, Political Science and Law 2018/7, 2 (13); *Wang Shiwei*, Journal of Library Science in China 2015/2, 72 (79).

167 *Wu Qingrong*, China Legal Science 2006/4, 62 (66); *Li Zhu*, 142; *Hu Xia*, Criminal Science 2017/5, 30 (32); *Wang Shizhou*, Crininal Science 2012/8, 9 (14 f.).

168 Das chinesische Strafgesetzbuch (刑法) vom 14.3.1997.

1. Preisgabe von Staatsgeheimnissen

a) Begriff des Staatsgeheimnisses

Staatsgeheimnisse betreffen Angelegenheiten, die mit Staatssicherheit und Staatsinteresse verbunden sind, nach rechtlichen Verfahren bestimmt und in einem beschränkten Zeitraum nur einem bestimmten Personenkreis zur Verfügung gestellt werden (§ 2 SGG).[169] Dabei sind formelle und materielle Merkmale zu unterscheiden.[170] In materieller Hinsicht hängt die Einordnung als Staatsgeheimnis davon ab, ob die Information für die Staatssicherheit und das Staatsinteresse entscheidend ist. Betroffen sind hiervon schwerwiegende Entscheidungen über Staatsangelegenheiten, Tätigkeiten der Landesverteidigung, Tätigkeiten in auswärtigen Angelegenheiten, der Entwicklung der Wirtschaft, Gesellschaft, Wissenschaft und Technik und die Verfolgung von Straftaten (§ 9 Abs. 1 SGG). Nicht auffällig und nicht ungewöhnlich ist in China, die geheimen Informationen der kommunistischen Partei den Staatsgeheimnissen zuzuordnen (§ 9 Abs. 2 SGG).[171] Daraus resultiert, dass ein materielles Staatsgeheimnis wiederum auf die abstrakte Staatssicherheit ausgerichtet ist und die genannten Bereiche des § 9 Abs. 2 SGG zur Konkretisierung des Begriffs nur bedingt beitragen können.

Entscheidend ist vielmehr das formelle Kriterium, ob die betroffenen Angelegenheiten nach dem gesetzlichen Verfahren von den zuständigen Behörden als Staatsgeheimnis eingestuft werden. Denn es ist den chinesischen Gerichten nicht gewährt, die von den Behörden unter das Staatsgeheimnis gestellten Angelegenheiten daraufhin zu beurteilen, ob sie tatsächlich dazu gehören. Über diese Kompetenz verfügt ausschließlich die zuständige Verwaltungsbehörde (§ 46 SGG). Hinzu kommt ebenfalls die Frage, ob die Verwaltungsbehörde *vor Gericht* den Betroffenen untersagen darf, die auf das Staatsgeheimnis bezogene Information zu erhalten, wenn der Kläger (Bürger) das Recht auf den freien Zugang zu solchen Informationen geltend macht und die Behörde nur behauptet, dass die begehrten Informationen unter das Staatsgeheimnis fallen. Dazu hat das chinesische Volksgericht freilich zugunsten der Behörde entschieden. In § 5 der Bestimmungen des Obersten

---

169 *Wang Zuofu*, 46; *Zhang Mingkai*, 599; *Wang Shizhou*, Crininal Science 2012/8, 9 (13).

170 *Wang Zuofu*, 50; *Wang Shizhou*, Crininal Science 2012/8, 9 (14); *Zhang Zhengping*, Studies in Law and Business 2012/2, 83 (87).

171 *Wang Zuofu*, 46; *Zhang Zhengping*, Studies in Law and Business 2012/2, 83 (86); *Wang Xixin*, Political Science and Law 2009/3, 2 (6).

Volksgerichts zu Fragen bei der Behandlung von Fällen der Offenlegung von Regierungsinformationen[172] wird es dem Gericht im Fall der Offenlegung von Regierungsinformationen untersagt, Staatsgeheimnisse im materiellen Sinne zu überprüfen.[173] Aufgrund der fehlenden Prüfungskompetenz des Gerichts könnte die zuständige Verwaltungsbehörde im Zweifel willkürlich entscheiden, welche schädlichen Informationen gegen den Staatsgeheimnisschutz verstoßen.

b) Preisgabe

Bei der Preisgabe von Staatsgeheimnissen ist des Weiteren im chinesischen Strafrecht zwischen Verrat von Staatsgeheimnissen ans Ausland (§ 111 chStGB) und Preisgabe von Staatsgeheimnissen – auch im Inland – (§ 398 chStGB) zu unterscheiden. Diese Tatbestände finden gemäß § 6 Auslegung des Obersten Volksgerichts zu Fragen der konkreten Anwendung des Rechts bei der Behandlung von Fällen des Verschaffens, Kaufens und illegalen Anbietens von Staatsgeheimnissen und der Informationen[174] auch für Online-Aktivitäten Anwendung.[175] Die beiden Straftaten unterscheiden sich in erster Linie darin, ob Staatsgeheimnisse im Inland oder im Ausland preisgegeben werden.[176] Alle chinesischen Medien sowie die sog. „neuen" Medien (z.B. Soziale Netzwerke) stehen im Inland vollständig unter staatlicher Kontrolle. Deshalb sind Fälle mit Auslandsbezug typisch für „Whistleblower". § 111 chStGB ist somit im Vergleich zu § 398 chStGB von maßgeblicherer Bedeutung.

c) Fall *Shi Tao*

Aufgrund des Verstoßes gegen § 111 chStGB wurde etwa der Journalist *Shi Tao* als erster Dissident, der geheime Dokumente über das Internet ins Ausland verschickte, zu zehn Jahren Haft verurteilt.[177] Bei diesen umstrittenen Dokumenten

---

172 Bestimmungen des Obersten Volksgerichts zu einigen Fragen bei der Behandlung von Fällen der Offenlegung von Regierungsinformationen (关于审理政府信息公开行政案件若干问题的规定) vom 13.12.2010.

173 *Wei*, 36; *Wang Xixin*, Political Science and Law 2009/3, 2 (8 ff.); *Jiang/Li*, Political Science and Law 2009/3, 12 (19 ff.).

174 Auslegung des Obersten Volksgerichts zu einigen Fragen der konkreten Anwendung des Rechts bei der Behandlung von Fällen des Verschaffens, Verschaffens, Kaufens und illegalen Anbietens von Staatsgeheimnissen und sonstigen sensiblen staatlichen Informationen (最高人民法院关于审理为境外窃取、刺探、收买、非法提供国家秘密、情报案件具体应用法律若干问题的解释) vom 17.1.2001.

175 *Wang Zuofu*, 49; *Zhang Jun*, 51; *Zhang Mingkai*, 599.

176 *Wang Zuofu*, 53, 1896; *Zhang Mingkai*, 1099.

177 (2005) Xiang Gao Fa Xing Yi Zhong Zi Nr. 177 (湘高法刑一中字第 177 号).

handelte es sich um eine von den Verwaltungsbehörden der KP und des Regierungsbüros[178] erteilte schriftliche Mitteilung, in der den chinesischen Massenmedien untersagt wird, über das Tian'anmen-Massaker und Falun Gong zu berichten. *Tao Shi*, ein bei einer regionalen Zeitung tätiger Journalist, erfuhr den Inhalt bei einer Sitzung und leitete danach seine Notizen einem ausländischen Freund weiter. Folge hiervon war, dass sich diese interne Mitteilung im Internet verbreitete. In der Verhandlung hat das Gericht ein Gutachten von der für den Schutz des Staatsgeheimnisses zuständigen Behörde angenommen, jedoch ohne zu überprüfen, ob die Mitteilung zum Zeitpunkt des Weiterleitens tatsächlich als Staatsgeheimnis einzuordnen war.[179]

d) Fall *Gao Yu*

Im zweiten Fall, der auch viel Aufsehen erregte, ging es ebenfalls um eine interne Mitteilung innerhalb der KP, die aufgrund ihres Inhalts über den „Status quo im chinesischen ideologischen Bereich" (das sog. Nr. 9 Dokument)[180] von großer Bedeutung war. Diese Mitteilung wurde allerdings schon vor der Weitergabe von der Journalistin *Gao Yu* an einen ausländischen Webseiten-Betreiber auf einer anderen Internetseite veröffentlicht. Es stellte sich daher die Frage, ob die bereits allgemein zugängliche Information noch als Staatsgeheiminis zu qualifizieren war. In Bezug auf die Definition des Staatsgeheimnisses spielt die allgemeine Zugänglichkeit keine Rolle, weil es einerseits nicht auszuschließen ist, dass die weitere Preisgabe der Information die Staatssicherheit und das Staatsinteresse noch gefährden könnte (materielles Merkmal). Andererseits bleiben sie gemäß § 16 Satz 1 der Verordnung für Anwendung des Staatsgeheimnisgesetzes[181] unverändert in der Kategorie des Staatsgeheimnisses, soweit sie nicht aus dieser Liste entfernt werden (formelles Merkmal). Abgesehen von dieser Problematik war es sachlich nicht klar, ob in diesem Fall die angebliche geheime Mitteilung tatsächlich dem Staatsgeheimnis zugeordnet war. Die 71-jährige kritische Journalistin *Gao Yu* wurde

---

178 中共中央办公厅和国务院办公厅.

179 (2005) Xiang Gao Fa Xing Yi Zhong Zi Nr. 177 (湘高法刑一中字第 177 号).

180 Mittelung des zentralen Büros der KP zum „Rundschreiben zur aktuellen Situation in Sachen Ideologie" (中共中央办公厅印发〈关于当前意识形态领域情况的通报〉的通知) vom 22.4.2013.

181 Verordnung für Anwendung des Staatsgeheimnisgesetzes (中华人民共和国保守国家秘密法实施条例) vom 17.1.2014.

letztlich wegen Verrats von Staatsgeheimnissen ans Ausland (§ 111 chStGB) zu fünf Jahren Haft verurteilt.[182]

2. Aufhetzung zur Untergrabung der Staatsgewalt

Neben § 111 chStGB wird § 105 Abs. 2 chStGB (Aufhetzung zur Untergrabung der Staatsgewalt) in Bezug auf politisch sensible Informationen häufig in der Gerichtspraxis angewandt, um Kritik an der politischen Führung zu unterbinden. Hervorzuheben ist, dass der Begriff der Untergrabung im chinesischen Strafrecht sehr weit zu fassen ist. Inhaltlich umfasst „Untergrabung" alle illegalen Mittel, die einem Umsturz oder einer Usurpierung der Gesetzgebung, vollziehenden Gewalt, Rechtsprechung, Militär und Staatsmacht dienen.[183]

Der Straftatbestand des § 105 Abs. 1 chStGB (Untergrabung der Staatsgewalt) ist von der Form der Untergrabung unabhängig, d.h. nicht entscheidend ist, ob der Täter mit oder ohne Gewalt, öffentlich oder heimlich handelt.[184] Als Handlungsdelikt setzt § 105 Abs. 1 chStGB keinen Erfolg voraus. Es genügt bereits die Organisation, Planung oder Umsetzung der Untergrabung gegen die Staatsmacht.[185] Da der Tatbestand des § 105 Abs. 1 chStGB sehr weit ist, ist der Frage nachzugehen, ob schon Kritik an der politischen Führung der KP oder der Staatsgewalt unter „Aufhetzung zur Untergrabung der Staatsgewalt" zu subsumieren ist. Das Oberste Volksgericht Chinas hat 1998 in einer Erklärung über die Rechtsanwendung gegenüber illegaler Presse klargestellt, dass sensible Inhalte in Presseerzeugnissen Mittel der Untergrabung i.S.v. § 105 Abs. 2 chStGB sein können (§ 1 der Auslegung des Obersten Volksgerichts zu einigen Fragen der konkreten Anwendung des Rechts bei der Behandlung von Fällen der strafrechtswidrigen illegalen Presse[186]). Aufgrund der Orientierung der Meinungskontrolle im Netz an der Presse erfüllt die Online-Aufhetzung gemäß § 2 Nr. 1 des Beschlusses des Ständigen Ausschusses des Nationalen Volkskongresses zur Sicherung der Cyber-Sicherheit somit den Tatbestand des § 105 Abs. 2 chStGB.[187]

---

182 (2014) San Zhong Xing Chu Zi Nr. 00755 (三中刑初字第 00755 号); das Aktenzeichen des Urteils in der Folgeinstanz ist nicht bekannt gemacht.

183 *Zhang Jun*, 29; *Zhang Mingkai*, 596.

184 *Zhang Jun*, 29; *Zhang Mingkai*, 596.

185 *Zhang Jun*, 29; *Zhang Mingkai*, 596.

186 Auslegung des Obersten Volksgerichts zu einigen Fragen der konkreten Anwendung des Rechts bei der Behandlung von Fällen der strafrechtswidrigen illegalen Presse (最高人民法院关于审理非法出版物刑事案件具体应用法律若干问题的解释) vom 23. 12.1998.

187 *Zhang Jun*, 30; *Zhang Mingkai*, 596.

Eine ganze Reihe von Netzdissidenten wurde demnach wegen Verstoßes gegen § 105 Abs. 2 chStGB zu Freiheitsstrafen verurteilt. Am bekanntesten ist das Urteil gegen den Friedensnobelpreisträger *Liu Xiaobo*, der langjährig Kritik an der KP in China äußerte und sie im Internet veröffentlichte.[188] Auch in anderen Fällen wurden Aktivisten oder Webseiten-Betreiber aus dem gleichen Grunde zu Freiheitsstrafen verurteilt.[189]

IV. Sozial schädliche Informationen

Der Cyberspace ist nicht nur Abbild des sozialen Lebens geworden,[190] sondern fungiert auch als ein Katalysator von sozialen Veränderungen. Folgende rechtswidrigen Informationen im Cyberspace, die dazu dienen, von der politischen Führung unerwünschte soziale Veränderungen herbeizuführen, sind in China häufig Gegenstand gerichtlicher Entscheidungen.

1. Verbreitung von Irrlehren und Aberglauben

Die in § 300 Abs. 1 chStGB normierte Straftat verbietet die Organisation oder die Befolgung von Irrlehren und Aberglauben, deren Ziele im Verstoß gegen staatliche Gesetze oder Verwaltungsrechtsnormen liegen.[191] Darunter fällt gemäß § 1 Abs. 1 Nr. 3 der zweiten Auslegung des Obersten Volksgerichts und der Obersten Volksstaatsanwaltschaft zu einigen Fragen der konkreten Anwendung des Rechts der Behandlung von Fällen der Organisation und Befolgung von Irrlehren[192] auch das Herstellen oder Verbreiten von einschlägigen Informationen im Internet. Für das Gericht ist es entscheidend, ob die betroffenen Informationen mit einer bereits als illegal bewerteten Religionsgruppe verbunden sind. In den letzten Jahren sind zahlreiche Religionsgruppen von „Falun Gong“ oder dem „Eastern Lightning

---

188 (2009）Yi Zhong Xing Chu Zi Nr. 3901 (一中刑初字第 3901 号); das Aktenzeichen des Urteils in der zweiten Instanz ist leider nicht Bekannt gemacht.

189 (2001) Cheng Xing Chu Zi Nr. 49 (成刑初字第 49 号); (2003) Shi Xing Chu Zi Nr. 170 (石刑初字第 170 号); (2004) Xiao Zhong Xing Chu Zi Nr. 20 (孝中刑初字第 20 号); (2004) E Xing Er Zhong Zi Nr. 153 (鄂刑二终字第 153 号); (2015) Guo Xing Chu Zi Nr. 00009 (涡刑初字第 00009 号); (2012) Qing Zhong Xing Chu Zi Nr. 35 (庆中刑初字 35 号).

190 *Hobe*, in: HStR, Bd. XI, § 231 Rn. 8.

191 *Wang Zuofu*, 1319; *Zhang Jun*, 1235 ff.; *Zhang Mingkai*, 946.

192 Zweite Auslegung des Obersten Volksgerichts und der Obersten Volksstaatsanwaltschaft zu einigen Fragen der konkreten Anwendung des Rechts der Behandlung von Fällen der Organisation und Befolgung von Irrlehren (最高人民法院、最高人民检察院关于办理组织和利用邪教组织犯罪案件具体应用法律若干问题的解释(二)) vom 6.11.2001.

Cult“[193] deswegen bestraft worden, obwohl einige der Veröffentlichungen davon nur auf ein Minimum begrenzt waren oder von einem kleinen Personenkreis abgerufen wurden.[194] Im chinesischen Recht kommen in diesen Fällen die verfassungsrechtlich geschützte Freiheit der Rede (Art. 35 chVerf[195]) und die Religionsfreiheit (Art. 36 Abs. 1 chVerf) allerdings nicht zur Anwendung, weil rechtswidrige Religion von vornherein nicht geschützt sind.[196]

2. Verbreiten von Gerüchten

Das Herstellen oder das Verbreiten von Gerüchten ist ein normales Phänomen, das der menschlichen Natur entspricht. Unter Gerüchten versteht man Informationen, die nicht bestätigt oder bewiesen, aber bereits in der Gesellschaft verbreitet sind. Darunter können Meinungen oder Tatsachenbehauptungen, wahre oder unwahre Äußerungen, politische Kritik oder private Unzufriedenheit fallen.[197]

Durch eine hochumstrittene Justizauslegung des Obersten Volksgerichts sowie der Obersten Volksstaatsanwaltschaft[198] war der Straftatbestand der Belästigung der Allgemeinheit[199] gemäß § 293 chStGB eine Norm zur umfassenden Kontrolle von Gerüchten auf Internetplattformen geworden. Strafbar gemäß § 293 Abs. 1 Nr. 4 chStGB ist das Verbreiten unwahrer Informationen oder solcher Informationen, die die öffentliche Ordnung erheblich stören (§ 5 Auslegung des Obersten Volks-

---

193 Falun Gong ist eine chinesische Qigong-Praktik der buddhistischen Schule. 1999 haben ca. 10.000 Mitglieder an den friedlichen Demonstrationen vor dem Gelände der Zentralregierung teilgenommen. Seitdem wird Falun Gong als eine unrechtmäßige Organisation bezeichnet, weil sie den Aberglauben verbreiten und die Massen betrügen würden. Dazu siehe *Ownby*, 23 ff. Eastern Lightning Cult oder „Kirche des Allmächtigen Gottes“ ist eine Religionsgemeinschaft in China und behauptet, dass die Wiederkunft Jesus Christus in China bereits stattgefunden hat. Der Organisation wird vorgeworfen, dass zahlreiche Straftaten, z.B. Diebstähle oder Angriffe auf Menschen, von den Mitgliedern dieser Religionsgemeinschaft begangen wurden. Dazu siehe *Dunn*, 68 ff.

194 (2014) Jia Xing Chu Zi Nr. 184 (郏刑初字第 184 号).

195 Verfassung der Volksrepublik China (宪法) vom 4.12.1982.

196 (2014) Meng Xing Chu Zi Nr. 00191 (**孟刑初字第** 00191 **号**); (2015) Jiao Xing San Zhong Zi Nr. 00044 (**焦刑三**终字第 00044 **号**).

197 *Liu/Wang*, Journal of Capital Normal University (Social Sciences Edition), 2015/5, 56 (56 f.); *Sun/Lu*, Law Science (**法学**) 2013/11, 3 (8 f.); *Liu Xianquan*, The Jurist 2016/6, 105 (106 f.); *Zhang Xinyu*, Studies in Law and Business 2016/3, 63 (64); *Li Dayong*, Law Science 2014/1, 100 (100 f.).

198 Auslegung des Obersten Volksgerichts und der Obersten Volksstaatsanwaltschaft zu einigen Fragen der Anwendung des Rechts bei der Behandlung von Fällen der Verleumdung mittels Internet, (**最高人民法院、最高人民**检察院关于办理利用信息网络实施诽谤等刑事案件适用法**律若干**问题的解释) vom 6. 9.2013.

199 寻衅滋事

gerichts und der Obersten Volksstaatsanwaltschaft zu einigen Fragen der Anwendung des Rechts bei der Behandlung von Fällen der Verleumdung mittels Internet).[200] Um die Anwendung des § 293 Abs. 1 Nr. 4 chStGB zu begrenzen, findet später § 291a Abs. 2 chStGB durch die 9. Änderung des chStGB als eine Sondernorm vor § 293 Abs. 1 Nr. 4 chStGB Anwendung.[201] Strafrechtswidrig ist gemäß § 291a Abs. 2 chStGB das Verbreiten unwahrer Informationen zu Gefahren, Epidemien oder Katastrophen im Internet oder auf anderen Medienplattformen.

Die betroffene Justizauslegung ist aufgrund der unklaren Konturen nicht unumstritten. Die Störung der öffentlichen Ordnung setzt gemäß dem Tatbestand des § 293 Abs. 1 Nr. 4 chStGB einen öffentlichen Raum voraus,[202] wobei der Cyberraum nicht unbedingt öffentlich zugänglich ist. Die Annahme, dass alle Internetforen, soziale Netzwerke, Bewertungsportale oder Webseiten die Eigenschaft der Öffentlichkeit innehaben, ist abzulehnen. Im Hinblick auf geschlossene Online-Communities und verschlüsselte Kommunikation zwischen Privaten, ist anzunehmen, dass in diesen geschlossenen Räumen ein privater und kein öffentlicher Raum existiert. In diesem Sinne sollte es keine Schwierigkeit bereiten, herauszufinden, ob eine bestimmte Plattform oder Kommunikationsform dem sozialen oder privaten Raum zugeordnet wird, wenn Posts zunächst nur in einem bestimmten Freundeskreis veröffentlicht werden. In der Rechtspraxis wurden solche Täter, die nur im geschlossenen Freundkreis oder in der geschlossenen Gruppe gepostet haben, allerding nicht selten wegen Belästigung der Allgemeinheit oder Störung der öffentlichen Ordnung bestraft.[203]

Es müssten bei §§ 291a Abs. 2, 293 Abs. 1 Nr. 4 chStGB noch unwahre oder falsche Tatsachen verbreitet werden, die eine erhebliche Störung der gesellschaftlichen Lebenswirklichkeit herbeiführen. Dabei sind zwei Merkmale entscheidend.

---

200 *Wang Zuofu*, 1276; *Zhang Jun*, 1194; *Zhang Mingkai*, 935.

201 (2016) Wan 12 Xing Zhong Nr. 216 (皖 12 刑终 216 号); *Wang Zuofu*, 1262; *Zhang Jun*, 1184; *Zhang Mingkai*, 932.

202 *Wang Zuofu*, 1276; Zhang Jun, 1280; *Zhang Mingkai*, 937.

203 (2014) Mi Xing Chu Zi Nr. 356 (密刑初字第 356 号); (2014) San Zhong Xing Zhong Zi Nr. 00906 (三中刑终字第 00906 号); (2015) Shuang Xing Chu Zi Nr. 357 (双刑初字第 357 号).

Zunächst muss es sich um eine unwahre Tatsache handeln. Die Meinungsfreiheit gemäß Art. 35 chVerf gewährt jedem, in jeder Form eigene Werturteile und Dafürhalten zu äußern.[204] Sachlich schützt Art. 35 chVerf aber nur die politische Meinung, damit sich der Grundrechtsberechtigte an den öffentlichen Angelegenheiten beteiligen und bei der Meinungsbildung der Öffentlichkeit mitwirken kann.[205] Nicht geschützt wird von Art. 35 chVerf die Verbreitung unwahrer oder falscher Tatsachen, da diese nicht zur Meinungsbildung beitragen können.[206] Handelt es sich um Kritik oder eine negative Bewertung der öffentlichen Gewalt sowie zur Kommunistischen Partei, werden solche Meinungen von der Meinungsfreiheit gemäß Art. 35 chVerf geschützt. In der Wirklichkeit sieht die chinesische Rechtsprechung häufig allerdings so aus, dass unerwünschte Meinungen mit unwahren oder falschen Tatsachenbehauptungen gleichgesetzt werden.[207] Dadurch wird Kritik oder eine negative Bewertung der öffentlichen Gewalt oder der Kommunistischen Partei als unwahre oder falsche Tatsachenbehauptung eingestuft und somit vom Schutzbereich des Art. 35 chVerf nicht gedeckt.

Das zweite Merkmal ist die erhebliche Störung der sozialen Ordnung. Die Tatbestände der §§ 291a Abs. 2, 293 Abs. 1 Nr. 4 chStGB liegen daher dem Wortlaut nach nicht vor, wo durch unwahre oder falsche Tatsachenbehauptungen nur geringfügige Effekte im Netz verursacht werden.[208] In der Rechtsprechung ist jedoch das Gegenteil zu beobachten.[209] Die Rechtsprechung der Volksgerichte schafft eine extensive Deutung der „Störung der sozialen Ordnung“, wodurch ihnen ein

---

204 *Hu*, 205; *Lin Laifan*, 371; *Zhang Qianfan*, 540; *Wei Yongzheng*, Cass Journal of Foreign Law 2001/1, 69 (69).

205 *Hu*, 205; *Zhang Mingkai*, China Legal Science 2015/3, 60 (69); *Lin Laifan*, 372; *Zhang Qianfan*, 542.

206 *Lin Laifan*, 373; *Zhang Qianfan*, 541; *Hu* 206; *Zhang Qianfan*, Law Science 2015/4, 3 (4).

207 *He Qinglian*, The fog of Censorship – Media Control in China, 32; *Li Dayong*, Law Science 2014/1, 100 (102); *Liu Xianquan*, The Jurist 2016/6, 105 (107).

208 *Wang Zuofu*, 1280; *Zhang Jun*, 1195; *Zhang Mingkai*, 1280; *Liu/Wang*, Journal of Capital Normal University (Social Sciences Edition), 2015/5, 56 (61 f.); *Sun/Lu*, Law Science (法学) 2013/11, 3 (12 f.); *Liu Xianquan*, The Jurist 2016/6, 105 (115); *Zhang Xinyu*, Studies in Law and Business 2016/3, 63 (67); *Zhang Qianfan*, Law Science 2015/4, 3 (6); dagegen in der Rechtspraxis, (2015) Xiang Xing Chu Zi Nr. 508 (香刑初字第 508 号); (2014) Fen Xing Chu Zi Nr. 229 (汾刑初字第 229 号); (2015) Lv Xing Zhong Zi Nr. 93 (吕刑终字第 93 号); (2013) Chao Xing Chu Zi Nr. 2584 (朝刑初字第 2584 号); (2015) Le Xing Chu Zi Nr. 2 (乐刑初字第 2 号); (2015) Dong Xing Zhong Zi Nr. 41 (东刑终字第 41 号).

209 (2014) Mi Xing Chu Zi Nr. 356 (密刑初字第 356 号); San Zhong Xing Zhong Zi Nr. 00906 (三中刑终字第 00906 号); (2013) Xiang Fa Xing Chu Zi Nr. 359 (湘法刑初字第 359 号).

weiter Einschätzungs- und Prognosespielraum eingeräumt wird. Damit entwickelte sich das chinesische Strafrecht zu einem effektiven Instrument zur Unterdrückung von Gerüchten im Internet und führte damit auch Einschüchterungseffekte herbei.

3. Andere unerlaubte sozialschädliche Inhalte

Die flächendeckende Liste der anderen unerlaubten sozialschädlichen Online-Inhalte spiegelt das besondere Schutzinteresse des chinesischen Gesetzgebers zur Sicherstellung eines sog. sauberen Netzes wider. Soweit es um Pornografie, Glücksspiel, Gewalt, Mord, Todschlag, Terrorismus oder Anstiftung zu Straftaten geht, decken sich jeweils die Anwendungsmöglichkeiten der Strafrechts- und Verwaltungsstrafrechtsparagrafen. Das Oberste Volksgericht lässt des Weiteren durchaus eine erweiternde und analoge Justizauslegung der Vorschriften zu.[210] Im Jahr 2015 wurden Terror-Informationen im Cyberspace mit dem Anti-Terror-Gesetz[211] abschließend geregelt, in dem allerdings keine Definition über verbotene Online-Inhalte zu finden ist. Noch unklar sind zudem die Definitionen von „Sozialmoral“ und dem „nationalen Kulturgut“, die in China ebenfalls vom positivem Recht geschützt werden.[212]

V. Private schädliche Informationen

Bei privat schädlichen Informationen handelt es sich um Inhalte, die die persönlichen und staatsbürgerlichen Rechte verletzen. In der Praxis konzentriert sich die

---

210 Erste Auslegung des Obersten Volksgerichts und der Obersten Volksstaatsanwaltschaft zu Fragen der Anwendung des Rechts beim Erzeugen, Kopieren, Veröffentlichen, Verkaufen und Verbreiten von pornografischen digitalen Informationen mittels Internet, mobilen Kommunikationsendgeräten und Telekommunikationsanlagen (**关于**办理利用互联网、移动通讯终端、**声**讯**台制作**、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释(**一**)) vom 3.9.2004; zweite Auslegung dazu vom 2.2.2010; Auslegung des Obersten Volksgerichts und der Obersten Volksstaatsanwaltschaft zu Fragen der Anwendung des Rechts bei der Behandlung von Fällen des Glückspiels (**最高人民法院、最高人民**检察院关于办理赌博刑事案件具体应用法律若干问题的解释) vom 11.5.2005.

211 Anti-Terror-Gesetz (**反恐法**) vom 27.12.2015.

212 Die Bestimmungen über die soziale Moral und die nationale Kultur findet man in § 16 Nr. 9 Verwaltungsregeln für audiovisuelle Programme im Internet (**互**联网视听节目**服**务管理规定) vom 20.12.2007, § 14 Nr. 9 Verwaltungsregeln zum Internet-Café (**互**联网上网服务营业场所管理条例) vom 6.2.2016, § 17 Nr. 9 vorläufigen Verwaltungsregeln zur Kultur im Netz (**互**联网文化管理暂行规定) vom 17.2.2011 und § 24 Nr. 9 Verwaltungsregeln zur Online-Presse (**网**络出版服务管理规定) vom 4.2.2016.

umfangreiche Kategorie der staatsbürgerlichen Rechte auf zwei Bereiche. Zum einen sind nationaler Hass, nationale Diskriminierung und die Solidarität beschädigende Meinungsäußerungen oder Tatsachen hiervon erfasst. Zum anderen kommen häufig die Fälle in Betracht, bei denen es um (radikale) Volksgruppen geht.[213] In Gerichtsentscheidung sind als radikale Volksgruppen nahezu ausschließlich die Uighuren in Erscheinung getreten. Außerdem sind Beleidigung und Verleumdung zum Schutz der persönlichen Rechte gesetzlich verboten. Dazu haben das Oberste Volksgericht und die Oberste Volksstaatsanwaltschaft durch den Erlass der Justizauslegungen[214] den Cyberraum herangezogen, um die beiden Aspekte der „privat schädlichen Informationen" näher zu bestimmen und von anderen abzuheben. Diese Justizauslegung hat später in der Literatur zahlreiche Kritik hervorgerufen, weil sie weit über die Auslegungsgrenze der Judikative hinausgeht.[215] Hochumstritten ist dabei, dass 5.000-maliges Lesen oder 500-maliges Weiterleiten eines Online-Posts gemäß § 2 Nr. 1 der Auslegung des Obersten Volksgerichts und der Obersten Volksstaatsanwaltschaft zu einigen Fragen der Anwendung des Rechts bei der Behandlung von Fällen der Verleumdung mittels Internet als *erhebliche Folge* der Straftat (§ 246 chStGB) interpretiert werden kann.[216] Umstritten ist zudem der Schutz der Hoheitsträger gegen Beleidung oder Verleumdung von Bürgerinnen oder Bürgern, die eigentlich nur Kritik an der Regierung oder der politischen Elite äußern.[217]

---

213 (2014) Xin Xing Chu Zi Nr. 979 (新刑初字第 979 号); (2015) Chao Xing Chu Zi Nr. 1072 (朝刑初字第 1072 号); (2016) Jing 0105 Xing Chu Nr. 871 (京 0105 刑初 871 号); (2015) Lin Tong Xing Chu Zi Nr. 00204 (临潼刑初字第 00204 号); (2014) Tai Yu Xing Chu Zi Nr. 837 (台玉刑初字第 837 号); (2015) Chao Xing Chu Zi Nr. 1769 (朝刑初字第 1769 号); (2014) Zhuang Xing Chu Zi Nr. 243 (庄刑初字第 243 号).

214 Auslegung des Obersten Volksgerichts und der Obersten Volksstaatsanwaltschaft zu Fragen der Anwendung des Rechts bei der Behandlung von Fällen der Verleumdung mittels Internet, (最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释) vom 6.9.2013.

215 *Zhang Mingkai*, China Legal Science 2015/3, 60 (60 ff.); *Yang Liu*, Law Science 2016/7, 137 (137 ff.); *Li Xiaoming*, Tribune of Political Science and Law 2014/1, 186 (186 ff.); *Yu Zhigang*, Law Science 2013/10, 102 (102 ff.).

216 (2013) Chao Xing Chu Zi Nr. 2584 (朝刑初字第 2584 号); *Zhang Mingkai*, China Legal Science 2015/3, 60 (71 ff.); *Yu Zhigang*, Law Science 2013/10, 102 (104).

217 *Yang Liu*, Law Science 2016/7, 137 (142); *Li Xiaoming*, Tribune of Political Science and Law 2014/1, 186 (188); *Yu Zhigang*, Law Science 2013/10, 102 (106).

VI. Zwischenergebnis

Gesetzlich wird in China der Begriff der schädlichen Informationen im Gegensatz zu dem der rechtswidrigen Informationen bevorzugt, weil die illegalen Online-Inhalte ähnlich wie Viren oder Schadsoftware beseitigt werden müssen. Im chinesischen Recht ist die Bestimmung der schädlichen Informationen sehr weit gefasst. Mit dem Muster in § 5 der „Bestimmungen zur Steuerung des Internet“ und dem § 15 der „Methode für Internet-Informationsdienste“ können die schädlichen Informationen in drei Bereiche untergliedert werden, und zwar der politische, soziale und private Bereich.

In Bezug auf die politischen schädlichen Informationen steht der Begriff der Staatssicherheit im Zentrum, weil in der Praxis immer wieder wegen Verstößen dagegen bestraft wird. Das aktuelle Staatssicherheitsgesetz definiert zwar den Begriff der Staatssicherheit (§ 2 SSG). Jedoch ist der Begriff nicht auf den politischen Bereich beschränkt. In der alten Fassung der Vorschrift war dies der Fall. Dies zeigt eine Tendenz, dass die Staatsicherheit weitergefasst wird. Für diese Arbeit bedeutet das, dass mehr Online-Inhalte als schädliche Informationen erfasst werden können.

Der *Shi Tao*-Fall und *Gao Yu*-Fall haben gezeigt, dass es den chinesischen Gerichten nicht gewährt ist, die als Staatsgeheimnis eingestuften Informationen daraufhin zu untersuchen, ob diese Einstufung gerechtfertigt ist. Ohne die Prüfungskompetenz bevorzugen die Gerichte, die Einstufung der Behörde zu akzeptieren. Neben der Straftat der Preisgabe von Staatsgeheimnissen (§ 111 chStGB) kommt die Aufhetzung zur Untergrabung der Staatsgewalt (§ 105 Abs. 2 chStGB) auch häufig in Betracht. Der Tatbestand des § 105 Abs. 2 chStGB ist aber sehr weit, sodass schon Kritik an der Staatsgewalt („Online-Aufhetzung“) darunter zu subsumieren ist.

Sozial schädliche Informationen sind insbesondere solche, die Irrlehren und Aberglauben verbreiten oder Gerüchten streuen. Dabei sind die Informationen gemäß § 300 Abs. 1 chStGB immer verboten, solange sie mit rechtswidrigen Religionsgemeinschaften verbunden sind. Mit der umstrittenen Auslegung des Obersten Volksgerichts sowie der Obersten Volksstaatsanwaltschaft wird die Kontrolle von Gerüchten auf Internetplattformen viel strenger vorgenommen als früher. Verboten ist danach gemäß §§ 291a Abs. 2, 293 Abs. 1 Nr. 4 chStGB das Verbreiten unwahrer Informationen oder solcher Informationen, die die öffentliche Ordnung erheblich stören. Die Kritik oder die negative Bewertung der öffentlichen Gewalt

sollte nicht einfach den unwahren Tatsachenbehauptungen zugeordnet werden. Von den Straftaten ist auch ausgeschlossen, wenn durch unwahre Tatsachenbehauptungen nur geringfügige Effekte im Internet ausgehen. Zu den sozial schädlichen Informationen gehören auch solche, die Pornografie, Glücksspiel, Gewalt, Mord, Todschlag, Terrorismus oder Anstiftung zu Straftaten betreffen.

Bei den privat schädlichen Informationen kommen die Inhalte, die staatsbürgerliche Rechte angreifen, in Betracht. Die sind zum einen nationaler Hass, nationale Diskriminierung und die Solidarität beschädigende Meinungsäußerungen. Auch erfasst sind Äußerungen, mit denen die Unterstützung von radikalen Volksgruppen zum Ausdruck gebracht wird. Außerdem werden Inhalte, durch die persönliche Rechte verletzt werden, als schädliche Informationen eingestuft. Kritisiert wird die Auslegung des Obersten Volksgerichts und der Obersten Volksstaatsanwaltschaft zur Fragen der Anwendung des Rechts bei der Behandlung von Fällen der Verleumdung mittels des Internet. Anzuwenden ist danach eine starre Grenze bei 5000-maligem Lesen oder 500-maligem Weiterleiten der Online-Posts für eine erhebliche Folge der Straftat. Konkrete Umstände des Einzelfalls werden hierbei nicht berücksichtigt. Dies führt dazu, dass sehr schnell hohe Strafen für Online-Posts verhängt werden. Insgesamt wird deutlich, dass in China viele Informationen als schädlich eingestuft werden. Die Vorschriften sind auch häufig nicht abschließend oder bestimmt. Für die Regierung besteht also viel Freiraum bei der Auswahl der schädlichen Informationen. So ist letztlich eine umfangreiche und effektive Kontrolle von Online-Inhalten möglich.

C. Lizenz als Auswahlmechanismus der Gatekeeper in China

Zu den Kontrollinstrumenten gehört einerseits die im vorigen Abschnitt dargestellte Liste der schädlichen Informationen. Andererseits werden strenge Anforderungen an diejenigen öffentlichen und privaten Akteure gestellt, die die Möglichkeiten zur Verbreitung von Informationen im Internet erst bereitstellen. Sie sind zur Inhaltskontrolle als Gatekeeper vom Staat gesetzlich ausgewählt, um dann Eingriffsmaßnahmen für den Staat durchzuführen.[218] Als wichtige Teilnehmer im Cyberraum spielen sie bei der Inhalteregulierung sowie bei Internetsperren im chinesischen Netz eine entscheidende Rolle. Welche Arten von Gatekeepern nach dem chinesischen Recht existieren, ist allerdings nicht einfach zu beantworten, da bislang eine Systematisierung bei der Gesetzgebung sowie der Rechtsanwendung in China nicht gegeben ist. Entsprechend dem deutschen Recht handelt es sich dabei sowohl um Telekommunikationsdiensteanbieter als auch um traditionelle Mediendienstanbieter und Telemediendienstanbieter.

I. Die Monopolstellung der Grundtelekommunikationsanbieter

Die Betriebsqualifikation der Grundtelekommunikationsdienste ist von der zuständigen Staatsratsabteilung für die Informationsindustrie (auf staatlicher Ebene: Ministerium für Industrie und Informationswesen) zu prüfen und zu genehmigen (§ 9 Abs. 1 Telekommunikationsregeln[219]), soweit sie alle Voraussetzungen des § 10 Telekommunikationsregeln erfüllen. Sie muss danach folgende Voraussetzungen erfüllen: Gesellschaft mit mindestens 51% staatseigenem Kapital (1.), Erstellung eines Machbarkeitsstudienberichts und eines Plans für die Strukturierung von Netzwerken (2.), genügend Kapital und spezialisiertes Personal (3), genügende Räumlichkeiten und Ressourcen (4), Gewährleistung der langfristigen Diensterbringung (5) und das Unternehmen muss dazu noch anderen Anforderungen aus sonstigen Regelungen nachkommen (6). Dabei ist zu betonen, dass ausländisches Kapital gemäß § 10 Telekommunikationsregeln zwar nicht grundlegend ausgeschlossen ist. Jedoch ist auch trotz Chinas Eintritt in die WTO bis jetzt noch kein

---

218 *Hu Ling*, in: Grundrecht und Konstitutionalismus, 411 (428); *Wei Yongzheng*, Cass Journal of Foreign Law 2001/1, 69 (69); *Zhang Qianfan*, Law Science 2015/4, 3 (5).

219 Telekommunikationsregeln (电信条例) vom 25.9.2000.

Cent aus dem Ausland in den chinesischen Grundtelekommunikationsmarkt investiert worden (oder durfte investiert werden).[220] Die Telekommunikationsregeln versprechen zwar dem Lizenzbewerber, dass die Erteilung der Grundtelekommunikationslizenz gemäß § 12 Abs. 2 Telekommunikationsregeln im Verfahren der Ausschreibung erfolgen soll. Stattdessen folgt der Staat jedoch dem Verteilungsprinzip der Planwirtschaft. Als Folge besitzen drei Staatsunternehmen (China Telekom, China Unicom und China Mobil) zusammen eine Monopolstellung im chinesischen TK-Markt. Ungeachtet des Ausschreibungsgebots werden strenge Kriterien gemäß § 12 Abs. 1 Telekommunikationsregeln für die Lizenzerteilung herangezogen. Insbesondere die umfassende Beurteilung im Rahmen des Lizenzierungsprozesses hinsichtlich Staatssicherheit, Sicherheit des Telekommunikationsnetzwerks und weitere Aspekt können potenzielle Interessenten abschrecken. Zur Konkretisierung der oben erörterten Lizenzierungsvoraussetzungen normiert die „Verwaltungsmaßnahme für die Betreiberlizenz der Telekommunikationsdienste“[221] weitere Voraussetzungen. § 5 Nr. 6 dieser Verwaltungsmaßnahme beinhaltet ein Gebot des Mindestkapitals (auf Provinzebene: 100 Mio. RMB; auf staatliche Ebene: 1 Bio. RMB), was in der Praxis dazu führt, dass die Monopolstellung der Telekommunikationsunternehmen bewahrt wird.

II. Weitere Genehmigungen für Access- und Netzwerk-Provider

Das Computernetz im Gebiet der VR China besteht gemäß § 3 der Vorläufigen Bestimmungen der VR China zur Lenkung des Internet aus drei Schichten, nämlich dem Zugangsnetz, dem Verbindungsnetz (oder Backbone-Netz) und dem WWW-Netz. Da Zugangsdienste von der Datenübermittelung in China getrennt sind, ist dieser Markt jedem offen, solange der gewerbliche Diensteanbieter einen Gewerbeschein hat oder der nichtgewerbliche Anbieter über eine entsprechende Genehmigung verfügt (§ 8 Abs. 2 und 3 Vorläufige Bestimmungen der VR China zur Lenkung des Internet). Datenübermittelung ist die Aufgabe der Netzwerk-Provider. Netzwerk-Provider sind in China die oben genannten Anbieter der Grund-

---

220 Die WTO trägt nur begrenzt zur wirtschaftlichen sowie politischen Reform in China bei. Im Gegensatz hierzu sind ausländische Investoren schnell an die chinesischen Spielregeln gewöhnt, *He Qinglian*, Media Control in China, 12 ff.

221 Verwaltungsmaßnahme für Betreiberlizenz der Telekommunikationsdienste (电信业务经营许**可管理**办法) vom 10.4.2009.

telekommunikationsdienste. Unter staatlicher Kontrolle sind darüber hinaus gemäß § 5 Verwaltungsmethode für internationale Datenzugangskanäle[222] alle sechs Verbindungsnetze und die internationalen Datenzugangskanäle. Da die Grundtelekommunikationsanbieter die der internationalen Kommunikation dienenden Eingangs- und Ausgangsporte sowie Router kontrollieren (§§ 3 Abs. 2 Nr. 1 und Abs. 3 Nr. 3 Verwaltungsmethode für internationale Datenzugangskanäle), werden Sperren- oder Filtertechniken bei solchen Anlagen eingestellt, sodass die beiderseitigen Datenströme zwischen der VR China und dem Ausland nach dem Willen der Hoheitsträger manipuliert werden können.[223]

III. Lizensierungen für Content- und Host-Provider

Ungeachtet des Gewerbezwecks versteht man unter Content- und Host-Provider gemäß § B25 Katalog der Telekommunikationsdiensten[224] einen Diensteanbieter, der selber über öffentliche Kommunikationsnetze Inhalte anbietet oder dem Endnutzer die Online-Dienstleistung unmittelbar anbietet, indem er Informationen erhebt, auswertet oder verarbeitet und Informationsplattformen errichtet, einschließlich der Informationsveröffentlichung und -übermittelung (Nachrichtenwebseiten, Foren etc.), Informationssuche (Suchmaschinen), Informations-Community (soziale Netzwerke, Blogs, Mikroblogs, virtual Communities, Chatrooms etc.), Echtzeitkommunikation (ICQ, WeChat) und Datensicherheit (Anti-Virus-Service). Zu unterscheiden ist zwischen allgemeinen und besonderen Content- und Host-Providern. Für letztere sind noch von den jeweiligen Aufsichtsbehörden erlassene Sondernormen zu beachten. Somit sind chinesische Telemedien nicht zulassungs- und anmeldefrei, sondern haben mehrere Lizenzen zu beantragen.

1. Lizenz für allgemeine Content- und Host-Provider

Gemäß § 4 i.V.m. §§ 7-8 Abs. 1 der Methode für Internet-Informationsdienst haben gewerbliche Content- und Host-Provider bei den zuständigen Behörden eine Lizenz zu beantragen, während nur eine Anmeldeverpflichtung für nicht gewerbliche Diensteanbieter gilt. Um das Anmeldegebot zu umgehen, kaufen zahlreiche

---

222 Verwaltungsmethode für internationale Datenzugangskanäle (国际通信出入口局管理办法) vom 26.6.2002.

223 *Herrera*, in: Power and security in the information age, 67 (84); *Wu*, 10 Harv. JL & Tech. 648 (651 ff.) (1997).

224 Katalog der Telekommunikationsdienste (电信业务分类目录) vom 12.5.2015.

Webseiten-Besitzer in der Praxis den Webspace sowie Domain unmittelbar bei ausländischen Host-Provider, was praktisch dazu führt, dass dieses gesetzliche Anmeldegebot ins Leere geht. Für sie besteht neben der potenziellen Untersagung der Inhaltsdienste aber noch die Gefahr, dass die im Ausland ansässige Webseite durch Filterung bei den internationalen Datenzugangskanälen teilweise oder sogar völlig gesperrt werden.

2. Lizenz für besondere Content- und Host-Provider

Für die Content- und Host-Provider, welche sich im Nachrichtenwesen, im Pressewesen, im pädagogischen Bereich, im Bereich Medizin und im Gesundheitswesen, in der Pharmazie oder in der Branche der medizinischen Geräte betätigen, ist bereits vor dem Antrag für die Lizenz im gewerblichen Fall oder vor der Anmeldung, soweit sie keinen gewerblichen Zweck verfolgen, eine zusätzliche Sondergenehmigung von jeweils zuständigen Behörden einzuholen (§ 5 Methode für Internet-Informationsdienst). Nähere Voraussetzungen dafür sind in zahlreichen Verwaltungsrechtsnormen enthalten. Angesichts der daneben noch existierenden Methode für Internet-Informationsdienste und anderer medienrechtlicher Normen bilden sie zusammen ein umfassendes, lückenloses und zensurorientiertes Kontrollsystem der Online-Inhalte. Im Folgenden soll der Fokus auf die im Netz tätigen Massenmedien gelegt werden (Nachrichten, Presse, Rundfunk). Eine große Rolle spielen auch die neuen Kommunikationsformen zwischen Privaten (Email, soziale Netzwerke, Echtzeitkommunikation). Es soll dargestellt werden, in welcher Weise die Anbieter solcher Dienste der Kontrolle des Staates unterliegen.

3. Sondergenehmigungen im Verlags- und Nachrichtenwesen

Chinesische Massenmedien haben dem Volk und dem Sozialismus zu dienen (Art. 22 chVerf). Als Propagandasprachrohr tragen sie in erster Linie nicht zur Meinungsbildung im demokratischen Sinne bei, sondern unterstützen die Parteileitung der chinesischen KP. Dies ist auch in offiziellen Parteidokumenten so zu lesen.[225] Massenmedien sowie deren Akteure unterstehen daher ausschließlich der Leitung der KP. Dies gilt ebenfalls für neue Medien.[226]

---

225 *Wei*, 30; *Hu*, 210; *Chen Zheng*, Contemporary Law Review 2014/4, 12 (16); *Lin Laifan*, 371; *Zhang Qianfan*, 563; *Fan Jinxue*, Modern Law Science 2013/2, 605 (608).

226 Die „Institutionalisierung" der Internetkontrolle ist der Medienkontrolle in China gefolgt, *He*, 8 ff.; *Ma Ling*, Contemporary Legal Science 2004/1, 60 (65); *Chen Zheng*, Contemporary Law Review 2014/4, 12 (18).

Wer Zeitungen, Zeitschriften, Bücher, Ton- und Bildträger oder elektronische Verlagserzeugnisse verlegen möchte, muss eine Sondergenehmigung beantragen (§ 9 Abs. 1 Verlagsverwaltungsregeln[227]). Organisatorisch bedürfen Presseunternehmen darüber hinaus einer internen Beaufsichtigungseinheit gespeist durch die Staatsratsabteilung für Verlagsverwaltung und einer vorgesetzten „Parteibehörde" (§11 Abs. 1 Nr. 2 Verlagsverwaltungsregeln). Die „Volkszeitung" wird beispielweise unmittelbar vom Zentralkomitee der KP kontrolliert. Angesichts der beiden Kontrollorgane ist eine Art Doppelversicherung im Verlagswesen gegeben. Verfahrensrechtlich entscheidet zunächst die vorgesetzte „Parteibehörde", ob ein Presseunternehmen zu gründen ist. Danach schließt sich ein weiteres Genehmigungsverfahren an, welches die unternehmensinterne Beaufsichtigungseinheit betrifft (§ 12 Satz 1 Verlagsverwaltungsregeln). Dies führt im organisatorischen Sinne zu einem parteiabhängigen Pressesystem.

In der jetzt gültigen Rechtsnorm für das Pressewesen im Internet – Verwaltungsregeln für Internet-Presse – wird zwischen den traditionellen und anderen Presseunternehmen unterschieden. Die Gründung eines im Netz tätigen Presseunternehmens ist gemäß § 8 Verwaltungsregeln zur Online-Presse[228] nach wie vor von einer betriebsinternen Beaufsichtigungseinheit und deren vorgesetzter Parteibehörde abhängig. Ein solches Presseunternehmen erhält die Bezeichnung „offizielle Presseeinheit". Von einer nicht offiziellen Presseeinheit wird dagegen nur mindestens ein Anfangskapital von 1 Mio. Yuan gefordert. Sie muss zudem mindestens acht vom Staat anerkannte Redakteurinnen und Redakteure anstellen (§ 9 Verwaltungsregeln zur Online-Presse).

Für Nachrichtenpublikationen gelten strengere Regelungen als bei der übrigen Presse. Bei der Genehmigungspflicht der Nachrichtenpublikationen bestehen drei Möglichkeiten. Erstens, wenn die herkömmlichen Presseeinheiten ausschließlich ihre Pressepublikationen digitalisieren und sie ins Netz stellen, sind sie gemäß § 9 Abs. 1 Verwaltungsregeln für Online-Nachrichtendienste[229] nur dazu verpflichtet, die Rechtsnormen für Presseeinheiten und zudem das Anmeldegebot bei ihrer Aufsichtsbehörde einzuhalten, da sie keine *neuen* Nachrichten bereitstellen. Zweitens, soweit sie über ihre offline erschienenen Publikationen hinaus *neue* Inhalte

---

227 Verlagsverwaltungsregeln (出版管理条例) vom 1.2.2002.

228 Verwaltungsregeln zur Online-Presse (网络出版服务管理规定) vom 4.2.2016.

229 Verwaltungsregeln zur Online-Nachrichtendienste (互联网新闻信息服务管理规定) vom 1.6.2017.

online bereitstellen, haben sie gemäß §§ 5 Abs. 1 und 9 Abs. 1 Verwaltungsregeln für Online-Nachrichtendienste zusätzlich eine Genehmigung bei der zuständigen Behörde zu beantragen, weil das Internet im Vergleich zu herkömmlichen Medien eine schnellere, kostengünstigere und schwieriger zu kontrollierende Übermittlung ermöglicht. Drittens, wenn die Einheiten nicht zu den traditionellen Presseinheiten zählen, haben sie nur das Recht, Nachrichten von lizenzierten Einheiten *weiterzuleiten* (§ 9 Abs. 1 Verwaltungsregeln zur Online-Nachrichtendienste).

Untersagt sind Publikationen von Individuen, da nur Presseunternehmen bzw. Presseeinheiten im chinesischen Recht zulässige Akteure im Pressewesen und bei Publikationen sind (§ 9 Verlagsverwaltungsregeln). Zu überlegen wäre hier eine Verfassungswidrigkeit und daher Nichtigkeit des § 9 Verlagsverwaltungsregeln, da die chinesische Verfassung die „Publikationstätigkeiten" der Bürgerinnen und Bürger nicht nur mit der Freiheit der Rede, sondern auch die Freiheit der Presse schützt (Art. 35 chVerf). Die Pressefreiheit gemäß Art. 35 chVerf gewährt *jedem* das Recht, durch Publikationen seine bzw. ihre Meinung zu äußern.[230] Der Schutzbereich der chinesischen Pressefreiheit gemäß Art. 35 chVerf wird allerdings dahingehend restriktiv ausgelegt, dass nur Presseerzeugnisse von staatlich erlaubten Presseeinheiten in den Schutzbereich fallen.[231] Eine Verfassungswidrigkeit des § 9 der Verlagsverwaltungsregeln liegt vor dem Hintergrund dieser engen Auslegung der Pressefreiheit nicht vor.

In der rechtlichen Grauzone gibt es allerdings im Netz zahlreiche „Publikationen" von Individuen, die in der Form der sog. WeMedia tätig sind. Diese ähneln den Publikationen der Massenmedien in vielerlei Hinsicht. Um sie aus der Grauzone herauszuholen, fordern die Methode für Internet-Informationsdienst und die Verwaltungsbestimmungen für Internet-Bulletin-Board-Dienste (einschließlich elektronischen schwarzen Brettern, Foren, Chatrooms, usw.) seit dem Jahr 2002 von den betroffenen Informationsdiensteanbietern einen besonderen Antrag oder eine besondere Meldung (§ 5 Abs. 1 Verwaltungsbestimmungen für Internet- Bulletin-Board-Dienste i. V. m. § 9 Methode für Internet-Informationsdienst).

---

230 *Hu Ling*, in: Grundrecht und Konstitutionalismus, 411 (422); *Wei*, 26 f.; *Fan Jinxue*, Modern Law Science 2013/2, 605 (608); *Hu*, 210; *Ma Ling*, Contemporary Legal Science 2004/1, 60 (63); *Lin Laifan*, 371; *Chen Zheng*, Contemporary Law Review 2014/4, 12 (15); *Zhang Qianfan*, 563.

231 *Fan Jinxue*, Modern Law Science 2013/2, 605 (606); *Chen Zheng*, Contemporary Law Review 2014/4, 12 (14); *Ma Ling*, Contemporary Legal Science 2004/1, 60 (62).

Das Gleiche geschieht auch bei der Kontrolle der WeMedia mittels Echtzeitkommunikationstechnik, zu denen WeChat mit einer Milliarde monatlich aktiven Nutzern als eine der populärsten Applikation in China zählt.[232] Die Diensteanbieter, welche nicht nur den Endnutzern Echtzeitkommunikation, sondern auch das Erstellen eines öffentlichen Kontos anbieten, haben neben den Lizenzen nach den Telekommunikationsregeln und der Methode der Internet-Informationsregeln zusätzlich eine Lizenz für Internet-Nachrichtendiensteanbieter einzuholen (§ 2 Abs. 2 Vorläufige Verwaltungsregeln für Entwicklung der öffentlichen Nachrichtendienste mittels Echtzeitkommunikation[233]). Ebenfalls gelten dabei die vorgesehenen Beschränkungen auf das Verfassen sowie Weiterleiten von aktuellen politischen Nachrichten (§ 7 Abs. 2 Satz 1 Vorläufige Verwaltungsregeln für Entwicklung der öffentlichen Nachrichtendienste mittels Echtzeitkommunikation). Wer auf einer Plattform für Echtkommunikation zwischen Privaten (die auf Basis der One-to-One Kommunikation stattfindende One-to-Many Kommunikation) ein öffentliches Konto eröffnet sowie damit einen öffentlichen Kanal betreibt, muss gemäß § 7 Abs. 1 Vorläufige Verwaltungsregeln für Entwicklung der öffentlichen Nachrichtendienste mittels Echtzeitkommunikation zunächst vom Echtzeitkommunikationsdienstanbieter überprüft werden und muss sich danach via dieses Diensteanbieters beim Staatlichen Büro für Internet und Information melden.

4. Das Modell des Regierungsrundfunks im Netz

Da Rundfunk im Vergleich zu Presse eine deutlich größere Reichweite und Suggestivkraft besitzt, wurde er in China bis zu den 1980er Jahren von einer Verwaltungsbehörde innerhalb der Regierung betrieben. Danach wurde der Rundfunk aus der Regierung ausgegliedert. Er befindet sich aber weiterhin unmittelbar unter staatlicher Aufsicht. Städtische Rundfunkanstalten können nur vom Rundfunkamt sowohl auf Provinzebene als auch auf zentraler Ebene gegründet werden (§§ 10 Abs. 1 und 11 Abs. 1 Satz 2 Verwaltungsregeln für gewerbliche Darbietungen[234]). Das staatliche Zentralamt für Rundfunk und Film entscheidet und genehmigt außerdem allein, ob Rundfunkanstalten auf staatlicher Ebene errichtet werden (§ 11 Abs. 1 Satz 1 Verwaltungsregeln für gewerbliche Darbietungen). Ausgeschlossen

---

232 Report vom WeChat 2018, abrufbar unter abrufbar < https://xw.qq.com/amphtml/20190109A0P6M000> [Stand: 7.8.2019].

233 Vorläufige Verwaltungsregeln für Entwicklung der öffentlichen Nachrichtendienste mittels Echtzeitkommunikationstechnik (即时通信工具公众信息服务发展管理暂行规定) vom 7.8.2014.

234 Verwaltungsregeln für gewerbliche Darbietungen (广播电视管理条例) vom 11.8.1997.

sind sowohl die Gründung von Rundfunkanstalten durch Private als auch durch chinesisch-ausländische Unternehmen (§ 10 Abs. 1 Satz 2 Verwaltungsregeln für gewerbliche Darbietungen), auch wenn diese im Pressewesen zulässig sind (§ 39 Verlagsverwaltungsregeln).

Eine Unterscheidung wie beim Pressewesen zwischen traditionellen und neuen Medien – Rundfunkveranstalter, Nachrichtendienstanbieter und andere Einheiten – findet nicht statt. In diesem Bereich gilt in China weiterhin das Gebot des sog. Regierungsrundfunks (§ 10 Verwaltungsregeln für gewerbliche Darbietungen).[235] Im Internet tätige Diensteanbieter von Audio- oder audiovisuellen Medien dürfen nur von Staatsunternehmen oder Unternehmen, bei denen der Staat mehrheitlich über die Gesellschaftsanteile verfügt (§ 8 Abs. 1 Satz 1 Verwaltungsregeln für gewerbliche Darbietungen), gegründet werden (§ 10 Abs. 1 Satz 1 Verwaltungsregeln für gewerbliche Darbietungen).

IV. Lizensierung für Nutzer mit Klarnamenpflicht?

Um der erschwerten Inhaltskontrolle vorzubeugen, ist die Einführung der sog. Klarnamenpflicht im chinesischen Netz eine effektive Maßnahme geworden. Die Strategie liegt darin, dass durch die Verbindung zwischen Identität und Verhalten der Nutzer einerseits die „Selbstzensur" oder weniger forsches und kritisches Verhalten online sichergestellt und andererseits die Feststellung der Adressaten zur Sanktionierung danach erleichtert werden kann.[236] Die Klarnamenpflicht funktioniert bei der Inhaltskontrolle demnach wie eine Lizenzierung. Die Klarnamenpflicht begleitet seit jeher die 30-jährige Entwicklung des Internets in der VR China.

Die jetzige vollständige Klarnamenpflicht für sämtliche Telemediendienste geht in ihrer Entwicklung auf verschiedene Versuche in den Teilgebieten zurück. Von besonderer Bedeutung für den heutigen Zustand waren die Klarnamenpflichten für Nutzer oder Besitzer der Domains (1997), Internet-Cafés (2003), Emails (2004), Bulletin Board Systems (BBS) innerhalb von Hochschulen (2004), Webseiten (2005), Online-Computerspielen (2005), Mikroblogging (2011), Hinterlassen von

---

235 *Wei*, 30; *Chen Zheng*, Contemporary Law Review 2014/4, 12 (17); *Ma Ling*, Contemporary Legal Science 2004/1, 60 (66).

236 *Hu Ling*, in: Grundrecht und Konstitutionalismus, 411 (421); *Qi Enping*, Law Science Magazine 2013/7, 60 (62); *Yang Fuzhong*, Studies in Law and Business 2012/5, 32 (34); *Han Ning*, Law Science 2012/4, 3 (6).

Nachrichten (2014 und 2017), Echtzeitkommunikation (2014), Internet-Literatur (2015), Webcast (2016), öffentliche Konten (2017) und Foren (2017).[237] Letztlich hat China dabei zahlreiche Erfahrungen aus dem In- und Ausland, vor allem Südkorea, gesammelt und danach den Mechanismus der „Klarnamen *hinter* der Internetplattform, Freiwilligkeit *vor* der Internetplattform" entwickelt, bei dem alle Nutzer, die ein Konto bei einem beliebigen Telemediendiensteanbieter einrichten wollen, neben der normalen Registrierung, wobei der Benutzername frei gewählt werden kann, gezwungen werden, auf einem Pop-up-Fenster die Informationen zur eindeutigen Identifizierung anzugeben (Namen, Handynummer oder ID-Nummer). Im Vergleich zu anderen Ansätzen zur Inhaltskontrolle (Zensur, Zugangskontrolle[238]) bietet die Klarnamenpflicht nach dem Duktus der chinesischen Regierung viele Vorteile. Da die Pop-up-Webseite von einem öffentlich-rechtlichen Verein[239] gehostet wird und sich die Identitätsinformationen der Nutzer direkt mit der staatlichen ID-Datenbank[240] überprüfen und dann bestätigen lassen, ist das Risiko von Identitätsdiebstahl oder -missbrauch relativ gering. Es entsteht auch fast kein Erfüllungsaufwand für die Nutzer und die Wirtschaft. Allerdings ist es zum einen zweifelhaft, ob alle Identitätsdaten bei der staatlichen ID-Datenbank nach heutigem Stand der Technik tatsächlich sicher sind. Zum anderen kann die jetzige Klarnamenpflicht teilweise sogar Kriminelle zum Identitätsdiebstahl bei Telemediendienstanbieter bewegen. Ebenfalls ist die vorgestellte Maßnahme in Bezug auf Minderjährige und Ausländer problematisch, da sie über keinen chinesischen Personalausweis verfügen. Trotz dieser Nachteile entwickelt sich die entsprechende Technik weiter, z.B. e-ID. Durch die Klarnamenpflicht und ihre Weiterentwicklung wird die chinesische Gesellschaft immer transparenter.

---

237 § 15 Vorläufige Verwaltungsmethode für Registrierung der Domainnamen (**互**联网络域名注册暂行管理办法) vom 30.5.1997; § 23 Verwaltungsregeln zum Internet-Café (**互**联网上网服务营业场所管理条例) vom 29.9.2002; § 9 Einige Bestimmungen zur Verwaltung des Mikroblogging in Peking (**北京市微博客**发展管理若干规定) vom 16.12.2011; § 6 Vorläufige Verwaltungsregeln für Entwicklung der öffentlichen Nachrichtendienste mittels Echtkommunikationstechnik (**即**时通信工具公众信息服务发展管理暂行规定) vom 7.8.2014; § 12 Verwaltungsregeln für Webcast im Internet (**互**联网直播服务管理规定) vom 1.12.2016; § 5 Verwaltungsregeln für Posten im Internet (**互**联网跟帖评论服务管理规定) vom 1.10.2017; § 6 Verwaltungsregeln für öffentliche Kontos im Internet (**互**联网用户公众账号信息服务管理规定) vom 8.10.2017; § 8 Verwaltungsregeln für Foren im Internet (**互**联网论坛社区服务管理规定) vom 1.10.2017.

238 Siehe hierzu Kapitel 3. D.-F.

239 **中国互**联网协会.

240 **全国公民身份**证号码查询服务中心.

V. Zwischenergebnis

Zur Inhaltskontrolle werden strenge Anforderungen an die chinesischen Telekommunikations-, Medien- und Telemediendiensteanbieter gestellt. Solche Gatekeeper müssen gesetzliche Voraussetzungen erfüllen, um die Lizenzen zu erhalten. Die Grundtelekommunikation und Datenübermittelung befinden sich zu 100% in staatlicher Hand. Dazu gehört auch die Verbindung zwischen dem Inland und dem Ausland durch internationale Datenzugangskanäle. Neben der allgemeinen Genehmigungspflicht oder der Anmeldeverpflichtung, müssen die Verlag- und Nachrichteneinheiten Sondergenehmigungen beantragen. Auch für WeMedia ist eine besondere Lizenz oder eine Anmeldung gesetzlich geregelt. Im Rundfunkbereich gilt das Gebot des Regierungsrundfunks. Die Klarnamenpflicht für Nutzer von Online-Foren und anderen sozialen Plattformen erfüllt letztendlich auch den Zweck einer Lizensierung. Folglich sind sämtliche Akteure, die Informationen im Internet veröffentlichen können, von Lizenzierungspflichten erfasst. Dies legt den Grundstein zur Kontrolle von Online-Veröffentlichungen.

D. Kontrolle von Veröffentlichungen

Zur effektiven Prävention illegaler Inhalte im Netz gehören solche Maßnahmen, die vor ihrer Veröffentlichung von den privaten Akteuren getroffen werden. Hierfür werden an Presse-, Nachrichten- sowie Rundfunkeinheiten besondere Anforderungen der Vorzensur gestellt. Ohne deren Erfüllung können die oben skizzierten Lizenzen entzogen werden. Viele Telemediendiensteanbieter setzen die Technik der Schlüsselwörterfilterung ein, um das Risiko des Lizenzentzugs zu reduzieren.

I. Zensurgebot der Presse und des Rundfunks im Internet

Bei den traditionellen Medien besteht in China eine strenge Vorzensur, da nur so die Beachtung der sog. „zwei Dienste" – dem Volk und dem Sozialismus dienen (Art. 22 chVerf) – sowie das Prinzip der Parteileitung sichergestellt werden kann. Die Funktion als Propagandasprachrohr wird auch auf neue Medien in China übertragbar sein.

Im Pressewesen sind bei sämtlichen Verlagserzeugnissen der Jahresverlagsplan und schwerwiegende Themen – das sind Themen, die die Staatssicherheit oder den

sozialen Frieden berühren – im Einzelnen von der Verlagsverwaltung zu überprüfen (§ 20 Verlagsverwaltungsregeln),[241] um die „Reinheit der Presse" frühzeitig sicherzustellen. Darüber hinaus wird gemäß § 24 Verlagsverwaltungsregeln bei Verlagseinheiten das Institut der sog. verantwortlichen Redakteure garantiert.[242] Dies sind einzelne Personen innerhalb der Redaktion, die die Presseerzeugnisse schon im Entstehungsprozess kontrollieren. Hierzu gehört stets der Chefredakteur. Hierdurch soll sichergestellt werden, dass die Inhalte der Verlagserzeugnisse nicht von den vorgesehenen Verwaltungsregeln abweichen. Da alle verantwortlichen Redakteure zum einen von den Parteiorganisationen in die Presseeinheiten nominiert werden und sie sich zum anderen vor den potenziellen Sanktionen fürchten, denen sie wegen systematisierter Nachzensur,[243] vor allem zu hochsensiblen Inhalten,[244] und einem Warnsystem gegen disziplin- und rechtsverletzende Verlagszeugnisse häufig ausgesetzt sind (§ 62 Verlagsverwaltungsregeln und § 49 Verwaltungsregeln für gewerbliche Darbietungen), kann von ihrer Linientreue ausgegangen werden. Auch findet eine Vorzensur zu illegalen Inhalten bei Online-Presseeinheiten statt (§ 17 Verlagsverwaltungsregeln), weil die Kontrolle durch die verantwortlichen Redakteure ebenfalls in den vorläufigen Verwaltungsregeln für die Internet-Presse vorgesehen ist (§ 21 Verlagsverwaltungsregeln). Betreffend das Nachrichtenwesen dürfen im Netz die aktuellen politischen Nachrichten gemäß §§ 16 und 17 Verwaltungsregeln für Online-Nachrichtendienste nur weitergeleitet werden, wenn die Vorzensur offline erfolgreich durchgeführt wird und die Nachrichten unverändert online übertragen werden.

Aufgrund der stärkeren Suggestivkraft ist die Vorzensur im Rundfunkwesen strenger als im Pressewesen. Vor jeder Programmübertragung und Sendungswiederholung haben die Rundfunkanstalten zu überprüfen, ob sie illegale Inhalte beinhalten (§§ 32 und 33 Verwaltungsregeln für gewerbliche Darbietungen).[245] Im Fall der Missachtung dieses Zensurgebots sind Sanktionen vorgesehen. Zudem sind die

---

241 *Wei*, 29; *Chen Zheng*, Contemporary Law Review 2014/4, 12 (13); *Fan Jinxue*, Modern Law Science 2013/2, 605 (607).

242 *Wei*, 27; *Hu*, 210; *Ma Ling*, Contemporary Legal Science 2004/1, 60 (66).

243 *He Qinglian*, The fog of Censorship – Media control in China, 75; *Zhang Qianfan*, 563; *Lin Laifan*, 371.

244 SCIO, Verwaltung für die Nachrichtenpublikationen, Auflistung abrufbar unter <http://www.scio.gov.cn/zhzc/10/Document/1014582/1014582.htm> [Stand: 7.8.2019].

245 *Wei*, 30; *Hu Ling*, in: Grundrecht und Konstitutionalismus, 411 (426); *Li Xiaoming*, Tribune of Political Science and Law 2014/1, 186 (189).

betroffenen Programme vom Staatsrat zu untersagen (§§ 43 und 49 Verwaltungsregeln für gewerbliche Darbietungen).[246] Auf der Internetplattform stammen sämtliche aktuelle politische Nachrichten aus traditionellen Fernseh- und Radiosendungen, die ihrerseits der Vorzensur unterliegen.

II. Filterung von Schlüsselwörtern

Problematisch ist zunächst, dass die Pflicht zur Filterung von Schlüsselwörtern vor der Veröffentlichung von Online-Posts für Telemediendiensteanbieter weder von der generell im Telemedienbereich geregelten Methode für Internet-Informationsdienste noch von den speziellen Regeln wie z.B. den Verwaltungsbestimmungen für Internet-Bulletin-Board-Dienste vorgesehen ist. Verwaltungsrechtlich ist eine Filterung somit nicht angezeigt. Nach den zivilrechtlichen Regelungen haben die Telemediendiensteanbieter zwar notwendige Maßnahmen zu ergreifen, wenn sie Kenntnis darüber erlangen, dass Nutzer die Rechte anderer Nutzer verletzen, um eine gesamtschuldnerische Haftung zu vermeiden (§ 36 Abs. 3 Gesetz über die Haftung für die Verletzung von Rechten[247]). Das heißt, dass der Telemediendiensteanbieter zunächst den Rechtsverletzer benachrichtigen muss, dass dieser mit seinen Posts die Rechte oder Güter der anderen verletzen könnte. Wenn der Rechtsverletzer nicht oder nicht zügig darauf reagiert oder die Tatsache der Rechtsverletzung offensichtlich gegeben ist, muss der Telemediendiensteanbieter den Post löschen oder unter das betreffende Konto zu löschen.[248] Im Falle der Nichterfüllung dieser Pflichten hat der Telemediendienstanbieter mit dem Nutzer die gesamtschuldnerische Haftung zu übernehmen (§ 36 Abs. 2 Gesetz über die Haftung für die Verletzung von Rechten). Allerdings besteht im chinesischen Zivilrecht keine allgemeine Überwachungspflicht für Telemediendiensteanbieter.[249] Eine Art Vorzensur geht von der beschriebenen Regelung, die im Wesentlichen dem europäischen „Notice and take down" entspricht,[250] aber dennoch aus.

Für Telemediendienstanbieter gilt somit zwar kein gesetzliches Gebot der Vorzensur, ihnen stehen jedoch zur effektiven Inhaltskontrolle außer der Filterung von

---

246 *Wei*, 30; *Zhang Mingkai*, China Legal Science 2015/3, 60 (68); *Yu Zhigang*, Law Science 2013/10, 102 (100).

247 Gesetz über die Haftung für die Verletzung von Rechten (侵权责任法) vom 26.12.2009.

248 *Yao Zhiwei*, Global Law Review 2018/1, 101 (102); *Zhang Qianfan*, Law Science 2015/4, 3 (5); *Xiong Wencong*, Journal of Comparative Law 2014/4, 122 (124).

249 *Xiong Wencong*, Journal of Comparative Law 2014/4, 122 (122); *Yao Zhiwei*, Global Law Review 2018/1, 101 (102 f.); *Wang Shengming*, 218.

250 Siehe hierzu Kap. 4. A. IV.

Schlüsselwörtern nur wenige Auswahlmöglichkeiten zur Verfügung. Als Beispiel versuchen die Diensteanbieter, die sich mit Video- oder Audiosendungen beschäftigen oder den Internetnutzern das Hoch- oder Herunterladen von Video- oder Audiodateien ermöglichen, zu vermeiden, unerlaubte Informationen bei ihnen erscheinen zu lassen, da Sanktionen einschließlich Lizenzentzug vorgesehen sind (§ 24 Abs. 2 i.V.m. § 16 Verwaltungsregeln für audiovisuelle Programme im Internet). Zudem können die Sanktionen gegen Online-Presse gemäß § 62 i.V.m. § 25 Verlagsverwaltungsregeln oder gegen Online-Nachrichtendienste gemäß § 27 i.V.m. § 9 Verwaltungsregeln für Online-Nachrichtendienste verhängt werden. Beim Filtern von Schlüsselwörtern handelt es sich um eine dynamische Liste mit sensiblen Wörtern, die teilweise von Diensteanbietern selbst entwickelt werden und teilweise auf Befehl von Aufsichtsbehörden heranzuziehen sind. Durch den im Hintergrund laufenden automatischen oder manchmal manuellen Vergleich zwischen der Wörterliste, werden die unerwünschten Inhalte gesperrt. Allerdings tritt diese Art der Vorzensur nicht unbedingt spürbar in Erscheinung, weil sie manchmal unerkannt Verbindungen zwischen Servern unterbricht, Nachrichten verzögert anzeigt oder sie heimlich sperrt. Hierzu kann der chinesische Telemediendienstanbieter „Sina Mikroblogging" als Beispiel angeführt werden, der ständig eine umfangreiche Liste mit mehr als 3.000 sensiblen Wörtern führt. Sina Mikroblogging ist eng mit der Politik verbunden.[251]

In der Praxis wird nur selten Klage gegen Telemediendiensteanbieter wegen des Filterns von Schlüsselwörtern erhoben, weil die Politik in diesem Bereich großen Einfluss auf die Justiz hat und ein Gerichtsprozess nur schwierig gewonnen werden kann. Im Fall von einem der bekanntesten Menschenrechtsanwälte *Liu Xiaoyuan* klagte dieser gegen den Anbieter Sohu Blog wegen Nichterfüllung des Dienstvertrags gemäß § 60 Abs. 1 Vertragsgesetz[252]. Sohu Blog hatte es untersagt, die neun auf Korruption, Privilegien der Kader und soziale Ungerechtigkeit in China bezogene Blog-Artikel von *Liu Xiaoyuan* zu veröffentlichen. Im Schriftsatz begründete der Kläger, dass er einerseits keine illegalen Inhalte gepostet habe und andererseits keine Vereinbarung zwischen beiden Parteien über die Filterung von Schlüsselwörtern bestände. Die Klage wurde vom Gericht als unzulässig gemäß § 112 Nr. 4 chZPO a.F. zurückgewiesen, obwohl sie gemäß § 108 Nr. 4 i. V. m. §

---

251 *Herrera*, in: Power and security in the information age, 67 (84); *Liu/Wang*, Journal of Capital Normal University (Social Sciences Edition), 2015/5, 56 (60); *Han Ning*, Law Science 2012/4, 3 (4).

252 Vertragsgesetz (合同法) vom 1.10.1999.

111 chZPO a. F. zulässig sein sollte. Vorher hatte auch das Oberste Volksgericht speziell zum Ausschluss der Fallgruppe der Inhaltskontrolle im Internet eine Mitteilung[253] erlassen. Dies führt zu einer Lücke im gerichtlichen Rechtsschutz.

III. Zwischenergebnis

Bereits vor der Veröffentlichung von Inhalten greift das Zensurgebot für Presse-, Nachrichten- sowie Rundfunkeinheiten. Als Propagandasprachrohr erfüllen die chinesischen Presse- und Nachrichteneinheiten ihre Zensuraufgaben. Wichtige und kritische Themen werden vor der Veröffentlichung überprüft. Hierfür sind „verantwortlichen Redakteure“ zu ernennen, die den gesamten Prozess der Presse und Nachrichten kontrollieren. Das Gleiche gilt auch für Online-Presseeinheiten. Für das Rundfunkwesen gilt auch das Zensurgebot. Die Rundfunkanstalten überprüfen die Inhalte vor jeder Programmübertragung und Sendungswiederholung. Eine Vorzensur der Telemediendiensteanbieter ist zwar im chinesischen Verwaltungsrecht nicht angezeigt und eine allgemeine Überwachungspflicht besteht auch nicht nach dem chinesischen Zivilrecht. Um die Sanktionen einschließlich Lizenzentzug zu vermeiden, filtern sie allerdings bereits vor der Veröffentlichung die Schlüsselwörter. Die unerwünschten Inhalte werden automatisch oder manchmal manuell gesperrt. Der Fall *Liu Xiaoyuan vs. Sohu Blog* wurde vom Zivilgericht zurückgewiesen, da das chinesische Oberste Volksgericht mit einer offiziellen Mitteilung die zivilrechtlichen Rechtsschutzmöglichkeiten solcher Fälle entzogen hat.

E. Kontrolle von Veröffentlichungen aus Ausland durch die „Great Fire Wall“

Um materielle und prozessuale Defizite bei der Bekämpfung rechtswidriger Online-Inhalte zu beheben, beruft sich China zur Legitimation der inländischen Regulierung auf die Internetsouveränität. Um auch auf Veröffentlichungen aus dem Ausland zu reagieren hat es eine virtuelle „Große Mauer” an der Grenze errichtet.

---

253 Mitteilung des Obersten Volksgerichts zur Überprüfung der Eröffnung des Verfahrens in Bezug auf Verwaltung des Internets (**最高人民法院关于涉及互**联网**管理案件立案**审查工作的通知) vom 13.7.2009.

I. Einschränkungen der traditionellen Medien aus dem Ausland

Bei ausländischen Pressezeugnissen sowie Nachrichten darf der Import nur unter Einschränkungen erfolgen. Sämtliche Publikationen aus dem Ausland sind gemäß §§ 4 und 9 Verwaltungsmethode für den Bezug importierter Presseerzeugnisse ausnahmslos von einem Staatsunternehmen und nach einer Inhaltskontrolle zu importieren.[254] Bereits vor der Gründung der VR China verbot die KP die Veröffentlichung von durch ausländische Nachrichtenagenturen angebotenen Nachrichten. 1992 wurde vom Ministerium für Propaganda ausdrücklich betont, dass außer dem kostenlosen Austausch zwischen der Nachrichtenagentur Xinhua und ausländischen Nachrichtenagenturen keine ausländischen Nachrichten im Gebiet der VR China verbreitet werden dürfen.[255] Dies gilt auch für die Veröffentlichung ausländischer Publikationen sowie Nachrichten im Internet.

Fernseh- oder Radiosendungen aus dem Ausland dürfen gemäß §§ 39 und 41 Verwaltungsregeln für gewerbliche Darbietungen nur mit Genehmigung importiert werden, wobei die auf aktuelle Politik bezogenen Programme gemäß § 2 Abs. 2 Verwaltungsregeln für das Einführen und Ausstrahlen der ausländischen TV-Programme[256] kategorisch ausgeschlossen sind. Ebenfalls untersagt ist es, dass Private gemäß § 6 Ausführungsbestimmung zu den Verwaltungsregeln für terrestrische Empfangsanlagen der durch Satellit übertragenen Rundfunksendungen[257] ohne Genehmigung mittels Satellit ausländische Signale empfangen.

II. Die offiziell nicht anerkannte Great Fire Wall und ihre objektive Existenz

Die sogenannte Great Fire Wall (GFW) wurde 1998 zur Inhaltskontrolle an der Grenze des chinesischen Internets „errichtet“. Es kann als Zensursystem bezeichnet werden, das aus der Überwachung, Filterung und Sperrung der internationalen

---

254 Verwaltungsmethode für Abonnements der importierten Presse (订户订购进口**出版物管理**办法) vom 17.3.2011.

255 *Wei*, 332.

256 Verwaltungsregeln für das Einführen und Ausstrahlen von ausländischen TV-Programmen (**境外**电视节目引进、播出管理规定) vom 23.9.2004.

257 Ausführungsbestimmung zu den Verwaltungsregeln für terrestrische Empfangsanlagen und der durch Satellit übertragenen Rundfunksendungen (《卫星电视广播地面接收设施管理规定》实施细则) vom 3.2.1994.

Kommunikation dienenden Soft- und Hardware besteht.[258] Wie oben bereits vorgestellt wurde, betreiben drei staatliche Telekommunikationsunternehmen die internationalen Datenzugangskanäle, so dass sie gezielt die GFW ausbauen können.

Die Inhaltskontrolle durch die GFW funktioniert in beide Richtungen, d.h. sie sperrt nicht nur die Informationen vom Aus- ins Inland, sondern auch solche, die von China ins Ausland gesendet werden. Bislang hat die chinesische Regierung mit wenigen Ausnahmen mehrfach die Existenz der GFW offiziell verneint.[259] Zum Beispiel wurde am 14.7.2014 ein Antrag auf Zugang zu behördlichen Informationen beim Ministerium für Industrialisierung und Information gemäß § 21 Telekommunikationsregeln i.V.m. § 9 Nr. 1 Verordnung für die Offenlegung von Regierungsinformationen gestellt. Der Antragsteller wollte wissen, warum er die Internetseite von Google nicht abrufen konnte. Der Antrag wurde mit der schlichten Begründung zurückgewiesen, dass beim Ministerium für Industrialisierung und Information keine einschlägigen Informationen hierzu vorlägen.[260]

Ungeachtet der fehlenden offiziellen Bestätigung der Existenz der GFW kann jeder Nutzer mit technischen Mitteln selbst überprüfen, ob seiner Internetaktivität an den internationalen Datenzugangskanälen virtuelle Grenzen gesetzt werden. So werden auf der im Ausland ansässigen Webseite „greatfire.org" rund um die Uhr Webseiten überprüft, für die der Zugang aus China gesperrt ist. Es gibt dort eine Liste von allen bisher erfassten gesperrten Webseiten. Gesperrt sind danach 154 von den geführten 1.500 Internetseiten (ca. 15%), einschließlich Facebook, Twitter, Google, Deutsche Welle etc., 3.900 von 30.000 Domains (13%), 5.000 von 15.000 IP-Adressen (30%), 160.000 URLs und sogar 2.310 von 11.000 verschlüsselten Https-Protokollen (21%).[261] Betroffen sind nicht nur politische Themen, sondern auch wirtschaftliche, kulturelle und unterhaltende Informationen.[262]

---

258 *Yuan Yuan*, 20; *Germann*, 299ff.; *Schöttle*, K&R 2007, 366 (368); *Geremie/ Ye*, The Great Firewall of China, abrufbar unter <https://www.wired.com/1997/06/china-3/> [Stand: 7.8.2019].

259 *Sieber*, 44; *Goldsmith/Wu*, 93; *He Qinglian*, The fog of Censorship, 257; Global Times, abrufbar unter <http://tech.huanqiu.com/internet/2015-01/5524442.html> [Stand: 7.8.2019].

260 Antwort des Ministeriums für Industrialisierung und Information zum Antrag auf Offenlegung von Regierungsinformationen wegen Sperren der Google-Seite, abrufbar unter <http://www.chinagfw.org/2014/08/blog-post_51.html> [Stand: 7.8.2019].

261 China Digital Times, <http://hikinggfw.org/blocked_sites> [Stand: 7.8.2019].

262 *Li Yonggang*, 74; *Fei*, 10; *Schöttle*, K&R 2007, 366 (367).

III. Ermächtigungsgrundlagen der Internetsperren sowie typische Fälle

1. Ermächtigungsgrundlagen der Internetsperren

Obwohl die Existenz der GFW bislang nicht offiziell bestätigt ist, bestehen doch zahlreiche Vorschriften, die als Ermächtigungsgrundlagen für Sperrungsverfügungen gegen rechtswidrige Informationen aus dem Ausland dienen.

Bereits in der ersten und bis heute noch gültigen chinesischen Rechtsnorm über IT-Sicherheit – Bestimmungen der VR China zur Steuerung des Internets (1997)[263] – ist es jeder Person verboten, via Internet schädliche Informationen herzustellen, zu kopieren, zu lesen oder zu verbreiten (§ 5). Im Fall des Verstoßes gegen diese Vorschrift müssen die Access-Provider, die Adresse und die Inhalte löschen oder, falls notwendig, die betroffenen Server schließen (§ 10). Von dieser Rechtsgrundlage sind die Betreiber der internationalen Datenzugangskanäle an der Staatsgrenze aber nicht umfasst, da sie nicht als Access-Provider fungieren. Dies ist der erste Grund, warum diese Norm nicht als Rechtsgrundlage für Sperrungen an den internationalen Datenzugangskanälen angesehen wird. Der zweite Grund besteht darin, dass hier zur Inhaltskontrolle nur eine *Löschungs*pflicht anstatt eines *Sperrungs*gebots normiert ist. Die GFW zeichnet sich aber dadurch aus, dass durch sie bereits im Vorfeld eine Sperrung (zum Zugang) eingerichtet wird.

Neben § 5 Bestimmungen der VR China zur Steuerung des Internets kämen noch andere Vorschriften als Rechtsgrundlage für die Durchführung der GFW in Betracht. Gemäß § 7 Beschluss des Ständigen Ausschusses des Nationalen Volkskongresses zur Cyber-Sicherheit, § 62 Telekommunikationsregeln, § 5 des Beschlusses des Ständigen Ausschusses des Nationalen Volkskongresses zur Verstärkung des Datenschutzes[264] sowie § 40 Cyber-Sicherheitsgesetz i.V.m. § 17 Verwaltungsmethode für internationale Datenzugangskanäle müssen die Betreiber der internationalen Datenzugangskanäle die zuständigen Behörden unterstützen und sich verpflichten, die illegalen Aktivitäten im Internet durch die Unterbrechung der Datenübermittelung oder mit anderen Maßnahmen zu verhindern. Ungeachtet der willkürlichen und politisch motivierten Maßstäbe zur Festlegung der

---

263 Bestimmungen zur Steuerung des Internet (计算机信息网络国际联网安全保护管理办法) vom 30.12.1997.

264 Beschluss des Ständigen Ausschusses des Nationalen Volkskongresses zur Verstärkung des Datenschutzes (全国人民代表大会常务委员会关于加强网络信息保护的决定) vom 28.12.2008.

rechtsverletzenden Online-Inhalte ist es für die Frage nach der Ermächtigungsgrundlage für Internetsperren relevant, ob diese Regelungen für die Errichtung von Internetsperren geeignet sind. Die Betreiber der internationalen Zugangskanäle sollen Maßnahmen ergreifen, mit denen die Datenübermittelung unterbrochen oder Inhalte beseitigt werden können. Letzteres – *Beseitigung von Inhalten* – zielt nicht auf Internetsperren ab. Mit „Unterbrechung der Datenübermittelung" sind jedoch auch Internetsperren gemeint. Der chinesische Normgeber hatte wohl gerade ein System wie die GFW vor Augen. Folglich besteht eine Ermächtigungsgrundlage im chinesischen Recht für die Errichtung der GFW durch die Einführung von Internetsperren.

Trotz alltäglich zum Einsatz kommender Internetsperren an der Staatsgrenze finden sich in den entsprechenden Datenbanken hierzu lediglich zwei Gerichtsentscheidungen. Beim Fall *Du vs. Shanghai Telekom* handelt es sich zwar um einen zivilrechtlichen Rechtsstreit auf Basis eines Telekommunikationsdienstvertrags. Es ist aber lohnenswert, Einsicht in die Gesinnung der rechtsprechenden Gewalt in Bezug auf Internetsperren zu erhalten. Hierdurch wird das Dilemma beim Rechtsschutz aus Sicht der Betroffen verständlich.

2. Fallstudien

a) Zugriffsverbot auf eigene im Ausland befindliche Webseiten: *Du vs. Shanghai Telekom*

Der Kläger *Du* fand im Februar 2007 heraus, dass er in Shanghai die eigene Webseite für seine Finanzdienstleistungen, die von einem Server im Ausland gehostet wurde, nicht abrufen konnte. Mit notarieller Bescheinigung des gesamten gesperrten Kommunikationsvorgangs reichte er Beschwerde beim Access-Provider – *Shanghai Telekom* – ein und bekam eine Rückmeldung, in der die Beschwerde mit einer „nicht beantwortbaren Ursache" zurückgewiesen wurde.[265] *Du* erhob daher aufgrund der Nichterfüllung des Dienstvertrags (§ 60 Abs. 1 Vertragsgesetz) vor dem zuständigen Gericht eine Klage gegen *Shanghai Telekom*. Das Gericht sah in der ersten Instanz keine vertragliche Pflichtverletzung, da diese „eine Störung beim Internetzugang" voraussetze, für die der Angeklagte die Beweislast trage. Der bloße Verdacht, die Internetverbindung zwischen dem eigenen Computer und dem ausländischen Server sei gesperrt, reiche dafür nicht aus. Des Weiteren liege

---

265 (2007) Pu Min Yi Chu Zi Nr. 6518 (浦民一初字第 6518 号).

hier auch keine „Störung beim Internetzugang“ vor, da die Verbindung mit dem globalen Internet zu jeder Zeit möglich war. Hierzu führte das Gericht an, dass der Kläger grundsätzlich andere im Ausland ansässige Webseiten aufrufen konnte und zumindest durch den Einsatz von Proxy-Servern auch die Zielseite erreichen könne[266]. Die Berufung des Angeklagten wurde ebenfalls zurückwiesen, weil das Gericht in der zweiten Instanz darüber hinaus argumentierte, dass *Shanghai Telekom* als Zugangsdienstanbieter keine Pflicht übernehme, dem Nutzer Zugriff auf alle Webseiten sicherzustellen, und dass zwischen beiden Vertragsparteien keine solche Vereinbarung vorliege, eine konkrete Seite stets abrufen zu können.[267]

Im vorliegenden Fall hatte der Anklagte zum möglichen Rechtsschutz aus taktischen Gründen den zivilrechtlichen Rechtsweg gewählt. Der zentrale Streitpunkt ist nämlich hierbei, ob eine (technische) Störung beim Internetzugang besteht. Der Kläger wollte auf diese Weise erfahren, was die „ungeklärte Ursache“ für den erfolglosen Zugang auf die Webseite war. Die Gerichte beider Instanzen haben allerdings dem beklagten Unternehmen nicht auferlegt, hierzu Stellung zu nehmen (§ 64 Abs. 1 chZPO a.F.). Insofern gibt dieses Urteil letztlich keine weiterführenden Hinweise auf die Hintergründe der GFW.

b) Blockade von Google-Diensten: *Wang vs. China Unicom*

Der unabhängige Journalist und Netzaktivist *Wang Long* hatte im Mai 2014 seinen Zugangs- und Netzwerkdienstanbieter China Unicom sowie ihre Tochterunternehmen vor Gericht gestellt, da er keine Verbindung zu den Webseiten der Google-Dienste herstellen konnte.[268] Wie beim Fall *Du vs. Shanghai Telekom*, lag *Wangs* Anspruchsgrundlage im Telekommunikationsdienstvertrag. So vermied er es, den öffentlich-rechtlichen Rechtsweg beschreiten zu müssen. Es mangelt bisher an einem umfassenden und effektiven Rechtsschutz im chinesischen öffentlichen Recht. Der Umfang der Sachverhalte, die Gegenstand eines Verwaltungsprozesses sein können, ist noch sehr begrenzt, sodass die Verwaltungsklage gegen behördliche Sperranordnung nicht zulässig ist.

---

266 (2007) Pu Min Yi Chu Zi Nr. 6518 (浦民一初字第 6518 号).

267 (2007) Hu Yi Zhong Min Yi Zhong Zi Nr. 4268 (沪一中民一终字第 4268 号).

268 Ein Mann aus Shenzhen verklagt China Unicom wegen Google-Sperren (深圳男子状告中国联通封锁谷歌); danach stellte er dazu auch einen Antrag auf Offenlegung von Regierungsinformationen, sein Antrag wurde allerding abgelehnt, siehe Antwort des Ministeriums für Industrialisierung und Information zum Antrag auf Offenlegung von Regierungsinformationen wegen Sperren der Google-Seite, abrufbar unter <http://www.chinagfw.org/2014/08/blog-post_51.html> [Stand: 7.8.2019].

In der Gerichtsverhandlung hatte der Rechtsanwalt des beklagten Unternehmens ausgesagt, dass Aussagen von *Wang* zutreffend seien. Allerdings wurde *Wang* wegen Weiterleitung von Protest-Nachrichten in Hongkong mittels Mikroblogging vor der Urteilsfrist festgenommen, sodass keine weiteren Verfahrensschritte durchgeführt wurden. Eine Aufklärung über die Gründe, warum der Zugang zu Google gesperrt war bzw. ist, blieb somit aus. Darüber hinaus führte die Festnahme dazu, dass die Absicht von *Wang* Bürgerinnen und Bürger aufzurufen für ihre eigenen Rechte zu kämpfen, ins Leere lief.

IV. Zwischenergebnis

In Bezug auf Veröffentlichen in China ist zwischen Informationen aus dem Ausland und dem Inland zu unterscheiden. Bei der Sperrung ausländischer Informationen spielt die chinesische Great Fire Wall eine entscheidende Rolle. Das Konzept der Einschränkungen auf Übermittelung der ausländischen Informationen ist aber nicht neu. Für den Import der traditionellen Medien galten schon immer weitreichende Einschränkungen. Nur Staatsunternehmen, staatliche Nachrichtenagenturen und Regierungsrundfunkanstalten dürfen ausländische Medieninhalte importieren. Dies ist auf das Internet zu übertragen. Die Great Fire Wall wurde zur Inhaltskontrolle zwischen dem Inland und dem Ausland eingerichtet und wird von den staatlichen Telekommunikationsunternehmen betrieben. Nutzern gegenüber macht sich die Great Fire Wall so bemerkbar, dass zahlreiche Internetseiten und Kommunikationswege gesperrt sind. Die Ermächtigungsgrundlagen für solche Sperrungen finden sich in verschiedenen Regelungen, etwa § 7 Beschluss des Ständigen Ausschusses des Nationalen Volkskongresses zur Cyber-Sicherheit, § 62 Telekommunikationsregeln, § 5 des Beschlusses des Ständigen Ausschusses des Nationalen Volkskongresses zur Verstärkung des Datenschutzes sowie § 40 Cyber-Sicherheitsgesetz i.V.m. § 17 Verwaltungsmethode für internationale Datenzugangskanäle. Danach müssen die Betreiber der internationalen Datenzugangskanäle die Datenübermittelung von rechtswidrigen Inhalte unterbrechen. In der Praxis fordern die Behörden die Betreiber der internationalen Datenzugangskanäle selten explizit auf, die konkreten illegalen Inhalte zu sperren. Drohende Bußgelder oder Strafen sind hier ausreichend, dass die Sperrungen vorgenommen werden.

F. „Bereinigung“ des Internet im Inland von schädlichen Informationen in Kooperation mit den Telemediendienstanbietern

Neben der Vorzensur bemühen sich Telemediendiensteanbieter mit verschiedenen Ansätzen, die im Inland kursierenden rechtsverletzenden Online-Inhalte zu löschen, zu sperren oder auf sonstige Weise zu unterbinden. Hierbei ist zunächst zwischen Content-, und Access-Providern zu unterscheiden, da sie bei der Haftung für Online-Inhalte nicht gleichzustellen sind. Im weiteren Sinne umfasst in China der Begriff Content-Provider auch Host-Provider, da diese eigene oder fremde Inhalte bereitstellen, während der Access-Provider nur für die *Übermittlung* der Online-Inhalte zuständig ist. Im engeren Sinne unterscheiden sich Content- und Host-Provider. Bei Host-Providern kann im Weiteren unterschieden werden zwischen Web-Hosting, Server-Hosting, Mail-Hosting und Domain-Hosting.[269]

I. Inhaltliche Steuerung von Web-Hosting

Ein Web-Hoster stellt dem Kunden Webspace bereit, damit diese die Informationen veröffentlichen, übermitteln, suchfähig und austauschbar machen.[270] Darunter fallen z.B. soziale Netzwerke, Internet-Bulletin-Boards, Chat-Räume und die Organisation einer Online-Community.

1. Gesetzliche Verpflichtung zur Implementierung von Internetsperren

Eine Verpflichtung zur Implementierung von Internetsperren für Web-Hosting findet sich erstmals in den Bestimmungen der VR China zur Steuerung des Internets von 1997 (§ 10 Nr. 7 Bestimmungen zur Steuerung des Internet), die im Jahr 2000 ebenfalls vom § 7 Beschluss des Ständigen Ausschusses des Nationalen Volkskongresses zur Sicherung der Cyber-Sicherheit formell gesetzgeberisch mit folgender Formulierung festgelegt wurde:

„Soweit schädliche Informationen entdeckt werden, sind Maßnahmen zur Unterbrechung der Übermittelung zu treffen. Jeder Vorfall ist bei den zuständigen Behörden zügig zu melden.“

---

269 *Hoeren/Bensinger*, 353; *Hollenders*, 111.

270 B.25 der Verwaltungsbestimmungen für Internet-Bulletin-Board-Dienste (互联网电子公告服务管理规定) vom 6.11.2000.

Seither sind solche Verpflichtungen in sämtlichen chinesischen Vorschriften zu Telekommunikation und Telemedien zu finden.[271]

Um die Verpflichtung zur Implementierung von Internetsperren zu erfüllen, legen Diensteanbieter in der Regel dem Internetnutzer Sorgfaltspflichten in Form von AGBs auf. Das chinesische Unternehmen Tencent, ein chinesischer Tech-Konzern mit einem großen Tätigkeitsportfolio – unter anderem betreibt er den Sofortnachrichtendienst WeChat – schreibt beispielsweise im Dienstvertrag zur Nutzung von WeChat vor, dass WeChat-Nutzer mit dem Kommunikationsdienst vermeiden müssen, rechtswidrige Online-Informationen herzustellen, zu kopieren oder zu verbreiten, damit Tencent nicht in politische und öffentliche Schwierigkeiten gerät (Art. 2 Benutzerbestimmungen des privaten WeChat-Kontos)[272]. In einigen Rechtsnormen ist eine Warnungspflicht vorgesehen, nach der die Diensteanbieter auf ihrer Webseite eine Liste von schädlichen Informationen sowie Sorgfaltspflichten gut erkennbar vorzuhalten haben (§ 10 Verwaltungsbestimmungen für

---

271 Sie sind zumindest die folgenden Regelungen: § 62 Telekommunikationsregeln (电信条例) vom 25.9.2000; § 16 Methode für Internet-Informationsdienst (**互**联网信息服务管理办法) vom 25.9.2000; § 13 Verwaltungsbestimmungen für Internet-Bulletin-Board-Dienste （**互**联网电子公告服务管理规定） vom 6.11.2000; § 27 Verwaltungsregeln zu Online-Nachrichtendiensten (**互**联网新闻信息服务管理规定) vom 1.6.2007; § 20 Verwaltungsregeln zur Online-Presse (**网**络出版服务管理规定) vom 4.2.2016; § 18 Verwaltungsregeln für audiovisuelle Programme im Internet (**互**联网视听节目服务管理规定) vom 20.12.2007; § 19 vorläufigen Verwaltungsregeln zur Kultur im Netz (**互**联网文化管理暂行规定) vom 17.2.2011; § 5 Beschluss des Ständigen Ausschusses des Nationalen Volkskongresses zur Verstärkung des Datenschutzes (**全国人民代表大会常**务委员会关于加强网络信息保护的决定) vom 28.12.2008; § 8 Abs. 2 Vorläufige Verwaltungsregeln für die Entwicklung der öffentlichen Nachrichtendienste mittels Echtzeitkommunikationstechnik (**即**时通信工具公众信息服务发展管理暂行规定) vom 7.8.201; § 19 Abs. 1 Satz 1 HS. 2 Anti-Terror-Gesetz (**反恐法**) vom 27.12.2015; § 8 Verwaltungsregeln für Suchmaschinen im Internet (**互**联网信息搜索服务管理规定) vom 1.8.2016; § 14 Verwaltungsregeln für Webcast im Internet (**互**联网直播服务管理规定) vom 1.12.2016; § 7 Verwaltungsregeln für Foren im Internet (**互**联网论坛社**区服**务管理规定) vom 1.10.2017; § 8 Verwaltungsregeln für Posten im Internet (**互**联网跟帖评论服务管理规定) vom 1.10.2017; § 11 Abs. 2 Verwaltungsregeln für öffentliche Konten im Internet (**互**联网用户公众账号信息服务管理规定) vom 8.10.2017; § 11 Abs. 2 Verwaltungsregeln für geschlossene Chatgruppen im Internet (**互**联网群组信息服务管理规定) vom 8.10.2017; § 12 Abs. 2 Verwaltungsregeln für Microblog im Internet (**微博客信息服**务管理规定) vom 20.3.2018.

272 Benutzerbestimmungen des privaten WeChat-Kontos (**微信个人**账号使用规范) vom 8.3.2016.

Internet-Bulletin-Board-Dienste[273] oder § 17 Verwaltungsregeln für audiovisuelle Programme im Internet).

2. Behördliche Entgegennahme von Anzeigen zu rechtswidrigen Inhalten aus diversen Quellen

Die Aufsichtsbehörde, vor allem das staatliche Büro für Internet und Informationstechnologie, aber auch die Polizei, erhält Anzeigen bezüglich rechtswidriger Online-Inhalte aus verschiedenen Quellen. Nutzer, Teilnehmer, Telemediendiensteanbieter sowie freiwillige Netzkontrolleure benachrichtigen die Behörde, wenn sie einen Hinweis auf rechtsverletzende Online-Angebote erhalten. Bemerkenswert ist sicherlich die Einrichtung der sog. Netzkontrolleure und die Förderung von Anzeigen durch Privatleute. Die Netzkontrolleure sind meistens von der Verwaltungsbehörde, den Institutionseinheiten oder unmittelbar von der KP angestellt oder rekrutiert und dann entgeltlich oder freiwillig für das Auffinden illegaler Online-Inhalte zuständig.[274] damit die zuständigen Behörden möglichst frühzeitig darauf reagieren können. Sämtliche Diensteanbieter sind dazu verpflichtet, dem Volk eine Möglichkeit zur Anzeige von illegalen Inhalten zu eröffnen. Sie haben damit selbst zu entscheiden, ob die angezeigten Inhalte als rechtswidrig anzusehen sind und ggf. aus dem entfernt werden müssen.[275] Gleichwohl ist jede Einzelper-

---

273 Verwaltungsbestimmungen für Internet- Bulletin-Board-Dienste（**互**联网电子公**告服**务管理规定）vom 6.11.2000.

274 Stellanzeige für freiwillige Kontrolleure vom chinesischen Anzeigezentrum über rechtswidrige und negative Online-Informationen (**中国互**联网违法和不良信息举报中心常年招募“义务监督员”), <http://jubao.12377.cn:13225/common/askSupervisor.html>, [Stand: 7.8.2019].

275 Die betroffenen Regelungen sind § 25 Verwaltungsregeln zur Online-Nachrichtendiensten (**互**联网新闻信息服务管理规定) vom 25.9.2005, § 16 Verwaltungsmethode für Email-Dienste(**互**联网电子邮件服务管理办法) vom 20.2.2006, § 4 Verwaltungsregeln für Nutzernamen im Internet (**互**联网用户账号名称管理规定) vom 4.2.2015, § 5 Vorläufige Verwaltungsregeln für Entwicklung der öffentlichen Nachrichtendienste mittels Echtkommunikationstechnik (**即**时通信工具公众信息服务发展管理暂行规定) vom 7.8.2014, § 12 Verwaltungsregeln für Suchmaschinen im Internet (**互**联网信息搜索服务管理规定) vom 1.8.2016, § 11 Verwaltungsregeln für Foren im Internet (**互**联网论坛社区服务管理规定) vom 1.10.2017, § 10 Verwaltungsregeln für Posten im Internet (**互**联网**跟帖**评论服务管理规定) vom 1.10.2017, § 15 Verwaltungsregeln für öffentliche Konten im Internet (**互**联网用户公众账号信息服务管理规定) vom 8.10.2017, § 12 Verwaltungsregeln für geschlossene Chatgruppe im Internet (**互**联网群组信息服务管理规定) vom 8.10.2017 und § 14 Verwaltungsregeln für Microblogs im Internet (**微博客信息服**务管理规定) vom 20.3.2018.

son berechtigt, Informationen auf den Internetplattformen, die Gesetze oder sonstige Rechtsnormen zur Inhaltskontrolle verletzen, bei der zuständigen Behörde zu melden und ein Beschwerdeverfahren einzuleiten.[276]

3. Typische Fälle

In den einschlägigen Rechtsnormen ist es nicht klar geregelt, welche Maßnahmen von den Diensteanbietern zu ergreifen sind, damit die betroffenen schädlichen Informationen nicht weiter übermittelt werden können. Generell sind in der Praxis die Maßnahmen entweder auf die Inhalte (Löschen, Verbot der Weiterleitung oder Verbot des Kommentierens) oder auf die Nutzerkonten (Einschränken der Kommentierungsfunktion, Verbot vom Freunde-Hinzufügen oder Löschung von Konten) bezogen. Zur Implementierung von solchen Maßnahmen durch Web-Hosting-Anbieter im chinesischen Cyberraum sind nur wenige Gerichtsentscheidungen zu finden.

Der chinesische marktbeherrschende Mikroblogging-Diensteanbieter Sina Weibo behält sich im Dienstvertrag zur Nutzung von Weibo vor, dass er berechtigt ist, notwendige Maßnahmen wie z.B. Löschen der Inhalte, Aussetzen oder Einstellen der Dienste zu ergreifen, soweit Nutzer schädliche Informationen bei Weibo hochladen, oder verbreiten. Hinsichtlich der Besonderheit der Netzdienste sind sie gemäß Vertrag ebenfalls berechtigt, ohne Unterrichtung der Nutzer jederzeit die Mikroblogging-Dienste zu ändern, zu unterbrechen oder ihn teilweise oder ganz zu untersagen. Im Fall *Xu vs. Sina Weibo* sah das Gericht der ersten Instanz solche Vereinbarungen im Dienstvertrag als rechtswidrig an, weil sie gegen das Prinzip der Angemessenheit verstoßen und unter Umständen verhindern, rechtmäßige Inhalte im Netz zu verbreiten.[277] In zweiter Instanz wurde das Urteil der ersten Instanz allerdings aufgehoben, weil der vorliegende Rechtsstreit nicht mehr zum Bereich des Zivilrechts gehöre (§ 108 Nr. 4 i.V. § 111 chZPO. a. F.).[278] Dies ist eine Argumentation, die häufig von Gerichten angeführt wird, wenn diese einen Fall nicht entscheiden wollen. Wie im oben dargestellten Fall *Liu Xiaoyuan vs. Sohu*

---

276 Das Staatliche Büro für Internet und Information (CSII) schließt öffentliche Konten auf WeChat, die unwahre Informationen der parteilichen und staatlichen Geschichte verbreiteten (国家网信办关闭传播歪曲党史国史信息公众号), <http://media.people.com.cn/n/2015/0121/c40606-26421593.html> [Stand: 7.8.2019].

277 (2011) Hai Min Chu Zi Nr. 26297 (海民初字第 26297 号).

278 (2012) Yi Zhong Min Zhong Zi Nr. 01854 (一中民终字第 01854 号).

Blog hat das Gericht die Beschwerde zurückwiesen, da es nach der inneren Weisung vom obersten Volksgericht[279] derartige Fälle nicht annehmen darf.

II. Untersagung kritischer Informationen beim Server-Hosting

Unter Server-Hosting versteht man ein Rechenzentrum, das dem Kunden die Infrastruktur und Betriebsunterstützung in technischer Hinsicht zur Verfügung stellt.[280]

Für Internetsperren beim Server-Hosting gelten in China nahezu keine Sondervorschriften, sondern nur die allgemeinen Rechtsnormen, nach denen sie verpflichtet sind, zur Unterbrechung der Übermittelung illegaler Inhalte die notwendigen Maßnahmen zu ergreifen. Die allgemeinen Rechtsnormen sind v.a. § 10 Nr. 7 Bestimmungen zur Steuerung des Internet, § 7 Beschluss des Ständigen Ausschusses des Nationalen Volkskongresses zur Sicherung der Cyber-Sicherheit oder § 62 Telekommunikationsregeln.

1. Zhang vs. Xiamen ZZY

In einem Fall hatte der Rechtsanwalt *Zhang* seinen Server-Hoster vor Gericht gestellt, der auf Befehl der lokalen Aufsichtsbehörde unter Verdacht geratene Online-Artikel löschen sollte (*Zhang vs. Xiamen ZZY*).[281] Darunter befand sich auch ein Artikel, der auf der Webseite von *Zhang* zu finden war. Aufgrund dessen schloss der Provider die Webseite des Klägers komplett. Bei dem betroffenen Artikel handelte es sich um einen vom Angeklagten auf der eigenen Seite „Rechtsanwälte in Westchina“ weitergeleiteten Artikel, der einen Kommentar über unberechtigte Kontrolle der Medien durch die öffentliche Gewalt enthielt. Der Artikel war bereits in anderen und insbesondere den traditionellen Medien veröffentlicht worden.

---

279 Mitteilung des Obersten Volksgerichts zur Überprüfung der Eröffnung des Verfahrens in Bezug auf Verwaltung des Internets (**最高人民法院关于涉及互**联网管理案件立案审查工作的通知) vom 13.7.2009.

280 B.11 und B.12 der Verwaltungsbestimmungen für Internet- Bulletin-Board-Dienste (互联网电子公告服务管理规定) vom 6.11.2000.

281 Löschungsverfügung abrufbar unter folgender Adresse: https://www.boxun.com/news/gb/china/2008/01/200801040137.shtml [Stand: 07.08.2019].

Die Gerichte der beiden Instanzen sprachen sich für den Standpunkt des Sever-Hosters aus, der die Schließung der Webseite nicht nur auf Befehl der Aufsichtsbehörde durchführte. Es wurde auch argumentiert, dass auch eine Vertragsklausel die Schließung von Webseiten ohne vorherige Unterrichtung zuließ. Im Gerichtsverfahren, so *Zhang*, fand ausschließlich die Beurteilung der Aufsichtsbehörde über die Rechtswidrigkeit des betroffenen Artikels Beachtung.

2. Hu vs. Beijing Xinnet

Ähnliches trug sich auch im Fall *Hu vs. Beijing Xinnet* zu, der als einer der bedeutendsten Fälle auf dem Gebiet der Medienkontrolle gilt. In diesem Fall hat der Kläger den Prozess gewonnen. Es ging um drei von *Prof. Hu* auf seiner eigenen Webseite veröffentlichte Artikel, die sich mit den Themen „Umerziehung durch Arbeit", „Kontrolle der öffentlichen Meinung" und „Korruption" beschäftigten. Im März 2009 wurde die betroffene Seite vom Server-Hoster *Beijing Xinnet* geschlossen, weil die Aufsichtsbehörde diese Artikel als rechtswidrig ansah und daher den Server-Hoster dazu aufgefordert hatte. Die Kläger, neben *Hu* noch mehr als 30 andere Rechtsprofessoren und Rechtsanwälte, waren mit ihrem Begehren erfolgreich. Dies lag zum einen an einem Zuständigkeitsmangel der verfügenden Behörde. Diese war örtlich nicht zuständig. Daneben führten aber auch Versäumnisse auf Seiten des Beklagten zum erfolgreichen Ausgang aus Sicht der Kläger. Es handelte sich um eine zivilrechtliche Klage. Hieran ist auffällig, dass Kläger in Fällen der Online-Inhalte-Kontrolle bevorzugt diesen Rechtsweg wählen. Die Gründe hierfür sollen in einem späteren Kapitel näher erläutert werden.[282]

In den zivilrechtlichen Fällen spielt außerdem die Vertragsausgestaltung stets eine entscheidende Rolle. Anders als im Fall *Zhang vs. Xiamen ZZY* war bei *Hu vs. Beijing Xinnet* im Dienstvertrag eine Unterrichtungspflicht vom Diensteanbieter und ein Berichtigungsrecht des Nutzers vorgeschrieben, falls der Server-Hoster wegen der rechtswidrigen Inhalte die Seite schließe.[283]

---

282 Siehe Kapitel 5.C.

283 Der Betreiber der gesperrten Webseite gewann den Prozess gegen den Vollstrecker der Sperrverfügung (被关停网站告赢封网执行者), < http://www.rmjdw.com/fazhi-bobao/20060501/9781.html >, [Stand: 7.8.2019].

III. Sperren durch Internetzugangsanbieter (Access-Provider)

Die chinesische öffentliche Gewalt fordert auch Zugangsanbieter auf, Internetseiten mit rechtsverletzenden Inhalten zu sperren. Einschlägig sind die oben erörterten allgemeinen Rechtsgrundlagen. Dies sind § 10 Nr. 7 Bestimmungen zur Steuerung des Internet, § 7 Beschluss des Ständigen Ausschusses des Nationalen Volkskongresses zur Sicherung der Cyber-Sicherheit, § 62 Telekommunikationsregeln oder § 27 Nr. 4 Verwaltungsmethode zur gewerblichen Genehmigung der Telekommunikationsdienste. Diese Vorschriften verpflichten Access-Provider dazu, die Inhalte auf von ihnen angeschlossenen Webseiten zu kontrollieren und ggf. den Zugang zu sperren, soweit sie Kenntnis über rechtswidrige Informationen erlangen.

In der Praxis übernehmen die Provider häufig nicht aus eigener Initiative die Verantwortung für die Durchführung von Sperrmaßnahmen. Vielmehr werden solche Pflichten in der unregelmäßig durchgeführten „Kampagne gegen schädliche Informationen“ in Kooperation mit der öffentlichen Gewalt erfüllt. Vom Ergebnis her sind diese Kampagnen sehr effektiv.[284] Sie werden oft vom Ministerium für öffentliche Sicherheit mit anderen Behörden wie dem Staatlichen Büro für Internet und Information, dem Staatlichen Büro für den Kampf gegen Pornographie und andere illegale Publikationen oder dem Ministerium für Industrie und Information geleitet und haben das Ziel, alle drei oder sechs Monaten gegen Cyberdelikte effektiv vorzugehen. Bei den Kampagnen überprüft die Behörde durch enge Zusammenarbeit mit Access-Providern und Host-Providern das Internet auf rechtswidrige Inhalte. Die Ermächtigungsgrundlage für diese Kampagne besteht in der Verpflichtung zur Implementierung von Internetsperren für Internetdiensteanbieter. Unter dem behördlichen Druck sowie einem in Aussicht gestellten Bußgeld kommen Internetdiensteanbieter den Anweisungen der Behörde zügig nach, die betroffenen Informationen zu sperren oder zu löschen, ohne selbst näher zu überprüfen, ob die Inhalte tatsächlich rechtswidrig sind.

---

284 *Hu Ling*, in: Grundrecht und Konstitutionalismus, 411 (413); Das Ergebnis der Kampagne des „Netz Aufräumen” 2014: mehr als 2200 Webseite sind geschlossen (2014 年“净网”成果：2200 余家网站被关闭), <http://www.infzm.com/content/107308>, [Stand: 7.8.2019]. Das Staatliche Büro für Internet und Information (CSII) schließt öffentliche Konten auf WeChat, die manipulierte Informationen der parteilichen und staatlichen Geschichte verbreiteten (国家网信办关闭传播歪曲党史国史信息公众号), <http://media.people.com.cn/n/2015/0121/c40606-26421593.html>, [Stand: 7.8.2019].

IV. Zusammenfassung

Im Inland unterstützen sämtliche Diensteanbieter den Staat bei der Etablierung von Internetsperren. Für Web-Hosting gilt zur Implementierung von Internetsperren die Verpflichtung, Maßnahmen zur Unterbrechung der Übermittelung zu treffen, soweit schädliche Informationen entdeckt werden. Um der Verpflichtung nachzukommen, legen Web-Hosting-Dienste dem Internetnutzer Sorgfaltspflichten in Form von AGBs auf. Zur Aufsicht und Kontrolle nehmen die Behörden die Anzeigen zu rechtswidrigen Inhalten aus diversen Quellen entgegen. Dazu gehören die von der Verwaltungsbehörde, den Institutionseinheiten oder unmittelbar von der KP angestellten oder rekrutierten Netzkontrolleure. Server-Hosting-Dienste sind auch verpflichtet, zur Unterbrechung der Übermittelung illegaler Inhalte die notwendigen Maßnahmen zu ergreifen. Hierzu kann die Löschung von Inhalten gehören. Die Behörden können aber auch Access-Provider auffordern, Internetseiten mit rechtsverletzenden Inhalten zu sperren. Häufig werden solche Pflichten in Form von unregelmäßig durchgeführten „Kampagnen gegen schädliche Informationen“ erfüllt.

G. Zwischenergebnis

In der Strategie zur Bekämpfung illegaler Inhalte in China hat die KP festgelegt, dass Inhaltsregulierung sowie Internetsperren einerseits auf „Rechtsnomen, Verwaltungsaufsicht, Selbstdisziplin der IT-Branche und Sicherung durch Technik“[285] angewiesen sind und andererseits eng mit dem Hebel der Online-Propaganda verbunden sein soll. Daraus ergibt sich auch, dass der chinesischen öffentlichen Gewalt schon früh bewusst war, wie wesentlich das Internet für die öffentliche Meinungsbildung ist.[286] Bei der Kontrolle der traditionellen Medien hat China zuvor genügend Erfahrung gesammelt hat, die ohne großen Aufwand auf den Cyberraum in Form von Inhaltsregulierung und Internetsperren übertragen werden kann.

---

285 Beschluss des Zentralkomitees der KP zur Verstärkung des Aufbaus der Regierungskompetenz (关于加强党执政能力建设的决定) vom 19.9.2004.

286 *Li Yonggang*, Journal of Nanjing Tech University 2007, 44 (46); *Liu Han*, Peking University Law Journal 2016/2, 518 (524); dagegen *Christiansen*, MMR 2000, 123 (124).

Das Konzept des Schutzes der Staatssicherheit steht im Mittelpunkt des chinesischen Internetrechts. Vor diesem Hintergrund sind die Inhaltsregulierung und Internetsperren gegen rechtswidrige Online-Inhalte in den Bereich der Netzwerk- und Informationssicherheit integriert. In China werden die illegalen Online-Inhalte im Grunde genommen so wie Viren oder Schadsoftware behandelt. Anknüpfungspunkt für die Gesetzgebung ist dann nicht nur der *rechtswidrige* Inhalt, sondern der *schädliche* Inhalt. Seit der Bestimmung zur Steuerung des Internet und der Methode für Internet-Informationsdienste wird eine Liste der politischen, sozialen und privaten schädlichen Informationen geführt. Im chinesischen Recht ist die Bestimmung solcher schädlichen Informationen sehr weit gefasst. Zur besseren Handhabung hat das oberste Volksgericht zwar Leitlinien zur Auslegung erlassen, die aber umstritten sind. Neben dem Ausstellen einer Liste der schädlichen Informationen werden Gatekeeper in strengen Genehmigungsverfahren ausgewählt. Betroffen sind die Diensteanbieter der Grundtelekommunikation, Access-, Host- und Content-Provider. Für Diensteanbieter, die im Verlags- oder Nachrichtenwesen tätig sind, müssen darüber hinaus noch Sondergenehmigungen beantragt werden. Im Rundfunkbereich gilt noch das Modell des Regierungsrundfunks.

Bei Internetsperren wird zwischen der Kontrolle *vor* und *nach* der Veröffentlichung von Informationen unterschieden. Bei der Vorzensur gilt sowohl das Zensurgebot der Online-Presse, des Online-Rundfunks und der Online-Nachrichtendienste als auch die Selbstdisziplin der Diensteanbieter, die durch Filtern der Schlüsselwörter ihre potenzielle Verantwortung für rechtswidrige Informationen vermeiden. Es besteht zwar im Presse- und Rundfunkbereich das gesetzliche Zensurgebot. Gegen die Telemediendiensteanbieter, die nicht zum Presse- und Rundfunkbereich zugeordnet sind, liegt keine Ermächtigungsgrundlage für das allgemeine Filtern der Schlüsselwörter vor der Veröffentlichung der Online-Angebote vor. Bei der Veröffentlichung wird zwischen Informationen aus dem Ausland und dem Inland unterschieden. Bei der Sperrung ausländischer Informationen spielt die berüchtigte chinesische GFW eine entscheidende Rolle, während im Inland sämtliche Diensteanbieter den Staat bei der Etablierung von Internetsperren unterstützen. Die Rechtsprechung in diesem Bereich lässt Rechtsschutzlücken erkennen. Es besteht für Netznutzer kaum die Möglichkeit, sich erfolgreich gegen den verweigerten Zugriff auf bestimmte Internetseiten zur Wehr zu setzen.

4. Kapitel SPERRMAßNAHMEN WEGEN RECHTSWIDRIGER ONLINE-INHALTE IN DEUTSCHLAND

Zur Staatsaufgabe gehört die Gewährleistung der Sicherheit der Staatsbürger, was ebenfalls die Bekämpfung illegaler Inhalte durch Internetsperren betrifft.[287] Angesichts des Bedürfnisses nach Sicherheit und angesichts der durch mögliche Sperren beschränkten Kommunikation zeigt allerdings die Entwicklung in Deutschland deutlich, dass Internetsperren – also Inhalte löschen, Sperren durch Access-Provider[288] – sowohl auf gesetzgeberischer Ebene als auch in der Rechtsprechung umstritten sind. Im Jahr 2017 wurde mit dem Netzwerkdurchsetzungsgesetz (NetzDG) ein Compliance-Modell zur Gewährleistung der schnelleren Löschung von rechtswidrigen Online-Inhalten erlassen.

Im Folgenden soll zunächst ein kurzer Überblick zur Inhaltsregulierung gegeben werden (A.). Dabei geht es um die Frage, welche Inhalte online rechtswidrig sind und wer als Adressat für Maßnahmen gegen rechtswidrige Inhalte in Frage kommt. Hier wird auch das Netzwerkdurchsetzungsgesetz (NetzDG) angesprochen. Dieses Gesetz enthält einen innovativen Ansatz für die Regulierung von Online-Inhalten auf sozialen Netzwerken. Im Anschluss daran soll der Fokus auf Sperrmaßnahmen gegenüber Zugangsanbietern gelegt werden (B.-F.). Die Sperrmaßnahmen gegenüber Zugangsanbietern eignen sich besonders gut für einen Rechtsvergleich, da sich hierzu in Deutschland engmaschige Kriterien für die Zulässigkeit herausgebildet haben. Bei Sperrmaßnahmen gegenüber Access-Providern handelt es sich des Weiteren um sehr einschneidende Maßnahmen. In China sind sie Gang und Gebe – in Deutschland nur unter bestimmten Voraussetzungen zulässig. Es sollen die relevanten Entwicklungen und die Rechtsprechung zu Sperrverfügungen in speziellen Bereichen dargestellt werden. Im Einzelnen geht es um die Düsseldorfer Sperrverfügungen gegen rechtsextremistische Online-Inhalte (B.). Danach soll das ehemalige Zugangserschwerungsgesetz gegen Kinderpornographie vorgestellt werden (C.). Relevant ist auch die Blockade illegaler Glücksspiele im Internet (D.). Noch zum öffentlichen Recht zählend ist kurz darzustellen, inwieweit Access-Provider unter Anwendung der ordnungs- oder polizeirechtlichen Generalklauseln in Anspruch genommen werden können (E.). Zudem sollen die

---

287 *Hobbes*, Kap. 17, 85 ff.; *Isensee*, Das Grundrecht auf Sicherheit, 4; Stoll, 4; *Thiel*, 149; *Germann*, 36 ff.

288 Siehe hierzu 1. Kap. D. und 3. Kap. D.

Möglichkeiten dargestellt werden, inwieweit zivilrechtliche Ansprüche auf Sperrmaßnahmen gegen Access-Provider gerichtet sein können (E.). Zum Ende des vierten Kapitels geht es um zivilrechtliche Sperrungsverlangen gegen Access-Provider (F.). Es soll dabei auch überlegt werden, ob dies auch Relevanz für die Zugangsregulierung hat.

Die Konzentration auf wenige Bereiche zeigt schon, dass in Deutschland wesentlich zurückhaltender mit Internetsperren umgegangen wird. Internetsperren sind vor allem in folgenden Bereichen diskutiert worden: rechtsextremistische Online-Angebote, Kinderpornografie, illegale Glücksspielangebote, wettbewerbswidrige Inhalte sowie Urheberrechtsverletzungen. Während China, wie gezeigt, ein praktisch lückenloses Internetsperrensystem aufgebaut hat, ist zu prüfen, inwieweit in Deutschland ein Sperrsystem besteht.

A. Grundsätzliches zur Inhalteregulierung in Deutschland

In Deutschland existiert keine Liste von schädlichen oder sonst wie rechtswidrigen Informationen wie in China. Während es in China eine lange Liste mit schädlichen Informationen gibt, bezieht sich die Inhalteregulierung auf viele verschiedene Regelungswerke. Vor der Behandlung der Möglichkeiten, gegen Access-Provider vorzugehen (ab B.), werden die Grundsätze der Inhaltsregulierung dargestellt.

I. Grundsatz der Meinungs- und Informationsfreiheit

Zunächst ist zu betonen, dass die Medienfreiheit der Grundsatz ist. Diese ist in Art. 5 Abs. 1 GG geregelt und besagt:

„Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt.“

Das heißt, dass grundsätzlich die Inhalte – auch online – frei sind. Von diesem Grundsatz geht in Bezug auf die Äußerung von Meinungen alles aus. Es darf keine Beschränkung erfolgen. In Satz 1 ist auch die Informationsfreiheit enthalten. Aus allgemein zugänglichen Quellen muss man sich frei unterrichten können. Diese

beiden verfassungsrechtlichen Bestimmungen führen dazu, dass grundsätzlich Zugangssperren gegen bestimmte Inhalte im Internet einen Eingriff in Grundrechte darstellen.

Die Meinungsfreiheit kann nach Art. 5 Abs. 2 GG eingeschränkt werden, wenn dies aus Sicherheitsgründen oder aus Gründen des Schutzes des allgemeinen Persönlichkeitsrechts erforderlich ist. Es sind hierbei verschiedene Interessen in Ausgleich zu bringen. Wenn also bestimmte Inhalte die Sicherheit gefährden oder auch eine Person unangemessen herabwürdigen, dann kann die Verbreitung dieser Inhalte im Einklang mit den Grundrechten unterbunden werden. Das Grundgesetz legt explizit fest, dass eine Zensur nicht stattfindet, Art. 5 Abs. 1 S. 3 GG. Hiermit ist die Kontrolle von Inhalten im Vorfeld der Veröffentlichung gemeint.[289] Dies ist ein Unterschied zu China, wo sogar ein Gebot zu Zensur besteht.[290]

II. Presse- und Rundfunkrecht: Medien sollen staatsfern sein

Die Tätigkeit als Presseunternehmen ist zulassungsfrei. Ebenso unterliegen auch Telemedien keinem Zulassungserfordernis.[291] Für private Rundfunkveranstalter gibt es ein Zulassungsverfahren.[292] Die Regelungen für die professionellen Medien sind in den Landespressegesetzen und dem Rundfunkstaatsvertrag niedergeschrieben. Die dortigen Regelungen sind darauf ausgerichtet, die Arbeit der Medien zu ermöglichen. Es handelt sich um Schutzbestimmungen, wodurch eine andere Regelungsintention gegeben ist als in China. Während in China, wie gezeigt[293], der Einfluss der kommunistischen Partei und der Regierung auf die Medien sehr groß ist, wird in Deutschland Wert auf die Staatsferne der Medien gelegt. Es findet keine Kontrolle statt. Es werden in inhaltlicher Hinsicht moderate Anforderungen an die Medien gestellt. Zu nennen sind hierbei die Sorgfaltspflichten

289 *Grabenwarter*, in: Maunz/Dürig, GG, Art. 5 Abs. 2, Rn. 116.
290 Siehe Kapitel 3. D. I.
291 § 4 TMG und § 54 I RStV.
292 § 20 RStV.
293 Siehe Kapitel 3. C.

bei der Recherche von Informationen.[294] Die Rundfunkanstalten haben zudem einen Vielfalts- und Integrationsauftrag.[295] Hier wird die Zielrichtung des öffentlichen Rundfunks deutlich, dass er die Demokratie fördern soll, indem er die Meinungsbildung in der Bevölkerung ermöglicht.

III. Bestimmte rechtswidrige Inhalte

In Deutschland gibt es, anders als in China, keine Liste von rechtswidrigen Informationen. Die Rechtswidrigkeit einer Information bestimmt sich vielmehr aus allgemeinen Gesetzen. Zuvörderst muss das Strafgesetzbuch angesprochen werden. Wenn mit dem Erstellen oder dem Verbreiten eines Inhalts eine Straftat begangen wird, ist dieser Inhalt zu löschen. Relevant sind vor allem die Straftatbestände der Beleidigung (§§ 185 ff. StGB), der Volksverhetzung (§ 130 StGB) oder der Androhung von Straftaten (§ 126 StGB). In zivilrechtlicher Hinsicht besteht ein Anspruch auf die Entfernung von Inhalten, wenn die persönliche Ehre verletzt wird. Der Betroffene kann in diesem Fall einen Anspruch auf Unterlassung nach § 1004 BGB analog geltend machen. Besondere Anforderungen an Inhalte können sich auch aus speziellen Vorschriften ergeben. Der Jugendmedienschutz-Staatsvertrag, sieht Schutzvorkehrungen für jugendgefährdende Inhalte auf Telemedien vor.

IV. Grundsatz der Inanspruchnahme von Content- und Host-Providern

Als Grundsatz ist hervorzuheben, dass primäre Adressaten von Maßnahmen gegen rechtswidrige Inhalte im Internet die Content- und Hostprovider sind. Dies ergibt sich in grundlegender Hinsicht aus dem Verfassungsrecht, da mit einer Sperrmaßnahme gegen einen Access-Provider ein tiefgreifender Eingriff verbunden ist. Access-Provider können in der Regel erst dann in Anspruch genommen werden, wenn Maßnahmen gegen den Content- oder Hostprovider nicht effektiv sind. Im Einzelnen ist die prioritäre Inanspruchnahme von Content- und Hostprovidern z.B. in § 59 Abs. 4 RStV, § 20 Abs. 4 JMStV oder auch § 8 TMG geregelt. Diese vornehmliche Inanspruchnahme von Content- und Host-Providern führt dazu, dass der Internetzugang in Deutschland relativ frei von Sperren ist. Die Inanspruchnahme von Access-Providern führt zu einer starken Beschränkung der Freiheit im

---

294 Bspw. § 10, 54 RStV; § 6 PresseG NRW, Ziffer 2 Pressekodex; verfassungsrechtlich Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, siehe hierzu *Schierbaum*, 265.

295 § 25 RStV.

Internet. Deshalb wird in diesem Abschnitt das Hauptaugenmerk auf die Access-Provider gerichtet. Die Anforderungen für die Inanspruchnahme dieser Dienste-anbieter machen deutlich, wie rechtsstaatliche Prinzipien sich auf die Durchsetzung des Rechts auswirken. Im Gegensatz hierzu steht das chinesische System, in dem alle Unternehmen, die im Internet tätig sind, zur Inhalteregulierung herangezogen werden.

Für Host-Provider gilt der Grundsatz „Notice-and-Take-down". Dieser ist in der E-Commerce-Richtlinie[296] geregelt und in § 7 TMG umgesetzt. Er besagt, dass derjenige, der nicht unmittelbar für den Inhalt verantwortlich ist, den Inhalt aber bereitstellt – so wie der Host-Provider –, nicht verpflichtet ist, seine Plattform nach rechtswidrigen Inhalten zu durchsuchen. Nur wenn er darauf aufmerksam gemacht wird oder sonst wie davon erfährt (*notice*), muss er dafür sorgen, dass auf den Inhalt nicht mehr zugegriffen werden kann (*take down*). Auch hier wird deutlich: Je weiter ein Akteur von der rechtswidrigen Handlung entfernt ist, desto höher sind die Anforderungen, dass dieser für die Beseitigung der Rechtsverletzung zuständig ist.

V. Neuer Regelungsansatz mit dem NetzDG

Das „Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken" (Netzwerkdurchsetzungsgesetz – NetzDG)[297] ist an soziale Netzwerke gerichtet. Diese stellen die Infrastruktur zur Kommunikation online bereit. Aufgrund dessen bietet es sich an, die sozialen Netzwerke in Anspruch zu nehmen, wenn es darum geht, die Kommunikation etwa frei von strafrechtlich relevanten Inhalten zu halten. Im Folgenden ist näher auf den Regelungsansatz des NetzDG einzugehen. Wird durch dieses gar ein neues Kapitel in der Sperrung von Online-Inhalten eingeleitet?

---

296 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr"), Amtsblatt Nr. L 178.

297 BGBl. I 2017, 3352.

1. Gesetzgebungshintergrund

Das NetzDG knüpft an die Erfahrungen mit dem Notice-and-Take-down-Verfahren an. Eigentlich sollte dieses sicherstellen, dass die Diensteanbieter den Löschpflichten nachkommen, ohne zu einer ständigen Überwachung verpflichtet zu sein. Wie in der Begründung des Entwurfs zum NetzDG zu lesen ist, war ein Ergebnis der Erhebungen der Task-Force der Bundesregierung gegen Hate-Speech und andere strafrechtswidrige Inhalte im Jahre 2015, dass die meisten sozialen Netzwerke ihren (Lösch-)Verpflichtungen nicht hinreichend nachkommen.[298] Rechtswidrige Inhalte bleiben meistens auf den sozialen Plattformen. Zwei maßgebliche Unternehmen in dieser Branche, nämlich Facebook und Twitter, löschten jeweils nur 39% und 1% der verbotenen Inhalte, während YouTube eine Quote von 90% erreichte.[299] Außerdem wurde auch ein Transparenzproblem bei der Behandlung der rechtswidrigen Inhalte auf sozialen Netzwerken festgestellt.[300] Um dies zu verbessern, wurde das NetzDG kurz vor der Bundestagswahl 2017 erlassen. Die Struktur des NetzDG ist klar aufgebaut und teilt sich in vier Bereiche, nämlich den Anwendungsbereich des NetzDG, die Berichtspflicht der sozialen Netzwerke, den Umgang mit Beschwerden über rechtswidrige Inhalte und die verwaltungsrechtlichen Sanktionen.

2. Anwendungsbereich des NetzDG und betroffene Inhalte

Der Anwendungsbereich des Gesetzes ist in § 1 NetzDG geregelt, wobei die Definition des sozialen Netzwerks und der Umfang der rechtswidrigen Inhalte die zwei wichtigsten Fragen sind. Unter einem sozialen Netzwerk versteht man danach einen Telemediendienstanbieter, der es als Geschäftsmodell den Nutzern ermöglicht, in einer bestimmten Form (Text, Bilder sowie Videos) mit anderen Nutzern beliebige Information zu teilen oder der Öffentlichkeit zugänglich zu machen (§ 1 Abs. 1 Satz 1 NetzDG). Ausgeschlossen sind zunächst Plattformen, die journalistisch-redaktionell gestaltete Inhalte anbieten (§ 1 Abs. 1 Satz 2 NetzDG). Nicht umfasst sind auch Dienste zur Individualkommunikation oder auch Emailservices. Im Entwurf der Fraktionen CDU/CSU und SPD wurde auch über den Austausch von Inhalten in geschlossenen Netzwerken (*gated community*), z.B. in einer Chat-Gruppe von einem Instant Messenger, diskutiert. Im Ergebnis fällt

---

298 BT-Drs. 18/12356, 9; hierzu auch *Holznagel*, ZUM 2017, 615 (615).

299 BT-Drs. 18/12356, 9; Weiteres hierzu siehe *Holznagel*, ZUM 2017, 615 (616); *Ders*., MMR 2018, 18 (20); *Ders*., ZUM 2017, 615 (615 f.); *Gersdorf*, MMR 2017, 439 (439).

300 BT-Drs. 18/12356, 9.

dies nicht unter den Begriff des sozialen Netzwerks i.S.d. NetzDG.[301] Angesichts des Erfordernisses des Austauschs oder der Zugänglichmachung *jeder beliebigen* Information sind zudem die Plattformen mit speziellen Inhalten, z.B. LinkedIn als Berufsportal oder Amazon als Verkaufsportal, ausgeschlossen (§ 1 Abs. 1 Satz 3 NetzDG). Um die Innovationsfähigkeit in der Internetbranche nicht zu blockieren und kleine Unternehmen nicht zu belasten, gilt das NetzDG ausschließlich für Plattformen mit mehr als 2 Mio. in Deutschland registrierten Nutzern (§ 1 Abs. 2 NetzDG). Diese Anzahl von Nutzern weisen nur die sehr großen Netzwerke auf.

Das NetzDG betrifft zudem nicht jegliche rechtswidrigen Inhalte auf den Plattformen. Um das Bestimmtheitsgebot und den Grundsatz der Verhältnismäßigkeit zu beachten, hat der Gesetzgeber die Pflichten aus dem NetzDG auf eine Auswahl von strafrechtlichen Normen beschränkt.[302] Betroffen sind insgesamt in 22 Straftaten geschützte Schutzgüter, die dem Schutz der Staatssicherheit, der öffentlichen Ordnung und der persönlichen Ehre dienen (§ 1 Abs. 3 NetzDG). Hierbei wird nur überprüft, ob der objektive Tatbestand und die Rechtswidrigkeit einer Straftat erfüllt sind, ohne die Schuld des Täters zu berücksichtigen.[303]

3. Umgang mit Beschwerden über rechtswidrige Inhalte

Neben der Berichtspflicht sind die sozialen Netzwerke noch verpflichtet, ein nutzerfreundliches Beschwerdeverfahren einzurichten, wodurch die Beschwerden erkennbar, unmittelbar und ständig übermittelt werden (§ 3 Abs. 1 NetzDG). Sofern die Plattformen in diesem effektiven und transparenten Verfahrensrahmen von der Beschwerde Kenntnis nehmen, müssen die sozialen Netzwerke zügig überprüfen, ob die jeweiligen Inhalte gemäß § 1 Abs. 3 NetzDG i.V.m. den entsprechenden Paragraphen aus dem Strafrechtsgesetzbuch rechtswidrige Inhalte darstellen (§ 3 Abs. 2 Nr. 1 NetzDG).

Umstritten ist die Unterscheidung zwischen *offensichtlich* rechtswidrigen und *anderen* rechtswidrigen Inhalten Die offensichtlich rechtswidrigen Inhalte müssen grundsätzlich innerhalb von 24 Stunden gesperrt oder gelöscht werden, während

---

301 BT-Drs. 18/12356, 10; *Gersdorf*, MMR 2017, 439 (439); *Holznagel*, ZUM 2017, 615 (619).

302 BT-Drs. 18/12727, 20; BT-Drs. 18/12356, 18; *Feldmann*, K&R 2017, 292 (293); *Holznagel*, ZUM 2017, 615 (620); *Peifer*, CR 2017, 809 (810).

303 BT-Drs. 18/13013, 21; BT-Drs. 18/12356, 10, 18; *Holznagel*, ZUM 2017, 615 (620); *Höld*, MMR 2017, 791 (791 f.).

die Frist zum Sperren und Löschen anderer rechtswidriger Inhalte sieben Tage beträgt (§ 3 Abs. 2 Nr. 2 und 3 NetzDG). Wenn der Umgang mit den Beschwerden noch von anderen Tatsachen abhängt und der Nutzer dazu Stellung nimmt oder das soziale Netzwerk im Fall von einer erhöhten Komplexität der Entscheidung von der Einrichtung der Regulierten Selbstregulierung[304] Gebrauch macht, kann die Frist von sieben Tagen überschritten werden (§ 3 Abs. 2 Nr. 3 NetzDG). Letztlich sind die sozialen Netzwerke verpflichtet, dem Nutzer und Beschwerdeführer die Entscheidung mit Begründung bekanntzugeben, damit sie entsprechende Schutzmaßnahmen treffen können (§ 3 Abs. 2 Nr. 2 und 3 NetzDG).[305]

4. Verwaltungsrechtliche Sanktionen und Vorabentscheidung

Für die Verletzung der Berichtspflicht gemäß § 2 NetzDG und der Pflichten beim Umgang mit Beschwerden über rechtswidrige Inhalte gemäß § 3 NetzDG sind Bußgeldregelungen vorgesehen. Daraus ergibt sich, dass die Verwaltungsmaßnahmen nicht gegen *Nutzer* von sozialen Netzwerken gerichtet sind, sondern gegen die Betreiber der sozialen Netzwerke. Ein Bußgeld wird nicht für *einzelne* Fehlentscheidungen des sozialen Netzwerks verhängt, sondern für das *organisatorische* und *systemische* Versagen des Beschwerde- und Berichtsverfahrens.[306] Um die Voraussetzungen für die Einleitung eines Bußgeldverfahrens zu konkretisieren und die Höhe der zu verhängenden Geldbuße zu bestimmen, hat das Bundesamt für Justiz (BfJ) 2018 Leitlinien zur Festsetzung von Geldbußen im Bereich des Netzwerkdurchsetzungsgesetzes (NetzDG-Bußgeldleitlinien) erlassen.[307]

Werden die rechtswidrigen Inhalte in einer Vielzahl von Fällen nicht entfernt oder gelöscht, sodass ein systemisches Entscheidungsdefizit vorliegt, soll sich die Behörde an das Gericht vorab wenden (§ 4 Abs. 5 1 NetzDG). In diesem Verfahren entscheidet das Gericht über die Rechtswidrigkeit der betroffenen Inhalte. Dies entspricht auch dem Gewaltenteilungsprinzip, da das Gericht für die Entscheidung der Rechtswidrigkeit der Inhalte zuständig sein soll.[308] Die Vorabentscheidung

---

304 Eine solche Einrichtung ist nach dem NetzDG von den sozialen Netzwerken selbst zu errichten. Bisher gibt es keine solche Einrichtung.

305 BT-Drs. 18/13013, 21; BT-Drs. 18/12356, 23; *Holznagel*, ZUM 2017, 615 (621).

306 *Guggenberger*, NJW 2017, 2577 (2580); Stellungnahme *Holznagel* vom 16.6.2017, 24; *Hain/Ferreau/Brings-Wiesen*, K&R 2017, 433 (435).

307 Leitlinien vom 22.3.2018, Abrufbar unter dem Link: https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/NetzDG_Bußgeldleitlinien.html [Stand: 7.8.2019].

308 BT-Drs. 18/12356, 24; *Feldmann*, K&R 2017, 292 (294); *Holznagel*, ZUM 2017, 615 (621); *Höld*, MMR 2017, 791 (792 ff.).

des Gerichts hat letztlich Bindungswirkung für die Behörde und ist damit nicht anfechtbar (§ 4 Abs. 5 NetzDG).

VI. Zwischenergebnis und Relevanz für die folgende Darstellung

Der kurze Überblick hat gezeigt, dass bei der Inhalteregulierung Unterschiede zum chinesischen System bestehen. In China existiert eine umfangreiche, detaillierte Liste von Informationen, die als schädlich eingestuft werden. In Deutschland ist dies nicht so. Hier bemisst sich die Rechtswidrigkeit eines Inhalts in der Regel danach, wenn dieser gegen strafrechtliche Bestimmungen oder privatrechtliche Schutzgesetze verstößt. In Deutschland sind jedoch primär die Content- und Hostprovider in Adressaten von administrativen oder zivilen Maßnahmen zur Entfernung des rechtswidrigen Inhalts. Dieses Verständnis ist notwendig, um die Darstellung zu den Accessprovidern in den Kontext zu setzen. Es wird deutlich, dass hierfür hohe Anforderungen zu erfüllen sind. Im Folgenden sollen diejenigen Fälle beschrieben werden, in denen Sperrmaßnahmen gegen Zugangsanbieter verhängt bzw. diskutiert wurden.

B. Die Düsseldorfer Sperrverfügungen gegen rechtsextremistische Online-Angebote

I. Überblick über die Düsseldorfer Sperrverfügungen

Im Jahr 2002 erließ die Bezirksregierung Düsseldorf Sperrverfügungen gegen insgesamt 76 in Nordrhein-Westfalen ansässige Access-Provider, um die von zwei in den USA gehosteten Internetseiten bereitgestellten rechtsradikalen und jugendgefährdenden Inhalte für Internetnutzer in NRW nicht mehr zugänglich zu machen.[309] Diese „Düsseldorfer Sperrverfügungen“ stellen den Auftakt einer Reihe

[309] Gegenstand des Verwaltungsverfahrens waren die zwei Internetseiten: http://www.stormfront.org und http://www.nazi-lauck-nsdapao.com; der Inhalt einer der Sperrverfügungen, abrufbar unter: http://odem.org/material/verfuegung/ [Stand: 7.8.2019]; zum Überblick über die von Webseiten angebotenen Inhalte sowie den Vorgang der Verfügungen siehe *Billmeier*, 29 ff.; *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (2); *Degen*, 42 f.; *Dietlein/Heinemann*, in: Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2003, 395 (395 ff.); *Engel*, MMR-Beil. 4/2003, 1 (2).

von staatlich sowie privat veranlassten Internetsperren dar.[310] Die Sperrverfügung war gestützt auf § 18 Abs. 3 des Staatsvertrags über Mediendienste (MDStV a.F.)[311]. Grund für die Sperrung war, dass die betroffenen Internetseiten rechtsradikale und jugendgefährdende Inhalte bereitstellen und darüber hinaus, dass eine Inanspruchnahme von Host- und Content-Providern in den USA nicht möglich war.[312]

Dem Access-Provider standen drei Sperrmöglichkeiten zur Auswahl (Ausschluss von Domains im Domain-Server, Verwendung eines Proxy-Servers und Ausschluss von IPs durch Sperrung im Router),[313] wobei die Domain-Sperre hinsichtlich der Verhältnismäßigkeitsprüfung bevorzugt heranzuziehen war.[314] Gegen die sofortige Vollziehung der Sperrverfügungen wurden mehrere Verfahren des einstweiligen Rechtsschutzes zum Wiederherstellen der aufschiebenden Wirkung i.S.d. § 80 Abs. 5 VwGO eingeleitet.[315] Es folgten auch viele Anfechtungsklagen vor den zuständigen Verwaltungsgerichten.[316]

---

310 *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (2); *Billmeier*, 32 ff.; *Engel*, MMR-Beil. 4/2003, 1 (2); *Spindler/Volkmann*, K&R 2002, 398 (398); *Bremer*, MMR 2002, 147 (147); *Zimmermann*, NJW 1999, 3145 (3145).

311 GV.NRW, 28.6.1997, S. 158; Aufgehoben durch Art. 2 StV v. 31. 7. 2006 (GVBl. S. 414).

312 Sperrverfügung vom 6.2.2002, abrufbar unter <http://odem.org/material/verfuegung/> [Stand: 7.8.2019], 6 f.; zur strafrechtlichen Verantwortlichkeit für den Inhalt von Internetseiten siehe *Dietlein/Heinemann*, in: Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2003, 395 (397 ff.).

313 *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (2); Sperrverfügung vom 6.2.2002, abrufbar unter <http://odem.org/material/verfuegung/> [Stand: 7.8.2019], 6 f.; BGH, U. v. 26.11.2015 - I ZR 174/14, Rn. 62 f.; OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 911; *Dietlein/Heinemann*, in: Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2003, 395 (395).

314 Sperrverfügung vom 6.2.2002, abrufbar unter <http://odem.org/material/verfuegung/> [Stand: 7.8.2019], 8 ff.

315 Verfahren des einstweiligen Rechtsschutzes: VG Aachen, B. v. 5.2.2003 - 8 L 1284/02; VG Arnsberg, B. v. 6.12.2002 - 13 L 1848/02; VG Düsseldorf, B. v. 19.12.2002 - 15 L 4148/02; VG Gelsenkirchen, B. v. 18.12.2002 - 1 L 2528/02; VG Köln, B. v. 7.2.2003 - 6 L 2495/02; VG Köln, B. v. 17.10.2003 - 6 L 699/03; VG Minden, B. v. 31.10.2002 - 11 L 1110/02; OVG NRW, B. v. 19.3.2003 - 8 B 2567/02; B. v. 25.3.2003 - 8 B 218/03; B. v. 25.3.2003 - 8 B 513/03; B. v. 26.3.2003 - 8 B 82/03; *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (2); *Degen*, 42 f.; *Dietlein/Heinemann*, in: Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2003, 395 (396).

316 Vgl. z.B. VG Arnsberg, U. v. 26.11.2004 - 13 K 3173/02; VG Köln, U. v. 3.3.2005 - 6 K 7151/02; VG Köln, U. v. 3.3.2005 - 6 K 7603/02; VG Düsseldorf, U. v. 10.5.2005 - 27 K 5968/02; VG Gelsenkirchen, U. v. 28.7.2006 - 15 K 2170/03.

II. Unterschiedliche Auffassungen im vorläufigen Rechtsschutz sowie im Hauptsacheverfahren

Im vorläufigen Verfahren waren die Auffassungen der zuständigen Verwaltungsgerichte höchst unterschiedlich. Die Verwaltungsgerichte verneinten eine offensichtliche Rechtmäßigkeit oder Rechtswidrigkeit.[317] Die unklaren Vorgaben zu Internetsperren spielten hierbei eine entscheidende Rolle. Im Rahmen der daraufhin durchzuführenden Abwägung kam es zu unterschiedlichen Ergebnissen. Während sich die Verwaltungsgerichte Arnsberg und Aachen für die öffentlichen Interessen und somit für eine Sperrverfügung aussprachen,[318] lehnte das Verwaltungsgericht Minden dies aufgrund der finanziellen Nachteile für den betroffenen Access-Provider ab.[319] Das OVG NRW hat zweitinstanzlich nach summarischer Prüfung die Rechtsmäßigkeit der Sperrverfügung zwar nicht ausdrücklich bejaht, aber dennoch neigt es im Beschluss vom März 2003 zu einer inhaltlichen Billigung der Sperrverfügung.[320] Die weiteren Beschlüsse vom OVG NRW wichen hiervon nicht ab.[321] Dem folgten die Gerichte in den Hauptsacheentscheidungen.[322] Auf die Einwände der Access-Provider reagiert z.B. das VG Köln mit sehr ausführlichen Begründungen, dass der Aufwand der Internetsperre zwar grundsätzlich zumutbar sei. Jedoch müsse auch dem Aufwand, der mit einer steigenden Zahl von Sperren einhergeht, Rechnung getragen werden.[323]

III. Ermächtigungsgrundlage der Sperrverfügungen gegen Zugangsanbieter und ihre materiellen Voraussetzungen

1. § 18 Abs. 3 MDStV a.F. als Ermächtigungsgrundlage

Die „Düsseldorfer Sperrverfügungen“ als präventive Maßnahmen sind auf § 18 Abs. 3 MDStV a.F. gestützt worden. In der Vorschrift hieß es:

---

317 VG Düsseldorf, B. v. 19.12.2002 - 15 L 4148/02; VG Gelsenkirchen, B. v. 18.12.2002 - 1 L 2528/02; VG Köln, B. v. 7.2.2003 - 6 L 2495/02.

318 VG Arnsberg, B. v. 6.12.2002 - 13 L 1848/02; VG Aachen, B. v. 5.2.2003 - 8 L 1284/02.

319 VG Minden, B. v. 31.10.2002 - 11 L 1110/02; *Billmeier*, 32 ff.

320 OVG NRW, B. v. 19.3.2003 - 8 B 2567/02; *Dietlein/Heinemann*, in: Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2003, 395 (396).

321 OVG NRW, B. v. 25.3.2003 - 8 B 218/03; B. v. 25.3.2003 - 8 B 513/03; B. v. 26.3.2003 - 8 B 82/03.

322 Vgl. z.B. VG Arnsberg, U. v. 26.11.2004 - 13 K 3173/02; VG Köln, U. v. 3.3.2005 - 6 K 7151/02; VG Köln, U. v. 3.3.2005 - 6 K 7603/02; VG Düsseldorf, U. v. 10.5.2005 - 27 K 5968/02; VG Gelsenkirchen, U. v. 28.7.2006 - 15 K 2170/03.

323 VG Köln, U. v. 3.3.2005 - 6 K 7151/02, Rn. 25.

„Erweisen sich Maßnahmen gegenüber dem Verantwortlichen […] als nicht durchführbar oder nicht erfolgversprechend, können Maßnahmen zur Sperrung von Angeboten nach Absatz 2 auch gegen den Anbieter von fremden Inhalten […] gerichtet werden, sofern der Anbieter unter Wahrung des Fernmeldegeheimnisses gemäß § 85 des Telekommunikationsgesetzes von den Inhalten Kenntnis erlangt und eine Sperrung technisch möglich und zumutbar ist."

Da solche Sperrverfügungen die Freiheit der Kommunikation gemäß Art. 5 Abs. 1 GG einschränken, muss die Rechtsgrundlage die Anforderungen von Art. 5 Abs. 2 GG erfüllen. Gemäß Art. 5 Abs. 2 GG findet die Freiheit der Kommunikation ihre Schranken, soweit allgemeine Gesetze und gesetzliche Bestimmungen zum Schutze der Jugend und zum Recht der persönlichen Ehre dies vorsehen. Das heißt, § 8 MDStV a.F. und § 7 Abs. 1 MDStV a.F. – in diesen Normen war geregelt, welche Inhalte unzulässig waren[324] und deren Durchsetzung § 18 MDStV a.F. diente – müssen entweder zu den allgemeinen Gesetzen, den Gesetzen zum Schutz der Jugend oder den Gesetzen zum Schutz der persönlichen Ehre zählen. Nur dann kann die Aufsichtsbehörde die Sperrung gegen den Adressaten anordnen. Art. 5 Abs. 2 GG beinhaltet insofern einen qualifizierten Gesetzesvorbehalt.

Zum Begriff der „allgemeinen Gesetze" werden zwei Theorien vertreten. Nach der Sonderrechtlehre ist ein Gesetz allgemein, wenn es eine bestimmte Meinung nicht als solche verbietet, sondern dem Schutz eines Rechtsguts schlechthin und ohne Rücksicht auf eine bestimmte Meinung dient."[325] Dagegen ist ein Gesetz aus Sicht

---

324 § 7 Abs. 1 MDStV a.F.: Für die Angebote gilt die verfassungsmäßige Ordnung. Die Vorschriften der allgemeinen Gesetze und die gesetzlichen Bestimmungen zum Schutz der persönlichen Ehre sind einzuhalten.
§ 8 Abs. 1 MDStV a.F.: Angebote sind unzulässig, wenn sie 1. zum Haß gegen Teile der Bevölkerung oder gegen eine nationale, rassische, religiöse oder durch ihr Volkstumbestimmte Gruppe aufstacheln, zu Gewalt- oder Willkürmaßnahmen gegen sie auffordern oder die Menschenwürde anderer dadurch angreifen, daß Teile der Bevölkerung oder eine vorbezeichnete Gruppe beschimpft, böswillig verächtlich gemacht oder verleumdet werden (§ 130 StGB), 2. grausame oder sonst unmenschliche Gewalttätigkeiten gegen Menschen in einer Art schildern, die eine Verherrlichung oder Verharmlosung solcher Gewalttätigkeiten ausdrückt oder die das Grausame oder Unmenschliche des Vorgangs in einer die Menschenwürde verletzenden Weise darstellt (§ 131 StOB), 3. den Krieg verherrlichen, 4. pornographisch sind (§ 184 StGB), 5. offensichtlich geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefährden, 6. Menschen, die sterben oder schweren körperlichen oder seelischen Leiden ausgesetzt sind oder waren, in einer die Menschenwürde verletzenden Weise darstellen und ein tatsächliches Geschehen wiedergeben, ohne daß ein überwiegendes berechtigtes Interesse gerade an dieser Form der Berichterstattung vorliegt; eine Einwilligung ist unbeachtlich.

325 *Häntzschel*, in: Anschütz/Thoma, Handbuch des Deutschen Staatsrechts II, 651 (659 f.); *Rothenbücher*, in: VVDStRL (4), 6 (20); *Dreier*, in: Dreier, GG, § 5 I, II, Rn. 139; *Sachs*, in: Staatsrecht IV, 1445; *Grabenwarter*, in: Maunz/Dürig, GG, Art. 5 Abs. 2, Rn. 122.

der Abwägungslehre dann allgemein, „wenn es deshalb Vorrang [...] hat, weil das von ihm geschützte gesellschaftliche Gut wichtiger ist als die Meinungsfreiheit.“[326] Das BVerfG hat beide Lehren im Lüth-Urteil in der Kombinationslehre zusammengeführt, sodass solche Gesetze allgemein sind, „die eine Meinung nicht als solche verbieten und die dem Schutz eines Gemeinschaftswertes dienen, der gegenüber der Betätigung der Meinungsfreiheit den Vorrang hat.“[327] Da der Schutz der Jugend und der persönliche Ehre eine besondere Bedeutung hinsichtlich des Schutzes der Meinungsäußerung haben, sind solche Gesetze neben allgemeinen Gesetzen gesondert erwähnt.[328] Weil §§ 7 Abs. 1 und 8 MDStV a.F. nicht gegen bestimmte Meinungen gerichtet sind und sie unterschiedliche höherrangige Rechtsgüter, inklusive jene Rechtsgüter der Jugend und persönlichen Ehre schützen, sind sie allgemeine Gesetze im Sinne vom Art. 5 Abs. 2 GG.[329]

2. Anwendung der Ermächtigungsgrundlage

Relativ unproblematisch war im Düsseldorfer Fall die Feststellung, dass die beiden Internetseiten rechtsextremistisches Gedankengut beinhalteten und somit gegen Bestimmungen des StGB verstießen (Kriegsverherrlichung und öffentliche Gefährdung von Kindern und Jugendlichen, § 8 Abs. 1 Ziff. 1 und 2 MdStV a.F.).[330] Diese Anforderung reicht aus, damit medienrechtliche Maßnahmen ergriffen werden. Wesentlich wichtiger für diese Arbeit ist die Frage, gegen wen und mit welchen Mitteln die „Düsseldorfer Sperrverfügungen“ getroffen wurden.

---

326 *Smend*, in: VVDStRL (4), 44 (52); *Schulze-Fielitz*, in: Dreier, GG, § 5 I, II, Rn. 140; *Sachs*, in: Staatsrecht IV, 1445; *Grabenwarter*, in: Maunz/Dürig, GG, Art. 5 Abs. 2, Rn. 122.

327 BVerfGE 7, 198 (209 f.); ferner BVerfGE 62, 230 (243 f.); 71, 162 (175); 85 248 (263); 93, 266 (291); 97, 125 (146); 102, 347 (360); 111, 147 (155); 120, 180 (200); 124, 300 (322 f.); 177, 244 (260); 113, 63 (79); siehe auch *Schulze-Fielitz*, in: Dreier, GG, § 5 I, II, Rn. 142; *Sachs*, in: Staatsrecht IV, 1446 f.; *Grabenwarter*, in: Maunz/Dürig, GG, Art. 5 Abs. 2, Rn. 122.

328 *Schulze-Fielitz*, in: Dreier, GG, § 5 I, II, Rn. 147 ff.; *Sachs*, in: Staatsrecht IV, 1453 ff.; *Grabenwarter*, in: Maunz/Dürig, GG, Art. 5 Abs. 2, Rn.190 ff.; 195ff.

329 Die gleiche Meinung zu den § 12 MDStV i.V.m. § 4 JMStV vertritt *Dietlein/Heinemann*, in: Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2003, 395 (411); zur Verfassungsmäßigkeit von § 18 MDStV, siehe *Stadler*, MMR 2002, 343 (343 f.).

330 Sperrverfügung vom 6.2.2002, abrufbar unter <http://odem.org/material/verfuegung/> [Stand: 7.8.2019], 5 ff.

a) Adressat der Ermächtigungsgrundlage

§ 18 Abs. 2 MdStV a.F. ermöglicht Maßnahmen gegen den Anbieter von *eigenen* Inhalten. Es werden auch Maßnahmen gegen Anbieter von *fremden* Inhalten ermöglicht. Diese sind gemäß § 18 Abs. 3 MdStV a.F. subsidiär heranzuziehen.[331] Es wird unterschieden zwischen drei Arten von Anbietern. Anbieter gemäß § 3 bzw. § 5 MdStV a.F. bestehen aus dem Rechtssubjekt, das eigene Inhalte bereitstellt (Content-Provider), und dem Rechtssubjekt, das fremde Inhalte bereitstellt (Host-Provider) und schließlich dem Rechtssubjekt, das lediglich den *Zugang* vermittelt (Access-Provider). Vom Wortlaut her können bei der Anwendung des § 18 Abs. 2 MdStV a.F. sämtliche Anbieter herangezogen sein. Allerdings ist davon auszugehen, dass im telelogischen Sinne bei der behördlichen Aufsicht zwischen inhaltsbezogenen Anbietern und technisch neutralen Anbietern zu unterscheiden ist. In beiden Absätzen (§§ 18 Abs. 2 und Abs. 3 MdStV a.F.) kann somit dem Content-Provider und Host-Provider sowohl Untersagung als auch Sperrung, im Vergleich dazu dem technisch neutralen Access-Provider allerdings nur Sperrung, angeordnet werden.[332] Nach *Koreng* gibt es beim Content- und Host-Provider keinen Unterschied zwischen Untersagung und Sperrung.[333] Für Access-Provider gilt nur die Sperrung, die zur Erschwerung der Kenntnisnahme der Online-Inhalte führen kann. Access-Provider ist somit lediglich möglicher Adressat einer Maßnahme nach § 18 Abs. 3 MdStV a.F.

b) Verhältnismäßigkeit der Sperrverfügungen

Eine weitere Frage ist, ob die Sperrverfügungen gegen das Verhältnismäßigkeitsgebot verstoßen. Der Grundsatz der Verhältnismäßigkeit wird aus dem Rechtsstaatsprinzip gemäß Art. 20 Abs. 3 GG hergeleitet.[334] Soweit der hoheitliche Eingriff in Grundrechte über eine Rechtsgrundlage gerechtfertigt ist, muss das Gesetz und die auf das Gesetz gestützte hoheitliche Maßnahme verhältnismäßig sein. Verhältnismäßigkeit liegt dann vor, wenn ein legitimer Zweck verfolgt wird und die Maßnahme geeignet, erforderlich sowie angemessen ist.[335]

---

331 Zwischen Untersagung und Sperrung gibt es keinen Unterschied beim Content-Anbieter, dazu *Koreng*, 159 ff.

332 Zur Diskussion über § 59 Abs. 3 und 4 RStV siehe *Koreng*, 156 f.

333 *Koreng*, 159 ff.

334 *Grzeszick*, in: Maunz/Dürig, GG, Art. 20, Rn. 107; *Sachs*, in: Sachs, GG, Art. 20 Rn. 146 f.; *Schulze-Fielitz*, in: Dreier, GG, Art. 20 Rn. 180.

335 *Grzeszick*, in: Maunz/Dürig, GG, Art. 20, Rn. 110 ff. *Schulze-Fielitz*, in: Dreier, GG, Art. 20 Rn. 180 ff.; BVerfGE 65, 1 (54); 67, 157 (173); 70, 278 (286); 92, 262 (273).

Bei der Prüfung der Verhältnismäßigkeit von Sperrverfügungen müsste zunächst der mit ihnen verfolgte Zweck legitim sein. Durch Sperren des Online-Zugangs zu den rechtsradikalen und jugendgefährdenden Inhalten können sowohl der Jugendschutz als auch die öffentliche Sicherheit, die freiheitliche demokratische Grundordnung sowie der öffentliche Friede gewährleistet werden.[336] Der hier verfolgte Zweck ist somit legitim. Die Geeignetheit der Sperrmaßnahmen kann auch angenommen werden, weil „eine vollständige Ausschaltung der Gefahr durch Sperren ohnehin praktisch unmöglich" sei.[337] Es reicht aus, wenn die Maßnahme eine zeitliche und technische Erschwerung des Zugangs für durchschnittliche Nutzer bedeutet.[338] In Betracht kommen auch keine anderen milderen Mittel, da etwa die vorgeschlagene Installation von Filtersoftware stark von Content-Providern sowie Nutzern abhängt und daher das angestrebte Ziel nicht erreichen kann.[339] In der Begründung zu den „Düsseldorfer Sperrverfügungen" erläutert die Behörde, dass es unmöglich sei, gegen Content-Provider sowie Host-Provider im Ausland vorzugehen.[340] Dabei liegt der entscheidende Grund im höheren Schutzniveau von Meinungsäußerungen in den USA. Angemessen ist die Maßnahme aus Sicht des Gerichts, weil die nachteiligen Folgen, die der Eingriff in die betroffenen Grundrechte, insbesondere die Berufsausübungsfreiheit (Art. 12 Abs. 1 GG) oder die Eigentumsfreiheit (Art. 14 Abs. 1 S. 1 GG), nach sich zieht, nicht außer Verhältnis zum durch § 130 Abs. 1 und 2 StGB geschützten öffentlichen Interesse stehen.[341]

---

336 *Billmeier*, 245; *Dietlein/Heinemann*, in: Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2003, 395 (413); *Spindler/Volkmann*, K&R 2002, 398 (405); *Zimmermann*, NJW 1999, 3145 (3150).

337 OVG NRW, B. v. 19.3.2003 - 8 B 2567/02, Rn. 90; ferner VG Köln, U. v. 3.3.2005 - 6 K 7151/02, Rn. 112 ff.

338 OVG NRW, B. v. 19.3.2003 - 8 B 2567/02, Rn. 90; *Billmeier*, 246 ff.; *Dietlein/Heinemann*, in: Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2003, 395 (413); *Spindler/Volkmann*, K&R 2002, 398 (405 f.); *Zimmermann*, NJW 1999, 3145 (3150).

339 OVG NRW, B. v. 19.3.2003 - 8 B 2567/02, Rn. 93.; *Billmeier*, 252 ff.; *Dietlein/Heinemann*, in: Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2003, 395 (414); *Spindler/Volkmann*, K&R 2002, 398 (406); *Zimmermann*, NJW 1999, 3145 (3150).

340 Sperrverfügung vom 6.2.2002, abrufbar unter <http://odem.org/material/verfuegung/> [Stand: 7.8.2019], 6 ff.

341 OVG NRW, B. v. 19.3.2003 - 8 B 2567/02, Rn. 94 ff.; *Billmeier*, 254 ff.; Dietlein/Heinemann, in: Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2003, 395 (414); *Spindler/Volkmann*, K&R 2002, 398 (407 f.); *Zimmermann*, NJW 1999, 3145 (3150 f.).

IV. Zusammenfassung und Bewertung

Die von der „Düsseldorfer Sperrverfügungen“ hervorgerufenen Reaktionen veranlassten nicht nur Gerichtsverfahren und Diskussionen in der juristischen Fachliteratur, sondern sie beeinflussten auch weitgehend die zukünftigen Entwicklungen in diesem Rechtsgebiet. Der Beschluss des OVG NRW und das Urteil des VG Köln waren grundlegend für die Anwendung von Sperrverfügungen. Bei ihnen lag das Schwergewicht auf der Frage nach der Ermächtigungsgrundlage der Sperrverfügungen, dem Adressaten der Verfügung und der Verhältnismäßigkeit der Sperrverfügungen. Die „Düsseldorfer Sperrverfügungen“ wurden die auf richtige Ermächtigungsgrundlage – § 18 Abs. 3 MDStV a.F. – gestützt. Aus der Struktur des § 18 Abs. 2 und 3 MdStV a.F. ergibt sich die Folgerung, dass Access-Provider lediglich Adressaten des § 18 Abs. 3 MdStV a.F. sind. OVG NRW und VG Köln nahmen die Verhältnismäßigkeit der Sperrverfügungen an, da sie legitime Zwecke verfolgen und geeignet, erforderlich sowie angemessen sind. Dennoch ist die rechtliche Natur des Access-Providers als TK-Diensteanbieter und folglich deren durch Art. 10 Abs. 1 GG geschützten TK-Geheimnisse hierbei noch nicht in Betracht gezogen worden.[342] Die Beachtung des TK-Geheimnisses ist in späteren Entscheidungen ein wesentlicher Streitpunkt beim Thema der Internetsperrverfügungen.

C. Zugangserschwerungsgesetz gegen Kinderpornografie

I. Vorgeschichte

In der deutschen Geschichte der Internetsperren gegen Kinderpornographie fing es mit dem Compuserve-Urteil aus dem Jahre 1998 an. Nach der Ansicht des AG München war der Geschäftsführer einer deutschen Tochtergesellschaft für das Handeln ihrer amerikanischen Muttergesellschaft verantwortlich, weil über die von Compuserve betriebenen Netzknoten auf jugendgefährdende Inhalte in

342 *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (2); *Billmeier*, 273 ff.; *Dietlein/Heinemann*, in: Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2003, 395 (401); *Spindler/Volkmann*, K&R 2002, 398 (399).

Deutschland zugegriffen werden konnte.[343] Folglich nahm das Gericht eine Straftat der Geschäftsführer der deutschen Tochtergesellschaft durch Unterlassung an. Das Urteil wurde vom LG München ein Jahr später, 1999, aufgehoben.[344]

Um sich zum Unterbinden der Verbreitung von Kinderpornografie eine klare gesetzliche Grundlage zu verschaffen, wurde 2010 das Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen (ZugErschwG) erlassen.[345] Mit dem ZugErschwG sollte der Abruf von kinderpornographischen Inhalten in Kommunikationsnetzen durch Internetsperren erschwert werden.[346] Allerdings kam das Gesetz nicht zur Anwendung,[347] da es in der Öffentlichkeit als Zensurgesetz wahrgenommen wurde.[348] Es wurde im Dezember 2011 durch Aufhebungsgesetz aufgehoben.[349]

Dennoch lohnt es, sich mit diesem Gesetz zu befassen, da es die Entwicklung von Internetsperren in Deutschland geprägt hat.

II. Inhalte des Zugangserschwerungsgesetzes

§§ 1 und 2 ZugErschwG waren die Kernparagraphen dieses Gesetzes, weil sie die Ermächtigungsgrundlage für das Erstellen einer Sperrliste durch das BKA, das Prinzip vom Vorrang der Löschung vor der Sperrung, die Benachrichtigungspflicht vom BKA und die Sperrpflicht für große Zugangsdienstanbieter regelten.

1. Sperrliste

§ 1 Abs. 1 ZugErschwG ermächtigte zunächst das BKA, eine täglich zu aktualisierende Sperrliste über Domainnamen, IP-Adressen und Zieladressen der Internetseiten zu erstellen, über die kinderpornographische Inhalte nach § 184b StGB

---

343 AG München, U. v. 28.5.1998 - 8340 Ds 465 Js 173158/95; zum Überblick über das Compuserve-Urteil siehe *Sieber*, JZ 1996, 429 (429); *Grewlich*, 39.

344 LG München I, U. v. 17.11.1999 - 20 Ns 465 Js 173158/95.

345 BGBl. I 2010, 78; zum Überblick über das ZugErschwG siehe *Marberth-Kubicki*, NJW 2009, 1792 (1792 ff.).

346 Dazu *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (3 f.); *Frey/Rudolph*, CR 2009, 644 (644 ff.); *Sieber*, JZ 2009, 653 (653 f.); *Koreng*, 120; *Schnabel*, JZ 2009 996 (996 ff.); *Gercke*, ZUM 2011, 609 (609 ff.); *Heliosch*, 250 ff.

347 BVerfG, B. v. 29.3.2011 - 1 BvR 508/11.

348 *Marberth-Kubicki*, NJW 2009, 1792 (1795); *Volkmann*, in: Recht der elektronischen Medien, § 59, Rn. 3; *Schnabel*, JZ 2009, 996 (996); *Frey/Rudolph*, CR 2009, 644 (644); *Sieber*, JZ 2009 653 (653); *Stadler*, MMR 2009, 581; Aufhebungsgesetz zum ZugErschwG, BT-Drucks, 17/646, 4.

349 BGBl. I 2011, 2958.

abgerufen werden konnten.[350] Gemäß § 1 Abs. 2 S. 2 ZugErschwG galt die Aufnahme der Internetseite in die Sperrliste im Vergleich zur Löschung aber nur als ultima ratio.[351] Um gerichtlichen Rechtsschutz des Content- sowie Hostanbieters zu gewährleisten, sollten sie vom BKA über die Aufnahme der Internetseite in die Sperrliste benachrichtigt werden (§ 1 Abs. 3 ZugErschwG).

2. Zugangserschwerung

Gemäß § 2 Abs. 1 ZugErschwG wurden Zugangsdiensteanbieter verpflichtet, die für mindestens 10.000 Teilnehmer oder Nutzungsberechtigte den Internetzugang vermitteln, aufgrund der Sperrliste unverzüglich „geeignete und zumutbare technische Maßnahmen“ zu ergreifen. Die Vorschrift lautete:

„Diensteanbieter nach § 8 des Telemediengesetzes, die den Zugang zur Nutzung von Informationen über ein Kommunikationsnetz für mindestens 10.000 Teilnehmer oder sonstige Nutzungsberechtigte ermöglichen, haben geeignete und zumutbare technische Maßnahmen zu ergreifen, um den Zugang zu Telemedienangeboten, die in der Sperrliste aufgeführt sind, zu erschweren.“

Welche Maßnahmen hierfür in Betracht kamen, war in § 2 Abs. 2 ZugErschwG geregelt. Hierzu zählen die DNS-Sperre und die Blockade von IP-Adressen und Sperrungen mithilfe eines Proxy-Servers. Nutzer wurden gemäß § 4 ZugErschwG danach auf eine Stoppmeldung umgeleitet und über die Gründe der Sperrung informiert. Internetzugangsanbieter waren im Rahmen der Umsetzung dieses Gesetzes von zivilrechtlicher Haft befreit (§ 7 Abs. 2 ZugErschwG). § 11Abs. 1 ZugErschwG regelte schließlich die Einschränkung vom Grundrecht des Fernmeldegeheimnisses.

---

350 Begr. ZugErschwG, BT-Drucks, 16/13411, 14.

351 Begr. ZugErschwG, BT-Drucks, 16/13411, 17; *Frey/Rudolph*, CR 2009, 644 (648); *Schnabel*, JZ 2009 996 (1001).

III. Kritik zum ZugErschwG aus Sicht des Bestimmtheitsgebots und der Verhältnismäßigkeit

Das ZugErschwG stieß vor und nach der Aufhebung auf Kritik. Umstritten war vor allem, ob es bei Auswahl der Sperrtechnik an dem Bestimmtheitsgebot mangelte. Verbreitet war auch der Vorwurf, dass das Gesetz relativ leicht umgangen werden konnte und dass es auch negative Nebeneffekte hatte.[352]

1. Vereinbarkeit mit dem Bestimmtheitsgebot

Das aus dem Rechtsstaatsprinzip gemäß Art. 20 Abs. 3 GG hergeleitete Bestimmtheitsgebot dient der Voraussehbarkeit für Bürger, klaren Handlungsmaßstäben für die Verwaltung und klaren Kontrollmaßstäben für Gerichte.[353] Dennoch schließt das Bestimmtheitsgebot für den Gesetzgeber die Verwendung von unbestimmten Rechtsbegriffen nicht aus. In Bereichen, die ständigen Entwicklungen unterliegen, kann die Verwendung unbestimmter Rechtsbegriffe sogar notwendig sein.[354] Gleichzeitig darf aber die Vorhersehbarkeit und Justitiabilität von Maßnahmen der Verwaltung nicht dadurch gefährdet werden.[355] Das Gesetz schrieb „geeignete und zumutbare technische Maßnahmen" (§ 2 Abs. 1 S. 1 ZugErschwG) vor und empfahl dem Zugangsanbieter eine DNS-Sperre. Im Grund war es ihm frei überlassen, welche Sperrtechnik er verwendet. Angesichts der Komplexität der Technikentwicklung konnte der Gesetzgeber nicht alles punktgenau vorschreiben. Das Fortschreiten der Technik zwingt ihn dazu, einen gewissen Freiraum für neue Entwicklungen zu lassen. Der demokratisch legitimierte Gesetzgeber muss deshalb nicht bis ins kleinste Detail vorgeben, in welchen Fällen mit welchem Mittel die Sperrung zu erfolgen hat.[356] Er muss nur den Mindestvorgaben des Grundsatzes des Bestimmtheitsgebots folgen. Im vorliegenden Fall ist ein Verstoß gegen das Bestimmtheitsgebot somit nicht gegeben.

---

352 *Sieber*, JZ 2009, 653 (658); *Schnabel*, JZ 2009, 996 (998); *Schöttle*, K&R 2007, 366; *Frey/Rudolph*, CR 2009, 644 (647); *Billmeier*, 138.

353 BVerfGE 31, 255 (264); 79, 106 (120); 83, 130 (145); 110, 33 (53); *Grzeszick*, in: Maunz/Dürig, GG, Art. 20, Rn. 58; *Sachs*, in: Sachs, GG, Art. 20 Rn. 126 f.

354 BVerfGE 80, 103 (108); 87, 234 (263 f.); 102, 254 (337); 103, 21 (33).; *Billmeier*, 130; *Grzeszick*, in: Maunz/Dürig, GG, Art. 20, Rn. 61.

355 BVerfGE 21, 73 (79 f.); *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (15).

356 VG Köln, U. v. 3.3.2005 - 6 K 7151/02, Rn. 100; Kritik dazu siehe *Frey/Rudolph*, CR 2009, 644 (647 ff.); *Heliosch*, 297; *Schnabel*, JZ 2009, 994 (998); *Sieber/Nolde*, 173; *Billmeier*, 138.

2. Verhältnismäßigkeit

Darüber hinaus wurde die Verhältnismäßigkeit der Sperrung im Hinblick auf die Umgehungsmöglichkeiten kritisch ins Feld geführt. Durch das ZugErschwG wurde eine Erschwerung des Abrufs auf Kinderpornographie geschaffen und dadurch das Interesse der Opfer geschützt.[357] Das Gesetz verfolgte somit einen legitimen Zweck. Die Sperrverfügungen mittels drei Sperrtechniken waren auch geeignet, weil sie trotz leichter Umgehungsmöglichkeiten die meisten betreffenden Internetnutzer daran hinderten, auf Kinderpornographie im Netz zuzugreifen.[358] Des Weiteren waren sie auch erforderlich, da andere mildere und gleich effektive Maßnahmen nicht ersichtlich waren. Hinsichtlich anderer Alternativen, wie das Löschen illegaler Inhalte, gilt das Sperren durch den Zugangsanbieter zwar als das letzte bzw. als das schärfste Mittel. Primär sollen nämlich Maßnahmen gegen den Anbieter der kinderpornographischen Inhalte durchgeführt werden, wenn sich feststellen lässt, wer der Anbieter ist.[359] Dies war allerdings bereits vom ZugErschwG berücksichtigt worden war (§ 1 Abs. 2 Satz 1 ZugErschwG). Erst wenn das Löschen gegen Rechtsverletzer oder Host-Provider nicht oder nicht in angemessener Zeit erfolgsversprechend ist, kann eine Sperrverfügung angeordnet werden. Bei der Prüfung der Angemessenheit mussten die Nebeneffekte – insbesondere ging es hierbei um das Phänomen des Overblocking – berücksichtigt werden. Bei der DNS-Sperre hatten zwar einige unter Subdomains gespeicherte Online-Angebote unter der Sperrung der Hauptdomain Schaden genommen, jedoch haben solche Sperren große Auswirkungen für die Verhinderung des Kontakts mit den kinderpornographischen Inhalten. Dieser positive Aspekt, das Interesse am Kindeswohl, überwiegt die negativen Folgen einer Sperre.[360] Die Verhältnismäßigkeit der Sperren ist somit nicht zu beanstanden.

IV. Zitiergebot aufgrund der Einschränkung des TK-Geheimnisses

Wie oben bei der Bewertung der „Düsseldorfer Sperrverfügungen“ bereits gezeigt, wurde das durch Art. 10 Abs. 1 GG geschützte TK-Geheimnis damals noch nicht

---

357 *Sieber*, JZ 2009, 653 (655); *Heliosch*, 68; *Schnabel*, JZ 2009, 996 (1000).

358 *Schnabel*, JZ 2009, 996 (1000); *Schöttle*, K&R 2007, 366; *Heliosch*, 82 ff.;

359 BT-Drucks, 16/13411, 13; *Heliosch*, 105 ff.; *Sieber*, JZ 2009 653 (661); *Schnabel*, JZ 2009, 996 (1000 f.); *Frey/Rudolph*, CR 2009, 644 (647 f.).

360 *Sieber/Nolde*, 186; *Frey/Rudolph*, CR 2009, 644 (647); *Degen*, 158; *Stadler*, Rn. 128; *Heliosch*, 135 ff., 144 ff.; *Sieber*, JZ 2009 653 (661); Kritik dazu siehe *Schnabel*, JZ 2009, 996 (1001).

berücksichtigt. § 11 ZugErschwG sah hingegen ausdrücklich vor, dass durch §§ 2 und 4 das „Grundrecht des Fernmeldegeheimnisses (Art. 10 GG) eingeschränkt“ wurde und „hierdurch Telekommunikationsvorgänge im Sinne des § 88 Abs. 3 TKG betroffen“ waren, sodass dem Zitiergebot aus Art. 19 Abs. 1 S. 2 GG Rechnung getragen wurde. Unter dem Zitiergebot versteht man, dass ein Gesetz durch es eingeschränkte Grundrechte unter Angabe des Artikels nennen muss.[361] Es hat eine Warn- und Besinnungsfunktion für die Gesetzgebung und eine Klarstellungsfunktion für die Gesetzesauslegung und -anwendung.[362] Um das Grundrecht des Telekommunikationsgeheimnisses besonders zu schützen, ist das sog. „kleine Zitiergebot“ aus § 88 Abs. 3 S. 3 TKG auch zu befolgen. Dies gilt dann, wenn TK-Diensteanbieter über den Zweck der Erbringung ihrer Dienste oder Schutz der technischen Systeme hinaus zusätzliche Kenntnisse über Kommunikationsinhalte und deren nähere Umstände speichern. Für andere Zwecke bedarf es einer gesetzlichen Vorschrift, die sich ausdrücklich auf Telekommunikationsvorgänge bezieht. Ungeachtet dessen, dass die gemäß §§ 2 und 4 ZugErschwG erlassenen Sperrverfügungen dem Zweck der geschäftsmäßigen Tätigkeit oder dem Schutz der technischen Systeme dienen müssen, wurde das Zitiergebot gemäß Art. 19 Abs. 1 S. 2 GG und das „kleine Zitiergebot“ aus § 88 Abs. 3 S. 3 TKG beachtet.

D. Blockade illegaler Glücksspiele im Internet

I. Maßnahme gegen Glücksspielanbieter

Ermächtigungsgrundlage für Sperrverfügungen gegen Online-Glücksspielanbieter ist § 9 Abs. 1 S. 3 Nr. 3 des Staatsvertrags zum Glücksspielwesen in Deutschland (GlüStV)[363], mit denen der Abruf von Angeboten von Glücksspielen sowie ihrer Werbung von Nutzern untersagt wird. Soweit sich die Maßnahmen einer zustän-

---

361 *Remmert*, in: Maunz/Dürig, GG, Art. 19 I Rn. 43; *Krebs*, in: v. Münch/Kunig, GG, Art. 19 Rn. 14; *Huber*, in: v. Mangoldt/Klein/Starck, GG, Art. 19 Abs. 1 Rn. 99.

362 *Axer*, in: HGR, Bd. III, § 67 Rn. 9 f.; *Hesse*, 148; *Sachs*, in: Sachs, GG, Art. 19 Rn. 25 ff.; *Dreier*, in: Dreier, GG, Art. 19 I Rn. 19; *Remmert*, in: Maunz/Dürig, GG, Art. 19 I Rn. 40 f.

363 Staatsvertrag zum Glücksspielwesen in Deutschland (Glücksspielstaatsvertrag – GlüStV) vom 15. Dezember 2011 (GVBl. 2012 S. 318, 319, 392, BayRS 02-30-I).

digen Behörde räumlich auf das Bundesgebiet beschränken, fehlt es der handelnden Behörde nicht an der Verbandskompetenz.[364] Auch gegenüber einer im Ausland ansässigen Firma kann eine deutsche Behörde eine Verfügung zur Schließung des Angebots anordnen, wenn die betroffenen Angebote sowie ihr Kundenservice in deutscher Sprache zur Verfügung gestellt wurden. Dies ergibt sich daraus, dass das Wirkungsprinzip aus dem Kartell- und Wettbewerbsrecht hier ebenfalls gelten muss.[365]

1. Lokalisierung der Anbieter als Problem

Die Schließungsanordnungen gegen Glücksspielanbieter kann mittels Lokalisierungstechnik erfolgen, was in der Praxis zur geographischen Bestimmung der Geräte sowie Nutzer angewandt wird. In der Welt des Internet wird jedem Rechner eine eindeutige IP-Adresse von einem hierarchisch organisierten Netzwerk gegeben. Anhand dieser IP-Adresse lassen sich die Geolokation eines Geräts sowie eines Nutzers identifizieren.[366] Solche Sperrmaßnahmen, die von der Geolokalisationstechnologie abhängig sind, könnten allerdings unverhältnismäßig sein, wenn man insbesondere die Zuverlässigkeit der Technik berücksichtigt.

2. Zuverlässigkeit der Lokalisierungstechnik

Das VG Düsseldorf hat die Funktion der Geolokation als zulässig erachtet. Die Sperrverfügungen gegen Glücksspielanbieter sind geeignet, das Zugreifen auf solche Angebote zu untersagen.[367] Alternative Maßnahmen wie z.B. das Einrichten eines Disclaimers, sind im Vergleich zu Geolokationsverfahren kein milderes Mittel.[368] Letztlich ist die tatsächliche Zuverlässigkeit der Geolokation für die Beurteilung der Angemessenheit der Verfügung entscheidend. Aus der Sicht des VG Düsseldorf sind Geolokation und Handy- bzw. Festnetzortung hinreichend zuver-

---

364 VG Düsseldorf, B. v. 18.5.2009 - 27 L 40/09, Rn. 39; BayVGH, B. v. 20.11.2008 - 10 CS 08.2399 -, ZfWG 2008, 455; BVerwG, U. v, 30.1.2002 - 9 A 20/01 -, NVwZ 2002, 984.

365 VG Düsseldorf, B. v. 18.5.2009 - 27 L 40/09, Rn. 39; *Ohler*, 327.

366 Zur technischen Grundlage der Geolokalisation, siehe *Hoeren*, ZfWG 2008, 229 (229 ff.); *Hoeren*, MMR 2007, 3 (4 f.).

367 VG Düsseldorf, B. v. 18.5.2009 - 27 L 40/09, Rn. 88 f.; OVG NRW, B. v. 22.2.2008 - 13 B 1215/07, ZfWG 2008, 122; OVG Berlin-Brandenburg, B. v. 16.3.2009 - 1 S 224.08; *Hoeren*, MMR 2007, 3 (6).

368 VG Düsseldorf, B. v. 18.5.2009 - 27 L 40/09, Rn. 99; BGH, U. v. 30.3.2006 - I ZR 24/03 -, BGHZ 167, 91.

lässig und daher angesichts der Verhältnismäßigkeitsprüfung nicht zu beanstanden.[369] Ganz anders stellte das OVG Lüneburg im Jahr 2009 fest, dass die oben genannte Technik bis heute noch nicht ausreichend zuverlässig ist, eine Sperre ausschließlich in einem Bundesland zu erteilen.[370] Wenn sie aber im ganzen Bundesgebiet Anwendung findet, fehlt es der zuständigen Landesbehörde an der entsprechenden Kompetenz.[371]

Aus der Rechtsprechung des VG Düsseldorf und des OVG Lüneburg kann man schließen, dass der Kernpunkt bei der Beurteilung der Verhältnismäßigkeit der hier getroffenen Sperrverfügungen die Zuverlässigkeit und Genauigkeit der Geolokationstechnik ist. Dabei ist der technische Vorgang, in dem auf den geographischen Ursprung eines Nutzers mittels realer IP-Adresse rückgeschlossen werden kann, entscheidend. Wie bei der Funktionsweise des Sperrmechanismus auf Umgehungsmöglichkeiten hingewiesen wurde (Kap. 1. D.), gibt es auch hier Möglichkeiten, der Geolokation zu entgehen. Eine Ortung ist nicht möglich, wenn Nutzer mit Proxy-Servern ihre reale IP-Adresse verschleiern.[372] Allerdings wird die Zuverlässigkeit und Genauigkeit der Geolokation mit dem technischen Fortschritt steigen und der Aufwand dafür wird auch immer vertretbarer.

3. Zwischenergebnis

Zusammenfassend liegt bei der Beurteilung von Schließungsanordnungen gegen den Glücksspielanbieter die Schwierigkeit in der Lokalisierung des Anbieters. Ob eine Sperrverfügung ein verhältnismäßiges Mittel darstellt, hängt von der Präzision und dem Aufwand von der Lokalisierung ab.[373] Im Ergebnis sind die Maßnahmen als zulässig einzustufen.

II. Sperrungsverfügungen gegen Internetzugangsanbieter

Trotz der oben erwähnten und umstrittenen „Düsseldorfer Sperrverfügungen“ aus dem Jahre 2002 erließ die Bezirksregierung Düsseldorf im Jahr 2010 erneut

---

369 VG Düsseldorf, B. v. 18.5.2009 - 27 L 40/09, Rn. 101 ff.; *Hoeren*, ZfWG 2008, 311 (315).

370 OVG Niedersachsen, U. v. 3.4.2009 - 11 ME 399/08, Rn. 42 ff.; siehe auch VG Ansbach, B. v. 14.12.2006 – AN 4S 06.03253; VG Bayern, B. v. 7.5.2007 – 24 ZS 7.10; OVG Sachsen-Anhalt, B. v. 27.7.2005 – 1 M 321/05.

371 OVG Niedersachsen, U. v. 3.4.2009 - 11 ME 399/08, Rn. 50.

372 *Schöttle*, K&R 2007, 366 (368); zur Umgehungserkennung und -behandlung der Verschleierungsmaßnahmen, siehe *Höeren*, ZfWG 2008, 311 (312 ff.); *Hoeren*, MMR 2007, 3 (6).

373 *Hoeren*, ZfWG 2008, 311 (313 ff.); *Hoeren*, MMR 2007, 3 (6).

Sperrverfügungen gegenüber Internetzugangsanbietern mit dem Ziel, die im ausländischen Server ansässigen rechtswidrigen Online-Glücksspielangebote sperren zu lassen.[374] Für beide Sperrverfügungen diente § 9 Abs. 1 S. 3 Nr. 5 GlüStV a.F. als Ermächtigungsgrundlage. Die nun nicht mehr im Staatsvertrag enthaltene Vorschrift lautete:

„Die zuständige Behörde des jeweiligen Landes kann die erforderlichen Anordnungen im Einzelfall erlassen. Sie kann insbesondere Diensteanbietern im Sinne von § 3 Teledienstegesetz[375] [Content-, Host- und Access-Provider], soweit sie nach diesem Gesetz verantwortlich sind, die Mitwirkung am Zugang zu unerlaubten Glücksspielangeboten untersagen.“[376]

Es ist zu diskutieren, ob diese Norm verfassungsgemäß war. Hieraus lassen sich wichtige Hinweise für die Anforderungen an Maßnahmen gegen Access-Provider ziehen.

1. Verstoß gegen das Bestimmtheitsgebot?

Wie beim ZugErschwG ist anzumerken, dass auch § 9 Abs. 1 Satz. 3 Nr. 5 GlüStV a.F. es dem Diensteanbieter überlässt, sich für den Anwendungsfall sowie die Sperrmöglichkeit selber zu entscheiden. Aus diesem Grund muss der Gesetzgeber nicht bis ins kleinste Detail vorschreiben, in welchen Fällen mit welchem Mittel die Sperrung erfolgt. Zu kritisieren ist allerdings, dass § 9 Abs. 1 S. 3 Nr. 5 GlüStV a.F. nicht wie beim ZugErschwG Benachrichtigungen an Content- und Hostanbieter oder Stoppmeldungen für Nutzer vorschreibt, so dass die beiden Gruppen die hoheitlichen Maßnahmen nicht erkennen können.[377]

2. Verstoß gegen Zitiergebot?

Es ist zu prüfen, ob der Gesetzgeber dem Zitiergebot nachgekommen ist. Die Normen des GlüStV a.F. zu den möglichen Sperrmaßnahmen schränken die Grundrechte, insb. das Grundrecht des Fernmeldegeheimnisses (Art. 10 Abs. 1 GG) ein. In den Vorschriften ist auf diese Grundrechtsrelevanz nicht hingewiesen. Somit ist das Zitiergebot aus Art. 19 Abs. 1 Satz 2 GG und aus § 88 Abs. 3 Satz 3 TKG, das

---

374 *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (14).
375 Außer Kraft, nun geregelt in § 2 Abs. 1 Nr. 1 TMG.
376 GV.NRW.2007 S. 445.
377 *Frey/Rudolph*, CR 2009, 644 (647); *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (15).

sog. „kleine Zitiergebot“ nicht beachtet.[378] Folglich wäre § 9 Abs. 1 Satz. 3 Nr. 5 GlüStV a.F. wegen des Verstoßes gegen Zitiergebot verfassungswidrig. Beim ZugErschwG wurde das Zitiergebot beachtet, indem § 11 ZugErschwG erklärte, dass durch §§ 2 und 4 ZugErschwG das „Grundrecht des Fernmeldegeheimnisses (Art. 10 Abs. 1 GG) eingeschränkt“ wurde und „hierdurch Telekommunikationsvorgänge im Sinne des § 88 Abs. 3 Satz TKG betroffen“ waren. Ob die Sperrmaßnahmen tatsächlich in den Schutz des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG eingreifen, werden erst in den Entscheidungen über die Sperrung im Urheberrecht ausführlich geklärt.[379]

3. Kritik an den Tatbestandsvoraussetzungen

a) Access-Provider in der Regel nicht mitverantwortlich für Content

§ 9 Abs. 1 Satz 3 Nr. 5 GlüStV a.F. verlangt zunächst „Verantwortlichkeit“ der Internetzugangsanbieter, um die „Mitwirkung“ am Zugang zu unerlaubten Glücksspielangeboten zu untersagen. Hierzu erklärt die Begründung zum GlüStV a.F. deutlich, dass Zugangsanbieter als Beihelfer gemäß § 284 Abs. 1, § 27 StGB mitwirken können und damit nach dem Sicherheits- und Ordnungsrecht der Länder zu belangen sind.[380] Problematisch ist es, ob Access-Provider vorsätzlich den Betreibern von illegalen Online-Glücksspielangeboten Hilfe leisten. Als Hersteller der Verbindung zwischen verschiedenen Netzinfrastrukturen und Vermittler der im Netz transportierten Datenpakete erhalten sie keine Kenntnis von den Inhalten und sind daher als inhaltsneutral zu qualifizieren.[381] Ohne vertragliche oder sonstige Beziehungen zwischen Access-Provider und Content-Provider ist es nicht überzeugend, dass „Vorsätzlichkeit“ sowie „Mitwirkung“ als eine der Tatbestandvoraussetzungen des § 9 Abs. 1 S. 3 Nr. 5 GlüStV a.F. vorliegt.[382] Access-Provider können somit regelmäßig nicht Adressaten von Sperrverfügungen sein. Hierdurch wird der Schutz beschnitten.

---

378 *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (15); zum Zitiergebot *Remmert*, in: Maunz/Dürig, GG, Art. 19 I Rn. 43; *Krebs*, in: v. Münch/Kunig, GG, Art. 19 Rn. 14; *Huber*, in: v. Mangoldt/Klein/Starck, GG, Art. 19 Abs. 1 Rn. 99.

379 Siehe hierzu unten.

380 *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (16); Begr. zum GlüStV, Landtag NRW, Drs. 14/4849, 41.

381 VG Düsseldorf, B. v. 17.5.2010 - 27 L 143/10, Rn. 43; *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (16); *Büssow/v. Schmeling*, ZfWG 2010, 239 (246).

382 VG Düsseldorf, B. v. 17.5.2010 - 27 L 143/10, Rn. 43; *Schöttle*, K&R 2007, 366 (366 ff.); zur Prüfung des Online-Verbots der Veranstaltung und Vermittlung von Glücksspielen nach den europäischen Rechten, siehe *Koenig*, K&R 2007, 257 (257 ff.).

b) „Untersagung“ keine taugliche Maßnahme für Access-Provider

Probleme ergeben sich schließlich aus der Formulierung des § 9 Abs. 1 S. 3 Nr. 5 GlüStV a.F., der die Diensteanbieter im Sinne von § 3 Abs. 1 Nr. 1 TDG (jetzt: § 2 Abs. 1 Nr. 1 TMG) verpflichtet, die Mitwirkung am Zugang zu unerlaubten Glücksspielangeboten zu „untersagen“, soweit sie dafür verantwortlich sind. Gemeint ist zunächst eine Untersagung, die ausgehend von §§ 59 Abs. 3 und 4 RStV ausdrücklich von der Sperrung zu unterscheiden ist.[383] Wie oben bei der Diskussion über die Ermächtigungsgrundlage für die „Düsseldorfer Sperrverfügungen“ bereits dargestellt, lässt der Gesetzgeber hier nicht offen, ob die Sperrung von den Providern zu verwenden ist. Untersagung ist der Sperrung nicht gleichgestellt und kann ausschließlich von Content- und Hostanbieter vorgenommen werden. Der Access-Provider ist daher vor diesem Hintergrund kein tauglicher Adressat des § 9 Abs. 1 S. 3 Nr. 5 GlüStV a.F.

III. Zwischenergebnis

Um illegale Glückspiele im Internet zu bekämpfen, sind sowohl gegenüber den in Deutschland ansässigen Glücksspielanbietern als auch gegenüber den Access-Providern, sofern der Server vom Ausland gehostet ist, Sperrverfügungen anzuordnen. Im ersten Fall gegen Online-Glücksspielanbieter spielen die technischen Ansätze, also Geolokation und Handy- bzw. Festnetzortung, eine entscheidende Rolle. Uneinig waren sich die Gerichte, ob Geolokation und Handy- bzw. Festnetzortung technisch hinreichend zuverlässig sind. Angenommen wurde, dass diese Maßnahmen nicht darauf abzielen, dass sämtlichen Nutzern im Bundesgebiet das Glücksspiel versagt wird und gleichzeitig keine Nutzer aus dem Ausland betroffen werden. Zu seiner Zeit war die Technik noch nicht so sicher, dass man Sperrungen in jedem Fall zielgenau vornehmen konnte. Angesichts der gegenwärtigen Lage sowie weiterer Entwicklung der Technik wird die Zuverlässigkeit der Geolokation und Handy- bzw. Festnetzortung steigen. Damit werden Maßnahmen gegen die Anbieter von Glückspielen eher durchzusetzen sein. Im zweiten diskutierten Fall ging es um § 9 Abs. 1 Satz 3 Nr. 5 GlüStV a.F. als Ermächtigungsgrundlage für Sperrungsverfügungen gegen Access-Provider. Nach der Überprüfung ist diese

---

383 *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (15); *Sieber/Nolde*, 23, 147; *Frey/Rudolph*, Haftungsregime für Host- und Access-Provider, 2009, Rn. 212 ff.

Ermächtigungsgrundlage zwar hinsichtlich Bestimmtheits- und Zitiergebot verfassungsgemäß. Soweit es sich um Sperrverfügungen gemäß § 9 Abs. 1 Satz 3 Nr. 5 GlüStV a.F. handelt, ergeben sich in Bezug auf die Tatbestandsvoraussetzungen, insbesondere „Mittwirkung“ sowie „Vorsätzlichkeit“ von Access-Provider, Bedenken. Außerdem ist der Access-Provider kein tauglicher Adressat einer Maßnahme, die sich auf § 9 Abs. 1 Satz 3 Nr. 5 GlüStV a.F. stützt, weil sich die darin geregelte „Untersagung“ an Content- und Hostanbieter richtet. Angesichts der oben genannten Probleme ist § 9 Abs. 1 Satz 3 Nr. 5 GlüStV a.F im Gesetz zum Ersten Glücksspieländerungsstaatsvertrag (GlüÄndStV)[384] gestrichen und in der neuen Fassung vom GlüStV, welcher am 1.7.2012 in Kraft getreten ist, nicht mehr enthalten.

E. Zugangsanbieter als Nichtstörer im polizei- und ordnungsrechtlichen Sinne?

Die polizei- und ordnungsrechtliche Generalklausel können als Ermächtigungsgrundlage für die Sperrungsverfügungen gegenüber Access-Providern für Fälle von rechtswidrigen Inhalten dienen. Access-Provider würden dann als Nichtstörer trotz der zivil- und strafrechtlichen Haftungsprivilegierung in Anspruch genommen werden.[385] Dann muss eine Gefahr im Sinne von Polizei- und Ordnungsrecht eingetreten sein, so dass eine Sachlage oder ein Verhalten vorliegt, die bei ungehindertem Ablauf und in absehbarer Zeit mit hinreichender Wahrscheinlichkeit zu einem erwartenden Schaden für die öffentliche Sicherheit oder die öffentliche Ordnung führen wird.[386] Der Access-Provider muss außerdem Störer und damit im Polizei- und Ordnungsrecht verantwortlich sein. Beim Störer ist zwischen Handlungsstörer, Zustandsstörer und Nichtstörer zu unterscheiden.[387] Während Content-Provider zu Handlungsstörern oder Zustandsstörern und Host-Provider zu Zustandsstörern gezählt werden können,[388] kommt für die Verantwortlichkeit der Access-Provider weder die Handlungsstörer-, noch die Zustandsstörereigenschaft

---

384 Nds. GVBl. 190.

385 VG Düsseldorf, B. v. 17.5.2010 - 27 L 143/10, Rn. 29 ff.

386 *Pieroth/Schlink/Kniesel*, 60; *Würtenberger*, in: Besonderes Verwaltungsrecht Bd. III, § 69 Rn. 232; *Schoch*, in: Besonderes Verwaltungsrecht, Kapitel 2, Rn. 133.

387 *Pieroth/Schlink/Kniesel*, 138; *Würtenberger*, in: Besonderes Verwaltungsrecht Bd. III, § 69 Rn. 244 ff.; *Schoch*, in: Besonderes Verwaltungsrecht, Kapitel 2, Rn. 167 ff.

388 *Spindler/Volkmann*, K&R 2002, 398 (402); *Zimmermann*, NJW 1999, 3145 (3148); Spindler, GRUR 2014, 826 (827).

in Betracht, da Access-Provider weder durch ihr Verhalten eine inhaltlich bezogene Gefahr verursachen, noch tatsächliche Herrschaft über die rechtswidrigen Inhalte haben.[389] Gegen Nichtstörer dürfen Maßnahmen zur Abwehr einer gegenwärtigen erheblichen Gefahr im Vergleich zu dem Verhaltens- und Zustandsstörer nur subsidiär und ausnahmsweise gerichtet werden.[390] Ob eine gegenwärtige erhebliche Gefahr bei Inanspruchnahme von Access-Provider tatsächlich besteht, ist im Einzelfall zu klären, wobei angesichts der strengen Voraussetzungen für die Inanspruchnahme des Nichtstörers die Verhältnismäßigkeit der Maßnahmen zu prüfen ist.

F. Zivilrechtliche Sperrungsverlangen gegen Access-Provider

Nicht nur im öffentlichen Recht, sondern auch zivilrechtlich wurde von Zugangsanbietern verlangt, bestimmte Internetseiten sowie Online-Inhalte zu sperren. Die rechtswidrigen Inhalte im Kommunikationsnetz könnten gegen Rechtsnormen des Wettbewerbs- oder Urheberrechts verstoßen. Die meisten Gerichte in den früheren Rechtsprechungen standen zwar auf der Seite der Zugangsanbieter, jedoch haben der EuGH und der BGH in neueren Entscheidungen eine andere Ansicht vertreten. Bevor auf die relevanten Entscheidungen und Gesetze eingegangen wird, sind der Regelungsrahmen der Haftung der Access-Provider sowie wichtige Entscheidungen auf europäischer und nationaler Ebene vorzustellen.

I. Haftungsregelungsrahmen für Access-Provider in der E-Commerce-Richtlinie und Umsetzung in Deutschland (Notice-and-Take-Down)

Beim Haftungsregime für Internetintermediäre spielt die Richtlinie über den elektronischen Geschäftsverkehr (E-Commerce-Richtlinie)[391] aus dem Jahr 2000 eine grundlegende Rolle. Zur Sicherung und Förderungen des gemeinsamen Markts

---

389 *Spindler/Volkmann*, K&R 2002, 398 (403); *Zimmermann*, NJW 1999, 3145 (3149); *Heliosch*, 288.

390 OVG NRW, B. v. 19.3.2003 - 8 B 2567/02, Rn. 83; *Zimmermann*, NJW 1999, 3145 (3149 f.); *Dietlein/Heinemann*, in: Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2003, 395 (406).

391 ABl. EG Nr. L 178 v. 17. 7. 2000; Zum Konzept der E-Commerce-Richtlinie, siehe Mitteilung der Kommission „Europäische Initiative für den elektronischen Geschäftsverkehr" v. 16. 4. 1997, KOM (97) 157 endg; die Entwicklung der Richtlinie, siehe *Tettenborn*, K&R 1999, 252 (252 ff.); *ders*., K&R 1999, 442 (443 ff.); *ders*., K&R 2000, 59 (60 ff.).

der EU müssen die Informationen im Netz in einem rechtlich bestimmten Rahmen vermittelt, übermittelt oder gespeichert werden. Gemäß Art. 12 Abs. 1 E-Commerce-Richtlinie haften Access-Provider grundsätzlich nicht für die übermittelten Informationen,[392] sofern er die Negativkriterien der Haftungsprivilegierung erfüllt. Das Haftungsprivileg greift nach dieser Vorschrift dann, wenn der Access-Provider die Übermittelung nicht veranlasst, den Empfänger nicht auswählt oder die Informationen nicht auswählt oder verändert.[393] Zudem trägt der Access-Provider zwar angesichts seiner Neutralität nicht die allgemeine Pflicht, die von anderen bereitgestellten Inhalte aktiv zu überwachen (Art. 15 Abs. 1 E-Commerce-Richtlinie).[394] Es ist aber möglich, dass ein Gericht oder eine Verwaltungsbehörde der Mitgliedstaaten trotz der Haftungsprivilegierung zum Abstellen oder Verhindern von Rechtsverletzungen gegenüber dem Access-Provider entsprechende Maßnahmen trifft (Art. 12 Abs. 3 E-Commerce-Richtlinie).[395]

Um die E-Commerce-Richtlinie umzusetzen, wurde in Deutschland das Telemediengesetz 2007 erlassen.[396] Die Grundsätze und die Begrenzung der Haftung für Telemediendienstanbieter sind zur Gewährleistung der Rechtssicherheit in den §§ 7 bis 10 TMG niedergelegt. Als „rechtsgebietsübergreifende Querschnittsregelung" gelten sie im Strafrecht, Zivilrecht und Verwaltungsrecht.[397] Die Haftungsregeln für Access-Provider gemäß § 8 TMG sind größtenteils wortwörtlich nach dem Modell des Art. 12 E-Commerce-Richtlinie ausgebaut. Access-Provider sind gemäß § 8 TMG in der Regel nicht für fremde Informationen verantwortlich, wenn keiner der in § 8 Abs. 1 Satz 1 Nr. 1-3 TMG aufgelisteten Tatbestände erfüllt ist („sofern sie die Übermittlung nicht veranlasst, den Adressaten der übermittelten Informationen nicht ausgewählt und die übermittelten Informationen nicht ausgewählt oder verändert"). Es wird zudem betont, dass Access-Provider nicht auf

---

392 Dienstanbieter gemäß Art. 12 Abs. 1 E-Commerce-Richtlinie umfasst Access-Provider, siehe *Grabitz/Hilf/Nettesheim*, Art. 12, Rn. 2;

393 *Grabitz/Hilf/Nettesheim*, Art. 12, Rn. 4, 6 f.; KOM (1998) 586, endg., v. 18. 11. 1998, Begründung zu Art. 12 Abs. 1 E-Commerce-Richtlinie; *Hollenders*, 105.

394 BGH, U. v. 26.11.2015 - I ZR 3/14, Rn. 20; 47. Begründung zu Art. 12 Abs. 1 E-Commerce-Richtlinie; *Grabitz/Hilf/Nettesheim*, Art. 12, Rn. 10.

395 47. Begründung zu Art. 12 Abs. 1 E-Commerce-Richtlinie; Grabitz/Hilf/Nettesheim, Art. 12, Rn. 10

396 BGBl. I 2007, 179; dazu *Spindler*, CR 2007, 239 (239 ff.); *ders*., NJW 2002, 921 (921 ff.); *Sieber/Höfinger*, in: Handbuch Multimedia-Recht, Teil 18.1, Rn. 10 ff.; *Härting*, 512; *Hoeren/Bensinger*, 19.

397 *Sieber/Höfinger*, in: Handbuch Multimedia-Recht, Teil 18.1, Rn. 1, 15, 20 ff.; *Beaucamp/Henningsen/Florian*, MMR 2018, 501 (503); *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (15); *Frey/Rodolph*, Rn. 3 ff.

Schadenersatz, Beseitigung oder Unterlassung einer Rechtsverletzung in Anspruch angenommen werden, sofern sie nicht für die rechtswidrige Handlung oder Rechtsverletzung verantwortlich sind (§ 8 Abs. 1 Satz 2 TMG). Als privilegierte Diensteanbieter sind Access-Provider auch nicht verpflichtet, „die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen“ (§ 7 Abs. 2 TMG). Dies schließt allerdings nicht aus, dass sie nach allgemeinen Gesetzen nach gerichtlicher oder behördlicher Aufforderung die Informationen entfernen oder sperren müssen (§ 7 Abs. 3 Satz 1 TMG).[398]

II. Störerhaftung als Ergänzung der Haftungsregeln, Unterlassungsanspruch anstelle von Schadensersatz – Fallbeispiel Auktionsplattform

Im Fall einer „Internetversteigerung“ machte die Firma Rolex gegenüber einer Auktionsplattform Ansprüche auf Unterlassung und Schadenersatz geltend, weil auf ihrer Plattform gefälschte Rolex-Uhren angeboten wurden.[399] Zunächst lehnte der BGH den Schadensersatzanspruch ab, da die Plattform in diesem Fall weder als Täter noch als Teilnehmer behandelt werden könnte.[400] Da § 7 Abs. 2 Satz 2 TMG dem Telemediendienstanbieter nur die Privilegierungen für Schadensersatzansprüche und nicht für Unterlassungs- und Beseitigungsansprüche ermöglicht,[401] kann der Betreiber der Internetplattform als Host-Provider noch zur Unterlassung verpflichtet werden.[402] Der Unterlassungsanspruch ergibt sich hierbei aus der analogen Anwendung des § 1004 BGB. Wer nicht als Täter oder Teilnehmer agiert, kann trotz der Haftungsprivilegierung noch auf Unterlassung in Anspruch genommen werden. Der Host-Provider ist als Störer zu qualifizieren, wenn er willentlich und adäquat an der Rechtsverletzung mitgewirkt hat, so hat es der BGH in der

---

398 BGH, U. v. 26.11.2015 - I ZR 3/14, Rn. 20; Erwägungsgrund 47 der Richtlinie 2000/31/EG; ferner BGH, U. v. 17. 8. 2011 - I ZR 57/09, BGHZ 191, 19 Rn. 22 ff.; BGH, U. v. 5. 2. 2015 - I ZR 240/12; zu den allgemeinen Gesetzen, siehe BT-Drs. 13/7385, 21; BT-Drs. 14/6098.

399 LG Köln, Urt. v. 31.10.2000 – 33 O 251/00, CR 2001, 417; OLG Köln, Urt. v. 2.11.2001 – 6 U 12/01, MMR 2002, 110 m. Anm. *Hoeren*; BGH, Urt. v. 11.3.2004 – I ZR 304/01, MDR 2004, 1369.

400 BGH, Urt. v. 11.3.2004 – I ZR 304/01, MMR 2004, 668; BGH, Urt. v. 19.4.2007 – I ZR 35/04, CR 2007, 523 m. Anm. *Rössel*.

401 BGH, U. v. 11.3.2004 - I ZR 304/01, MMR 2004, 668 (668); BGH, U, v. 19.4.2007 - I ZR 35/04, MMR 2007, 507 (508); BGH, U. v. 12.7.2007 - I ZR 18/04, MMR 2007, 634 (635); OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, GRUR-RR 2014, 140 (143).

402 BGH, Urt. v. 19.4.2007 – I ZR 35/04, CR 2007, 523 m. Anm. *Rössel*.

Entscheidung „Internetversteigerung“ begründet und dabei besondere Anforderungen an die Störerhaftung entwickelt.[403] Um diese Störerhaftung zu begrenzen, setzt die Verletzung der Prüfungspflichten eine rechtliche und tatsächliche Zumutbarkeit voraus.[404] Im geschäftlichen Verkehr sei es dem Betreiber zumutbar, dass er technisch und rechtlich überprüft, ob Schutzrechte von Dritten vom betroffenen Angebot verletzt würden. Seit der Internetversteigerung-Entscheidung begründet der BGH auch in vielen weiteren Fällen die Unterlassungspflicht der Intermediäre mit der Störerhaftung.[405]

Bei der Internetversteigerung-Entscheidung handelt es sich um die Störerhaftung des Host-Providers für Unterlassung oder Schadenersatz. Die Frage ist danach, ob und wie die vom BGH entwickelte Störerhaftung auch für Access-Provider gilt. In den folgenden Entscheidungen aus dem Bereich des Wettbewerbs- und Urheberrechts wurde die Anwendung der Störerhaftung ausführlich diskutiert.

III. Sperrverlangen gegen Access-Provider wegen wettbewerbswidriger Inhalte

Access-Provider sind vielfach aufgefordert worden, den Abruf von jugendschutzrechtswidrigen Seiten und strafbaren Erotik-Webseiten durch Sperrung zu erschweren.[406] Im Folgenden ist zu untersuchen, ob Access-Provider aus wettbewerbsrechtlichen Gründen zur Sperrung von solchen Inhalten aufgefordert werden können. Hierzu werden die zitierten Fälle mit Anpassung an die aktuelle Rechtslage analysiert.

---

403 BGH, U. v. 11.3.2004 - I ZR 304/01, Rn. 43; weitere Rechtsprechungen BGH, U. v. 30.4.2008 - I ZR 73/05; U. v. 12.3.2010 - I ZR 121/08, BGHZ 185, 330 Rn. 19; U. v. 18. 11. 2011 - I ZR 155/09; U. v. 12. 6. 2012 - I ZR 18/11, BGHZ 194, 339 Rn. 19; U. v. 26.11.2015 - I ZR 3/14; U. v. 26.11.2015 - I ZR 174/14; U. v. 30.3.2017 – I ZR 19/16; *Czychowski/Nordemann*, GRUR 2013, 986 (989); *Ohly*, NJW-Beil. 2014, 47 (50); *Köhler*, GRUR 2008, 1 (6).

404 BGH, U. v. 11.3.2004 - I ZR 304/01, Rn. 44.

405 BGH, U. v. 30.4.2008 - I ZR 73/05; U. v. 12.3.2010 - I ZR 121/08, BGHZ 185, 330 Rn. 19; U. v. 18. 11. 2011 - I ZR 155/09; U. v. 12. 6. 2012 - I ZR 18/11, BGHZ 194, 339 Rn. 19; U. v. 26.11.2015 - I ZR 3/14; U. v. 26.11.2015 - I ZR 174/14; U. v. 30.3.2017 – I ZR 19/16.

406 LG Kiel, U. v. 23.11.2007 - 14 O 125/07; LG Frankfurt, Beschl. v. 5.12.2007 - 2/03 O 526/07; LG Düsseldorf, U. v. 13.12.2007 - 12 O 550/07; OLG Frankfurt, Beschl. v. 22.1.2008 - 6 W 10/08; LG Frankfurt, U. v. 8.2. 2008 - 3/12 O 171/07.

1. Nichtvorliegen der Tatbestandvoraussetzung der Anspruchsgrundlage aus UWG und StGB

Als Anspruchsgrundlagen für Sperrungen von pornographischen, jugendgefährdenden Webseiten kommen im Wettbewerbsrecht §§ 3a, 4 Nr. 4, 8 Abs. 1 S. 1, Abs. 3 Nr. 1 UWG i.V.m. den entsprechenden Paragraphen des StGB (z.B. § 184 Abs. 1 Nr. 1, 184a, 184b, 184c StGB) sowie des § 15 JuSchG und §§ 4, 5 JMStV in Betracht. Handlungen sind z.B. nach § 4 Nr. 4 UWG wettbewerbswidrig, wenn sie die Mitbewerber gezielt behindern sollen, oder nach § 3a UWG, die einer gesetzlichen Vorschrift zuwiderlaufen, die auch dazu bestimmt ist, das Marktverhalten zu regeln. Hierzu kann man sich auf die strafrechtliche Vorschrift zum Verbot pornographischer Schriften (§ 184 StGB), die Verbreitung gewalt-, oder tierpornographischer Schriften (§ 184a StGB) und kinderpornographischer Schriften (§ 184b StGB) und jugendpornographische Schriften (§184c StGB) berufen.

Unabhängig von der konkreten Anspruchsgrundlage nach dem UWG setzt der Anspruch gegenüber dem Zugangsanbieter ein Wettbewerbsverhältnis zwischen dem Zugangsanbieter und Anbietern von pornographischen Filmen und Bildern voraus. Aufgrund der Neutralität des Zugangsanbieters bei der Übermittelung der Informationen ist der Tatbestand i.S.d. § 2 Abs. 1 Nr. 1 UWG aber nicht erfüllt. Die geschäftliche Handlung des Access-Providers liegt nicht in dem Anbieten der Inhalte, sondern nur in der Ermöglichung des Zugangs zum Internet.[407]

Darüber hinaus scheitert der wettbewerbsrechtliche Anspruch bei Zuwiderhandeln gegen eine gesetzliche Vorschrift insbesondere daran, dass Access-Provider weder Täter noch als Teilnehmer von Wettbewerbsverstößen nach § 3a UWG sein können.[408] Access-Provider bieten selber keine rechtswidrigen Inhalte an, stellen lediglich „unternehmensbedingt“[409] Verbindungen zu einem Kommunikationsnetz her und sind schließlich ohne Vorsatz sowie Garantenstellung nicht als Gehilfe im Sinne von § 27 StGB anzusehen.[410]

---

407 LG Kiel, U. v. 23.11.2007 - 14 O 125/07, Rn. 52; LG Frankfurt, Beschl. v. 5.12.2007 - 2/03 O 526/07, Rn. 8; LG Düsseldorf, U. v. 13.12.2007 - 12 O 550/07, Rn. 22 f.; LG Frankfurt, U. v. 8.2.2008 - 3/12 O 171/07, Rn. 36.

408 LG Kiel, U. v. 23.11.2007 - 14 O 125/07, Rn. 50; LG Frankfurt, Beschl. v. 5.12.2007 - 2/03 O 526/07, Rn. 5 ff.; LG Frankfurt, U. v. 8.2.2008 - 3/12 O 171/07, Rn. 32.

409 LG Frankfurt, U. v. 8.2.2008 - 3/12 O 171/07, Rn. 32.

410 LG Kiel, U. v. 23.11.2007 - 14 O 125/07, Rn. 51; LG Frankfurt, Beschl. v. 5.12.2007 - 2/03 O 526/07, Rn. 7; LG Frankfurt, U. v. 8.2.2008 - 3/12 O 171/07, Rn. 32.

2. Keine Verletzung der wettbewerbsrechtlichen Verkehrspflicht

Die wettbewerbsrechtliche Verkehrspflicht ist vom BGH im Fall „Jugendgefährdende Medien bei eBay“[411] entwickelt worden. Wer als Unternehmen bei einem Dritten wettbewerbsrechtliche Verletzungen hervorruft und dabei im eigenen geschäftlichen Interesse handelt, ist verpflichtet, die wettbewerblichen Verletzungen im Rahmen des Möglichen und Zumutbaren zu begrenzen.[412] Die Gerichte haben es abgelehnt, den Grundsatz der wettbewerbsrechtlichen Verkehrspflicht auf Zugangsanbieter anzuwenden.[413] Denn eine Gefahr schafft der Access-Provider nicht, weil er zunächst weder Betreiber der Webseite noch ihr Vertragspartner ist und daher nicht in seinem „eigenen Verantwortungsbereich eine Gefahrenquelle für Wettbewerbsverstöße“[414] eröffne. Außerdem betreibt der Access-Provider, wie im Fall „Jugendgefährdende Medien bei eBay“, keine Plattform, auf der die unlautere Handlung sowie Bereitstellung rechtswidriger Inhalte von anderen ermöglicht wird. Daher lässt sich der für Host-Provider entwickelte Grundsatz nicht auch auf Zugangsanbieter übertragen.[415] Das OLG Frankfurt führt dazu aus, dass im Vergleich zu Kunden einer Plattform, die Kunden eines Zugangsanbieters „nicht Urheber dieser Wettbewerbsverstöße, sondern allenfalls deren Nutznießer oder Opfer“ seien.[416] Der Zugangsanbieter schafft demgemäß in seinem eigenen Verantwortungsbereich keine Gefahrenquelle. Eine Bejahung der Anspruchserstreckung auf Access-Provider ist daher abzulehnen.[417]

3. Unterlassungsanspruch auch wegen fehlender Störereigenschaft und Unzumutbarkeit der Maßnahme verneint

Um Adressat eines Unterlassungsanspruchs zu sein, muss der Access-Provider nicht als Täter oder Teilnehmer agieren. Er muss aber willentlich und adäquat kausal an der Rechtsverletzung mitwirken. Der Zugangsanbieter kann zunächst auch mangels Vorsatzes weder als Täter noch Teilnehmer haften. Er hat außerdem keine

---

411 BGH, U. v. 12.7.2007 - I ZR 18/04.

412 BGH, U. v. 12.7.2007 - I ZR 18/04, Rn. 36 ff.

413 LG Kiel, U. v. 23.11.2007 - 14 O 125/07, Rn. 53; LG Düsseldorf, U. v. 13.12.2007 - 12 O 550/07, Rn. 24 ff.; OLG Frankfurt, Beschl. v. 22.1.2008 - 6 W 10/08, Rn. 8 ff.; LG Frankfurt, U. v. 8.2.2008 - 3/12 O 171/07, Rn. 33 ff.

414 OLG Frankfurt, Beschl. v. 22.1.2008 - 6 W 10/08, Rn. 11; LG Frankfurt, U. v. 8.2.2008 - 3/12 O 171/07, Rn. 34.

415 LG Kiel, U. v. 23.11.2007 - 14 O 125/07, Rn. 53; LG Frankfurt, U. v. 8.2.2008 - 3/12 O 171/07, Rn. 41.

416 OLG Frankfurt, Beschl. v. 22.1.2008 - 6 W 10/08, Rn. 11.

417 Ebd., Rn. 11, das Gericht erachtet in der Anwendung des wettbewerblichen Unterlassungsanspruchs auf Access-Provider eine „Überspannung“ der rechtlichen Grundlagen.

vertragliche Beziehung zum Content- oder Host-Provider. Es soll ihm als reinem Diensteanbieter der TK-Infrastruktur die rechtswidrige Beeinträchtigung der darin vermittelten Inhalte nicht zuzurechnen sein.

Ferner muss das Sperrverlangen auch zumutbar sein. Dies setzt eine rechtliche und tatsächliche Zumutbarkeit voraus. Da es bei der DNS-Sperre leichte Umgehungsmöglichkeiten gibt, sei es im technischen Sinne nicht zumutbar.[418] Somit liegen die wesentlichen Tatbestandsvoraussetzungen der Störerhaftung nicht vor.[419] Ein Zugangsanbieter haftet im Wettbewerbsrecht folglich weder als Täter oder Teilnehmer, noch als Störer, während er aber in den neueren Entscheidungen des BGH im Urheberrecht als Störer herangezogen wurde.[420]

4. Stellungnahme

Im wettbewerbsrechtlichen Sinne erscheint eine Haftung des Access-Providers zunächst fragwürdig, da kein Wettbewerbsverhältnis zwischen Access-Provider und Inhalt- oder Host-Provider besteht. Der Anspruch von Wettbewerbern nach § 3a UWG scheitert aufgrund der Neutralität des Access-Providers. Bereits bei der Ablehnung einer wettbewerbsrechtlichen Verkehrspflicht wurde zwischen dem Access-Provider und dem Betreiber der Webseite unterschieden. Auf dieser Basis hat das Gericht aber unzutreffender Weise abgelehnt, dass ein von der Rechtsprechung für Host-Provider entwickelter Grundsatz auf einen anderen Intermediär zu übertragen ist.[421] § 7 Abs. 3 Satz 2 TMG schließt die gerichtliche oder behördliche Sperranordnungen gegen Telemediendienstanbieter nicht aus. Im Wettbewerbsrecht hat das Gericht diese gesetzlich vorausgesetzte Sperrmöglichkeit gegen Access-Provider aber ausgeschlossen. Ebenfalls ist die Rechtsprechung bei der Prüfung der „Störerhaftung“ von der neutralen Rolle des Access-Providers und der Untauglichkeit der Sperrtechnik ausgegangen. Die neutrale Rolle des Access-Providers spricht in der Tat grundsätzlich gegen die Störereigenschaft. Allerdings kann die Störereigenschaft bejaht werden, soweit er willentlich und adäquat an der Rechtsverletzung mitgewirkt hat. Dies kann bejaht werden, wenn er Kenntnis von

---

418 LG Kiel, U. v. 23.11.2007 - 14 O 125/07, Rn. 54; OLG Frankfurt, Beschl. v. 22.1.2008 - 6 W 10/08, Rn. 12; LG Hamburg, U. v. 12.11.2008 - 308 O 548/08, ZUM 2009, 587.

419 LG Kiel, U. v. 23.11.2007 - 14 O 125/07, Rn. 54 ff.

420 BGH, U. v. 26.11.2015 - I ZR 3/14; BGH, U. v. 26.11.2015 - I ZR 174/14, hierzu sogleich

421 Gegen die Übertragbarkeit der Störerhaftung auf Access-Provider, siehe *Döring*, WRP 2008, 1155 (1155 ff.); *Gercke*, CR 2006, 210 (214).

der Rechtsverletzung erlangt. Im Urheberrecht sah der BGH – dazu sogleich Näheres –, dass Sperrmaßnahmen gegen Access-Provider auf Grundlage der Störerhaftung zulässig sein können, wobei Access-Provider nur subsidiär zu Inhalts- und Host-Providern in Anspruch zu nehmen sind.[422]

Des Weiteren ist die Annahme zu kritisieren, dass die Sperrtechnik untauglich ist. Die Sperrmaßnahme unterbindet zwar den Zugang zu allen rechtswidrigen Online-Angeboten nicht, aber sie bewirkt dennoch eine spürbare Erschwerung der Auffindbarkeit bestimmter Inhalte. Noch zu kritisieren ist, dass Internetsperren im wettbewerbsrechtlichen Bereich einstimmig von der Rechtsprechung untersagt wurden, ohne die Eingriffsmöglichkeit und Interessenabwägung aus der Perspektive des Grundrechtsschutzes vorzunehmen,[423] während im Urheberrecht hier das Diskussionszentrum liegt. Dies ist Gegenstand des nächsten Abschnitts.

IV. Sperrverlangen wegen Urheberrechtsverletzung

Deutsche Gerichte haben sich in den letzten Jahren bei privatrechtlicher Internetsperrung hauptsächlich mit drei Fällen im Bereich des Urheberrechts beschäftigt.[424] Bei den Fällen von „g-stream.in“, „3dl.am“ und „goldesel.to“ geht es immer um die Frage, ob und unter welchen Voraussetzungen ein Rechtsinhaber von einem Access-Provider verlangen kann, den Zugang zu den urheberrechtlich rechtswidrigen Online-Inhalten zu sperren. Gegenstand dieses Abschnitts ist die Darstellung der Entwicklung der Rechtsprechung und des Rechts.

1. Urheberrechtliche Störerhaftung in den früheren deutschen Rechtsprechungen

Urheber oder Verwertungsgesellschaften forderten in einer Reihe von Klagen vom Internetzugangsanbieter, den Zugang zu einer urheberrechtlich rechtswidrigen Internetseite zu sperren.[425] Im Wettbewerbsrecht gilt in Bezug auf Internetsperren,

---

422 BGH, U. v. 26.11.2015 - I ZR 174/14; dazu *Heidrich/Heymann*, MMR 2016, 370 (370); *Leistner*, JZ 2014, 846 (856).

423 *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (3).

424 „g-stream.in“: LG Hamburg, U. v. 12.11.2008 - 308 O 548/08; OLG Hamburg, U. v. 22.12.2010 - 5 U 36/09; „3dl.am“, LG Hamburg, U. v. 12.3.2010 - 308 O 640/08; OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10; BGH, U. v. 26.11.2015 - I ZR 3/14; „Goldesel“, LG Köln, U. v. 31.8.2011 - 28 O 362/10; OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11; BGH, U. v. 26.11.2015 - I ZR 174/14.

425 LG Hamburg, U. v. 12.11.2008 - 308 O 548/08; OLG Hamburg, U. v. 22.12.2010 - 5 U 36/09; LG Hamburg, U. v. 12.3.2010 - 308 O 640/08; OLG Hamburg, U. v. 21.11.2013 -

dass Zugangsanbieter mangels Kenntnis weder als Täter noch Teilnehmer haften können.[426] In Betracht kommt dann nur die Haftungsmöglichkeit nach der Störerhaftung, wenn der Störer willentlich und adäquat kausal an der Rechtsverletzung mitgewirkt hat. Als Rechtsgrundlage für die Störerhaftung im Urheberecht kommt § 1004 Abs. 1 BGB i.V.m. §§ 97 Abs. 1, 19a UrhG in Betracht. Für die Störerhaftung müssen wieder die Voraussetzungen der adäquaten Kausalität, der rechtlichen und tatsächlichen Zumutbarkeit erfüllt werden.

Alle Gerichte bejahten – im Unterschied zu den oben geschilderten wettbewerbsrechtlichen Konstellationen – im Urheberrecht die adäquate Kausalität des Verhaltens des Zugangsanbieters, weil er durch das Vermitteln des Zugangs zum Internet im Allgemeinen den Aufruf und Download sowie die Vervielfältigungshandlungen der Kunden herbeiführt.[427] Das LG Hamburg und das OLG Hamburg unterscheiden im „3dl.am"-Fall zwischen tatsächlicher und rechtlicher Unmöglichkeit der Sperrung. Anders als in den wettbewerbsrechtlichen Fällen, in denen die technische Möglichkeit der Sperrung infolge von leichten Umgehungsmöglichkeiten nicht bejahrt wurde, war dies in urheberrechtlichen Entscheidungen als gegeben angesehen worden.[428] Eine Beeinträchtigung der Grundrechte könne trotz der technischen Möglichkeit der Sperrung dennoch zur rechtlichen Unmöglichkeit führen.[429] Zunächst ist die Frage zu beantworten, ob Sperrverlangen zur Verhinderung von Urheberrechtsverletzungen mit den Grundrechten der Betroffenen zu vereinbaren sind. Dafür ist zunächst zu prüfen, ob die Sperrverfügungen gegenüber Access-Providern einen Eingriff in das Telekommunikationsgeheimnis darstellen (a)). Im Anschluss daran wird die Effektivität solcher Maßnahmen zu thematisieren sein (b)), ehe eine Interessenabwägung vorgenommen wird (c)).

---

5 U 68/10; LG Köln, U. v. 31.8.2011 - 28 O 362/10; OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11.

426 LG Hamburg, U. v. 12.11.2008 - 308 O 548/08, Rn. 23; OLG Hamburg, U. v. 22.12.2010 - 5 U 36/09, Rn. 33; LG Hamburg, U. v. 12.3.2010 - 308 O 640/08, Rn. 38; OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 61; OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 948.

427 LG Hamburg, U. v. 12.11.2008 - 308 O 548/08, Rn. 27; OLG Hamburg, U. v. 22.12.2010 - 5 U 36/09, Rn. 60; LG Hamburg, U. v. 12.3.2010 - 308 O 640/08, Rn. 42; OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 70; LG Köln, U. v. 31.8.2011 - 28 O 362/10, Rn. 71; OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 949; *Sessing/Putzki*, MMR 2016, 660 (662 f.).

428 LG Hamburg, U. v. 12.11.2008 - 308 O 548/08, Rn. 29 ff.; OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 970.

429 LG Hamburg, U. v. 12.3.2010 - 308 O 640/08, Rn. 45; OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 72.

a) Eingriff in den Schutz des Telekommunikationsgeheimnisses und Erforderlichkeit einer speziellen Rechtsgrundlage?

aa) Relevanz des Telekommunikationsgeheimnisses für Sperrverfügungen gegen Access-Provider

Das Grundrecht gilt nicht nur als Abwehrrecht gegenüber staatlichen Eingriffen,[430] sondern das Grundrecht hat auch mittelbare Drittwirkung, wonach die Grundrechte in Privatrechtsverhältnissen zwar nicht unmittelbar gelten.[431] Der Staat ist jedoch dazu verpflichtet, grundrechtlich geschützte Interessen des Betroffenen vor Grundrechtsverletzungen oder Gefährdungen durch Dritte zu schützen.[432] Die Gerichte haben demnach die Beeinträchtigung des Schutzes des Telekommunikationsgeheimnisses geprüft. Das durch Art. 10 Abs. 1 GG geschützte Telekommunikationsgeheimnis gewährt dem Einzelnen die unkörperliche Übermittlung von Informationen mittels Telekommunikationsverkehr, ohne dabei von der öffentlichen Gewalt abgehört zu werden.[433] Da die Übermittelung der Nachrichten mittels des Telekommunikationsnetzes das Risiko der Kenntnisnahme erhöht, soll Art. 10 Abs. 1 GG solche räumlich getrennten Kommunikationsvorgänge besonders schützen.[434] Das Telekommunikationsgeheimnis schützt daher die Privatheit der Kommunikation.[435] Art. 10 Abs. 1 GG umfasst sowohl den Schutz des Inhalts der Telekommunikation, als auch die sonstigen Umstände des Telekommunikationsvorgangs.[436] Bei den näheren Umständen handelt es sich darum, wer mit wem, wann, wie oft und wo kommuniziert hat oder versucht hat zu kommunizieren.[437]

---

430 *Durner*, in: Maunz/Dürig, GG, Art. 10, Rn. 122.

431 BVerfGE 7, 198 (198 ff.); 81, 242 (242 ff.); 89, 214 (214 ff.); *Durner*, in: Maunz/Dürig, GG, Art. 10, Rn. 111; *Durner*, ZUM 2010, 833 (835); *Gusy*, in: v. Mangoldt/Klein, GG, Art. 10, Rn. 55; *Hermes*, in: Dreier, GG, Art. 10, Rn. 92; *Löwer*, in: v. Münch/Kunig, GG, Art. 10, Rn. 5.

432 BVerfG NJW 2002, 3619, 3620 - Mithörfalle; *Baldus,* in: BeckOK GG, Art.10 Rz.24; zur Schutzpflicht, BVerfGE 7, 198 (205); 35, 79 (114); 39, 1 (41); 49, 89 (140 ff.); 53, 30 (57 ff.); 56, 54 (73f.); 79, 174 (201f.); 88, 203 (251); Calliess, in: HGR, Bd. II, § 44 Rn. 964 f.; *Schmidt-Aßmann*, in: HStR, Bd. II, § 26 Rn. 32; *Murswiek*, in: Sachs, GG, Art. 2 Rn. 24; Dreier, in: Dreier, GG, Vorb. Rn. 101 ff.

433 OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 929.

434 *Stettner*, in: HGR, Bd. IV, § 92 Rn. 18; *Pagenkopf*, in: Sachs, GG, Art. 10 Rn. 2 ff.; *Hermes*, in: Dreier, GG, Art. 10 Rn. 36 ff.; *Durner*, in: Maunz/Dürig, GG, Art. 10 Rn. 81 ff.

435 BVerfGE 85, 386(395); 113, 348(356); 115, 166(182).

436 BVerfGE 67, 157(172); 85, 386(396); 106, 28(37); 115, 166(183); 120, 274(308); 125, 260(365); LG Hamburg, U. v. 12.3.2010 - 308 O 640/08, Rn. 46; OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 84.

437 BVerfG, B. v. 20-06-1984 - 1 BvR 1494/78; BVerfG, B, v. 25-03-1992 - 1 BvR 1430/88; BVerfG, U. v. 14.7.1999 - 1 BvR 2226/94, 2420/95 u. 2437/95; *Durner*, in: Maunz/Dürig, GG, Art. 10, Rn. 86.

bb) Vorliegen eines Eingriffs

Die Beeinträchtigung des Schutzes des Telekommunikationsgeheimnisses setzt die Kenntnisnahme von Inhalten oder den näheren Umständen der Kommunikation voraus.[438] Der Zugangsanbieter erlangt im Falle einer IP-Sperre oder DNS-Sperre die IP-Adresse und im Fall der URL-Sperre die Standortangaben von Informationen auf bestimmten Servern.[439] Durch Einsatz von Proxyservern verrät die URL auch bereits die Kommunikationsinhalte, da sie oftmals einen kurzen Text zu den Inhalten auf der Internetseite enthält.[440]

(1) Auffassung des OLG Hamburg: Inanspruchnahme des Access-Providers bedeutet Eingriff in TK-Geheimnis der Nutzer

Das OLG Hamburg vertrat die Meinung, dass bei den automatisierten Vorgängen der Internetsperrung ein Eingriff in das TK-Geheimnis vorliegt.[441] Zur Begründung des Eingriffs in Art. 10 GG bezieht sich das Gericht auf die Regelungen im § 88 TKG, die die Schutzpflicht des Art. 10 GG umsetzen.[442] Gemäß § 88 Abs. 2 Satz 1 TKG verpflichtet sich jeder TK-Dienstanbieter, das Telekommunikationsgeheimnis zu gewährleisten. Unter anderem verbietet § 88 Abs. 3 Satz 1 TKG dem TK-Dienstanbieter nur die Kenntnisnahme von Informationen, die für die Geschäftszwecke oder den Schutz der technischen Systeme erforderlich sind. Andere Informationen oder Umstände dürfen nicht erfasst werden. Gemäß § 88 Abs. 3 Satz 2 TKG gilt der Grundsatz der Zweckbindung, wonach dem TK-Dienstanbieter lediglich Kenntnis über für die Erbringung der Dienste erforderlichen Informationen – also zweckgebunden – verwenden kann. Daneben gilt das sog. kleine Zitiergebot gemäß § 88 Abs. 3 Satz 3 TKG. Hiernach bedarf es einer gesetzlichen Vorschrift, die ausdrücklich auf die durch das Gesetz legalisierten Eingriff in Telekommunikationsvorgänge hinweist.

---

438 LG Hamburg, U. v. 12.3.2010 - 308 O 640/08, Rn. 47 ff.; OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 87 ff.; LG Köln, U. v. 31.8.2011 - 28 O 362/10, Rn. 74.

439 *Frey/Rudolph*, Rechtsgutachten zur Evaluierung des Haftungsregimes für Host- und Access-Provider im Bereich der Telemedien, abrufbar unter <https://docplayer.org/3963933-Rechtsgutachten-zur-evaluierung-des-haftungsregimes-fuer-host-und-access-provider-im-bereich-der-telemedien.html > [Stand: 7.8.2019], 27; *Sieber/Nolde*, 83; OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 90; OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 936.

440 *Sieber/Nolde*, 85 f.

441 OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 92 ff.

442 *Durner*, in: Maunz/Dürig, GG, Art. 10, Rn. 120.; *Durner*, ZUM 2010, 833 (836).

Das OLG Hamburg hat festgestellt, dass Access-Provider bei der IP-, DNS- und URL-Sperre Kenntnis von den näheren Umständen, gegebenenfalls auch Inhalte, der Telekommunikation erlangen.[443] Dies geht über den Geschäftszweck und auch über den Schutzzweck der technischen Systeme im Sinne vom § 88 Abs. 3 Satz 1 TKG hinaus und verstößt gegen § 88 Abs. 3 Satz 2 TKG.[444] Als Beispiel nahm das OLG Hamburg die DNS-Sperre im damaligen Zugangserschwerungsgesetz.[445] § 11 ZugErschwG sah vor, dass durch §§ 2 und 4 das „Grundrecht des Fernmeldegeheimnisses (Art. 10 Abs. 1 GG) eingeschränkt" wurde und „hierdurch Telekommunikationsvorgänge im Sinne des § 88 Abs. 3 Satz TKG betroffen" waren. Übertragbar ist die Auffassung des Gesetzgebers beim ZugErschwG auf die Zugangserschwerung zu urheberrechtsverletzenden Angeboten.[446] Ein unmittelbarer Eingriff in den Schutzbereich des TK-Geheimnisses gemäß Art. 10 Abs. 1 GG liegt folglich vor. Die ungeschriebenen Grundsätze der Störerhaftung reichen im vorliegenden Fall nicht aus und für die Sperrmaßnahmen bedarf es einer ausdrücklichen gesetzlichen Grundlage.[447] Zur Bestimmtheit einer solchen gesetzlichen Grundlage müssen die Voraussetzungen der Sperrmaßnahmen im Einzelnen im Rahmen des Grundsatzes der Verhältnismäßigkeit berücksichtigt werden.[448] Aus der Sicht des OLG Hamburg spricht für eine spezielle Rechtsgrundlage auch, dass Sperrmaßnamen in die Rechte und Interessen der anderen verschiedenen Teilnehmer eingreifen können.[449]

(2) Vorzugswürdige Auffassung des OLG Köln: Nur URL-Sperre stellt Eingriff in TK-Geheimnis dar – IP- und DNS-Sperre nicht

Es soll aber der Auffassung des OLG Köln gefolgt werden, dass IP-Sperre und DNS-Sperre nicht in das Grundrecht auf Schutz des Telekommunikationsgeheimnisses eingreifen. Der entscheidende Grund liegt darin, dass der Schutzbereich des TK-Geheimnisses lediglich die Erlangung der Kommunikationsinhalte sowie näherer Umstände aber keine Verhinderung oder Erschwerung der Kommunikation

---

443 OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 93, 95.
444 OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 93.
445 OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 94 ff., 101 ff.; OLG Hamburg, U. v. 22.12.2010 - 5 U 36/09, Rn. 77 ff.; hierzu siehe Kapitel 4. C.
446 OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 94; OLG Hamburg, U. v. 22.12.2010 - 5 U 36/09, Rn. 77.
447 OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 99, 105.
448 OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 99.
449 OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 100; OLG Hamburg, U. v. 22.12.2010 - 5 U 36/09, Rn. 66.

umfasst.[450] Es liegt bei der IP-Sperre und DNS-Sperre nur eine schlichte Verhinderung der Kommunikation vor.[451] Durch die Anfrage des Nutzers erlangt der Vermittler mit der IP-Sperre und der DNS-Sperre keine Kenntnis über weitere Umstände als die, die er ohne Einsatz der Sperrtechnik für die Herstellung der Telekommunikationsverbindung benötigt.[452] Dagegen stellt die URL-Sperre aufgrund der Kenntniserlangung in Bezug auf die Kommunikationsinhalte einen Eingriff in das Grundrecht dar.[453] Für die Durchführung einer URL-Sperre setzt der Access-Provider zusätzlich einen Proxy-Server ein, sodass er den Datenverkehr des Nutzers überprüft. Bei diesem Vorgang nimmt er mehr als nur die Inhalte wahr, die für die Bereitstellung der Telekommunikationsverbindung erforderlich sind.[454] Es wird zwar in § 11 ZugErschwG darauf hingewiesen, dass alle Sperrmaßnahmen i.S.v. §§ 2 und 4 ZugErschwG das Grundrecht aus Art. 10 GG einschränken, weil der Gesetzgeber „vorsorglich" hierzu das Zitiergebot berücksichtigt hat.[455] Der Grund für § 11 ZugErschwG liegt dahin, dass das ZugErschwG der Behörde neben der DNS- und IP-Sperre auch die URL-Sperre (§ 2 Abs. 2 ZugErschwG) und die Speicherung der Verkehrs- und Nutzungsdaten (§ 6 ZugErschwG) erlaubt. Hierdurch erhält der Access-Provider über die reine Verhinderung der Kommunikation hinaus noch zusätzlich Kenntnis über Kommunikationsinhalte und deren nähere Umstände.[456] Anders als das OLG Hamburg kommt das OLG Köln zum Ergebnis, dass nur die URL-Sperre einen Eingriff in den Schutzbereich des TK-Geheimnisses darstellt.[457] Angesichts der mittelbaren Drittwirkung und der Schutzpflicht des Gesetzgebers in Bezug auf Art. 10 Abs. 1 GG muss der Schutz des TK-Geheimnisses im Rahmen der Anwendung und Auslegung der Störerhaftung berücksichtigt werden. Für die URL-Sperre ist eine ausdrückliche gesetzliche Grundlage erforderlich.[458] Für IP- oder DNS-Sperre hingegen ist eine spezialgesetzliche Grundlage nicht erforderlich, auch wenn sie mittelbar andere Grundrechte wie z.B. Meinungsfreiheit aus Art. 5 Abs. 1 Satz 1 Halbsatz 1 GG, die Berufsausübungsfreiheit aus Art. 12 Abs.1 GG oder das Eigentumsgrundrecht aus Art. 14 Abs. 1

---

450 OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 936.
451 OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 937 f.; *Durner*, ZUM 2010, 833 (841); dagegen *Sieber/Nolde*, 85.
452 OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 937.
453 Ebd., Rn. 943.
454 Ebd., Rn. 939.
455 Ebd., Rn. 400; *Durner*, ZUM 2010, 833 (834).
456 OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 940.
457 Ebd., Rn. 942.
458 Ebd., Rn. 943.

GG, berührt. Hierfür ist die Anspruchsgrundlage für die urheberrechtliche Störerhaftung aus §§ 1004 BGB i.V.m. §§ 97 Abs. 1, 19a UrhG ausreichend.[459]

b) Effektivität der Sperrung – Gefahr des Overblockings?

Für die Zumutbarkeit der Sperrmaßnahme gegenüber dem Access-Provider spricht es, wenn die Maßnahmen den Zugang zu den rechtsverletzenden Inhalten effektiv unterbinden können. Die Effektivität der Sperrung kann aber zu Overblocking führen, wovon auch rechtmäßige Inhalte betroffen sein können.[460] Nach Auffassung des OLG Hamburg führt z.B. eine DNS-Sperre unvermeidlich zu Kollateralschäden[461], da sich zahlreiche Zieladressen hinter einem Domain-Namen verbergen. Hingegen befand das OLG Köln, dass die Vorgabe der Effektivität der Sperrung keine vollständige Beseitigung der Rechtsverletzung verlangt. Bereits eine Erschwerung des Zugangs auf den unerlaubten Inhalten reiche aus.[462] Leichte Umgehungsmöglichkeit in Bezug auf die Sperrung führen nicht per se zur Ineffektivität der Maßnahme. Wie betroffene Nutzer auf entsprechende Sperrungen reagieren – dass sie etwa versuchen, die Sperrung zu umgehen –, ist im Vorhinein schwierig einzuschätzen.[463]

c) Interessenabwägung zwischen Zugangsanbieter und Urheberrechtsinhaber

Bei der Zumutbarkeit muss die Interessen- und Gefährdungslage des Zugangsanbieters berücksichtigt werden. Auch in Gestalt von DNS- oder IP-Sperre ist ein finanzieller, technischer und organisatorischer Zusatzaufwand unvermeidbar, auch wenn der Access-Provider eventuell bereits über die erforderlichen hardwaretechnischen Vorrichtungen verfügt.[464] Zudem entstehen Sicherheitsrisiken. Bei Fehleingaben können Störungen des Netzverkehrs die Folge sein.[465] Anderseits erzielt der Urheberrechtsinhaber durch Sperrmaßnahmen einen wirtschaftlichen Vorteil. Das OLG Hamburg steht mit seinen Begründungen, dass die Dienstleistung von Access-Providern „inhaltlich neutral, sozial und von der Rechtsordnung erwünscht“ ist und anders als Content- und Host-Provider keine inhaltliche

---

459 Ebd., Rn. 942.
460 OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 100.
461 Ebd., Rn. 102 ff.
462 OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 983.
463 OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 78.
464 OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 988 ff.
465 OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 999.

Rechtsbeziehung zum Urheberrechtsinhaber hat, auf der Seite der Access-Provider.[466] Es kommt bei der Abwägung zum Ergebnis, dass die Interessen des Access-Providers überwiegen und eine Inanspruchnahme deshalb nicht angemessen ist. Das OLG Köln hat die hingegen den wirtschaftlichen Vorteil für die Urheberrechtsinhaber betont.[467]

d) Zwischenergebnis

Bei den früheren deutschen Entscheidungen ging es um die Frage, ob der Urheber vom Access-Provider verlangen kann, den Zugang zu einer urheberrechtlich rechtswidrigen Internetseite zu sperren. Die erste Frage ist, ob § 1004 Abs. 1 BGB i.V.m. §§ 97 Abs. 1, 19a UrhG als Rechtsgrundlage für die Störerhaftung allein ausreicht. Dies hing damals nach den Ausführungen der Gerichte noch allein davon ab, ob die Sperrmaßnahmen in das Grundrecht des TK-Geheimnisses (Art. 10 Abs. 1 GG) eingreifen. Der Schutz des TK-Geheimnisses gemäß Art. 10 Abs. 1 GG muss angesichts der mittelbaren Drittwirkung und der Schutzpflicht des Gesetzgebers im Rahmen der Anwendung und Auslegung der Störerhaftung berücksichtigt werden. Das OLG Hamburg hat dies bejaht, weil Access-Provider bei der IP-, DNS- und URL-Sperre Kenntnis von den näheren Umständen, gegebenenfalls auch Inhalte, der Telekommunikation erlangen würden. Ein unmittelbarer Eingriff in den Schutzbereich des TK-Geheimnisses gemäß Art. 10 Abs. 1 GG liege damit vor. Die ungeschriebenen Grundsätze der Störerhaftung reichten im vorliegenden Fall nicht aus und für die Sperrmaßnahmen bedürfe es einer ausdrücklichen gesetzlichen Grundlage. Dagegen vertritt das OLG Köln die Meinung, dass eine solche Rechtsgrundlage nur für die URL-Sperre erforderlich sei. Der Schutzbereich des TK-Geheimnisses gemäß Art. 10 Abs. 1 GG soll keine schlichte Verhinderung der Kommunikation bei der IP-Sperre und DNS-Sperre umfassen. Bei der URL-Sperre ist aber nach der Auffassung des OLG Köln zu berücksichtigen, dass der Access-Provider zusätzlich die Kommunikationsinhalte vom Nutzer erlangt. Für die URL-Sperre ist danach eine ausdrückliche gesetzliche Grundlage erforderlich. Die Frage, ob es hierzu um den Grundsatz des Wesentlichkeitsvorbehalts geht und ob dieser Grundsatz wie im vorliegenden Fall zwischen Privaten gilt, wurde nicht von den früheren deutschen Rechtsprechungen handelt.

---

466 OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 80 ff.
467 OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 1002 ff.

Die zweite Frage ist, ob die Umgehungsmöglichkeiten der Sperrmaßnahmen der Effektivität der Sperrmaßnahmen entgegenstehen. Dies ist für die Beurteilung der Zumutbarkeit der Maßnahme entscheidend. Anders als das OLG Hamburg hat das OLG Köln die Effektivität der Sperrmaßnahmen bejaht, weil sie den Zugriff auf den illegalen Inhalten zumindest erschweren können und leichte Umgehungsmöglichkeiten nicht per se zur Ineffektivität der Maßnahme führen. Bei der letzten Frage, die auch für die Zumutbarkeit der Maßnahme wichtig ist, geht es um die Interessenabwägung zwischen Access-Provider und Urheberrechtsinhaber. Die frühen Rechtsprechungen haben dazu den unangemessenen finanziellen, technischen und organisatorischen Zusatzaufwand des Access-Providers und den wirtschaftlichen Vorteil für die Urheberrechtsinhaber betont.

2. Die Entwicklung der Rechtsprechung in der EU

In zwei grundlegenden Urteilen hat sich der EuGH zu der Störerhaftung geäußert.

a) „Scarlet/SABAM"-Entscheidung

Im ersten Fall (Scarlet/SABAM) wurde ein Zugangsanbieter durch eine gerichtliche Entscheidung dazu verpflichtet, die Übertragung von urheberrechtlich verbotenen Inhalten durch sog. P2P-Programme zu unterbinden. Ein Zugangsanbieter sei nach Ansicht des EuGH ein Vermittler, gegen den eine gerichtliche Anordnung auch zur Vorbeugung von urheberrechtlichen Verletzungen beantragt werden kann.[468] Die einzelnen gerichtlichen Anordnungen müssen allerdings verhältnismäßig sein. Hierzu ist eine Abwägung der betroffenen grundrechtlichen Positionen durchzuführen. Zur Abwägung zwischen dem Schutz des Urhebers nach Art. 17 Abs. 2 GrCH und anderen einschlägigen Interessen der betroffenen Teilnehmer kommen vor allem die unternehmerische Freiheit aus Art. 16 GrCH, der Schutz der personenbezogenen Daten aus Art. 8 GrCH sowie die Informationsfreiheit aus Art. 11 GrCH in Betracht. Angesichts der zeitlich unbegrenzten und kostenintensiven Einrichtung eines Filtersystems scheidet diese Möglichkeit bereits wegen des zu weitgehenden Eingriffs in die unternehmerische Freiheit gemäß Art. 16 GrCH aus.[469] Die umfangreiche Kenntnis aller Inhalte und IP-Adressen widerspricht des Weiteren dem Schutz der personenbezogenen Daten aus Art. 8

---

468 EuGH, Slg. 2011, I-12006 – Scarlett Extended, Rn. 30.
469 Ebd., Rn. 48.

GrCH.[470] Schließlich verstößt die Sperrmaßnahme – die Einführung des Filtersystems – auch gegen den Schutz der Informationsfreiheit aus Art. 11 GrCH, da sie unvermeidbar zu Kollateralschäden, einer Unterdrückung von zulässigen Inhalten führt.[471]

b) „UPC Telekabel"-Entscheidung

Im zweiten Fall („UPC Telekabel" und „Kino.to") wurde ein Zugangsanbieter vom Gericht aufgefordert, den Zugang zu Kino.to zu sperren.[472] In dem Vorabentscheidungsverfahren sah der EuGH zunächst, dass die für Sperrmaßnahmen einschlägige Norm des Art. 8 Abs. 3 RL 2001/29/EG auch Access-Provider umfasst, da zum besseren urheberechtlichen Schutz jeder, der zum Übertragen der Schutzgegenstände einen Beitrag geleistet hat (Access-Provider als „Vermittler"), die Verstöße verhindern soll.[473] Angesichts der Vorbeugungsfunktion der RL 2001/29/EG spielt es zudem keine Rolle, ob Kunden tatsächlich auf die Internetseite zugegriffen haben.[474] Dem Internetnutzer ist schließlich die Möglichkeit zum Rechtsschutz gewährt, wenn ihm die Sperrmaßnahmen des Access-Providers bekannt sind.[475]

Anders als im ersten Fall spricht sich der EuGH grundsätzlich für eine Vereinbarkeit von Sperrverfügungen gegenüber Access-Providern mit dem Unionsrecht aus. Die ergriffenen Sperrmaßnahmen sind zuerst hinreichend auf die Verhinderung oder zumindest Erschwerung der illegalen Zugriffe auf die Internetseite auszuweiten.[476] Da sich der Zugangsanbieter selber zur Sperrung entscheiden kann, verletzen die Sperrmaßnamen nicht unbedingt seine unternehmerische Freiheit aus Art. 16 GrCH.[477] Das Gleiche gilt auch für den Schutz der Informationsfreiheit aus Art. 11 GrCH, da die Nutzer gerichtlich gegen Sperren rechtmäßiger Inhalte vorgehen können.[478]

---

470 Ebd., Rn. 51.
471 Ebd., Rn. 52.
472 EuGH, U. v. 27.3.2014 - C-314/12; *Spindler*, GRUR 2014, 826 (826 f.).
473 EuGH, U. v. 27.3.2014 - C-314/12, Rn. 23 ff.
474 Ebd., Rn. 37 ff.; EuGH, Slg. 2011, I-12006; Spindler, GRUR 2014, 826 (828).
475 EuGH, U. v. 27.3.2014 - C-314/12, Rn. 57.
476 Ebd., Rn. 62 f.; OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 926.
477 EuGH, U. v. 27.3.2014 - C-314/12, Rn. 48 ff.
478 Ebd., Rn. 55 ff.

c) Stellungnahme zu den Entscheidungen des EuGH

aa) Vereinbarkeit mit EU-Richtlinien

Bei den zwei vorgestellten Urteilen des EuGH geht es um die Grundlage der vorbeugenden Unterlassungspflicht des Access-Providers. Der Access-Provider wird hierbei als Vermittler angesehen. Die Mitgliedstaaten sind in den urheberrechtlichen Richtlinien gemäß Art. 8 Abs. 3 InfoSoc-RL[479] und Art. 11 Satz 3 Enforcement-RL[480] verpflichtet, den Urheberrechtsinhabern gerichtliche Ansprüche gegen Vermittler zu ermöglichen. Der Access-Provider ist „an jeder Übertragung einer Rechtsverletzung im Internet zwischen einem seiner Kunden und einem Dritten zwingend beteiligt […], da er durch die Gewährung des Zugangs zum Netz diese Übertragung möglich macht“[481]. Deshalb wird er als „Vermittler“ angesehen.[482] Dies entspricht den Haftungsregelungen der E-Commerce-Richtlinie. Gemäß Art. 12 Abs. 1 E-Commerce-Richtlinie haftet der Access-Provider grundsätzlich nicht für die übermittelten Inhalte.[483] In besonderen Fällen kann ein Gericht oder eine Verwaltungsbehörde gemäß Art. 12 Abs. 3 E-Commerce-Richtlinie zum Abstellen oder Verhindern einer Rechtsverletzung dem Access-Provider entsprechende Maßnahmen auferlegen.[484] Ausgeschlossen ist gemäß Art. 15 Abs. 1 E-Commerce-Richtlinie aber die allgemeine Pflicht für Access-Provider, dass diese die übermittelten Informationen zeitlich unbefristet und anlasslos zu überwachen.[485] Ein Filtersystem, mit dem jedes rechtswidrige Angebot gesperrt werden kann, ist daher unionsrechtlich nicht zulässig.[486] Die gerichtliche Sperranordnung bezogen auf einen bestimmten Inhalt (IP-Adresse, URL, DNS) führt aber nicht zu einer allgemeinen Überwachungspflicht der Zugangsanbieter und ist mit Art. 15 Abs. 1 RL 2000/31/EG vereinbar.

---

479 RL 2001/29/EG des Europäischen Parlaments und des Rates v. 22.5.2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl. EG Nr. L 167 v. 22.6.2001, 10 ff.

480 RL 2004/48/EG des Europäischen Parlaments und des Rates v. 29.4.2004 zur Durchsetzung der Rechte des geistigen Eigentums, ABl. EU Nr. L 195 v. 2.6.2004, 16 ff.

481 EuGH, 27.3.2014 - C-314/12, Rn. 32; EuGH, Slg. 2009, I-1230.

482 EuGH, U. v. 27.3.2014 - C-314/12, Rn. 23 ff.; EuGH, Slg. 2011, I-12006, Rn. 30; Kritik zu dem uferlosen Begriff des Vermittlers, siehe *Marly*, GRUR 2014, 468 (473).

483 Dienstanbieter gemäß Art. 12 Abs. 1 E-Commerce-Richtlinie umfasst Access-Provider, siehe *Grabitz/Hilf/Nettesheim*, Art. 12, Rn. 2;

484 47. Begründung zu Art. 12 Abs. 1 E-Commerce-Richtlinie; *Grabitz/Hilf/Nettesheim*, Art. 12, Rn. 10.

485 EuGH, U. v. 24.11.2011 - C-70/10.

486 EuGH, U. v. 16.2.2012 - C-360/10, Rn. 38.

bb) Grundrechtskonformität

Bei der Frage, ob die gerichtliche Sperranordnung gegen EU-Grundrechte verstößt, vertritt der EuGH in zwei Rechtsprechungen die Meinung, dass der Grundsatz der Verhältnismäßigkeit bei der Abwägung zwischen den Interessen des Urhebers, der Access-Provider und Nutzer eingehalten werden muss.[487] Betroffen sind insbesondere für Access-Provider die unternehmerische Freiheit aus Art. 16 GrCH, für Nutzer der Schutz der personenbezogenen Daten aus Art. 8 GrCH sowie die Informationsfreiheit aus Art. 11 GrCH. Nicht erwähnt werden in dieser Aufzählung aber die Meinungs-, die Medienfreiheit des Inhalteanbieters sowie der Schutz des Telekommunikationsgeheimnisses für Nutzer.[488] Anders als im Fall „Scarlet/SABAM" stand der EuGH im Fall „UPC Telekabel" mehr auf der Seite des Urheberrechtsinhabers. Die angeführten Gründe des EuGH sind in vielen Punkten vertretbar. Zum einen ist der Zugangsanbieter gegenüber dem Content- oder Hosting-Anbieter subsidiär heranzuziehen.[489] Soweit der Urheberrechtsinhaber alle anderen zumutbaren Maßnahmen ergriffen hat, kann der Zugangsanbieter Adressat einer Sperrverfügung sein. Gleichzeitig dürfen die Sperrmaßnahmen nicht unverhältnismäßig in die Grundrechte des Zugangsanbieters und Nutzers eingreifen und dem Zugangsanbieter müssen Möglichkeiten zum Rechtsschutz gewährt werden.[490] Zu kritisieren ist allerdings, dass nach der Meinung des EuGH dem Provider bei der Wahl der „streng zielorientierten" Sperrmaßnahmen überlassen wird, welche Maßnahme er genau ergreifen möchte.[491] Da unterschiedliche Sperrtechniken unterschiedliche Vor- und Nachteile für sowohl Urheberrechtsinhaber, als auch Nutzer und Anbieter haben, besteht durch eine unklare Regelung zu den zu wählenden Sperrtechniken eine Gefahr für die Rechtssicherheit und den Grundsatz des Gesetzesvorbehalts.[492] Welche Sperrtechnik das Gericht dem Zugangsanbieter auferlegt, muss folglich klargestellt werden. Noch zu kritisieren ist, dass der EuGH bei der Interessenabwägung das Grundrecht auf Achtung der Kommunikation nach Art. 7 GrCH nicht erwähnt.[493] Mit diesem in den deutschen Entscheidungen wichtigen Streitpunkt setzt sich etwa der BGH vertiefend auseinander.[494]

---

487 EuGH, Urt. v. 27.3.2014 – C-314/12, Rn. 53.
488 *Spindler*, GRUR 2014, 826 (829).
489 EuGH, Urt. v. 27.3.2014 – C-314/12, Rn. 53.
490 Ebd., Rn. 54, 56 f.
491 EuGH, Urt. v. 27.3.2014 – C-314/12, Rn. 55.
492 *Spindler*, GRUR 2014, 826 (829).
493 Ebd., 826 (830).
494 BGH, U. v. 26.11.2015 - I ZR 3/14, Rn. 57.

3. Richtungsänderung durch neue Netzsperren-Urteile des BGH

Der EuGH hat die Sperrverfügungen gegenüber Access-Providern nach den europäischen Vorgaben im „UPC Telekabel"- oder „Kino.to"-Urteil unter gewissen Umständen goutiert. Als Mitgliedstaat muss auch Deutschland die europäischen Grundrechte beachten und muss das nationale Recht richtlinienkonform und in Einklang mit den EU-Grundrechten auslegen.[495] Im November 2015 hat der BGH zwei entscheidende Urteile gesprochen. In der Reihe von Rechtsstreitigkeiten wegen urheberrechtlicher Sperranordnungen wurde hauptsächlich über die Störerhaftung, insbesondere über die Zumutbarkeit als deren Kerntatbestand, diskutiert.

a) Kein Eingriff in den Schutzbereich des TK-Geheimnisses durch Internetsperren

aa) Bestätigung der Auffassung des OLG Köln

Der BGH hält einen Eingriff in den Grundrechtsschutz des Telekommunikationsgeheimnisses nach Art. 10 Abs. 1 GG für nicht gegeben.[496] Hierzu folgt der BGH der Meinung, dass Art. 10 Abs. 1 GG nur die Individualkommunikation und nicht die Kommunikation in öffentlichen Foren schütze.[497] Außerdem sei die technische Kommunikationsweise nicht entscheidend, weil der Schutzzweck des Art. 10 Abs. 1 GG den Schutz der Privatheit umfasse.[498] Im vorliegenden Fall erfolgt der Abruf der urheberrechtswidrigen Inhalte zwar mittels individueller Kommunikationsverbindung, die Angebote selbst sind aber öffentlich. Die Privatsphäre der beiden Kommunikationspartner sei somit nicht betroffen. Zudem zitiert der BGH hier die Auffassung des BVerfG, nach der die Sperrmaßnahmen nicht in den sachlichen Schutzbereich des Art. 10 Abs. 1 GG eingreifen, weil die Kommunikationsvorgänge nur „technikbedingt erfasst und anonym, spurenlos und ohne Erkenntnisinteresse für die Behörden umgehend ausgesondert" werden,[499] sodass sie ohne Gefährdung der Privatsphäre nur die Kommunikationsverhinderung herbeiführt. Sofern es sich um „die Erfassung und Verwendung … [der für die] Herstellung der Kommunikationsverbindung" notwendigen Daten handelt, sei dies auch

---

495 EuGH, U. v. 29.1.2008 - C-275/06, Rn. 68; EuGH, U. v. 24.11.2011 - C-70/10, Rn. 46; EuGH, U. v. 16.2.2012 - C-360/10, Rn. 44, 48; EuGH, Urt. v. 27.3.2014 – C-314/12, Rn. 46.

496 BGH, U. v. 26.11.2015 - I ZR 3/14, Rn. 55 ff.

497 Ebd., Rn. 55.

498 Ebd., Rn. 55.

499 Ebd., Rn. 56; BVerfGE 100, 313 (366); 107, 299 (328).

gemäß § 88 Abs. 3 Satz 1 TKG nicht zu beanstanden.[500] Der BGH hat folglich die Auffassung des OLG Hamburg nicht vertreten und sich der Auffassung des OLG Köln angeschlossen. § 88 Abs. 3 Satz 1 verbietet dem TK-Dienstanbieter die Kenntniserlangung über Kommunikationsinhalte und deren nähere Umstände. Soweit für die Geschäftszwecke und den Schutz der technischen Systeme erforderlich, können bzw. müssen hierfür Daten zur Kenntnis genommen werden. Aus Sicht des BGH ist die Kommunikationsverhinderung Teil der Herstellung der jeweiligen Verbindung und dient damit noch den Geschäftszwecken des Zugangsanbieters. Kommt es hierbei zur Kenntniserlangung von Kommunikationsinhalten und näheren Umständen der Kommunikation, werde nicht gegen § 88 Abs. 3 Satz 1 verstoßen.[501] Da dies nicht über den Geschäftszweck sowie Schutzzweck der technischen Systeme im Sinne vom § 88 Abs. 3 Satz 1 TKG hinausgeht, verstößt es auch ohne spezielle gesetzliche Grundlage nicht gegen § 88 Abs. 3 Satz 2 TKG.

bb) Stellungnahme

Eine Differenzierung zwischen unterschiedlichen Sperrtechniken sowie diesbezügliche Grundrechtsprüfungen des BGH sind zu begrüßen. Die Annahme, dass die Privatheit als Schutzzweck des Art. 10 Abs. 1 GG nicht von der Sperrung gefährdet ist, ist auch zutreffend. Eine individuelle Kommunikationsverbindung liegt dabei nicht vor, weil die abzurufende Webseite sowie die darauf angebotenen Inhalte öffentlich sind.[502] Das BVerfG hat in der Vorratsdatenspeicherung-Entscheidung zwar erwähnt: „Da eine Unterscheidung zwischen Individual- und Massenkommunikation ohne eine der Schutzfunktion des Grundrechts zuwiderlaufende Anknüpfung an den Inhalt der jeweils übermittelten Information nicht möglich ist, ist bereits in der Speicherung der den Internetzugang als solchen betreffenden Daten ein Eingriff zu sehen, auch wenn sie Angaben über die aufgerufenen Internetseiten nicht enthalten."[503] Es handelt sich vorliegend aber nicht um Vorratsdatenspeicherung. Durch die IP- und DNS-Sperre werden nur die Kommunikationsvorgänge „technikbedingt erfasst und anonym, spurenlos und ohne Erkenntnisinteresse für die Behörden umgehend ausgesondert"[504]. Nur die Daten, die ohnehin zur Herstellung der Kommunikationsverbindung benötigt werden,

---

500 BGH, U. v. 26.11.2015 - I ZR 3/14, Rn. 56.
501 Ebd., Rn. 56.
502 *Czychowkski*, MMR 2004, 514 (518); *Durner*, ZUM 2010, 833 (840 f.); *Billmeier*, 182 ff., 273 f.; *Kropp*, 162.
503 BVerfGE 125, 260 (311).
504 BGH, U. v. 26.11.2015 - I ZR 3/14, Rn. 56; BVerfGE 100, 313, 366; 107, 299, 328.

werden vom Access-Provider erfasst und werden „unmittelbar nach der Erfassung technisch wieder anonym, spurenlos und ohne weitergehendes Erkenntnisinteresse gelöscht".[505] Der BGH hat sich folglich zutreffend auf den Schutzzweck des Art. 10 Abs. 1 GG konzentriert und die technische Kommunikationsverhinderung vom Schutzbereich des Art. 10 Abs. 1 GG ausgeschlossen.

b) Wesentlichkeitsvorbehalt nicht berührt

aa) Zum Grundsatz des Wesentlichkeitsvorbehalts

Bei der Zugangssperrung sind aus verfassungsrechtlicher Sicht verschiedene Grundrechtspositionen der Betroffenen zu berücksichtigen, wie z.B. die Berufsfreiheit (Art. 12 Abs. 1 GG) und die Eigentumsfreiheit (Art. 14 Abs. 1 GG) für Access-Provider, die Informationsfreiheit (Art. 5 Abs. 1 Satz 1 Halbsatz. 2 GG) für Nutzer sowie die Meinungsfreiheit (Art. 5 Abs. 1 Satz 1 Halbsatz. 1 GG) für Inhalts- und Host-Provider. Die Herausforderung liegt allerdings nicht nur in der Prüfung der jeweiligen Grundrechte, sondern bereits in der Beachtung grundrechtlicher Wertungen im Privatrecht. Das OLG Hamburg und das OLG Köln haben in den Entscheidungen nur auf die mittelbare Drittwirkung sowie staatliche Schutzpflicht *hingewiesen,* ohne sich näher damit auseinanderzusetzen. Der Eingriff in grundrechtliche Positionen könnte dazu führen, dass die Sperrung gegenüber Zugangsanbietern gegen den Wesentlichkeitsvorbehalt verstößt.[506] Dieser aus Art. 20 Abs. 3 GG hergeleitete Grundsatz verlangt eine Regelung durch den Gesetzgeber, wenn es sich um wesentliche Aspekte, insbesondere um Grundrechtseingriffe, handelt.[507] Aufgrund der Grundrechtsbeeinträchtigungen ist auch der Wesentlichkeitsvorbehalt bei Internetsperren zu beachten.

bb) Zutreffende Subsumtion des BGH

Im vorliegenden Fall hat der BGH zutreffend die Anwendbarkeit des Wesentlichkeitsvorbehalts ausgeschlossen, weil er „nur für das Verhältnis zwischen Staat und

---

505 BGH, U. v. 26.11.2015 - I ZR 3/14, Rn. 56.

506 LG Hamburg, U. v. 12.3.2010 - 308 O 640/0, Rn. 47 ff.; OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 91 ff.; LG Köln, U. v. 31.8.2011 - 28 O 362/10, Rn. 74.

507 *Kokott*, in: HGR, Bd. I, § 22 Rn. 74 ff.; *Lerche*, in: HGR, Bd. I, § 62 Rn. 54 ff.; *Sachs*, in: Sachs, GG, Art. 20 Rn. 117; *Dreier*, in: Dreier, GG, Vorb. Rn. 136.

Bürgern“ gilt.[508] Die Wesentlichkeitstheorie dient vor allem der Kontrolle im Rahmen „der Delegation von Rechtssetzung vom Parlament auf die Exekutive“,[509] während bei „gleichgeordneten Grundrechtsträgern“ die rechtsprechende Gewalt selbst die Rechtsgrundlagen zu finden hat.[510] Bei der Störerhaftung zwischen Privaten ist diese Aufgabe dem Gericht überlassen. §§ 1004 BGB i.V.m. §§ 97 Abs. 1, 19a UrhG sind als Anspruchsgrundlage für urheberrechtliche Störungen ausreichend.[511] Ein Verstoß gegen den Wesentlichkeitsvorbehalt und die Erforderlichkeit einer ausdrücklichen gesetzlichen Grundlage ist somit nicht gegeben.

c) Effektivität der Sperrmaßnahmen – Relevanz von Umgehungsmöglichkeiten und der Gefahr des Overblocking

Umgehungsmöglichkeiten sind weder für Nutzer noch für Betreiber entscheidende Faktoren für die Ermittlung der Effektivität von Sperrmaßnahmen, weil die vom Access-Provider ergriffenen Maßnahmen „die unerlaubten Zugriffe auf die Schutzgegenstände verhindern oder zumindest erschweren und die Internetnutzer [...] zuverlässig [vom Zugriff] abhalten“.[512] Es wird angenommen, dass ein illegaler Zugriff auf urheberrechtliche Angebote durch Internetsperren effektiv unterbunden wird. Mit einer Umgehung dieser Sperren ist eher nicht zu rechnen bzw. eine solche fällt nicht allzu sehr ins Gewicht.[513] Darüber hinaus ist die Schutzlosigkeit der Inhaber von Urheberrechten ebenfalls zu berücksichtigen.[514] Die von der früheren Rechtsprechung vertretene Meinung, dass die Sperrung nicht zumutbar ist, weil auch rechtmäßige Inhalte von den möglichen Sperrmaßnahmen höchstwahrscheinlich betroffen und damit die Rechte Dritter verletzt wären („Overblocking“), wird vom BGH nicht geteilt. Der BGH verlangt zutreffend nähere Feststellungen zur Betroffenheit legaler Inhalte, um zum gleichen Ergebnis wie das OLG Hamburg zu kommen.[515] Eine allgemeine Feststellung der Unverhältnismäßigkeit von Sperren wegen betroffener legaler Inhalte wäre nicht richtig, weil die Löschung von legalen Inhalten in geringem Umfang nicht unbedingt zur Unzumutbarkeit der urheberrechtlichen Schutzmaßnahmen führt.[516] Es ist somit

---

508 BGH, U. v. 26.11.2015 - I ZR 3/14, Rn. 59.
509 Ebd., Rn. 59.
510 Ebd., Rn. 60.
511 Ebd., Rn. 61.
512 EuGH, Slg. 2014, 192, Rn. 62 – UPC Telekabel Wien.
513 BGH, U. v. 26.11.2015 - I ZR 174/14, Rn. 48.
514 Ebd., Rn. 49.
515 BGH, U. v. 26.11.2015 - I ZR 3/14, Rn. 42 ff.
516 Ebd., Rn. 44 ff.

eine Gesamtbeachtung des Gewichts der rechtmäßigen Inhalte im Vergleich zum Gewicht der unrechtmäßigen Inhalte, zu denen jeweils der Zugang gesperrt wurde, vorzunehmen.[517]

4. Änderung der §§ 7 und 8 TMG und die BGH-Entscheidung „Dead Island"

Im Jahre 2017 wurde das TMG novelliert. Hierbei spielten die bis hierhin dargestellten Entwicklungen eine entscheidende Rolle. Es wurde nun die Möglichkeit ins Gesetz geschrieben, aus urheberrechtlichen Schutzgründen gegen Access-Provider vorzugehen. Gleichzeitig wurde aber auch mit dem Ansatz der Störerhaftung gebrochen. Dieser soll in Zukunft nicht mehr Anwendung finden. Die entscheidenden Regelungen sind kurz vorzustellen (a)). Es erging kurz nach der Gesetzesänderung eine Entscheidung des BGH zu den neuen Normen. Hierbei formulierte das Gericht Vorgaben zur Auslegung (b)).

a) TMG-Novelle

§ 8 Abs. 1 S. 2 TMG sieht nun vor, dass Diensteanbieter, sofern sie – insbesondere Access-Provider[518] – nicht verantwortlich sind, nicht wegen einer rechtswidrigen Handlung eines Nutzers auf Schadensersatz oder Beseitigung oder Unterlassung einer Rechtsverletzung in Anspruch genommen werden können. In der alten Fassung war eine solche Regelung nicht vorhanden. Da der Haftungsausschluss die fehlende Verantwortlichkeit voraussetzt, ist der oben dargestellte Streitstand zur Anwendung der Störerhaftung nicht ausdrücklich ad acta gelegt. Der Gesetzesbegründung zufolge ist diese Norm jedoch als Absage an die Störerhaftung der Access-Provider zu verstehen.[519] Dies gilt jedoch nur für zivilrechtliche Ansprüche. In Bezug auf öffentlich-rechtliche Sperrverfügungen gilt dieser Ausschluss nicht. Auf die polizei- und ordnungsrechtliche Generalklausel gestützt können nach den Prinzipien des Störerbegriffs auch weiterhin Sperrmaßnahmen gegenüber Access-Providern verfügt werden.[520]

---

517 Ebd., Rn. 44 ff.

518 Die Bedeutung dieser Vorschrift für Access-Provider hebt hervor *Paal* BeckOK Informations- und Medienrecht, TMG, § 8 Rn. 25 b.

519 BT-Drs. 18/12202, 11

520 *Paal*, BeckOK Informations- und Medienrecht, TMG, § 8 Rn. 25 d; *Spindler*, Spindler/Schmitz, TMG, § 8 Rn. 19.

Eng mit der Regelung des § 8 Abs. 1 S. 2 TMG hängt der neue § 7 Abs. 4 S. 1 TMG zusammen.[521] Dieser sieht vor:

„Wurde ein Telemediendienst von einem Nutzer in Anspruch genommen, um das Recht am geistigen Eigentum eines anderen zu verletzen und besteht für den Inhaber dieses Rechts keine andere Möglichkeit, der Verletzung seines Rechts abzuhelfen, so kann der Inhaber des Rechts von dem betroffenen Diensteanbieter nach § 8 Absatz 3 die Sperrung der Nutzung von Informationen verlangen, um die Wiederholung der Rechtsverletzung zu verhindern. Die Sperrung muss zumutbar und verhältnismäßig sein."

Bei den Diensteanbietern nach § 8 Abs. 3 TMG handelt es sich um Diensteanbieter, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen (WLAN-Anbieter). § 7 Abs. 4 S. 1 TMG Regelung beinhaltet nun einen ausdrücklichen Anspruch auf Netzsperren gegenüber diesen Anbietern.[522] Der Bundesgesetzgeber reagiert hiermit auf die oben herausgearbeiteten Vorgaben des EuGH. Dieser Anspruch ist als Ersatz für die richterrechtlichen Anpassungen der Störerhaftung gegenüber Access-Providern im Rahmen von Unterlassungsansprüchen wegen Urheberrechtsverstößen zu verstehen.[523] Es sind auch hier, wie in der Norm explizit geregelt, Verhältnismäßigkeit und Zumutbarkeit der Maßnahme zu beachten. Weiterhin sind Access-Provider nur subsidiär in Anspruch zu nehmen.[524] Es ist aber als Kernaussage festzuhalten, dass für das Urheberrecht nun eine spezielle Regelung für Sperrmaßnahmen gegen Access-Provider besteht. Außerhalb des Urheberrechts, insbesondere des Gefahrenabwehrrechts, sind oben herausgearbeiteten Grundsätze zur Störereigenschaft weiterhin anzuwenden.[525]

b) „Dead Island"-Entscheidung des BGH

Im Urteil „Dead Island" aus Juli 2018 machte der BGH grundlegende Aussagen zu den neuen Regelungen.[526] Der Sachverhalt bestand darin, dass der Nutzungsberechtigte des Online-Spiels „Dead Island" gegen das illegale Herunterladen des Spiels auf Sharing-Plattformen vorging. Hierzu konzentrierte sich der Nutzungs-

---

521 *Paal*, BeckOK Informations- und Medienrecht, TMG, § 8 Rn. 25 a.
522 *Paal*, BeckOK Informations- und Medienrecht, TMG, § 8 Rn. 25 b.
523 BGH, GRUR 2018, 1044 (1048) – Dead Island.
524 *Sesing/Baumann*, MMR 2017, 583 (587).
525 *Paal*, BeckOK Informations- und Medienrecht, TMG, § 8 Rn. 25 d; *Spindler*, Spindler/Schmitz, TMG, § 8 Rn. 19.
526 BGH, GRUR 2018, 1044 – Dead Island.

berechtigte vornehmlich auf den Zugangsanbieter. In den ersten beiden Instanzen[527] wurde eine Verantwortlichkeit des Zugangsanbieters nach den Grundsätzen der Störerhaftung bejaht. In Ansehung des § 8 Abs. 1 S. 2 TMG kann dies aber nicht mehr aufrechterhalten werden. Dort ist die Haftung des Zugangsanbieters positiv ausgeschlossen. Im „Dead Island"-Fall wurden die Urteile der Instanzgerichte somit aufgehoben. Der BGH verwies die Entscheidung aber zurück an das OLG mit dem Hinweis auf die Einschlägigkeit des Anspruchs nach § 7 Abs. 4 TMG.[528] Mit diesem könne der Kläger sein Klageziel erreichen. Er muss nun positiv beantragen, dass die Informationen durch den Zugangsanbieter gesperrt werden. Beim oben beschriebenen ehemaligen Unterlassungsanspruch war es aus Gründen der Gefährdungshaftung nicht notwendig, dass der Kläger beschreibt, wie der Beklagte dem Begehren entspricht. Dies hat sich nun mit § 7 Abs. 4 TMG geändert. Der Kläger muss positiv formulieren, was er beantragt.[529] Der Urheberrechtsinhaber kann eine *Netzsperre* verlangen.[530] Der BGH stellt auch klar, dass die Begrenzung auf WLAN-Anbieter in § 7 Abs. 4 TMG den Anforderungen des EuGH[531] nicht gerecht werde, dass Maßnahmen gegen Mittelpersonen völlig entfallen. Der Anspruch ist vielmehr auch auf andere Vermittler eines Zugangs zu erstrecken.[532] Ansonsten wäre der Sperranspruch nach § 7 Abs. 4 TMG insoweit ungeeignet, den Ausschluss des Unterlassungsanspruchs zu kompensieren.[533]

5. Zwischenergebnis

Viel ausführlicher als im Wettbewerbsrecht haben sich die deutschen Gerichte und zuletzt auch der deutsche Gesetzgeber mit der Störerhaftung des Access-Providers im Urheberrecht auseinandergesetzt. In der Revision hat der BGH tendenziell eine Anlehnung an den EuGH im Fall „kino.to"[534] sowie an das OLG Köln[535] vorgenommen. Folglich entschied der BGH, dass Sperrverfügungen gegenüber Access-

---

527 LG Düsseldorf, U. v. 13.1.2016 - 12 O 101/15; OLG Düsseldorf, U. v. 16.3.2017 - I-20 U 17/16.

528 BGH, GRUR 2018, 1044 (1050) – Dead Island.

529 BGH, GRUR 2018, 1044 (1050) – Dead Island; zu den Folgen dieses Wechsels vom Unterlassungs- zum Leistungsanspruch für den einstweiligen Rechtsschutz, siehe *Rehart*, MMR 2018, 784.

530 Zur spezifischen Ausgestaltung dieser Sperre *Grisse*, MMR 2018, 649 (654).

531 EuGH, Slg. 2011, I-12006 – Scarlett Extended, Rn. 31; EuGH, U. v. 27.3.2014 - C-314/12, Rn. 31.

532 BGH, GRUR 2018, 1044 (1047 f.) – Dead Island; *Spindler*, GRUR 2018, 1012 (1014).

533 BGH, GRUR 2018, 1044 (1048) – Dead Island.

534 EuGH, U. v. 27.3.2014 - C-314/12.

535 OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11

Providern auf Grundlage der Störerhaftung grundsätzlich zulässig sind. Access-Provider sind hiernach allerdings subsidiär gegenüber den Inhalts- und Host-Providern in Anspruch zu nehmen.[536]

Im Zentrum bei Sperren aufgrund urheberrechtlicher Verstöße wegen Störereigenschaft stand die Streitfrage nach dem Eingriff der Sperrmaßnahmen in das Grundrecht des TK-Geheimnisses. Nach der Entscheidung des OLG Hamburg bedurfte die Sperrmaßnahme einer spezialgesetzlichen Grundlage, weil *alle* in Frage kommenden Sperrtechniken des Access-Providers in Art. 10 GG eingreifen.[537] Das OLG Köln hatte zutreffend die Erforderlichkeit einer solchen Rechtsgrundlage bei der IP-Sperre und DNS-Sperre verneint und nur bei der URL-Sperre angenommen.[538] Es war dabei entscheidend, ob die im Rahmen der Kommunikationsverhinderung erlangte Kenntnis über nähere Umstände des Kommunikationsvorgangs auch dem Schutzbereich des Art. 10 GG unterfallen. Da der Vermittler mit der IP-Sperre und DNS-Sperre keine näheren Umstände als im normalen Geschäft erlangt, umfasst der Schutzbereich des Art. 10 GG keine solche schlichte Verhinderung der Kommunikation. Mit der URL-Sperre erlangt der Access-Provider allerdings zusätzlich die Inhalte des Datenpakets vom Nutzer, sodass sie in den Schutz des TK-Geheimnisses eingreift. Der BGH ging noch weiter als das OLG Köln. Der BGH hatte den Schutzzweck der Privatheit des Art. 10 Abs. 1 GG betont und zutreffend festgelegt, dass Art. 10 Abs. 1 GG nur die Individualkommunikation und nicht die in öffentlich zugänglichen Online-Kommunikationsräumen stattfindende Kommunikation schützt. Außerdem greifen IP- und DNS- sowie URL-Sperre nicht in das Grundrecht des TK-Geheimnisses aus Art. 10 Abs. 1GG ein, weil hierbei nur eine schlicht *technische* Kommunikationsverhinderung gegeben ist.

Diese Frage nach dem Eingriff in das Grundrecht war an dieser Stelle eng mit dem Grundsatz des Wesentlichkeitsvorbehalts verbunden. Es handelt sich hier darum, ob der Grundsatz des Wesentlichkeitsvorbehalts auch zwischen Privaten gilt. Der Verstoß gegen den Wesentlichkeitsvorbehalt könnte bei der Beurteilung der Störerhaftung des Zugangsanbieters auch dazu führen, dass die Sperrung rechtlich

---

536 *Heidrich/Heymann*, MMR 2016, 370 (370); *Leistner*, JZ 2014, 846 (856).

537 OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 100; OLG Hamburg, U. v. 22.12.2010 - 5 U 36/09, Rn. 66.

538 OLG Köln, U. v. 18.7.2014 - I-6 U 192/11, 6 U 192/11, Rn. 936 ff.

unmöglich oder unzumutbar ist.[539] Diese Fragen wurden in den Entscheidungen vom OLG Köln und OLG Hamburg zwar erwähnt, aber nicht vertiefend diskutiert, und erst vom BGH konkreter behandelt. Der BGH lehnte die Anwendbarkeit des Grundsatzes des Wesentlichkeitsvorbehalts auf das Privatrechtsverhältnis ab, da dieser nur im Verhältnis von Staat zu Bürger gilt. Ob der Eingriff in Form der Sperrung gerechtfertigt war, bestimmt sich vielmehr nach einer Grundrechtsabwägung zwischen der Freiheit des Inhabers des Urheberrechts, der Berufsfreiheit des Zugangsanbieters und des von der Sperrung Betroffenen.[540] Der BGH schloss sich hier der Meinung des EuGH im „UPC Telekabel"-Fall an, dass den Anträgen der Klägerinnen angesichts der „strengen Zielorientierung" der Sperrmaßnahmen sowie des geringen Umfangs der Kollateralschäden nachzukommen ist.[541] Auch in Bezug auf die Effektivität der Sperrmaßnahmen folgt der BGH den Feststellungen von EuGH im Fall „Kino.to" und vom OLG Köln im Fall „Goldesel". Die Umgehungsmöglichkeiten, so seinerzeit die Einschätzung des BGH, stehen der Effektivität der Sperrmaßnahmen nicht entgegen, weil die Sperrungen den Zugang zu den illegalen Inhalten zumindest erschweren.

Diese an den Grundrechten entwickelte Rechtsprechung ist nun durch die TMG-Novelle nicht mehr aktuell. Es besteht nun in § 7 Abs. 4 TMG ein eigener Anspruch gegen den Access-Provider. Dieser ähnelt unterm Strich den von der Rechtsprechung herausgearbeiteten Anforderungen an die urheberrechtliche Störerhaftung, wie sie von den Gerichten entwickelt wurde. Die Darstellung der Rechtsprechungsentwicklung hat gezeigt, dass die Inanspruchnahme von Access-Providern stark grundrechtlich geprägt ist. Dies ist eine wichtige Erkenntnis für die Zwecke dieser Arbeit. Nicht zu vernachlässigen ist, dass natürlich auch die Gesetzesänderung im TMG Ausdruck des grundrechtlichen Schutzanspruchs ist.

---

539 LG Hamburg, U. v. 12.11.2008 - 308 O 548/08, Rn. 33 ff.; LG Köln, U. v. 31.8.2011 - 28 O 362/10, Rn. 76.

540 BGH, U. v. 26.11.2015 - I ZR 174/14, Rn. 55.

541 Ebd., Rn. 55; EuGH, Slg. 2014, 192, Rn. 56 ff. – UPC Telekabel Wien.

G. Zusammenfassung

I. Öffentlich-rechtliche Inanspruchnahme

Beim Thema der Internetsperren in Deutschland kommen sowohl im öffentlichen Recht als auch im Zivilrecht verschiedene Regelungsansätze zum Einsatz. Die „Düsseldorfer Sperrverfügungen“ haben eine Tür zu öffentlichen Sperrmaßnahmen geöffnet, die von den zuständigen Gerichten unterstützt wurden. Das ZugErschwG wurde zwar aufgehoben. Es mangelte aber nicht an der gesetzlichen Bestimmtheit und es lag auch kein Verstoß gegen die Verhältnismäßigkeit beim Eingriff in Grundrechte vor. § 1 Abs. 2 Satz 1 ZugErschwG hat bereits gegenüber dem Löschen illegaler Inhalte die Subsidiarität der Sperrverfügung gegen Access-Provider bestimmt. Im Vergleich zum mitunter unvermeidbaren Overblocking ist das Interesse des Kindeswohls höher zu gewichten. Bei der Blockade illegaler Glücksspiele im Internet kommt neben Zugangsanbietern auch eine Sperranordnung gegenüber den Content-Anbietern in Betracht. Anhand zuverlässiger Geolokation können in Deutschland ansässige Content-Anbieter ermittelt werden. Diese sind dann vorrangig Adressaten von Löschverfügungen. Bei der Sperrverfügung gegenüber Access-Providern in diesem Bereich ist jedoch die Voraussetzung der Ermächtigungsgrundlage nicht erfüllt. Dem Access-Provider wird es in der Regel am Vorsatz mangeln, den Betreibern von illegalen Online-Glücksspielangeboten Hilfe zu leisten. Damit ist keine Verantwortlichkeit i.S.d. Ermächtigungsgrundlage im GlüStV gegeben. Zudem sind sie auch aus dem Grunde keine richtigen Adressaten, da die *Untersagung* i.S.v. § 9 Abs. 1 Satz 3 Nr. 5 GlüStV a.F. nur von Content- und Hostanbieter vorgenommen werden kann.

II. Zivilrechtliche Inanspruchnahme

Im Zivilrecht ist die Frage nach der Zulässigkeit der Sperranordnung gegenüber Access-Providern vertieft behandelt worden. Während eine klare Ablehnung der Sperranordnung gegen Access-Provider im Wettbewerbsrecht herausgestellt wurde, führten zwei jüngere Urteile des BGH eine Wende in dieser Hinsicht herbei, die schließlich in der Novelle des TMG mündete. Der BGH ist der Auffassung des EuGH und des OLG Köln gefolgt. Sperrmaßnahmen seien danach auf Grundlage der Störerhaftung grundsätzlich zulässig. Access-Provider seien den Inhalts- und Host-Provider gegenüber aber subsidiär in Anspruch zu nehmen. Durch private Sperrmaßnahmen sei kein Eingriff in das Telekommunikationsgeheimnis gegeben.

Der Grundsatz des Wesentlichkeitsvorbehalts gelte nicht zwischen Privaten. Die Umgehungsmöglichkeiten stünden der Effektivität der Sperrmaßnahmen nicht entgegen. Man könne davon ausgehen, dass die Sperrtechnik die urheberrechtlichen Rechtsgüter effektiv schützt. Diese Auffassung hat den Gesetzgeber maßgeblich dazu bewegt, die Inanspruchnahme von Access-Providern gesetzlich zu verankern. Die Inanspruchnahme als Störer war nicht kodifiziert und war sozusagen Richterrecht. Nun ist die Inanspruchnahme von Access-Providern wegen Urheberrechtsverstößen auf den von ihnen zur Verfügung gestellten Verbindungen gesetzlich geregelt.

Um die Rechtsdurchsetzung in sozialen Netzwerken zu verbessern, wurde das NetzDG kurz vor der letzten Bundestagswahl erlassen. Das Compliance-Modell des NetzDG ist zu begrüßen. Das NetzDG ist insofern von Bedeutung für das Thema dieser Arbeit, als dass hierdurch ein neuer Ansatz im Umgang mit rechtswidrigen Inhalten verfolgt wird. Es beinhaltet nicht die Implementierung von neuen im Löschpflichten. Diese ergeben sich bereits aus den allgemeinen Gesetzen. Der Gesetzgeber gibt mit dem NetzDG Anreize, den Löschverpflichtungen schneller nachzukommen. Dies ist insofern ein Ansatz, der auch auf andere Bereiche übertragbar ist: von staatlicher Seite mehr Druck auf die Internetdiensteanbieter auszuüben. Auf Sperren gegenüber Access-Providern ist das Modell allerdings nur bedingt unmittelbar übertragbar, da sie nur subsidiär Adressaten von Sperrverfügungen sind. Es kann aber in Deutschland die Tendenz ausgemacht werden, dass der Staat vermehrt sicherstellen will, dass das Recht im Internet durchgesetzt wird. Hierbei könnten zu einem gewissen Grad auch Access-Provider miteinbezogen werden.

5. Kapitel VERGLEICHENDER TEIL

Die bisherigen Ausführungen waren darstellender Natur. In Bezug auf China wurde gezeigt, dass dort ein geradezu lückenloses Sperrsystem gegeben ist, welches sicherstellt, dass schädliche Informationen aus dem Internet ferngehalten werden. Hierzu gehört auch die Inanspruchnahme von Access-Providern, die zielgerichtet und auch präventiv den Zugang zu schädlichen Informationen sperren können. Wegen der staatlichen Struktur dieser Unternehmen gestaltet sich dies relativ problemlos. In Deutschland sieht dies, wie gezeigt, anders aus. Es findet zwar eine Inhalteregulierung statt, diese ist jedoch dadurch geprägt, dass stets auf die Grundrechte zu achten ist. Host-Provider müssen dafür sorgen, dass rechtswidrige Informationen, wenn sie davon Kenntnis erlangen, gelöscht werden. Hier wurde jedoch ein Rechtsdurchsetzungsdefizit offenbart. Dieses soll durch das NetzDG behoben werden. Bei der Inanspruchnahme von Access-Providern wurde besonders deutlich, dass hier dem Verhältnismäßigkeitsgrundsatz Rechnung zu tragen ist. Da sie in der Regel nur für die technische Komponente der Internetaktivität zuständig sind, ist es begründungsbedürftig, sie für die Inhalte in Anspruch zu nehmen. Da sie jedoch technisch die Möglichkeit haben, Inhalte zu sperren, möchte sich auch der deutsche Gesetzgeber die Inanspruchnahme von Access-Providern nicht versperren. Die Anforderungen sind jedoch hoch.

In diesem Kapitel soll rechtsvergleichend überlegt werden, welche der dargestellten Konzepte überzeugen. Hierbei ist insbesondere auf die rechtsstaatlichen Verankerungen einzugehen. Zum besseren Verständnis des chinesischen Recht wird zunächst ein Überblick zur Entwicklung des Rechts in China gegeben. Dies ist eingebettet in die Grundlagen für den Rechtsvergleich (A.). Im Einzelnen sind folgende Aspekte in diesem Kapitel zu beleuchten: Herausarbeitung der Unterschiede der beiden Länder in Bezug auf Internetsperren (B.). Anschließend soll das chinesische Sperrensystem auf untersucht werden. Hierbei geht es um eine Kritik anhand deutscher Verfassungsstandards (C.). Vor dem Hintergrund dieser Ergebnisse gilt es, Vorschläge für eine rechtmäßige Inhaltsregulierung zu formulieren (D.).

A. Grundlagen

I. Ziel eines Rechtsvergleichs

Der langsame Integrationsprozess der Nationalstaaten führt zu einer Globalisierung des Rechts.[542] Ent- und Reterritorialisierung als solche sind zudem gleichzeitig sowohl der Grund als auch die Folge für rechtsvergleichende Betrachtungen und führen zu einer Vielzahl an verschiedenen Rechtsräumen und Rechtstraditionen.[543] In diesem Sinne kann das Ziel des Rechtsvergleichs darin erkannt werden, allgemein anerkannte und auch allgemeingültige Lösungen zu finden. Darüber hinaus kann der Rechtsvergleich helfen, das Recht in einem bestimmten Rechtsraum zu verbessern, indem auf Erfahrungen in einem anderen Rechtsraum abgestellt wird. Diese Zielsetzung liegt der vorliegenden Arbeit zugrunde. Die Erfahrungen in Deutschland mit der Regulierung von Online-Inhalten sollen für die chinesische Praxis fruchtbar gemacht werden.

II. Vorbedingungen des Rechtsvergleichs

Die Rechtsvergleichswissenschaft als solche beruht auf der als gleich angesehenen Natur des Menschen, die von unterschiedlichen Faktoren wie zum Beispiel der Sprache oder der gesellschaftlichen und staatlichen Organisationsform beeinflusst sind.[544] Gesetze sind zwar von geographischen, geschichtlichen, kulturellen und politischen Bedingungen abhängig, dienen jedoch in jedem Staat vergleichbaren Zwecken. Hauptsächlich geht es darum, ein geordnetes Zusammenleben zu ermöglichen.

III. Überblick zur Entwicklung des Rechts in China – Vier Phasen

In China hat die Rechtsvergleichung traditionell eine wichtige Rolle. Bei der Entwicklung des eigenen Rechts orientiert sich China stark an den Erfahrungen anderer Länder. Häufig genannt wird hierbei auch die Rechtsrezeption, also die Über-

---

542 *Shapiro*, 1 Ind. J. Global Legal Stud. 37 (37) (1993).

543 Zum Beitrag der Rechtsvergleiche zur Rechtsangleichung im globalen Rechtsraum siehe *Busse*, 262 ff.

544 Ebd., 337 (339).

nahme eines Rechts. Dennoch interpretiert China die rezipierten Normen. Die Entwicklung des Rechts soll im Folgenden kurz dargestellt werden. Hierbei können vier Phasen identifiziert werden.[545]

1. Erste Phase

Der erste Zeitraum erstreckt sich von den 1830er Jahren bis 1901. In ihm wurde eine Vielzahl abendländischer Gesetze sowie klassischer Werke von christlichen Missionaren sowie den ersten Gruppen chinesischer Eliten nach China gebracht.

2. Zweite Phase

Nach dieser Vorbereitungszeit fing die Kodifikationswelle mit vielen Übersetzungs- und Rechtsvergleichsarbeiten an. Dies konnte in den letzten zehn Jahren der Qing-Dynastie (1902-1911) beobachtet werden. Als Beispiel können das chHGB (1903), das chStGB (1911), die chZPO (1906) sowie das chBGB (1911) angeführt werden. Diese Gesetze wurden zumeist unter der Leitung von japanischen Juristen ausgebracht.[546] Bemerkenswert ist dabei noch, dass der Fachbegriff „Rechtsvergleich“[547] bereits zu dieser Zeit entstand.[548] Diese Ambitionen zeigen deutlich, dass die Qing-Dynastie mit der neuen chinesischen Rechtsordnung das alte Regime sowohl im industriellen Sinne als auch vom Politik- und Rechtssystem her wieder zu einer Weltmacht machen wollte.[549]

3. Dritte Phase

In der dritten Phase wurden zahlreiche Kodifikationsprojekte in der neu gegründeten chinesischen Republik verfolgt und es entstand eine einheitliche und vollständige Rechtsordnung. In der Zwischenzeit ging die Forschung der Rechtsver-

---

545 Allgemein zu modernen Rechtsreformen in China siehe *Kischel*, 744 ff.; zur historischen Entstehung und Entwicklung der Rechtsvergleiche siehe *Pan*, Journal of Comparative Law 1990/2, 1 (2 ff); *Ni*, in: Law and Modernization 1997, 368 (390 ff.); *He Qinhua*, Journal of Comparative Law 2006/6, 125 (125 ff.).

546 *He Haibo*, Journal of Comparative Law 1990/6, 42 (42); *Pan*, Journal of Comparative Law 1990/2, 1 (5); *Kischel*, 756; *He Qinhua*, Journal of Comparative Law 2006/6, 125 (126).

547 比较法.

548 *He Qinhua*, Journal of Comparative Law 2006/6, 125 (127 ff.).

549 *Pan*, Journal of Comparative Law 1990/2, 1 (5).

gleiche aber auch in die Tiefe. So wurden etwa die Vereinigung der Rechtsvergleichswissenschaft und die Fakultät für Rechtsvergleichswissenschaft an der Suchou Universität gegründet.[550]

4. Vierte Phase

Nachdem die Volksrepublik China von 1949 bis 1978 aus ideologischen Gründen lediglich die Sowjetunionen als Vorbild ansah, boomt der rechtsvergleichende Forschungsmarkt aller Rechtsgebiete seit der Reform- und Öffnungspolitik, die ihren Anfang in den 1980er Jahren nahm.

IV. Beziehung zwischen Deutschland und China auf dem Gebiet des Rechts

Die Verbindung zwischen chinesischem und deutschem Recht ist japanischen Juristen zu verdanken, da diese in der zweiten Phase ihre Rezeptionserfahrungen aus dem deutschem Recht durch die Übersetzung der klassischen Werke, auch in China verbreiteten. Japanische Gelehrte unterrichteten an chinesischen Universitäten und verbreiteten die Kodifikationen in China.[551] Dieser „aktive Vorgang von Aufnehmen, Annehmen und Entgegennehmen“ [552] zeigt sich sowohl in den Rechtsbegriffen, den Rechtsinstituten und den Grundsätzen des chinesischen Rechts als auch in der vertiefenden Kooperation und dem Dialog zwischen den beiden Ländern.[553]

V. Wert des Rechtsvergleichs in der globalisierten Welt und in Zeiten des Internet

In der globalisierten Welt und der Informationsgesellschaft ist der Rechtsvergleich besonders nützlich, da sich stets und vielerorts rechtliche Fragen stellen, wie Kon-

---

550 *Zhang Yanying*, Journal of Comparative Law 2014/5, 191 (192); *Pan*, Journal of Comparative Law 1990/2, 1 (7); *Ni*, in: Law and Modernization 1997, 368 (401).

551 *Starck*, JZ 2016, 377 (379); *Kischel*, 756.

552 *Starck*, Rechtsrezeptionen in Ostasien, JZ 2016, 377 (377).

553 *Bu*, JZ 2016, 382 (389); *Stürner*, JZ 2012, 10 (17); zum Einfluss des deutschen Rechts auf Taiwan siehe *Chen Hsin-min*, in: Jahrbuch des Deutsch-Chinesisches Instituts für Rechtswissenschaft der Universitäten Göttingen und Nanjing, 47 (47 ff.).

flikte zwischen Wertvorstellungen und der Nutzung von Technologien und zwischen Globalisierung und Nationalbewusstsein am besten zu lösen sind.[554] Traditionell und auch gegenwärtig ist das chinesische Recht stark vom deutschen Recht geprägt. Angesichts der verschiedenen Werteordnungen und Entwicklungsstufen der beiden Nationalstaaten besteht zwar kein Konsens über das „Wie", aber über das „Ob" der Regulierung und des Sperrens von Online-Inhalten.[555] Jedoch besteht kein Zweifel, dass beide Staaten bei der Frage des „Ob" der Regulierung und des Sperrens eine gewisse Antwort geben können.

B. Unterschiede und Gemeinsamkeiten in Bezug auf Internetsperren

Nach *Hoffmann-Riem* lässt sich Regulierung im Verwaltungsrecht in drei Grundtypen gliedern: in die staatlich-imperative Regulierung, die regulierte gesellschaftliche Selbstregulierung und die gesellschaftliche Selbstregulierung.[556] Beim Sperren im Internet kommen alle drei Typen sowohl in China als auch in Deutschland in Betracht. Freilich neigt China mehr zur staatlich-imperativen Regulierung als Deutschland. In diesem Abschnitt ist zu untersuchen, inwieweit die chinesische Regulierung als Vorbild für Deutschland dienen kann.

I. Monopolisierte Telekommunikation und teilweise Unabhängigkeit der Telemedien

1. Situation in China

Wie in Kapitel 3.B. gezeigt wurde, unterliegt die chinesische Grundtelekommunikation dem Monopol der drei staatlichen Unternehmen, sodass sich Zugangsnetz, Verbindungsnetz und WWW-Netz völlig in staatlicher Hand befinden. Die GFW als ein umfassendes und effektives Projekt kann daher in China ohne institutionelle Hindernisse aufgebaut werden. Mit Hilfe der GFW schafft China eine nur

---

554 *Menzel*, 133 ff.; Die globale Harmonisierung der Beziehung zwischen Menschen und Natur wird in China auf den Gedanken des „unter dem Himmel" zurückgeführt, dazu *Mi*, in: FS Blaurock, 337 (337 ff.).

555 *Mayer*, NJW 1996, 1782 (1791); *Roßnagel*, MMR 2002, 67 (70).

556 *Hoffmann-Riem*, in: Hoffmann-Riem/Schmidt-Aßmann, Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen – Systematisierung und Entwicklungsperspektiven, 261 (300 ff.).

teilweise offene Netzwelt, die zwar mit dem Ausland verbunden ist. Angesichts des intensiven Filterns sind Inhalte jedoch in großem Umfang beschränkt. Um dies zu rechtfertigen, argumentiert China politisch und rechtlich mit der sog. Internet-Souveränität. Diese besagt, dass jeder Nationalstaat die Regeln zum Gebrauch des Internets selbst aufstellen kann. Eine organisatorische Rahmenbedingung ist hier das Genehmigungserfordernis der (Tele-)Medien. Im Presse- und Rundfunkbereich gilt stets das Sondergenehmigungsregime. Die traditionellen Medien werden dadurch vollständig vom Staat kontrolliert. Darüber hinaus müssen chinesische Telemedien mehrere Lizenzen beantragen und sind daher weder zulassungs- noch anmeldefrei. Als Gatekeeper sind Telekommunikations- und Telemediendienste-anbieter auch nach dem Erhalt der entsprechenden Lizenzen zur Einhaltung von Regeln verpflichtet. Bei Verstoß droht der Entzug der Lizenzen. Hierbei ist die Erfüllung der Verpflichtung zur Implementierung von Internetsperren ein bestimmender Faktor.

2. Situation in Deutschland

In Deutschland bestand in der Telekommunikationsbranche bereits ab den 1980er Jahren kein natürliches Monopol mehr.[557] Seither liegen Telekommunikationsdienste, die in der Regel gegen Entgelt erbracht werden und zumindest überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen (§ 3 Nr. 24 TKG), nicht mehr komplett in staatlicher Hand. Gemäß dem verfassungsrechtlichen Auftrag in Art. 87f GG dient die Regulierung des TKG dem chancengleichen Wettbewerb (§ 2 Abs. 2 Nr. 2 TKG). Die Bundesnetzagentur als Regulierungsbehörde fördert danach den infrastrukturbasierten Wettbewerb (§ 2 Abs. 3 Nr. 3 TKG). Durch verschiedene Instrumente der Regulierung, vor allem der Markt- und Entgeltregulierung, kann das Ziel der Wettbewerbssicherung sowie der Grundsatz der Wettbewerbsförderung realisiert werden.[558]

Inhaltlich wird die Vielfalt und Unabhängigkeit der deutschen herkömmlichen Medien im Lichte der Medienfreiheit gemäß Art. 5 Abs. 1 S. 2 GG sichergestellt.

---

557 *Kühling/Schall/Biendel*, 31 ff.; *Holznagel/Enaux/Nienhaus*, 20 ff; *Neumann/Koch*, Kap. 2 Rn. 7 ff.

558 *Kühling/Schall/Biendel*, 91 ff.; *Mayen*, in: Scheurle/Mayen, Telekommunikationsgesetz, § 116 Rn. 3 ff.; *Gersdorf*, in: Spindler/Schuster, Recht der elektronischen Medien, TKG § 9 Rn. 19 ff.

Die Pressefreiheit schützt sämtliche mit der Herstellung und Verbreitung von Presseerzeugnissen zusammenhängenden Tätigkeiten.[559] Darüber hinaus wird die institutionelle Eigenständigkeit der Presse geschützt, einschließlich freier Gründung von Presseorganen und freiem Zugang zu Presseberufen.[560] Von einer Zulassung ist die Pressetätigkeit daher unabhängig.[561] Unzulässig ist, dass der Staat selbst Presseerzeugnisse herausgibt.[562] Genauso garantiert die Rundfunkfreiheit als dienende Freiheit den Schutz vor staatlicher Beherrschung und Einflussnahme auf sämtliche mit der Veranstaltung von Rundfunk zusammenhängenden Tätigkeiten.[563] Abschließend sind Telemedien ungeachtet ihrer schwierigen Abgrenzung von Presse und Rundfunk zulassungs- und anmeldefrei (§ 4 TMG und § 54 Abs. 1 RStV). Wenn es sich um Meinungsäußerungs- und Medienfreiheit handelt, darf keine Vorzensur durch den Staat stattfinden (Art. 5 Abs. 1 S. 3 GG).

3. Vergleichbarkeit der Medienregulierung in Deutschland und China

Die Medienregulierung in China und in Deutschland sind nur bedingt miteinander vergleichbar. Dabei spielt der technische und organisatorische Rahmen eine wichtige Rolle und hat großen Einfluss auf die Inhaltsregulierung im Netz. Dennoch besteht eine Vergleichsbasis zwischen beiden Ländern. Auf der einen Seite ist es nicht ausgeschlossen, dass das Monopol der drei chinesischen staatlichen Telekommunikationsunternehmen enden wird. Seit Ende 2013 hat das Ministerium für Industrialisierung und Information an 19 private Unternehmen Betriebslizenzen im Mobilfunkbereich verteilt.[564] Die Durchsetzbarkeit von Sperrmaßnahmen ist dann nicht mehr an die Monopolstellung des Staates in der TK-Branche gekoppelt.[565] Auf der anderen Seite sind chinesische Telemedien nicht wie herkömmliche Medien verpflichtet, dem Volk und dem Sozialismus zu dienen. Sie sind daher

---

559 BVerfGE 95, 28 (35); *Grabenwarter*, in: Maunz/Dürig, GG, Art. 5 Abs. 1 u. 2, Rn. 239 ff.; *Schulze-Fielitz*, in: Dreier, GG, Art. 5 Abs. 1, 2 Rn. 89; *Wendt*, in: v. Münch/Kunig, GG, Art. 5 Rn. 30.

560 BVerfGE 20, 162 (175); 66, 116 (133); 80, 124 (133); 117, 244 (258 f.); *Grabenwarter*, in: Maunz/Dürig, GG, Art. 5 Abs. 1 u. 2, Rn. 353 ff.; *Schulze-Fielitz*, in: Dreier, GG, Art. 5 Abs. 1, 2 Rn. 213.

561 Vgl. z.B. § 2 PresseG NRW.

562 *Grabenwarter*, in: Maunz/Dürig, GG, Art. 5 Abs. 1,2, Rn. 375 ff.; *Stern*, in: Staatsrecht IV/1, 1555; *Trute*, in HGR, Bd. IV, § 104 Rn. 35.

563 BVerfGE 12, 205 (260 ff.); 73, 118 (166); 83, 238 (322); 121, 30 (41 ff.) *Grabenwarter*, in: Maunz/Dürig, GG, Art. 5 Abs. 1,2, Rn. 736 ff.; *Degenhart*, in: Kahl/Waldhoff/Walter, Bonner Kommentar zum Grundgesetz, Bd. 2, Art. 5 Abs. 1, 2, Rn. 280.

564 *Qi Enping*, Communication World 2018/1, 11 (11).

565 *Yun Qin*, Communications World 2017/25, 32 (32 f.); *Qie Yongzhi*, Communications World 2018/1, 11 (11); *Wu Yuxin*, Foreign Investment in China (中国外资) 2018/11, 46 (46 f.).

von der vollständigen Kontrolle des Staates befreit. Sicherlich wird Deutschland ein teilweise geschlossenes Netzwerk mit Sperrtechniken wie der GFW auf Kosten der Freiheit nicht aufbauen wollen. Gegen Hate-Speech und Fake-News zu kämpfen ist, wie das NetzDG zeigt, jedoch auch eine wichtige Aufgabe der Inhaltsregulierung in Deutschland. Diesbezüglich verfügt China über viel Erfahrung. Diese Erfahrungen können für die deutsche Diskussion durchaus fruchtbar gemacht werden. Dies soll im Folgenden dargestellt werden.

II. Compliance-Modell braucht mehr Kooperation zwischen Staat und Unternehmen und mehr staatliche Aufsicht

1. China – aktive Rolle des Staates

Im Vergleich zu China hat Deutschland eher zögerlich eine Inhaltsregulierung im Netz vorgenommen. Auch Internetsperren gegenüber den Zugangsanbietern genießen in Deutschland einen zweifelhaften Ruf. Seit 2000 sind in China zahlreiche Rechtsnomen erlassen worden, die ein umfassendes Regelungssystem bilden. In China gilt das Internet als völlig unterschiedlich zu den traditionellen Medien und wird als spezielles Regulierungsobjekt wahrgenommen. Dies führt dazu, dass für etliche Referenzgebiete eine besondere Regelungsnorm besteht.[566] Diese gesetzgeberische Einstellung entspricht den rapiden Veränderungen und der Flexibilität in der Informationsgesellschaft. Neben den unmittelbaren gesetzlichen Versuchen

---

566 Methode für Internet-Informationsdienste (互联网信息服务管理办法) vom 25.9.2000; Verwaltungsbestimmungen für Internet- Bulletin-Board-Dienste （互联网电子公告服务管理规定）vom 6.11.2000; Vorläufige Verwaltungsregeln zur Kultur im Netz (互联网文化管理暂行规定) vom 17.2.2011; Vorläufige Verwaltungsregeln für Entwicklung der öffentlichen Nachrichtendienste mittels Echtzeitkommunikationstechnik (即时通信工具公众信息服务发展管理暂行规定) vom 7.8.2014; Verwaltungsregeln zur Online-Presse (网络出版服务管理规定) vom 4.2.2016; Verwaltungsregeln für Suchmaschinen im Internet (互联网信息搜索服务管理规定) vom 1.8.2016; Verwaltungsregeln für Webcast im Internet (互联网直播服务管理规定) vom 1.12.2016; Verwaltungsregeln zur Online-Nachrichtendienste (互联网新闻信息服务管理规定) vom 1.6.2017; Verwaltungsregeln für Foren im Internet (互联网论坛社区服务管理规定) vom 1.10.2017; Verwaltungsregeln für Posten im Internet (互联网跟帖评论服务管理规定) vom 1.10.2017; Verwaltungsregeln für öffentliche Kontos im Internet (互联网用户公众账号信息服务管理规定) vom 8.10.2017; Verwaltungsregeln für geschlossene Chatgruppen im Internet (互联网群组信息服务管理规定) vom 8.10.2017; Verwaltungsregeln für videoelle und audioelle Programme im Internet (互联网视听节目服务管理规定) vom 20.12.2007; Verwaltungsregeln für Microblog im Internet (微博客信息服务管理规定) vom 20.3.2018.

tragen auch andere Hilfsmaßnahmen, vor allem die Klarnamenpflicht und Vorkehrung im Sinne der IT-Sicherheit, zur Inhaltsregulierung und zu Internetsperren bei. Darüber hinaus trägt der Staat bei der Durchsetzung der Gesetze auch aktiv viel Verantwortung. Zur Konkretisierung von Sperr- und Löschanordnungen in Bezug auf rechtswidrige Inhalte arbeiten Aufsichtsbehörden und private Unternehmen zusammen. Unter der ständigen Anleitung der Aufsichtsbehörden sind die Intermediäre der Aufgabe besser gewachsen, rechtswidrige Inhalte zu sperren oder zu löschen. Letztlich erfüllen die Behörde sowie die Staatsanwaltschaft dem Nutzer gegenüber auch aktiv ihre eigene Verantwortung, soweit der Nutzer gegen ein gesetzliches Ge- oder Verbot verstößt.

2. Deutschland – eher passive Rolle des Staates

Vor dem Erlass des NetzDG galt die Inhaltsregulierung im Netz sowie die Implementierung von Internetsperren in Deutschland als unsystematisch und als zu gravierender Eingriff in grundrechtliche Positionen. Sperrverfügungen sind, wie gezeigt auf wenige Bereiche beschränkt. Gegen rechtswidrige Inhalte, die auf inländischen Plattformen bereitgestellt werden, wird dann auf die bestehenden gesetzlichen Regelungen vertraut. Zudem spielt das Haftungsregime der §§ 7-10 TMG als Ergebnis der Umsetzung der E-Commerce-Richtlinie im Zivilrecht eine grundlegende Rolle. Wegen des Durchsetzungsdefizits wurde das Compliance-Modell des NetzDG zur Regulierung der sozialen Netzwerke eingeführt. Zwar soll das chinesische verstärkte Compliance-Modell nicht als ein Vorbild für die Durchführung von Internetsperren in Deutschland gelten. Positiv hervorzuheben sind jedoch durchaus die vielfältigen gesetzgeberischen Maßnahmen im Internetrecht sowie die aktive Teilnahme der Aufsichtsbehörde an der Inhaltsregulierung.

III. Verantwortlichkeit der Provider

1. Notice-and-take-down-Verfahren für Content- und Hostprovider in Europa bzw. Deutschland – seltene Inanspruchnahme von Access-Providern

Für die Verantwortlichkeit der Provider in der EU und Deutschland sind vor allem die E-Commerce-Richtlinie und das TMG von Bedeutung. Die dortigen Regelungen der Haftung gelten im Zivilrecht, Strafrecht und Verwaltungsrecht.[567] Im Verwaltungsrecht wird in Deutschland die Neutralität von Access- und Host-Providern anerkannt. Dogmatisch spielt hier die Rechtsfigur der Gefahrenabwehr im Polizei- und Ordnungsrecht eine wichtige Rolle. Host- und Access-Provider können unter Umständen den Zustands- oder Nichtstörern zugerechnet werden, damit die Verantwortlichkeit als eine der Voraussetzungen der Gefahrenabwehr erfüllt wird. Trotz dieser grundsätzlichen Anwendungsmöglichkeit findet die allgemeine Ermächtigungsgrundlage im Ordnungsrecht (z.B. § 8 Abs. 1 PolG NRW oder § 14 OBG NRW) in der Praxis selten Anwendung. Dabei gilt nur für zwei Bereiche eine Ausnahme, nämlich das Medienrecht und das Glücksspielrecht. Als Ermächtigungsgrundlage für Sperrverfügungen gegen Host- und Access-Provider kommen z.B. § 59 Abs. 4 RStV, § 20 Abs. 4 JMStV i.V.m. § 59 Abs. 4 RStV oder § 9 Abs. 1 Satz 3 Nr. 3 GlüStV in Betracht. Damit können zum einen Sperrverfügungen gegen inländische *Host*-Provider angeordnet werden. Um gegen im Ausland ansässige Host-Provider vorzugehen wurden zum anderen auch häufig Sperrmaßnahmen gegen inländische *Access*-Provider erlassen.

2. China – zahlreiche verwaltungsrechtliche Regelungen nehmen alle Provider in die Pflicht

Im chinesischen Recht wurde der Haftungsgrundsatz und die Haftungsprivilegierung für Internetdiensteanbieter auch mit dem Gesetz über die Haftung für die Verletzung von Rechten nach dem Vorbild der E-Commerce-Richtlinie übernommen. Dies hat jedoch nur Einfluss auf das Zivilrecht. Im chinesischen Zivilrecht besteht auch keine allgemeine Überwachungspflicht oder aktive Forschungspflicht für Internetdiensteanbieter. Durch zahlreiche besondere Regelungen sind

---

567 *Sieber/Höfinger*, in: Handbuch Multimedia-Recht, Teil 18.1, Rn. 1, 15, 20 ff.; *Beaucamp/Henningsen/Florian*, MMR 2018, 501 (503); *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (15); *Frey/Rudolph*, Rn. 3 ff.

allerdings die Internetdiensteanbieter, ohne hierbei zwischen Content-, Host- und Access-Providern zu unterscheiden, verwaltungsrechtlich verpflichtet, alle schädlichen Informationen zu sperren oder zu löschen, wenn sie der gesetzlichen Liste[568] unterfallen. Verstoßen sie gegen die betroffenen Rechtsnormen, werden sie verwaltungsrechtlich oder strafrechtlich belangt. Ein solches Konzept geht auf das chinesische Medienrecht und das Sicherheitsrecht zurück. Im chinesischen Medienrecht steht die staatliche Propaganda im Zentrum. Dabei wird ein systematisches Kontroll- und Zensursystem gebildet. Durch die Anerkennung der Inhaltssicherheit im Netzwerk- oder Informationsrecht vergrößert sich die Wichtigkeit und Erforderlichkeit der Implementierung von Internetsperren.

IV. Durchsetzung der nationalen Gesetze

1. Deutschland – Verwaltungsrechtlicher Druck erst mit NetzDG – nur subsidiäre Inanspruchnahme von Access-Providern

Erst seit dem NetzDG wurde das Modell der Compliance-Regulierung in Deutschland eingeführt. Ein Compliance-Modell sorgt dafür, dass soziale Netzwerke ihren Löschverpflichtungen möglichst schnell nachkommen. Soziale Netzwerke sind hiernach verpflichtet, ein für Nutzer transparentes Beschwerdeverfahren vorzuhalten und Löschungen von rechtswidrigen Inhalten zu löschen. Dazu sind die zu den aufgelisteten Straftaten gehörenden rechtswidrigen Inhalte innerhalb einer bestimmten Frist zu löschen oder zu sperren. Der verwaltungsrechtliche Druck bezieht sich hierbei nur auf Host-Provider und dabei auch nur auf mitgliederstarke soziale Netzwerke. Access-Provider werden vom NetzDG nicht tangiert. Dem NetzDG liegt aber die Intention zugrunde, dass das Recht im Internet durchgesetzt wird. Der Notice-and-Take-Down-Ansatz hatte hierbei nicht den erhofften Erfolg gebracht. Das NetzDG ist nicht imperativ wie die chinesischen Regelungen. Es beinhaltet ein „Nudging“, das die sozialen Netzwerke zur Einhaltung des Rechts anhalten soll.

Abgesehen vom NetzDG existiert keine derartige Form des Nudging. Für andere Bereiche und andere Anbieter – Access-Provider – greifen die allgemeinen Regelungen. Hierunter fällt das Polizei- und Ordnungsrecht. In zivilrechtlicher Hinsicht spielt das Notice-and-Take-Down-Verfahren eine wichtige Rolle. Dieses soll zwar

---

568 Siehe hierzu Kapitel 3. B.

auch dazu führen, dass die Anbieter ihren Verpflichtungen nachkommen. Die Praxis hat hierzu jedoch Lücken offenbart. Zudem werden Access-Provider nur subsidiär in Anspruch genommen.

2. China – Aufsicht der Verwaltung über Einhaltung der gesamten Rechtsordnung

In der chinesischen Regelungspyramide ist zunächst der Adressatenkreis von verwaltungsrechtlich Verpflichteten nicht nur auf soziale Netzwerke begrenzt, sondern auf sämtliche Provider. Der Umfang der schädlichen Informationen ist darüber hinaus nicht nur auf bestimmte strafrechtliche Paragrafen, die sich auf verbotene Inhalte beziehen, beschränkt, sondern umfasst sämtliche zivil-, verwaltungs- und strafrechtlich rechtswidrigen Inhalte. Unter der Aufsicht von einer bestimmten Behörde – Chinas Staatlichen Büros für Internet und Information (CSII) – und weiteren Instrumenten wie z.B. der Klarnamenpflicht der Nutzer, das Credit-System und eine Schwarze Liste für Anbieter und Nutzer, werden rechtswidrige Inhalte effektiv gesperrt. Ohne größere Hürden können Sperrverfügungen gegenüber Access-Providern ergehen. Letztlich werden diese aber schon freiwillig den Zugang zu schädlichen Inhalten sperren.

3. Kritik an der chinesischen Regelungsintensität

Angesichts der offensichtlich sehr weitgehenden Regelungsintensität ist die chinesische Lösung für Inhaltsregulierung zu kritisieren. Informelles Handeln, z.B. ein Gespräch oder eine gemeinsame Stellungnahme, wird zwar auch als weniger einschneidende Methode angewandt. Da der Umfang des chinesischen Verwaltungssanktionsrechts größer als das deutsche Ordnungswidrigkeitsrecht ist, werden neben dem Bußgeld noch z.B. der Entzug der Lizenz einer Plattform, das Schließen eines Servers oder auch Haftstrafen gegenüber den unmittelbaren Verantwortlichen verhängt. Um diese Sanktionen zu vermeiden, neigen die Internetdienstanbieter dazu, freiwillig verdächtige Inhalte zu entfernen oder zu löschen. Unter Anleitung der Aufsichtsbehörde kommen die Internetdiensteanbieter (Content-, Host- und Accessprovider) zuverlässig ihren Verpflichtungen nach. Die behördliche Anleitung ist dabei notwendig, da die gesetzlichen Vorgaben zu umfangreich und zu diffus sind. Im Ergebnis sind die Internetdiensteanbieter faktisch gezwungen, alle fraglichen Inhalte dem Willen der Hoheitsträger nach zügig aus dem Netz zu entfernen.

V. Zusammenfassung

Wenn es darum geht, die Gemeinsamkeiten und Unterschiede in Bezug auf Internetsperren zwischen Deutschland und China herauszuarbeiten, überwiegen eindeutig die Unterschiede. Die Struktur der Telekommunikationsdiensteanbieter ist in Deutschland wettbewerblich geprägt, während in China der Staat die Netze kontrolliert. Insofern besteht hier schon andere Handlungsmöglichkeiten. Aber es sind auch Gemeinsamkeiten auszumachen. So verfolgen beide Länder das Ziel, schädlichen oder rechtswidrigen Inhalten keinen Raum zu geben. In China nimmt hierbei der Staat eine aktive Rolle ein. In Deutschland hält sich der Staat eher zurück. Nur ausnahmsweise erlässt der Staat Maßnahmen gegen die Access-Provider. Diese sind bei der Inhalteregulierung von Relevanz, da sie zuverlässig und auch mit Wirkung für die Zukunft Inhalte bekämpfen können. Bei der Inhalteregulierung hat der deutsche Gesetzgeber erkannt, dass er den privaten Interessen nicht freien Lauf lassen darf. Um hier die Rechtsdurchsetzung zu gewährleisten, wurde das NetzDG erlassen. Dieses macht den sozialen Netzwerken Druck, ihren Löschverpflichtungen nachzukommen. Das NetzDG ist der Kritik ausgesetzt, dass es die Meinungsfreiheit beeinträchtigen könnte. Im Vergleich zu China ist das NetzDG jedoch als sehr harmlos einzustufen. Dies führt zum nächsten Abschnitt: Dass nämlich die Regelungsintensität sehr hoch ist und auch die rechtsstaatlichen Gewährleistungen nicht eingehalten werden.

C. Kritik zu chinesischen Internetsperren im Netz durch den funktionellen Rechtsvergleich mit dem deutschen Recht

In diesem Abschnitt sind die chinesischen Internetsperren zu untersuchen. Hierbei ist zu prüfen, inwieweit sie rechtsstaatlichen Verbürgungen gerecht werden. Dabei soll zum einen immer ein Blick auf die Lage in Deutschland gerichtet sein. Dies ermöglicht einen vertieften Zugang zu den Anforderungen. Gleichzeitig wird deutlich, welche Unterschiede zwischen Deutschland und China in rechtsstaatlicher Hinsicht bestehen. Es geht um folgende Grundsätze: Vorbehalt des Gesetzes (I.), Bestimmtheitsgrundsatz (II.), Verhältnismäßigkeit (III.) und Rechtsschutz (IV.).

I. Aushöhlung des Vorbehalts des Gesetzes

1. Der Grundsatz des Wesentlichkeitsvorbehalts

Unter dem Wesentlichkeitsvorbehalt versteht man, dass der demokratisch legitimierte Gesetzgeber selbst die wesentlichen Aspekte vorgeben muss, wenn es sich um Grundrechtseingriffe handelt.[569] In China wurde über die Dogmatik vom Wesentlichkeitsvorbehalt in der Literatur viel diskutiert.[570] Der Wesentlichkeitsvorbehalt wurde durch das Gesetzgebungsgesetz[571] gesetzlich in das chinesische Recht eingeführt. Durch Sperrmaßnahmen gegen Access-Provider könnte in Deutschland in eine Vielzahl von Grundrechten, nämlich in die Berufsfreiheit und in die Eigentumsfreiheit für Access-Provider, den Schutz des Fernmeldegeheimnisses und die Informationsfreiheit für Nutzer sowie in die Meinungsfreiheit für Inhalts- und Host-Provider, eingegriffen werden.[572] So sah z.B. das ZugErschwG in Deutschland vor, dass die Sperrmaßnahmen das Grundrecht des Telekommunikationsgeheimnisses einschränken (§ 11 ZugErschwG).

2. Wesentlichkeitsvorbehalt auch zwischen Privaten?

Die Frage ist darüber hinaus, ob der Wesentlichkeitsvorbehalt auch auf die Interessenabwägung zwischen beiden Parteien im Zivilfall einwirkt. In den Auseinandersetzungen über die Zumutbarkeit der Sperrmaßnahmen als eines der wesentlichen Tatbestandsmerkmale der Störerhaftung ist umstritten, ob die Anspruchsgrundlage in § 1004 BGB analog dem Wesentlichkeitsprinzip hinreichend Rechnung trägt. Das LG Hamburg und das OLG Hamburg verlangten eine klare Gesetzesgrundlage und lehnten die durch Rechtsfortbildung von der Rechtsprechung entwickelte Anspruchsgrundlage für Sperrmaßnahmen gegenüber Access-Providern ab.[573] Der BGH folgte dieser Auffassung allerdings nicht, weil der Grundsatz des Wesentlichkeitsvorbehalts nicht zwischen Privaten gelte und in diesem Fall

---

569 *Kokott*, in: HGR, Bd. I, § 22 Rn. 74 ff.; *Lerche*, in: HGR, Bd. I, § 62 Rn. 54 ff.; *Sachs*, in: Sachs, GG, Art. 20 Rn. 117; *Dreier*, in: Dreier, GG, Vorb. Rn. 136.

570 *Zhang Wei*, Administrative Law Review 2011/2, 113 (113 ff.); *Deng Yi*, Administrative Law Review 2006/1, 17 (17 ff.); *Zhao Hong*, The Jurist 2011/2, 152 (152); *Zhang Xiang*, Die verfassungsrechtliche Dogmatik, 125 ff.; *ders*., Die normative Konstruktion der Grundrechte, 67 ff.

571 Gesetzgebungsgesetz (立法法) vom 15.3.2015.

572 LG Hamburg, U. v. 12.3.2010 - 308 O 640/0, Rn. 47 ff.; OLG Hamburg, U. v. 21.11.2013 - 5 U 68/10, Rn. 82, 91 ff.; LG Köln, U. v. 31.8.2011 - 28 O 362/10, Rn. 74; OLG Hamburg, U. v. 22.12.2010 - 5 U 36/09, Rn. 66.

573 LG Hamburg, U. v. 12.11.2008 - 308 O 548/08, Rn. 33 ff.; LG Köln, U. v. 31.8.2011 - 28 O 362/10, Rn. 76; OLG Hamburg, U. v. 22.12.2010 - 5 U 36/09, Rn. 77 ff.

die Aufgabe, zwischen den betroffenen Interesse der Grundrechtsträger abzuwägen und einen Ausgleich zu erreichen, der Rechtsprechung überlassen bleiben soll.[574]

3. Wesentlichkeitsvorbehalt in China

a) In der Regel: Einschränkung von Online-Inhalten durch Verwaltungsnormen

Im Vergleich zu Deutschland ist China ein sich zum Rechtsstaat entwickelndes Land. Fast sämtliche Rechtsgrundlagen für schädliche Online-Inhalte sowie Internetsperren sind nicht Gesetze im engeren Sinne, sondern auf Verwaltungsnormen und Verwaltungsregeln. Bei der Abgrenzung von schädlichen und nicht schädlichen Informationen in China gilt die Verlautbarung des Ministeriums für öffentliche Sicherheit[575] als der wichtigste Auslegungshinweis. Die davon ausgehenden umfangreichen Auflistungen von schädlichen Informationen wurden zunächst in drei Verwaltungsnormen, nämlich „Filmverwaltungsregeln", „Verwaltungsregeln für gewerbliche Darbietungen " und „Verlagsverwaltungsregeln", und danach in verschiedenen Verwaltungsnormen oder Verwaltungsregeln niedergeschrieben. Obwohl diese die Grundrechte, vor allem die Redefreiheit oder Pressefreiheit (Art. 35 chVerf), beeinträchtigen, wurde aufgrund des damaligen fehlenden Grundsatzes des Gesetzesvorbehalts und aufgrund der bis heute noch fehlenden Verfassungsgerichtsbarkeit in China nicht juristisch darüber diskutiert.

Des Weiteren setzte die damalige Generalverwaltung für Presse und Publikation – eine der wichtigsten für Ideologie zuständigen Abteilungen des Staatsrats – mit seiner Verwaltungsfunktion zwei neue Gegenstände auf die Liste der verbotenen Inhalte: zum einen Inhalte, die illegale Versammlungen, Vereinigung, Umzüge und Demonstrationen betreffen, die die soziale Ordnung stören, und zum anderen Inhalte, die von in China nicht zugelassenen Nichtregierungsorganisationen bereitgestellt werden (§ 19 Nr. 9 und 10 Verwaltungsregeln zur Online-Nachrichtendienste). Am Ende der Liste behält sich die Hoheitsgewalt noch vor, dass sie durch Verwaltungsrechtsnormen, staatliche Bestimmungen und Regeln aller Ministerien und Ausschüsse des Staatsrates diese Liste ständig erweitern kann. Angesichts der

---

574 BGH U. v. 26.11.2015 - I ZR 3/14, Rn. 59 ff.

575 *Yin*, Political Science and Law 2015/1, 102 (105); *Yu Zhigang*, Legal Forum 2014/6, 5 (8); *Wang Shiwei*, Journal of Library Science in China 2015/2, 72 (76).

ständigen verstärkten Internet-Kontrolle wurden und werden immer mehr unerwünschte Informationen dieser Liste hinzufügt. Die notwendigen Ermächtigungsgrundlagen der Internetsperren beruhen in China somit auf exekutiver Normsetzung.

b) Hinkender Wesentlichkeitsvorbehalt

Im chinesischen Rechtssystem gilt allerdings nur der sog. hinkende Wesentlichkeitsvorbehalt, da §§ 8 und 9 Gesetzgebungsgesetz lediglich vier Regelungsbereiche nennen, die unter dem absoluten Vorbehalt des Nationalen Volkskongresses und seines Ständigen Ausschusses stehen.[576] Das sind die Angelegenheiten der Straftaten und Strafen, der Aberkennung der politischen Rechte von Bürgern, der die körperliche Freiheit beschränkenden Zwangsmaßnahmen sowie Sanktionen und der Gerichtsorganisation (§ 9 Gesetzgebungsgesetz).

Der chinesische Wesentlichkeitsvorbehalt bezieht sich auf folgende Grundrechte: die körperliche Freiheit und politische Rechte, die im Einzelnen die Freiheit der Rede (Art. 35 chVerf), Publikationsfreiheit (Art. 35 chVerf), Informationsfreiheit (Art. 34 und 35 i.V.m. 41 chVerf), Freiheit der Korrespondenz und der Schutz der Korrespondenz (Art. 40 chVerf) umfassen. In der Konstellation der Sperrmaßnahmen im Internet sind diese Rechte durchaus betroffen. Der Meinung, dass in den §§ 8 und 9 Gesetzgebungsgesetz geregelte Aberkennung der politischen Rechte nach dem Wortlaut lediglich auf eine der Strafen im Sinne des Strafrechts verweise, ist aus systematischer Sicht jedoch nicht zu folgen. Da §§ 8 und 9 Gesetzgebungsgesetz bereits die Angelegenheit der Straftaten und Strafen als eine Kategorie auflistet, deutet „Aberkennung“ vielmehr auf „Einschränkung“ der politischen Rechte hin.[577] Wird die politische Freiheit beschränkt, ist nach dem Gesetzgebungsgesetz ein Gesetz zur Regelung dieses Sachverhalts – Internetsperren – erforderlich. Demnach ist ein Verstoß gegen den Wesentlichkeitsvorbehalt gemäß §§ 8 und 9 Gesetzgebungsgesetz gegeben.

---

576 *Zhang Xiang*, Die verfassungsrechtliche Dogmatik, 126.; *ders.*, Die normative Konstruktion der Grundrechte, 68; *Zhao Hong*, The Jurist 2011/2, 152 (153).

577 *Zhang Wei*, Administrative Law Review 2011/2, 113 (115); *Deng Yi*, Administrative Law Review 2006/1, 17 (20); *Zhang Fengzhen*, Tribune of Political Science and Law 2018/4, 35 (38).

II. Unbestimmtheit der Ermächtigungsgrundlagen

1. Deutschland – Anzuwendende Sperrtechniken in ZugErschwG und GlüStV

In Deutschland überließ es der Gesetzgeber sowohl gemäß ZugErschwG als auch gemäß GlüStV a.F. den Zugangsanbietern, welche Sperrtechnik sie verwenden.[578] Aufgrund verschiedener Funktionsweisen und Umgehungsmöglichkeiten der Sperrmaßnahmen sowie von ihnen herbeigeführten Kollateralschäden wurde kritisiert, dass der demokratische Gesetzgeber selbst klar bestimmen muss, in welchen Fällen mit welchem Mittel die Sperrung zu erfolgen hat. Soweit die Sperrmaßnahmen in die Grundrechte eingreifen, darf es hier nicht an Bestimmtheit mangeln. Das Bestimmtheitsgebot schließt dennoch die Anwendung von unbestimmten Rechtsbegriffen nicht aus, soweit die Vorhersehbarkeit und Justitiabilität der öffentlichen Handlungen dadurch nicht gefährdet ist.[579] In den angesprochenen Beispielen ist vor diesem Hintergrund von der Vereinbarkeit mit dem Bestimmtheitsgrundsatz auszugehen.

2. China – unbestimmte Rechtsbegriffe als Mittel der Kontrolle

Die in China oft herangezogene Internet-Souveränität dient vor allem der Selbstständigkeit der chinesischen Internetregulierung und der Implementierung von Internetsperren. Internet-Souveränität steht aber auch für die Ablehnung einer universalen Werteordnung und für die willkürliche Kontrolle von Online-Inhalten. Als ein Aspekt der willkürlichen Kontrolle gilt die Unbestimmtheit der Ermächtigungs- und Rechtsgrundlagen für Internetsperren, die in folgenden Punkten zu erörtern sind.

a) Potenzielle Adressaten von Maßnahmen

Zur wichtigsten Ermächtigungsgrundlage der Bekämpfung schädlicher Informationen gehört § 10 Nr. 7 der Bestimmungen zur Steuerung des Internet. Soweit schädliche Informationen bekannt werden, haben Diensteanbieter danach zur Unterbrechung derer Übermittelung Maßnahmen zu treffen und danach die Vorfälle

---

578 Begr. ZugErschwG, BT-Drucks, 16/13411, 17; *Frey/Rudolph*, CR 2009, 644 (648); *Schnabel*, JZ 2009 996 (1001); *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (15).

579 BVerfGE 21, 73 (79 f.); 80, 103 (108); 87, 234 (263 f.); 102, 254 (337); 103, 21 (33).; *Billmeier*, 130; *Grzeszick*, in: Maunz/Dürig, GG, Art. 20, Rn. 61; *Frey/Rudolph/Oster*, MMR-Beil. 2012, 1 (15).

zügig bei den zuständigen Behörden zu melden. Wie bereits im Kapitel 3.B. ausführlich erklärt, sind verschiedene Lizenzen für unterschiedliche Dienstleister einzuholen. In den Ermächtigungsgrundlagen ist keine Untergliederung von Diensteanbietern und keine Unterscheidung ihrer Verantwortung vorgesehen. Dies zeigt aber bereits einen großen Fortschritt, wenn man auf die früher betroffenen Regelungen zurückblickt. In den Bestimmungen zur Steuerung des Internet war es *jeder Einheit* oder *jeder Person* verboten, mittels Internet schädliche Informationen herzustellen, zu kopieren, durchzusehen oder zu verbreiten. Im Gegensatz dazu stellt die Beschränkung auf Diensteanbieter in der zitierten Norm einen Fortschritt dar. Von einer hinreichenden Bestimmtheit kann aber dennoch nicht ausgegangen werden.

b) Begriff der zuständigen Behörde

Es kann auch über die Bestimmtheit der Formulierung „zuständige Behörde" nachgedacht werden. Vor der Gründung des Staatlichen Büros für Internet und Information (CSII) im Jahre 2011 war die Bekämpfung illegaler Inhalte als dezentrale Aufgabe deklariert. In der Praxis konnte diese Aufgaben nur von der Behörde wahrgenommen werden, welche die ermächtigten Verwaltungsregeln erlassen hatte. In Gesetzen oder den von der zentralen Regierung erlassenen Verwaltungsnormen kann allerdings festgelegt werden, wer als zuständige Behörde die Sperrungsanordnungen gegen Diensteanbieter erlassen muss oder kann. Erst seit 2011 ist das CSII zur einzigen Aufsichtsbehörde geworden, das unmittelbar dem „Office of the Central Leading Group for Cyberspace Affairs" der KP[580] zugeordnet ist, deren Leiter der Staatspräsident und Parteichef ist. Die Gründung des CSII gilt als Wendepunkt in den letzten Jahren, da sämtliche Inhalte im Netz seither effektiver als zuvor kontrolliert werden.

c) Mögliche Maßnahmen zur Bekämpfung von Online-Inhalten

Unklar ist zudem, welche Maßnahmen zur Bekämpfung der Online-Informationen im konkreten Fall eingesetzt werden sollen. Entsprechend könnten die Regelungen gegen das Bestimmtheitsgebot verstoßen. Anders als § 10 der Bestimmungen zur Steuerung des Internets, in dem das Löschen der betroffenen Inhalte oder das Schließen der Server als bestimmte Maßnahmen vorgesehen sind, enthalten später erlassene Rechtsvorschriften andere Formulierungen. So heißt es beispielsweise

---

580 中共中央网络安全和信息化领导小组办公室.

„Unterbrechung der Datenübermittelung“ oder „Beseitigung der schädlichen Informationen“[581]. Die Frage, in welchen Fällen welche konkrete Sperr- oder Löschtechnik zu verwenden ist, überlässt der Normgeber in China der Behörde und dem Dienstanbieter.

d) Begriff der schädlichen Informationen

Schließlich liegt ein Verstoß gegen das Bestimmtheitsgebot auch vor, wenn die Liste der schädlichen Online-Informationen als solche zu unbestimmt ist. Wie im Kapitel 3.A. ausführlich dargestellt, sind die sog. „schädlichen Informationen“ im Internet in China zentral aufgelistet. Diese Liste taucht dann wiederum in verschiedenen Gesetzen auf. Das Ministerium für öffentliche Sicherheit versucht hierbei, schädliche Informationen zu definieren. Ihr Schutzumfang umfasst schwerwiegende Bedrohungen der Staatssicherheit aber auch nicht so schwerwiegende Delikte, wie z.B. Beleidigung oder Verleumdung. Im Einzelnen heißt es:

„Informationen, die (1) die Staatssicherheit beschädigen, vor allem die volksdemokratische Regierung, den Sozialismus, die politischen Führungskräfte der Partei sowie des Staates und die nationale Solidarität angreifen, oder (2) die soziale Ordnung stören, vor allem Aberglauben, Obszönität oder Pornographie, Mord o-

---

581 § 62 Telekommunikationsregeln (电信条例) vom 25.9.2000; § 16 Methode für Internet-Informationsdienst (**互**联网信息服务管理办法) vom 25.9.2000; § 13 Verwaltungsbestimmungen für Internet-Bulletin-Board-Dienste （**互**联网电子公告服务管理规定） vom 6.11.2000; § 27 Verwaltungsregeln zu Online-Nachrichtendiensten (**互**联网新闻信息服务管理规定) vom 1.6.2007; § 20 Verwaltungsregeln zur Online-Presse (**网**络出版服务管理规定) vom 4.2.2016; § 18 Verwaltungsregeln für audiovisuelle Programme im Internet (**互**联网视听节目服务管理规定) vom 20.12.2007; § 19 vorläufigen Verwaltungsregeln zur Kultur im Netz (**互**联网文化管理暂行规定) vom 17.2.2011; § 5 Beschluss des Ständigen Ausschusses des Nationalen Volkskongresses zur Verstärkung des Datenschutzes (**全国人民代表大会常**务委员会关于加强网络信息保护的决定) vom 28.12.2008; § 8 Abs. 2 Vorläufige Verwaltungsregeln für die Entwicklung der öffentlichen Nachrichtendienste mittels Echtkommunikationstechnik (**即**时通信工具公众信息服务发展管理暂行规定) vom 7.8.201; § 19 Abs. 1 Satz 1 HS. 2 Anti-Terror-Gesetz (**反恐法**) vom 27.12.2015; § 8 Verwaltungsregeln für Suchmaschinen im Internet (**互**联网信息搜索服务管理规定) vom 1.8.2016; § 14 Verwaltungsregeln für Webcast im Internet (**互**联网直播服务管理规定) vom 1.12.2016; § 7 Verwaltungsregeln für Foren im Internet (**互**联网论坛社区服务管理规定) vom 1.10.2017; § 8 Verwaltungsregeln für Posten im Internet (**互**联网跟帖评论服务管理规定) vom 1.10.2017; § 11 Abs. 2 Verwaltungsregeln für öffentliche Kontos im Internet (**互**联网用户公众账号信息服务管理规定) vom 8.10.2017; § 11 Abs. 2 Verwaltungsregeln für geschlossene Chatgruppe im Internet (**互**联网群组**信息服**务管理规定) vom 8.10.2017; § 12 Abs. 2 Verwaltungsregeln für Microblog im Internet (**微博客信息服**务管理规定) vom 20.3.2018.

der Totschlag und Anstiftung zu Straftaten, und die (3) Funktionalität des informationstechnischen Systems und Integrität sowie Vertraulichkeit der Daten gefährden."[582]

In Strafrechtsnormen wird auf diese Liste verwiesen.[583] Die hierbei verwendeten Begriffe sind bislang noch nicht hinreichend juristisch erfasst. Zudem sind sie ideologisch geprägt. Außerdem ist die Auflistung der schädlichen Informationen in den chinesischen Rechtsordnungen immer wieder Aktualisierungen und Neueinfügungen unterworfen. Beispielsweise wurde für den Medien- und Kulturbereich die bereits umfangreiche Liste umfassend erweitert. Danach sind Informationen, die „soziale Moral" oder „national herausragende kulturelle Traditionen" gefährden, nicht erlaubt.[584]

III. Unverhältnismäßigkeit der Eingriffe in Grundrechte durch einschränkende Gesetze

1. Verhältnismäßigkeitsbetrachtungen für deutsche Sperren

In Deutschland ist die Prüfung der Verhältnismäßigkeit immer in Betracht zu ziehen, wenn es um Internetsperren geht. Die Düsseldorfer Sperrverfügungen gegen rechtsextreme Online-Angebote waren auf § 18 Abs. 3 MDStV a.F. gestützt. Ein Access-Provider konnte allerdings nicht als Adressat in Anspruch genommen werden, weil die Sperranordnungen unverhältnismäßig waren. Beim ZugErschwG wurde das Ziel verfolgt, die Verbreitung von Kinderpornografie zu unterbinden und dadurch das Interesse der Opfer zu schützen. Die auf diesem Gesetz beruhenden Sperrverfügungen begegnen keinen Bedenken, wenn mildere alternative Maßnahmen wie das Löschen der rechtswidrigen Inhalte nicht durchgesetzt werden können. Dies war vom ZugErschwG zutreffend berücksichtigt worden. Angemessen war das ZugErschwG auch, weil die vom Gesetz vorgesehenen Sperrtechniken

---

582 *Ma*, Grundkurs der Informationssicherheit im Internet, 28; *Yu Zhigang*, Legal Forum 2014/6, 5 (6 f.).

583 Die Bestimmungen über sozialen Moral und die nationale Kultur findet man im § 16 Nr. 9 Verwaltungsregeln für audiovisuelle Programme im Internet (互联网视听节目服务管理规定) vom 20.12.2007, § 14 Nr. 9 Verwaltungsregeln zum Internet-Café (互联网上网服务营业场所管理条例) vom 6.2.2016, § 17 Nr. 9 vorläufigen Verwaltungsregeln zur Kultur im Netz (互联网文化管理暂行规定) vom 17.2.2011 und § 24 Nr. 9 Verwaltungsregeln zur Online-Presse (网络出版服务管理规定) vom 4.2.2016.

584 V. a. §§ 105 Abs. 1, § 105 Abs. 2, 111, 246, 291a Abs. 2, 293 Abs. 1 Nr. 4, 300 Abs. 1, 398 chStGB.

keine schwerwiegenden Eingriffe in die Grundrechte der Betroffen herbeiführen. Allerding waren die Sperrmaßnahmen bei der Blockade illegaler Glücksspiele nach dem GlüStV gegen inländische Online-Glücksspielanbieter unangemessen, da die damalige Geolokationstechnik nicht hinreichend zuverlässig war und die dadurch verursachten Eingriffe in die Grundrechte als gravierender eingestuft wurden. Berücksichtigt man die seitdem erfolgte Weiterentwicklung von Lokationstechniken, so wäre hier nun eine andere Betrachtungsweise angezeigt.

Letztlich ist die Verhältnismäßigkeit auch im Privatrecht zu beachten. Es gibt zwar keine unmittelbare Einwirkung der Grundrechte auf die Beziehung zwischen den Privatrechtssubjekten. Jedoch erachtet das Bundesverfassungsgericht die Grundrechte als eine objektive Werteordnung,[585] sodass sie mittelbar auch für Zivilrechtsverhältnisse gelten. Einerseits war bei den urheberrechtlichen Sperrungsanordnungen umstritten, ob die gerichtliche Rechtsfortbildung für private Sperrungsanordnungen eine taugliche Rechtsgrundlage darstellte. Andererseits wurden die betroffenen Grundrechte bei der Auslegung und Anwendung der Störerhaftung in die Abwägung mit einbezogen. Durch das Tatbestandsmerkmal der Störerhaftung wurde die Verhältnismäßigkeit der Sperrungsanordnung auch zwischen Privaten sichergestellt. Dies geschieht nun auch durch die im neuen Anspruch zur Inanspruchnahme von Access-Providern aus § 7 Abs. 4 TMG kodifizierte Verhältnismäßigkeitsprüfung. Hiernach können Access-Provider nur in Anspruch genommen werden, wenn dies verhältnismäßig ist. Dies rührt hier daher, dass sie nicht maßgeblich an der Urheberrechtsverletzung mitwirken, sie stellen in den meisten Fällen nur die Infrastruktur.

2. China

a) Relevanz des Verhältnismäßigkeitsgrundsatzes in China

In China ist das Internet bei der Verwirklichung der Grundrechte von immenser Bedeutung. Der Grund liegt vor allem darin, dass für die in der analogen Welt nicht zu entfaltenden Grundrechte, wie z.B. Meinungsfreiheit, Medienfreiheit, Vereinigungsfreiheit und Versammlungsfreiheit, das Internet in dieser Hinsicht

585 *Hesse*, 290 ff.; *Sachs*, in: Sachs, GG, Vor I Rn. 28; *Dreier*, in: Dreier, GG, Vorb. Rn. 82.

Entfaltungsmöglichkeiten bietet.[586] So wird eine Form der bürgerlichen Gesellschaft ermöglicht.[587] Der Grundsatz der Verhältnismäßigkeit ist im chinesischen Verwaltungsrecht bereits als eines der grundlegenden Rechtsprinzipien anerkannt, allerdings noch nicht verfassungsrechtlich.[588] Bei chinesischen Internetsperren handelt es sich häufig um hoheitliche Maßnahmen, die entweder von der Behörde selbst oder von Privaten als Verwaltungshelfer ergriffen werden.

b) Prüfung der Verhältnismäßigkeit

aa) Legitimer Zweck und Geeignetheit

In China zielen die Sperrungsmaßnahmen darauf ab, Staatssicherheit, soziales öffentliches Interesse und legales Rechtsinteresse der natürlichen und juristischen Personen sowie anderer Organisationen zu schützen. Hierin sind legitime Zwecke zu sehen. Die verschiedenen Sperrverfügungen sind weiterhin als geeignet anzusehen, da die gewünschten Erfolge mithilfe der Internetsperren zumindest gefördert werden können. Zu hinterfragen ist allerdings, ob anstatt der Sperrungen noch andere mildere gleich effektive Mittel bestehen.

bb) Alternativen zu den Sperrverfügungen

Das Löschen rechtswidriger Inhalte oder das Schließen von Servern kommt als alternatives Mittel in Betracht. Bereits in den chinesischen Bestimmungen zur Steuerung des Internet war das Löschen rechtswidriger Inhalte und das Schließen der betroffenen Server vorgesehen (§ 10 Nr. 7 Bestimmungen zur Steuerung des Internet). Es gibt zumindest drei Gründe, diese beiden alternativen Mittel vorrangig heranzuziehen, womit die Erforderlichkeit der Sperrungen zu verneinen ist.

Zunächst bietet der Access-Provider ohne Kenntnis der vermittelten Inhalte lediglich den Zugang zum Internet an und ist aus dem Grunde schon nicht der richtige Adressat, wenn es um die Regulierung (Sperrung) der Inhalte geht. Im Gegensatz hierzu wirkt der Inhalt- und Hostanbieter maßgeblich auf die Inhalte im Internet

---

586 *Li Yonggang*,149; *Thiel*, in: Der Begriff der Souveränität in der transnationalen Konstellation, 215 (221); *Herrera*, in: Power and security in the information age, 67 (71).

587 *Thiel*, in: Der Begriff der Souveränität in der transnationalen Konstellation, 215 (221); *Sassen*., 5 Ind. J. Global Legal Stud. 545 (549).

588 *Yang Dengfeng*, China Legal Science 2016/3, 88 (90); *Chen Jinghui*, China Legal Science 2016/3, 279 (292); *Fan Jinxue*, Journal of Comparative Law 2018/5, 106 (109).

ein. Ein Vorgehen gegen die Content- und Hostanbieter ist deshalb vorrangig in Betracht zu ziehen.

Zudem kann das Löschen oder Schließen nicht umgangen werden Auf die gelöschten rechtswidrigen Inhalte kann nicht mehr zugegriffen werden. Bei Internetsperren besteht die Möglichkeit, dass durch Umgehungstechniken weiterhin auf die Inhalte zugegriffen wird (Proxyserver).

Zuletzt wird durch die angeführten alternativen Maßnahmen geringer in grundrechtliche Positionen eingegriffen, da das Löschen oder Schließen exakt auf die illegalen Inhalte ausgerichtet ist.

cc) Interessenabwägung unter „chinesischen Vorzeichen“

Schließlich setzt die Angemessenheit der Sperrung vor allem voraus, dass das öffentliche Interesse an der Zugangsverhinderung zu bestimmten Inhalten die privaten Interessen an einem freien Zugang zu Inhalten überwiegt. In diesem Zusammenhang spielt es eine entscheidende Rolle, dass dem öffentlichen Interesse im chinesischen Recht höchste Priorität eingeräumt wird. In China unterliegen die Aufgaben der Inhaltsregulierung im Internet der Gewährleistung der Netzwerk- und Informationssicherheit. Dies gilt als einer der wichtigsten Aspekte der Staatssicherheit. Vor diesem Hintergrund tritt das Interesse des Einzelnen regelmäßig hinter dem öffentlichen Interesse der Staatssicherheit zurück.[589] Die Begriffe wie Staatssicherheit, öffentliche Sicherheit sowie öffentliches Interesse müssen aber vom Gesetzgeber konkretisiert werden und juristisch überprüfbar sein.[590] Ausgehend hiervon wäre eine Prüfung der Angemessenheit möglich. Derzeit ist zu konstatieren, dass die Sperrungen in China sehr umfangreich sind. Es ist zu bezweifeln, dass dies – auch unter „chinesischen Vorzeichen“ – einer grundrechtlichen Prüfung standhalten würde.

---

589 *Ma*, Netinfo Security 2007/1, 13 (13); *Yu Zhigang*, Legal Forum 2014/6, 5 (8); *Wang Shiwei*, Journal of Library Science in China 2015/2, 72 (78).

590 *Chen Hsin-min*, 189, 195; *Wu Qingrong*, China Legal Science 2006/4, 62 (65); *Yang Fuzhong*, Studies in Law and Business 2012/5, 32 (35).

IV. Mangel an gerichtlichem Rechtsschutz

1. Garantie für effektiven Rechtsschutz in Deutschland

Die Rechtsschutzweggarantie gemäß Art. 19 Abs. 4 GG gewährt jedermann einen lückenlosen und effektiven gerichtlichen Rechtsschutz.[591] Aufgrund dieser Rechtsschutzgarantie war z.B. im ZugErschwG der Verwaltungsrechtsweg vorgesehen (§ 12 ZugErschwG). Außerdem werden inländische Content- sowie Hostanbieter vom zuständigen BKA benachrichtigt, damit sie sich gerichtlich gegen etwaige Anordnungen zur Wehr setzen können (§ 1 Abs. 3 ZugErschwG). Die Diensteanbieter, die entweder ihren Sitz im Ausland haben oder trotz des Angebots legaler Inhalte gesperrt sind, erfahren dies zwar erst nach der Sperrung. Für sie ist aber jedenfalls nachträglicher Rechtsschutz möglich.

2. Rechtsschutzgarantie in China

a) Kodifizierung der Rechtsschutzgarantie in der chinesischen Verfassung

Die Rechtsschutzgarantie besteht ebenfalls im chinesischen Verfassungsrecht. Jede Handlung, die gegen die Verfassung oder Gesetze verstößt, kann Gegenstand einer gerichtlichen Kontrolle werden (Art. 5 Abs. 3 Satz 2 chVerf). Wie die Untersuchungen im Einzelnen ablaufen, liegt wiederum in der Hand des Gesetzgebers. Die Frage bleibt allerdings, ob eine gerichtliche Überprüfung z.B. im Fall von hoheitlichen Internetsperrungen in der Praxis gewährleistet ist.

b) Begrenzte Klagemöglichkeiten in der Realität

In China ist die Bekämpfung illegaler Inhalte hauptsächlich auf die Strafjustiz und in weniger schwerwiegenden Fällen auf die Verwaltungsstrafe angewiesen. Abgesehen vom strafprozessrechtlichen Rechtsschutz ist es im chinesischen Verwaltungsrecht nicht in jedem Fall möglich, gegen Maßnahmen der Verwaltung Klage zu erheben.[592] Im Verwaltungsprozessrecht besteht ein Numerus clausus an zulässigen Klagegründen Hierzu gehören auch die Verwaltungsstrafen. Zwar beinhaltet

---

591 *Hesse*, 150; *Sachs*, in: Sachs, GG, Art. 19 Rn. 11; *Dreier*, in: Dreier, GG, Vorb. Rn. 82.; *Schulze-Fielitz*, in: Dreier, GG, Art. 19 IV Rn. 35 ff.; *Schmidt-Aßmann*, in: Maunz/Dürig, GG, Art. 19 IV Rn. 229; *Liu Fei*, 18.

592 *Tan Weijie*, Administrative Law Review 2015/1, 89 (92); *Zhu Mang*, ECUPL Journal 2015/6, 60 (65); *Yan Erbao*, Journal of National Prosecutors College 2015/4, 16 (19).

das chinesische Verwaltungsprozessrecht eine Öffnungsklausel auch für andere Klagegründe, nach der der Verwaltungsrechtsweg auch eröffnet ist, soweit in das Persönlichkeits- und Eigentumsrecht der Betroffenen eingegriffen wird (§ 12 Abs. 1 Nr. 12 Verwaltungsprozessrecht[593]). In der Rechtspraxis spielt diese Öffnungsklausel nur eine untergeordnete Rolle, sodass zahlreiche Verwaltungsrechtsstreite vor Gericht nicht geklärt werden können. Werden die Täter wegen Internetsperrung nicht bestraft, so kommt die Rechtsschutzmöglichkeit also lediglich theoretisch in Betracht. Dies erklärt teilweise die Privatisierung der Verwaltungsklage, wobei die Betroffenen anstatt der Verwaltungsklage nun die Zivilklage bevorzugen, sowie bereits in den Fällen *Du vs. Shanghai Telekom*, *Wang vs. China Unicom*, *Xu vs. Sina Weibo*, *Zhang vs. Xiamen ZZY* und *Hu vs. Beijing Xinnet*, gezeigt.[594] Das Oberste Volksgericht hat dennoch eine Mitteilung innerhalb vom Justizsystem[595] erlassen, in der Klagen gegen die staatliche Inhaltskontrolle im Internet ausgeschlossen werden. Es besteht also letztlich kein Rechtsschutz gegen Sperrverfügungen oder sonstige Anordnungen, die im Rahmen der Inhaltskontrolle des Internet ergehen. Es besteht also ein großer Mangel am gerichtlichen Rechtsschutz.

c) Fehlen einer Verfassungsgerichtsbarkeit

Auf der verfassungsrechtlichen Ebene fehlt es in China bislang noch an der Verfassungsgerichtsbarkeit. Es ist auch nicht damit zu rechnen, dass sich hieran etwas in naher Zukunft ändern wird. Zwar wird der chinesischen Verfassung die höchste Geltungskraft zugesprochen (Art. 5 chVerf). Diese Aussage ist jedoch nicht mit Inhalt gefüllt. Nach herrschender Meinung kommt eine Verfassungsgerichtsbarkeit wie in Deutschland nicht in Frage, weil lediglich der Nationale Volkskongress

---

593 Verwaltungsprozessgesetz (**行政**诉讼法) vom 1.7.2017.

594 (2007) Pu Min Yi Chu Zi Nr. 6518 (**浦民一初字第** 6518 **号**); ein Mann aus Shenzhen verklagt China-Unicom wegen Google-Sperren (**深圳男子状告中国**联通封锁谷歌), <http://www.bbc.com/zhongwen/simp/china/2014/09/140904_china_activist_google.shtml >, ［Stand: 7.8.2019］; (2011) Hai Min Chu Zi Nr. 26297 (**海民初字第** 26297 **号**); (2012) Yi Zhong Min Zhong Zi Nr. 01854 (**一中民**终字第 01854 **号**); die geschlossene Webseite gewann den Prozess gegen den Vollstrecker des Internetsperrens (**被关停网站告**赢封网执行者.

595 Mitteilung des Obersten Volksgerichts zur Überprüfung der Eröffnung des Verfahrens in Bezug auf Verwaltung des Internets (**最高人民法院关于涉及互**联网管理案件立案审查工作的通知) vom 13.7.2009.

als das höchste Organ sowie sein ständiger Ausschuss das Recht hat, die Durchführung der Verfassung zu überwachen.[596] Darüber hinaus betont die kommunistische Partei Chinas ausdrücklich, dass in China kein Raum für Gewaltenteilung, den westlichen Konstitutionalismus sowie den westlichen Rechtstaat besteht. Es gehe vielmehr darum, einen eigenen Weg hin zu einem modernen Staat zu finden.

d) Aufsicht über Einhaltung der Verfassung durch den nationalen Volkskongress

Als Alternative zum Verfassungsgericht wurde zur Einhaltung und Umsetzung der Verfassung die Aufsicht durch den nationalen Volkskongress sowie seines ständigen Ausschusses vorgeschlagen.[597] Folglich wurde eine Abteilung, die für die Kontrolle der Verfassungsmäßigkeit und Rechtsmäßigkeit der Gesetze im materiellen Sinne zuständig ist, eingerichtet. Formelle Gesetze wurden von der Kontrolle durch den Ausschuss ausgeschlossen. Bislang wurden nur einige Anträge von der Abteilung angenommen.[598] Aufgrund des Fehlens der Verfassungsgerichtsbarkeit wird über eine Normenkontrolle und den Grundrechtsschutz in Fällen der Internetsperren nicht diskutiert.

e) Fazit

Die Gesetze, die zu Internetsperrverfügungen ermächtigen, weisen theoretisch zwar verfassungsrechtliche Mängel auf. Jedoch kann in China keine entsprechende Normenkontrolle oder Verfassungsbeschwerde stattfinden. Gegen eine Strafe, sowohl aus dem Strafrecht als auch aus dem Verwaltungsstrafrecht, wird der Rechtschutz lediglich auf das eigene Rechtschutzsystem beschränkt. In den anderen Fällen haben die Betroffenen zwar bewusst Zivilklagen erhoben, jedoch wurden diese entweder vom Gericht nicht angenommen oder zurückgewiesen.

---

596 *Cai Dingjian*, Chinese Journal of Law 2015/5, 110 (111 ff.); *Yu Wenhao*, China Legal Science 2018/6, 43 (44); *Xie Yu*, Political Science and Law 2018/7, 66 (67).

597 *Yu Wenhao*, China Legal Science 2018/6, 43 (43); *Miao Lianying*, Law Review 2018/6, 1 (3); *Fan Jinxue*, ECUPL Journal 2018/4, 13 (14.)

598 *Yu Wenhao*, China Legal Science 2018/6, 43 (45 f.); *Fan Jinxue*, ECUPL Journal 2018/4, 13 (14 ff.); *Tian Wei*, ECUPL Journal 2018/4, 29 (30 ff.).

V. Zusammenfassung

Die Darstellung hat gezeigt, dass das chinesische Sperrensystem Schwächen hinsichtlich rechtsstaatlicher Gewährleistungen aufweist. Obwohl von der Rechtsordnung vorgeschrieben, bestehen Defizite. Da die Sperrmaßnahmen kaum Begrenzungen unterliegen, werden die Anforderungen des Verhältnismäßigkeitsgrundsatzes in der Regel nicht erfüllt sein. Am auffälligsten sind die Mängel in Bezug auf den Rechtsschutz. Das Fehlen einer Verfassungsgerichtsbarkeit führt dazu, dass Bürger Sperrmaßnahmen nicht auf den Grund gehen können. Warum eine Information gesperrt wurde, ist keiner gerichtlichen Kontrolle unterworfen. Dies gilt auch für Sperrmaßnahmen zwischen Privaten. Legt man deutsche Maßstäbe an, so sind auch die Ausgestaltungen in Bezug auf den Grundsatz des Vorbehalts des Gesetzes zu kritisieren. Viele der relevanten Vorschriften für Internetsperren sind nicht in Gesetzen, sondern in untergesetzlichen Ausführungsbestimmungen geregelt. Der Grundsatz des Vorbehalts des Gesetzes ist in China jedoch nicht so ausgeprägt wie in Deutschland. Diese Dogmatik kann auch nicht einfach auf das chinesische Rechtssystem übertragen werden, weshalb die chinesischen Rechtstraditionen zu berücksichtigen sind.

D. Vorschläge für die Inhaltsregulierung sowie Internetsperren vor dem Hintergrund des politischen Systems in China

Die Ausführungen unter C. haben Defizite der Rechtslage in China offenbart. In diesem Abschnitt werden Vorschläge formuliert, wie diesen Defiziten begegnet werden kann. Hierbei sollen die Besonderheiten des politischen Systems in China berücksichtigt werden. Die folgenden Vorschläge sind somit als Annäherung an eine rechtsstaatlichen Gewährleistungen gerecht werdende Inhalteregulierung. Als zentral haben sich drei Defizite herausgestellt, die dringend behoben werden sollten:

I. Unterscheidung zwischen Inhaltsregulierung und Netzwerk- und Informationssicherheit

Aufgrund der Verwischung zwischen Datensicherheit und Inhaltssicherheit ist Inhalts*regulierung* in China der Netzwerk- und Informationssicherheit zugeordnet.

Der Gegenstand der Inhaltsregulierung setzt zwar die Integrität, Nutzbarkeit, Vertraulichkeit, Kontrollierbarkeit und Unveränderlichkeit der Daten voraus. Das heißt aber nicht, dass Datensicherheit der Inhaltssicherheit gleichzustellen ist. In der Tat werden rechtswidrige Online-Inhalte in China wie z.B. Viren rechtlich als schädliche Informationen bezeichnet. Die „schädlichen" Informationen sind zwar in der Form von Spam oder Viren im Internet verbreitet, allerdings sind die meisten im *technischen* Sinne nicht schädlich. Wenn Sperrmaßnahmen unter der Netzwerk- und Informationssicherheit geführt werden, gewinnen die entsprechenden Regulierungsmaßnahmen sowie diesbezügliche Gesetze viel eher die Akzeptanz des Volkes. Dies führt jedoch streng genommen zur Rechtswidrigkeit der Sperrmaßnahmen sowie der Rechtsvorschriften, weil sie nicht den Zweck des Schutzes der Netzwerk- und Informationssicherheit erfüllen können. Um diesen nach hier vertretener Ansicht groben Fehler zu korrigieren, muss die Regulierung der Online-Inhalte mit Internetsperren aus dem „Deckmantel" der IT-Sicherheit herausgenommen und im Bereich der Inhaltsregulierung im medienrechtlichen Sinne diskutiert werden.

II. Systematisierung der Basisgesetze des Internetrechts

Das Internetrecht kann als interdisziplinäres Rechtsgebiet bezeichnet werden. In Deutschland haben insbesondere das Presserecht und das Telekommunikationsrecht viel zur Diskussion beigetragen. Ungeachtet der bisweilen schwierigen Differenzierung zwischen Internet, Presse und Rundfunk wird die Meinungsäußerung auf Internetplattformen rechtlich entweder unter presserechtlichen oder unter rundfunkrechtlichen Gesichtspunkten beurteilt. China hat in der virtuellen Welt einen pragmatischen, aber in rechtlicher Hinsicht destruktiven Weg gewählt: Zur Regulierung des Internets sind die meisten Gesetze in Form von speziellen und kleinteiligen Gesetzen erlassen worden. Dies hat zur Zersplitterung des Rechtssystems, z.B. zur Widersprüchlichkeit von Begriffen, geführt. Auch ist die Anwendung der Rechtsvorschriften erschwert. Um diesem Missstand zu begegnen braucht es eine Neuordnung und Systematisierung der derzeit bestehenden Gesetze.

III. Garantie des gerichtlichen Rechtsschutzes in China

Aufgrund des Verfassungsgebotes der Rechtsschutzweggarantie im chinesischen Recht sind der Gesetzgeber, die vollziehende Verwaltung sowie die Rechtsprechung dazu verpflichtet, in ihren Aufgabenfeldern einen Rechtsweg zu eröffnen. Unter dem Dach des sozialistischen Rechtsstaates besteht derzeit zwar wenig Raum für eine unmittelbare Verfassungsgerichtsbarkeit, jedoch entspricht die Rechtsschutzgarantie auch der Zielsetzung der KP. In diesem Sinn sind in den letzten Jahren zahlreiche chinesische Prozessordnungen novelliert worden[599], insbesondere das Verwaltungsprozessrecht, um einen umfassenderen und effektiven Rechtsschutz zu erreichen. Wie gezeigt, ist der Umfang der möglichen Klagegegenstände allerdings sehr begrenzt. Die Abteilung des nationalen Volkskongresses und ihr ständiger Ausschuss, die zur Überprüfung der Verfassungsrechtsmäßigkeit und Rechtsmäßigkeit der Gesetze im materiellen Sinne verpflichtet sind, spielen beim Rechtschutz noch eine geringe Rolle. Die Kompetenz im Bereich der verfassungsrechtlichen Normenkontrolle und der unmittelbaren Verfassungsbeschwerde muss in Zukunft weiterhin gestärkt werden.

In Deutschland zeigt sich, dass mithilfe der Rechtsinstitute der verfassungskonformen Auslegung, der mittelbaren Drittwirkung der Grundrechte und der Schutzpflicht des Staates der Verfassungsrechtsschutz durch die Instanzgerichte verstärkt wird. Eine solche Dogmatik existiert in China nicht. Es gilt zu überlegen, ob diese Instrumente zur Durchsetzung des Rechts auch in China eingesetzt werden sollten.

---

599 Wie z.B. das chinesische Verwaltungsprozessgesetz (2015), die chZPO (2017) und die chStPO (2018).

6. Kapitel ZUSAMMENFASSUNG DER WESENTLICHEN ERGEBNISSE

Als Ergebnis lässt sich festhalten, dass sowohl China als auch Deutschland zur Inhaltsregulierung Sperrmaßnahmen gegen Internetzugangsanbieter vorsehen. In China sind Anforderungen an Sperrmaßnahmen gegen Internetzugangsanbieter kaum vorhanden. Dadurch kann der Zugang zu Inhalten beliebig beschränkt werden. Die Arbeit hat gezeigt, wie sehr die Zugangsanbieter von der Politik abhängig sind. Aus rechtlicher Sicht sollten rechtsstaatlichen Belange besser zur Geltung kommen. Dies sind insbesondere der Vorbehalt des Gesetzes, der Bestimmtheitsgrundsatz und der Grundsatz der Verhältnismäßigkeit.

A. Ursprung von Internetsperren

Mit der Entwicklung der Informations- und Telekommunikationstechnik können Nationalstaaten heute in den digitalen Raum eingreifen. Ein ökonomisches Regelungsbedürfnis, der Kampf gegen Internetdelikte und der Streit um die Online-Ressourcen bieten ausreichend Gründe, traditionelle Steuerungsmittel auf die Regulierung von Internetplattformen zu übertragen. Dabei gelten die im Internet vermittelten *Informationen* als bevorzugte Regelungsobjekte. Werden Inhalte im Inland generiert, unterliegen sie der Kontrolle des betreffenden Staates. Hinsichtlich Online-Inhalten, die im Ausland generiert werden, gestaltet sich eine Inhalte-Regulierung dagegen schwieriger. Hier greifen zahlreiche Staaten auf Sperrmaßnahmen zurück. Dadurch wird der Zugang auf die betreffende Seite verhindert.

B. Internet und Souveränität

Der Cyberspace ist kein regelungsloser Raum. Vielmehr wies der Cyberspace nur kurz in seiner Anfangsphase eine große Unabhängigkeit auf. Die damaligen Internetnutzer, wovon die meisten Internet-Techniker waren, teilten gemeinsame Werteordnungen und Kodizes. Mit der These der „Souveränität des Cyberspace“ wurde in den USA versucht, den Ausschluss der Hoheitsgewalt aus diesem Raum zu begründen, da die sog. Netizen in Form eines gesellschaftlichen Vertrags ähnlichen Vertrages hier selbst Regelungen festlegten. Nach Ansicht der Netizen besitze der Cyberspace eigene virtuelle Gebiete und übe darüber selbstständig die

Gewalt aus. Gemäß der Definition aus der allgemeinen Staatslehre stellt der nur aus Netizen gebildete virtuelle Raum allerdings keinen Staat dar, da er über kein physisches Hoheitsgebiet verfügt. Vielmehr ist es so, dass sich die Souveränität der Nationalstaaten auch auf das Cyberspace erstreckt. Die Erstreckung der traditionellen Souveränität eines Staates auf den Cyberspace begründet die sog. Internet-Souveränität.

C. Sperrverfügungen in Deutschland

In Deutschland wurde über Sperranordnungen im öffentlichen Recht gegen rechtsextreme Online-Angebote, Kinderpornografie sowie Glücksspiel und im Privatrecht gegen wettbewerbs- sowie urheberrechtliche Rechtsverletzung diskutiert. Aufgrund technischer Unzuverlässigkeit, insbesondere hinsichtlich der Umgehungsmöglichkeiten von Sperrtechniken wie Schlüsselwörter-Filtern, Eingriff in DNS-Server, Blockade von IP-Adressen, und unvermeidbaren Kollateralschäden, sind all diese Sperrmaßnahmen im öffentlichen Recht Bedenken ausgesetzt. Die gerichtlichen Entscheidungen in Zusammenhang mit den „Düsseldorfer Sperrverfügungen" sind daher zu kritisieren. Es muss nämlich berücksichtigt werden, dass die Sperrverfügungen gegen Online-Inhalte in die Grundrechte der Betroffenen eingreifen. Durch Internetsperren könnte in eine Vielzahl von Grundrechten, wie z.B. in die Berufsfreiheit und in die Eigentumsfreiheit für Access-Provider, in den Schutz des Fernmeldegeheimnisses und in die Informationsfreiheit der Nutzer sowie in die Meinungsfreiheit der Inhaltsprovider, ohne verfassungsmäßig gerechtfertigt werden zu können, eingegriffen werden. Zu begrüßen ist daher die spätere Aufhebung des Zugangserschwerungsgesetzes und das Streichen ähnlicher Klauseln im Glücksspielstaatsvertrag.

Im Zivilrecht hat sich die Rechtsprechung hingegen in eine andere Richtung. Der BGH bejahte in jüngeren Urteilen die Sperrverlangen gegen Diensteanbieter wegen Urheberrechtsverletzung, wobei die Begründungen strittig. Der Gesetzgeber hat nun mit § 7 Abs. 4 TMG Klarheit geschaffen. Die Inanspruchnahme von Access-Providern ist danach möglich. Die Einhaltung von Grundrechten hängt entscheidend davon ab, dass dieser Durchsetzung des Anspruchs einer strengen Verhältnismäßigkeitsprüfung unterliegt.

D. Sperren in China

Als „Rechtsentwicklungsstaat“, der in der Rechtsgeschichte grundsätzlich eng mit Deutschland verbunden ist, hat sich China beim Thema der Internetsperren unabhängig von Deutschland entwickelt. Technisch baut China zur Inhaltskontrolle im Internet die GFW auf, die sowohl ausländische Informationen aus dem eigenen System herausdrängt als auch inländische Inhalte sperrt. Rechtlich legitimiert der Staat dies einerseits mit der Internet-Souveränität. Andererseits nutzt er zur Durchführung dieser Politik den Belang der Sicherheit, hier der IT-Sicherheit, als einen universalen Rechtfertigungsgrund. Systematisch unzutreffend ist die Bekämpfung rechtswidriger Online-Inhalte in China derzeit der IT-Sicherheit zugeordnet. Dies erklärt, warum in den letzten Jahren unzählige Gesetze zur Internetregulierung, vor allem zur Inhaltskontrolle, ohne große Diskussion in Kraft getreten sind. Die Ermächtigungsgrundlagen zum Erlass von Internetsperrmaßnahmen müssen allerdings als verfassungs- und rechtswidrig bezeichnet werden. Die Eingriffe in Grundrechte, die von den einschränkenden Gesetzen herrühren, sind am Maßstab der chinesischen Verfassung als nicht verhältnismäßig einzustufen. Die konkreten Sperrverfügungen, die auf der Basis von solchen verfassungs- und rechtswidrigen Ermächtigungsgrundlagen erlassen werden, sind abzulehnen. Wendet man deutsche Maßstäbe an, verstoßen die Gesetze gegen den Grundsatz des Gesetzesvorbehaltes. Ferner liegen auch Mängel hinsichtlich der Bestimmtheit und den Anforderungen an gerichtlichen Rechtsschutz vor.

Die dargestellten rechtlichen Defizite sind zu beseitigen. Inhaltsregulierungen sowie Internetsperren müssen rechtlich aus dem Bereich der IT-Sicherheit herausgenommen werden. Es sollte erkannt werden, dass Sperrmaßnahmen, die sich auf die Inhalte im Internet beziehen, der Inhaltsregulierung zuzuordnen sind. Dies bringt auch in materieller Hinsicht Änderungen mit sich.

E. Rechtsschutz gegen zu weitgehende Inhalteregulierung in China

Auch im sozialistischen Rechtsstaat sollte die Rechtsschutzgarantie ebenfalls sichergestellt werden. Abgesehen von einer unmittelbaren Verfassungsgerichtsbarkeit in China sollte der nationale Volkskongress sowie sein ständiger Ausschuss die Aufgaben im Bereich der Normenkontrolle und der unmittelbaren Verfassungsbeschwerde künftig erfüllen. Internetregulierung ist nicht nur auf repressive

und präventive Rechtsmittel angewiesen ist. Es sollte daher ein mehrdimensionales Regulierungssystem aufgebaut werden, in dem die technischen Ansätze, die Selbstregulierung der privaten Teilnehmer und die internationalen Kooperationen gemeinsam eine gewichtige Rolle spielen.

F. Kann sich Deutschland auch etwas von China abgucken?

Während sich Deutschland mit dem NetzDG auf dem Weg zu befinden scheint, den Privaten die Verantwortung für die Einhaltung des Rechts im Online-Bereich zu übergeben, ist dies in China in staatlicher Hand. Das NetzDG verdeutlicht aber auch, dass dem deutschen Gesetzgeber die Durchsetzung des Rechts im Internet sehr wichtig ist. Wenn es um die Durchsetzung des Rechts geht, ist der Staat – klar: insbesondere ein „starker" Staat –, der nicht von wirtschaftlichen Interessen geleitet wird, im Zweifel der bessere Akteur. Unternehmen werden ihrer Pflicht nur mit entsprechenden Sanktionsandrohungen nachkommen. Um hier ein Gleichgewicht zu schaffen, sollten in Deutschland die Behörden mehr Verantwortung und auch mehr Aufgaben in Bezug auf die Inhaltsregulierung übernehmen.

Die Darstellung des chinesischen Rechts hat gezeigt, dass dort viele kleinteilige Regelungen existieren, die jeweils auf bestimmte Angebote im Internet zugeschnitten sind. So gibt es für Messenger-Dienste, für Online-Foren oder auch für soziale Netzwerke spezielle Kodifikationen. In Deutschland hingegen werden Regelungen geschaffen, die für sämtliche Diensteanbieter gelten. Dies führt zu Abgrenzungsschwierigkeiten. In der Arbeit wurde dies am Beispiel der Access-Provider gezeigt. Diese zählen zu den Internetdiensteanbietern, werden aber letztlich ganz anders behandelt als Content- oder Hostprovider. Spezielle Regelungen betreffend die einzelnen Arten von Anbietern von Internet-Diensten könnten hier zu einer verbesserten Rechtsdurchsetzung führen.

LITERATURVERZEICHNIS

Abel, Ralf-Bernd, Geschichte des Datenschutzes, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht, München 2003, 194.

Albers, Marion, Grundlagen und Ausgestaltung der Informationsfreiheitsgesetze, ZJS 2009, 614.

Dies., Informationelle Selbstbestimmung, Baden-Baden 2005.

Anschütz, Gerhard/Thoma, Richard, Handbuch des Deutschen Staatsrechts II, Tübingen 1932.

Axer, Peter, Zitiergebot, in: Merten, Detlef/Papier, Hans-Jürgen (Hrsg.), HGR Bd. III, Heidelberg 2009, § 67.

Badura, Peter, Staatsrecht, 5. Aufl., München 2012.

Baldus, Manfred, Zur Relevanz des Souveränitätsproblems für die Wissenschaft vom öffentlichen Recht, Der Staat 1997, 381.

Baldwin, Robert/Cave, Martin/Lodge, Martin (ed.), The Oxford Handbook of Regulation, Oxford 2010.

Beaucamp, Sophie/Henningsen, Sebastian/Florian, Martin, Strafbarkeit durch Speicherung der Bitcoin-Blockchain? MMR 2018, 501.

Becker, Kim-Björn, Internetzensur in China - Aufbau und Grenzen des chinesischen Kontrollsystems, Wiesbaden 2009.

Billmeier, Eva, Die Düsseldorfer Sperrungsverfügung, Münster 2007.

Brinkmann, Tomas, Zur Aktualität des Vielfaltgebots in den Massenmedien, ZUM 2013, 193.

Bodin, Jean, Les six livres de la république, Paris 1583.

Ders., Über den Staat; Auswahl, Übersetzung und Nachwort von Gottfried Niedhart, Stuttgart 1976.

Boehme-Neßler, Volker, Das Ende des Staates? - zu den Auswirkungen der Digitalisierung auf den Staat, ZÖR 2009, 145.

Böckenförde, Ernst Wolfgang, Recht, Staat, Freiheit, Frankfurt 1991.

Bremer, Karsten, Radikal-politische Inhalte im Internet - ist ein Umdenken erforderlich? MMR 2002, 147.

Brousseau, Eric/Marzouki, Meryem, Internet Governance: Old Issues, New Framings, Uncertain Implications, in: Brousseau, Eric/Marzouki, Meryem/Meadel Ecile (eds.), Governance, Regulation and Powers on the Internet, Cambridge University Press, 2013.

Bu, Yuanshi, Rechtsdogmatik – vom Transfer des deutschen Rechts zum Transfer des deutschen Konzepts der Rechtswissenschaft, JZ 2016, 382.

Bünnigmann, Kathrin, Polizeifestigkeit im Presserecht, JuS 2016, 894.

Büssow, Jürgen/Schmeling, Margret von, Die Internetaufsicht über unerlaubtes Glücksspiel – Ein Praxisbericht aus der Sicht einer Ordnungsbehörde, ZfWG 2010, 239.

Bull, Hans Peter, Die Staatsaufgaben nach dem Grundgesetz, Heidelberg 1977.

Busse, Carl-David von: Die Methoden der Rechtsvergleichung im öffentlichen Recht als richterliches Instrument der Interpretation von nationalem Recht, Baden-Baden 2015.

Cai, Dingjian (蔡定剑), Zum Weg der chinesische Verfassungsgerichtsbarkeit (中国宪法司法化路径探索), Chinese Journal of Law (法学研究) 2015/5, 110.

Calliess, Christian, Schutzpflichten, in: Merten, Detlef/Papier, Hans-Jürgen (Hrsg.), HGR, Bd. II, Heidelberg 2006, § 44.

Chen, Hongyi (陈弘毅), Die Aufhebung der Antwort auf den Fall Qi Yuling und die Probleme der Verweisung auf Verfassung in den ordentlichen Gerichten (齐案“批复”的废止与“宪法司法化”和法院援引宪法问题), Legal Science (法学) 2009/3, 11.

Chen, Hsin-min (陈新民), Der Einfluss des deutschen Grundgesetzes auf das taiwanische öffentliche Recht, (德国基本法对台湾公法学的影响) in: Shao, Jiandong (邵建东)/Fang, Xiaomin (方晓敏) (Hrsg.), Jahrbuch des Deutsch-Chinesischen Instituts für Rechtswissenschaft der Universitäten Göttingen und Nanjing (中德法学论坛), 47.

Ders., Grundtheorien des deutschen öffentlichen Rechts (1. Teil) (德国公法学基础理论（上册）), Shandong 2001.

Chen, Peng (陈朋), Der chinesische Internet-Plan (中国的互联网计划), Radio and TV Broadcast Engineering (广播与电视技术), 1996/4, 69.

Chen, Zheng (陈征), Zum Schutzbereich der Pressefreiheit (论宪法出版自由的保护范围), Contemporary Law Review (当代法学), 2014/4, 12.

Chen, Jinghui (陈景辉), Die Allgemeinheit des Grundsatzes der Verhältnismäßigkeit und die Eigenschaft der Grundrechte (比例原则的普遍化与基本权利的性质), China Legal Science (中国法学), 2017/5, 279.

Christiansen, Per, Selbstregulierung, regulatorischer Wettbewerb und staatliche Eingriffe im Internet, MMR 2000, 123.

Clough, Jonathan, Principles of Cybercrime (2nd ed.), Cambridge University Press, 2015.

Collin, Peter, Regulierte Selbstregulierung der Wirtschaft: neue Normierungsstrukturen im späten 19. und frühen 20. Jahrhundert, ZNR 2015, 10.

Cornils, Matthias, Entterritorialisierung im Kommunikationsrecht, in: VVDStRL (76), 391.

Czychowski, Christian, Auskunftsansprüche gegenüber Internetzugangsprovidern „vor" dem 2. Korb und „nach" der Enforcement-Richtlinie der EU, MMR 2004, 514.

Ders./Nordemann, Jan Bernd, Grenzenloses Internet – entgrenzte Haftung? GRUR 2013, 986.

Degen, Thomas A., Freiwillige Selbstkontrolle der Access-Provider: ein Beitrag zur Gewährleistung einer gemeinwohlverträglichen Informationsfreiheit, Stuttgart 2007.

Ders./Emmert, Ulrich, Elektronischer Rechtsverkehr, München 2016.

Deng, Yi (邓毅), Zum Grundsatz des deutschen Gesetzesvorbehalts (德国法律保留原则论析), Administrative Law Review (行政法学研究) 2006/1, 17.

Dennert, Jürgen, Ursprung und Begriff der Souveränität, Stuttgart 1964.

Detlef, Merten, Verhältnismäßigkeitsgrundsatz, in: Merten, Detlef/Papier, Hans-Jürgen (Hrsg.), HGR Bd. III, Heidelberg 2009, § 68.

Di Fabio, Udo, Das Recht offener Staaten, Tübingen 1998.

Dietlein, Johannes/Heinemann, Jan, Intervention im Internet - Rechtsfragen der Sperrung des Zugangs zu rechtsextremistischen Internetseiten, in: Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2003, 395.

Dong, Yuanyuan (董媛媛), Netzneutralität in den USA und ihr Sinn in der Gesetzgebung (论美国"网络中立"及其立法价值), Universität des Journalismus (新闻大学) 2011/2, 57.

Döring, Reinhard, Die zivilrechtliche Inanspruchnahme des Access-Providers auf Unterlassung bei Rechtsverletzungen auf fremden Webseiten, WRP 2008, 1155.

Dörr, Dieter, Informationsfreiheit, in: Merten, Detlef/Papier, Hans-Jürgen (Hrsg.), HGR Bd. IV, Heidelberg 2011, § 103.

Dreier, Horst (Hrsg.), GG-Kommentar, 3. Aufl., Tübingen 2013.

Ders., Souveränität, in: ders., Idee und Gestalt des freiheitlichen Verfassungsstaates, Tübingen 2014, 111.

Ders./Fischer, Veronika/Raay, Anne van/ Spiecker gen. Döhmann, Indra (Hrsg.), Informationen der öffentlichen Hand - Zugang und Nutzung, Baden-Baden 2016.

Ders./Hofmann, Hasso, Parlamentarische Souveränität und technische Entwicklung, Berlin 1986.

Dunn, Emily, Lightning from the East: Heterodoxy and Christianity in Contemporary China, Brill, Leiden 2015.

Durner, Wolfgang, Fernmeldegeheimnis und informationelle Selbstbestimmung als Schranken urheberrechtlicher Sperrverfügungen im Internet, ZUM 2010, 833.

Eichensehr, Kristen E., The Cyber-Law of Nations, 103 Geo. L. J., 317 (2015).

Engel, Christoph, Globale Netze und lokale Werte, AfP 2002, 119.

Ders., Das Internet und der Nationalstaat, Bonn 1999.

Ders., Die Internet-Service-Provider als Geiseln deutscher Ordnungsbehörden: eine Kritik an den Verfügungen der Bezirksregierung Düsseldorf, MMR-Beil. 4/2003, 1.

Ewer, Wolfgang/Thienel, Tobias, Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals, NJW 2014, 30.

Fan, Jinxue (范进学), Pressefreiheit und der verfassungsrechtliche Schutz (出版自由与宪法权利的保障), Modern Law Science (现代法学) 2013/2, 605.

Ders., Zum Grundsatz der Verhältnismäßigkeit im Verfassungsrecht (论宪法比例原则), Journal of Comparative Law (比较法研究) 2018/5, 106.

Ders., Die Funktion und die Aufgabe des Komitees für Verfassung und Gesetz (全国人大宪法和法律委员会的功能与使命), ECUPL Journal (华东政法大学学报) 2018/4, 13.

Fang, Binxing (方滨兴) (Hrsg.), Zur Souveränität im Cyberspace (论网络空间主权), Peking 2017.

Fei, Liwei (费立伟), Forschung über Verbesserung des Systems der Internetsperrung (网络封锁系统的改进探索), Masterarbeit, Qingdao Universität 2009.

Feldmann, Thorsten, Zum Referentenentwurf eines NetzDG: eine kritische Betrachtung, K&R 2017, 292.

Feng, Jianpeng (冯健鹏), Die Verweisung auf die Verfassung in den chinesischen Rechtsprechungen und ihre Funktion (我国司法判决中的宪法援引及其功能), Chinese Journal of Law (法学研究), 2017/3, 44.

Franzese, Patrick W., Sovereignty in Cyberspace: Can It Exist? 64 A. F. L. Rev. 1, 1 (2009).

Franzius, Claudio, Regulierte Selbstregulierung als Koordinationsstrategie, in: Darnaculleta i Gardella, Maria Mercè/Pardo, José Esteve/ Spiecker gen. Döhmann, Indra (Hrsg.), Strategien des Rechts im Angesicht von Ungewissheit und Globalisierung Vollansicht, Baden-Baden 2015, 248.

Frey, Dieter/Rudolph, Matthias, Zugangserschwerungsgesetz, CR 2009, 644.

Dies./Oster, Jan, Internetsperren und der Schutz der Kommunikation im Internet, MMR-Beil. 2012, 1.

Dies., Haftungsregime für Host- und Access-Provider, Norderstedt 2009.

Gao, Jiawei (高家伟), Zur Strategie der Informationen als Ressource in der öffentlichen Hand (论政府信息资源化战略), Administrative Law Review (行政法学研究), 2005/3, 1.

Gerber, Carl Friedrich Wilhelm von, Grundzüge des Deutschen Staatsrechts, 1. Aufl., Leipzig, 1865.

Gercke, Marco, Zugangsprovider im Fadenkreuz der Urheberrechtsinhaber, CR 2006, 210.

Germann, Michael, Gefahrenabwehr und Strafverfolgung im Internet, Berlin 2000.

Gersdorf, Hubertus, Hate Speech in sozialen Netzwerken, MMR 2017, 439.

Goldsmith, Jack L., Internet and the Abiding Significance of Territorial Sovereignty, 5 Ind. J. Global Legal Stud. 475 (1997).

Ders./ Wu, Tim, Who controls the Internet? – Illusions of a borderless world, Oxford 2006.

Gong, Pixiang (公丕祥), Der Prozess und der Zeitplan des Wegs zum chinesischen Rechtsstaat (中国特色社会主义法治道路的时代进程), China Legal Science (中国法学), 2015/5, 29.

Gornig, Gilbert-Hanno, Territoriale Souveränität und Gebietshoheit als Begriffe des Völkerrechts, in: Gornig, Gilbert H./Horn, Hans-Detlef (Hrsg.), Territoriale Souveränität und Gebietshoheit, Berlin 2016, 35.

Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin (Hrsg.), Das Recht der Europäischen Union, 40. Aufl., München 2009.

Greve, Holger, Technische Grundlagen und Aspekte der Netzneutralität - Bericht über den Vortrag von Constanze Kurz, in: Kloepfer, Michael (Hrsg.), Netzneutralität in der Informationsgesellschaft, 13.

Ders., Access-Blocking: Grenzen staatlicher Gefahrenabwehr im Internet, Berlin 2012.

Grewlich, Klaus W., Konstitutionalisierung des "Cyberspace" - zwischen europarechtlicher Regulierung und völkerrechtlicher Governance, Baden-Baden 2001.

Grimm, Dieter, Souveränität: Herkunft und Zukunft eines Schlüsselbegriffs, Berlin 2009.

Grisse, Karina, Internetangebotssperren nach der Änderung des TMG, Ein Regelungsvorschlag zu Sperranordnungen, MMR 2018, 649.

Grundel, Jörg, Ordnungsbehördliches Vorgehen gegen Rundfunksendungen? ZUM 2010, 770.

Guggenberger, Nikolas, Das Netzwerkdurchsetzungsgesetz in der Anwendung, NJW 2017, 2577.

Guo, Yujun (郭玉军)/*Gan, Yong* (甘勇), Zur „long-arm-jurisdiction“ in den Rechtsprechungen von den U.S.A. (美国法院的“长臂管辖权”), Journal of Comparative Law (比较法研究), 2000/3, 266.

Guo, Yujun (郭玉军)/*Xiang, Zaisheng* (向在胜), Long-arm-jurisdiction in den Rechtsprechungen über Rechtstreiten im Cyberspace in den U.S.A. (网络案件中美国法院的长臂管辖权), China Legal Science (中国法学), 2002/6, 156.

Habermas, Jürgen, Hat die Demokratie noch eine epistemologische Dimension? in: ders., Ach, Europa, Frankfurt 2008, 138.

Häberle, Peter, Grundrechtsgeltung und Grundrechtsinterpretation im Verfassungsstaat - zugleich zur Rechtsvergleichung als “fünfter” Auslegungsmethode, JZ 1989, 913.

Ders., Zur gegenwärtigen Diskussion um das Problem der Souveränität, AöR 1967, 259.

Ders., Verfassungsstaatliche Staatsaufgabenlehre, AöR 1986, 595.

Härting, Niko, Internetrecht, 5. Aufl., Köln 2014.

Hain, Karl-Eberhard/Ferreau, Frederik/Brings-Wiesen, Tobias, Regulierung sozialer Netzwerke revisited, K&R 2017, 433.

Haltern, Ulrich R., Was bedeutet Souveränität?, Tübingen 2007.

Han, Ning (韩宁), Zur Rechtsmäßigkeit der Klarnamenpflicht vom Mikroblogging (微博实名制之合法性探究), Law Science (法学), 2012/4, 3.

Hasse, Florian F., Einführung in die Methodik der Rechtsvergleichung, JA 2005, 232.

Haug, Volker, Grundwissen Internetrecht, Stuttgart 2016.

He, Haibo (何海波), Ausländische Rechtsquellen in der chinesischen Verwaltungsrechtswissenschaft (中国行政法学的外国法渊源), Journal of Comparative Law (比较法研究), 2007/6, 42.

He, Qinhua (何勤华), Rechtsvergleichung im neuzeitlichen China (比较法在近代中国), Journal of Comparative Law (比较法研究), 2006/6, 125.

Ders./Wang, Jing (王静), Rechtsschutz für Rechte und Güter im Informationsrecht (信息化时代的信息利益法律保护探索), Political Science and Law (政治与法律), 2018/7, 2.

He, Qinhua (何勤华), Zum Weg zum chinesischen Rechtsstaat (论中国特色社会主义法治道路), Law and Social Development (法制与社会发展), 2015/3, 32.

He, Qinglian (何清涟), Media control in China (中国政府如何控制媒体), New York 2004.

Ders., The fog of Censorship – Media control in China (雾锁中国 — 中国大陆控制媒体策略大揭秘), Taipei 2006.

He, Yilun (何贻纶), Zur Konzeption der Staatssicherheit (国家安全观刍议), Cass Journal of Political Science (政治学研究), 2004/3, 117.

Heckmann, Dirk/Wimmers, Jörg, Stellungnahme der DGRI zum Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG), CR 2017, 310.

Heidrich, Joerg/Heymann, Britta, Die Büchse der Pandora erneut geöffnet – Der BGH und Websperren. Eine kritische Analyse der Rechtsprechung zu Internetsperren durch Access-Provider, MMR 2016, 370.

Heidrich, Joerg/Wegener, Christoph, Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten Problemfall Logging, MMR 2015, 487.

Heliosch, Alexandra, Verfassungsrechtliche Anforderungen an Sperrmaßnahmen von kinderpornographischen Inhalten im Internet: unter besonderer Berücksichtigung des Zugangserschwerungsgesetzes, Göttingen 2012.

Heller, Hermann, Staatslehre, Leiden 1934.

Ders., Die Souveränität – ein Beitrag zur Theorie des Staats- und Völkerrechts, Berlin 1927.

Herrera, Geoffrey L., Cyberspace and sovereignty – thoughts on physical space and digital space, in: Dunn Cavelty, Myriam/Mauer, Victor/Krishna-Hensel, Sai Felicia, Power and security in the information age – Investigating the role of the state in cyberspace, Farnham/Aldershot 2007, 67.

Herzog, Roman, Ziele, Vorbehalte und Grenzen der Staatstätigkeit, in: Isensee, Josef/Kirchhof, Paul (Hrsg.), HStR Bd. IV, 3. Aufl., Heidelberg 2006, § 72.

Hesse, Konrad, Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, 20. Aufl., Heidelberg 1995.

Hobbes, Thomas, Leviathan, 1676.

Hobe, Stephan, Der offene Verfassungsstaat zwischen Souveränität und Interdependenz: eine Studie zur Wandlung des Staatsbegriffs der deutschsprachigen Staatslehre im Kontext internationaler institutionalisierter Kooperation, Berlin 1998.

Ders., Cyberspace - der virtuelle Raum, in: Isensee, Josef/Kirchhof, Paul (Hrsg.), HStR Bd. XI, 3. Aufl., Heidelberg 2006, § 231.

Höch, Dominik, Nachbessern: ja, verteufeln: nein: das NetzDG ist besser als sein Ruf, K&R 2017, 289.

Höld, Florian, Das Vorabentscheidungsverfahren nach dem neuen NetzDG, MMR 2017, 791.

Hoeren, Thomas, Geolokalisation und Glücksspielrecht (Teil 1), ZfWG 2008, 229.

Ders., Geolokalisation und Glücksspielrecht (Teil 2), ZfWG 2008, 311.

Ders., Zoning und Geolocation - Technische Ansätze zu einer Reterritorialisierung des Internet, MMR 2007, 3.

Ders./Sieber, Ulrich/Holznagel, Bernd (Hrsg.), Handbuch Multimedia-Recht, 41 Aufl., 2018 München.

Ders./Bensinger, Viola, Haftung im Internet, Berlin 2014.

Hoffmann-Riem, Wolfgang, Auffangordnungen, in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen – Systematisierung und Entwicklungsperspektiven, 261.

Ders., Selbstregelung, Selbstregulierung und regulierte Selbstregulierung im digitalen Kontext, in: Fehling, Michael/Schliesky Utz (Hrsg.), Neue Macht- und Verantwortungsstrukturen in der digitalen Welt, Baden-Baden 2016, 27.

Hollenders, Anna-Sophie, Mittelbare Verantwortlichkeit von Intermediären im Netz, Baden-Baden 2012.

Holznagel, Bernd, Das Compliance-System des Entwurfs des Netzwerkdurchsetzungsgesetzes, ZUM 2017, 615.

Ders., Regulierte Selbstregulierung im Medienrecht, Die Verwaltung Beil. 4/2001, 83.

Ders., Recht der IT-Sicherheit, München 2003.

Ders./Kussel, Stephanie, Möglichkeiten und Risiken bei der Bekämpfung rechtsradikaler Inhalte im Internet, MMR 2001, 347.

Ders./Ricke, Thorsten, Sicherung der Netzneutralität – wechselseitige Auffangordnung von Rundfunk- und Telekommunikationsrecht, DuD 2011, 611.

Ders./Enaux, Christoph/Nienhaus, Christian, Telekommunikationsrecht, 2. Aufl., München 2006.

Horn, Hans-Detlef, Der Staat und "sein" Gebiet – eine durch Rechtsgrenzen gesicherte Schicksalsgemeinschaft, in: Gornig, Gilbert H./Horn, Hans-Detlef (Hrsg.), Territoriale Souveränität und Gebietshoheit, Berlin 2016, 21.

Hornig, Michael, Möglichkeiten des Ordnungsrechts bei der Bekämpfung rechtsextremistischer Inhalte im Internet, ZUM 2001, 846.

Hu, Jinguang (胡锦光), die chinesische Verfassung (中国宪法学), 3. Aufl., Peking 2106.

Hu, Ling (胡凌), Regulierung für Meinungsäußerung im chinesischen Internet (中国网络言论表达的规制), in: Fu, Hualing (傅华伶)/ Zhu, Guobin (朱国斌), Grundrecht und Konstitutionalismus (宪法权利与宪政), Hongkong 2012, 411.

Hu, Xia (胡霞), Der strafrechtliche Ansatz aus der Sicht des Staatssicherheitschutzes (国家安全视阈下刑法的预防性路径研究), Criminal Science (中国刑事法杂志) 2017/5, 30.

Huang, Zhixiong (黄志雄) (Hrsg.), Zur Internet-Souveränität: Rechtstheorie, Rechtspolitik und Praxis (网络主权论——法理、政策与实践), Peking 2017.

Imboden, Max/Johannes Bodinus, und die Souveränitätslehre: Rektoratsrede gehalten an der Jahresfeier der Universität Basel am 22. November 1963, Basel 1963.

Isensee, Josef, Staat und Verfassung, in: Isensee, Josef/Kirchhof, Paul (Hrsg.), HStR Bd. II, 3. Aufl., Heidelberg 2004, § 15.

Ders., Staatsaufgabe, in: Isensee, Josef/Kirchhof, Paul (Hrsg.), HStR Bd. IV, 3. Aufl., Heidelberg 2006, § 73.

Ders., Das Grundrecht auf Sicherheit, Berlin 1983.

Jellinek, Georg, Allgemeine Staatslehre, 3. Aufl., Berlin 1929.

Jensen, Eric Talbot, Cyber Sovereignty: The Way Ahead, 50 Tex. Int'l L. J. 275 (2015).

Jiang, Bixin (江必新)/*Li, Guangyu* (李广宇), Einige verwaltungsrechtliche Frage im Bereich der Offenlegung von Regierungsinformationen (政府信息公开行政诉讼若干问题探讨), Political Science and Law (政治与法律) 2009/3, 12.

Johnson, David R./Post, David, Law and Borders - The Rise of Law in Cyberspace, 5 Stanford Law Review 1367 (1996).

Jureit, Ulrike/Tietze, Nikola, Postsouveräne Territorialität: Die Europäische Union als supranationaler Raum, Der Staat 2016, 353.

Kahl, Wolfgang/Waldhoff, Christian/Walter, Christian (Hrsg.), Bonner Kommentar zum Grundgesetz, Stand: 195 Lfg., Heidelberg 2018.

Kalathil, Shanthi/Boas, Taylor C., The Internet and state control in authoritarian regimes – China, Cuba and the counterrevolution, Washington, D.C., 2001.

Kelsen, Hans, Allgemeine Staatslehre, Berlin 1925.

Ders., Das Problem der Souveränität und die Theorie des Völkerrechts - Beitrag zu einer reinen Rechtslehre, Tübingen 1920.

Ders., Der Wandel des Souveränitätsbegriffs, in: Del Vecchio, Giorgio, Studi filosofico-giuridici dedicati a Giorgio del Vecchio nel 25 anno di insegnamento (1904-1929), vol. 2, Modena 1931, 1.

Koenig, Christian, Das Online-Verbot der Veranstaltung und Vermittlung von Glücksspielen im Lichte der Dienstleistungsfreiheit, K&R 2007, 257.

Kersten, Jens, Schwarmdemokratie: der digitale Wandel des liberalen Verfassungsstaats, Tübingen 2017.

Ders., Georg Jellinek und die klassische Staatslehre, Tübingen 2000.

Ders., Anonymität in der liberalen Demokratie, JuS 2017, 193.

Kielmansegg, Peter, Volkssouveränität: eine Untersuchung der Bedingungen demokratischer Legitimität, Stuttgart 1977.

Kimminich, Otto, Deutsche Verfassungsgeschichte, 2. Aufl., Baden-Baden 1987.

Kischel, Uwe, Rechtsvergleichung, München 2015.

Knauff, Matthias, Der Regelungsverbund: Recht und Soft Law im Mehrebenensystem, Tübingen 2010.

Köhler, Helmut, „Täter" und „Störer" im Wettbewerbs- und Markenrecht, GRUR 2008, 1.

Kondylis, Panajotis, Montesquieu. Naturrecht und Gesetz, Der Staat 1995, 351.

Kokott, Juliane, Grundrechtliche Schranken und Schrankenschranken, in: Merten, Detlef/Papier, Hans-Jürgen (Hrsg.), HGR Bd. I, Heidelberg 2011, § 22.

Koppensteiner, Hans-Georg, Die europäische Integration und das Souveränitätsproblem, Baden-Baden 1963.

Koreng, Ansgar, Zensur im Internet, Baden-Baden 2010.

Krämer, Rike/Märten, Judith Janna, Der Dialog der Gerichte – die Fortentwicklung des Persönlichkeitsschutzes im europäischen Mehrebenenrechtsverbund, EuR 2015, 169.

Kriele, Martin, Einführung in die Staatslehre (die geschichtlichen Legitimierungsgrundlagen des demokratischen Verfassungsstaates), 5. Aufl., Opladen 1994.

Kropp, Jonathan, Die Haftung von Host- und Access-Providern bei Urheberrechtsverletzungen, Berlin 2012.

Krüger, Hartmut, Eigenart, Methode und Funktion der Rechtsvergleichung im öffentlichen Recht, in: Ziemske, Burkhardt (Hrsg.), Staatsphilosophie und Rechtspolitik - Festschrift für Martin Kriele zum 65. Geburtstag, München 1997.

Krüger, Herbert, Allgemeine Staatslehre, Stuttgart 1964.

Ders. Souveränität und Staatengemeinschaften, in: Zum Problem der Souveränität: Berichte der Deutschen Gesellschaft für Völkerrecht, Heft 1, Karlsruhe 1957, 1 ff.

Kühling, Jürgen, Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht, NJW 2014, 681.

Ders./Schall, Tobias/Biendel, Michael, Telekommunikationsrecht, 2. Aufl., Heidelberg 2014.

Ladeur, Karl-Heinz, Zur Kooperation von staatlicher Regulierung und Selbstregulierung des Internet - zugleich ein Beitrag zum Entwurf eines Informations- und Kommunikationsdienste-Gesetzes des Bundes und eines Staatsvertrags über Mediendienste der Länder, ZUM 1997, 372.

Ders./Gostomzyk, Tobias, Das Netzwerkdurchsetzungsgesetz und die Logik der Meinungsfreiheit: Ergebnisse eines Gutachtens zur Verfassungsmäßigkeit des Regierungsentwurfs, K&R 2017, 390.

Dies., Gutachten zur Verfassungsmäßigkeit des Entwurfs eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in den sozialen Netzwerken.

Lang, Andrej, Netzwerkdurchsetzungsgesetz und Meinungsfreiheit, AöR 2018, 220.

Lessig, Lawrence, Code, 2. ed., New York 2006.

Leistner, Matthias, Urheberrecht in der digitalen Welt, JZ 2014, 846.

Lerche, Peter, Vorbehalt des Gesetzes und Wesentlichkeitstheorie, in: Merten, Detlef/Papier, Hans-Jürgen (Hrsg.), HGR Bd. III, Heidelberg 2009, § 62.

Li, Dayong (李大勇), Gerüchte, Meinungsfreiheit und rechtliche Regulierung (谣言、言论自由与法律规制), Law Science (法学), 2014/1, 100.

Li, Huizong (李惠宗), Verfassungsrecht (宪法要义), 5. Aufl., Taipei 2009.

Li, Xiaoming (李晓明), Die Straftat der Verleumdung wird nicht vom Verhalten anderer bestimmt (诽谤行为是否构罪不应由他人的行为来决定), Tribune of Political Science and Law (政法论坛), 2014/1, 186.

Li, Yonggang (李永刚), Unsere Firewall – Meinungsäußerung und Kontrolle in der Ära des Internet (我们的防火墙 - 网络时代的表达与监管), Guangxi 2009.

Ders., Wandel der Inhalteregulierung im chinesischen Internet – eine Untersuchung unter Studying Public Policy (中国互联网内容监管的变迁轨迹——基于政策学习理论的简单考察), Journal of Nanjing Tech University (南京工业大学学报(社会科学版)) 2007, 44.

Li, Zhu (李竹), Das chinesische Staatssicherheitsrecht (中国国家安全法), Peking 2006.

Liesching, Marc, Die Durchsetzung von Verfassungs- und Europarecht gegen das NetzDG, MMR 2018, 26.

Lin, Feng (林峰), Die Aufhebung der Antwort auf den Fall Qi Yuling und die Zukunft der Anwendung der chinesischen Verfassung (齐案“批复”的废止与中国宪法适用的未来), Legal Science (法学), 2009/3, 27.

Lin, Laifan (林来梵), Lehrbuch der Verfassungsrechtswissenschaft (宪法学讲义), 2. Aufl., Peking 2015.

Lin, Xiaowen (林孝文), Empirische Studien über die Verweisung von ordentlichen Gerichten auf die Verfassung (我国司法判决书引用宪法规范的实证研究), Science of Law (法律科学), 2015/4, 181.

Liu, Fei (刘飞), Rechtschutz im deutschen öffentlichen Recht (德国公法权利救济), Peking 2009.

Liu, Han (刘晗), Domainsystem, Internet-Souveränität und Internet-Governance – ein historischer Rückblick und Vorschlag für heute (域名系统、网络主权与互联网治理——历史反思及其当代启示), Peking University Law Journal (中外法学), 2016/2, 518.

Liu, Hao (刘浩)/*Wang, Kai* (王锴), Regulierung von Gerüchten im Internet aus der Sicht der Verfassung (网络谣言的宪法规制), Journal of Capital Normal University, Social Sciences Edition (首都师范大学学报, 社会科学版), 2015/5, 56.

Liu, Xianquan (刘宪权), Die Gestaltung und Verbesserung des strafrechtlichen Systems für den Kampf gegen Online-Gerüchte (网络造谣、传谣行为刑法规制体系的建构与完善), The Jurist (法学家), 2016/6, 105.

Liu, Yanhong (刘艳红), Zur strafrechtlichen Jurisdiktion im Cyberspace (论刑法的网络空间效力), China Legal Science (中国法学), 2018/3, 89.

Locke, John, The Second Treatise of Government, Über die Regierung, Reclam 1974.

Ma, Ling (马岭), Der Berechtigte der Meinungsfreiheit, Pressefreiheit, Nachrichtendienstfreiheit und sein Rechtsschutz (言论自由、出版自由、新闻自由的主体及其法律保护), Contemporary Legal Science (当代法学), 2004/1, 60.

Ders., Zu den Gründen der Aufhebung der Antwort auf den Fall Qi Yuling (齐玉苓案“批复”废止“理由”析), Legal Science (法学), 2009/4, 18.

Ma, Minhu (马民虎), Zum Informationssicherheitsrecht (信息安全法研究), Shanxi 2004.

Ders., Grundkurs der Informationssicherheit im Internet (互联网信息内容安全管理教程), Peking 2007.

Ders., Rechtssystem der Informationssicherheit – Seele und Schwerpunkt (信息安全法律体系: 灵魂与重心), Netinfo Security (信息网络安全), 2007/1, 13.

Mankowski, Peter, Wider ein transnationales Cyberlaw, AfP 1999, 138.

Marberth-Kubicki, Annette, Der Beginn der Internet-Zensur, NJW 2009, 1792.

Maurer, Hartmut, Staatsrecht I - Grundlagen, Verfassungsorgane, Staatsfunktionen, 6. Aufl., München 2010.

Maunz, Theodor/Dürig, Günter (Hrsg.), GG-Kommentar, 85. EL, München 2019.

Mankowski, Peter, Die Düsseldorfer Sperrungsverfügung – alles andere als rheinischer Karneval, MMR 2002, 277.

Mayer, Franz C., Recht und Cyberspace, NJW 1996, 1782.

Mei, Xiaying (梅夏英)/*Liu, Ming* (刘明), Die wirkliche Grenze und der Wertegedanke der Haftungsregel bei Cyberdelikten (网络侵权归责的现实制约及价值考量), Science of Law (法律科学), 2013/2, 82.

Menthe, Darrel C., Jurisdiction in Cyberspace: A Theory of International Spaces, 4. Mich. Telecom, & Tech. L. Rev. 69 (1998).

Menzel, Jörg, Internationales Öffentliches Recht – Verfassungs- und Verwaltungsgrenzrecht in Zeiten offener Staatlichkeit, Tübingen 2011.

Mi, Jian, Rechtsvergleichung – Jus Commune – Weltbürgertum, in: Jung, Peter/Lambrecht, Philipp/Blasek, Katrin/Schmidt-Kessel, Martin (Hrsg.), Einheit und Vielheit im Unternehmensrecht - Festschrift für Uwe Blaurock zum 70. Geburtstag, Tübingen 2013, 337.

Miao, Lianying (苗连营), Das anfängliche Modell und die Konkretisierung der Überprüfung der Verfassungsmäßigkeit (合宪性审查的制度雏形及其展开), Law Review (法学评论), 2018/6, 1.

Mueller, Milton, Networks and states: the global politics of Internet governance, Cambridge 2010.

Naughton, John, A brief history of the future – the origins of the internet, 4. imp., London 2001.

Negroponte, Nicholas, Being digital, London 1996.

Nelson, Leonard, Die Rechtswissenschaft ohne Recht – kritische Betrachtungen über die Grundlagen des Staats- und Völkerrechts, insbesondere über die Lehre von der Souveränität, 2. Aufl., Göttingen/Hamburg 1949.

Neumann, Andreas/Koch, Alexander, Telekommunikationsrecht, 2. Aufl., Frankfurt am Main 2013.

Ni, Zhengmao (倪正茂), Zur historischen Entwicklung der Rechtsvergleichungswissenschaft (论比较法学的历史发展), in: Law and Modernization (法制现代化研究) 1997, 368.

Niedhart, Gottfried, Jean Bodin - über den Staat, Ditzingen 1986.

Nolte, Georg, Hate-Speech, Fake-News, das „Netzwerkdurchsetzungsgesetz" und Vielfaltsicherung durch Suchmaschinen, ZUM 2017, 552.

Ohler, Christoph, Die Kollisionsordnung des Allgemeinen Verwaltungsrechts, Tübingen 2005.

Ohly, Ansgar, Urheberrecht in der digitalen Welt – Brauchen wir neue Regelungen zum Urheberrecht und zu dessen Durchsetzung? NJW-Beil. 2014, 47.

Örücü, Esin, The Enigma of Comparative Law - Variations on a Theme for the Twenty-first Century, Dordrecht 2004.

Ownby, David, Falun Gong and the Future of China, Oxford 2008.

Pan, Handian (潘汉典), Rechtsvergleichungswissenschaft in China – Rückblick und Ausblick (比较法在中国：回顾与展望), Journal of Comparative Law (比较法研究) 1990/2, 1.

Pelinka, Anton, Meinungsfreiheit und Revolution unter besonderer Berücksichtigung der arabischen Welt, Jahrbuch Menschenrechte 2013, 30.

Peifer, Karl-Nikolaus, Fake News und Providerhaftung, CR 2017, 809.

Christiansen, Per, Selbstregulierung, regulatorischer Wettbewerb und staatliche Eingriffe im Internet, MMR 2000, 123.

Perritt, Henry H., Internet as a Threat to Sovereignty? - Thoughts on the Internet's Role in Strengthening National and Global Governance, 5:2 Ind. J. Global Legal Stud. 423 (1998).

Peters, Hans, Öffentliche und staatliche Aufgaben, in: Dietz, Rolf/Hübner, Heinz (Hrsg.), Festschrift für Hans Carl Nipperdey zum 70. Geburtstag, Band II, München und Berlin 1965, 877.

Peukert, Alexander, Gewährleistung der Meinungs- und Informationsfreiheit in sozialen Netzwerken, MMR 2018, 572.

Pi, Yong (皮勇), Forschung der Cybersicherheitsrecht (网络法原论), Peking 2008.

Pichler, Rufus, Internationale Zuständigkeit im Zeitalter globaler Vernetzung, München 2008.

Pieroth, Bodo/Schlink, Bernhard/Kniesel, Michael, Polizei- und Ordnungsrecht, 9. Aufl., München 2016.

Post, David G., The "Unsettled Paradox": The Internet, The State, and the Consent of the Governed, 5 Ind. J. Global Legal Stud. 521 (1998).

Pound, Roscoe, Rechtsvergleich und seine Geschichte auf der Basis des chinesischen Rechts (以中国法为基础的比较法和历史), übersetzt von Wang, Xiao Hong (王笑红), in: Wang, Jian (王健) (Hrsg.), Einflüsse des abendländischen Rechts auf den Osten – Ausländische Gelehrte und die Reform des chinesischen Rechts in der Neuzeit (西法东渐——外国人与中国近代法的变革), 2001 Peking, 78.

Putzki, Andreas/Sesing, Anna, Störerhaftung als Grundlage für Netzsperren, MMR 2016, 660.

Qi, Aimin (齐爱民), The Authentic Thesis on Information Law (信息法原论), Wuhan 2010.

Qi, Enping (齐恩平), Konflikt zwischen der Klarnamenpflicht und dem Zivilrechtsschutz (实名制政策与私权保护的博弈论), Law Science Magazine (法学杂志) 2013/7, 60.

Qie, Yongzhi (郄勇志), Mögliche Verteilung der Genehmigung vom Ministerium für Industrialisierung und Information 2018 (2018 年工信部或将发放牌照), Communications World (通信世界) 2018/1, 11.

Quaritsch, Helmut, Staat und Souveränität, Frankfurt am Main 1970.

Ders., Souveränität, Berlin 1986.

Randelzhofer, Albrecht, Staatsgewalt und Souveränität, in: Isensee, Josef/Kirchhof, Paul (Hrsg.), HStR Bd. II, 3. Aufl., Heidelberg 2004, § 17.

Rehart, Nikolaus Konstantin, Inanspruchnahme von Access-Providern im Eilverfahren, MMR 2018, 784.

Rossi, Matthias, Informationszugangsfreiheit und Verfassungsrecht - zu den Wechselwirkungen zwischen Informationsfreiheitsgrenzen und der Verfassungsordnung in Deutschland, Berlin 2004.

Ders., Staatliche Daten als Informationsrohstoff, in: Dreier, Thomas/Fischer, Veronika/Raay, Anne van/Spiecker gen. Döhmann, Indra (Hrsg.), Informationen der öffentlichen Hand – Zugang und Nutzung, Baden-Baden 2016, 145.

Roßnagel, Alexander, Konflikte zwischen Informationsfreiheit und Datenschutz? MMR 2007, 16.

Ders., Weltweites Internet - globale Rechtsordnung? MMR 2002, 67.

Ders., Zur Reichweite der staatlichen Verantwortung für Teilhabe in der digitalen Zeit, in: Fehling, Michael/Schliesky Utz (Hrsg.), Neue Macht- und Verantwortungsstrukturen in der digitalen Welt, Baden-Baden, 2016, 73.

Rottenbücher, Karl, Das Recht der freien Meinungsäußerung, in: VVDStRL (4), 6.

Rousseau, Jean-Jacques, Du contrat social ou Principes du droit politique, Amsterdam 1762.

Rubin, Alfred P., Is International Criminal Law "Universal"?, 2001 U. Chi. Legal F. 351 (2001).

Sachs, Michael (Hrsg.), GG-Kommentar, 8. Aufl., München 2018.

Sassen, Saskia, On the Internet and sovereignty, 5 Ind. J. Global Legal Stud. 545 (1998).

Schaar, Peter, Digitale Souveränität, digma 2015, 40.

Scheurle, Klaus-Dieter/Mayen, Thomas, Telekommunikationsgesetz, 3. Aufl., München 2018.

Schierbaum, Laura, Sorgfaltspflichten von professionellen Journalisten und Laienjournalisten im Internet, Baden-Baden 2016.

Schiff, Alexander, Meinungsfreiheit in mediatisierten digitalen Räumen, MMR 2018, 366.

Schmidt-Aßmann, Eberhard, Zum Standort der Rechtsvergleichung im Verwaltungsrecht, ZaöRV 2018, 807.

Ders., Regulierte Selbstregulierung als Element verwaltungsrechtlicher Systembildung, in: Ders., Aufgaben und Perspektiven verwaltungsrechtlicher Forschung: Aufsätze 1975-2005, Tübingen 2006, 255.

Ders., Der Rechtsstaat, in: Isensee, Josef/Kirchhof, Paul (Hrsg.), HStR Bd. II, 3. Aufl., Heidelberg 2004, § 26.

Schliesky, Utz, Souveränität und Legitimität von Herrschaftsgewalt, Tübingen 2004.

Ders., Eine Verfassung für den digitalen Staat? ZRP 2015, 56.

Ders., Ist der digitale Staat ein besserer Staat? in: in: Fehling, Michael/Schliesky Utz (Hrsg.), Neue Macht- und Verantwortungsstrukturen in der digitalen Welt, Baden-Baden 2016, 97.

Schmidt, Georg, Geschichte des Alten Reiches, München 1999.

Schnabel, Christoph, "Porn not found" - die Arcor-Sperre, K&R 2008, 26.

Ders., Das Zugangserschwerungsgesetz – zum Access-Blocking als "ultima ratio" des Jugendschutzes, JZ 2009, 996.

Schoch, Friedrich, Informationsfreiheitsgesetz, 2. Aufl., München 2016.

Ders., Polizei- und Ordnungsrecht, in: ders. (Hrsg.), Besonderes Verwaltungsrecht, 15. Aufl., Berlin, 2013, Kapitel 2.

Ders., Das Recht auf informationelle Selbstbestimmung in der Informationsgesellschaft, in: Michael Sachs/Helmut Siekmann/Hermann-Josef, Blanke/Johannes Dietlein/Michael Nierhaus/Günter Püttner (Hrsg.), Der grundrechtsgeprägte Verfassungsstaat - Festschrift für Klaus Stern zum 80. Geburtstag, Berlin 2012, 1491.

Schöbener, Burkhard/Knauff, Matthias, Allgemeine Staatslehre, 2. Aufl., München 2013.

Schöttle, Hendrik, Sperrungsverfügungen im Internet – machbar und verhältnismäßig? K&R 2007, 366.

Schulze-Gävernitz, Hermann Johann Friedrich von, Lehrbuch des deutschen Staatsrechtes Bd. 1, Leipzig, 1881.

Schulze, Sven-Hendrik, Cyber-"War" – Testfall der Staatenverantwortlichkeit, Tübingen 2015.

Schwarzenegger, Christian, Sperrverfügungen gegen Access-Provider – über die Zulässigkeit polizeilicher Gefahrenabwehr durch Sperranordnungen im Internet, in: Arter, Oliver/ Jörg, Florian S. (Hrsg.), Internet-Recht und electronic commerce law, 3. Tagungsband, Bern 2003, 249.

Sesing, Andreas/Baumann, Jonas, Sperranspruch statt Störerhaftung?, MMR 2017, 583.

Shen, Zongling (沈宗灵), Grundfragen der Rechtsvergleichungswissenschaft (比较法学的几个基本理论问题), Journal of Peking University, Philosophical and Social Sciences (北京大学学报 哲学社会科学版) 1985/1, 29.

Sieber, Ulrich, Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen: neue Herausforderungen des Internet (1), JZ 1996, 429.

Ders., Verantwortlichkeit im Internet - technische Kontrollmöglichkeiten und multimediarechtliche Regelungen: zugleich eine Kommentierung von § 5 TDG und § 5 MDStV, München 1999.

Ders., Sperrverpflichtungen gegen Kinderpornographie im Internet, JZ 2009, 653.

Ders./Nolde, Malaika, Sperrverfügungen im Internet: Nationale Rechtsdurchsetzung im globalen Cyberspace? Berlin 2008.

Simitis, Spiros, Chancen und Gefahren der elektronischen Datenverarbeitung - Zur Problematik des „Datenschutzes", NJW 1971, 673.

Shapiro, Martin, The Globalization of Law, 1 Ind. J. Global Legal Stud. 37 (1993).

Smend, Rudolf, Verfassung und Verfassungsrecht, Berlin 1928.

Ders., Staatsrechtliche Abhandlungen und andere Aufsätze, 2. Aufl., Berlin 1968.

Ders., Das Recht der freien Meinungsäußerung, in: VVDStRL (4), 44.

Sommermann, Karl-Peter, Funktionen und Methoden der Grundrechtsvergleichung, in: Merten, Detlef/Papier, Hans-Jürgen (Hrsg.), HGR Bd. I, Heidelberg 2011, § 16.

Spies, Axel/Ufer, Frederic, Quo vadis Netzneutralität? Status quo und Ausblick – ein langer Weg zu einem tragfähigen Kompromiss in der EU, Deutschland und den USA, MMR 2015, 91.

Spindler, Gerald, Störerhaftung für Access-Provider reloaded, GRUR 2018, 1012.

Ders./Schmitz, Peter/Liesching, Marc, Telemediengesetz, Kommentar, 2. Aufl. München 2018.

Ders., Das Netzwerkdurchsetzungsgesetz, K&R 2017, 533.

Ders., Zivilrechtliche Sperrverfügungen gegen Access Provider nach dem EuGH-Urteil „UPC Telekabel", GRUR 2014, 826.

Ders., Das neue Telemediengesetz - Konvergenz in sachten Schritten, CR 2007, 239.

Ders., Das Gesetz zum elektronischen Geschäftsverkehr: Verantwortlichkeit der Diensteanbieter und Herkunftslandprinzip, NJW 2002, 921.

Ders./Volkmann, Christian, Die öffentlich-rechtliche Störerhaftung der Access-Provider, K&R 2002, 398.

Ders./Schuster, Fabian, Recht der elektronischen Medien, München 2015.

Stadler, Thomas, Sperrungsverfügung gegen Access-Provider, MMR 2002, 343.

Ders. Haftung für Information im Internet, 2. Aufl., Berlin 2005.

Ders., Kein erschwerter Zugang, MMR 2009, 581.

Starck, Christian, Staat und Religion, JZ 2000, 1.

Ders., Rechtsrezeptionen in Ostasien, JZ 2016, 377.

Ders., Rechtsvergleichung im öffentlichen Recht, JZ 1997, 1021.

Stern, Klaus, Das Staatsrecht der Bundesrepublik Deutschland, Band IV/1, Der Schutz und die freiheitliche Entfaltung des Individuums, München, 2006.

Ders., Das Staatsrecht der Bundesrepublik Deutschland, Band V, Die geschichtlichen Grundlagen des deutschen Staatsrechts, München, 2000.

Stettner, Rupert, Schutz des Brief-, Post- und Fernmeldegeheimnisses, in: Merten, Detlef/Papier, Hans-Jürgen (Hrsg.), HGR Bd. IV, Heidelberg 2011, § 92.

Stoll, Peter-Tobias, Sicherheit als Aufgabe von Staat und Gesellschaft, Tübingen, 2003.

Stürner, Rolf, Das Zivilrecht der Moderne und die Bedeutung der Rechtsdogmatik, JZ 2012, 10.

Sun, Wanhuai (孙万怀)/*Lu, Hengfei* (卢恒飞), Rationale Behandlung zur Online-Gerüchte im Strafrecht (刑法应当理性应对网络谣言), Law Science (法学) 2013/11, 3.

Sunstein, Cass R., Republic.com, New Jersey 2001.

Taeger, Jürgen, Die Entwicklung des IT-Rechts 2013, NJW 2013, 3698.

Tan, Weijie (谭炜杰), Über den passiven Umfang der Zulässigkeit im Verwaltungsprozess (行政诉讼受案范围否定性列举之反思), Administrative Law Review (行政法学研究), 2015/1, 89.

Tang, Shoulian (唐守廉), Internet und Governance (互联网及其治理), Peking 2008.

Tang, Zicai (唐子才) /*Liang, Xiongjian* (梁雄健), Theorie und Praxis der Internetregulierung (互联网规制理论与实践), Peking 2008.

Tettenborn, Alexander, Europäischer Rechtsrahmen für den elektronischen Geschäftsverkehr, K&R 1999, 252.

Ders., Auf dem Weg zu einem einheitlichen Rechtsrahmen für den elektronischen Rechtsverkehr, K&R 1999, 442.

Ders., E-Commerce-Richtlinie: politische Einigung in Brüssel erzielt, K&R 2000, 59.

Thiel, Markus, Die "Entgrenzung" der Gefahrenabwehr - Grundfragen von Freiheit und Sicherheit im Zeitalter der Globalisierung, Tübingen 2011.

Thiel, Thorsten, Internet und Souveränität, in: Volk, Christian/Kuntz, Friederike (Hrsg.), Der Begriff der Souveränität in der transnationalen Konstellation, Baden-Baden 2014, 215.

Tian, Wei (田伟), Die Prozessarten für die Überprüfung der Verfassungsmäßigkeit im Komitee für Verfassung und Gesetz (宪法和法律委员会规范合宪性审查的程序类型), ECUPL Journal (华东政法大学学报), 2018/4, 29.

Trachtman, Joel P., Cyberspace, Sovereignty, Jurisdiction, and Modernism, 5 Ind. J. Global Legal Stud. 561 (1998).

Triepel, Heinrich, Völkerrecht und Landesrecht, Leipzig 1899.

Trute, Hans-Heinrich, Die Verwaltung und das Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung, DVBL 1996, 950.

Twining, William, Globalization and Comparative Law, übersetzt von Wu, Dawei (吴大伟) in: Örücü, Esin/Nelken, David (Hrsg.), Comparative Law - A Handbook, chinesische Übersetzung, Peking 2012, 78.

von Mangoldt, Hermann/Klein, Friedrich/Starck, Christian, Grundgesetz-Kommentar, 7. Aufl. München 2018.

von Münch, Ingo/Kunig, Philip (Hrsg.), Grundgesetz-Kommentar, 6. Aufl. München 2012.

Wang, Dongguang (王东光), Prüfung der Staatssicherheit (国家安全审查), Peking University Law Journal (中外法学), 2016/5, 1289.

Wang, Jianjun (王建军), Ein erster Gerichtsfall zwischen Blogger und der Kläger, den der Blogger gewinnt (首例博客告博客原告一审胜诉), Legal Daily (法制日报), v. 12.9.2006.

Wang, Shengming (王胜明) (Hrsg.), Kommentar zum Gesetz über die Haftung für die Verletzung von Rechten (中华人民共和国侵权责任法释义), Peking 2013.

Wang, Shizhou (王世洲), Die Dogmatik der Straftat der Gefährdung der Staatssicherheit (危害国家安全罪的信条学考察), Criminal Science (中国刑事法杂志), 2012/8, 9.

Wang, Shiwei (王世伟), Zur Informationssicherheit, Cybersicherheit und Sicherheit im Cyberspace (论信息安全、网络安全、网络空间安全), Journal of Library Science in China (中国图书馆学报), 2015/2, 72.

Wang, Xigen (汪习根), Fragen auf dem Weg zum chinesischen Rechtsstaat (法治中国的道路选择), Law Science Magazine (法学杂志) 2018/1, 17.

Wang, Xixin (王锡锌), Zum Staatsgeheimnis im Informationsfreiheitsrecht (政府信息公开语境中的“国家秘密”探讨), Political Science and Law (政治与法律) 2009/3, 2.

Wang, Yi (王怡), Volkes Stimme im Internet und „Verfahrensgerechtigkeit“ (网络民意与“程序正义”), China Newsweek (中国新闻周刊), 2004/3, 64.

Wang Zuofu (王作富), Strafrecht BT in der Praxis (刑法分则实务研究) Band I-III, 3. Aufl., Peking 2007.

Wei, Yongzheng (魏永征), Lehrbuch des Rechts für Journalismus und Kommunikation (新闻传播法教程), 3. Aufl., Peking 2010.

Ders., Meinungsfreiheit und Verleumdung im Internet (言论自由和网上诽谤), Cass Journal of Foreign Law (环球法律评论) 2001/1, 69.

Wimmers, Jörg/Heymann, Britta, Zum Referentenentwurf eines Netzwerkdurchsetzungsgesetzes (NetzDG): eine kritische Stellungnahme, AfP 2017, 93.

Wu, Timothy S., Cyberspace Sovereignty – The Internet and the International System, 10 Harv. JL & Tech. 648 (1997).

Wu, Qingrong (吴庆荣), Zur Staatssicherheit als juristischer Begriff (法律上国家安全概念探析), China Legal Science (中国法学), 2006/4, 62.

Wu, Yuxin (吴雨欣), Öffnung der virtuellen Telekommunikationsdienste für das ausländische und private Kapital (虚商大门向民资、外资打开), Foreign Investment in China (中国外资), 2018/11, 46.

Würtenberger, Thomas, Polizei- und Ordnungsrecht, in: Ehlers, Dirk/Fehling, Michael/Pünder, Hermann (Hrsg.), Besonderes Verwaltungsrecht Bd. III, 3. Aufl., Heidelberg 2013, § 69.

Xie, Yongjiang (谢永江)/*Ji, Fankai* (纪凡凯), Zur Verbesserung des Internetrechts (论我国互联网管理立法的完善), Journal of Chinese Academy of Governance (国家行政学院学报), 2010/5, 94.

Xie, Yu (谢宇), Die Umgestaltung der Theorie und des Regimes der Verfassungsgerichtsbarkeit (宪法司法化理论与制度生命力的重塑), Political Science and Law (政治与法律), 2018/7, 66.

Xie, Zhiyong (解志勇)/*Yu, Peng* (于鹏), Rechtsvergleichung im Bereich der Informationssicherheit (信息安全立法比较研究), Peking 2007.

Xing, Binwen (邢斌文), Wie verweist das Gericht auf die Verfassung? (法院如何援引宪法), China Law Review (中国法律评论), 2015/1, 127.

Xiong, Wencong (熊文聪), Das Notice-and-Takedown-Verfahren nach dem „Safe Harbor"-Prinzip (避风港中的通知与反通知程序), Journal of Comparative Law (比较法研究), 2014/4, 122.

Xu, Yongzhong (徐永忠), Der Status quo und die Entwicklung von CHINANET (CHINANET 的现状与发展), China Information Industry Policy & Decisionmaking (电子展望与决策), 1997/6, 12.

Xu, Wei (徐伟), Die Grenzen des Notice-and-Takedown-Verfahrens und die Verbesserungsmöglichkeiten für das Cyberdeliktsrecht (网络侵权治理中通知移除制度的局限性及其破解), Law Science (法学) 2015/1, 131.

Ders., Die Frage nach der gemeinsamen Haftung für Internetdienstanbieter (网络服务提供者连带责任之质疑), Law Science (法学), 2012/5, 82.

Yan, Erbao (闫尔宝), Die Entwicklung und die Probleme des Umfangs der Zulässigkeit im Verwaltungsprozess (行政诉讼受案范围的发展与问题), Journal of National Prosecutors College (国家检察官学院学报), 2015/4, 16.

Yao, Zhiwei (姚志伟), Das „Safe Harbor"-Prinzip im Schatten des öffentlichen Rechts (公法阴影下的避风港), Global Law Review (环球法律评论), 2018/1, 101.

Yang, Dengfeng (杨登峰), Vom Prinzip der Rationalität zum einheitlichen Grundsatz der Verhältnismäßigkeit (从合理原则走向统一的比例原则), China Legal Science (中国法学) 2016/3, 88.

Yang, Fuzhong (杨福忠), Der verfassungsrechtliche Schutz für anonyme Meinungsäußerungen im Internet (公民网络匿名表达权之宪法保护), Studies in Law and Business (法商研究), 2012/5, 32.

Yang, Liu (杨柳), Die rechtdogmatische Analyse zum 500-maligen Weiterleiten von Online-Posts ("诽谤信息转发 500 次入刑"的法教义学分析), Law Science (法学) 2016/7, 137.

Yin, Jianguo (尹建国), Feststellung des Umfangs der schädlichen Informationen in China (我国网络有害信息的范围判定), Politcal Science and Law (政治与法律), 2015/1, 102.

Yu, Wenhao (于文豪), Die Ausübung der Befugnisse des Komitees für Verfassung und Gesetz (宪法和法律委员会合宪性审查职责的展开), China Legal Science (中国法学), 2018/6, 43.

Yu, Zhigang (于志刚), Das Eindringen des Problems der Cybersicherheit in die öffentliche Sicherheit sowie Staatssicherheit und Gegenmaßnahmen (网络安全对公共安全、国家安全的嵌入态势和应对策略), Legal Forum (法学评论), 2014/6, 5.

Ders., Der Anwendungsbereich des traditionellen Strafrechts in der „doppelten Gesellschaft“ (“双层社会”中传统刑法的适用空间), Law Science (法学) 2013/10, 102.

Yuan, yuan (原媛), Design der GFW zum Filtern der rechtswidrigen Meinungsäußerungen (基于感情色彩词的非法信息过滤防火墙的设计), Masterarbeit, Universität Shanxi 2008.

Yun, Qin (云晴), Beobachtung und Nachdenken über eine Reform im Telekommunikationswesen (通信业改革的观察和思考), Communications World (通信世界) 2017/25, 32.

Zippelius, Reinhold, Allgemeine Staatslehre, 13 Aufl., München 1999.

Ders. Geschichte der Staatsideen, 9. Aufl., München 1994.

Zhang, Fengzhen (张峰振), Zum Gesetzesvorbehalt im Verfassungsrecht (), Tribune of Political Science and Law (论宪法保留) 2018/4, 35.

Zhang Jun (张军), Neue Auslegung zum Strafrecht BT (刑法<分则>及配套规定新释新解) Band I-II, 3. Aufl., Peking 2013.

Zhang Mingkai (张明楷), Strafrechtswissenschaft (刑法学), 4. Aufl., Peking 2011.

Ders., Zum Streitstand der rechtlichen Behandlung der Verleumdung im Internet (网络诽谤的争议问题探究), China Legal Science (中国法学) 2015/3, 60.

Zhang, Qianfan (张千帆), Einführung in das Verfassungsrecht (宪法学导论), 3. Aufl., Peking 2014.

Ders., Die Anwendung des Strafrechts muss sich an den Grundgedanken der Verfassung orientieren (刑法适用应遵循宪法的基本精神), Law Science (法学), 2015/4, 3.

Zhang, Wei (张慰), Zusammenfassung und Kritik zum Wesentlichkeitsvorbehalt ("重要性理论"之梳理与批判), Administrative Law Review (行政法学研究), 2011/2, 113.

Zhang, Xiang (张翔), Die verfassungsrechtliche Dogmatik (宪法释义学), Peking 2014.

Ders., Die normative Konstruktion der Grundrechte (基本权利的规范建构), Peking 2017.

Zhang, Xinyu (张新宇), Verwaltungsrechtliche Regulierung und Verbesserung der Handhabung von Online-Gerüchten (网络谣言的行政规制及其完善), Studies in Law and Business (法商研究), 2016/3, 63.

Zhang, Yanying (章彦英), Rechtsvergleichung in China vor dem Hintergrund der Globalisierung – Geschichte, Notlage und Ausweg (全球化背景下的中国比较法:历史、困境与前路), Journal of Comparative Law (比较法研究), 2014/5, 191.

Zhang, Zhengping (张正平), Die Subjektivität und ihre Überwindung bei der Qualifizierung der Staatsgeheimnisse (定密的主观性及其克服), Studies in Law and Business (法商研究), 2012/2, 83.

Zhao, Hong (赵宏), Schranken der Schranken (限制的限制), The Jurist (法学家), 2011/2, 152.

Zhi, Zhenfeng (支振锋), Der Rechtsweg zum globalen Internet-Governance (互联网全球治理的法治之道), Law and Social Development (法制与社会发展), 2017/1, 91.

Zhou, Huifang (周慧芳), Technik und ihre Probleme bei der Implementierung von Internetsperren (因特网中不良信息的过滤技术及存在问题), Journal of intelligence (情报杂志) 2004/6, 25.

Zhou, Shangjun (周尚君)/Cao, Ting (曹庭), Einschränkung des Rechts aus der Sicht der umfassenden Staatssicherheit (总体国家安全观视角下的权利限制), Law and Social Development (法制与社会发展), 2018/3, 40.

Zhu, Mang (朱芒), Der allgemeine Umfang der Zulässigkeit im Verwaltungsprozessrecht (概括主义的行政诉讼"受案范围"), ECUPL Journal 2015/6, 60.

Zimmermann, Andreas, Polizeiliche Gefahrenabwehr und das Internet, NJW 1999, 3145.

Zweigert, Konrad/Kötz, Hein, Einführung in die Rechtsvergleichung auf dem Gebiet des Privatrechts, Tübingen 1996.