*Marco Gercke**

Die Sperrung von Internetseiten im Kampf gegen illegale Inhalte im Internet

Seit mehreren Jahren werden neben juristischen Ansätzen zur Bekämpfung der Internetkriminalität, wie der Harmonisierung von Strafvorschriften und internetspezifischen prozessualen Ermittlungsinstrumenten, auch technische Lösungsansätze diskutiert. Ein solcher Lösungsansatz ist die Verhinderung der Möglichkeit des Zugriffs auf illegale Inhalte im Internet. Der Beitrag gibt einen Überblick über die Entwicklung der Diskussion in Deutschland und stellt die Möglichkeiten und Probleme entsprechender Maßnahmen dar.

1 Von der Diskussion um Sperrmaßnahmen zum Zugangserschwerungsgesetz

1.1 Diskussion um die Sperrung von Inhalten in Deutschland bis 2008

Zu einem Zeitpunkt, zu dem im europäischen[1] und nicht-europäischen[2] Ausland bereits seit mehreren Jahren unterschiedliche technische Ansätze zur Verhinderung des Zugriffs auf illegale Inhalte diskutiert und teilweise auch eingesetzt wurden, beschränkte sich die Diskussion in Deutschland bis 2008 im Wesentlichen auf Sperrverfügungen im Hinblick auf extremistische Internetangebote.[3] Abgesehen von diesen verwaltungsrechtlichen Ansätzen wurde lediglich in geringem Umfang seitens der Industrie der Versuch unternommen, Zugangsprovider auf zivilrechtlichem Wege zu verpflichten, einen Zugriff auf Internetseiten mit jugendgefährdenden Inhalten („YouPorn"-Sperrung[4]), bzw. Urheberrechtsverletzungen unterstützenden Inhalten („E-Donkey"-Linkseiten[5]) zu sperren.

---

* Prof. Dr. Marco Gercke ist Direktor des Cybercrime Research Institute und Honorarprofessor an der Universität zu Köln.

1 Vgl. beispielsweise: *Clayton*, Failures in a Hybrid Content Blocking System in: Privacy Enhancing Technologies, 2006, S. 79; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, S. 46 ff.; Schweden: *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, S. 59 ff; *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Research Service, Nov. 2008, S. 6; Schweiz: *Sieber/Nolde*, Sperrverfügungen im Internet, 2008, S. 55; *Schwarzenegger*, Sperrverfügungen gegen Access-Provider in: Arter/Joerg, Internet-Recht und Electronic Commerce Law, S. 250.

2 Vgl. beispielsweise: China: *Clayton/Murdoch/Watson*, Ignoring the Great Firewall of China, abrufbar unter: http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf; *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfügungen gegen Access-Provider, Technisches Gutachten, abrufbar unter: http://www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf.

3 Vgl. dazu beispielsweise: VG Düsseldorf, CR 2005, 885 ff; VG Düsseldorf, ITRB 2003, 194 ff.; VG Köln, CR 2006, 201; *Stadler*, MMR 2002, 343 ff; Weiterführend: *Gercke* in Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rn. 31.

4 Vgl. *Frey*, MMR 2009, 222.

5 Vgl. dazu *Gercke*, ZUM 2006, 593 ff.

1.2 Diskussion um die Sperrung von Internetseiten mit kinderpornographischen Inhalten

Ab dem Jahr 2008 erhielt die Diskussion neuen Auftrieb. Den Anfang machte im August 2008 der Chef des Bundeskriminalamts. Dieser forderte, Internetzugangsprovider gesetzlich zur Sperrung kinderpornographischer Inhalte zu verpflichten.[6] Im November 2008 schloss sich die Bundesfamilienministerin der Forderung nach einer Sperrung von Internetseiten mit kinderpornographischen Inhalten an.[7] Dabei folgte auch sie zunächst dem Ansatz einer gesetzlichen Verpflichtung der Zugangsprovider zur Sperrung bestimmter Internetseiten.[8] Vor dem Hintergrund der einsetzenden Diskussion um die Möglichkeiten und Grenzen der Beteiligung der haftungsprivilegierten Diensteanbieter[9] brachte die Ministerin eine freiwillige, vertragliche Verpflichtung der Zugangsprovider in die Diskussion ein.[10] Einen federführend vom Familienministerium ausgearbeiteten Vertrag haben die fünf größten Zugangsanbieter in Deutschland und das BKA am 17.04.2009 unterzeichnet.[11] Die bekannt gewordene Entwurfsfassung des Vertrages sah dabei vor, dass die Zugangsanbieter innerhalb von 6 Stunden nach Erhalt der vom BKA täglich aktualisierten Sperrlisten den Zugriff auf die aufgeführten vollqualifizierten Domainnamen sperren könnten. Eine Vertragsstrafe oder vergleichbare Konsequenzen einer Missachtung der Pflicht waren nicht vorgesehen. Allein für Verletzungen der Pflichten des BKA ist im bekannt gewordenen Entwurf eine Haftungsregelung vorgesehen.[12]

1.3 Ansätze im Ausland

Wie oben bereits angedeutet, werden Diskussionen um die Sperrung von Internetinhalten im Ausland seit längerem geführt. Entsprechende Verpflichtungen wurden in Europa in unterschiedlichem Unfang beispielsweise in Norwegen[13], Schweden[14], der Schweiz[15], Großbritannien[16], der Türkei

6 Vgl. dazu *Krempl*, BKA fordert Sperrung kinderpornographischer Webseiten, Heise-Online, Nachricht vom 27.8.2008; *Gercke*, ZUM 2009, 525f.

7 *Frey*, MMR 2009, 221.

8 *Gaugele/Röttger*, Kinderpornos: Ministerin will Internetseiten sperren, Hamburger Abendblatt, 20.11.2008.

9 Zu den bestehenden Pflichten der Diensteanbieter im Kampf gegen Kinderpornographie vgl. Gercke, CRi 2009, 65ff.

10 Die Entwurfsfassung des Vertrages ist abrufbar unter: http://www.ccc.de/press/releases/2009/20090213/20090211-vertragsentwurf-bka-isp.pdf.

11 Vgl. *Höhne*, Das Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten, jurisPR-ITR 13/2009 sowie die Kleine Anfrage der FDP Fraktion, BT-Drs. 16/13245.

12 § 4 des Vertragsentwurfs.

13 „Telenor Norge: Telenor and KRIPOS introduce Internet child pornography Filter." Telenor Press Release, 21.09. 2004; *Clayton*, Failures in a Hybrid Content Blocking System in: Privacy Enhancing Technologies, 2006, S. 79; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, S. 46ff.; The Cybercrime Convention Committee (T-CY), Examples of how the private sector has blocked child pornograpyh sites, T-CY (2006) 04, S. 3.

14 *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, S. 59ff.; *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Resarch Service, Nov. 2008, S. 6.

15 *Sieber/Nolde*, Sperrverfügungen im Internet, 2008, S. 55; *Schwarzenegger*, Sperrverfügungen gegen Access-Provider in: Arter/Joerg, Internet-Recht und Electronic Commerce Law, S. 250.

16 *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Resarch Service, Nov. 2008, Seite 4; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, S. 64ff.

und Italien[17] eingeführt. Außerhalb Europas ist bekannt, dass Länder wie China[18], Iran[19] und Thailand[20], aber auch einige arabische Länder den Zugang zu bestimmten Internetseiten sperren.

Die technischen Konzepte, die Art und Weise der Verpflichtung (Selbstverpflichtung oder Gesetz) sowie die Reichweite der Maßnahmen unterscheidet sich dabei deutlich. In Australien wurde beispielsweise zunächst ein freiwilliger Sperransatz verfolgt und erst kürzlich der Fokus auf verpflichtende Maßnahmen gelegt.[21] Hintergrund ist der Umstand, dass in der Testphase der freiwilligen Sperrung Australiens größter Zugangsprovider hat mitteilen lassen, dass er sich an der Sperrung nicht beteiligen wird.[22] In Großbritannien erfolgt die Sperrung freiwillig. Trotz der Freiwilligkeit beteiligt sich, nicht zuletzt aufgrund des politischen Drucks, die überwiegende Zahl der Provider an der Sperrung. Die Liste der zu sperrenden Internetseiten wird dabei von der Internet Watch Foundation zusammengestellt.[23]

Auf EU-Ebene wird derzeit der Entwurf einer Richtlinie zur Bekämpfung von Kinderpornographie diskutiert.[24] Die Verfasser des Entwurfs haben hervorgehoben, dass die Computer- und Informationstechnologie die Herstellung und Verbreitung von Kinderpornographie unterstützt.[25] Neben der Ausweitung der Kriminalisierung zur Schließung von Strafbarkeitslücken im Bereich des download-unabhängigen Konsums enthält der Entwurf der Richtlinie einen Ansatz zur technischen Verhinderung des Zugriffs auf Internetseiten mit kinderpornographischen Inhalten. Ob dieser Bestandteil der Richtlinie nach der Neuausrichtung der Politik in einigen europäischen Ländern sowie der Resolution des Europaparlaments vom 15.06.2010[26] konsensfähig ist, ist derzeit noch offen.[27]

---

17 *Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007, S. 89ff; *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Resarch Service, Nov. 2008, S. 6ff; *Sieber/Nolde*, Sperrverfügungen im Internet, 2008, S. 54.

18 *Clayton/Murdoch/Watson*, Ignoring the Great Firewall of China, available at: http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf; *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfügungen gegen Access-Provider, Technisches Gutachten, abrufbar unter: http://www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf; *Sieber/Nolde*, Sperrverfügungen im Internet, 2008, S. 53; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, S. 73;

19 *Sieber/Nolde*, Sperrverfügungen im Internet, 2008, S. 53; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, S. 73.

20 *Sieber/Nolde*, Sperrverfügungen im Internet, 2008, S. 55.

21 Vg.. Zu den Filteransätzen: Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety, ACMA, 2008.

22 http://www.itu.int/osg/blog/2008/12/12/NetFirmsRebuffFilteringPlan.aspx.

23 *Stol/Kaspersen/Kerstens/Leukfeldt/Lobber*, Governmental filtering of websites: The Dutch case, Computer Law & Security Review 2009, S. 251.

24 Vorschlag einer Richtlinie des Europäischen Parlaments und des Rates zur Bekämpfung des sexuellen Mißbrauchs un der sexuellen Ausbeutung von Kindern sowie der Kinderpornographie und zur Aufhebung des Rahmbenbeschlusses 2004/68/JHA des Rates, COM (2010) 94; Vgl. dazu *Gercke*, ZUM 2010, 633ff.

25 Vorschlag einer Richtlinie des Europäischen Parlaments und des Rates zur Bekämpfung des sexuellen Mißbrauchs un der sexuellen Ausbeutung von Kindern sowie der Kinderpornographie und zur Aufhebung des Rahmbenbeschlusses 2004/68/JHA des Rates, COM (2010) 94, S. 2.

26 European Parliament Resolution of 15 June 2010 on Internet Governance: The Next Steps, 2009/2229(INI): „ 3. Calls on governments to desist from imposing restrictions on internet access by way of censorship, blocking, filtering or otherwise, and from requiring private entities to do so; insists on safeguarding an open internet, where users are able to access and distribute information or run applications and services of their choice as provided for by the reformed electronic communications regulatory framework".

27 Weiterführend: *Gercke*, ZUM 2010, 633ff.

1.4 Zugangserschwerungsgesetz

Nach der oben dargestellten Diskussion in Deutschland[28] und dem Abschluss der Verträge mit 5 großen Zugangsanbietern haben gleichwohl sowohl die Bundesregierung[29] wie auch die Fraktionen von CDU/CSU und SPD[30] Entwürfe zur Begründung einer gesetzlichen Verpflichtung der Zugangsprovider vorgelegt.

Die legislative Initiative wurde damit begründet, dass der „Großteil der Kinderpornographie im Bereich des World-Wide-Web [...] mittlerweile über kommerzielle Webseiten verbreitet“ werde, die in Drittländern außerhalb der Europäischen Union betrieben werden und es vielen Staaten nicht gelinge, Betreiber kinderpornographischer Angebote haftbar zu machen.[31] Dabei wurde im Rahmen des Gesetzgebungsverfahrens der Eindruck vermittelt, eine Haftbarmachung scheitere an fehlenden Strafgesetzen in den Ländern. Die ohne Belege erfolgten Ausführungen verwundern insoweit, als die Bundesregierung auf eine Kleine Anfrage der FDP Fraktion im Jahr 2009 mitteilte, dass ihr überhaupt keine gesicherte Kenntnis über Länder vorlägen, in denen die Verbreitung von Kinderpornographie nicht unter Strafe steht.[32] Auch die Frage nach der Zahl der Server mit Kinderpornographie in Ländern, in denen die Verbreitung nicht strafbar ist, blieb unbeantwortet.[33]

Am 18.06.2009 hat der Bundestag gleichwohl das Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen (ZugErschwG) beschlossen.[34] Das Gesetz basiert auf den Beschlussempfehlungen des Ausschusses für Wirtschaft und Technologie.[35] Grundlage des Gesetzes ist eine Verpflichtung der Zugangsprovider zur Erschwerung des Zugriffs auf solche Internetangebote, die vom Bundeskriminalamt in eine Sperrliste aufgenommen wurden.[36] Dabei ist zu berücksichtigen, dass mit § 7 Abs.2 S. 2 TMG bereits eine rechtliche Grundlage für Sperrverfügungen existiert. Während die Gesetzesentwürfe der Bundesregierung[37] sowie der Fraktionen von CDU/CSU und SPD[38] vor diesem Hintergrund ursprünglich eine Ergänzung des Telemediengesetzes um einen § 8a TMG vorsahen, wurde schließlich die Auslagerung in ein gesondertes Gesetz vorgezogen. Gemäß § 1 des Gesetzes führt das Bundeskriminalamt eine Liste mit voll qualifizierten Domainnamen, Internetprotokoll-Adressen und Zieladressen von Telemedienangeboten mit Kinderpornographie, die täglich aktualisiert wird. Dabei ist festgelegt, dass vorrangig eine Entfernung der Inhalte angestrebt wird.[39] Gemäß § 2 ZugErschwG sind Zugangsprovider i.S.d. § 8 TMG, die eine Inanspruchnahme ihrer Dienste für mindestens 10.000 Teilnehmer ermöglichen, verpflichtet, die in § 2 Abs.2 ZugErschwG konkretisierten aber nicht näher spezifizierten Maßnahmen zur Erschwerung des Zugriffs auf die Adressen der Sperrliste zu ergreifen und den Nutzern, die auf entsprechende Inhalte zugreifen möchte, auf eine Stoppmeldung umzuleiten (§ 4 ZugErschwG).

---

28 Vgl. zu Diskussion *Gercke*, ZUM 2009, 527f.
29 BT-Drs. 16/13125; BT-Drs. 16/ 13385.
30 BT-Drs. 16/12850.
31 BT-Drs. 16/12850, S.5.
32 BT-Drs. 16/13347, S. 3
33 BT-Drs. 16/13347, S. 4.
34 *BGBl*. I, 2010, S. 78, Vgl. zum Abstimmungsergebnis: http://www.bundestag.de/parlament/plenargeschehen/abstimmung/20090618_kinderpornografie.pdf.
35 BT-Drs. 16/13411.
36 *Frey/ Rudolph*, CR 2009, 644ff.; *Schnabel*, JZ 2009, 996 ff.; *Gercke*, ZUM 2010, 633ff.
37 BT-Drs. 16/13125; BT-Drs. 16/ 13385.
38 BT-Drs. 16/12850.
39 Vgl. § 1 Abs.2, S.1 ZugErschwG.

Der Bundespräsident hat das Gesetz zunächst nicht unterzeichnet und um ergänzende Stellungnahme der Bundesregierung gebeten.[40] Überraschend hat er dann am 17.02.2010 das Gesetz unterzeichnet und dabei zum Ausdruck gebracht, dass er davon ausgeht, dass nunmehr „auf der Grundlage des Zugangserschwerungsgesetzes Kinderpornographie im Internet effektiv und nachhaltig bekämpft" werde.[41] Das Gesetz wurde am 22.02.2010 im Bundesgesetzblatt verkündet[42] und ist am 23.02.2010 in Kraft getreten.[43] Obwohl nunmehr die gesetzlichen Grundlagen für die Verpflichtung der Zugangsprovider zur Sperrung von Internetseiten geschaffen war, hat sich die Bundesregierung nach der durch die Bundestagswahl erfolgte Regierungsumbildung[44] entschieden, vorerst keine Sperrungen vornehmen zu lassen. Mit Schreiben vom 17.02.2010 hat das Innenministerium das für die Sperrung zuständige Bundeskriminalamt angewiesen, von der Möglichkeit der Sperrung von Internetseiten vorerst nicht Gebrauch zu machen. Trotz des Inkrafttretens des Gesetzes erfolgt in Deutschland mithin keine Sperrung von kinderpornographischen Inhalten.

2 Hintergrund: Herausforderungen bei der Bekämpfung der Internetkriminalität

Die Bewertung der Diskussion um die Zugangssperren fällt leichter, wenn man diese vor dem Hintergrund der Herausforderungen der Strafverfolgungsbehörden bei der Bekämpfung der Internetkriminalität betrachtet. Aus dem Katalog von Herausforderungen, zu denen unter anderem auch der vermehrte Einsatz von Verschlüsselungstechnologie und die Möglichkeiten anonymer Kommunikation zählen, sind für die Diskussion insbesondere die fehlenden Kontrollinstrumente, die weltweite Verfügbarkeit von Inhalten und die transnationalen Bezüge vieler Internetdelikte von Bedeutung.

2.1 Fehlende Kontrollinstrumente

Die dem Internet zugrundeliegenden Netzwerkprotokolle wurden für militärische Einrichtungen entwickelt.[45] Dieser Umstand ist für die Strafverfolgungsbehörden insofern von Bedeutung als da die außerhalb des Internets bestehenden Eingriffs- und Kontrollmöglichkeiten der Strafverfolgungsbehörden in dieser Form im Internet nicht bestehen.[46] Anstelle dieser standen bei der Konzeption des militärisch genutzten Netzwerkes Aspekte wie die Resistenz gegen Angriffe von außen und die Sicherung der Kommunikation selbst im Falle eines Ausfalls einzelner Infrastrukturelemente im Vordergrund.[47] Im Rahmen des Übergangs von einer militärischen zu einer militärisch/wissenschaftlichen Nutzung und der letztendlichen Öffnung des Netzwerks für die Allgemeinheit wurde trotz der geänderten Anforderungen an das Netzwerk die grundlegende Struktur bei-

40 Vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Wunderlich, Sitte, Alpers und weitere Abgeordnete der Fraktion DIE LINKE, BT-Drs. 17/313, S. 2.
41 Vgl. Pressemitteilung des Bundespräsidialamtes vom 17.02.2010.
42 BGBl. 2010 I 78.
43 Vgl. zum Gesetz *Schnabel*, JZ 2009, 996ff.; *Frey/Rudolph*, CR 2009, 644ff.; *Gercke* in Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rn. 61b.
44 Vgl. zu den Bezügen zum Koalitionsvertrags die Kleine Anfrage der Abgeordneten Wunderlich, Sitte, Alpers und weitere Abgeordnete der Fraktion DIE LINKE, BT-Drs. 17/313, S. 2.
45 *Hoeren*, NJW 1995, 3295; *Steinhaus/Rosdale/de Pol*, Basiswissen Internet, 1999, S. 24.
46 Vgl. zu den rechtlichen Konsequenzen des dezentralen Aufbaus auch *Dietz/Richter*, CR 1998, 528.
47 *Ramamohanarao/Gupta/Peng/Leckie*, The Curse of Ease of Access to the Internet, in Information Systems Security, 2007, S. 234ff.

behalten.[48] Erfahrungen mit der Praxis der Strafverfolgung im Internet zeigen, dass diese mit der Netzwerkarchitektur einhergehenden Eigenschaften des Netzwerkes für die Arbeit der Strafverfolgungsbehörden eher hinderlich sind.[49]

In Ermangelung einer effektiven Selbstregulierung bemühen sich zahlreiche Länder, die rechtlichen Voraussetzungen zu schaffen, um das Geschehen im Internet ähnlichen Prinzipien zu unterwerfen, wie sie für Handlungen außerhalb des Netzwerkes existieren.[50] Dies betrifft nicht zuletzt das Internetstrafrecht.[51] Gerade im Hinblick auf das Strafrecht erweist sich die mit der Netzwerkarchitektur einhergehende Einschränkung der Ermittlungsmöglichkeiten der Strafverfolgungsbehörden aber als besonders problematisch, da ohne ein Eingreifen der Strafverfolgungsbehörden das Strafrecht seine Lenkungswirkung nicht entfalten kann.[52] Als besonders problematisch erweist sich insofern zunächst die Resistenz gegen Eingriffe von außen, die nicht die Möglichkeiten von Ermittlungen der Strafverfolgungsbehörden einschränkt. So fehlen beispielsweise der Straßenleitführung vergleichbare Kontrollinstrumente, die es den Ermittlungsbehörden ermöglichen, bestimmte Kommunikationswege zu blockieren[53], da die Flexibilität des zugrunde liegenden Protokolls zur Folge hat, dass die Sperrung einzelner Kommunikationswege häufig nicht zur Sperrung der Inhalte oder den Ausschluss einzelner Nutzer führt, da die Informationen auf anderen Wegen erreicht werden können. Ein weiteres Problem ist die globale Dimension des Internets und die im Vergleich dazu durch das völkerrechtliche Souveränitätsprinzip erheblich eingeschränkten Handlungsmöglichkeiten nationaler Strafverfolgungsorgane im Hinblick auf Delikte, die im Ausland begangen wurden.[54] Selbst in den Fällen, in denen das deutsche Strafrecht auf einen Fall mit Auslandsbezug anwendbar ist,[55] sind einer Ausübung hoheitlicher Befugnisse außerhalb des Staatsgebietes rechtlich enge Grenzen gesetzt.

2.2 Probleme bei der Verfolgung transnationaler Kriminalität

Grenzüberschreitende Ermittlungen setzen eine enge Zusammenarbeit der Strafverfolgungsbehörden in den betroffenen Staaten voraus[56], da die Möglichkeiten der nationalen Strafverfolgungsbehörden Ermittlungen außerhalb des eigenen Staatsgebietes durchzuführen aufgrund des völkerrechtlichen Souveränitätsprinzips begrenzt sind.[57] Die Rahmenbedingungen für eine Zusammenarbeit werden zumeist durch Rechtshilfeabkommen geregelt, die für die Zusammenarbeit ein im Vergleich zur Geschwindigkeit von Datentransferprozessen zeitaufwendiges, formelles Verfahren vorsehen.[58] Was die Verfolgung von Internetdelikten angeht, erweist sich insbesondere die Dauer der

48 Vgl. zu den rechtlichen Konsequenzen des dezentralen Aufbaus auch *Dietz/Richter*, CR 1998, 528.
49 Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rn. 29; *Gercke*, MMR 2008, 295f.
50 Eine Übersicht über den Stand der Gesetzgebung im Bereich des Internetstrafrechts in ausgewählten Ländern ist auf der Internetseite des Europarates abrufbar. Vgl. www.ceo.int.
51 Zum Schutz der Gesellschaft mit den Mitteln des Strafrechts vgl. *Gercke*, CR 2004, 784f.
52 Vgl. *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.
53 Zu den Kontrollmöglichkeiten vgl. *Knupfer* in Schriftenreihe der Strafverteidigervereinigung, Bd. 27, 139ff.
54 Vgl. dazu *Streinz*, in: Sachs, Grundgesetz,Art. 25 Rn. 52.
55 Vgl. zur extensiven Auslegung der Normen des internationalen Strafrechts im Zusammenhang mit Internetdelikten BGHST 46, 212ff.
56 Zur Notwendigkeit der internationalen Kooperation vgl. : *Putnam/Elliott*, International Responses to Cyber Crime, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, S. 35ff.; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, S.1ff; *Gercke*, CR 2004, 785.
57 Vgl. zum völkerrechtlichen Souveränitätsprinzip *Streinz*, in: Sachs, Grundgesetz, Art. 25 Rn. 52.
58 Vgl. *Gercke* CRi 2006, 141.

Bearbeitung von Rechtshilfeersuchen als problematisch. Viele der für die Rückverfolgung erforderlichen Daten werden, sofern in den betroffenen Ländern keine gesetzliche Verpflichtung zur Speicherung besteht, oft schon nach kurzer Zeit gelöscht, so dass für die Ermittlungen nur kurze Zeitfenster zur Verfügung stehen.[59] Im Regelfall setzt die grenzüberschreitende Zusammenarbeit weiterhin eine doppelte Strafbarkeit voraus[60], die aufgrund der bislang nur begrenzten Harmonisierung im Internetstrafrecht nicht in jedem Fall gegeben ist.[61]

2.3 Unabhängigkeit des Speicherorts

Eine weitere Konsequenz der Netzwerkarchitektur ist die Unabhängigkeit von Tat- und Handlungsort. Bedingt durch die zugrundeliegende Netzwerkarchitektur ist grundsätzlich ein weltweiter Zugriff auf im Internet bereitgehaltene Inhalte möglich. Dies hat für den Täter den Vorteil, dass die Begehung einer Internetstraftat weder voraussetzt, dass er an dem Ort, an dem der Erfolg seiner Tat eintritt, anwesend ist, noch dass Daten, die sich an Nutzer in einem Land richten, auf Servern in diesem Land gespeichert werden müssen. Mithin sind für Internetnutzer in Deutschland ohne entsprechende Sperrungen jegliche Daten verfügbar, die ohne Zugriffsbeschränkungen bereitgehalten werden. Ob diese im Inland oder im Ausland gespeichert werden, ist insoweit unerheblich. Dies ist für die Strafverfolgung insoweit relevant als dass die dem Schutzzweck des § 184b StGB zugeordnete Verhinderung einer Initialwirkung, die Konsumenten zum sexuellen Missbrauch von Kindern bewegen könnte, durch die Verfügbarkeit und nicht den Speicherort gefährdet wird.[62] Da in Deutschland aber nicht nur das Anbieten, sondern auch der Besitz von Kinderpornographie strafbar ist, stehen den Strafverfolgungsbehörden zumindest in Ansätzen andere Möglichkeiten als Zugangssperren zur Verfügung, um gegen den mit dem Download zusammenfallenden Konsum von Kinderpornographie vorzugehen.

3 Kritische Aspekte des Ansatzes

Während die Argumente der Befürworter von Sperrungen, die insbesondere auf den Schutz der Opfer sexuellen Missbrauchs vor der fortbestehenden Verfügbarkeit der Bilder im Internet sowie der Verhinderung eines Auslöseeffekts bei ungewollter Konfrontation verweisen, im Gesetzgebungsverfahren weitreichende Beachtung gefunden haben, konzentriert sich die folgende Darstellung auf kritische Aspekte der Bestrebungen zur Sperrung von Internetinhalten.

59 Durch die Einführung der Vorratsdatenspeicherungspflicht wird sich im Hinblick auf Internetprovider, die der Pflicht zur Vorratsdatenspeicherung unterliegen, bezüglich der von der Vorratsdatenspeicherung umfassten Daten, die zur Verfügung stehende Zeit erhöhen.

60 Vgl. zum Einfluss auf strafrechtliche Ermittlungen im Bereich der Internetkriminalität: “United Nations Manual on the Prevention and Control of Computer-Related Crime”, 269, abrufbar unter: http://www.uncjin.org/Documents/EighthCongress.html ; *Schjolberg/Hubbard*, “Harmonizing National Legal Approaches on Cybercrime”, 2005, Seite 5, abrufbar unter: www.itu.int/osg/spu/cybersecurity/ presentations/session12_schjolberg.pdf .

61 Zur begrenzten Reichweite der bisherigen Harmonisierungsansätze vgl. Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime, 12th UN Congress on Crime Prevention and Criminal Justice, A/CONF.213/9.

62 *Hörnle* in MüKo-StGB, § 184b, Rn. 1.

3.1 Keine Beseitigung der Inhalte

Ein zentraler Kritikpunkt ist der Umstand, dass die Internetsperren nicht zur Beseitigung der illegalen Inhalte, sondern nur zu deren Nichtverfügbarkeit führen und mithin die Rechtsverletzung (das Zugänglichmachen) nicht beenden.[63] Dies ist insoweit zutreffend, als die Inhalte nur für die Nutzer unerreichbar werden, die durch die Sperrung an einem Zugriff gehindert werden. Ein Zugriff über Internetanbieter, die keiner Sperrpflicht unterliegen, sowie ein Zugriff unter Umgehung von Zugangssperren ist weiterhin möglich. Zwar bekräftigt das in § 1 Abs.2 ZugErschwG niedergelegte Subsidiaritätsprinzip den Vorrang der Löschung – gleichwohl bleibt die Verfügbarkeit der Daten ein Kernproblem des Ansatzes. Konsequent begründet das Innenministerium insoweit die Anweisung an das BKA, das Gesetz nicht anzuwenden, damit, dass sich die Bundesregierung „intensiv für die Löschung derartiger Seiten" einsetze.

3.2 Netzneutralität

Während auch unter Kritikern des Gesetzes Einigkeit herrscht, dass Anbieter kinderpornographischer Inhalte keines Schutzes bedürften, wird die Bedeutung der Diskussion erst dadurch erkennbar, wenn man den Umstand einbezieht, dass die Implementierung der für die Sperrung der Internetseiten erforderlichen Technologie sich nicht nur zur Sperrung von Internetseiten mit kinderpornographischen Inhalten, sondern auch anderen Inhalten nutzen ließe. Dies hat zu Befürchtungen einer grundlegenden Abkehr von der Netzneutralität geführt.[64] Vor dem Hintergrund dieser grundlegenden Bedenken hat der Europarat im März 2008 Empfehlungen über Maßnahmen zur Stärkung des Rechts auf freie Meinungsäußerung und Informationsfreiheit im Hinblick auf den Einsatz von Filtertechnologie im Internet angenommen.[65] Darin empfiehlt der Europarat zum Schutz des durch Art. 10 der Menschenrechtskonvention gewährten Rechts der freien Meinungsäußerung einen restriktiven Einsatz staatlich kontrollierter Internetfilter.[66]

3.3 Umgehungsmöglichkeit

Die technischen Möglichkeiten der Provider zur Sperrung von Zugriffen unter Verwendung der derzeit diskutierten DNS-Sperren sind beschränkt.[67] Insbesondere aufgrund der zahlreichen Umgehungsmöglichkeiten stoßen die Verpflichtungen auf Bedenken.[68] So lassen sich DNS-Sperrungen relativ einfach durch den Einsatz von Anonymisierungsdiensten umgehen. Sofern ein Nutzer über einen Anonymisierungsdienst, der die Kommunikation mit dem Nutzer verschlüsselt und keine Sperrungen vornimmt, eine Internetseite aufruft, wird die Netzsperrung umgangen.[69]

---

63 *Süme*, im Rahmen des Öffentlichen Expertengesprächs des Unterausschusses Neue Medien vom 12.2.2009, S. 12 ff.

64 Vgl. zur möglichen Ausweitung auch: *Frey* im Rahmen des Öffentlichen Expertengesprächs des Unterausschusses Neue Medien vom 12.2.2009, S. 8.

65 Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters- adopted by the Committee of Ministers on 26 March 2008 at the 1022nd meeting of the Ministers' Deputies.

66 Vgl. dazu *Gercke*, Update Strafrecht in Taeger/Wiebe, Von AdWords bis Social Networks, 2008, S. 437f.

67 Vgl. dazu die Stellungnahme von *Federrath* im Rahmen des Öffentlichen Expertengesprächs des Unterausschusses Neue Medien vom 12.2.2009 sowie *Schöttle*, KR 2007, 366 ff.

68 Vgl. dazu dazu grundlegend: *Sieber/Nolde*, Sperrverfügungen im Internet, 2008; *Gercke*, Legal issues of Liability and Obligations of Internet Service Providers with regard to Child Pornography, Gutachten im Auftrag des Europarates, 2009, S. 17, abrufbar unter www.coe.int.

69 *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfügungen gegen Access-Provider, Technisches Gutachten, abrufbar unter:

3.4 Risiko der Veröffentlichung der Listen

Zugangssperrungen, wie sie in Deutschland diskutiert und implementiert wurden, basieren auf dem Prinzip von Sperrlisten. Diesbezüglich gibt es zwei Ansatzpunkte zur Kritik. Zunächst einmal ist eine Evaluation der Listeneinträge erforderlich, um sicherzustellen, dass der Zugang zu legitimen Seiten nicht beeinträchtigt ist. Darüber hinaus wird immer wieder darauf verwiesen, dass Listen mit ernst zunehmenden Sicherheitsrisiken einhergehen.[70] Die Veröffentlichung der australischen Sperrliste mit hunderten von Internetadressen kinderpornographischer Inhalte[71], die nunmehr von Tätern zum Auffinden der Inhalte genutzt werden können, verdeutlicht das Risiko. Selbst wenn die Sperrlisten nicht an die Öffentlichkeit gelangen, besteht mitunter die Möglichkeit, durch „reverse engineering" an die Einträge zu gelangen.[72]

4 Fazit

Vor dem Hintergrund der intensiven Diskussion um technische Ansätze zur Bekämpfung der Internetkriminalität im Ausland war es nur eine Frage der Zeit, bis dieser Ansatz von der deutschen Politik aufgegriffen wird. Dabei hätten die Erfahrungen mit Sperrverfügungen im Hinblick auf rassistische und pornographische Inhalte vor 2008 sowie der Umstand, dass die Bedenken gegen Sperransätze im Ausland bereits bekannt waren und sich selbst der Europarat bereits des Themas angenommen hatte, dazu beitragen können, dass politische Schnellschüsse bei einem so wichtigen Thema wie der Bekämpfung der Kinderpornographie unterbleiben. Der Umstand, dass zunächst auf eine Selbstverpflichtung der Industrie gesetzt wird, dann trotz des Abschlusses entsprechender Verträge zusätzlich ein Gesetz auf den Weg gebracht wird, das kurz nach Inkrafttreten faktisch suspendiert wird, verdeutlicht, dass die Chance nicht genutzt wurde.

Verf.: Dr. Marco Gercke, Direktor des Cybercrime Research Institute und Lehrbeauftragter für Medienstrafrecht an der Universität zu Köln, Niehlerstr. 35, 50733 Köln; E-Mail: marco@gercke.de; info@cybercrime.de

http://www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf; Vgl. zu den Möglichkeiten der Umgehung chinesischer Zensurbestrebungen: 26. Tätigkeitsbericht 2004 des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, Kap. 15 – abrufbar unter: https://www.datenschutzzentrum.de/material/tb/tb26/kap15.htm.

70 *Callanan/Gercke/De Marco/Dries-Ziekenheiner*, Internet Blocking – Balancing Cybercrime Response in Democratic Societies, 2009, S. 11.

71 Vgl. dazu *Moses*, Leaked Australian blacklist reveals banned sites, Sydney Morning Herald, 19.03.2009; *Suzor/Pappalardo/Graham*, Submission to the Department of Broadband, Communications and the Digital Economy ‚Mandatory internet service provider (ISP) filtering: Measures to increase accountability and transparency for Refused Classification material' consultation, 2010.

72 *Callanan/Gercke/De Marco/Dries-Ziekenheiner*, Internet Blocking – Balancing Cybercrime Response in Democratic Societies, 2009, S. 11.