

Forschungsbericht

**Internet-Zugangssperrung**

**Überblick zur Internet-Kriminalität in demokratischen Gesellschaften  
(Executive Summary)**

Erstellt von

Cormac Callanan (Irland)  
Marco Gercke (Deutschland)  
Estelle De Marco (Frankreich)  
Hein Dries-Ziekenheiner (Niederlande)

Die Erstellung des Berichts wurde durch die Förderung des Open Society Instituts unterstützt.

Kontakt

Weitere Informationen erhalten Sie von:

**Hr. Cormac Callanan**

Tel.: +353 87 257 7791

Email: [cormac.callanan@aconite.ie](mailto:cormac.callanan@aconite.ie)

**Hr. Marco Gercke**

Tel.: +49 221 2707205

Email: [gercke@cybercrime.de](mailto:gercke@cybercrime.de)

**Fr. Estelle De Marco**

Tel.: +33 4 90 84 16 70

Email: [estelle.de.marco@inthemis.fr](mailto:estelle.de.marco@inthemis.fr)

**Hr. Hein Dries-Ziekenheiner**

Tel.: +31 71 711 3243

Email: [hein@vigilo.nl](mailto:hein@vigilo.nl)

Die in diesem Bericht geäußerten Meinungen spiegeln nicht unbedingt die des Open Society Instituts wider.

## Die Autoren

### CORMAC CALLANAN

### IRLAND

Cormac Callanan ist Direktor von Aconite Internet Solutions ([www.aconite.com](http://www.aconite.com)) und hat Expertise im Bereich der Richtlinienentwicklung für Internet-Kriminalität und Schutz & Sicherheit im Internet.

Er studierte Informatik (MSc) und besitzt über 25 Jahre Berufserfahrung im Bereich internationale Computernetzwerke und 10 Jahre Erfahrung auf dem Gebiet der Internet-Kriminalität. Für das Interpol, Europol und Strafverfolgungsbehörden hat er weltweit Fortbildungsmaßnahmen durchgeführt. Zurzeit bietet er weltweit Beratungsdienste an und arbeitet im Bereich der Richtlinienentwicklung für den Europarat und das UNODC.

Zusammen mit Mitautor Marco Gercke legte er in 2008 ein Forschungsbericht zu den Best-Practice-Richtlinien für die Zusammenarbeit von Dienstleistungsanbietern und Gesetzeshütern gegen Internet-Kriminalität ([www.coe.int/cybercrime](http://www.coe.int/cybercrime)) vor, der entsprechend in 2008 auf der Octopus Konferenz verabschiedet wurde. Zusammen mit Nigel Jones erstellte er die 2Zentrumsstudie (Internet-Kriminalitätszentren für Exzellenznetzwerke zur Ausbildung, Forschung und Fortbildung), die die internationale Best-Practice-Computer-Forensikausbildung für Gesetzeshüter diskutiert.

Cormac war Präsident und CEO von INHOPE – die Internationale Gesellschaft von Internet Hotlines ([www.inhope.org](http://www.inhope.org)). INHOPE unterstützt und koordiniert die Arbeit von Internet-Hotlines, die Fragen hinsichtlich des illegalen Gebrauchs und illegaler Inhalte beantworten. Als Mitautor veröffentlichte er in 2007 den ersten Globalen Internet-Trendbericht von INHOPE, der eine bahnbrechende Publikation zur Kinderpornografie darstellte.

Cormac war 1997 gründender Vorsitzender der Internet Service Provider Association von Irland ([www.ispai.ie](http://www.ispai.ie)), die er für 5 Jahre bis Februar 2003 geleitet hatte und diente als Generalsekretär für die European Service Provider Association ([www.euroispa.org](http://www.euroispa.org)). Er war zudem in 1998 gründender Direktor des irischen Dienstes [www.hotline.ie](http://www.hotline.ie) und antwortete auf Berichte über illegale Kinderpornografie und Hassreden im Internet. Er schrieb den Verhaltenskodex (Code of Conduct) für das ISPAI.

1991 gründete Cormac in Irland das erste kommerzielle Internet-Dienstleistungsgeschäft - EUnet Ireland – das 1996 verkauft wurde. Er ist Vorstandsmitglied der Copyright Association of Ireland ([www.cai.ie](http://www.cai.ie)). Er war in der Rightswatch ([www.rightswatch.com](http://www.rightswatch.com)) UK

& Ireland Working Group tätig und entwickelte Best-Practice-Richtlinien für Notice- und Takedown-Maßnahmen in Verbindung mit dem geistigen Eigentumsrecht (IPR: Intellectual Property Rights).

**MARCO GERCKE****DEUTSCHLAND**

Dr. Marco Gercke ist Direktor des Instituts für Medienstrafrecht - ein unabhängiges Forschungsinstitut zu den legalen Aspekten der Computer- und Internet-Kriminalität.

Er promovierte im Bereich Strafrecht (Dr. jur.), lehrt seit mehreren Jahren die Gesetzgebung zur Internet-Kriminalität und zum europäischen Strafrecht an der Universität zu Köln und ist Gastdozent für internationales Strafrecht an der Universität Macau.

Sein Forschungsschwerpunkt bezieht sich auf Gesetzesaspekte der Internet-Kriminalität. In dieser Rolle arbeitet er als Experte für verschiedene internationale Organisationen (z. B. Europarat, Europäische Union, Vereinte Nationen und Internationalen Fernmeldeunion). Ein Schlüsselement dieser Forschung bezieht sich auf den Kampf gegen die Internet-Kriminalität und den diesbezüglichen verfassungsrechtlichen Abweichungen, die zwischen dem allgemeinen Gesetz und dem zivilen Strafrecht auftreten. Das jüngste Projekt beinhaltet die Aktivitäten von Terroristorganisationen im Internet, legale Maßnahmen gegen Identitätsdiebstahl, Geldwäsche und terroristische Finanzaktivitäten, die die Internet-Technologie und die Verantwortung der ISPs miteinbezieht.

Marco hält oft Vorträge, national und international, und er ist Autor von mehr als 60 Publikationen, die sich mit der Internet-Kriminalität beschäftigen. Neben Zeitschriftartikeln und Büchern veröffentlichte er verschiedene Forschungsberichte, u.a. auch eine vergleichende Analyse von Gesetzen für den Europarat. Die Verantwortung der ISPs beim Kampf gegen die Internet-Kriminalität war das Thema einer Studie für den Europarat, die im März 2009 veröffentlicht wurde. Seine jüngste 255 Seiten lange Publikation zur Internet-Kriminalität wird zurzeit in alle Sprachen der UN übersetzt.

Marco war gemeinsamer Vorsitzender einer Arbeitsgruppe des Europarats, um die Richtlinien für die Zusammenarbeit zwischen Gesetzeshütern und Internet-Service-Provider gegen Internet-Kriminalität zu erstellen, die in 2008 auf der Octopus Konferenz verabschiedet wurden; ebenso war er Mitglied der ITU High Level Expert Group.

Er ist Mitglied der deutschen Anwaltsvereinigung und Geschäftsführer der Strafrechtsabteilung der deutschen Gesellschaft für Recht und Informatik.

Eine vollständige Liste der Veröffentlichungen und Vorträge finden Sie unter: [www.cybercrime.de](http://www.cybercrime.de).

**ESTELLE DE MARCO****FRANKREICH**

Dr. Estelle De Marco ist ein Berater für legale und regulatorische IT-Fragen und ist Geschäftsführer des Forschungszentrums für Informationsschutz and Internet-Kriminalität (CRESIC, Montpellier).

Sie promovierte im Bereich Privatrecht und Strafwissenschaften (Dr. jur.) und ist insbesondere auf den Gebieten des Zivil- und Strafrechts, des IT-Rechts und der Menschenrechte ausgewiesen; sie kann auf mehr als 10 Jahre Erfahrung im Bereich des IT-Rechts zurückblicken und hat 7 Jahre Erfahrung hinsichtlich der Gesetzgebung und Richtlinien von illegalen Inhalten (einschließlich der Haftung von Internet-Darstellern, IPR und Datenschutz). Sie ist Mitglied der Europol Arbeitsgruppe zur Harmonisierung der Ausbildung von Internet-Kriminalitätsuntersuchungen.

Estelle war für 6 Jahre rechtliche und regulatorische Beraterin bei der französischen Internet Service Providers Association (AFA). Sie ist sehr mit den technischen Gegebenheiten der Informationstechnologie vertraut. Sie arbeitete als Manager der AFA-Hotline gegen illegale Inhalte mit der Internet-Kriminalitätsabteilung der französischen Polizei zusammen und nahm an INHOPE-Projekten teil. Sie repräsentierte die französische Internet-Sektor auf vielen internationalen Foren.

Sie war Mitglied der Arbeitsgruppe des Europarats, die die Richtlinien zur Zusammenarbeit von Gesetzeshütern und Internet-Service-Providers gegen Internet-Kriminalität, die in 2008 auf der Octopus Conference verabschiedet wurden, erstellte. Sie verfasste verschiedene Gesetzesstudien über Kinderfürsorge, Internet-Kriminalität, IPR und technologische Gefahren, um die Stellung des Sektors gegenüber dem Kulturminister, dem Wirtschaftsminister und gegenüber der Europäischen Kommission zu behaupten. In Zusammenarbeit mit AFA-Mitgliedern verfasste sie die Internet-Politik hinsichtlich des Kampfes gegen Spam and die ersten Einzelheiten zum Signal-Spam-Mechanismus, der es dem ISP ermöglicht, Informationen über mögliche Netzwerk-Spam-Attacken zu erhalten ([www.signal-spam.fr](http://www.signal-spam.fr)). Sie nahm an der Schaffung des Signal-Spams teil und war Mitglied des Vorstands. Estelle arbeitete auch für 4 Jahre am Amtsgericht von Montpellier.

Estelle ist Mitglied von Cyberlex ([www.cyberlex.org](http://www.cyberlex.org)), ein französische Gesellschaft für Fachleute im rechtlich-technischen Bereich, und des wissenschaftlichen Rats von Juriscom.net ([www.juriscom.net](http://www.juriscom.net)), eine Online-Zeitschrift, die auf dem Gebiet der IT-Gesetzgebung spezialisiert ist und die regelmäßig Beiträge von Rechtsanwälten, u.a. auch von

Wissenschaftlern, veröffentlicht. Seit 10 Jahren aktualisiert sie die von ihr für technische Experten geschaffene Website des 'Comité Réseaux des Universités' (Netzwerkkomitee der Universitäten) über 'Gesetz und Ethik' des Internets.

## **HEIN DRIES-ZIEKENHEINER DIE NIEDERLANDE**

Hein Dries-Ziekenheiner LL.M ist CEO von VIGILO Consult, eine holländische Beraterfirma, die im Bereich Internet-Vollzug, Internet-Kriminalität, IT-Gesetz und verwandte Themen arbeitet. Hein studierte holländisches Zivilrecht (Master) an der Leiden Universität, und er besitzt mehr als fünf Jahre technische Erfahrung auf den Gebieten der forensischen IT und der Internet-Strafverfolgung.

Auf Grund seiner Rolle als juristischer und regulatorischer Berater und Repräsentant der holländischen ISP Gesellschaft (NLIP) ist Hein sehr kompetent und besitzt mehr als zehn Jahre Erfahrung im Bereich Internet-Netzwerk, Internet-Politik und verwandte Themen, die mit der Strafverfolgung im Zusammenhang stehen.

Hein wurde in den Vorstand der European Internet Service Providers Association (EuroISPA) berufen. In dieser Rolle verfasste er gemeinsam Beiträge über Maßnahmen und Politik hinsichtlich verschiedener Themenbereiche, u.a. auch das 2002-Reformpaket, das ISP-Haftungssystem und auf den Datenschutz bezogene Fragestellungen. Er repräsentierte den niederländischen ISP-Sektor auf vielen (inter)nationalen Foren.

Als Mitglied eines Teams für Internet-Sicherheits der sehr erfolgreichen OPTA (Onafhankelijke Post en Telecommunicatie Autoriteit), eine holländische Regulationsbehörde für die Telekommunikation, war Hein für das erste Email-Spam-Bußgeld gemäß der Rahmenbedingungen der EU von 2002 verantwortlich, und er arbeitete ebenso am bekannten DollarRevenue Spyware-Fall. Er leitete verschiedene andere Anti-Spam und Anti-Malware-Fälle, die OPTA, Hollands unabhängige Post- und Telekommunikationsbehörde, entdeckte.

Hein bietet regelmäßig Weiterbildungsmaßnahmen für Verantwortliche im Bereich Anti-Spam und Anti-Malware-Kriminaltechnik an; er hat ebenso weltweit mit vielen Gesetzeshütern bezüglich verschiedener Spam-Fälle zusammengearbeitet (z. B. US FTC und FBI, australische ACMA und EU CPC Netzwerk der Agenturen für Verbraucherschutz). Hein ist ein Mitglied der holländischen Gesellschaft für Gesetz und IT, und seine Firma, VIGILO Consult, ist Mitglied der Industriebeobachter beim Londoner Aktionsplan gegen Spam (LAP: London action plan on spam).

Hein veröffentlicht Beiträge auf regelmäßiger Basis und hält Vorträge über Themen, die die Internet-Strafverfolgung und die Internet-Kriminalität behandeln.

## **Inhalt**

<b>Executive Summary</b> .....	<b>7</b>
1.1 Einführung .....	7
1.2 Was ist Internet-Sperrung? .....	7
1.3 Internet-Sperrung: Diskussion und Motivation .....	11
1.4 Technische Aspekte der Internet-Sperrung .....	15
1.5 Internet-Sperrungen und das Gesetz .....	22
1.6 Abwägen der fundamentalen Freiheiten .....	29
1.7 Schlussfolgerung .....	36

## EXECUTIVE SUMMARY

---

### 1.1 Einführung

Der vorliegende Bericht erklärt, was Internet-Sperrung bedeutet, was die Motivationen sind, Internet-Sperrungen einzuführen, die die Gesellschaft betreffen, welche technischen Möglichkeiten zur Verfügung stehen und was die gesetzlichen Voraussetzungen sind, von denen die Internet-Sperrstrategien betroffen werden.

Anmerkung: Zitate, die im vorliegenden Executive Summary erwähnt werden, sind nicht unmittelbar den Autoren zuzuordnen. Diese Zitate werden deutlich zwischen Anführungszeichen hervorgehoben und können in den Originalbeiträgen mit detailliertem Literaturhinweis (Autor und Quelle) aufgesucht werden. Falls diese Zitate dem vorliegenden Beitrag entnommen werden, dürfen sie nicht wiedergegeben werden, ohne dass der ursprüngliche Autor des Zitats SOWIE die relevante Seite des betreffenden Kapitels des Beitrags, wo der ursprüngliche Autor des Zitats erwähnt wird, angeführt wird.

### 1.2 Was ist Internet-Sperrung?

Diese Studie liefert eine umfassende Analyse über den aktuellen Stand der Internet-Sperrung, einen Überblick zu den gegenwärtigen regulatorischen und gesetzlichen Rahmenbedingungen hinsichtlich der Internet-Sperrung, einen Kommentar über die Wirksamkeit der Internet-Sperrung und deren Einfluss auf den Kampf gegen Internet-Kriminalität und auf die Unterstützung von Demokratie und der persönlichen Sicherheit.

Eine Ausgewogenheit zwischen Kinderschutz und demokratischer Freiheit zu finden, ist eine sehr komplexe Fragestellung, die nur auf höchster nationaler Ebene durch intensive Diskussionen zwischen den relevanten Interessengruppen eines jeden Landes in Bezug auf entsprechende verbindliche internationale Instrumente wie die Europäische Menschenrechtskonvention gelöst werden kann.

Ein ungehinderter Internet-Zugriff ohne Eingriffe ist gemäß der Mitglieder des Europäischen Parlaments ein Recht von sehr weitreichender Bedeutung. Das Internet, das durch das Recht der Meinungsfreiheit geschützt ist, obwohl es gegenwärtig nicht selber als ein fundamentales Recht angesehen wird, ist eine „unüberschaubare Plattform, die es ermöglicht, sich auf kulturelle Art und Weise auszudrücken, Zugriff auf Wissen zu erhalten, demokratisch am europäischen Erfindungsgeist mitzuwirken und Generationen auf Grund der Informationsgesellschaft zusammenzuführen.“<sup>1</sup>

In den letzten Jahren haben einige demokratische Staaten Internet-Sperrmethoden in Bezug auf verschiedene Kategorien von Inhalten unterstützt. Sie beziehen sich hierbei darauf, dass es im Interesse der Öffentlichkeit ist, bestimmte Sperrungen vorzunehmen, um verschiedene Aspekte der öffentlichen Ordnung aufrechtzuerhalten und zwar in Fällen, bei denen das

---

<sup>1</sup> Beschluss des Europäischen Parlaments vom 10. April 2008 über kulturelle Industriezweige in Europa, 2007/2153(INI), § 23; unter dieser Adresse abrufbar: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0123+0+DOC+XML+V0//EN>. Siehe Abschnitt 6.3.2.2.

Internet (internationale) Strafverfolgungsmaßnahmen hervorrufen. Die Themenbereiche variieren von Nazi-Memorabilia, verfügbar über den Online-Markt, bis zu Glücksspiel-Websites, die in Ländern ausgerichtet werden, die eine liberale Auffassung gegenüber dem Online-Glücksspiel vertreten. Andere Länder mit weniger freizügigen Auflagen benutzen 'Sperrung' als eine technische Quelle, um innerhalb der Online-Welt ihre Praxis der Informationskontrolle auszubauen.

### **Was ist Internet-Sperrung?**

Internet-Sperrung (manchmal auch Internet-Filterung genannt) ist keine neue Aktivität. Sie besteht schon seit mehreren Jahren. Dieser Begriff umfasst ein großes Spektrum an Verordnungen, Hardware, Software und Dienstleistungen, und es wäre falsch anzunehmen, dass alle Arten der Internet-Sperrung gleich, vergleichbar effektiv und rechtlich gleich sind, oder dass ein System problemlos für mehrere Inhaltskategorien verwendet werden kann.

Die Hauptanliegen der Internet-Sperrung besteht darin, dass durch ein Software- oder Hardware-Produkt, das alle Internet-Kommunikationen überprüft und über den Empfang und/oder Wiedergabe von bestimmten Inhalten entscheidet, die Inhaltsübertragung auf den persönlichen Computer bzw. auf den Computer-Bildschirm verhindert wird.

Zum Beispiel kann eine Email gesperrt werden, weil angenommen wird, dass sie Spam enthält, eine Website kann gesperrt werden, weil sie möglicherweise Malware aufweist oder eine Peer-to-Peer Austausch könnte unterbrochen werden, weil vermutet wird, dass kinderpornografische Inhalte ausgetauscht werden.

Der Begriff „Internet-Sperrung“ ist selber irgendwie eine Fehlbezeichnung, weil dieser vermuten lässt, dass eine Internet-Sperrung leicht implementiert werden kann, und dass man die Wahl hat diese Sperrung an- und auszuschalten. Nichts wäre unzutreffender, denn das Potential der Internet-Sperrtechniken ist ziemlich komplex und kann oftmals ohne großen Aufwand umgangen werden. Hierfür gibt es verschiedene Gründe, aber einer der Hauptgründe ist, dass das Internet dezentralisiert konzipiert wurde, d.h. es besitzt eine inhärente Kapazität, die es den Daten ermöglichen, jegliche Schranken zu 'umgehen', die im Wege stehen.<sup>2</sup>

Der Versuch Internet-Inhalte zu sperren, die in anderen Ländern legal sind, aber die im eigenen Land als illegal kategorisiert werden, wird manchmal als ein Versuch der Länder angesehen, ihre eigenen nationalen kulturellen Standards in Zeiten des globalen Zugriffs aufrechtzuerhalten.

Man kann sagen, dass die Internet-Sperrung vor 2 Dekaden begann, indem unerwünschte Emails (Spams) gesperrt wurden. Dies geschah aus unterschiedlichen Gründen, aber ursprünglich wollte man eine Überlastung der Netzwerk-Ressourcen vermeiden. Dies war stets ein Forschungs- und Entwicklungsbereich und es bestand ein kontinuierlicher Wettbewerb zwischen Anti-Spam-Initiativen und Spam-Aktivitäten. Trotz weitreichender Initiativen über einen längeren Zeitraum hinweg blieb der hundertprozentige Erfolg der Spam-Sperrung, wie jeder Email-Benutzer weiß, aus, denn Spam wurde noch nicht vollkommen aus dem Internet verdrängt.

Es ist wichtig anzumerken, dass alle Internet-Sperrsysteme falsche-negative<sup>3</sup> und falsche-positive<sup>4</sup> Probleme haben und in modernen Systemen werden diese durch das Design der verwendeten Sperrmethoden minimalisiert.

---

<sup>2</sup> Die komplexe Bandbreite technologischer Fragestellungen wird in Kapitel 5 zusammengefasst.

<sup>3</sup> Ein falsch-negatives Ergebnis liegt vor, wenn ein Element vom Spam-Filter erlaubt wird, weil es überprüft und als negativ klassifiziert wurde, aber in Wirklichkeit handelt es sich um Spam. Daher ist das Ergebnis falsch-negativ.

<sup>4</sup> Ein falsch-positives Ergebnis liegt vor, wenn ein Element, das nicht gesperrt werden sollte, vom Filter gesperrt wird, weil es ein positives Ergebnis produziert. Da das positive Ergebnis falsch ist, wird es als falsch-positiv bezeichnet.

Diese Probleme treten mehr in den Vordergrund und haben einen größeren Einfluss, wenn die Internet-Sperrsysteme im öffentlichen Internet verwendet werden und wenn alle Internet-Benutzer in allen Bereichen davon automatisch betroffen sind. Es sind aus diesem Grund wichtige Annahmen zu berücksichtigen, die sich auf die Gesellschaft insgesamt beziehen. Da diese Systeme oftmals ohne direkte Erlaubnis der Benutzer des Internet-Dienstes mit minimaler und nicht angemessener öffentlicher Aufsicht oder Diskussion implementiert werden, müssen diese deutlich transparenter und kontrollierbarer konzipiert, entwickelt, verwaltet, implementiert und überwacht werden.

Es gibt unterschiedliche Formen der Internet-Sperrung. Persönliches Filtern und Netzwerk-Sperrung sind die beiden häufigsten Methoden, die jedermann benutzt. Es gibt auch Systeme, die hybride Formen dieser beiden Ausrichtungen sind.

Die Sperrung durch den Endverbraucher erlaubt den Benutzer selber zu entscheiden, welche Inhalte gesperrt werden sollen und zwar hinsichtlich der Kriterien, die jeder einzelne Computer-Benutzer bestimmt und die maßgeschneidert bezüglich verschiedener Personengruppen (z. B. Eltern, Kind, Lehrer, Student usw.) eingestellt werden können. Diese Art der Sperrung ist am spezifischsten, aber dies hindert Benutzer nicht daran, Inhalte, die möglicherweise illegal sind, abzurufen, die sie trotzdem sehen und herunterladen möchten.

Auf Grund von netzwerk-basierender Internet-Sperrung kann der Service Provider (Internet Access Provider, Arbeitgeber, Verein usw.) entscheiden, welche Art von Inhalten oder Aktivitäten für ALLE Benutzer des Dienstes gesperrt wird - zumindest bezüglich der Inhalte, die direkt über zuführende-Netzwerksysteme des Providers abgerufen werden, bei denen die Sperrmethoden implementiert sind. (Manchmal kann das System individuell eingestellt werden, um die auf Benutzeridentifikation beruhenden Sperrungskriterien festzulegen.)

Es gibt zwei entscheidende Themen, die diskutiert werden müssen, wenn die Methode der Internet-Sperrung Anwendung findet:

- Wie bestimmen wir aus technischer Sicht, was gesperrt werden soll?  
Die Prozesse, die Inhalte sammeln, überprüfen, bewerten und kategorisieren, um festzustellen, welche Inhalte gesperrt werden sollen, sind komplex und ressourcenintensiv. Diese Prozesse müssen entwickelt, getestet und implementiert werden und Mitarbeiter müssen eingestellt und ausgebildet werden.
  - Sperrlisten ist die am häufigsten verwendeten Sperrstrategien.
  - Automatische Identifikationen werden entwickelt, aber sie sind nur begrenzt erfolgreich.
  - Bewertungssysteme werden seit Jahren benutzt, aber sind nicht erfolgreich.
- Wer soll bestimmen, was im Internet gesperrt werden soll?
  - In den Ländern, in denen die Justiz unabhängig von der Gesetzgebung und Regierung ist - dies sollte für alle liberalen Demokratien zutreffen – sollte nur der Richter die Autorität besitzen, bestimmte Inhaltselemente, Situationen oder Aktionen als illegal zu erklären.
  - Dieser Aspekt stellt eine der größten Herausforderungen für Internet-Sperrsysteme dar. Die gegenwärtigen nationalen und internationalen legalen Prozesse funktionieren nicht adäquat hinsichtlich der Herausforderungen, die das Internet und die Kommunikationsgeschwindigkeit der Internet-Dienste stellen. Daher gibt es seitens der Justiz selten hinlängliche Beteiligungen in Bezug auf Internet-Sperrentscheidungen.

Die Organisation 'International Network of Internet Hotlines' (INHOPE) koordiniert ein Hotline-Netzwerk in mehr als 30 Ländern und bearbeitet Berichte über Kinderpornografie im Internet. Die Hotlines erhielten im Jahr 2005 mehr als 500.000 Meldungen, im Jahr 2006 805.000 Meldungen und im Jahr 2007 1 Million Meldungen; diese Zahlen erhöhen sich jedes Jahr.

Genauere Zahlen für das Jahr 2008 wurden bislang nicht veröffentlicht. Bei den Meldungen, die zwischen September 2004 und Dezember 2006 eingegangen sind, wurden weniger als 20% als illegal ODER gefährlich eingestuft und nur 10% der gesamten Meldungen wurden seitens der Hotlines als illegal angesehen.

Ein kritischer Aspekt der Sperrlisten bezieht sich auf Schutz und Integrität. Eine solche Inhaltsliste wird bevorzugt hinsichtlich derjenigen Personen erstellt, die eine Disposition dafür haben, derartiges Material einzusehen. Ohne dass Sperrlisten direkt auf das Internet durchsickern, Untersuchungen verdeutlichen, dass es möglich sein sollte, die vom Service Provider verwendete Sperrliste zu dekompileieren.

Internet-Sperrungen von Kinderpornografie verhindert nicht Kindesmissbrauch. Die Bilder verschwinden nicht oder werden nicht aus dem Internet entfernt. Die effektivste Antwort auf Bilder, die Kinderpornografie / Kindesmisshandlungen zeigen, besteht darin, dass diese aus dem Internet entfernt werden und dass zur gleichen Zeit der Bildproduzent strafverfolgt wird, damit das Kind vor weiteren Missbrauch geschützt und zwecks Behandlung und Genesung in ein sicheres Umfeld gebracht wird.

Internet-Sperrungen verhindern, dass derartige Inhalte leicht abgerufen werden können (hängt vom übernommenen Sperrsystem ab), sodass nur Personen dies umgehen können, die entschlossener und technisch versierter sind (abhängig von der verwendeten Client-Software). Im Falle, dass die Bilder persönlich identifizierbare Informationen über das Opfer enthalten, kann die Sperrung der Bilder das Opfer vor weiteren Ausbeutungen schützen.<sup>5</sup>

Unglücklicherweise werden gegenwärtig einige illegale Website-Inhalte, die mit Kinderpornografie in Verbindung stehen, von Ländern und Internet-Hosting-Anbietern geliefert, bei denen die nationale Gesetzgebung und die politische Aufsicht und Intervention nicht mit dem gegenwärtigen internationalen Best-Practice-Standards vergleichbar ist und bei denen direkte Verfahren zur Meldung und Entfernung rechtswidriger Inhalte nur rudimentär bestehen bzw. nicht funktionieren. Die Initiativen, die diesen Gesichtspunkt ansprechen, müssen unterstützt werden.

Es ist wichtig hervorzuheben, dass die vielen Sperrstrategien von intrusiver Natur sind. Dies trifft insbesondere auf granulärere, inhalts-basierende Filtermethoden zu, die eine inhaltliche Einsicht des Materials, das zwischen den Benutzern ausgetauscht wird, erfordert. Dies ist nicht nur aus der Investitionsperspektive problematisch (die erforderliche Investition ist ausnahmslos hoch in diesen Szenarios), sondern auch aus globaler und gesellschaftlicher Sicht.

Die Verhältnismäßigkeit der Internet-Sperrmaßnahmen ist im Allgemeinen schwierig zu beurteilen, weil sie hauptsächlich vom spezifischen 'legitimen Ziel'<sup>6</sup> abhängig ist, das in jeder einzelnen Situation aufrechtzuerhalten ist, aber auch von der Nützlichkeit der Maßnahme, um das legitime Ziel in einer spezifischen Situation zu erreichen, und von den Sperreigenschaften und deren Einflüsse auf Rechte und Freiheiten.

Die Konsequenzen, die die Internet-Sperrung nach sich zieht, werden als Eingriffe in die fundamentale Freiheit angesehen und werden in Kapitel 6 und 7 hervorgehoben. Andere mögliche Eingriffe werden durch verschiedene Internet-Sperrmaßnahmen hervorgerufen und zwar auf Grund der Natur der Methode, die verwendet wird, um die Sperrung zu implementieren.

Die Verhältnismäßigkeit jeder Maßnahme, die im Gegensatz zu bestimmten Freiheiten steht, muss erstens hinsichtlich des legitimen Ziels und zweitens bezüglich allgemeiner Auswirkungen überprüft werden; dies sollte nur bis zu dem Punkt erfolgen, um das Erreichen des legitimen Ziels zu ermöglichen, und in jedem Fall sollten einige 'Spielräume' unter dem

---

<sup>5</sup> Dies wird in Kapitel 6 genauer diskutiert

<sup>6</sup> In Bezug auf Abschnitt 7.4

Gesichtspunkt der eingeschränkten Freiheit erhalten bleiben, sodass diese nicht 'ausgelöscht' wird.

Immer dann, wenn eine Sperrmaßnahme erlaubt wird, um das legitime Ziel zu erreichen, muss ihre Funktionsweise nicht unbedingt die Freiheit anderer unverhältnismäßig einschränken, und einige Garantien müssen implementiert werden, damit diese Sperrmaßnahme nicht derartig verwendet wird, dass die Freiheiten noch stärker gefährdet werden.

Es sollte auf jeden Fall hervorgehoben werden, dass es in dem gegenwärtigen Bericht keine Strategie gibt, die vollkommen eine zu starke Sperrung (Übersperrung) ausschließt. Dies ist der Hauptgesichtspunkt, wenn versucht wird, eine Ausgewogenheit zwischen der Sperrung von Kinderpornografie und der Notwendigkeit, Menschenrechte und Pressefreiheit zu garantieren, zu finden. Es scheint zwangsläufig der Fall zu sein, dass legaler Inhalt gesperrt wird, wenn Sperrungen implementiert werden.

Da Internet-Inhalte über verschiedene Internet-Technologien ausgetauscht werden können, dürfte die Handhabung, nur eine begrenzte Zahl von diesen Inhalten zu sperren (z. B., wenn nur der Datenfluss auf Web-Server gesperrt wird), problemlos die Benutzung einer alternativen Datenübertragungsmethode bewirken. Diejenigen, die davon besessen sind illegale Inhalte zu verbreiten, besitzen eine Myriade von Möglichkeiten, dies trotz Netzwerk-Sperrungen umzusetzen. Aus technischer Sicht können Sperrversuche nur dann den Benutzer schützen, wenn er aus Versehen diese Inhalte abrufen. Es scheint unwahrscheinlich zu sein, dass Sperrstrategien, wie sie in dem vorliegenden Dokument diskutiert werden, in der Lage sind, substantiell oder wirksam Kriminalität oder Wiederholungstat vorbeugen können.

Der Versuch, Inhalte zu sperren, kann als ein Unterfangen der Re-Territorialisierung verstanden werden, indem Länder sicher stellen möchten, dass nationale Standards auf globale Inhalte angewendet werden, die den Internet-Benutzern innerhalb des jeweiligen Landes zur Verfügung stehen.

Es gibt verschiedene Arten von Sperrversuchen, denn alle Inhalte sind verschieden und es gibt verschiedene Formen von Straftaten.

### **1.3 Internet-Sperrung: Diskussion und Motivation**

Die Diskussion zur Internet-Sperrung sollte sich nicht auf eine bestimmte Annahme konzentrieren. Die Diskussion ist ebenso komplex wie das Thema selber. Es gibt verschiedene kritische Bereiche, und für die politischen Entscheidungsträger sind die Herausforderungen, auf Probleme mit Internet-Inhalten zu reagieren, sehr komplex.

Es gibt vielfältige Motivationen, warum soziale Gesellschaften zurzeit daran glauben (oder in einigen Fällen hoffen), dass Internet-Sperrversuche einige größere soziale Probleme lösen würden, da andere Maßnahmen wenig erfolgsversprechend zu sein scheinen. Es gibt verschiedene Einrichtungen, die gegenwärtig Sperrungen implementiert haben. Diese Sperrversuche zielen auf ein bestimmtes, aber großes Materialspektrum ab. Internet-Sperrversuche können auf verschiedene Art und Weise umgesetzt werden, und dies hängt davon ab, auf wen diese Sperrversuche abzielen. Verschiedene Länder haben bereits bestimmte Internet-Sperrsysteme verabschiedet.

Das Internet ist ein riesengroßes komplexes Netzwerk mit einer Myriade von Hardware-Systemen, Protokollen und implementierten Diensten. Der erste Schritt einer Internet-Sperrinitiative besteht darin zu entscheiden, wo Internet-Sperrversuche durchgeführt werden können. Ein zweiter Gesichtspunkt bezieht darauf zu bestimmen, wer entscheidet was gesperrt werden sollte, und wer bestimmt, welche Benutzer und Organisationen welches Wissen haben, um entsprechende Internet-Inhalte zu sperren. Ein großes Inhaltsspektrum kann bei verschiedenen sozialen Gesellschaften Probleme erzeugen und jede Sperrmaßnahme

muss die Vielfalt der Inhalte beschreiben, auf die sie abzielt, aber auch wie einige Regierungen Internet-Sperrversuche als eine mögliche Lösung für einige dieser Probleme implementiert haben. Die primären Motivationen, die politische Entscheidungsträger dazu veranlasst haben, Internet-Sperrungen einzuführen, müssen angesprochen werden, aber auch wie in einigen Fällen alternative Ansätze offenbar fehlgeschlagen sind. Internet-Sperrmaßnahmen richten sich gewöhnlich gegen den Erzeuger oder den Konsumenten der illegalen Inhalte und sind je nach Ausrichtung unterschiedlich wirksam.

Die komplexe Bandbreite unterschiedlicher Ansätze und Motivationen hinsichtlich der Internet-Sperrversuche müssen differenziert werden, um diese verschiedenen Ansätze vergleichen zu können.

Das erste Kriterium, das verwendet wird, um zwischen verschiedenen Sperransätzen unterscheiden zu können, bezieht sich auf das Ziel der Sperrmethode. Im Allgemeinen gibt es vier verschiedene Zielsperrungen, auf die man sich konzentrieren kann:

- Dienst-basierender Ansatz: z. B. Email
- Inhalts-basierender Ansatz: z. B. Hassrede, Kinderpornografie, Glücksspiel-Websites
- Benutzer-basierender Ansatz: z. B. Benutzer, die illegale Musik herunterladen oder Spam versenden
- Suchmaschinen-basierender Ansatz, z. B. Sperren von Suchergebnissen für illegale Websites

Ein zweites Kriterium, das verwendet werden kann, um zwischen verschiedenen Internet-Sperransätzen zu unterscheiden, besteht darin, sich auf die Rolle des politischen Entscheidungsträgers in Bezug auf illegale Inhalte zu konzentrieren. Der politische Entscheidungsträger ist die Person oder Institution, die darüber entscheidet, **was** gesperrt werden sollte.

- Individuell motiviert
- Institutionell motiviert
- Gesetzgebung / Gericht

Die Internet-Sperrung wird als eine technische Lösung in Bezug auf ein großes Spektrum von illegaler Aktivitäten diskutiert. Zu einem großen Maße – jedoch nicht notgedrungen – werden diese Aktivitäten in einem Land kriminalisiert, das beabsichtigt, Sperrmethoden zu implementieren oder das bereits diese Methoden implementiert hat; jedoch erfolgt die Kriminalisierung nicht immer auf gleiche Weise in dem Land, wo der Inhalt verwaltet wird. Kinderpornografie stellt eine Inhaltskategorie dar, bei der der Inhalt auf Grund des Strafrechts zu sperren ist.

Die Durchführung des Gesetzes ist im Internet nur schwer umzusetzen, weil Material oftmals legal außerhalb des Landes erstellt wird. Dies stellt eine direkte Konsequenz von unterschiedlich implementierten nationalen Standards hinsichtlich der Veröffentlichung von Material dar. Der Versuch, Inhalte zu sperren, die außerhalb des Landes legal zur Verfügung stehen, aber innerhalb des Landes als illegal angesehen werden, stellt für bestimmte Länder eine Möglichkeit dar, den Versuch zu unternehmen, in Zeiten des globalen Zugriffs den eigenen national-kulturellen Standard aufrechtzuerhalten.

Andere Inhalte, auf die die Internet-Sperrversuche ausgerichtet sind, beziehen sich auf folgende Aspekte:

- Spam – Email-Dienste berichten, dass es sich gegenwärtig bei 85 bis 90 Prozent der Emails um Spam handelt. Die meisten Spam-Sperrungen erfolgen mit Zustimmung der Kunden.

- Erotisches und pornografisches Material – oftmals von politischen Entscheidungsträgern in dem Zusammenhang erwähnt, dass Minderjährige keinen Zugriff auf Inhalte haben sollten, die als gefährlich eingestuft werden. In einigen Ländern wurden 'Altersschutzsysteme' entwickelt, um zu verhindern, dass Minderjährige Zugriff auf nicht-jugendfrei Inhalte haben. Andere Länder kriminalisieren jeglichen Austausch von pornografischem Material, auch zwischen Erwachsenen.
- Kinderpornografie – wird universell verurteilt und Verstöße in Bezug auf Kinderpornografie werden im Allgemeinen als kriminelle Straftaten angesehen. Trotz eines beträchtlichen Aufwands und hoher Kosten, haben sich die Täter nicht von den Initiativen, die versuchten, die Internet-Versendung von Kinderpornografie zu kontrollieren, abschrecken lassen.
- Kontroverse politische Themen / Hassreden / Xenophobie – Einige Länder kriminalisieren die Veröffentlichung von Rassenhass, Gewalt und Xenophobie, während derartiges Material legal in anderen Ländern publiziert werden können, weil diese, wie z. B. die USA, den Schutz der Pressefreiheit garantieren.
- Illegales Glücksspiel – Das Internet ermöglicht, dass die Glücksspielbeschränkungen umgangen werden können. Online-Kasinos sind weitverbreitet und zwecks des Internet-Glücksspiels werden die meisten in Ländern mit liberalen Gesetzen oder ohne Auflagen angeboten.
- Verleumdungen und die Veröffentlichung von falschen Informationen – Websites können falsche oder verleumderische Informationen veröffentlichen, besonders in Foren und Chat-Rooms, in denen Benutzer Mitteilungen ohne Moderatorverifikation versenden können.
- Inhalte, die von terroristischen Organisationen veröffentlicht werden – Die Veröffentlichung von Propaganda und Informationen, die zu Straftaten anstiften, ist üblich.
- Verletzung von Copyrights – umfasst den Austausch von urheberrechtlich geschützten Liedern, Daten und Software-Produkten in File-Sharing Systemen sowie das Umgehen von Digital Rights Management Systemen. Peer-to-Peer (P2P) Technologie spielt eine vitale Rolle im Internet.

### **Warum sollten Internet-Sperrungen eingesetzt werden?**

- Fehlende Internet-Kontrollmethoden

Da das Internet ursprünglich auf der Grundlage einer dezentralisierten Netzwerk-Architektur entwickelt wurde, das gegen Fehler und Attacken robust ist, ist das Internet gegenüber externen Kontrollversuchen resistent. Die Sperrversuche könnte man als einen Versuch verstehen Kontrollfunktionen zu implementieren, aber dies wurde nicht vorhergesehen als das Netzwerk entwickelt wurde.

- Internationale Dimension

Eine internationale Kooperation, die auf den Prinzipien des traditionellen Rechtswegs beruht, ist oftmals sehr langsam und zeitaufwendig. Die formalen Anforderungen und der Zeitaufwand, der benötigt wird, um mit ausländischen Strafverfolgungseinrichtungen zusammen zu arbeiten, verhindert oftmals eine Untersuchung. Die Sperrversuche könnten aus diesem Grund als ein Ansatz verstanden werden, der dann zum Zuge kommt, wenn die Beschränkungen der gegenwärtigen internationalen Zusammenarbeit bestimmte Maßnahmen in einem angemessenen Zeitraum verhindern.

- Verminderte Bedeutung der nationalen Hosting-Infrastruktur

Die Veröffentlichung von Inhalten kann in einem Land vollkommen legal sein, kann jedoch in einem anderen Land als eine Straftat angesehen werden. Die Versuche, die Inhalte zu sperren, können daher als eine Art von Re-Territorialisierung bezeichnet werden, wobei die entsprechenden Länder beabsichtigen zu gewährleisten, dass die nationalen Standards in Bezug auf die globalen Internet-Inhalte, die innerhalb des Landes den Benutzern zur Verfügung stehen, angewendet werden.

### Wer sollte gesperrt werden?

Die Sperrung von illegalen Internet-Inhalten ist nicht nur eine Methode, die sich ausschließlich auf die Täter bezieht, die Inhalte online zur Verfügung stellen (Erzeuger), aber es ist auch eine Methode, um den Benutzer daran zu hindern, illegale Inhalte herunterzuladen (Konsument).

- Die Erzeuger von illegalen Inhalten – die illegalen Inhaltsanbieter.

Das Internet stellt heute die primäre Methode dar, um Kinderpornografie zu versenden; sie hat eine Reihe von Vorteilen für den Straftäter, die die Untersuchungen sehr erschweren. Entsprechend sind moderne Digitalkameras und digitale Camcorder die wichtigsten Geräte zur Erstellung von Kinderpornografie.

Der Grund, Sperrtechnologien zu implementieren, ist daher vergleichbar mit den Gründen Kinderpornografie zu kriminalisieren, z. B. um das Ausmaß der Straftat zu reduzieren und um die Kinder zu schützen.

- Der Konsument von illegalen Inhalten.

Zusätzlich zu der Produktion, Veröffentlichung und Bereitstellung von Kinderpornografie kriminalisiert eine nicht undeutende Anzahl von Ländern den Besitz von Kinderpornografie. Der Bedarf nach diesem Material könnte eine kontinuierliche Erstellung des Materials begünstigen. Auch gehen eine Reihe von Ländern noch einen Schritt weiter, indem sie nicht nur den Besitz von Kinderpornografie kriminalisieren, jedoch auch die Aktivität, **Zugriff** auf Kinderpornografie zu erhalten.

Die Tatsache, dass die Internet-Sperrung *nicht* Inhalte an der Quelle entfernt, verhindert, dass diese Methode in der Lage ist, die Tat der Bereitstellung von Inhalten zu verhüten; die Methode, falls sie technisch wirksam ist, besitzt das **Potential Taten einiger Benutzer, die versuchen, Zugriff auf eine Website zu bekommen, um Kinderpornografie anzusehen oder herunterzuladen, zu verhindern**. Der Erfolg hängt von der Wirksamkeit der eingesetzten Sperrtechnologie ab sowie von der Motivationsstärke und dem Wissen des Benutzers.

Das Hauptproblem der Sperrmethode besteht darin, dass die Inhalte nicht an der Quelle entfernt werden und dass es viele Möglichkeiten gibt, diese Technologie zu umgehen. Diese Gesichtspunkte besitzen verschiedene Implikationen:

- Die Inhalte können durch alternative Verbindungen abgerufen werden, die nicht den Zugriff sperren.
- Wenn eine Sperrmethode entwickelt und implementiert wird, kann diese Methode für andere Zwecke verwendet werden. Einer der Hauptgründe für dieser Problematik bezieht sich auf die nicht-transparente Implementierung einer solchen Technologie.
- Die Tatsache, dass die Inhalte noch nicht entfernt wurden, gestattet es den Benutzern den Zugriff zu versuchen, indem die technischen Schutzmaßnahmen umgangen werden.
- Es gibt unterschiedliche Methoden, wie diese gegenwärtig diskutierten Sperransätze umgangen werden können.

- Die Tatsache, dass Inhalte nicht entfernt wurden, lässt Benutzer vermuten, dass diese Websites hinsichtlich des Zugriffs sicherer sind, weil es den Verantwortlichen nicht gelungen ist, diese Sites zu entfernen oder zu untersuchen.
- Der Austausch von Kinderpornografie über File-Sharing Systeme oder durch verschlüsselten Email-Austausch wird durch die gegenwärtigen web-basierenden Ansätze nicht abgedeckt.
- Falls das Material nicht einsehbar gemacht wird, kann dies zu einer fehlgeleiteten politischen Debatte führen, weil der Eindruck geweckt werden könnte, dass das Problem der Online-Kinderpornografie adäquat bearbeitet wurde und dass dadurch in diesem Bereich das bürgerliche Bedenken reduziert wird.

Neben systematischen Einschränkungen von Sperrmethoden, müssen auch technische und legale Bedenken in Betracht gezogen werden.

Andere Ansätze ohne Sperrmethoden

- Verbesserte Mittel zur internationalen Zusammenarbeit, um der Zeitversetzung zwischen der Identifikation der illegalen Inhalte, die außerhalb des Landes abgespeichert sind, und der Entfernung der Inhalte gerecht zu werden.
- In der Absicht sein, diese Inhalte entfernen zu lassen, um ernsthafte Täter daran zu hindern, dass sie Zugriff auf diese Inhalte nehmen können.
- Untersuchen von kinderpornografischen Bildern, um zu gewährleisten, dass die Opfer auf diesen Bildern identifiziert werden und von diesem Missbrauch befreit werden.

Verschiedene europäische Länder wie Finnland, Norwegen, Schweden, die Schweiz, Großbritannien und Italien sowie nicht-europäische Länder wie Australien, China, Iran und Thailand benutzen Internet-Sperrungen. Die technischen Ansätze, das Ziel der Filtermethode und das Ausmaß der Industriebeteiligung ist jedoch unterschiedlich.

Zum Beispiel wird in Australien eine Sperrliste, die durch die ACMA (Australian Communications and Media Authority) erstellt wurde, verwendet und in absehbarer Zukunft wird dies für alle ISPs obligatorisch sein. In Großbritannien wird die Sperrliste durch die IWF (Internet Watch Foundation) erstellt. Die Technologie, die verwendet wird, ist BT Cleanfeed oder URL Filtering. In Dänemark wird die Sperrliste durch das National High Tech Crime Centre der dänischen Nationalpolizei Dänemark und durch 'Save the Children Dänemark' bearbeitet. In Finnland wurde die Domainliste zu Beginn von der finnischen Polizei zur Verfügung gestellt. Die meisten ISPs beteiligen sich heute an diesem Ansatz, der auf DNS-Sperrung beruht.

#### **1.4 Technische Aspekte der Internet-Sperrung**

Die Entwicklung und Implementierung verschiedener Arten von Internet-Sperrmethoden ist keine moderne Entwicklung. Seit längerer Zeit sind Spam, internet-basierende Viren, Malware und viele andere Inhaltsformen, die seitens des Endverbrauchers unerwünscht sind und unaufgefordert geschickt wurden, Zielscheiben von Sperrmaßnahmen, die von der Industrie zwecks Schutz und Benutzerfreundlichkeit eingeführt wurde bzw. durch die Regierung in ihrer Funktion als Entwickler und Hüter von Gesetzen und Verordnungen.

Es ist sowohl ein technischer Überblick zu den wichtigsten Internet-Sperrsystemen, die heute verwendet werden, notwendig als auch eine Erklärung darüber, wie diese Systeme bei verschiedenen Internet-Diensten Anwendung finden.

Zusätzlich zu den Bedenken hinsichtlich der Wirksamkeit derartiger Sperrsysteme, gibt es auch signifikante technische Einflüsse und Herausforderungen, die durch diese Systeme

entstanden sind. Es gibt auch viele Möglichkeiten, diesen Sperrsystemen aus dem Weg zu gehen und eine Analyse der Wirksamkeit dieser Systeme wird ebenfalls vorgestellt.

Demokratische Länder haben den Gebrauch der Internet-Sperrmethoden hinsichtlich verschiedener Aufgabenbereiche unterstützt und beziehen sich auf die Forderungen des Öffentlichkeit, dass bestimmte Sperrungen implementiert werden, um verschiedene Gesichtspunkte der öffentlichen Ordnung aufrecht zu erhalten, bei denen die Eigenschaften des Internets (internationale) Probleme der Umsetzung mit sich bringen. Länder mit strikterer Informationspolitik benutzen Sperrmethoden als eine technische Quelle, um ihre Handhabung der Informationskontrolle auf Online-Medien auszudehnen.

Alle diese Entwicklungen hängen von der Verfügbarkeit der Internet-Sperrmethoden ab. Je nach technischen Eigenschaften unterscheiden sie sich in ihrer Wirksamkeit sowie in ihrem Potential umgangen zu werden. Die Methoden zur Sperrung von kinderpornografischen Inhalten stehen im Mittelpunkt, aber es ist wichtig anzumerken, dass viele Sperrmethoden für andere Inhaltsarten oder Aktivitäten ohne großen Zusatzaufwand eingesetzt werden können.

### Spezifische Inhalte

Zur Durchführung von inhaltlichen Sperrversuchen werden Identifikatoren benötigt, auf Grund derer eine Sperrentscheidung implementiert werden kann. Die Inhalte, auf die sich der vorliegende Bericht bezieht, ist gewöhnlich von visueller Natur; dies bedeutet, dass die Inhalte entweder aus Standbildern oder Video-Aufnahmen mit Kindesmissbrauch bestehen.

- IP-Adresse
- Domainname und DNS
- URLs
- Dateiinhalt und Dateiname
- Schlüsselwörter
- Inhaltsmerkmale (Hash-Werte)

### Feststellen der Wirksamkeit

1. Es ist nicht möglich die Wirksamkeit bezüglich der **Inhaltmenge, die im Vergleich zu der Gesamtmenge an illegalen Inhalten korrekt gesperrt wurde, auszudrücken**, da die Gesamtmenge von verfügbaren illegalen Inhalten unbekannt ist.
2. Weil es oftmals unklar ist, woher die Zugriffe auf eine Website kommen, **Mengenangaben, die sich auf das Zugriffsvolumen einer bestehenden Liste beziehen, sind allenfalls sehr allgemeine Hinweise.**
3. Analysen zum **Über- und Untersperrungspotential** können als Indikatoren zur Wirksamkeit der Internet-Sperrmethoden verwendet werden.
4. Ein anderer Hinweis für die Wirksamkeit besteht darin, wie **leicht eine Sperrung umgangen** werden kann. Falls eine Sperrung leicht umgangen oder deaktiviert werden kann, wird der Zugriff auf das gesperrte Material wahrscheinlich davon nicht betroffen werden.
5. **Die Verfügbarkeit von alternativen Methoden, um den gleichen Inhalt abzurufen** (welche Mittel auch immer verwendet werden), kann als ein Maß für die Wirksamkeit der Sperrung angesehen werden, wobei detaillierte Daten nicht vorliegen.
6. **Die Verfügbarkeit anderer Mittel zur Rechtsdurchführung**, die andere, effektivere Methoden anbieten, um den Zugriff auf das Material zu verhindern, können auch abgerufen werden – speziell, wenn diese preisgünstiger, weniger intrusiv oder effektiver sind bezüglich der Bereitstellung des Materials.

### Eigenschaften der Sperrstrategien

- **Zulassungsliste versus Sperrliste** – Filter, die entsprechend konfiguriert sind, dass sie 'zulässige' Inhalte automatisch passieren lassen, aber ebenso über bestimmte Listen verfügen, um Inhalte zu sperren, werden gewöhnlich Sperrlisten genannt, wobei Filter, die automatisch konfiguriert sind, um alle Inhalte mit Ausnahme von bestimmten aufgeführten Inhalten zu sperren, als *Zulassungslisten* bezeichnet werden.
- **Menschliches Eingreifen (dynamische und nicht-dynamische Sperrung)** – Normalerweise basieren Kinderpornografie-Filter auf Beschwerden der Verbraucher und auf Untersuchungen des Gesetzeshüter. Die Inhalte der Filter werden gewöhnlich manuell ausgewählt, da der Listen-Administrator persönlich die Inhalte mit den Kriterien der Sperrlisten überprüft und vergleicht. Andererseits benutzen viele Filter wie Email-Filter und bestimmte Virus-Scanner oft vordefinierte Kriterien, um die Inhalte zu filtern und ohne menschliches Eingreifen zu sperren. Diese Kriterien können vielfältig und komplex sein.
- **Sperrpunkt** – Sperrstrategien können hinsichtlich des Levels, auf denen sie operieren, unterschieden werden. Ein Filter für den Benutzer-Level ermöglicht Eltern und Computer-Administratoren, bestimmte Inhalte auszuwählen und zu sperren. Andere Filter-Methoden werden bei Organisationen, ISPs oder auf Regierungsebene eingesetzt. Diese erfordern normalerweise, dass der gesamten Datenstrom durch zentrale Maschinen läuft, die wiederum die Daten analysieren.

### Detailstufen oder Spezifität

- **IP-Adresse** – Die Sperrung einer *IP-Adresse* bedeutet, dass andere Internet-Dienste und Benutzer, die die gleiche Adresse verwenden, auch gesperrt werden.
- **Domainname** – Die Sperrung eines Domainnamens wird **alle** Inhalte sperren, die unter diese Domäne fallen.
- **Uniform Resource Locators (URLs)** – Die besten Ergebnisse in Bezug auf die Spezifität wird durch einen Filterprozess erzielt, der auf einem URL basiert. Da diese Filter leicht umgangen werden können, weist die Sperrung durch diesen Identifikator ein großes Risiko für Untersperrung auf.
- **Inhaltsmerkmale** – Inhalte mit bestimmten Merkmalen können blockiert werden, die eine Klassifikation von zuvor als illegal eingestuften Inhalten ermöglicht. Neue Inhalte bleiben bei diesem Filter relativ leicht unentdeckt. Die Verschlüsselung der Inhalte führt dazu, dass diese Methode bedeutungslos ist.
- **Schlüsselwörter** – Die Sperrung beruht auf Schlüsselwörter, die Teil eines Dateinamen, eines URL oder eines auf einen Inhaltsort bezogenen Textes, auf den Zugriff genommen wird, sind. Eine komplexe Analyse der entdeckten Schlüsselwörter mit ihren Verwendungszusammenhängen muss durchgeführt werden.

### Internet-Zulieferungsmethoden von Kinderpornografie

Kinderpornografische Produkte können im ganzen Internet auftreten, indem verschieden Methoden über Internet-Verbindungen mit Hochgeschwindigkeit verwendet werden. Neben der Versendung von statischen Inhalten (Bilder und Video-Material), dienen diese auch als ein Startpunkt für vergleichbare Aktivitäten wie missbräuchliche Anfreundung (*Grooming*) und Internet-Schikanierung (*Cyber Bullying*). Die verstärkte Benutzung von sozialen Netzwerken ist insbesondere für die zuletzt erwähnten Aktivitäten von großer Bedeutung.

- Websites

Websites sind die primären Vertriebsmethoden für Internet-Inhalte. Web-Inhalte befinden sich normalerweise auf dem Server, aber Inhalte können auch dynamisch abgerufen werden oder dynamisch kreiert werden, wobei meistens eine Datenbank verwendet wird, um entsprechende Daten bereitzustellen. Für viele verschiedene Web-Server, die von verschiedenen Besitzern betrieben werden, trifft zu, dass sie nur mit einer IP-Adresse verbunden sind.

- Email und Spam (unaufgeforderte Email)  
Die Email ist der am häufigsten benutzte Internet-Dienst; dieser wird häufiger benutzt als das Web oder soziale Netzwerk-Websites.
- Usenet-Newsgroups  
Der entscheidende Unterschied zwischen Newsgroups und Email besteht darin, dass die Nachrichtenströme, die zwischen den Usenet-Servers passieren (auch häufig als 'Newsfeeds' bezeichnet), in Gruppen organisiert sind, die einen Hinweis auf die Inhalte der Nachrichten, die ausgetauscht werden, geben.
- Peer-to-Peer Netzwerke (P2P)  
Peer-to-Peer File-Sharing geschieht im Bereich des Datenaustauschs direkt zwischen den Computern der Endverbraucher und umgehen dazwischen geschaltete Server. Obwohl diese Methode legitim ist, führt dies dazu, dass Musik- und Video-Dateien ausgetauscht werden, und stellte daher die Inhaber von Copyrights vor großen Problemen.
- Suchmaschinen  
Durch die Indizierung der Website-Inhalte sind Suchmaschinen in der Lage, relevante Inhalte durch das Aufsuchen von Schlüsselwörtern und durch komplexe Suchalgorithmen zu identifizieren.
- IM und andere Methoden  
Ein andere wichtige Methode, um kinderpornografische Inhalte auszutauschen ist Instant-Messaging. Die IM-Kanäle dienen hauptsächlich als Prüf- und Einführungsmechanismus, wobei Inhalte direkt über andere Methoden ausgetauscht werden.

### Sperrstrategien & Wirksamkeit

- Website-Sperrung  
Die Sperrung von Websites wird gewöhnlich mittels eines von zwei verschiedenen Identifikatoren ausgeführt.
  - Der Server, der die Website speichert, könnte auf der Ebene der IP-Adresse gesperrt werden und hindert jeden daran, der den Filter benutzt, Zugriff auf diese Adresse zu erhalten. Eine Sperrliste würde dann nur aus den IP-Adressen bestehen, die mit illegalen Inhalten in Verbindung stehen.
  - Eine Sperrmethode könnte übernommen werden, die auf dem Domainname, möglicherweise auf dem URL einer bestimmten Datei oder auf einer von einer Website bereitgestellten Site basiert.
 Falls diese Form der Sperrung innerhalb des Zugriffsnetzwerks geschieht und nicht auf den Benutzergeräten, Überlistung ist, relativ gesprochen, für den Benutzer schwieriger, denn der Benutzer bräuchte einiges Grundwissen über die Funktionsweise des Internets.
- Email-Sperrung  
Die meisten Email-Filter kommen am oder kurz vor dem '**Empfangenden** Email-Server' zum Einsatz, der für Benutzer eines Netzwerks hereinkommende Mail empfängt. Es gibt zwei Arten von Email-Filterung:
  - Es gibt auf Verbindungen basierende Filter, die die ursprüngliche IP-Adresse des 'Schickenden Mail-Servers' hinsichtlich verschiedener Schwarzslisten überprüfen.
  - Die Filter können die Inhalte von Nachrichten verwenden, um inadäquate Inhalte auszusortieren.

Die Möglichkeit der Übersperrung besteht, wenn IP-Adressen oder sogar komplette ursprüngliche Mail-Server gesperrt werden, weil Fälle von Kinderpornografie aufgetreten sind.

- **Usenet-Sperrung**  
Die Sperrungsversuche von Usenet-Inhalte werden gewöhnlich durch die Sperrung des Zugriffs auf Teile der Gruppenhierarchie umgesetzt oder durch die Zurückweisung der Bereitstellung einer bestimmten Newsgroup. Internet-Access-Providers haben herausgefunden, dass bei Zugangssperrung auf verdächtige Hierarchien Benutzer dazu tendieren, ihre illegalen Inhalte unter weniger verdächtigere Bezeichnungen zu versenden, was möglicherweise dazu führt, dass illegales Material häufiger zufällig abgerufen wird.
- **Sperrung der Ergebnisse von Suchmaschinen**  
Es ist möglich, den Zugriff auf Suchergebnisse auf der Ebene des Suchmaschinenanbieters zu verhindern. Eine wichtige Fragestellung bezieht sich auf die Sichtbarkeit der Filterung und zwar wie sie auf den Ergebnisseiten der Suchmaschinen angezeigt werden. Einige Anbieter nehmen deutlich Stellung zum Konzept der Ergebnisaussortierung, andere äußern sich nicht. Das Umgehen des Filters ist ein leichtes Unterfangen: Es reicht aus, die Inhalte direkt abzurufen.
- **Peer-to-Peer und IM-Sperrung**  
Sperrversuche von Peer-to-Peer Datenfluss ist keine einfache Aufgabe. Viele P2P-Protokolle werden verteilt, d.h., dass heruntergeladene Dateien von verschiedenen Quellen generiert werden und daher besitzt kein einzelner Datenstrom die ganze Datei.
  - Eine Möglichkeit besteht darin, den Zugriff auf P2P-Inhalte zu sperren, indem die P2P-Netzwerkinhalte dadurch überprüft werden, dass man vorgibt, Benutzer des Dienstes zu sein. Durch Dateianfragen oder durch die Überwachung der Anfragen und Antworten anderer Benutzer ist es möglich Benutzer herauszufinden, die Teile dieser Datei auf deren Harddrive gespeichert haben. Die Sperrung ihrer IP-Adressen oder die Entfernung der Verbindung mit diesen Benutzern, falls es aus legaler und technischer Sicht umsetzbar ist, ist nur ein extremes Gegenmittel, das zur Verfügung steht.
  - Eine andere Möglichkeit, um mit maximaler Wirksamkeit Inhalte in diesen Netzwerken zu sperren, besteht darin, eine Methode vergleichbar mit der Deep Packet Inspection anzuwenden, um die Dateien während des Austausch zu erkennen.

### Zusammenfassung

Diese Tabelle führt Eigenschaften aller hier diskutierten Sperrstrategien auf. Sie verdeutlicht die Wahrscheinlichkeit von Über- und Untersperrung nach Maßgabe unserer Schätzungen, die erforderlichen Quellen zur Durchführung der Sperrstrategien, verschiedene Formen von Sperrlisten, den Aufwand zur Aufrechterhaltung derartiger Listen und zeigt in der letzten Spalte, ob hinsichtlich dieser Strategie (DPI-Technologie oder eine vergleichbare Methode) die Kommunikationsinhalte intensiv analysiert werden müssen, um die Sperrung effektiv zu gestalten.

Medium	Sperrung	Wirksamkeit				Sperrliste		DPI
		ÜBER-Sperrung	UNTER-Sperrung	Quelle erforderlich	Umgehen	Wartungsaufwand	Identifikatoren	
<b>Web</b>	DNS	SEHR UNW.	WAHRSCH.	WENIG	LEICHT	MITTEL	Domainname	-
	Domaine	SEHR UNW.	WAHRSCH.	MITTEL	MITTEL	MITTEL	IP-Adresse des Domainnames	-
	URL	WENIGER UNW.	SEHR UNW.	MITTEL	MITTEL	VIEL	URL	+

	IP	SEHR UNW.	WAHRSCH.	WENIG	MITTEL	MITTEL	IP-Adresse	-
	Dynamisch	SEHR UNW.	SEHR UNW.	VIEL	MITTEL	WENIG	Schlüsselwörter, Bilder, Erkennungs- Methoden usw.	+
	Merkmale	WENIGER UNW.	SEHR UNW.	VIEL	MITTEL	VIEL	Hash	+
	Hybrid (IP+Merkmal/URL)	WENIGER UNW.	SEHR UNW.	MITTEL	MITTEL	VIEL	IP und Hash oder URL	+
<b>Email</b>	Dynamisch	WAHRSCH.	WAHRSCH.	MITTEL	SCHWIERIGER	WENIG	Schlüsselwörter usw.	-
	URL	WAHRSCH.	WAHRSCH.	MITTEL	SCHWIERIGER	VIEL	URL	-
	IP-Adresse	SEHR UNW.	WAHRSCH.	MITTEL	SCHWIERIGER	VIEL	IP-Adresse	-
	Merkmale	WENIGER UNW.	WAHRSCH.	VIEL	SCHWIERIGER	VIEL	Hash	+
<b>Usenet</b>	Pro Gruppe	WAHRSCH.	WAHRSCH.	WENIG	LEICHT	WENIG	Gruppenname	-
	Pro Hierarchie	SEHR UNW.	WENIGER UNW.	WENIG	LEICHT	WENIG	Gruppenhierarchie	-
<b>Suche</b>	Schlüsselwort	SEHR UNW.	SEHR UNW.	VIEL	LEICHT	MITTEL	Schlüsselwörter	-
<b>P2P</b>	Pro Protokoll	SEHR UNW.	WENIGER UNW.	MITTEL	SCHWIERIGER	WENIG	Protokollerken- nung	+
	Pro Datei (Merkmal)	WENIGER UNW.	SEHR UNW.	VIEL	SCHWIERIGER	VIEL	Hash	+
	Pro Datei (dynamisch)	WAHRSCH.	SEHR UNW.	SEHR VIEL	SCHWIERIGER	WENIG	Komplexe Algorithmen	+

Während die Verteilungsmethoden unterschiedlich sein können, kann jede einzelne Methode als ein angemessener Ersatz für eine andere Methode fungieren. Unabhängig von der Wirksamkeit der Inhaltsspernung innerhalb eines Mediums, Fehler bei der Sperrung des gleichen Inhalts innerhalb eines anderen Mediums führt dazu, dass die Verteilungsmethode geändert wird.

Die meisten kinderpornografischen Internet-Aktivitäten umfassen heute vielfältige Dienste und Systeme des Internets. Es gibt verschiedene Fälle, die untersucht wurden, bei denen der Kontakt zwischen dem Erwachsenen und dem Kind in einem öffentlichen Chat-Room begann und mittels privatem Chat-Rooms, persönlichen Emails, privatem SMS- (Short Messaging Service) Mitteilungen innerhalb des Handy-Netzwerks weitergeleitet wurde und schließlich zu einem persönlichen Treffen, das mit einem privaten Handy-Anruf arrangiert wurde, führte. Die Analysen derartiger Aktivitäten sind sehr schwierig und erfordern ein großes Wissen seitens der Ermittler hinsichtlich aller Aspekte der Internet-Technologie und der Telekommunikation.

### Umgehen von Internet-Spernung

- Proxy-Servers

Das Umgehen dieser Filtermethode funktioniert sehr einfach. Um direkt einen Filtersperrzugriff zu umgehen, kann der Benutzer einen nicht-lokalen Proxy-Server auffordern, die Inhalte in seinem/ihrem Auftrag abzurufen und solange der nicht-lokale Server nicht gesperrt ist, kann der Benutzer das lokale Filtersystem umgehen und Zugriff auf den Inhalt erhalten.

- Tunnelling

Tunnelling-Software ermöglicht, einen verschlüsselten 'Tunnel' in Bezug auf eine andere Maschine im Internet zu schaffen, die die Filter-Software daran hindert, die Web-Anfrage einzusehen. Im Fall, dass ein Tunnel auf eine andere Maschine geschaffen

wurde, können alle Internet-Anfragen durch diesen Tunnel passieren und zwar durch die Maschine auf der anderen Seite hindurch und dann auf das Internet.

- Hosting or URL-Rotation

Aus der Sicht des Publizisten, der den Inhalt verbreiten möchte, ist eine Änderung der Website-Konfiguration hinsichtlich einer Adressenänderung ebenfalls trivial und würde problemlos IP, URL oder die Filter, die auf dem Domainname beruhen, umgehen.

- Botnets

Die Rotation des Domainnamens oder das Ausblenden der IP-Adresse geschieht oftmals durch die Verwendung der Botnet-Technologie, wobei kompromittierte unschuldige Endverbraucher-Maschinen benutzt werden, um als Portal für die Inhalte des Webservers zu fungieren. Im Wesentlichen wird der Computer des Benutzers in eine Non-Caching Proxy umgewandelt.

- Umgehen von DNS-basierenden Filtern

Wenn die Sperrung auf der Ebene der DNS-Abfrage erfolgt, kann dies sogar noch leichter umgangen werden. Die Benutzung eines anderen DNS-Servers des Anbieters (der nicht Teil der Sperrsysteme ist) ist ausreichend, diese Sperrmethode vollkommen zu umgehen.

Wenn andere Sperrmethoden verwendet werden als die, die sich auf die gesamten URL (Pfadname) oder auf bestimmte Inhaltsmerkmale beziehen, besteht ein großes Risiko der Übersperrung. Umgekehrt besitzen URL oder Inhaltsmerkmale ein großes Potential für Untersperrung.

Um die Web-Kommunikation effektiv zu sperren (z. B. Zugangssperrung des Benutzers auf die Inhalte und nicht nur die Anwendung von DNS-Filtern), ist eine beträchtliche Investition in die Infrastruktur der Proxy Deep Packet Analyse sowie eine substantielle Unterbrechung aller Internet-Kommunikationen erforderlich.

Die Filter bieten die Möglichkeit, den Straftätern, die illegale kinderpornografische Websites betreiben, nützliche 'Intelligenz' zu liefern. Wenn sie eine Website betreiben, die auf eine Sperrliste gesetzt wurde, wissen sie Bescheid, dass ihre Website seitens der Gesetzeshüter identifiziert wurde und dass die Wahrscheinlichkeit groß ist, dass sie Gegenstand krimineller Ermittlungen und Beobachtungen sind.

- Die Straftäter können dann Schritte einleiten, um jegliche Nachweise zu zerstören UND sie können auch ihren Dienst auf einen neuen Ort irgendwo sonst auf der Welt verlegen.
- Sie können entweder ihre Ausblendungsmethoden gegenüber dem Erkennungssystem überprüfen, um festzustellen, welche Methode längeren Schutz gegen Aufdeckung und Sperrung liefert.
- Sperraktivitäten verursachen auch Störungen für diejenige, die diese Websites besuchen, wobei sie die Website-Betreiber dazu zwingen, den Ort ihrer Inhalte häufig zu wechseln. Diese Veränderungen können auch analysiert werden und bieten eine nützliche Intelligenz für Ermittler, diese Veränderungen aufzuspüren und Ermittlungsdaten zu sammeln.

Die Kapazitäten und die Leistungen, die auf Grund des konstanten und anonymen Umgehens der Sperraktivitäten erforderlich sind, sollten nicht unterschätzt werden. Es ist wahrscheinlich, dass dies zu Fehlern führt, die früher als gedacht auftreten können. Es ist jedoch wichtig hervorzuheben, dass die Kapazitäten und Leistungen, die erforderlich sind, um ein Internet-Sperrsystem zu schaffen und aufrechtzuerhalten, ebenso von großer Bedeutung sind, insbesondere, wenn man auf permanente Umgehungsaktivitäten reagieren will.

### **Implikationen für eine demokratische Gesellschaft**

- Schutzannahmen

Die Infrastruktur erfordert, dass eine Sperrstrategie in der Lage ist, mit vielen kritischen Elementen der Internet-Verbindungen des Endverbrauchers interferieren kann. Der Inhalt von Sperrlisten ist für paedosexuelle Straftäter von großer Bedeutung, denn sie wollen die Sperrlisten aus Gründen verwenden, die im Gegensatz dazu stehen, wofür sie entwickelt wurden:

- Über- und Untersperrung

Es wurde in dem vorliegenden Bericht keine Strategie diskutiert, die in der Lage ist Übersperrung zu verhindern. Diese ist ein Hauptproblem beim Abwägen zwischen Kinderschutz und Menschenrechte / Freiheit. Es scheint unausweichlich zu sein, dass legale Inhalte gesperrt werden, wenn Sperrungen implementiert werden. Untersperrung ist ebenso ein universelles Phänomen, das insbesondere bei verhältnismäßigeren und spezifischeren Sperrstrategien auftritt.

- 'Mission-Creep' Potential und Re-Territorialisierung

Viele Sperrstrategien sind sehr intrusiv für die Internet-Kommunikation. Je granulärer sie sind, desto mehr sind inhalts-basierende Filtermethoden erforderlich, um Informationen über die Inhalte des Materials, das zwischen den Benutzern ausgetauscht wird, zu erhalten.

Es ist von Bedeutung, dass eine öffentliche Debatte stattfindet und dass diese Diskussion sowohl die wesentlichen Methoden und die legalen Unterschiede zwischen den verschiedenen Inhaltsarten berücksichtigt als auch das Verhältnis der Sperrungen in Bezug auf andere Methoden der Gefahrenminderung, der Straftatenvorbeugung und der Internet-Ermittlungen.

## 1.5 Internet-Sperrungen und das Gesetz

Der Versuch illegales Material zu sperren beinhaltet nicht, dass der Zugriff auf spezifische Bilder, Videos oder Websites vollkommen entfernt wird. Die unvermeidbaren Umgehungsmöglichkeiten, Untersperrung, Übersperrung, Mission-Creep, Gesetzeskonflikte und das Problem, dass Sperrungen nicht verhindern, dass das Material immer noch online zur Verfügung steht, alles dies bedeutet, dass der entscheidende Punkt nicht einfach darin besteht 'sperren oder nicht sperren', aber darin, welche Sperrmethoden eingeführt werden können, die in einer demokratischen Gesellschaft verhältnismäßig und akzeptabel sind. Entsprechend ist eine Überprüfung der legalen und demokratischen Herausforderungen, die die Internet-Sperrungen bewirken, von wesentlicher Bedeutung.

Ein umfassender Überblick zu den Internet-Sperrmaßnahmen und zum Gesetz erfordert eine Überprüfung der relevanten legalen Instrumente, von denen die Internet-Sperrsysteme betroffen sind. Moderne liberale Demokratien haben eine Schlüsselrolle bei der Verteidigung von fundamentalen Freiheiten und Bürgerrechten. Nationale als auch internationale Instrumente müssen berücksichtigt werden, um festzulegen, was fundamentale Rechte in Bezug auf die Internet-Sperrung bedeutet und welche fundamentale Rechte die Internet-Sperrung unterstützen. Die Rolle der Internet Service Provider ist grundlegend in Bezug auf die Internet-Sperrmaßnahmen, und sie operieren in unüberschaubaren Situationen hinsichtlich konkurrierender und manchmal widersprüchlicher Gesetzesanforderungen.

Aus der Sicht des Gesetzes stellt Internet-Sperrung eine Maßnahme dar, die uns hinsichtlich des Ziels, ein spezifisches Interesse zu schützen, das Recht geben zu sperren, die technischen Mittel zu wählen, die zur Umsetzung erforderlich sind und die Inhalte auszuwählen, die gesperrt werden sollen, alles unter der Annahme, dass dies Bürger schafft, die nicht das Recht besitzen, bestimmte Inhalte abzurufen oder zur Verfügung zu stellen.

Internet-Sperrung ist daher eine Maßnahme, die bestimmte Rechte oder Freiheiten schützen soll, die aber gleichzeitig einen direkten und sofortigen Einfluss auf andere Rechte und Freiheiten hat. Da die Rechte und Freiheiten durch das Gesetz festgelegt sind, erfordert eine

Analyse der Legitimierung der Internet-Sperrung (daher) eine eingehende Analyse der Gesetzeselemente, die hinsichtlich dieser Maßnahme relevant sind oder in Widerspruch stehen.

Da Internet-Sperrung eine Maßnahme ist, die international debattiert wird, konzentriert sich der gegenwärtige Bericht auf das internationale und europäische Gesetz, wobei einige Anwendungsbeispiele bezüglich nationaler Gesetze vorgestellt werden.

Innerhalb dieser legalen Systeme sind Internet-Sperrungen in Bezug auf zwei Bereiche des Gesetzes inkonsistent, nämlich in Bezug auf die Menschenrechten und die fundamentalen Freiheiten sowie hinsichtlich spezifischer Richtlinien, die sich auf die elektronische Kommunikation beziehen. Die Sperrung könnte mit einigen Aspekte dieser Rechte und Freiheiten verträglich sein, aber dies hängt von der Verhältnismäßigkeit der übernommenen Internet-Sperrungsmaßnahmen ab.

Die Herausforderung besteht in der Bestimmung, inwieweit eine Freiheit beschränkt werden kann, um eine andere zu erhalten. Jede einzelne Freiheit muss im Detail überprüft werden, um Schlussfolgerungen über die Bedingungen abzuleiten, die hinsichtlich legaler Prinzipien einer Internet-Sperrung akzeptabel erscheinen lässt.

Verschiedene nationale, europäische und internationale Verfassungen haben Menschenrechte und fundamentale Freiheit fest verankert, die offenbar eine Sperrmaßnahme rechtfertigen oder die durch eine solche Maßnahme nicht verhältnismäßig betroffen sind.

Die Aufrechterhaltung der Menschenrechte, insbesondere die, die im Widerspruch zu den Internet-Sperrmethoden stehen (z. B. das Recht auf ein Privatleben oder das Recht auf Pressefreiheit<sup>7</sup>), werden oftmals in demokratischen Gesellschaften als intrinsisch angesehen. Es gibt drei Aspekte, die das Verhältnis zwischen Demokratie und Freiheiten beleuchten:

- Wahlen – Das Prinzip, das jedermann am öffentlichen Leben teilnehmen kann.
- Gewaltenteilung – Die institutionelle Struktur sieht eine Trennung der Gewalten vor.
- Fundamentale Rechte – Die Bereitschaft und Engagement des Staates diese Freiheiten zu respektieren.

Die Unterschiede zwischen den Menschenrechten, den fundamentalen Freiheiten und den Bürgerechten beziehen sich hauptsächlich auf den *Eigentümer* der Rechte, der von den Inhalten der erhaltenen Rechte abhängig ist, auf den Wert der gesetzlichen Vorgaben und auf die Priorität des Schutzes. Wie es in vielen Ländern üblich ist, kann ein bestimmtes Recht entsprechend dem Recht auf eine geschützte Privatsphäre und dem Recht auf Meinungsfreiheit diese drei Qualifikationen erhalten. Bürgerliche Freiheiten stellen Beschränkungen der Gewalten seitens der Behörden in Bezug auf die Bürger dar.

Den Begriffen Menschenrechte und Bürgerrechte wurde der Begriff 'fundamentale Rechte' oder 'fundamentale Freiheiten' hinzugefügt. Fundamentale Rechte und Freiheiten sollen

- vor der Regierung und vor der Macht des Parlaments schützen;
- werden nicht nur durch die Gesetzgebung, aber vor allem durch das Grundgesetz oder durch einen internationalen und übernationalen Gesetzestext geschützt.
- werden durch die Regierung und der Justiz sichergestellt, indem das Grundgesetz (oder internationale Gesetzestexte) eingehalten wird und die Zuständigkeit nicht bei gewöhnlichen Richter liegt, sondern auch bei Verfassungsrichtern und sogar bei internationalen Richtern.

Die ersten Gesetzestexte, die die Menschenrechte und die fundamentalen Freiheiten erklärten, waren nationale Gesetzestexte. Internationale Gesetzestexte wurden nach dem Zweiten

---

<sup>7</sup> Siehe oberer Abschnitt **Error! Reference source not found.** and **Error! Reference source not found.**.

Weltkrieg verabschiedet und trugen dazu bei, die nationalen legalen Systeme zu modifizieren. Deren Inhalte wurden auch von Einrichtungen der Europäischen Union anerkannt.

Internet-Sperrversuche müssen aus der Sicht der prinzipiellen fundamentalen Freiheiten analysiert werden, die offenbar im Widerspruch zu denselbigen stehen – einschließlich Meinungsfreiheit und Recht auf Privatsphäre und Familienleben - und die sie gleichzeitig selber unterstützen – einschließlich das Recht der Kinder, gegen Gewalt und Ausbeutung geschützt zu werden.

Internationale Instrumente, die sich auf die Menschenrechte und fundamentale Freiheiten beziehen, wurden im Rahmen der Vereinten Nationen und des Europarats verabschiedet und setzen sich folgendermaßen zusammen:

- UN-Charta
- UN Allgemeine Erklärung der Menschenrechte (UDHR)
- UN Internationale Pakte über bürgerliche und politische Rechte
- UN-Konvention über die Rechte des Kindes
- UN-Konvention über die Rechte der Menschen mit Behinderungen
- UN Internationales Übereinkommen zur Beseitigung jeder Form von Rassendiskriminierung
- Europäische Menschenrechtskonvention (ECHR) des Europarats
- Übereinkommen des Europarats über Computerkriminalität

Obwohl die Europäische Union noch nicht die Europäische Menschenrechtskonvention übernommen hat, hat die Europäische Union erkannt, dass es notwendig ist, fundamentale Freiheiten zu schützen und die ECHR zu respektieren. Die Europäische Union unterstützt ebenso bestimmte Rechtskategorien und internationaler Gesetzestexte wie Kinderrechte, Behindertenrechte oder Rechte gegen Diskriminierung.

### **Fundamentale Freiheiten, die offenbar in Widerspruch zum Sperren stehen**

Internet-Sperrung kann einen Einfluss auf einige Menschenrechte und fundamentale Rechte haben.

- Internet-Sperrungsversuche können mit dem Recht auf die Privatsphäre interferieren, indem sie die Speicherung von Internet-Daten erlauben oder erzwingen, die durch die Privatsphäre geschützt sind, oder die einige Personen davon abhalten, das Internet-Potential auszunutzen and verhindern daher die Möglichkeit, dass bestimmte Verbindungen geschaffen werden oder bestimmte Verbindungen ausgewählt werden können, was dem Recht der Privatsphäre zuzuordnen ist. Dies trifft insbesondere beim unvermeidlichen Übersperren zu, weil vollkommen harmlose Websites davon betroffen werden.
- Internet-Sperrversuche können in Widerspruch mit der **Meinungsfreiheit** stehen, indem Personen daran gehindert werden, Zugriff auf Online-Informationen zu haben oder nicht die Möglichkeit haben, diese Informationen zur Verfügung zu stellen. Dies hat einen negativen Einfluss auf die Verbreitung von Informationen, Kommunikation und Empfang.
- Internet-Sperrungen stehen in Widerspruch mit spezifischen Rechten, die einige Personengruppen erhalten haben; zum Beispiel **das Recht von Behinderten**, Zugriff auf elektronische Kommunikationswege zu erhalten.
- Internet-Sperrungen können als ein Ersatz angesehen werden, um die Verpflichtungen der Kinderrechtskonvention nachzukommen, die Länder auffordern, alle angemessenen internationale Maßnahmen einzuleiten, um die Ausbeutung von Kindern zwecks pornografischer Absichten zu verhindern.

Das Recht auf Privatsphäre und Familienleben ist sowohl ein Menschenrecht als auch eine fundamentale Freiheit und stellt daher ein Bürgerrecht dar. Davon sind direkt Erwachsene und Kinder betroffen, und die Konvention der Vereinten Nationen hinsichtlich der Kinderrechte ergänzt dies sogar mit einer spezifischen Erklärung zum Kinderrecht mit dem Hinweis in Artikel 16, die Privatsphäre zu respektieren.

### Recht auf Privatsphäre

Diese Gesetzestexte schützen Personen vor willkürlichen Eingriffen in Bezug auf die Privatsphäre, die Familie, das Zuhause und die Korrespondenz, aber auch vor Attacken auf deren Ehre und Ruf. Die UDHR erklärt, „*Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen*“. Die ICCPR erklärt das Gleiche und fügt hinzu, dass **Eingriffe legal sein müssen**, was einige nicht legal abgesicherte marktführende Sperrinitiativen in Frage stellt. Die ECHR erlaubt einige Eingriffe unter den Bedingungen, die im Zusammenhang mit der sogenannten „öffentlichen Orderklausel“ (einschließlich des Rechtmäßigkeitsprinzips) beschrieben werden.

Das Prinzip des Briefgeheimnisses, das der Europäische Gerichtshof für Menschenrechte als „*Schutz der Vertraulichkeit privater Kommunikation*“ auslegt, ist eines der fundamentalen Freiheiten, die direkt durch eine Internet-Sperrmaßnahme untergraben werden könnte.

Unter Berücksichtigung des zu sperrenden Ziels (Inhaltsart, Kommunikationsprotokoll), der angewandten Sperrmittel und der zusätzlichen Regeln, die möglicherweise zum Einsatz kommen, um ein spezifisches Ziel im Rahmen des gesamten Vorgangs zu erreichen, können Internet-Sperrversuche manchmal zur Verfügbarkeit von Kommunikationsinhalten führen oder einige Details dieser Inhalte können in Bezug auf eine bestimmte Person freigelegt werden, ohne dass diese Person dem zugestimmt hat.

Auch im Fall, dass diese Kommunikationen, die eine Person erhält oder abschickt, nicht als Korrespondenz eingestuft werden, sind sie dennoch durch das Recht auf die Privatsphäre geschützt. Unter Berücksichtigung dieses Prinzips steht eine Sperrmaßnahme, die zur Überwachung oder Sicherstellung von Daten hinsichtlich der Inhalte, die eine Person empfängt, abschickt oder konsultiert (auch wenn es sich nur um die Beratung einer Website von bestimmter Natur handelt), in Widerspruch zum Recht auf die Privatsphäre. Dies würde ebenso in Widerspruch zum Recht auf persönlichen Datenschutz stehen.

Das Prinzip des Schutzes von persönlichen Daten impliziert die Diskretion dieser Daten, wenn sie mit Daten kombiniert werden können, die direkt oder indirekt die Identifikation einer natürlichen Person ermöglicht. Jedes Datenelement, das die Kontrolle von Personen ermöglicht, wird insbesondere in einem demokratischen Staat als gefährlich eingestuft, auch dann, wenn die Daten nicht benutzt werden.

Die Freiheit der Privatsphäre kann als eine Freiheit verstanden werden, um Beziehungen zu schaffen und aufrechtzuerhalten (auch auf elektronischem Kommunikationsweg), aber ebenso, um Optionen im Bereich Kultur, Freizeit oder Konsum online wahrnehmen zu können, oder um frei zu surfen und Informationen innerhalb des Netzwerkes abzurufen. Die Freiheit der Korrespondenz, die sich in der Kompetenz ausdrückt, mit ausgewählten Personen zu korrespondieren, ist selber durch das Recht des Briefgeheimnisses geschützt.

Eine Internet-Sperrmaßnahme, die einen negativen Einfluss auf die Freiheit der Korrespondenz haben würde, würde daher in Widerspruch zu Artikel 8 der Menschenrechtskonvention (ECHR) stehen.

Die Internet-Sperrung kann derartig ausgelegt werden, dass sie in Widerspruch zu einer fundamentalen Freiheit steht und zwar solange, wie **das Risiko des Eingriffs in eine Freiheit besteht, auch dann, wenn dies nicht zum Zweck geschieht, diese Funktionalität einzusetzen, die mit diesem Risiko verbunden ist.**

## Meinungsfreiheit

Die Meinungsfreiheit ist ein Menschenrecht und eine fundamentale Freiheit und daher ein Bürgerrecht. Sie wird auf Erwachsene und Kinder angewandt und die UN-Kinderrechtskonvention fügt eine spezifische Erklärung über das Recht des Kindes auf Meinungsfreiheit hinzu.

Dieses Recht beinhaltet *„unabhängig von Grenzen, die Freiheit zu besitzen, eine Meinung zu haben sowie Informationen und Ideen zu erhalten und zu teilen“*. Dieses Recht sollte *„ohne Eingriffe seitens der Behörden“* ausgeübt werden können.

Die Universelle Erklärung der Menschenrechte (UDHR) und der Internationale Pakt für bürgerliche und politische Rechte (ICCPR) fügt die Freiheit hinzu, Informationen und Ideen *„durch jegliche Medien zu suchen“*, und die ICCPR erklärt, dass dieses Recht *„entweder mündlich, schriftlich, in Druck, künstlerisch oder je nach Wahl durch jedes andere Medium“* ausgeübt werden kann.

Die ICCPR und die ECHR behaupten, dass mit der Ausübung der Meinungsfreiheit *„Pflichten und Verantwortungen“* verbunden sind, die bestimmten Auflagen erliegen.

Die Meinungsfreiheit umfasst das Recht Informationen zu erhalten, insbesondere durch das Internet. Jede Internet-Sperrmaßnahme, die eine Person daran hindert Inhalte abzurufen, würde daher in Widerspruch zu dieser Freiheit stehen. Es wäre für eine Maßnahme noch schlimmer, wenn für die Entfernung des Internet-Zugriffs plädiert wird, wobei eine Person davon abgehalten bzw. daran gehindert wird, das gesamte Internet-Netzwerk oder entsprechende Subdomains zu benutzen.

Im Rahmen der Reform zur Fernmeldegesetzgebung hat das Europäische Parlament erneut am 6. Mai 2009 bekräftigt, dass *„fundamentale Rechte und Freiheiten des Endverbrauchers keinen Einschränkungen unterliegen, solange keine vorausgehende Verabschiedung seitens der Justizbehörden stattgefunden hat (...) wenn die öffentliche Sicherheit sich in Gefahr befindet“*. Verschiedene Autoren und Abgeordnete des Europäischen Parlaments glaubten, dass dies eine Bestätigung dafür war, dass der Internet-Zugriff als ein fundamentales Recht anzusehen ist.

Unabhängig davon, ob der Internet-Zugriff ein *unabhängiges* fundamentales Recht ist oder nicht, es wird zumindest als ein Mittel zur Ausübung von Meinungsfreiheit geschützt, und jede Internet-Sperrmaßnahme, die Personen daran hindert, Informationen abzurufen, steht daher in Widerspruch zu dieser Freiheit. Jede Sperrmaßnahme beschränkt das Recht auf Meinungsfreiheit, mehr oder weniger in Abhängigkeit von den Sperreigenschaften und dem Grad der Übersperrung, um dem angestrebten Ziels dieser Maßnahme, den Zugriff auf spezifische Inhalte zu limitieren, gerecht zu werden.

## Die Rechte der Kinder

Jede Internet-Sperrmaßnahme, die Kinder daran hindert Informationen abzurufen, die für ihrer Entwicklung und Erziehung hinsichtlich eines verantwortungsvollen Lebens nützlich sind, würde in Widerspruch zur Kinderrechtskonvention und sicherlich zum Recht auf Meinungsfreiheit stehen, insbesondere, wenn dies nicht gemäß elterlicher Kontrolle geschieht.

## Die Rechte der Behinderten

Behinderte Personen haben zusätzlich das Problem, dass ihre Behinderung sie manchmal daran hindert, ihre Rechte vollkommen wahrnehmen zu können. Sie können durch den Gebrauch von elektronischer Kommunikation (einschließlich Internet-Dienste) Unterstützung erfahren. Demzufolge könnte eine Internet-Sperrmaßnahme behinderte Personen daran hindern, elektronische Kommunikation abzurufen, und verhindert, dass sie einige

fundamentale Rechte ausüben können, die nicht-behinderte Personen trotz Verbot, das Internet oder Subdomains davon zu benutzen, immer noch ausüben können.

### **Fundamentale Rechte und Freiheiten, die die Internet-Sperrung unterstützen könnten**

Der Schutz einiger Rechte und Freiheiten könnten die Internet-Sperrung unterstützen. Drei dieser Rechte sind folgende:

- Das Recht der Kinder vor Gewalt geschützt zu werden.
- Das Recht der Menschen, dass sie nicht diskriminiert werden.
- Das Recht des geistigen Eigentums.

Kinder werden sehr vor Gewalt geschützt. Es gibt zwei Aspekte des Schutzes des Wohlergehens der Kinder, die in dem vorliegenden Zusammenhang von großer Bedeutung sind.

- Die große Anzahl von Gesetzestexten, die mentale und physische Gewalt gegen Kinder untersagen, insbesondere wenn diese Gewalt von sexueller Natur sind.
- Im Rahmen des Verbots von Kinderpornografie besteht das Verbot von Bildern, die derartige sexuelle Verbrechen gegen Kinder zeigen.

Die Notwendigkeit gegen Kinderpornografie vorzugehen als auch die Notwendigkeit Kinder gegen Gewalt und gegen eine gestörte persönliche Entwicklung zu schützen, wird oftmals als ein Argument verwendet, um die Implementierung von Internet-Sperrmaßnahmen zu rechtfertigen. Dies ist oftmals die einzige Rechtfertigung seitens der Regierungen oder privater Einrichtungen, die die Internet-Sperrung unterstützen.

Wenn man die Argumente zur Unterstützung der Sperrung berücksichtigt, ist es aus juristischer Sicht schwierig zu verstehen, warum sich die Sperrmaßnahmen nur auf Kinderpornografie beziehen, da das Gesetz explizit andere Personengruppen vor Gefahren schützt und zwar insbesondere solche Gefahren, die durch Diskriminierung entstehen.

Die Menschenrechte und die fundamentalen Freiheiten gebühren ohne Ausnahme jeder einzelnen Person. Aus dem Grund, dass Diskriminierung war bzw. ist möglicherweise immer noch ein Problem in einigen Ländern, wurden verschiedene Gesetzestexte verabschiedet, um insbesondere das Recht einer jeden Person vor Diskriminierung geschützt zu werden. Internet-Inhalte, die unter diese Verbote fallen, können Texte sein, die Diskriminierung unterstützen, jedoch auch Bilder zu Folter und Tötung, aus rassistischen Beweggründen begangen. Diese Bilder sind äußerst störend and sollten einen vergleichbaren Status innehaben wie Kinderpornografie, um die Internet-Sperrung zu rechtfertigen.

Das Recht des geistigen Eigentums (IPR: Intellectual property rights) wird durch zahlreiche Abkommen auf internationaler Ebene geschützt. Die allgemeinen Erklärungen dieser Rechte, insbesondere die Copyrights and vergleichbare Rechte, *„schützen die Rechte der Autoren, Darsteller, Produzenten und Sendeanstalten, und tragen zur kulturellen und wirtschaftlichen Entwicklung der Länder bei“*. Das Recht auf den Schutz der IPR wird daher als ein Menschenrecht und als eine fundamentale Freiheit angesehen und stellt in einigen Länder auch ein Bürgerrecht dar. Man kann sich daher auf dieses Recht beziehen, um Internet-Sperrmaßnahmen zu rechtfertigen, solange diese Maßnahme dem Zweck dient, dieses tatsächlich zu schützen.

### **Besondere Verordnungen hinsichtlich elektronischer Kommunikation**

Eine Sperrmaßnahme, die seitens der Europäischen Union vorgesehen wird, muss zudem mit den europäischen Bestimmungen, die auf elektronische Kommunikationsformen angewendet werden, im Einklang stehen.

- Diese Bestimmungen umfassen die Obligationen des Internet Service Provider in Sinne der **Qualität des Dienstes** und **universellen Dienstobligationen** sowie der **Neutralitätsobligationen** seitens des Internet Service Providers.
- Die Bestimmungen, die sich auf die **Haftbarkeit** des Internet Service Providers beziehen, stellen für Internet Service Provider eine weitere Grundlage dar, gegen Sperrmaßnahmen zu argumentieren, die außerhalb des gesetzlichen Rahmens implementiert werden.

Die Dienste, die Teil des **universellen Dienstes** darstellen, sind grundlegende Kommunikationsdienste und umfassen mündliche Kommunikation und eine Internet-Verbindung. Jede Sperrmaßnahme, die einen Internet-Benutzer daran hindert, Zugriff auf das öffentliche Telefonnetzwerk zu erhalten, würde daher in Widerspruch zu den universellen Dienstobligationen stehen. Den Bürgern Zugriff auf das Internet zu gewähren bleibt ein Thema, dass mit anderen Rechten oder Freiheiten sowie mit dem allgemeinen Interesse der Öffentlichkeit in Einklang gebracht werden muss.

Falls eine schnelle Internet-Verbindung in Zukunft als Bestandteil eines universellen Dienstes angesehen wird und falls die gegenwärtigen Modifikationen der EU-Fernmeldegesetzgebung verabschiedet werden, würde ein einzelner Staat nicht autorisiert sein, jegliche Art von Sperrmaßnahmen zu implementieren, ohne Berücksichtigung der Europäischen Menschenrechtskonvention und zwar insbesondere auf die Notwendigkeit hin, die öffentliche Ordnungsklausel und das Recht auf ein ordnungsgemäßes Gerichtsverfahren zu respektieren.

Elektronische Kommunikationsdienste müssen ebenso eine bestimmte **Qualität des Zugriffsdienstes**, den sie anbieten, gewährleisten. Sie stehen in der Verantwortung, neben der Gewährleistung eines universellen Dienstes und einer öffentlichen Dienstobligation auch öffentliche Dienstinformationen zu transportieren.

Öffentliche Computer-Netzwerke sind aus technischer Sicht sehr komplex und viele Internet-Sperrmaßnahmen erhöhen die Netzwerkanfälligkeit in Bezug auf Abstürze und Verzögerungen. Demzufolge **verhalten sich elektronische Kommunikationsnetzwerke und Sperrungen aus philosophischer Sicht konträr zu einander** und erfordern seitens des Anbieters, eine Sperrmaßnahme derartig zu implementieren, dass zwei Obligationen mit gegensätzlichen Auswirkungen respektiert werden.

Internet Service Provider besitzen die Obligation sich gegenüber elektronischen Kommunikationsinhalten, die im Internet ausgetauscht werden, neutral zu verhalten und sollten dem Beispiel anderer Betreiber (z. B. herkömmliche Telefondienste und Postdienste) hinsichtlich anderer Kategorien folgen. Diesem Prinzip entsprechend kann der Internet Service Provider nicht wählen, in Abhängigkeit von den Inhalten nur bestimmte Daten weiterzureichen; als Ausnahme gilt eine grundlegende Vereinbarung seitens der Verbraucher oder eine gesetzliche Obligation, die das Nicht-Respektieren des Neutralitätsprinzips gerechtfertigt.

Mit der Ausnahme von spezifischen Obligationen, die gesetzlich verankert sind, kann ein Internet Service Provider nicht Inhalte kontrollieren, die in seinem Netzwerk ausgetauscht werden. Jede Sperrmaßnahme, die eine Kontrolle der im Netzwerk ausgetauschten Inhalte erfordert, um bestimmte illegale Inhalte zu identifizieren, würde daher nicht erlaubt werden, es sei denn, dass diese Maßnahme durch ein Gesetz, welches die europäische öffentlichen Ordnungsklausel respektiert, Unterstützung erhält.

Ohne ein Gesetz, das Internet Service Provider verpflichtet, spezifische Inhalte zu sperren, Internet Service Provider sind nicht erlaubt, Web-Inhalte zu kontrollieren und zu sperren, ohne dass sie gegen die Bedingungen ihres Haftschutzes gemäß der EU-Direktive verstoßen, und daher riskieren sie die Haftung für die Inhalte, die sie weiterreichen.

Ein Internet Service Provider, der ohne gesetzliche Verpflichtung zwecks Sperrung bestimmte Inhalte selektiert, würde dafür anfällig sein, außerhalb der festgelegten Anforderungen der gegenwärtigen Haftpflicht zu agieren. Dieser Internet Service Provider würde daher das Risiko eingehen, dass seine Haftung vor Gericht diskutiert wird und zwar in Bezug auf jeden durch seinen Dienst übertragenen illegalen Inhalt bzw. Aktivität. Dies würde eine ziemlich vage legale Situation darstellen. Es würde die Aktivität des Internet Service Provider selber in Frage stellen und im Allgemeinen auch die technische Entwicklung des jeweiligen Landes.

## 1.6 Abwägen der fundamentalen Freiheiten

Aus der Sicht des Internationalen Pakts über bürgerliche und politische Rechte und der Europäische Menschenrechtskonvention steht die Ausgewogenheit der Freiheiten immer im Zusammenhang mit der Einschränkung einer geschützten Freiheit, um eine andere aufrechtzuerhalten.

Im Rahmen einer Internet-Sperrmaßnahme müssen die Rechte der Kinder, die Rechte der Personen gegen Diskriminierung und die Rechte des geistigen Eigentums gegenüber den in Widerspruch stehenden Rechten und Freiheiten des Familienlebens und der Meinungsfreiheit abgewägt werden.

Einige Rechte, die im Internationalen Pakt über bürgerliche und politische Rechte und in der Europäische Menschenrechtskonvention festgelegt wurden, sind als 'absolut' zu verstehen (z. B. das Recht auf Leben oder nicht einer Folter ausgesetzt zu werden), während andere 'konditional' sind, weil sie Ausnahmegenehmigungen und/oder Einschränkungen zulassen (z. B. das Recht auf Privatsphäre und das Recht auf Meinungsfreiheit).

Ein erfolgreiches Abwägen der konditionalen fundamentalen Freiheiten, wenn verschiedene Rechte in Widerspruch zueinander stehen, kann durch eine Analyse der Prozesse erzielt werden, die vom Europäischen Gerichtshof für Menschenrechte angenommen werden und die Richtlinien dafür liefern, wie Internet-Sperrmaßnahmen implementiert werden können. Dies muss **der strikten 'öffentlichen Ordnungsklausel'** Rechnung tragen, die **das Prinzip der Notwendigkeit in einer demokratischen Gesellschaft** miteinbezieht. Diese Prinzipien werden dann auf verschiedene Internet-Sperrinitiativen angewendet, indem die Zielstellung dieser Initiativen untersucht wird und wie sie gemäß der ECHR-Richtlinien interpretiert werden könnten. Eine Überprüfung der legitimen Zielstellungen einer Internet-Sperrinitiative und die Gültigkeit einiger Systeme müssen in Frage gestellt werden. Ein schrittweises Vorgehen kann angewendet werden, um in der Lage zu sein, den Internet-Sperrvorschlag hinsichtlich seiner Legitimierung innerhalb einer demokratischen Gesellschaft zu überprüfen.

### The 'öffentliche Ordnungsklausel'

Die Möglichkeit, die konditionalen Rechte zu limitieren, kann zwei verschiedene Formen annehmen:

- Einige Bestimmungen, die die konditionalen Rechte proklamieren, spezifizieren bestimmte Situationen, in denen eine Einschränkung akzeptabel ist.
- Andere Bestimmungen, die die konditionalen Rechte proklamieren (z. B. Artikel 8 und 10 der ECHR in Bezug auf die Rechte der Privatsphäre und der Meinungsfreiheit), verweisen auf ein allgemeines Prinzip oder auf eine „*allgemein-öffentliche Ordnungsklausel*“ in dem Sinne, dass Eingriffe, die „**gesetzlich vorgeschrieben**“ sein müssen, „**ein legitimes Ziel oder Ziele**“ gemäß des Artikels haben, der das konditionale Recht erklärt, welches „**innerhalb einer demokratischen Gesellschaft hinsichtlich des Ziels bzw. der Ziele, die zuvor erwähnt wurden, als notwendig**“ angesehen wird.

Diese öffentliche Ordnungsklausel enthält daher folgende drei Hauptprinzipien:

- Die **exklusive Kompetenz des Gesetzes bei beschränkten Freiheiten**;
- Die **Notwendigkeit, die legitimen Ziele zu verfolgen, die durch die Konvention festgelegt wurden**;
- Die **'Notwendigkeit' des Eingriffs in einem 'demokratischen Land'** wird durch den Europäischen Gerichtshof für Menschenrechte in dem Sinne ausgelegt, dass die Eingriffe *„in einer Gesellschaft demokratisch bleiben“*
  - korrespondiert zu **„Druck auf die soziale Notwendigkeit“**
  - verhält sich **„verhältnismäßig zu den verfolgten legitimen Zielen“**.

### **Das Prinzip der Rechtmäßigkeit**

Jede Sperrmaßnahme, zumindest im Rahmen der ECHR, muss einem Gesetz folgen, dass folgende Eigenschaften aufweist:

- „der Zugriff auf *das Gesetz* muss adäquat sein“
- „eine Norm kann nicht als ein 'Gesetz' angesehen werden, es sei denn, dass sie mit einer ausreichende Genauigkeit verfasst wurde, um dem *Bürger darin beizustehen, seinen Verhaltenskodex zu bestimmen*“.

Der Vertrag zwischen dem Internet-Benutzer und dem Internet Service Provider wäre das einziges Abkommen, das eine Sperrmaßnahme erlaubt. Die Legalität einer solchen Sperrmaßnahme würde größtenteils von der Art des Inhalts, auf dem Zugriff genommen wird, abhängig sein; des Weiteren wären Informationen über die Natur des Verstoßes sowie Evidenzen erforderlich. Falls dies nicht auf angemessene Art und Weise spezifiziert wurde, ist es leicht, sich solche Verträge vorzustellen und wenn ein Verstoß in Hinsicht auf die von der EU proklamierten missbräuchlichen Klauseln in Verbraucherverträgen vorliegt, insbesondere dann wenn dem Internet Service Provider gestattet wird, einseitige Sanktionsmaßnahmen gegen den Verbraucher zu vollziehen.

### **Das Prinzip eines legitimen Ziels**

Die Menschenrechtskonvention und die ICCPR in Bezug auf die Meinungsfreiheit führen umfassend die legitimen Ziele auf, bei denen ein Eingriff in die fundamentalen Freiheiten legitim sein kann.

Ein legitimes Ziel, das durch das Gesetz, das eine Internet-Sperrmaßnahme erlaubt, verfolgt wird, ist jedoch nicht ausreichend, um eine Beschränkung gemäß der Europäischen Gesetzgebung als legitim ansehen zu können. Die Maßnahme muss innerhalb eines demokratischen Landes als *notwendig* gelten.

In Bezug auf die Privatsphäre erlaubt die ECHR folgende Eingriffe (Art. 8):

- *„im Interesse der nationalen Sicherheit, öffentlichen Sicherheit oder der wirtschaftlichen Gesundheit des Landes*
- *Verhüten von Störungen oder Straftaten*
- *Schutz von Gesundheit und Moral*
- *Schutz von Rechten und Freiheiten anderer Personen“*.

In Bezug auf das Recht der Meinungsfreiheit erlaubt die ECHR folgende Eingriffe (Art. 10):

- *„im Interesse der nationalen Sicherheit, territorialen Integrität oder öffentlichen Sicherheit*
- *Verhüten von Störungen oder Straftaten*
- *Schutz von Gesundheit und Moral*

- *Schutz der Ehre oder Rechte anderer Personen*
- *Verhüten der Freilegung von Informationen, die vertraulich empfangen wurden*
- *Aufrechterhaltung der Autorität und Neutralität der Justiz*“.

In Bezug auf das Recht der Meinungsfreiheit erlaubt die ICCPR folgende Eingriffe (Art. 19)

- *„Respekt der Rechte und Ehre anderer Personen“*
- *„Schutz der nationalen Sicherheit oder der öffentlichen Ordnung (ordre public) oder der öffentlichen Gesundheit oder Moral“.*

Um legitim zu sein, muss jede Sperrmaßnahme eine der Interessen verfolgen, die im relevanten Gesetzestext erwähnt wird; dies ist anhängig von der Konvention, dem ein Land angehört, und von der fundamentalen Freiheit, die die Maßnahme beschränkt. Einer der Schlüsselpunkte kann sein, das verfolgte Interesse bzw. das Ziel der Maßnahme zu bestimmen.

- **Spam-Sperrung**

Das Ziel der Spam-Sperrung bezieht sich als erstens auf den Schutz der Rechte des ISP, um den Bestand des Email-Dienstes aufrechtzuerhalten, und zweitens auf den Schutz der Freiheit auf Mitteilungen seitens des Benutzers des Dienstes. Das Ziel der Spam-Sperrmaßnahme, die die Freiheit auf Mitteilungen limitieren kann und daher die Freiheit auf Privatsphäre, scheint *„der Schutz der Rechte und Freiheiten anderer Personen zu sein“*, das gemäß Artikel 8 der ECHR ein legitimes Ziel ist.

- **Das Ziel, das Interesse des Opfers zu vertreten**

Einer der Ziele einer Sperrmaßnahme, die illegale Inhalte verfolgt, könnte das Interesse des Opfers sein, nicht im Zusammenhang mit einer kriminellen Umgebung gesehen zu werden. Daher entspricht dies dem Ziel, das oben als *„Schutz der Rechte anderer Personen“* definiert wurde, wenn zutrifft, dass entweder das Recht der Privatsphäre oder das der Meinungsfreiheit beschränkt wird. Da nicht jedes kinderpornografische Material identifizierbare Informationen enthält, könnte es nicht immer ein legitimes Ziel haben, und auf Grund der technischen Inadäquatheit der Sperrmaßnahmen kann die Sperrung bestenfalls einen partiellen Anspruch erheben, um diesem Kriterium *vollkommen* gerecht zu werden.

- **Das Ziel, Personen davon abzuhalten, sich illegale Inhalte anzuschauen: Moral oder Schutz der individuellen Anfälligkeit**

Eine Internet-Sperrmaßnahme, die illegale Inhalte verfolgt, um Personen davon abzuhalten, illegale Inhalte anzuschauen, schützt die Moral oder die Anfälligkeit schwächerer Mitglieder der Gesellschaft und kann mit dem Interesse auf *„Schutz von Gesundheit und Moral“* übereinstimmen. Falls das Ziel darin besteht, die Anfälligkeit schwächerer Bürger zu schützen, kann dies als legitim bezeichnet werden; demgegenüber scheint nur ein schwacher Zusammenhang in Bezug auf moralische Aspekte zu bestehen, insbesondere in Europa, weil die Menschen gewöhnlich illegale Inhalte zur Untersuchung melden. In diesem Zusammenhang ist es sinnvoll darauf hinzuweisen (wie oben erwähnt), dass das meiste Material, das gemeldet wurde, nicht von illegaler Natur ist.

- **Das Ziel Straftaten vorzubeugen**

Neben dem Ziel illegale Inhalte zu verfolgen, könnten Internet-Sperrmaßnahmen dazu dienen, Straftaten vorzubeugen.

- Das Anschauen von Kinderpornografie könnte bei einigen Personen, die nicht paedophil sind, dazu führen, dass sie ein solches Verhalten entwickeln, indem Sie regelmäßig kinderpornografische Bilder ansehen, obwohl es nur geringfügige Belege dafür gibt, dass dies tatsächlich der Fall ist.

- Internet-Sperrmassnahmen können kommerzielle kinderpornografische Geschäfte beeinträchtigen und daher Straftaten verhüten, falls das relevante Geschäft nicht eine Technologie implementiert hat, dass das Sperrsystem umgehen kann.

- **Das Ziel Straftaten zu unterdrücken**

Im Allgemeinen besitzt Internet-Sperrung nicht das Ziel, Straftaten zu unterdrücken, da eine Internet-Sperrmaßnahme nicht die Inhalte aus dem Internet entfernt. Internet-Sperrungen können stets umgangen werden, und sie erleichtern nicht die Ermittlungen, um die Hersteller, Zulieferer oder Opfer zu finden.

Einige Länder könnten den Entschluss fassen, Personen vom Internet-Zugriff auszusperrern, um eine Straftat oder eine Rechtsverletzung zu sanktionieren. Diese Sanktion könnte auch Straftaten verhüten.

## Das Prinzip des Bedarfs in einer demokratischen Gesellschaft

Das dritte und letzte Prinzip, das die öffentliche Ordnungsklausel enthält, ist das Prinzip des 'Bedarfs', dass der Europäische Gerichtshof für Menschenrechte dahingehend auslegt, dass ein Eingriff in Rechte und Freiheiten „*innerhalb einer Gesellschaft, die demokratisch bleiben möchte*“, eng mit der Dringlichkeit „*auf soziale Notwendigkeit*“ verbunden ist und im „*Verhältnis zum verfolgten legitimen Ziel steht*“. Das Prinzip des Bedarfs impliziert daher zwei Gesichtspunkte : der dringliche soziale Bedarf und Verhältnismäßigkeit zwischen dem Eingriff und dem verfolgten legitimen Ziel.

- **Ein dringlicher sozialer Bedarf**

Für den Europäischen Gerichtshof für Menschenrechte „*impliziert das Adjektiv 'notwendig' (...) den Anspruch auf einen dringlichen sozialen Bedarf und ist nicht synonym mit 'unverzichtbar' und hat nicht die Flexibilität wie die Ausdrücke 'zulässig', 'gewöhnlich', 'nützlich', 'angemessen' oder 'wünschenswert'*. Eine Internet-Sperrmaßnahme muss daher tatsächlich mit einem wirklichen Bedarf der Gesellschaft im Zusammenhang stehen und die Wirksamkeit dieser Maßnahme, um diesen Bedarf zu erfüllen, muss nachgewiesen werden.

Ein derartiger dringender 'sozialer Bedarf' könnte folgende Aspekte umfassen:

- Schutz des Rechts des geistigen Eigentums
- Moral und Schutz vor dem Anschauen von Kinderpornografie
- Schutz der Opfer
- Vorbeugen der Straftat (z. B. Vorbeugen, dass Personen paedophil werden, Beeinträchtigung des kinderpornografischen Geschäftsmodells, Vorbeugen, dass kinderpornografisches Material nicht ausgetauscht wird)
- Verdrängen der Straftat

- **Verhältnismäßigkeit zum verfolgten legitimen Ziel**

Die hinsichtlich einer fundamentalen Freiheit ausgeübten Eingriffe, die durch die Internet-Sperrung verursacht werden, müssen im Verhältnis zu dem verfolgten Ziel stehen (zusätzlich zur gesetzlichen Verankerung), um eine der *restriktiven* Ziele, die durch die ECHR vorgegeben sind, zu verfolgen und um dies als eine Antwort auf einen dringlichen sozialen Bedarf bewerten zu können. Es gibt eine Reihe von Faktoren, die verwendet werden können, um zu entscheiden, wo die Ausgewogenheit bei einem spezifischen Fall liegt. Einer dieser Faktoren bezieht sich auf „**den Gesamteffekt einer einzelnen Restriktion**“. Ein anderer Faktor bezieht sich darauf, „**ob eine ausreichende Basis für den Glauben bestand, dass ein besonderes Interesse in Gefahr war**“. Der Europäische Gerichtshof für Menschenrechte kann ebenso die Verhältnismäßigkeit von '*wirklichem Verhalten*', das eingeschränkt wird, überprüfen.

## Internet-Sperrung und Verhältnismäßigkeitskriterien

Die Analyse der Verhältnismäßigkeit der Sperrmethode im Vergleich zum verfolgten Ziel und in Anbetracht aller Kriterien, die oben analysiert wurden, erfordert eine hinsichtlich des Ziels der spezifischen Maßnahme basierende Abgrenzung, die deutlich den Unterschied jeder einzelnen Maßnahme hervorhebt.

- **Spam-Sperrung**

Spam-Sperrung basiert auf einer tatsächlichen Gefahr, die der Email-Dienst ausgesetzt ist, während das Verhalten, das eingeschränkt wird, bezieht sich auf das Recht Emails zu senden, ohne dass die implementierten Regeln eingehalten werden, um Spam zu vermeiden. Dies scheint ein angemessener Eingriff zu sein in Anbetracht der Gefahr, keine Emails senden zu können oder dass der Benutzer dem Email-Dienst nicht mehr vertraut. Schließlich scheint es momentan nicht der Fall zu sein, dass eine **weniger restriktive Maßnahme** die Ziele aufrechterhalten kann, die eine Spam-Sperrmaßnahme verfolgt.

- **P2P- oder Web-Sperrung im Interesse der Industrie für die geistigen Eigentumsrechte**

Eine Wen- oder P2P-Sperrmaßnahme, die das Interesse der Eigentümer der Rechte dienen würde, würde wahrscheinlich einen negativen Gesamteffekt nach sich ziehen.

- Erstens, falls gezeigt werden kann, dass P2P-Sperrung zur Verschlüsselung von P2P Kommunikationen führt, sodass Inhaltskontrolle weitestgehendst vermieden werden kann, würde es fast oder vollkommen unmöglich werden, diese Kommunikationen zu überwachen, auch dann, wenn es die Bedingungen erlauben.
- Zweitens würde es höhere Kosten für die Internet-Industrie, für die Regierung und für den Internet-Benutzer bedeuten.
- Drittens würde dies zur Sperrung von illegalen Dateien führen.

In Bezug auf das Kriterium, das den Anspruch erhebt, dass „eine ausreichende Basis für den Glauben besteht, dass“ die Rechte der Eigentümer 'in Gefahr' sind, können wir behaupten, dass keine Evidenz für eine solche Gefahr besteht. Es gibt keinen derartigen Beleg zu Natur und Ausmaß der möglichen Verluste, unter denen der Eigentümer auf Grund von P2P- oder Web-Rechtsverletzung leiden würde; entsprechende Studie bezüglich dieser Annahme sind unzureichend und weisen das Gegenteil nach.

- **Web- oder P2P-Sperrung von illegalen Inhalten mit dem Ziel, die Ehre des Opfers zu schützen**

Diese Verhältnismäßigkeit scheint akzeptabel im Sinne eines 'generellen Effektes' zu sein, solange die Sperrmaßnahme nicht den Effekt hat, andere Inhalte zu sperren. Leider würden wahrscheinlich auf Grund der Schwäche der Internet-Sperrsysteme andere Inhalte gesperrt werden, aber auch aus dem Grund, weil kinderpornografische Bilder eine kriminelle Szene zeigen, ohne dass das Opfer erkannt werden kann.

In Bezug auf 'Basis für den Glauben besteht, dass' bezieht sich das Interesse des Opfers auf 'in Gefahr sein'; das Interesse des Opfers könnte ebenso dazu dienen, den Leuten ein größeres Bewusstsein über die Straftat zu verschaffen, um Hotline-Meldungen zu unterstützen und um einen erhöhten Druck seitens der Bürger auf die Regierungen auszuüben gegen diese Straftaten vorzugehen, damit die Ermittlungen und deren Ressourcen verbessert werden.

Die Verhältnismäßigkeit des Verhaltens Kinderpornografie abzurufen kann aus der Sicht der Öffentlichkeit geschehen, die an der Identifizierung des Opfers interessiert ist, und hängt von der Motivation einer jeden Person ab, die diese Inhalte anschaut. Diese Motivationen könnten den Wunsch oder Absicht beinhalten, eine Straftat aus Kuriosität anzusehen, was nicht angemessen ist; es könnte der Wunsch sein, mehr über den Bestand der Straftat zu erfahren, um dagegen vorgehen zu können; oder es könnte der Wunsch sein, diese Bilder zwecks Ermittlungen zu melden.

- **Web- oder P2P-Sperrung von illegalen Inhalten mit dem Ziel, Moral oder das Interesse von empfindlichen Personen zu schützen**

Eine Sperrmaßnahme könnte dazu führen, dass diese Personen auf Grund der Schwäche der technischen Methode nicht in der Lage ist, nicht-kontroverse Inhalte abzurufen. Weiterhin wird dies Straftäter nicht davon abhalten, Zugriff auf die Inhalte zu nehmen. Entsprechend könnte das zum allgemeinen Effekt führen, dass Recht der Meinungsfreiheit wertgemindert wird, während Straftäter immer noch in der Lage sein würden, unmoralische und schockierende Inhalte abzurufen, und Personen würden auch auf schockierende und unmoralische Inhalte, die unterschiedlicher Natur sind, zugreifen. Eine solche Situation wäre nicht angemessen.

- **Web- oder P2P-Sperrung von illegalen Inhalten mit dem Ziel, Straftaten zu verhüten**

Das Ziel der Verbrechensverhütung sollte versuchen zu verhüten, dass Personen eine Straftat begehen oder eine Straftat unterstützen, indem sie illegale Inhalte kaufen, herunterladen oder verkaufen. Die Verhältnismäßigkeit würde vom Anteil der Bevölkerung abhängig sein, die eine Straftat nicht mehr begehen würde, weil sie auf illegale Inhalte keinen Zugriff mehr hat, was gegenüber den Einschränkungen der Bürgerrechte, die durch diese Maßnahme entstehen würden, gewichtet werden müsste. Die Auswirkungen der Maßnahme könnten derart sein, dass keine entscheidende Verminderung der Meinungsfreiheit oder der Freiheit der Privatsphäre für *den einzelnen* Bürger vorliegt.

Zurzeit liegt keine Evidenz vor, dass eine Sperrmaßnahme zur Abnahme dieser Straftat führen würde, während dies gleichzeitig einige legitime und verhältnismäßige Verhaltensweisen beschränken würde.

- **Sperrung des Internet-Zugriff für eine Person mit dem Ziel, Straftaten zu unterdrücken und zu verhüten**

Im Allgemeinen hat die Internet-Sperrung (und manchmal auch die Sperrung des Telefon- und TV-Dienstes) für eine Person das Ziel, Straftaten zu unterdrücken und zu verhüten. Dieser Effekt ist ausgewogen, weil dieser Person der Freiheit beraubt wird, elektronische Mitteilungen zu empfangen und zu versenden, aber auch der Freiheit der Ausübung der Privatsphäre und des Familienlebens und der Freiheit innerhalb der elektronischen Welt zu korrespondieren. Es kann nur verhältnismäßig sein, wenn es in Bezug auf die begangene Straftat gerechtfertigt wird und es dem Ziel der Unterdrückung und der Verhütung dient.

### **Weitere Konsequenzen des Prinzips des dringlich Bedarfs eines Eingriffs**

Zusätzliche Eingriffe werden durch verschiedene Internet-Sperrmaßnahmen aktiviert und zwar auf Grund der Natur der Methode, die eingesetzt wird, um die Sperrung zu implementieren. Einige Spam-Sperrmethoden ermöglichen zum Beispiel einen ISO, jede einzelne gesendete oder empfangene Mitteilung zu scannen, was zur gleichen Zeit andere Eingriffe erlaubt wie die Retention von persönlichen Daten in Bezug auf die gesamte Mitteilung und hinsichtlich bestimmter Wörter, die in den Inhalten auftreten.

Die Verhältnismäßigkeit jeder Maßnahme, die mit einigen Freiheiten interferiert, muss erstens hinsichtlich des beabsichtigten Ziels untersucht werden, und zweitens in Bezug auf den allgemeinen Effekt, der nicht weiter reichen sollte als die notwendige Vorgabe des Ziels; auf jeden Fall müssen **'Spielräume vorgesehen' werden, damit die eingeschränkte Freiheit ausgeübt werden kann und nicht 'beseitigt' wird.**

Jedes Mal, wenn eine Internet-Sperrmaßnahme erlaubt wird, müssen einige Garantien implementiert werden, um zu verhüten, dass durch die Anwendung dieser Sperrmethode Freiheiten noch mehr gefährdet werden als es durch das Erreichen des Ziel notwendig vorgegeben ist. Dies ist notwendig, auch wenn die Maßnahme ein legitimes Ziel verfolgt und ihre prinzipielle Funktion andere Freiheit nicht unverhältnismäßig einschränkt. Diese

Maßnahme kann vor den Risiken, die im ersten Paragraphen des Unterabschnitts ausgeführt wurden, schützen. Derartige Garantien können technischer Natur sein, indem die Funktionalitäten überprüft werden, die weitere Freiheiten gefährden, oder von legaler Natur sein, indem weitere Funktionalitäten verboten werden oder wenn deren Anwendungen unterlassen werden, wenn sie nicht für die Sperrmethode relevant sind. Einem Richter muss jedes Mal erlaubt werden, die Verhältnismäßigkeit einer einzelnen Sperrmethoden zu überprüfen.

### **Die Kompetenz des Richters, die Verhältnismäßigkeit der Eingriffe in Bezug auf fundamentale Freiheiten zu überprüfen**

Der Europäische Gerichtshof für Menschenrechte kontrolliert die Maßnahmen der Vertragsstaaten, wenn fundamentale Freiheiten sowie die Interpretation nationaler Gerichte in Frage gestellt wird. Die nationalen Gerichte haben ebenso das Recht ein Urteil hinsichtlich des Disputs über Sperrmaßnahmen, von denen ein Bürger betroffen ist, zu fällen, aber ebenso über Inhalte, die ein Bürger gerne senden, empfangen oder begutachten möchte.

Falls es ein fundamentales Recht ist, dass man auf Grund einer möglichen Freiheitsverletzung eine Entscheidung vor Gericht in Frage stellen darf, dann bedeutet dies, dass die Einschränkung bereits vollzogen wurde und dass der Bürger bereits unter diesen Auswirkungen leidet. Daher ist es von Bedeutung, dass ein Richter eingreifen kann, bevor eine Sperrentscheidung stattgegeben wird. Unter Berücksichtigung der Internet-Sperrung beziehen sich diese Situationen erstens auf die Überprüfung und Beurteilung des illegalen Inhalts bzw. Der illegalen Aktion und zweitens auf die Bewertung der Verhältnismäßigkeit der Antwort hinsichtlich dieser illegalen Situation.

In Bezug auf das oben Genannte und auf die Details, die in **Error! Reference source not found.** beschrieben werden, scheint die einzige Internet-Sperrmaßnahme, die keine Entscheidung seitens eines Gerichtes bedarf, die *Spam-Sperrung* zu sein, wenn *sie dem Ziel dient, Moral aufrecht zu erhalten*, obwohl mit dem Letzteren eine Reihe anderer legaler und praktischer Einwände verbunden sind.

### **Bedingungen, unter denen Internet-Sperrung akzeptabel sein kann**

Liberale Demokratien müssen fundamentale Freiheiten respektieren sowie die Bedingungen der Auflagen, die einem Gericht für Menschenrechte erlegen ist. Internet-Sperrmaßnahmen können nur dann korrekt implementiert werden, wenn folgende Schritte berücksichtigt werden:

1. Schritt      Internet-Sperrungen müssen derartig implementiert werden, dass andere Rechte und Freiheiten nicht verletzt werden.
2. Schritt      Das Bestimmen der Rechte und Freiheiten, die eingeschränkt werden.
3. Schritt      Das Ausmaß der Einschränkung bestimmen.
4. Schritt      Das Ziel bzw. die Ziele genau verfolgen.
5. Schritt      Festlegen, ob das Sperrziel mit der Realität zu vereinbaren ist.
6. Schritt      Bestimmen, ob die Sperrung hinsichtlich des festgelegten Ziels eine angemessene Antwort auf einen dringlichen sozialen Bedarf darstellt.
7. Schritt      Analysieren der Verhältnismäßigkeit des Eingriffs in Bezug auf das verfolgte Ziel.
8. Schritt      Berücksichtigen der Prinzipien, die die Sperrung hinsichtlich der Kriterien des Europäischen Gerichtshofs regeln (Bedarf in einer demokratischen Gesellschaft, ein dringender sozialer Bedarf).
9. Schritt      Festlegen, ob ein Gesetz benötigt wird, um den Gebrauch bestimmter Funktionen der Sperrmethode zu verhüten.

10. Schritt Sperrung muss im Rahmen der Gesetzgebung erfolgen.

### **Erforderliche Studien**

Im Rahmen der Prozessanalyse zur Ausgewogenheit fundamentaler Freiheiten wurden je nach Bedarf verschiedene Studien identifiziert, um eine ausreichende Evaluierung der Anforderungen für Verhältnismäßigkeit zu ermöglichen. Ohne Forschung kann diese Verhältnismäßigkeit nicht aufgezeigt werden. Dies umfasst folgende Gesichtspunkte:

- Internet-Sperrung und Schutz vor Pädophilie
- Eingriff in Kommerzielle Kinderpornografische Geschäftsmodelle
- Internet-Sperrung: Reduzierung des Austauschs von Kinderpornografie
- Internet Blocking: Schutz der Empfindlichen Personen oder Moral
- Internet Blocking: Schutz des Interesses des Opfers
- Internet Blocking: Schutz des Rechts des geistigen Eigentums

### **1.7 Schlussfolgerung**

Auf Grund des fundamentalen Einflusses auf unsere Rechte frei zu kommunizieren, besteht ein dringlicher Bedarf in unserer Gesellschaft, den Einfluss der Internet-Sperrmaßnahmen zu verstehen, auch dann, wenn der Begriff der Internet-Sperrung aus umgangssprachlicher Sicht zunächst unproblematisch zu sein scheint. Es gibt viele gut-begründete Motivationen, warum die Gesellschaft den Einsatz von Internet-Sperrung in Betracht zieht, allerdings sind die Menschenrechte und die legalen, vertraglichen, politischen und technischen Annahmen sehr komplex. In den Fällen, bei denen Sperrversuche implementiert wurden, entstanden oftmals Enttäuschungen und Verwirrungen hinsichtlich der Wirksamkeit des oder der Ziele dieser Systeme. Internet-Sperrung hat auch entscheidende Implikationen für alle Bürger hinsichtlich der Privatsphäre und Sicherheit. Der vorliegende Bericht evaluiert die Bedeutung der Internet-Sperrung und weist auf die praktischen und legalen Konsequenzen hin.

Der Bericht beschreibt die Motivationen, die der Internet-Sperrung zugrunde liegen und wie offenbar andere Ansätze fehlgeschlagen sind. Er prüft kritisch, wer die Sperrung durchführt, was gesperrt werden könnte, wie die Sperrung angegangen werden kann und wer das Ziel der Internet-Sperrversuche sein wird.

Sowohl der technische Überblick zu den wichtigsten Internet-Sperrsystemen, die heute verwendet werden, als auch eine Beschreibung dessen, wie diese Systeme von verschiedenen Internet-Diensten verwendet werden, betonen den Anstieg der Inhaltsbreite und die Dienste, die für Sperrinitiativen angewendet werden. Eine Analyse der Wirksamkeit der Internet-Sperrsysteme weisen auf die vielen unbeantworteten Fragen hinsichtlich des Erfolgs dieser Systeme hin, aber auch auf deren Fähigkeiten, die angestrebten Ziele zu erreichen. Fast alle Systeme haben einen technischen Einfluss auf die Belastbarkeit des Internets und fügen im bereits sehr komplexen Netzwerk eine weitere sehr komplexe Komponente hinzu. Alle Internet-Sperrsysteme können umgangen werden und manchmal ist nur geringfügiges technisches Wissen notwendig, um dies zu erzielen. Es gibt eine Reihe von zur Verfügung stehenden Software-Lösungen im Internet, die dazu beitragen können, den Internet-Sperrmaßnahme zu entkommen.

Die umfassende Zusammenfassung zur Internet-Sperrung und zum Gesetz, insbesondere in Bezug auf Menschenrechte, fundamentale Freiheiten und Bürgerechte, lässt große Bedenken hinsichtlich des gegenwärtig implementierten Sperrsystems aufkommen. Der Überblick zum legalen Status umfasst nationale und internationale Instrumente und berücksichtigt, welche fundamentalen Rechte in Widerspruch zu Internet-Sperrungen stehen und welche fundamentalen Rechte Internet-Sperrungen unterstützen. Die Komplexität der ausgewogenen Rechte, die sich im Widerspruch befinden, müssen seitens der Richter, die hinsichtlich dieser komplexen Fragestellungen ausgebildet wurden, beurteilt werden.

Die Internet Service Provider sind kommerzielle profit-orientierte Einrichtungen, die vermehrt aufgefordert werden, soziale Verordnungen ohne angemessene Kontrolle oder Nachweisbarkeit zu implementieren. Sie operieren in einer sehr undurchsichtigen Situation in Bezug auf wettbewerbsorientierten und manchmal aus legaler Sicht widersprüchlichen Anforderungen. Zum Beispiel, auf der einen Seite wird ein hoher Standard hinsichtlich der Qualität des Internet-Zugriffs angeboten und auf der anderen Seite werden Zugriffssperrungen auf bestimmte Dienste implementiert.

Der Hauptgesichtspunkt hinsichtlich der Ausgewogenheit fundamentaler Freiheiten, wenn verschiedene Rechte in Widerspruch zueinander stehen, besteht darin, dass eine genaue Analyse stattfinden muss, die die vom Europäischen Gerichtshof für Menschenrechte ratifizierten Prozesse simuliert; dies verschafft indirekt Richtlinien dafür, wie Internet-Sperrmaßnahmen eingesetzt werden sollen, wenn diese als angemessen, verhältnismäßig und technisch machbar angesehen werden. Diese Analyse muss der strikten öffentlichen Ordnungsklausel und dem Bedarfsprinzip einer demokratischen Gesellschaft Rechnung tragen. Diese Prinzipien werden dann hinsichtlich verschiedener Internet-Sperrungsinitiativen angewendet, indem die Aufgabenstellung dieser Initiativen überprüft wird und wie sie in Bezug auf die Richtlinien des Europäischen Gerichtshofs für Menschenrechte interpretiert werden würde. Dieser Bericht überprüft die legitimen Ziele der Internet-Sperrungsinitiativen und stellt die Gültigkeit einiger zurzeit in Anwendung befindlichen Systeme in Frage.

Die technische Implementierung der Internet-Sperrmaßnahmen kann nicht isoliert geschehen und muss dem tatsächlichen Einfluss auf die zu verhütende Straftat Rechnung tragen. Sie müssen auch die Korrektheit und Wirksamkeit der Sperrmaßnahmen berücksichtigen und müssen unmissverständlich die negativen Konsequenzen hinsichtlich des *legalen* Inhalts und Internet-Gebrauchs bestimmen. Die Beurteilung der technischen Wirksamkeit muss expliziter Bestandteil der Ausgewogenheitsevaluierung der Rechte sein.

Viele Sperrmaßnahmen sind leicht zu umgehen und sind daher hinsichtlich vieler angestrebter Ziele vollkommen unwirksam. Überraschenderweise stellt die DNS-Sperrung, die heute von vielen nationalen Sperrsystemen verwendet werden, eines der Systeme dar, das am leichtesten umgangen werden kann - absichtlich oder zufällig. Es wird festgestellt, dass eine signifikante Enttäuschung hinsichtlich der Ineffizienz im Rahmen der internationalen Internet-Kriminalitätskooperation besteht, was auch die ausbleibende Antwort einiger Länder auf Kinderpornografie, Hassreden und Terrorismus mit einbezieht. Anstelle, dass wir unsere Hände zur Aufgabe hochhalten und uns nach nationalen protektionistischen Strategien richten, müssen wir diese internationalen System verbessern und ihre Effektivität für das 21. Jahrhundert vorbereiten.

Zurzeit gibt es nur wenige implementierte Internet-Sperrmaßnahmen, die auf Grund einer informierten öffentlichen Debatte, die in einer transparenten und nachvollziehbaren Weise durchgeführt wurde, bestehen. Da es komplexe Annahmen hinsichtlich der Menschenrechte und anderer legaler Gesichtspunkte gibt, die einen Einfluss auf die Verabschiedung der Internet-Sperrdienste ausüben, empfiehlt dieser Bericht ein schrittweises Vorgehen zu folgen, um die Internet-Sperrvorschläge hinsichtlich ihrer Legitimierung im Kontext einer demokratischen Gesellschaft beurteilen zu können.

Es ist fragwürdig, warum illegale Inhalte wie Kinderpornografie, die weitverbreitet in vielen Ländern illegal ist, und andere Inhalte, die universell abgelehnt und fast universell als illegal gelten<sup>8</sup>, online bleiben und von einigen Internet-Benutzer immer noch abgerufen und heruntergeladen werden können. Es ist ebenso fragwürdig, dass der private Sektor und nicht-gewählte Repräsentanten durch Regierungen ermächtigt und unterstützt werden, umfassende Sperrungen von Inhalten auf eine nicht-transparente und nicht-nachweisbare Weise zu implementieren. Nach angemessener Untersuchung und legaler Beurteilung (und falls eine

---

<sup>8</sup> Im Dezember 2008 haben 193 Länder (jedes Mitglied der Vereinten Nationen mit Ausnahme der USA und Somalia) eine UN-Konvention bezüglich des Kinderrechts ratifiziert. Es sei jedoch zu erwähnen, dass sogar die USA eine Gesetzgebung für Kinderpornografie besitzt.

Sperrung verabschiedet wird) besteht die Funktion der Justiz darin zu klären, was im Internet gesperrt werden kann, wie es gesperrt werden soll und wie die Überwachung und öffentliche Nachweisbarkeit dieser System erfolgen kann. Es ist überraschend, dass viele EU-Regierungen, die nicht direkt in der Lage sind Internet-Sperrungen zu legalisieren, weiterhin industrielle Initiativen in diesem Sektor unterstützen. Ironischerweise werden manchmal die Sperrlisten dieser Ländern, die zwecks Internet-Sperraktivitäten durch regierungsfreundlichen Organisationen erstellt werden, ohne unabhängige Kontrolle eingeführt.

Der Hauptgesichtspunkt einer Internet-Sperrmaßnahme bezieht sich auf die Verhältnismäßigkeit. Die Maßnahme muss verhältnismäßig mehr Auswirkungen auf negative Effekte der illegalen Inhalte und kriminellen Internet-Aktivitäten haben als auf legale Inhalte und Aktivitäten. Eine derartige Maßnahme muss im Einklang mit dem Gesetz stehen und muss derartig implementiert werden, dass andere Rechte und Freiheiten nicht verletzt werden.

Um es auf den Punkt zu bringen, Internet-Sperrung basiert auf technischen Lösungen, die für sich genommen selber inadäquate sind und die des Weiteren durch die Verfügbarkeit von alternativen Protokollen des Abrufs und Herunterladens von illegalem Material umgangen werden. Daher muss die Beurteilung der Verhältnismäßigkeit nicht nur die verschiedenen Rechte, die wirksam werden können, abwägen, sie muss auch der Inadäquatheit der Sperrmethoden Rechnung tragen, um die relevanten Rechte und die Risiken der unbeabsichtigten Konsequenzen zu schützen; zum Beispiel ein verminderter politischer Druck für umfassende Lösungen oder die Möglichkeit, dass der Anbieter von illegalen Websites in Betracht zieht neue Strategien zu entwickeln, um schließlich Sperrungen zu vermeiden, die dazu führen, dass Ermittlungen seitens der Gesetzeshüter in der Zukunft noch schwieriger werden.

Die Ergebnisse der Studie bestätigen, dass die praktischen, technischen und legalen Annahmen, die in Verbindung mit der Sperrmethode stehen, nicht einfach auf die Wahl 'sperrn oder nicht sperrn' bezogen werden können. Die Länder, die bereits verschiedene Sperrmethoden implementiert haben, und die Länder, die sich in der Absicht befinden, müssen zwei konkrete Schritte einleiten:

- Die Tatsache, dass Sperrung eine Option darstellt, die in Betracht gezogen wird, geht einher mit dem Erkennen (und falls nicht, dann zumindest mit einer impliziten Akzeptanz), dass Fehler in der internationalen Kooperationen hinsichtlich fundamentaler Annahmen begangen wurden, die die menschliche Würde und den Schutz der am leichtesten Verletzbarsten in unserer Gesellschaft (in Bezug auf Internet-Kinderpornografie) betreffen.

Eine angemessene Analyse der exakten Natur dieses Fehlers ist erforderlich, sodass diesem Aspekt besser Rechnung getragen werden kann. Auf der Grundlage dieser Analyse sollte alle Länder einen formalen Bericht entwerfen, der gemäß Artikel 34 der UN-Konvention Auskunft über ihre Anstrengungen zu den Rechten des Kindes gibt, und der jährlich als Teil der periodische Berichterstattung gemäß Artikel 44 veröffentlicht werden sollte. Dies würde den Vorteil haben, dass die Länder auf diesem Gebiet aktiver werden mit der Konsequenz, dass der öffentliche Zugriff auf diese Websites entzogen wird und dass mehr Kinder von Missbräuchen befreit werden.

- Eine Überprüfung des praktischen Einflusses (auf den zufälligen Zugriff, den bewussten Zugriff, das Geschäft der Kinderpornografie und die Benutzung alternativer Methoden zur illegalen Inhaltsverbreitung) ist möglich und notwendig, indem Daten der bestehenden Sperrsysteme verwendet werden. Ohne diese Überprüfung bleibt die Verhältnismäßigkeit der Sperrung –und daher die Legalität gemäß fundamentaler Menschenrechtsinstrumente – fragwürdig. Falls dieser Überprüfung nicht nachgekommen wird, ist es notwendig, die Verpflichtungen vieler Länder in Bezug auf die Prinzipien der Rechtsstaatlichkeit mit einem Fragezeichen zu versehen.

- Sperrsysteme müssen mittels nationaler Gesetzgebungen implementiert werden; andernfalls sollte man auf eine Implementierung verzichten. Sperrsysteme mit Selbstkontrolle besitzen inadäquate Transparenz und Nachweisbarkeit.