B M I - R e f e r a t V I 3

Berlin, den 17. Februar 2009

V I 3 -

Hausruf: 45532

L:\Grundrechte\Grundrechtliche Einzelfragen\Innere Sicherheit\Sperrverfügungen\09-02-17 V I 3 Prüfauftrag Sperrung Internetseiten.doc

Referat ÖS I 3

Abdruck

Betr.: Sperrungen von Internetseiten mit kinderpornographischem Inhalt

Zu den mir übermittelten Fragen nehme ich wie folgt Stellung:

I. Bei welcher Sperrtechnik ist der Schutzbereich des Fernmeldegeheimnisses aus Art. 10 GG berührt?

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.

   Nach einer im Schrifttum vertretenen Auffassung greifen **hoheitlich angeordnete Sperrverfügungen**, die sich bestimmter Sperrtechnologien bedienen, daher in das Fernmeldegeheimnis der Nutzer aus Art. 10 Abs. 1 GG ein, **soweit sie die vom Nutzer übermittelten IP-Adressen, Port-Nummern und URIs analysieren** (vgl. etwa *Sieber/Nolde*, Sperrverfügungen im Internet, Freiburg 2008, S. 79ff; noch weitergehend *Frey/Rudolph*, Rechtsgutachten zur Evaluierung des Haftungsregimes für Host- und Access-Provider im Bereich der Telemedien, 2008; eine Berufung der Access-Provider auf Art. 10 GG scheidet aus, vgl. *Billmeier*, Die Düsseldorfer Sperrungsverfügung, Berlin 2007, S. 185, da die für die Übermittlung der

Kommunikation genutzte Übermittlungseinrichtung nicht Träger des Grundrechts aus Art. 10 GG ist, *Jarass*, in: *Jarass/Pieroth*, GG, Art. 10, Rn. 10[1]). In der bisherigen Rechtsprechung zu Sperrverfügungen ist ein Eingriff in Art. 10 Abs. 1 GG dagegen bisher nicht angenommen worden; noch nicht einmal ansatzweise diskutiert worden, obgleich dort die Wahl der jeweiligen Sperrtechnik in das Belieben der Zugangsanbieter gestellt worden war.

Aus hiesiger Sicht berührt keine der derzeit diskutierten Sperrtechnologien den Schutzbereich des Fernmeldegeheimnisses aus Art. 10 GG. Während dies für das Sperrkriterium **„Sperrung über das Domain System (DNS)"** zum Teil anerkannt wird (*Sieber/Nolde*, Sperrverfügungen im Internet, Freiburg 2008, S. 85; dagegen *Frey/Rudolph*, Rechtsgutachten zur Evaluierung des Haftungsregimes für Host- und Access-Provider im Bereich der Telemedien, 2008, Rn. 168), weil die dort betroffenen Kommunikationspartner nicht in den Schutzbereich des Art. 10 GG einbezogen sind, gilt dies nach hiesiger Einschätzung auch für die beiden anderen Sperrtechniken **„Sperrung der Internet-Adresse (IP-Adresse)"** und **„Sperrung über den Uniform Ressource Identifier (URI)"**.

2. Folgende Argumente sprechen dafür, den Schutzbereich des Artikels 10 GG bei keiner der oben aufgeführten Sperrtechniken anzunehmen:

- Zum einen bedarf der Schutzbereich des Fernmeldegeheimnisses für den Bereich des Internet einer differenzierten Betrachtung. Während für den Bereich der über die Dienste des Internet geführten **Individualkommunikation** weitgehend unstreitig der Schutzbereich des Art. 10 GG einschlägig ist (vgl. für die Überwachung eines Voice over IP-Gesprächs BVerfG Urteil vom 27. Februar 2008, Rn. 190; a.A. aber offenbar *Pagenkopf*, in: *Sachs*, GG, Art. 10, Rn. 14 m.w.N.), ist dies für den Fall der **Massekommunikation im Internet**, wie etwa den Aufruf einer Website mit allgemein zugänglichen Informationen, unklar. In derartigen Fällen fehlt es an einer Individualkommunikation zwischen zwei (oder mehreren) Personen, es kommt lediglich zu einem Abruf von an die Allgemeinheit gerichteten Inhalten.

[1] Soweit nicht anders angegeben beziehen sich die Angaben zu Kommentaren auf die jeweils neueste

Zum Teil wird vertreten, auf die Differenzierung von Individual- und Massenkommunikation für den Bereich des Internet vollständig zu verzichten, da der Staat anderenfalls erst unter Umständen in Art.10 GG eingreifen müsste, um festzustellen, ob dieser einschlägig ist (*Sieber/Nolde*, Sperrverfügungen im Internet, Freiburg 2008, S. 80f; *Schmidt*, in: *Umbach/Clemens*, GG, Art. 10, Rn. 43a).

Aus hiesiger Sicht sollte indes an der grundsätzlichen Unterscheidung zwischen Individual- und Massenkommunikation auch für den Bereich des Internet festgehalten werden (ebenso *Löwer*, in: *von Münch/Kunig*, GG, Art. 10, Rn. 18; *Groß*, in: *Friauf/Höfling*, GG, Art. 10, Rn. 10, Rn. 19; *Pagenkopf*, in: *Sachs*, GG, Art. 10, Rn. 14a; *Stern*, Staatsrecht, IV, München 2006, S. 228; *Badura*, in: BK, GG, Art. 10 fordert einen „individuellen Kommunikationsvorgang"). Dem Schutz des Fernmeldegeheimnisses unterfällt nicht das World Wide Web an sich, sondern nur bestimmte Formen der Kommunikation darin (vgl. *Gusy*, in: von *Mangoldt/Klein/Starck*, GG, Art. 10, Rn. 43). Auch das Bundesverfassungsgericht hat in seinem Urteil vom 27. Februar 2008 ausgeführt: „*Die Gewährleistung des Telekommunikationsgeheimnisses nach Art. 10 Abs. 1 GG schützt die unkörperliche Übermittlung von Informationen an* ***individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs***", Rn. 182, Hervorhebung durch den Unterzeichner). Das Bundesverfassungsgericht hat im Zusammenhang mit Artikel 10 GG regelmäßig den Personenbezug hervorgehoben (BVerfGE 113, 348, 365: „*In den Schutzbereich fällt auch die Erlangung der Kenntnis, ob, wann, wie oft und* ***zwischen welchen Personen*** *Telekommunikation stattgefunden hat oder versucht worden ist.*"; vgl. BVerfGE 67, 157, 172; 85, 386, 396; 100, 313, 358; 107, 299, 312f und im Hinblick auf den Einsatz eines IMSI-Catchers BVerfG Beschluss vom 22. August 2006). Es ist daher abzulehnen, dass Fernmeldegeheimnis auf alle telekommunikationstechnischen Übertragungswege (und damit das Internet insgesamt) zu erstrecken, nur weil hierauf möglicherweise individuelle Kommunikationswege abgewickelt werden können. Wegen des engen Bezugs des Grundrechts zum allgemeinen Persönlichkeitsrecht, sollte auch für den Bereich des Internets vielmehr daran festgehalten werden, dass Kommunikationsprozesse, die dem Bereich der Massenkommunikation,

---

Auflage.

wie etwa der Abruf von öffentlich zugänglichen Webseiten, nicht unter den Schutzbereich des Art. 10 GG fallen.

Auch das Argument, es würde anderenfalls unter Umständen in den Schutzbereich eingegriffen, um festzustellen, ob dieser betroffen ist, verfängt nicht. Das Bundesverfassungsgericht selbst unterscheidet in der Frage, ob Daten (noch) von Art. 10 Abs. 1 GG geschützt sind, danach, ob der Kommunikationsvorgang abgeschlossen ist (BVerfGE 115, 166ff). Eine solche Feststellung wird sich aber oftmals erst nach einem Zugriff auf diese Daten feststellen lassen. Gleichwohl hat das Bundesverfassungsgericht davon abgesehen, diese Daten insgesamt und pauschal dem Schutz des Art. 10 Abs. 1 GG zu unterstellen. Auch hat es im Hinblick auf den Schutz des Kernbereichs der persönlichen Lebensgestaltung das Argument, es bedürfe, um festzustellen, ob dieser betroffen sei, bereits eines Eingriffs in diesen, gleichwohl davon abgesehen, die Maßnahmen der Wohnraumüberwachung insgesamt als unzulässig anzusehen (BVerfGE 109, 279ff, so aber ausdrücklich das Sondervotum der Richterinnen *Jaeger* und *Hohmann-Dennhardt* in BVerfGE 109, 382, 383).

Grundsätzlich ist daher auch für den Bereich des Internet zwischen Individual- und Massenkommunikation zu trennen. In Fällen der Massenkommunikation dürfte es aber an dem speziellen Schutzbedürfnis für die Vertraulichkeit solcher Kommunikation fehlen (dies zugestehend *Sieber/Nolde*, Sperrverfügungen im Internet, Freiburg 2008, S. 80). Nur wo eine Unterscheidung technisch überhaupt nicht möglich ist, könnte auf dieses Differenzierungskriterium verzichtet werden (ebenso *Löwer*, in: *von Münch/Kunig*, GG, Art. 10, Rn. 18). Es besteht indes kein Grund zur Annahme, dass dies der Fall ist.

Die Sperrtechniken sollen den Aufruf bestimmter öffentlich zugänglicher Webseiten mit kinderpornographischem Inhalt verhindern. Sie knüpfen damit nicht an einen von dem Nutzer ausgehenden Akt individueller Kommunikation und an einen Nachrichtenaustausch zwischen zwei Personen an, so dass für diese Fälle in Rahmen hoheitlicher Sperrverfügungen (s. dazu unter Ziffer 2) aus hiesiger Sicht der Schutz des Fernmeldegeheimnisses aus Art. 10 GG nicht einschlägig wäre. Die Verwendung der Daten des Abrufs solcher Seiten (sozusagen der „Trefferfall") unterfällt nicht dem Schutzbereich des Artikel 10 GG.

- Soweit es für die Durchführung der Sperrung bei einzelnen Sperrtechniken auch zur Verarbeitung von grundsätzlich dem Fernmeldegeheimnis aus Artikel 10 GG unterliegenden Daten aus individuellen Kommunikationsvorgängen kommt, etwa wie der Nutzung eines E-Mail-Dienstes über das World Wide Web (an sich „Nicht-Trefferfälle", da nur der Zugang zu öffentlich zugänglichen Webseiten gesperrt werden soll), stellt sich im Hinblick auf diese Daten die **Frage der Eingriffsqualität**. 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 Übertragungsvorgangsentfalten. 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 Eingriff in Artikel 10 GG durch bestimmte Sperrtechniken übertragen bedeut dies, dass hinsichtlich von solchen 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. Keine der Sperrtechniken erfordert eine Erhebung von Daten, die nicht ohnehin beim Geschäftsbetrieb der Zugangsanbieter anfallen. [Das könnte BKA uU noch näher ausführen. Auch wäre eine eindeutige Aussage darüber, welche Daten im einzelnen durch wen verarbeitet werden, wenn die Zugangsvermittlung durchgeführt werden. Die Aussage der DT AG war hier war unklar. Handelt es sich um Verkehrsdaten oder Nutungsdaten nach dem TMG? Welche Rechtsvorschriften erlauben bereits jetzt eine Erhebung und Nutzung der Daten?]

- 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).

Nach alledem ist durch keine aufgrund einer hoheitlichen Maßnahme genutzten Sperrtechniken ein Eingriff in Art. 10 GG zu sehen.

II. Entfällt ein Eingriff in das Fernmeldegeheimnis aus Art. 10 GG, wenn eine Zustimmung des Kunden vorliegt?

1. Unabhängig von der Frage, ob und durch welche der möglichen Sperrtechnologien der Schutzbereich des Art. 10 GG berührt wird, 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 ich 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.

2. 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 ist weitgehend unscharf. Einigkeit dürfte aber darin bestehen, 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 vertreten 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). [Frage an ÖS I 3: Ist § 58 VwVfG problematisiert worden? Sollen wir uns hierzu lieber verschweigen?

Frenz, Selbstverpflichtungen der Wirtschaft, Tübingen 2001, S. 211 lehnt deshalb auch § 58 VwVfG für solche Fälle ab.]

3. 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). [Hier wäre der Beitrag des BMWi einzusetzen, der, wenn man konsequent sein will, den Umfang des Schutzes aus Art. 88 TKG an den obigen Ausführungen orientieren müsste.]

4. Nähme man gleichwohl einen staatlichen Eingriff in Artikel 10 GG an, könnte dieser durch eine **Einwilligung des Kunden** wieder entfallen. Der Schutz des Fernmeldegeheimnis ist verzichtbar (*Schmidt*, in: *Umbach/Clemens*, GG, Art. 10, Rn. 71a m.w.N.). Liegt eine Einwilligung in die Verletzung des Fernmeldegeheimnisses durch staatliche Stellen vor, entfällt daher die Annahme eines Eingriffs in Art. 10 GG (vgl. BVerfGE 85, 386, 398; BVerwG Beschluss vom 10. August 1981, NJW 1982, 840; *Groß*, in: *Friauf/Höfling*, GG, Art. 10, Rn. 10, Rn. 30; *Löwer*, in: *von Münch/Kunig*, GG, Art. 10, Rn. 7, wobei die hier nicht weiter relevante Frage streitig ist, ob hierfür die Zustimmung eines der Kommunikationsteilnehmer ausreicht). Voraussetzung ist allerdings, dass die Einwilligung ausreichend konkret sein muss (*Jarass*, in: *Jarass/Pieroth*, GG, Vorb. vor Art. 1, Rn. 36, sie kann grundsätzlich konkludent erteilt werden, vgl. BVerfGE 106, 28, 44f; BVerfG Beschluss vom 2. April 2003, NJW 2003, 2375) und freiwillig erfolgt (*Dreier*, in: *Dreier*, GG; Vorb., Rn. 131). Letzteres dürfte dann nicht vorliegen, wenn eine Täuschung, Drohung oder Zwang ausgeübt wird (*Sachs*, in: *Sachs*, GG, Vor Art. 1, Rn. 56).

   Eine ausdrückliche Regelung in den Allgemeinen Geschäftsbedingungen dürfte den an eine Einwilligung zu stellenden Anforderungen gerecht werden, wobei es indes nach der hier vertretenen Auffassung nicht darauf ankommt, da es bereits an einem Eingriff in Art. 10 GG fehlt.

III. Wie wäre der Betrieb einer STOP-Seite beim BKA (verfassungs)rechtlich zu beurteilen?

1. Beim Versuch des Abrufs einer gesperrten Seite soll diese Anfrage an das Bundeskriminalamt weitergeleitet werden und dem Nutzer von dort dann eine STOP-Seite übermittelt werden. Dabei dürfte es wohl zumindest zu einer Weiterleitung der IP-Adresse des anfragenden Rechners kommen.

   Nach den obigen Ausführungen werden derartige Weiterleitungen nur in Fällen der Massenkommunikation, nämlich des Abrufs einer Webseite kommen, erfolgen, die nicht dem Schutz des Artikel 10 GG unterfallen. Selbst im Fall einer hoheitlich angeordneten Sperrverfügung und gesetzlich verankerten Pflicht zur Weiterleitung der Anfrage an das Bundeskriminalamt wäre dies nach hiesiger Auffassung kein Eingriff in Art. 10 GG (s. unter I.).

2. Bei der Angabe der IP-Adresse des anfragenden Rechners dürfte es sich indes um personenbezogenes Datum handeln, dass dem Schutz des Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG unterfällt. Auch wenn ein Eingriff mangels hoheitlichen Handelns beziehungsweise aufgrund der Einwilligung des Nutzers zu verneinen ist (s. unter I.), dürfte für eine solche Weitergabe eine einfachgesetzliche Regelung erforderlich sein. Dabei dürfte zu beachten sein, dass bereits heute Zugangsprovider bei technischen Schwierigkeiten mit dem Abruf einer bestimmten Webseite Seiten mit einem entsprechenden Hinweis anzeigen. [Hier müsste noch der Beitrag des BMWi eingefügt werden.]

Dr. Stawowy