

Bundesministerium für Familie, Senioren, Frauen und Jugend

Bundesministerium des Innern

Bundesministerium für Wirtschaft und Technologie

Berlin, den 19. Februar 2009

Betr.: Grundrechtliche, telekommunikations- und telemedienrechtliche Fragen im Zusammenhang mit der Sperrung kinderpornographischer Inhalte im Internet

Bezug: Sitzung der Arbeitsgruppe „Access Blocking“ am 13. Februar 2009 in Berlin

I. Eingriff in den Schutzbereich des Fernmeldegeheimnisses aus Art. 10 GG?

1. Grundsätzlich schützt Art. 10 GG nicht nur den Inhalt der Telekommunikation, sondern auch die näheren Umstände der Telekommunikation (BVerfGE 107, 299, 312, st. Rspr.). Dazu gehört insbesondere, ob, wann und wie oft zwischen welchen Personen oder Endeinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist. Daher kann grundsätzlich jede **staatliche Kenntnisnahme** von Daten, die einen Rückschluss auf eine von Art. 10 GG geschützte Telekommunikation zulässt, ein Eingriff in Art. 10 Abs. 1 GG darstellen.

Bei einer „Sperrung über das Domain Name System (DNS)“ kommt es zu folgendem Ablauf: Der Nutzer versucht den Abruf einer Webseite üblicherweise über die Eingabe eines Uniform Resource Locator (URL), der als Bestandteil immer einen Domainnamen aufweist. Er wird dann zu einem DNS-Server geleitet, der die zum Domainnamen gehörende IP-Adresse ausgibt, unter der die Webseite letztlich abrufbar ist. Das DNS ist insoweit lediglich

eine Vereinfachung für den Nutzer, der sich die Eingabe der wesentlich komplizierteren Ziffernfolge der IP-Adresse erspart. Der DNS-Server meldet bei einer DNS-Sperrung keine IP-Adresse sondern i.d.R. einen Fehler. Infolgedessen kann keine Verbindung zur Webseite hergestellt werden und der Browser (=Computerprogramm beim Nutzer zum Betrachten von Webseiten im Netz) meldet den Fehler an den Nutzer zurück. Das heißt, es kommt gar nicht erst zu einem Aufruf einer Internet-Seite oder einem Verbindungsversuch. Die „Sperrung über das Domain-System“ spielt sich also noch im Bereich des Nutzers ab, es ist noch gar nicht zum Versuch eines Verbindungsaufbaus oder einer Kommunikation gekommen. Der Schutzbereich des Fernmeldegeheimnisses, das ja die Verbindung an sich, und dabei sowohl den Inhalt als auch die näheren Umstände einer Verbindung schützt, ist dementsprechend nicht berührt, da es noch gar keine schützenswerte Verbindung oder einen entsprechenden Versuch gibt. Der DNS-Server fungiert bei der Eingabe einer bestimmten Adresse (also zum Beispiel www.bundesregierung.de) als Telefonbuch, also sozusagen als vorgelagerte Anlaufstelle, die den Aufruf einer Seite im Internet erst ermöglichen soll. Der DNS-Server unterfällt somit nicht dem Schutzbereich des Art. 10 GG (ähnlich *Sieber/Nolde*, Sperrverfügungen im Internet, Freiburg 2008, S. 85; weil die dort betroffenen Kommunikationspartner nicht in den Schutzbereich des Art. 10 GG einbezogen sind).

Selbst wenn man annehmen würde, dass der Schutzbereich eröffnet ist, würde es an einem Eingriff fehlen. Dabei ist zu beachten, dass sich die Schutzwirkung von Artikel 10 GG zwar grundsätzlich auf den gesamten Prozess der Informations- und Datenverarbeitung erstreckt. Artikel 10 GG kann seine Schutzwirkungen daher schon in einem frühen Stadium des technischen Übertragungsvorgangs entfalten. Nicht erst die staatliche Kenntnisnahme vom Inhalt der Kommunikation oder Kommunikationsumstände kann einen Eingriff in das Grundrecht darstellen, sondern schon die Erfassung der Daten selbst (BVerfGE 100, 313, 366). Auch jeder weitere Datenverarbeitungsprozess, der sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließt und in dem Gebrauch von den erlangten Kenntnissen gemacht wird, stellt ferner einen eigenständigen Eingriff

in das durch Artikel 10 GG geschützte Grundrecht dar (BVerfGE 100, 313, 359; 110, 33, 68f.; 113, 348, 365).

Eine Ausnahme hiervon ist aber anzunehmen, wenn Telekommunikationsvorgänge **ungezielt und allein technikbedingt zunächst miterfasst, aber unmittelbar nach der Signalaufbereitung technisch wieder spurenlos ausgesondert werden** (BVerfGE 100, 313, 366; 107, 299, 328; ähnlich zur Erfassung von durch Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG geschützten Daten: BVerfGE 115, 320, 343f – Rasterfahndung; BVerfG Urteil vom 11. März 2008, Rn. 68 – Automatisierte Kennzeichenerfassung; ebenso Landesverfassungsgericht Mecklenburg-Vorpommern Urteil vom 27. November 2008, NordÖR 2009, 20, 21). Das Bundesverfassungsgericht hat damit für bestimmte Fallgestaltungen anerkannt, dass es hinsichtlich solcher Datenverarbeitungsvorgänge an einem Grundrechtseingriff fehlt.

Auf die Frage eines Eingriffs in Artikel 10 GG übertragen, bedeutet dies, dass hinsichtlich solcher Daten, bei denen ein Individualkommunikationsbezug gegeben ist, derartige Daten lediglich kurzzeitig automatisiert erfasst, als „Nichttreffer“ indes aber nicht weiter verarbeitet, sondern im normalen Geschäftsablauf verbleiben, beziehungsweise wieder gelöscht werden. Die Sperrtechnik auf DNS-Basis erfordert keine Erhebung von Daten, die nicht ohnehin beim Geschäftsbetrieb der Zugangsanbieter anfallen.

In der bloßen **Verhinderung des Zugangs** zu einer bestimmten Information, etwa der Seite mit kinderpornographischem Inhalt, liegt nach einhelliger Auffassung ohnehin kein Eingriff in Art. 10 Abs. 1 GG (*Jarass*, in: *Jarass/Pieroth*, GG, Art. 10, Rn. 12 m.w.N.; *Degen*, *Freiwillige Selbstkontrolle der Access-Provider*, Stuttgart 2007, 289, der aus dem Grunde generell einen Eingriff in Art. 10 GG verneint).

2. Darüber hinaus ist festzustellen, dass, sofern es zu einer Sperrung auf der Grundlage eines öffentlich-rechtlichen Vertrages zwischen dem Zugangsanbieter und dem Bundeskriminalamt kommt, es bereits an einem **hoheitlichen Eingriff** fehlt. Ein Eingriff in das Fernmeldegeheimnis liegt nur dann

vor, wenn sich **staatliche Stellen ohne Zustimmung der Beteiligten Kenntnis von dem Inhalt oder den Umständen eines fernmeldetechnisch vermittelten Kommunikationsvorgangs verschaffen, die so erlangten Informationen speichern, verwerten oder weitergeben** (*Hermes*, in: *Dreier*, GG, Art. 10, Rn. 53). Es muss sich um eine Kenntnisnahme durch den **Staat** handeln (vgl. BVerfGE 113, 348, 364; 106, 28, 37; 100, 313, 366; 85, 386, 398; *Bizer*, in: AK GG, Art. 10, Rn. 69a). Ein solcher Eingriff liegt erkennbar nicht vor.

Allenfalls wäre daran zu denken, in der Durchführung einer Sperrmaßnahme auf der Grundlage eines öffentlich-rechtlichen Vertrages mit dem Bundeskriminalamt einen **mittelbaren Eingriff** zu sehen. Während der herkömmliche Grundrechtseingriff in imperativer Form, also durch Gesetz, Verordnung, Satzung oder Verwaltungsakt, erfolgt, ist der Begriff des mittelbaren Grundrechtseingriffs weitgehend unscharf. Einigkeit dürfte aber darin bestehen, dass zwar auch faktische oder mittelbare Grundrechtseingriffe möglich sind (vgl. BVerfGE 105, 252, 273), für die Annahme eines solchen Eingriffs allerdings besondere Voraussetzungen zu fordern sind, da letztlich jegliches staatliches Handeln Auswirkungen auf grundrechtlich geschützte Positionen haben kann. Ein mittelbarer Eingriff kann daher nur angenommen werden, wenn die beanstandete Maßnahme die belastenden Wirkung bezweckt (BVerwGE 71, 183, 193f; 90 112, 121f) oder eine besondere Schwere der Belastung vorliegt (*Jarass*, in: *Jarass/Pieroth*, GG, Vorb. vor Art. 1, Rn. 29). Ferner kann von Bedeutung sein, ob die Beeinträchtigung Ausdruck der Gefahr ist, vor der das betreffende Grundrecht schützen soll (BVerwGE 71, 183, 192).

Nach diesen Anforderungen wäre in dem Abschluss eines öffentlich-rechtlichen Vertrages durch das Bundeskriminalamt auch kein mittelbarer Eingriff in Art. 10 GG zu sehen, unabhängig von der Frage, ob der Schutzbereich überhaupt betroffen ist (s. oben I.). Eine besondere Schwere kann dem Eingriff nicht attestiert werden, insbesondere nicht im Hinblick auf die „Nicht-Trefferfälle“. Zudem gilt es zu bedenken, dass ein (nach der hier vertretenen Auffassung abzulehnender) Eingriff in das Fernmeldegeheimnis der Kunden

erst eine Folgewirkung des öffentlich-rechtlichen Vertrages wäre, nicht aber unmittelbar Vertragsgegenstand (vgl. § 2 Abs. 1 des Entwurfs, wonach etwaig notwendige Änderungen der Allgemeinen Geschäftsbedingungen erst noch vorzunehmen sind (vgl. *Frenz*, Selbstverpflichtungen der Wirtschaft, Tübingen 2001, S. 275ff).

Davon zu trennen ist die Frage, ob hier nicht die **objektiv-rechtliche Schutzwirkung des Artikels 10 GG** verletzt sein könnte. Artikel 10 GG enthält insoweit einen Schutzauftrag an den Staat, auch Eingriffen Dritter in das Fernmeldegeheimnis entgegenzutreten. Einfachgesetzlich hat dies seinen Niederschlag in der Regelung des **§ 88 Absatz 1 des Telekommunikationsgesetzes** gefunden (BVerfGE 106, 28, 34), der in seinem Anwendungsbereich der Rechtsprechung des Bundesverfassungsgerichts zum Fernmeldegeheimnis entspricht (*Schmidt*, in: *Umbach/Clemens*, GG, Art. 10, Rn. 69).

Unter anderem deswegen ergänzt § 88 TKG den Schutz des Fernmeldegeheimnisses in Art. 10 GG. Während sich Art. 10 GG gegen staatliche Eingriffe in die Telekommunikation richtet, wendet sich § 88 TKG an die privaten Erbringer von Telekommunikationsdiensten. Dies wurde im Zuge der Privatisierung der Telekommunikation erforderlich, als die privaten Anbieter von Telekommunikation aus dem Anwendungsbereich des Art. 10 GG herausfielen. Die Geltung des Fernmeldegeheimnisses für die privaten Diensteanbieter wird nunmehr durch § 88 TKG festgeschrieben.

Für einen Eingriff in das Fernmeldegeheimnis aus § 88 TKG durch den Einsatz einer DNS-Sperre gilt entsprechend schon das zu Art. 10 GG Ausgeführte. Zu beachten ist hier allerdings, dass bei dieser Prüfung zusätzlich berücksichtigt werden muss, welche Daten der jeweilige Diensteanbieter im Rahmen seiner Dienstleistung benötigt. § 88 Abs. 3 TKG erlaubt die Verwendung von Kenntnissen überhaupt nur, wenn diese Kenntnisse bereits für die geschäftsmäßige Erbringung angefallen sind. Der Diensteanbieter darf sich also nicht Kenntnis von Daten verschaffen, die er für die Erbringung

seiner Dienste gar nicht braucht. Dies ergibt sich bei einer Sperrung über das Domain System aber nicht.

Nach alledem ist in der Sperrung über das Domain System kein Eingriff in Art. 10 GG bzw. § 88 TKG zu sehen.

II. Verfassungs-, telekommunikations- und telemedienrechtliche Beurteilung des Betriebs einer STOPP-Seite

1. Auch die Weiterleitung einer Anfrage auf eine bei dem Diensteanbieter geführte STOPP-Seite stellt keinen Eingriff in das Fernmeldegeheimnis dar, und zwar weder aus Art. 10 GG noch aus § 88 TKG.

Bei der Weiterleitung auf eine bei dem Diensteanbieter geführte STOPP-Seite kommt es zwar anders als bei der bloßen Sperre über das Domain-System zum Aufbau einer Verbindung, da der Nutzer ja eine Internet-Seite aufruft. Der Schutzbereich des § 88 TKG dürfte also eröffnet sein. Der Zugangsvermittler ermöglicht einen Telekommunikationsvorgang, den er allerdings „manipuliert“, in dem er die Zieleingabe verändert. Der Server des Diensteanbieters, auf dem die STOPP-Seite gespeichert ist, übermittelt diese genau wie beim Aufruf anderer Internet-Seiten auch über den Internet-Zugang des Zugangsvermittlers an die IP-Adresse des Nutzers.

Es liegt aber kein Eingriff in den Schutzbereich vor, da die Frage, ob der Nutzer die Internet-Seite aufrufen konnte, die er dem DNS-Server genannt hat, sich nicht nach Maßgabe des Fernmeldegeheimnisses beurteilt. Dieses schützt die Verbindung an sich, nicht aber eine Verbindung zu einem bestimmten Ziel.

Wird die STOPP-Seite vom Diensteanbieter betrieben, erhält auch niemand, der sonst keine Kenntnis von den Daten des Nutzers hätte, Kenntnis derselben.

Die Weiterleitung auf eine vom Diensteanbieter betriebene STOPP-Seite stellt daher keinen Eingriff in Art. 10 GG bzw. § 88 TKG dar.

2. Die „Stopp“-Seite selbst ist ein Telemedienangebot. Sie unterliegt den datenschutzrechtlichen Anforderungen des TMG. Der Webserver, auf dem die „Stopp“-Seite gespeichert ist, speichert kurzfristig für die Zeit der technischen Bearbeitung die IP-Adresse des Nutzers, um die Daten der Seite an diese Adresse übermitteln zu können.

Sämtliche Daten, die auf dem Webserver der „Stopp“-Seite ankommen und dort gespeichert werden, sind Nutzungsdaten im Sinne des TMG (§ 15). Der Diensteanbieter darf diese Daten verarbeiten, soweit dies erforderlich ist, um die Inanspruchnahme der „Stopp“-Seite zu ermöglichen. Das ist in jedem Fall die IP-Adresse des Nutzers. Nach Übermittlung der Webseite entfällt dieser Zweck und die Daten sind unverzüglich zu löschen. Dies muss der Diensteanbieter durch technische und organisatorische Vorkehrungen gewährleisten (Systemdatenschutz, § 13 Abs. 4 TMG). Zum notwendigen Systemdatenschutz gehört u. a. auch, dass der Nutzer die „Stopp“-Seite gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann.

Denkbar ist, dass auf der „Stopp“-Seite ein Zähler eingerichtet wird, der die Abrufe der „Stopp“-Seite rein zahlenmäßig registriert. Diese Zahlen enthalten keinerlei Personenbezug und sind daher datenschutzrechtlich irrelevant. Sie könnten nach hiesiger Einschätzung ohne weiteres beliebig verwendet werden, d. h. auch an das BKA für statistische Zwecke übermittelt werden.

Wird die STOPP-Seite vom Diensteanbieter betrieben erhält auch niemand, der sonst keine Kenntnis von den Daten des Nutzers hätte, Kenntnis derselben.