Max-Planck-Institut
für ausländisches und
internationales Strafrecht

Sperrverfügungen im Internet

Kurzinformation zum Forschungsprojekt am Max-Planck-Institut für ausländisches und internationales Strafrecht

Das Internet ermöglicht einen weltweiten Zugriff auf eine Vielzahl von rechtmäßig angebotenen Daten. Es wird aber auch für die Begehung von Straftaten genutzt, wie die Verbreitung von gewaltverherrlichenden oder kinderpornographischen Inhalten sowie Urheberrechtsverletzungen, illegales Glücksspiel oder die Werbung für terroristische Ziele.

Eine Verhinderung und Verfolgung dieser Delikte bereitet häufig Schwierigkeiten, da die Kompetenzen der nationalen Sicherheitsbehörden an den Staatsgrenzen enden. Auch wenn der Anwendungsbereich des materiellen Strafrechts auf ausländische Server ausgedehnt wird, ist die internationale Rechtsdurchsetzung wegen der fehlenden Gebietshoheit in der Praxis schwierig. [1] Die Nationalstaaten können deswegen in vielen Fällen nicht wirksam gegen illegale Inhalte auf ausländischen Servern vorgehen. Das gilt vor allem dann, wenn diese Inhalte im Ausland nicht strafbar sind, wie es etwa in den USA bei nationalsozialistischer Propaganda oder vielen gewaltverherrlichenden Äußerungen der Fall ist. [2]

Zahlreiche Staaten versuchen daher, ihr nationales Territorium gegen illegale Inhalte im Internet abzuschotten: Wenn nicht direkt gegen die auf ausländischen Servern gespeicherten Inhalte vorgegangen werden kann, so sollen wenigstens technische Sperrmaßnahmen einen Zugriff der Bürger unterbinden. Bekannt sind die Maßnahmen der Volksrepublik China oder des Iran, welche die Informations- und Meinungsfreiheit stark beschränken. Seit einigen Jahren implementieren jedoch auch westliche Demokratien wie Großbritannien zunehmend technische Sperren gegen illegale Inhalte im Internet. Auch in Deutschland bestehen bereits gesetzliche Grundlagen für die Anordnung derartiger Zugangssperren durch die Medienaufsicht. Diese „Sperrverfügungen“ waren in Deutschland bisher allerdings in der praktischen Umsetzung wenig erfolgreich und wurden in der (Fach-)Öffentlichkeit wegen ihrer technischen Probleme und ihrer Eingriffe in die Informations- und Meinungsfreiheit überwiegend kritisch beurteilt.

Aufgrund der bestehenden technischen und rechtlichen Unsicherheiten beauftragte die in Deutschland für Sperrverfügungen zuständige Kommission für Jugendmedienschutz (KJM) das Freiburger Max-Planck-Institut für ausländisches und internationales Strafrecht sowie die Technische Universität Dresden mit entsprechenden Studien. Ziel war zum einen die Untersuchung

Anschrift:
Günterstalstraße 73
79100 Freiburg i. Br.

Telefon / Fax:
Tel: +49 (0)761 7081-1
Fax: +49 (0)761 7081-294

Online:
info@mpicc.de
www.mpicc.de

Direktoren:
Prof. Dr. Dr. h.c. Ulrich Sieber
Prof. Dr. Dr. h.c. Hans-Jörg Albrecht

der technischen Möglichkeiten, zum anderen die Prüfung der rechtlichen Zulässigkeit von Sperrmaßnahmen im Internet. Besonders die vom Max-Planck-Institut durchgeführte juristische Analyse führte zu unerwarteten Ergebnissen.

Technische Möglichkeiten der territorialen Zugriffsbeschränkung im globalen Internet

In der Diskussion über die Grundstrukturen von internationalen Computernetzen dominiert heute noch immer das Paradigma des national kaum regulierbaren „globalen Cyberspace“. Gerade frühe Visionäre des Informationsrechts stellen inzwischen jedoch die Frage nach einer „Territorialisierung“ des Internets, um den Nationalstaaten auch online einen Restbestand ihrer Souveränität zu erhalten und die Durchsetzung von Normen und Werten nicht allein dem Markt zu überlassen.

Entsprechende Möglichkeiten zeigen sich gerade im Bereich der Sperrmaßnahmen gegen bestimmte Inhalte: Seitdem diese vor einigen Jahren in Deutschland erstmals gerichtlich überprüft wurden, hat sich die Technik von Internetsperren erheblich weiterentwickelt. Die Umsetzungsmöglichkeiten hängen in erster Linie vom Diensteangebot der Provider ab, die zur Einrichtung von Zugriffssperren herangezogen werden. Denkbare Akteure für Sperrmaßnahmen sind Access-Provider, die den Einwahlknoten zum Internet bereitstellen, und Network-Provider, die die Infrastruktur betreiben. [3]

Entscheidend für die Durchführung von Sperrmaßnahmen sind dabei die Daten, die den jeweiligen Anbietern bei ihrer Geschäftserbringung vorliegen. Stark vereinfacht lässt sich feststellen, dass drei Ansätze zur Verfügung stehen: „Grobe“ Sperrtechniken (wie solche anhand der IP-Adresse) sind einfach durchzuführen, aber nicht trennscharf, da sie oft zahlreiche legale Inhalte miterfassen, die nur zufällig am gleichen Ort gespeichert sind. „Feinere“ Sperrtechniken (insbesondere auf der Basis von URL-Adressen) sind zwar von größerer Treffsicherheit, setzen jedoch einen hohen technischen und organisatorischen Aufwand voraus und können von zahlreichen Providern nicht im Rahmen der üblichen Geschäftsabwicklung implementiert werden. Die in den letzten Jahren neu entwickelten hybriden Sperrtechnologien kombinieren die Vorteile beider Verfahren, indem sie zunächst eine grobe Filterung auf „verdächtige“ (IP-)Adressen vornehmen und dann nur diese vorselektierte Kommunikation noch weiter im Hinblick auf URL-Adressen analysieren. Das erfordert allerdings eine Infrastruktur zur Überwachung des Internetverkehrs, die mit beträchtlichen Eingriffen in das Fernmeldegeheimnis und Missbrauchsrisiken verbunden ist.

Zudem können (mehr oder weniger) fachkundige Nutzer sämtliche geschilderten Sperren umgehen. Insoweit spielen die jeweils nutzbare Netzinfrastruktur (mit verschiedenen Zugangsvermittlern im Inland, einer möglichen Einwahl über ausländische Access-Provider oder dem Zugriff auf Anonymisierungsdienste) sowie das jeweilige Regierungssystem (Demokratie oder totalitärer Staat) eine wichtige Rolle. Gleichwohl sind Sperrmaßnahmen auch in marktwirtschaftlich geprägten und freiheitlichen Demokratien nicht völlig nutzlos oder auf eine symbolische Politik reduziert. Trotz der bestehenden alternativen Zugangsmöglichkeiten werden insbesondere Kinder und Jugendliche jedenfalls vor einem zufälligen Kontakt mit schädlichen Inhalten geschützt und Nutzer ohne Kenntnisse der Umgehungsmöglichkeiten vom gewünschten Zugriff auf illegale Inhalte abgehalten.

Rechtliche Grenzen für Zugriffssperren

Problematischer als das dargestellte Umgehungsrisiko sind die durch Zugriffssperren verursachten Eingriffe in Grundrechte. Zu berücksichtigen sind insbesondere die Berufsfreiheit und der Eigentumsschutz der Zugangsdiensteanbieter, die Meinungsfreiheit der Content-Provider sowie die Informationsfreiheit der Nutzer. [4] [5] Diese – in Rechtsprechung und Literatur auch bisher schon diskutierten Eingriffe – wurden in der Untersuchung des Max-Planck-Instituts detailliert analysiert.

Ein neuer verfassungsrechtlicher Schwerpunkt der Untersuchung ergab sich aus der Erkenntnis, dass die Umsetzung von Sperrverfügungen in vielen Fällen durch die Analyse der angeforderten IP-Adressen und URLs auch in das *Fernmeldegeheimnis* eingreift. Das beruht darauf, dass dieses Grundrecht nicht nur den Inhalt, sondern auch die näheren Umstände der Kommunikation schützt. Darunter fallen nach den Ergebnissen der Studie auch die Adressen und Port-Nummern, die bei den meisten Sperrtechnologien flächendeckend ausgewertet werden müssen, um den Zugriff auf bestimmte Angebote zu verhindern.

Die Eingriffsintensität von Sperrmaßnahmen bei der Analyse von dem Fernmeldegeheimnis unterliegenden Daten war weder der Öffentlichkeit noch dem Gesetzgeber ausreichend bewusst. Die Legislative hat deswegen in ihrer komplizierten und höchst unübersichtlichen Regelung der Sperranordnungen nicht normiert, ob und inwieweit bei der Umsetzung in das Fernmeldegeheimnis eingegriffen werden darf. Dabei hat sie nicht nur gegen die Zitiergebote von Art. 19 Abs. 1 Satz 2 Grundgesetz und § 88 Abs. 3 Satz 3 Telekommunikationsgesetz verstoßen, weil sie in der Ermächtigungsgrundlage an keiner Stelle die Möglichkeit einer Einschränkung des Fernmeldegeheimnisses erwähnt. In der Normenkette des Jugendmedienschutz-Staatsvertrages, des Staatsvertrages über Rundfunk und Telemedien und des Telemediengesetzes wurde – im Gegenteil – vielmehr festgelegt, dass auch bei Sperrverpflichtungen das Fernmeldegeheimnis „zu wahren“ ist.

Die geltende Rechtslage erlaubt somit gegenwärtig keine Sperrmaßnahmen, die in das von Art. 10 Grundgesetz und § 88 Telekommunikationsgesetz geschützte Fernmeldegeheimnis eingreifen. Damit scheiden derzeit alle Ansätze – einschließlich der hybriden Sperrtechniken – aus, die auf der Analyse von IP-Adressen, Port-Nummern, URLs oder Inhaltsdaten beruhen. Zulässig bleiben nur die – nicht in das Fernmeldegeheimnis eingreifenden – Manipulationen von Domain-Namen an den entsprechenden Servern sowie die Unterdrückung von Einträgen in der Trefferliste von Suchmaschinen.

Diese Beschränkung der zulässigen Sperrtechniken beruht nicht nur auf einer formalen Gesetzesanwendung. Sie ist auch in der Sache berechtigt. Insbesondere die neuen hybriden Technologien ermöglichen nicht nur die Sperrung von ausländischen Internetadressen, sondern könnten mittels einer zentralen Kontrollarchitektur potenziell sogar eine effektive und flächendeckende *inhaltliche* Überwachung der Internetkommunikation erleichtern. Der Einsatz solcher, unter Umständen sehr eingriffsintensiven Kontrolltechniken setzt voraus, dass sich der parlamentarisch legitimierte Gesetzgeber über die damit verbundenen Einschnitte in die Freiheitsrechte seiner Bürger umfänglich im Klaren ist und ihre Verhältnismäßigkeit gründlich abwägt.

Weitere Fragen und Zukunftsperspektiven

Die Untersuchung des Freiburger Max-Planck-Instituts für ausländisches und internationales Strafrecht geht über die hier dargestellte Problematik hinaus, beleuchtet zahlreiche weitere Fragestellungen des geltenden Rechts und gibt eine Gesamteinschätzung der gegenwärtigen Rechtslage. Dabei erweisen sich die bestehenden Regelungen auch in anderen Punkten als unausgereift. Dies gilt sowohl im Hinblick auf die Effektivität als auch auf den Schutz der von Sperrverfügungen tangierten Grundrechte. Zu kritisieren sind die Zuständigkeiten unterschiedlicher Behörden für Sperrverfügungen, die zukünftig zu Durchsetzungsproblemen führenden Verweisungsketten und weitere Systembrüche.

Der mangelhafte Schutz der von Sperrmaßnahmen massiv tangierten Grundrechte zeigt sich nicht nur an der fehlenden Regelung zu Eingriffen in das Fernmeldegeheimnis, sondern auch an den unzureichenden Überlegungen und Normen zu Transparenz, Kontrolle und spezifischen Rechtsschutzmöglichkeiten sowie an der nicht vorhandenen Kostenregelung. Bei der Durchführung von nationalen Sperrmaßnahmen im Internet geht es um derart zentrale Fragestellungen für die Freiheitsrechte der Bürger und die Integrität des gesamten Internets, dass der Aufbau eines einigermaßen effektiven Systems auch insoweit nicht ohne intensive Überlegungen und Leitentscheidungen des Gesetzgebers erfolgen darf.

Will die Legislative eine – in ihren Erfolgsaussichten gleichwohl fragliche – wirkungsvollere, präzisere, transparente und kontrollierte nationale Abschottung gegen illegale Inhalte im Internet ermöglichen, so sind gesetzliche Neuregelungen notwendig, die sich keinesfalls nur auf die Gestattung von Eingriffen in den Fernmeldeverkehr beschränken dürfen. Dies erfordert eine Grundsatzdiskussion über technische Konzepte zur „Territorialisierung des Internets“ in freiheitlichen Gesellschaften, über die jeweiligen rechtlichen Möglichkeiten und ihre Begrenzung durch Freiheitsrechte sowie vor allem auch über alternative Schutzstrategien. Diese Grundsatzdiskussion muss vor entsprechenden Reformschritten geführt werden. [6]

Literaturhinweise

[1] Cybercrime and Jurisdiction in Germany.
U. Sieber:
In: B.-J. Koops, S. Brenner, Susan (Hrsg.), Cybercrime and Jurisdiction – A Global Survey, Den Haag 2006, 183–210.

[2] Die Bekämpfung von Haß im Internet – Technische, rechtliche und strategische Grundlagen für ein Präventionskonzept.
U. Sieber:
Zeitschrift für Rechtspolitik 34, 97–103 (2001).

[3] Verantwortlichkeit im Internet – Technische Kontrollmöglichkeiten und multimediarechtliche Regelungen.
U. Sieber:
C.H. Beck Verlag München, 1999.

[4] Internet-Service-Provider als Geiseln deutscher Ordnungsbehörden.
C. Engel:
MultiMedia und Recht (Beilage 4) 6, 1–36 (2003).

[5] Haftung für Informationen im Internet.
Th. Stadler:
2. Aufl., Verlag E. Schmidt, Berlin 2005.

[6] Sperrverfügungen im Internet.
U. Sieber, M. Nolde:
Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht – Strafrechtliche Forschungsberichte. Erscheint im Juni 2008

Projektinformationen

Forschungsprojekt am Max-Planck-Institut für ausländisches und internationales Strafecht (Referat Informationsrecht & Rechtsinformatik).

Bearbeiter:	Prof. Dr. Dr. h.c. Ulrich Sieber Malaika Nolde, LL.M. (Rechtsinformatik)
Projektlaufzeit:	2005-2007
Publikation:	Juni 2008
Projektstatus:	Abgeschlossen
Projektförderung:	Kommission für Jugendmedienschutz der Landesmedienanstalten (KJM)
Nähere Informationen:	http://www.mpicc.de/ww/de/pub/forschung/forschungsarbeit/strafrecht/sperrverfuegungen.htm