

Positionspapier des BVDW : „Sperrung“ kinderpornographischer Inhalte im Internet

Der Bundesverband Digitale Wirtschaft (BVDW) e.V. begrüßt die durch das Familien-, das Innen- und das Wirtschaftsministerium angestregte Initiative, wirksam und effektiv gegen die Verbreitung kinderpornographischer Inhalte im Internet vorzugehen, sehr. Problematisch allerdings ist nach Auffassung des BVDW dabei die Frage, wer wann und wie handelt.

Bis dato werden – aufgrund einer Initiative der Bundesfamilienministerin von der Leyen vom Dezember letzten Jahres - freiwillige Maßnahmen der Provider und/oder Vereinbarungen zwischen den beteiligten Zugangs Providern (Access-Provider), der Politik und den Strafverfolgungsbehörden diskutiert. Erklärtes Ziel ist es dabei, zunächst eine freiwillige Vereinbarung zwischen der Branche und der Politik zu erzielen, um dann im zweiten Schritt eine entsprechende - notwendige - gesetzliche Grundlage dafür zu schaffen.

Dieses Vorgehen muss aus mehreren Gründen als problematisch angesehen werden.

Rechtliche Bewertung

Der Bundesverband Digitale Wirtschaft (BVDW) e.V. hat im Januar 2009 ein umfangreiches [Rechtsgutachten zur Evaluierung des Haftungsregimes für Host- und Access-Provider](#) im Bereich der Telemedien vorgelegt, welches zu dem eindeutigen Ergebnis kommt, dass hoheitliche Sperrverfügungen aufgrund eines damit verbundenen rechtswidrigen Eingriffs in das Telekommunikationsgeheimnis grundsätzlich rechtlich unzulässig sind. Dies gilt auch für entsprechende Vereinbarungen zwischen Wirtschaft, Politik und Strafverfolgungsbehörden.

Dies begründet sich in den mit freiwilligen Sperrungen einhergehenden technischen Verfahren und deren rechtlicher Bewertung: technisch können Sperrungen von bestimmten Inhalten im World Wide Web über (a) die IP-Adresse, (b) den Domain Name Server (DNS), (c) über die Einrichtung eines Zwangs-Proxy-Servers oder aber (d) über hybride Systeme (z.B. Cleanfeed) erfolgen. Alle diese technischen Möglichkeiten verstoßen jedoch gegen Verfassungsrecht – insbesondere gegen den Schutz des Telekommunikationsgeheimnisses aus Artikel 10 Grundgesetz (GG) - und

sind damit gem. § 20 Abs. 1 und Abs. 4 JMStV i.V.m. § 59 Abs. 3 und Abs. 4 RStV nicht zulässig.

Denn: Art. 10 GG (Telekommunikationsgeheimnis) schützt das Vertrauen in die Fernkommunikation. Geschützt werden damit aber nicht nur die Inhalte, sondern auch die "Umstände" der Telekommunikation, d.h. auch ob, wann und wie oft zwischen wem Telekommunikation stattgefunden hat oder versucht wurde (vgl. auch § 88 TKG).

Sobald ein Internetnutzer über die Browserzeile eine Internetadresse eingibt (z.B. <http://www.spiegel.de>) stellt der Access-Provider technisch den Zugang zu der aufgerufenen Internetseite her. Um ihren Kunden die Möglichkeit einzuräumen, ihre Rechner mit dem Internet zu verbinden, betreiben Access-Provider die regelmäßig für das Weiterleiten (Routen) der IP-Pakete erforderlichen Router sowie DNS-Server zur Auflösung von DNS-Namen in für die Kommunikation im Internet erforderliche IP-Adressen. Wird also eine Internetadresse in die Browserzeile (z.B. www.spiegel.de) eingegeben und nutzerseitig versucht, eine Verbindung zu dieser Webseite herzustellen, dann löst der Access-Provider den eingegebenen Domainnamen über den DNS-Server in die entsprechende IP-Adresse der Seite (z.B. 195.71.11.67) auf. Dies ist ein automatischer Vorgang und für den Internetnutzer nicht erkennbar. Dennoch handelt es sich bei diesem Verfahren zweifelsfrei um einen „Umstand der Telekommunikation“, der ebenfalls dem Telekommunikationsgeheimnis unterliegt. Von den damit verbundenen Informationen, die hier verarbeitet werden und möglicherweise eine Gefahr begründen, haben Access-Provider aktuell grundsätzlich keine Kenntnis.

Soweit die Auffassung vertreten wird, DNS-Sperren stellen keinen Eingriff in das Telekommunikationsgeheimnis dar (vgl. Sieber, „[Sperrverfügungen im Internet](#)“), da der Betrieb eines DNS-Servers als „*eigenständige Funktion entsprechend einer Ebene oberhalb der Internetschicht zugeordnet wird ... und ... gesondert zu beurteilen ist*“, kann dies nicht überzeugen. Die Kommunikation zwischen dem Nutzer und der aufgerufenen Internetseite erfolgt stets über den DNS-Server, so dass dieses Vorgehen zwingend als „Umstand der Telekommunikation“ zu bewerten ist, der unter den Schutz des Artikel 10 GG fällt.

Vergegenwärtigt man sich zudem, dass das avisierte technische Verfahren, welches mit den gerade diskutierten „freiwilligen Sperren“ einhergehen soll, eben nicht auf den DNS-Server, sondern auf der Verwendung eines hybriden Modells aufsetzen soll, so erscheint dieses Vorgehen erst recht rechtlich nicht zulässig.

Hinzu kommt, dass auch das Zensurverbot (Art. 5 Abs. 1 S. 3 GG) und das Verbot der Vorzensur (s. Rechtsprechung des BVerfG) zu beachten sind.

Vor diesem Hintergrund erscheinen freiwillige Vereinbarungen in diesem Zusammenhang schon aus rechtlichen Gründen zweifelhaft.

Politische Bewertung

Sperrmaßnahmen der Provider – aufgrund hoheitlicher Sperrverfügungen oder aufgrund von Vereinbarungen dergestalt, wie sie aktuell diskutiert werden – greifen stets auch in Grundrechte ein. Im Zusammenhang mit der Sperrung kinderpornographischer Inhalte sind eine ganze Reihe – wichtiger - konfligierender Grundrechte - so etwa Art. 5, 10 und 12 GG - betroffen, so dass grundsätzlich sehr sorgsam vorgegangen werden sollte. Die einzelnen Grundrechte und ein möglicher Eingriff in diese müssen wohlbedacht gegeneinander abgewogen werden, nicht nur, um einer gerichtlichen Überprüfung standhalten zu können. Zudem sind auch gemeinschaftsrechtliche Vorgaben (u.a. eCommerce-Richtlinie, EU-Konsultationsverfahren) zu beachten.

Ein – sinnvolles - Vorgehen gegen die Verbreitung der bezeichneten Inhalte sollte daher zunächst auf einer klaren gesetzlichen Basis (Ermächtigungsgrundlage für den Grundrechte-Eingriff im Gesetz) erfolgen. Der vorgezogene Abschluss einer Vereinbarung unter Verweis darauf, dass die notwendige gesetzliche Grundlage dann zu einem späteren Zeitpunkt geschaffen werden soll/wird, ist sehr kritisch zu sehen.

Darüber hinaus sollte das – sorgsame und wohlbedachte – Vorgehen stets aufgrund eines rechtsstaatlichen und parlamentarischen Prozesses erfolgen. Zunächst wäre also ein ordentlicher Gesetzgebungsprozess unter Abwägung des gewünschten Ziels, der Schwere der Eingriffe in die betroffenen Grundrechte sowie der entsprechenden technischen Verfahren erforderlich. Nur auf Basis einer entsprechenden rechtsstaatlichen und demokratisch erzielten Grundlage könnte dann auch der Abschluss entsprechender Vereinbarungen zwischen den Zugangs Providern und der Politik erfolgen. Ein "Schnellschuss" einzelner Ministerien lässt befürchten, dass die oben bezeichneten Grundsätze nicht oder zumindest nicht ausreichend beachtet werden.

Die technischen Verfahren zur Sperrung von Inhalten müssen nach geltendem und auch ggf. zu schaffendem Recht zudem geeignet sein, die bezeichneten Inhalte isoliert zu sperren, um „Kollateralschäden“ – wie etwa im Zuge der „youporn-Sperrung“ geschehen - zu vermeiden. Darüber hinaus muss der individuelle Aufwand beim jeweiligen Provider für eine Sperrung im Verhältnis zu der mit ihr erzielten Wirkung stehen. Eine vollständige Sperrung, d.h. die Verhinderung der Erreichbarkeit eines rechtswidrigen Inhalts ist aufgrund der dezentralen Strukturen des Internets aktuell ohnehin schlicht unmöglich – allenfalls sind Zugangsbeschränkungen realisierbar, die sich jedoch mit einfachen Mitteln umgehen lassen.

Zudem sind weitere Fragen wie etwa der Umfang des technischen Aufwands sowie damit verbundene Kosten bislang nicht geklärt.

Daher wäre eine gesetzliche Neuregelung, die den Umfang bestimmt, in dem Access-Provider zu Eingriffen in das Telekommunikationsgeheimnis berechtigt sind, als erster Schritt notwendig und sinnvoll. Bestandteil dieser gesetzlichen Regelung sollte dann auch eine umfassende Freistellung von Haftungsansprüchen sowie eine ausdrückliche gesetzliche Regelung zur Kostenerstattung für Access-Provider sein. Erst im zweiten Schritt könnte dann eine freiwillige Sperrverpflichtung der Provider aufgrund einer möglichen Vereinbarung mit Politik und Strafverfolgungsbehörden unter genauer Festlegung der technischen und rechtlichen Verfahren sinnvoll sein.

Ein vorschnelles Handeln einzelner Ministerien, welches Gefahr läuft, der Vielzahl an rechtlichen, technischen und organisatorischen Fragen, die mit einer „Sperrung“ von Inhalten im Internet einhergehen und die im aktuellen Diskussionsprozess bislang weder ausreichend erörtert noch sachkundig beantwortet wurden, nicht gerecht zu werden, kann nicht gewünscht sein. Auch kann ein möglicherweise erzieltetes Ergebnis – eine Vereinbarung zwischen den Akteuren - dem letztlich das Scheitern vor den Gerichten prognostiziert werden kann, keine sinnvolle Handlungsoption sein. Hier wäre vielmehr ein umfassender demokratischer und gesellschaftlicher Willensbildungsprozess wünschenswert.

Berlin, den 10. Februar 2009

Gerd M. Fuchs
Justiziar / Referent Medienpolitik