Mark Bedner

Rechtmäßigkeit der „Deep Packet Inspection“

Projektgruppe verfassungsverträgliche Technikgestaltung (provet)

Universität Kassel

2009

CASED

ITeG

Ass. iur. Mark Bedner, LL.M.[1]

RECHTMÄßIGKEIT DER „DEEP PACKET INSPECTION“

1 EINLEITUNG

„Deep Packet Inspection“ (DPI), die „tief gehende Paketanalyse“, ist eine Technologie, die es den Internetprovidern[2] erlaubt übertragene Internetpakete in Echtzeit näher zu untersuchen, sprich „tiefer hineinzuschauen“ welche konkreten Inhalte über ihre Infrastruktur übertragen werden und diese Inhalte in gewissen Fällen ebenso in Echtzeit zu manipulieren.

In den Medien[3] und Fachzeitschriften[4] wird das Thema derzeit noch relativ selten erwähnt und nur sporadisch im Zusammenhang mit der sogenannten „Netzneutralität“ beiläufig angesprochen. Dabei hat die DPI das Potential das Internet, wie man es bisher kennt und dessen künftige Nutzung, nicht unbedingt zum Positiven neu zu ordnen. Umso wichtiger ist es daher, dass frühzeitig auf die sich daraus ergebenden Gefahren hingewiesen wird. Je früher der Allgemeinheit bewusst wird, welche Gefahren drohen oder bereits bestehen, umso eher werden technische und juristische Lösungen entwickelt, um das von der DPI ausgehende Gefahrenpotential zu reduzieren.

---

[1] Der Autor ist Stipendiat des CASED (Center for Advanced Security Research Darmstadt) und Mitarbeiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel. Er bedankt sich bei den beiden CASED-Mitarbeitern Dipl.-Wirtsch.-Inform. Tobias *Ackermann* und Dipl.-Ing. Sascha *Mühlbach* für die hilfreichen Hinweise zum technischen Teil sowie bei Dipl.-Pol. Ralf *Bendrath*, der eine rechtliche Betrachtung der DPI im Blog netzpolitik.org vorschlug.

[2] Access- und Networkprovider; nachfolgend als „Provider“ bezeichnet.

[3] Sir Tim *Berners-Lee* warnte schon frühzeitig vor den Gefahren der DPI; siehe dazu http://news.zdnet.co.uk/security/0,1000000189,39625971,00.htm; http://www.w3.org/DesignIssues/NoSnooping.html; ansonsten wurde das Thema mehrfach von Ralf *Bendrath* aufgegriffen; siehe zum Beispiel den Nachweis in Fußnote 1 oder seinen Vortrag auf der SIGINT 2009, abrufbar unter http://events.ccc.de/sigint/2009/Fahrplan/attachments/1304_Bendrath-DPI.pdf; einige Erwähnungen der DPI gab es auch im Rahmen der Berichterstattung zu den Aufständen im Iran und der dort staatlicherseits eingesetzten Überwachung des Internets; siehe dazu auch die weiteren Nachweise in den Fußnoten 10, 62 und 63.

[4] Beispielsweise *Spies*, MMR 2008, XII ff, der die Lage in den USA insbesondere unter dem Blickwinkel der personalisierten Werbung darstellt.

Die DPI-Technologie gibt den Providern vielfältige Möglichkeiten auf die übertragenen Daten einzuwirken. Die Spanne reicht von heimlich[5] durchgeführten Echtzeitanalysen bis hin zu inhaltlichen Manipulationen, wobei Letzteres teilweise mit dem Begriff „Deep Packet Modification" umschrieben wird. Die Provider können die Daten in Echtzeit verändern, umleiten oder ganz unterdrücken. Außerdem besteht die Möglichkeit die Daten parallel zur Übertragung von und zum Kunden auch beim Provider zu speichern. Bildlich lässt sich das Verfahren durch einen Vergleich mit der Briefpost verdeutlichen. Kernaufgabe eines Providers ist das direkte Zustellen der ungeöffneten Briefe anhand der Adressen auf dem Briefumschlag. Die Anwendung von DPI bedeutet aber, dass alle Briefe geöffnet werden und diese gelesen werden. Abhängig vom Inhalt wird die Zustellung künstlich verlangsamt, Inhalte mit Zusätzen (meist Werbung) versehen, handschriftliche Texte in Schreibmaschinentext umgewandelt, einige Briefe inhaltlich verkürzt ausgeliefert, andere vernichtet und alle oder ein bestimmter Teil davon als Kopie aufbewahrt.

Die Gründe für den Einsatz von DPI-Verfahren sind vielfältig. Ursprünglich wurde DPI entwickelt, um die Netzwerksicherheit zu gewährleisten. Ein weiterer derzeit verstärkt aufkommender Grund ist die Priorisierung von bestimmten Inhalten (Stichworte sind „Netzwerkmanagement", „Traffic Shaping" oder „Quality of Service"), was dem oben erwähnten Bereich der „Netzneutralität" zuzuordnen ist. Die bevorzugte und damit vergleichsweise schnellere Übertragung von gewissen Inhalten würden sich die Provider zum einen zusätzlich vergüten lassen und zum anderen die finanziellen Aufwendungen für den dann eigentlich notwendigen Bandbreitenausbau ersparen. Hinsichtlich der Priorisierung besteht im Vergleich zur Briefpost jedoch ein wesentlicher Unterschied. Während die Post Expressdienste bereit hält, ohne hierfür die reguläre Zustellung verlangsamen zu müssen, kann ein Provider zwar Pakete bevorzugt behandeln, jedoch erfolgt dies immer zu Lasten anderer Pakete, die dementsprechend verlangsamt übertragen werden müssen, soweit die vorhandene Bandbreite bereits vollständig ausgenutzt ist. Die gezielte Drosselung von gewissen Paketen ist folglich bei einer vollständigen Auslastung der Bandbreite zwingende Voraussetzung, um andere „schneller" übertragen zu können. Daneben kann der Provider unabhängig von einer Überlastung der Leitungen gewisse Pakete gezielt limitieren, so dass die vorhandene Leitungskapazität nicht ausgelastet wird. Ohne Eingriffe sind alle Pakete mit maximaler Geschwindigkeit unterwegs. Eine diskriminierungsfreie Beschleunigung der Übermittlung ist nur durch einen Bandbreitenausbau möglich.

Ein weiterer Grund für den Einsatz von DPI sind Werbeeinnahmen. So integrieren Provider oder beauftragte Drittfirmen[6] personalisierte und damit zielgerichtete Werbung in fremde Webseiten, die den Vorlieben und Interessen des Nutzers möglichst genau entspricht (sogenanntes „behavioral targeting"). Hierzu werden Nutzerprofile anhand der bisher besuchten Webseiten und deren Inhalte, aber auch aus sonstigen übermittelten Inhalten erstellt. Zu Letzteren zählen insbesondere Kommunikationsinhalte wie E-Mails oder Chats.[7] Bei dieser Inhaltsauswertung wird nach Schlüsselwörtern gesucht. Wird das Potential der Tiefenanalyse ausgeschöpft, besteht die Möglichkeit einer Komplettauswertung des übermittelten Traffic. Bildet man eine Analogie zur Sprachtelefonie würde dies dem Abhören aller Kundengespräche durch den Telekommunikationsanbieter und der Suche nach Schlüsselwörtern und im Extremfall der Komplettauswertung der Gesprächsinhalte mitsamt Profilbildung gleichkommen. Solche Komplettüberwachungsszenarien sind

[5] DPI wurde im Vereinigten Königreich durch die British Telecom (BT) in Zusammenarbeit mit der Firma Phorm heimlich eingesetzt und anfänglich sogar geleugnet; der Einsatz des DPI-Verfahrens wurde eher zufällig durch einzelne Kunden entdeckt; siehe dazu http://www.theregister.co.uk/2008/03/17/bt_phorm_lies/.

[6] Erstmals in den USA durch die Firma NebuAd praktiziert; im Vereinigten Königreich war bis vor kurzem die Firma Phorm und ihr „Webwise"-System beim Provider BT aktiv, während die Provider Virgin Media und Carphone Warehouse an Tests interessiert sind; dazu unten mehr.

[7] http://www.heise.de/newsticker/Provider-sollen-Kunden-umfassend-ausgespaeht-haben--/meldung/106086.

allenfalls von Geheimdiensten[8] oder totalitären Staaten wie China[9] oder dem Iran[10] bekannt. Werden zusätzlich Inhalte manipuliert und Pakete umgeleitet, käme dies im Szenario der Sprachtelefonie dem Fall gleich, dass der Kunde eine Nummer anruft, der Anruf jedoch vom Anbieter abgefangen wird und der Kunde stattdessen mit einem Call-Center verbunden wird, um ihn beispielsweise über einen kostenlosen Dienst zu informieren.[11]

Der Einblick in die übertragenen Inhalte und deren Durchleuchtung bzw. Umleitung ist rechtlich problematisch. Es wird in das Fernmeldegeheimnis (Art. 10 GG) und das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG iVm Art. 1 Abs. 1 GG) eingegriffen. Zwar bedienen sich die deutschen Behörden derzeit noch nicht oder nur eingeschränkt[12] dieser Methode,[13] jedoch werden die beiden Rechtsgüter auch einfachgesetzlich und zwischen Privaten geschützt. Erwähnt seien das Bundesdatenschutzgesetz oder die strafrechtlichen Vorschriften in § 206 StGB, § 202b und § 303a StGB. Ob und inwieweit die Voraussetzungen der Vorschriften erfüllt sind, wird weiter unten zu prüfen sein.

---

[8] Erwähnt sei das Überwachungsprogramm der National Security Agency (NSA) und der damit zusammenhängende AT&T-Spitzelskandal; siehe hierzu http://www.heise.de/newsticker/NSA-Lauschprogramm-weiter-aktiv--/meldung/140674 und http://www.spiegel.de/wirtschaft/0,1518,411769,00.html; das auf NSA-Technologie („Tutelage“) basierende sogenannte „Einstein 3“-Programm soll dem Department of Homeland Security (DHS) die inhaltliche Überwachung der Kommunikation mit zivilen US-Behörden ermöglichen, http://www.heise.de/newsticker/USA-verzoegern-Ausbau-des-Schutzes-vor-Cyber-Attacken--/meldung/141612; http://online.wsj.com/article/SB124657680388089139.html.

[9] http://www.focus.de/digital/internet/great-firewall_aid_265552.html.

[10] http://www.sueddeutsche.de/politik/479/472998/text/; http://www.sueddeutsche.de/wirtschaft/392/472912/text.

[11] http://www.zdnet.de/sicherheits_analysen_lauschangriff_dpi_so_hoeren_die_provider_ihre_kunden_ab_story-39001544-41001975-1.htm

[12] Zum Beispiel durch das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10) und dessen enge Voraussetzungen in § 3.

[13] Anders hingegen die Pläne im Vereinigten Königreich – erwähnt seien das Interception Modernisation Programme (http://www.timesonline.co.uk/tol/news/uk/article4882600.ece) und das damit zusammenhängende und weitergehende MTI-Project (http://www.theregister.co.uk/2009/05/03/gchq_mti); in den USA werden Provider staatlicherseits an den digitalen Pranger gestellt, wenn sie sich weigern kinderpornografische Dateien anhand von Blacklists zum Beispiel mittels der DPI-Anwendung „Copy Router“ auszufiltern; http://www.msnbc.msn.com/id/27198621; deren Funktionsweise wird unter http://msnbcmedia.msn.com/i/msnbc/Sections/NEWS/PDFs/081016_copyrouter.pdf beschrieben.

2 DEFINITION DER „DEEP PACKET INSPECTION“

Die Betonung beim Begriff „Deep Packet Inspection“ liegt auf „deep“. Daher ist zu klären, was genau daran tiefergehender ist verglichen mit der „normalen“ Paketanalyse.

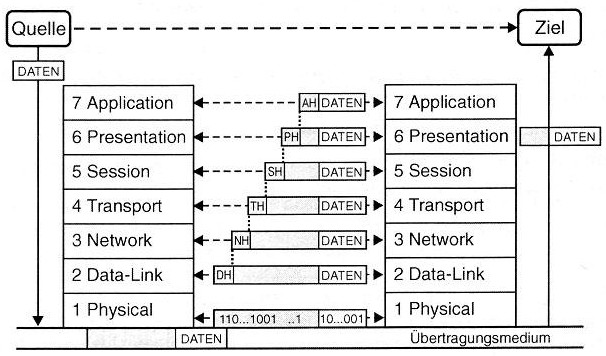
Erster Anknüpfungspunkt ist der Paketbegriff. Über sogenannte „Pakete“ werden die Daten im Internet transportiert. Deren Zusammensetzung ist im sogenannten „OSI-Schichtenmodell (Open Systems Interconnection Reference Model)“ definiert. Das Modell beschreibt das Durchlaufen von sieben Schichten (Layer) in denen Funktionen und Protokolle definiert sind und einer bestimmten Aufgabe bei der Kommunikation zwischen zwei Systemen zugeordnet sind. Es basiert auf dem vierschichtigen DoD-Schichtenmodell, das auch als TCP/IP-Referenzmodell bezeichnet wird.[14]

<table>
<tr><th>DoD-Schichtenmodell</th><th>OSI-Schichtenmodell</th></tr>
<tr><td rowspan="3">Anwendungsschicht
Application Layer</td><td>Anwendungsschicht</td></tr>
<tr><td>Darstellungsschicht</td></tr>
<tr><td>Kommunikationsschicht</td></tr>
<tr><td>Transportschicht
Transport Layer</td><td>Transportschicht</td></tr>
<tr><td>Internetschicht
Internet Layer</td><td>Vermittlungsschicht</td></tr>
<tr><td rowspan="2">Netzzugangsschicht
Network Access Layer</td><td>Sicherungsschicht</td></tr>
<tr><td>Bitübertragungsschicht</td></tr>
</table>

Quelle: http://www.elektronik-kompendium.de/sites/net/0907011.htm

In diesem Zusammenhang ist jedoch nur wichtig, dass ein solches Datenpaket – eben wegen diesen sieben Schichten – aus mehreren Teilen besteht. Dies sind die Nutzdaten, die die eigentlichen Inhaltsdaten darstellen, und die sogenannten Kopfdaten, die auch als Header bezeichnet werden. Jede Schicht fügt den eigentlichen Inhaltsdaten einen eigenen Header hinzu. Die siebte Schicht, die Anwendungsschicht (oft auch als „Application Layer“ oder „Layer 7“ bezeichnet) enthält deswegen nur den (Application) Header und die Nutzdaten. Jede weitere Schicht enthält die Nutzdaten, den eigenen Header und die Header der darunter liegenden Schichten.

[14] RFC 760, http://www.faqs.org/rfcs/rfc760.html.



Schichten-Modell

Quelle: http://www.borg-gs.at/grof/hp_grof/informatik/netzwerk/osi_schichtenmodell.jpg

Für das weitere Verständnis ist aber zunächst nur der Header auf der dritten Schicht, nämlich der sogenannte IP-Header, relevant.

IPv4-Header (Farbliche Hervorhebung durch den Autor)

0–3	**4–7**	**8–11**	**12–15**	**16–18**	**19–23**	**24–27**	**28–31**
Version	IHL	Type of Service		Gesamtlänge			
Identifikation				Flags	Fragment Offset		
TTL		Protokoll		Header-Prüfsumme			
Quell-IP-Adresse							
Ziel-IP-Adresse							
evtl. Optionen …							

Quelle: http://de.wikipedia.org/wiki/IPv4#Header-Format

Als nächsten Schritt muss man sich klar machen, welche Aufgaben Network- und Accessprovider haben und wie diese technisch umgesetzt werden. Internetprovider in diesem Sinne sollen Daten von einem Ausgangspunkt zu einem Zielpunkt innerhalb des Internets weiterleiten (sogenanntes „Routing“). Unter Accessproviding ist das Gewähren, Aufrechterhalten und nötigenfalls Resynchronisieren des technischen Zugangs zu vorhandenen geschlossenen oder offenen Netzen zu verstehen. Der Accessprovider tritt dabei als Zugangsvermittler auf.[15] Networkprovider vermitteln keine Kundenzugänge zum Internet, sondern betreiben

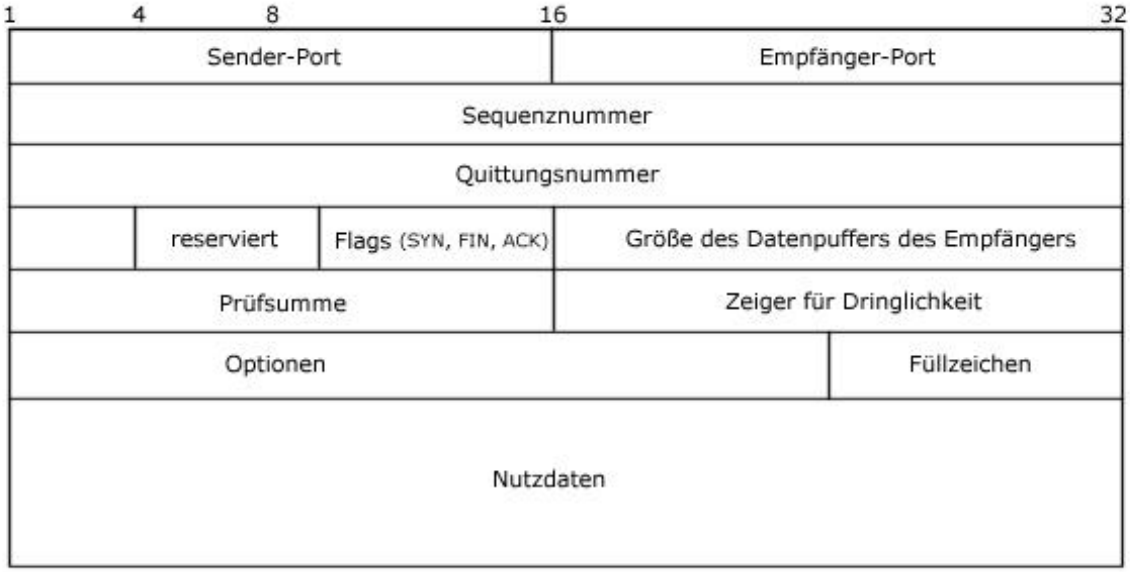
[15] *Härting/Müßig*, Kommunikation und Recht 2009, 233.

die TK-Infrastruktur, über die die Informationen durchgeleitet werden.[16] Um dies zu ermöglichen müssen die Router an den jeweiligen Knotenpunkten „wissen“ an welche IP-Adresse die Daten gesendet werden sollen. Diese Information in Form von Quell- und Zieladressen befindet sich im eben genannten IP-Header. Im Vergleich mit der Briefpost wäre dies der Briefumschlag auf dem die Absender- und Empfängeradressen stehen.

Damit ein Provider seine Aufgabe erfüllen kann, reicht es demzufolge aus nur den IP-Header eines Pakets auszuwerten. Daraus kann ein Router die Information entnehmen, von wem das Paket kommt und wohin es gesendet werden soll. Vom Inhalt des Pakets muss ein Provider folglich keine Kenntnis nehmen.[17] Dieses Auswerten des Pakets mit dem Ziel die IP im Header ausfindig zu machen ist – vereinfacht gesagt – die „Inspection“ aus dem Begriffspaar „Packet Inspection“.

Eine Vorstufe der „Deep Packet Inspection“ ist die „Shallow Packet Inspection“ (SPI), auch als „Stateful Packet Inspection“ bezeichnet. Im Vergleich zur DPI wird bei der SPI nur „oberflächlich“ ausgewertet. Hierunter fällt insbesondere die Auswertung des TCP- bzw. UDP-Headers auf Schicht vier. Dadurch kann der Provider die genutzten Ports[18] ermitteln.[19]

TCP-Header



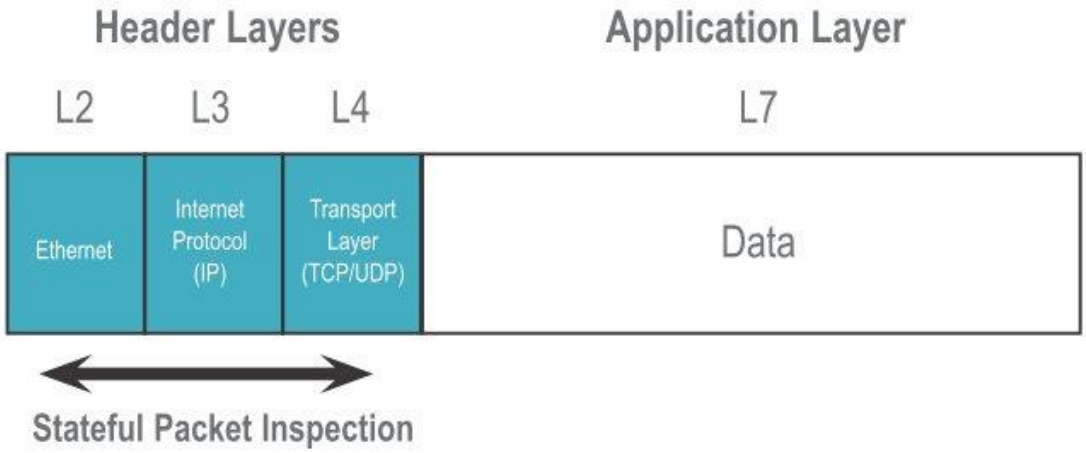
Quelle: http://www.schule.de/schulen/wvs/faecher/informatik/material/internet/internet/bilder/tcp-header.jpg

[16] Hoeren/Sieber/*Höfinger*, Handbuch Multimedia-Recht, 19. Ergänzungslieferung 2008, 18.1 Rn. 33.

[17] http://www.zdnet.de/sicherheits_analysen_lauschangriff_dpi_so_hoeren_die_provider_ihre_kunden_ab_story-39001544-41001975-1.htm.

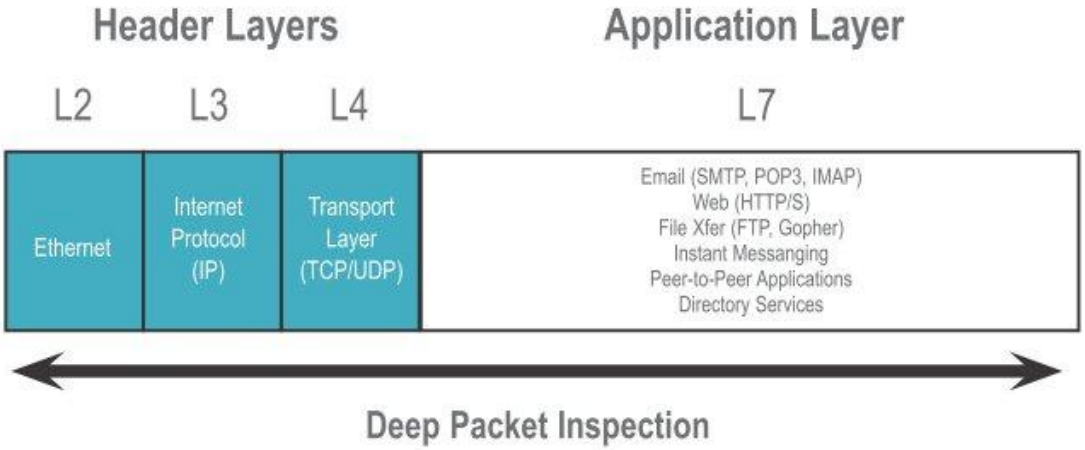
[18] Zu Definition des Begriffs „Port“ siehe http://de.wikipedia.org/wiki/Port_%28Protokoll%29; üblicherweise nutzen Internetdienste und -anwendungen, wie zum Beispiel E-Mail, Webserver oder FTP vordefinierte Standardports (unverschlüsselter E-Mail-Versand üblicherweise Port 25, Webserver den Port 80 und FTP die Ports 20 und 21).

[19] Zur praktischen Anwendung siehe dazu unten den Abschnitt „Netzwerkmangagement“.



Quelle: http://www.esoft.com/pdf/whitepaper/DPI_white_paper.pdf

Jede Art der Auswertung, die darüber hinausgeht ist als „deep“ anzusehen. Je höher also die Schicht und umso eher Nutzdaten betroffen sind, umso tiefergehend ist die Auswertung.



Quelle: http://www.esoft.com/pdf/whitepaper/DPI_white_paper.pdf

DPI betrifft folglich, in Abgrenzung zur SPI, die höheren Schichten fünf bis sieben des OSI-Modells.[20] Es werden die Header aller Schichten und vor allem die Nutzdaten auf Schicht sieben ausgewertet.

Nach einem strengen Verständnis[21] wird nicht zwischen SPI und DPI unterschieden, stattdessen erfolgt die Abgrenzung anhand der ureigenen Aufgabe des Providers, nämlich dem simplen Routing. Nach dieser strengen

[20] http://arstechnica.com/hardware/news/2007/07/Deep-packet-inspection-meets-net-neutrality.ars.

[21] http://www.zdnet.de/sicherheits_analysen_lauschangriff_dpi_so_hoeren_die_provider_ihre_kunden_ab_story-39001544-41001975-2.htm.

Sicht sind bereits Auswertungen der Ports im Header der vierten Schicht als DPI anzusehen. Weil aber auch Nutzer Firewalls einsetzen, die auf dieser vierten Schicht agieren, ist neben der Einordnung „Datenauswertung innerhalb einer der Schichten vier bis sieben des OSI-Schichtenmodells“ nach dieser strengeren Definition zusätzlich zu differenzieren *wer* die Daten auswertet. Die Auswertung muss demzufolge durch den Provider oder von ihm Beauftragte erfolgen.

3 MOTIVE DER INTERNETPROVIDER FÜR DEN EINSATZ VON DPI-TECHNOLOGIE

Wieso sich Provider nicht auf ihre eigentliche Aufgabe der Datenweiterleitung beschränken und es dennoch zum Einsatz von DPI-Technologie kommt, soll im Folgenden erörtert werden. Es bestehen verschiedene Motivationslagen und Ursachen für deren Einsatz.[22] Um diese nachvollziehen zu können, ist es wiederum nötig die Feinheiten der eingesetzten Technik näher zu erläutern.

3.1 NETZWERKSICHERHEIT

Wie einleitend festgestellt war das ursprüngliche Ziel bei der Entwicklung der DPI die Wahrung der Netzwerksicherheit.[23] Angesichts neuer Bedrohungen wie verseuchten Webseiten, die dem Besucher unbemerkt Schadsoftware unterschieben (sogenannte „Drive-by-Downloads“), verwundert es nicht, dass moderne Firewalls, Intrusion Detection Systeme (IDS) und Intrusion Prevention Systeme (IPS) mittlerweile auch DPI-Verfahren nutzen. Als Beispiel seien Application Layer Firewalls (ALF), auch als Web Application Firewalls (WAF) bezeichnet, genannt. Diese agieren auf Schicht sieben und können über Schlüsselwörter oder Black- und Whitelists gesteuert werden, wodurch eine gezielte Contentfilterung ermöglicht wird. Ein solcher Eingriff in die Inhaltsdaten ist erheblich intensiver als eine bloße Identifizierung der Art des übertragenen Traffic. Diese neuartigen Firewalls sind die Nachfolger der sogenannten „Stateful Packet Inspection-Firewalls“, die lediglich auf der vierten OSI-Schicht agierten und daher nicht unter die hier vertretene Definition von DPI fielen. Erstere sind teilweise bereits bei Providern installiert und so in der Lage frühzeitig Schadsoftware aus dem Datenstrom herauszufiltern und verhindern dadurch, dass die Kunden damit in Kontakt kommen.[24] Sehr viel öfter finden sich solche modernen Firewalls in Unternehmensnetzwerken, da es weniger aufwändig ist zentral gewisse Schadroutinen[25] auszufiltern, anstatt lokal an unzähligen Einzelrechnern,[26] die teilweise gar nicht dem Zugriff durch den Netzwerkadministrator unterliegen, wie beispielsweise von Firmenbesuchern mitgebrachte Laptops.

3.2 NETZWERKMANAGEMENT

Netzwerkmanagement wird eingesetzt, wenn die Übertragungskapazitäten des Netzwerks nicht mehr ausreichen und es zur Überlastung des Providers kommt. Dieser steht dann vor den Alternativen die eigene Infrastruktur auszubauen oder die Last (meist zu Spitzenzeiten) zu reduzieren, indem gewisse Dienste, überwiegend Filesharing, ausgebremst werden, um den übrigen Traffic zu bewältigen, also zu verhindern, dass es zu Paketverlusten und langsamerer Datenübertragung kommt. Es ist dann eine ökonomische Frage, ob er die Kapazitäten ausbaut oder ob er DPI-fähige Hard- und Software anschafft und damit steuernd in den Datenfluss eingreift. Hinsichtlich der Technik gibt es auch preisliche Abstufungen, je nachdem wie viele Anschlüsse überwacht werden sollen und wie tiefgehend die Paketanalyse erfolgen soll. Je mehr Anschlüsse überwacht

[22] Eine ähnliche Klassifikation nimmt *Bendrath* vor in „Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection“, International Studies Annual Convention New York City, 15-18 February 2009, S. 15.

[23] *Bendrath*, S. 14.

[24] So nutzt der alternative DNS-Anbieter „OpenDNS“ (durch den Nutzer abschaltbare) Filter, die verhindern, dass die Domains von malwareverseuchten Webseiten in IP-Adressen aufgelöst werden und demzufolge nicht mit dem Browser angesteuert werden können.

[25] Pufferüberlauf-, Denial-of-Service-Angriffe sowie verschiedene Arten von Schadsoftware, vgl. http://www.searchsecurity.de/glossar/Deep%20Packet%20Inspection/articles/181757/.

[26] Beispielsweise mittels Desktop Firewalls oder direkt im Browser.

werden und je tiefer dies erfolgt, umso leistungsfähiger muss die Hard- und Software sein und umso teurer ist dementsprechend die Anschaffung. Die Notwendigkeit einer gewissen Leistungsfähigkeit der Hardware ist im Übrigen die Ursache, wieso das Thema DPI nicht schon früher aufkam. Die gleichzeitige Überwachung von vielen verschiedenen Datenströmen erfordert eine gewisse Rechenleistung, die es früher nicht gab.[27]

Als Vorstufe[28] zur DPI nutzten einige Provider die im TCP-Header verzeichneten Quellen- und Zielports, meist vordefinierte Ports, die sogenannten „well known ports" 0-1023 und gewisse „registered ports" 1024-49151, als Anhaltspunkt für die Art des übermittelten Traffic und limitierten bei bekannten Filesharing-Ports[29] einfach die verfügbare Bandbreite oder sperrten sie ganz. Da jedoch über die vordefinierten Ports nicht zwingenderweise die vordefinierten Anwendungen kommunizieren und die entsprechende Art der Daten übertragen wird, weil grundsätzlich jeder Dienst auf jeder Portnummer funktioniert und sich neuere Software nicht an die ursprüngliche Portaufteilung hält oder auch einfach vom Nutzer abänderbar ist, wurde diese Art des Trafficmanagements mit der Zeit sinnlos. Peer-to-Peer-Software oder VoIP-Software (insbesondere Skype) nutzen heutzutage die (offenen) Ports teilweise zufällig oder sogar so, wie sie gerade verfügbar sind.[30] Es gibt seit wenigen Jahren sogar Netzwerkprotokolle, wie beispielsweise STUN,[31] die schon von ihrem eigentlichen Zweck her so ausgestaltet sind, dass sie portbasierte Firewalls oder NAT-Router ungehindert durchdringen können.

Trafficmanagement erfolgt deswegen nicht mehr anhand der Ports, sondern auf der Anwendungsschicht. Es kommt dabei weniger auf die konkreten Inhaltsdaten an, sondern auf die Identifizierung der Art der Daten. Es soll die genutzte Anwendung identifiziert werden und deren Traffic anschließend ausgebremst oder bevorzugt behandelt werden. VoIP-Traffic wird üblicherweise am höchsten priorisiert, während Filesharingtraffic verlangsamt[32] oder ganz blockiert wird.

Den eingesetzten Erkennungs- und Drosselungsverfahren liegen verschiedene Methoden zugrunde.

---

[27] http://www.zdnet.de/sicherheits_analysen_lauschangriff_dpi_so_hoeren_die_provider_ihre_kunden_ab_story-39001544-41001975-4.htm.

[28] Siehe oben die Ausführungen zur „Shallow Packet Inspection".

[29] Legendär ist Port 4662, der voreingestellt bei der Filesharingsoftware „Edonkey" und „EMule" verwendet wird.

[30] Zur Umgehung von Firewalls durch Skype siehe http://www.heise.de/security/Wie-Skype-Co-Firewalls-umgehen--/artikel/82054.

[31] Bereits der Name verdeutlicht den Zweck; STUN steht für „Session Traversal Utilities for NAT"; http://de.wikipedia.org/wiki/STUN.

[32] Der Kabelinternetanbieter „Kabel Deutschland" wird in Internetforen verdächtigt regional wechselnd und zu bestimmten Zeiten Filesharing- und FTP-Dienste aktiv zu drosseln, http://www.onlinekosten.de/forum/showthread.php?t=102193; der Anbieter bestreitet zwar die Drosselung, räumt jedoch ein, dass es bei gewissen Anwendungen zu „vorübergehenden Einschränkungen" kommen kann, http://www.onlinekosten.de/news/artikel/35204/0/Kabel-Deutschland-nimmt-Stellung-zu-Beschwerden.

3.2.1 ERKENNUNGSVERFAHREN

3.2.1.1 SIGNATURBASIERT

Technisch werden bei diesem Verfahren Signaturen der genutzten Anwendungen aufgespürt. Signaturen in diesem Sinne sind regelmäßig und typisch vorkommende Datenfolgen im Datenstrom, die durch die Nutzung von spezifischer Software auftreten.[33] Beispiele für solche Datenfolgen sind Textfolgen oder Nummern, die typischerweise bei der Benutzung von bestimmten Anwendungen auftreten. Insbesondere wenn Filesharingsoftware auf Port 80 betrieben wird, werden hauptsächlich die ebenfalls über diesen Port übertragenen Webinhalte gegengeprüft.[34]

3.2.1.2 VERHALTENSBASIERT

Bei der Verhaltensanalyse wird mittels statistischer und heuristischer Verfahren analysiert, wie sich eine unbekannte (weil beispielsweise die Protokollinformationen oder die Daten verschlüsselt oder verschleiert[35] sind) Anwendung verhält. So kann auch bei verschlüsselten Verbindungen erkannt werden, ob sich typische Verhaltens- und Vorgehensweisen einer bestimmten (Filesharing)software oder Softwaregattung ergeben. Beispielsweise wenn eine aktive UDP-Verbindung in eine TCP-Verbindung unter Beibehaltung der IP und Portnummern umgewandelt wird. Ein weiteres Beispiel ist die Anzahl der Verbindungen, die innerhalb eines bestimmten Zeitraums von und zu einer IP aufgebaut werden. Während bei klassischem Webtraffic üblicherweise wenige und nur sporadisch Verbindungen zu Servern aufbaut werden, ist es bei Filesharingsoftware so, dass konstant viele und vergleichsweise langanhaltende Verbindungen aufgebaut werden. Ähnlich ist die Analyse numerischer Eigenschaften, wie die Länge der Nutzlast in Paketen oder die Anzahl von Antwortpaketen auf eine bestimmte Anfrage.[36]

Eine Möglichkeit das Netzwerkmanagement zu umgehen ist die Nutzung von Tunneln (beispielsweise Virtual Private Networks), wobei die übertragenen Daten zusätzlich verschlüsselt werden. Diese Kombination ist eine effektive Möglichkeit Netzwerkmanagementeingriffe zu verhindern. Hingegen ist die bloße Verschlüsselung ohne Nutzung eines Tunnels keine Gewähr, dass nicht doch erkannt wird welche Art von Traffic verschlüsselt übertragen wird, wie man am verhaltensbasierten Erkennungsverfahren sehen kann.

3.2.2 DROSSELUNGSVERFAHREN

3.2.2.1 BANDBREITENLIMITIERUNG

Wie oben bereits festgestellt kann ein Provider die Bandbreite an gewissen Ports oder für den kompletten Internetzugang limitieren.

[33] http://www.allot.com/index.php?option=com_docman&task=doc_view&gid=88.

[34] http://www.allot.com/index.php?option=com_docman&task=doc_view&gid=88, dort S. 6.

[35] Bei Bittorrent als „protocol encryption“ oder bei der Software Emule als „obfuscation“ bezeichnet.

[36] http://www.allot.com/index.php?option=com_docman&task=doc_view&gid=88, dort S. 6-7.

3.2.2.2 GEFÄLSCHTE TCP-RESET-PAKETE („COMCASTMETHODE“)

Bei dieser Methode verschickt der Provider an die, am Filesharing beteiligten Anschlüsse nach einer gewissen (vom Provider vorgegebenen) Zeit gefälschte TCP-Reset-Befehle, wodurch dem jeweiligen Anschluss vorgetäuscht wird die jeweilige Gegenseite habe die Verbindung beendet, wodurch es nur zu einer teilweisen Übertragung der angeforderten Daten kommt.[37] Damit wird nicht nur in die Telekommunikation der eigenen Kunden, sondern auch in die der jeweils am Datenaustausch Beteiligten eingegriffen. An diesem Vorgehen entzündete sich ein Streit, der letztlich von der FCC zu Lasten von Comcast entschieden wurde.[38]

3.2.3 NETZNEUTRALITÄT

Mittlerweile hat sich die FCC zur Netzneutralität bekannt und einen Plan zu deren Stärkung vorgestellt,[39] an dem sich nunmehr auch die Bundesnetzagentur in Deutschland orientiert.[40] Ein Punkt sieht vor, dass Provider die Techniken für das Netzwerkmanagement einsetzen, ihre Kunden detailliert darüber in Kenntnis setzen müssen.[41] In anderen Ländern herrscht hingegen ein Klima der Restriktionen. So erwägt die britische Regierung Bandbreitenlimitierungen als Mittel gegen Filesharing einzusetzen,[42] während in Frankreich Filesharer nach drei erfolglosen Warnungen komplett ohne Internetzugang bleiben.[43] In Deutschland haben sich die CDU, CSU und FDP in ihren Koalitionsvereinbarungen – mehr oder weniger deutlich – zur Wahrung der Netzneutralität bekannt.[44]

3.3 CONTENTFILTERUNG UND BLOCKIERUNG VON WEBSEITEN

3.3.1 FILTERUNG UND BLOCKIERUNG VON (MEDIEN)DATEN

Mittels Contentfilter, als Teil einer Application-Layer-Firewall, kann der ein- und ausgehende Traffic effektiv überwacht werden. Neben der Blockierung von Malware im eingehenden Traffic ist es Providern möglich Dateien in beiden Richtungen herauszufiltern und damit dem Nutzer nicht mehr zugänglich zu machen oder deren Versand zu unterbinden. Eine solche Contentfilterung gezielt nach einzelnen Dateien ist natürlich erst recht möglich, wenn bereits einzelne Schlüsselwörter herausfilterbar sind. Einzelne bekannte Dateien werden

[37] http://www.eff.org/wp/packet-forgery-isps-report-comcast-affair.

[38] http://arstechnica.com/old/content/2008/07/hammer-drops-at-last-fcc-opposes-comcast-p2p-throttling.ars.

[39] http://www.heise.de/ct/US-Regulierer-stellt-Plan-zur-Staerkung-der-Netzneutralitaet-vor--/news/meldung/145641; http://www.openinternet.gov/read-speech.html.

[40] http://www.heise.de/newsticker/Eco-Kongress-Bundesnetzagentur-bekennt-sich-zu-Netzneutralitaet--/meldung/146083.

[41] http://www.heise.de/ct/US-Regulierer-stellt-Plan-zur-Staerkung-der-Netzneutralitaet-vor--/news/meldung/145641; http://www.openinternet.gov/read-speech.html.

[42] http://www.heise.de/newsticker/Britische-Regierung-erwaegt-Bandbreiten-Drosselung-fuer-illegales-Filesharing--/meldung/140578.

[43] http://www.heise.de/newsticker/meldung/Frankreich-Internetsperre-fuer-Urheberrechtsverletzer-gebilligt-837138.html.

[44] http://www.heise.de/newsticker/meldung/Union-und-FDP-setzen-auf-offene-Standards-und-Open-Source-834219.html; http://www.spiegel.de/netzwelt/netzpolitik/0,1518,657486-8,00.html.

über deren Hashwert identifiziert, mittels Blacklists gefiltert und anschließend blockiert oder sogar mit einer Datei ersetzt, die beispielsweise eine Warnmeldung der Behörden enthalten kann.[45] So ist es – neben der Filterung von kinderpornographischen Dateien – denkbar, dass Urheber und deren Vertreter an Provider herantreten oder diese gerichtlich verpflichten lassen gewisse Inhalte nicht mehr zu übertragen. Während diese Filterung über Hashwerte bereits seit einiger Zeit bei sogenannten One-Click-Hostern praktiziert wird,[46] ist es natürlich ebenso möglich (wenn auch aufwändiger) die Filterung im Datenstrom beim Provider durchzuführen.[47]

3.3.2 FILTERUNG, BLOCKIERUNG UND SPERRUNG VON WEBSEITEN UND DIENSTEN

Ebenfalls eine Art Contentfilterung mittels DPI ist eine Blockierung (Sperrung) von Webseiten durch DNS-Sperren. Die Provider lösen gewisse Webseitenadressen (URLs) im providereigenen Nameserver nicht mehr auf oder leiten die Anfrage sogar um, indem sie eine falsche IP-Adresse zurückgeben, die dann vom Browser angesteuert wird (sogenannter DNS-Redirect). Da der DNS-Dienst innerhalb der Schichten fünf bis sieben läuft, sind Eingriffe in die Inhalte, sprich die vom Nutzer eingegebenen Webseitenadressen und die verfälschte Rückgabe der „zugehörigen" IP-Adresse (Umleitung auf Stoppseite) oder gar keine Rückgabe einer IP-Adresse (eigentliche Blockierung) als DPI im Sinne des obigen Verständnisses anzusehen.

Die Filterung von DNS-Anfragen kann also sowohl zur Gewährleistung der Netzwerksicherheit als auch dazu dienen, den Zugriff auf gewisse Webseiten zu erschweren und optional den versuchten Zugriff darauf zu protokollieren.

Um die Möglichkeit der Nutzung von providerfremden DNS-Servern zu unterbinden, gibt es auch das aufwändigere DPI-Verfahren den gesamten Traffic nach gewissen URLs oder IP-Adressen zu filtern und den Zugriff darauf mittels Blacklists zu verhindern. So wird entweder die Namensauflösung auf allen Nameservern unterbunden, indem die Anfrage nicht mehr weitergeleitet oder die zu filternde URL oder IP komplett blockiert wird, so dass auch eine eventuell erfolgreiche Namensauflösung ins Leere führt, da die Seite dann IP-technisch nicht mehr zu erreichen ist. Die erfolglosen Zugriffe können wieder optional protokolliert und auch auf andere Server umgeleitet werden. Eine gezielte URL-Filterung hat außerdem den Vorteil, dass es nicht zum Overblocking kommt, wenn mehrere Webseiten unter einer einzigen IP erreichbar sind und nur eine einzelne oder einige wenige Web(unter)seiten gezielt blockiert werden sollen. Eine Umgehung dieser Art von Sperren ist nur noch durch verschlüsselte Tunnel (beispielsweise Anonymisierungsdienste über VPN) möglich, die ihrerseits keinerlei Sperrmaßnahmen implementiert haben.

Ähnlich ist die Methode DNS-Anfragen an providerfremde Nameserver über Port 53 abzufangen und durch providereigene (zensierte) Nameserver zu beantworten.[48] Diese Form der DNS-Manipulation ist jedoch durch einen eigenen lokalen Caching-DNS-Server umgehbar.[49]

---

[45] http://www.msnbc.msn.com/id/27198621.

[46] http://www.chip.de/news/Rapidshare-Neues-System-gegen-Raubkopierer_33519932.html; http://futurezone.orf.at/stories/316067; http://www.heise.de/newsticker/Gericht-Sharehoster-muss-Veroeffentlichung-von-Musik-unterbinden--/meldung/140965.

[47] Zur Funktionsweise von „CopyRouter" siehe http://msnbcmedia.msn.com/i/msnbc/Sections/NEWS/PDFs/081016_copyrouter.pdf.

[48] http://www.zdnet.de/sicherheit_in_der_praxis_sperre_von_freien_dns_servern_so_umgeht_man_die_blockade_story-39001543-41502966-1.htm; dies wurde dem Provider Vodafone zeitweise vorgeworfen; man beachte

Neben einzelnen Inhalten können auch komplette Dienste gezielt blockiert werden. So ist es bei über Mobilfunktechnologie angebotenen Datendiensten (GPRS, UMTS) üblich die Nutzung von VoIP oder Messengern zu unterbinden, damit das Sprachtelefonie- oder SMS-Geschäft der Mobilfunkbetreiber nicht geschädigt wird.[50]

3.4 UMLEITUNGEN

3.4.1 ERSTE ALTERNATIVE

DNS-Redirects durch Provider sind mittlerweile an der Tagesordnung. Immer mehr Provider[51] geben in ihren Benutzeranleitungen und -hinweisen standardmäßig DNS-Server an, die die leer laufenden Webseitenanfragen (sprich die anzusteuernde Domain existiert nicht) auf providereigene Suchseiten umleiten anstatt eine Fehlermeldung auszugeben. Nicht selten verdienen die Provider daran, indem direkt auf der Suchseite Werbung geschaltet wird oder die Suchseiten gesponsert werden.[52] Bei Volumentarifen kommt erschwerend hinzu, dass dadurch zusätzlicher Traffic generiert wird, den der Kunde bezahlen muss. Angesichts der (insbesondere früher) horrenden Preise bei der Nutzung des Internets über Mobilfunk ein nicht zu verachtender Gesichtspunkt.

3.4.2 ZWEITE ALTERNATIVE

Ähnlich zu werten sind Umleitungen bei existierenden Adressen auf providereigene Webseiten, wie beispielsweise bei der erstmaligen mobilen Nutzung des Internets über T-Mobile. Statt der vom Nutzer eingegeben URL und der entsprechenden Webseite wird eine Webseite mit Einstellungen oder Hinweisen angesteuert und angezeigt.[53] Der erste DNS-Request[54] wird folglich immer auf die IP der Einstellungsseite aufgelöst.

---

jedoch die Überarbeitung des Artikels und den Kommentar des Autors *Hochstätter* vom 3. Oktober 2009, 13:31 Uhr; demnach kann das Abfangen derzeit nicht mehr bestätigt werden kann.

[49] http://www.zdnet.de/sicherheit_in_der_praxis_sperre_von_freien_dns_servern_so_umgeht_man_die_blockade_story-39001543-41502966-1.htm inklusive der Folgeseiten.

[50] http://www.onlinekosten.de/news/artikel/17924; http://www.theregister.co.uk/2009/07/06/bt_phorm.

[51] In Deutschland nutzen fast alle großen Provider dieses Verfahren, so zum Beispiel Kabel Deutschland, T-Online, Hansenet und Freenet; http://www.codedifferent.de/2009/04/26/t-online-kapert-mit-ihrer-navigationshilfe-google-subdomains-und-schaltet-yahoo-werbung/; einige bieten zumindest Opt-Out-Lösungen, wie zum Beispiel der Provider Freenet unter der Webadresse http://kundenservice.freenet.de/hilfe/komplett/hardware/weitere-themen/dns-redirect/dnsredirect-deaktivieren/deaktivieren/index.html.

[52] http://www.heise.de/newsticker/DNS-Redirect-Jedem-seinen-eigenen-Sitefinder--/meldung/66925; http://en.wikipedia.org/wiki/Site_Finder.

[53] http://www.zdnet.de/sicherheits_analysen_lauschangriff_dpi_so_hoeren_die_provider_ihre_kunden_ab_story-39001544-41001975-1.htm.

3.4.3 DRITTE ALTERNATIVE

Einfacher funktionieren die ursprünglich angedachten „DNS-Sperren“ der Bundesregierung. Hierbei werden bestimmte „blockierte“ Webadressen mit der IP der Stoppschildseite aufgelöst, anstatt mit der ihnen eigentlich zugewiesenen. Dabei werden die gesperrten IP-Adressen durch die IP der Stoppseite ersetzt.

3.4.4 VIERTE ALTERNATIVE

Die oben geschilderte Methode des gezielten Abfangens von DNS-Abfragen an providerfremde DNS-Server und Beantwortung durch providereigene DNS-Server stellt ebenfalls eine Umleitung dar. Diese Art der Sperre scheint sich mittlerweile, in Abkehr zur dritten Alternative, als Methode zur Umsetzung des, derzeit für ein Jahr ausgesetzten, Zugangserschwerungsgesetzes herauszukristallisieren.[55]

3.5 PROFILBILDUNG ZWECKS GEZIELTER WERBEEINBLENDUNG

Hauptanwendungsfeld der DPI dürfte aber, wie einleitend anhand der ersten „Gehversuche“ in den USA und dem Vereinigten Königreich dargestellt, der Einsatz von personalisierter Werbung sein. Durch die Kooperation mit Werbeunternehmen erwirtschaften die Provider zusätzliche Einnahmen.

Mittels zwischengeschalteter transparenter Webproxies wird das Aussehen der angesteuerten Webseiten durch Einbettung von Javascript- oder HTML-Code in den Datenstrom heimlich manipuliert und im Ergebnis Werbung gezeigt, die auf der eigentlichen Webseite nicht vorkommt.[56] Das wäre im Vergleich zur Briefpost so, als ob die Post jeden Briefumschlag öffnet und auf die darin liegenden Briefe Werbung aufdruckt.

Als am besten dokumentiertes Beispiel gilt der Einsatz des Produkts „Webwise“ der US-Firma „Phorm“ durch den Provider British Telecom (BT). Mittlerweile wurde der als „Testphase“ bezeichnete Einsatz von „Webwise“ durch BT vorerst beendet.[57] Die britischen Provider Virgin Media und Carphone Warehouse sind jedoch laut Phorm weiterhin an Tests interessiert und auch BT will diese (noch nicht gestarteten) Tests der beiden Konkurrenzprovider abwarten, bevor über einen künftigen Einsatz oder den endgültigen Verzicht auf die Nutzung von „Webwise“ entschieden wird.[58] Das in den USA eingesetzte Verfahren von NebuAd wird ebenfalls nicht mehr eingesetzt.

---

[54] Im konkreten Fall bei T-Mobile wird der erste HTTP-Request umgeleitet, was aber im Ergebnis den gleichen Effekt hat, weil der Unterschied nur bei der direkten Eingabe einer IP statt einer Domain zum Tragen käme.

[55] http://www.zdnet.de/news/wirtschaft_sicherheit_security_geheime_technische_details_zum_internetzensurgesetz_aufgetaucht_story-39001024-41515822-1.htm.

[56] http://yro.slashdot.org/article.pl?sid=07/06/23/1233212; http://www.spikelab.org/blog/btProxyHorror.html; Der kanadische Provider „Rogers Communication Inc.“ machte beispielsweise Eigenwerbung für seine Dienstleistungen, indem er hierfür die Webseiten von Google und später von Flickr in Echtzeit manipulierte; siehe hierzu http://www.thestar.com/Business/article/284761, http://www.p2pnet.net/story/23991 und http://www.gulli.com/news/kanada-isp-f-gt-inhalte-in-2009-06-26/.

[57] http://www.heise.de/newsticker/BT-legt-Plaene-fuer-umstrittenes-Werbesystem-auf-Eis--/meldung/141635.

[58] http://futurezone.orf.at/stories/1613426/; http://www.theregister.co.uk/2009/07/06/bt_phorm.

3.6 MANIPULATION VON WEBINHALTEN ZWECKS EFFIZIENTERER ÜBERTRAGUNG

Ähnlich der obigen Einfügung von Code und der damit einhergehenden Manipulation einer Webseite durch Werbung ist die derzeit von einigen Mobilinternetprovidern praktizierte Unsitte fremde Webseiten während des Abrufs durch Neuzusammensetzen mittels Manipulation des Sourcecodes (mehr oder minder) inhaltlich und insbesondere in ihrem Aussehen zu verfälschen.[59] Ziel dieses schwerwiegenden Eingriffs ist die Reduktion der zu übertragenden Daten. So werden insbesondere Bilder komprimiert, so dass deren Aussehen darunter leidet. Hierfür werden komplette Teile des Quelltextes in Echtzeit entfernt oder sogar fremder Javascriptcode injiziert, um zu den gewünschten Ergebnissen zu gelangen. Die Inhaltsdaten (Quelltext der Webseite) der sendenden Server werden dazu auf einem Server des Providers (sogenannter „Performance Enhancement Proxy“) zwischenverarbeitet und danach erst an den abrufenden Kunden manipuliert weitergeleitet. Denkbar ist außerdem, dass oft abgerufene Webseiten verändert zwischengespeichert werden (Cachingfunktion des Proxy-Servers). Hat der Nutzer keine Vorstellung von dem Vorgehen des Providers, kann dies den Webseitenbetreiber in einem schlechten Licht stehen lassen, beispielsweise wenn die Grafiken durch die Kompression unsauber aussehen oder der Quellcode scheinbar nicht valide ist. Die Codemanipulation kann sogar dazu führen, dass gewisse Webseiten (Ajax-Anwendungen zum Beispiel) überhaupt nicht mehr oder nur noch eingeschränkt funktionieren.

Zwar bietet beispielsweise T-Online eine Einstellungsseite an, auf der die Kompression abgeschaltet werden kann, jedoch funktioniert diese Abschaltung angeblich nicht, was die Frage aufwirft, ob dies absichtlich geschieht oder ob die Auswahloption durch einen (temporären) technischen Effekt nicht funktioniert.[60] Beides spricht nicht unbedingt für ein gesteigertes Interesse an der Beachtung und Durchsetzung der Kundenwünsche. Andere Provider weisen auf die Manipulationen angeblich überhaupt nicht hin.[61]

3.7 BEREITSTELLUNG VON STAATLICHER ÜBERWACHUNGS- UND ZENSURINFRASTRUKTUR

DPI erlaubt ein lückenloses Abhören, Mitschneiden und Verändern der übertragenen Inhalte. Da ist es wenig verwunderlich, wenn von staatlicher Seite Begehrlichkeiten nach einem Zugriff auf diese Datenschätze geweckt werden. So soll der Iran beispielsweise den gesamten inländischen Internetverkehr mittels DPI überwachen.[62] Dies erfolgt angeblich unter Zuhilfenahme von deutscher und europäischer Technologie.[63] Außer China setzt

---

59 http://www.zdnet.de/sicherheits_analysen_internet_per_umts_so_faelschen_deutsche_provider_webinhalte_story-39001544-41515603-1.htm.

60 http://www.zdnet.de/sicherheits_analysen_internet_per_umts_so_faelschen_deutsche_provider_webinhalte_story-39001544-41515603-3.htm.

61 http://www.heise.de/tp/r4/artikel/22/22180/1.html.

62 http://online.wsj.com/article/SB124562668777335653.html.

63 So soll „Nokia Siemens Networks“ angeblich DPI-fähige Technologie an die iranische Regierung verkauft haben, was das Gemeinschaftsunternehmen aber bestreitet; siehe hierzu http://www.golem.de/showhigh2.php?file=/0906/67893.html und http://www.spiegel.de/wirtschaft/0,1518,631862,00.html.

auch Tunesien DPI-Technologie ein.[64] Durch die gezielte Veränderung von Webseiten in Echtzeit ergeben sich auch neue Möglichkeiten der Zensur. Anstatt den Zugriff zu blockieren werden totalitäre Staaten, soweit sie es nicht bereits praktizieren, regimekritische Webseiten zielgenau manipulieren können. Durch das Aufspalten, Filtern und Neuzusammenstellen der Seiteninhalte in Echtzeit ist es möglich einzelne Passagen zu entfernen und andere hinzuzufügen.[65] Was früher Zensoren bei Zeitungen in mühevoller Kleinarbeit machten, ist nunmehr in Echtzeit online möglich. Erst im direkten Vergleich mit der unzensierten Originalseite fallen solche subtilen Änderungen auf, wodurch die Zensur auch nicht so leicht zu entdecken ist wie eine augenscheinliche komplette Zugriffsblockade.

Geheimdienste, auch in der westlichen Welt, werden in die Lage versetzt neben dem Mitschneiden und Auswerten von Inhalten zielgerichtet in die Internetkommunikation, insbesondere in unverschlüsselte E-Mailinhalte und Webcontent, manipulierend einzugreifen. Die Überprüfung der Verlässlichkeit von Onlineinformationen, auch im journalistischen Bereich, wird künftig sehr viel schwieriger werden. Das Einschleusen von Überwachungssoftware (Stichwort: BKA-Trojaner) wird ebenfalls eminent erleichtert. Statt Werbung, wie im obigen Fall, wird dem Nutzer die Überwachungssoftware untergeschoben.

[64] *Wagner*, Deep Packet Inspection and Internet Censorship: International Convergence on an „Integrated Technology of Control“, S. 8; abrufbar unter http://advocacy.globalvoicesonline.org/wp-content/uploads/2009/06/deeppacketinspectionandinternet-censorship2.pdf.

[65] *Wagner*, S. 9 f.

4 RECHTLICHE WÜRDIGUNG

Im Vordergrund der rechtlichen Betrachtung stehen das Strafrecht und das Datenschutzrecht. So wird das in Art. 10 GG verfassungsrechtlich kodifizierte Fernmeldegeheimnis als Abwehrrecht gegen den Staat in § 88 TKG, aufgrund des Schutzauftrags des Staates, auf das privatrechtliche Verhältnis zwischen Telekommunikationsdiensteanbieter (in diesem Fall der Internetprovider) und TK-Nutzer erstreckt. Die strafrechtliche Sanktionierung von Verstößen richtet sich jedoch nach § 206 StGB und zivilrechtlich nach § 44 TKG.[66] § 88 TKG enthält keine Sanktionen.

Geschützt sind in § 88 Abs. 1 Satz 1 TKG die Inhalte der Kommunikation und ihre näheren Umstände. § 206 Abs. 5 Satz 2 StGB wiederholt diese Definition, so dass der Schutzgegenstand der beiden Vorschriften identisch ist. Soweit die Provider die Nutzdaten auswerten, sind dies geschützte Kommunikationsinhalte im Sinne der Definition.

In weiteren Strafvorschriften werden das formelle Geheimhaltungsinteresse an den Daten (§ 202a StGB) und der nichtöffentlichen Datenkommunikation (§ 202b StGB)[67] sowie das Interesse des Verfügungsberechtigten an der unversehrten Verwert- und Verwendbarkeit der Daten (§ 303a StGB) geschützt.[68]

Datenschutzrecht betrifft personenbezogene Inhaltsdaten (§ 1 BDSG). Für die – nachfolgend getrennt rechtlich zu würdigenden Anwendungsgebiete der DPI – ist folglich immer zu prüfen, ob und inwieweit überhaupt solche Daten betroffen sind.

4.1 PRIVILEGIERUNG DURCH DAS TELEMEDIENGESETZ

Eine, nach einer Auffassung vorab zu prüfende, Verantwortlichkeitsprivilegierung der Provider gemäß §§ 7 ff. TMG ist nicht einschlägig, da sich die Provider gerade nicht auf die schlichte Durchleitung beschränken,[69] sondern selber die Informationen[70] mehr oder weniger intensiv verändern (§ 8 Abs. 1 Satz 1 Nr. 3 Alt. 2 TMG und § 9 Satz 1 Nr. 1 TMG im Fall des Umgestaltens zwecks schnellerer Übertragung und gleichzeitigen Cachens), so dass auch die dogmatischen Streitstände hinsichtlich der Einordnung der Verantwortlichkeit[71] nicht relevant werden. Eine Privilegierung setzt in § 8 Abs. 1 Nr. 3 TMG unter anderem (kumulatives Vorliegen von Nr. 1, 2 und 3) voraus, dass der Provider Inhalte in ihrer ursprünglichen Form und in derjenigen Zusammenstellung weitergibt, wie sie vom jeweiligen Nutzer nachgefragt wurden.[72] Soweit es zur Zwischenspeicherung zum Zweck der beschleunigten Übermittlung von Informationen kommt (§ 9 TMG), muss die Integrität der Ursprungsinformation gewährleistet sein, sprich die Kopie muss dem Original entsprechen.[73]

---

[66] Spindler/Schuster/*Eckhardt*, TKG § 88 Rn. 1 ff.

[67] *Rengier*, Strafrecht Besonderer Teil II, 2009, S. 251, 255.

[68] *Joecks*, Strafgesetzbuch – Studienkommentar, 2009, § 303a, Rn. 1; *Eichelberger*, MMR 2004, 595.

[69] Spindler/Schuster/*Zimmermann/Stender-Vorwachs*, Recht der elektronischen Medien, 1. Auflage 2008, TMG § 8 Rn. 58.

[70] Der an der E-Commerce-Richtlinie orientierte Begriff meint alle Daten, die mittels eines Teledienstes übermittelt werden können; vgl. Spindler/Schuster/*Hoffmann*, TMG § 7 Rn. 10.

[71] Vgl. hierzu *Bedner*, JurPC Web-Dok. 94/2007, Abs. 13 ff; http://www.jurpc.de/aufsatz/20070094.htm#u9.

[72] Spindler/Schuster/*Zimmermann/Stender-Vorwachs*, TMG § 8 Rn. 58.

[73] Spindler/Schuster/*Hoffmann*, TMG § 9 Rn. 17.

Zu beachten ist, dass der Begriff der „Veränderung“ im Sinne des TMG nicht mit den Veränderungsbegriffen im BDSG oder dem StGB vergleichbar ist. Eine Veränderung im Sinne von § 8 Abs. 1 Satz 1 Nr. 3 Alt. 2 TMG und § 9 Satz 1 Nr. 1 TMG liegt immer dann vor, wenn der Provider einen Eingriff in die Integrität der übermittelten Informationen vornimmt, wenn also die eingehenden Daten mit den ausgehenden Daten nicht identisch sind.[74] Die Veränderung muss willentlich erfolgen.[75] Beides ist in den folgenden Anwendungsfällen der Fall.

4.2 NETZWERKSICHERHEIT

4.2.1 DATENSCHUTZRECHT

Eingriffe zur Wahrung der Netzwerksicherheit mittels DPI-fähiger Application Layer Firewalls erfolgen auf der Nutzdatenebene, jedoch werden dadurch – bei entsprechender Einstellung – keine personenbezogenen Daten, sondern bekannte Schadroutinen herausgefiltert. Datenschutzrechtlich ist dieser Vorgang auf den ersten Blick unbedenklich. Zu beachten ist jedoch, dass dazu ausnahmslos alle übermittelten Inhalte automatisiert mit den Blacklists gegengeprüft werden müssen. Bei einer solchen Prüfung des gesamten Traffic sind mit an Sicherheit grenzender Wahrscheinlichkeit personenbezogene Daten betroffen.

Sind personenbezogene Daten bei diesem Abgleich involviert, so liegt ein Erheben im Sinne des § 3 Abs. 3 BDSG vor. Erheben ist das Beschaffen von Daten über den Betroffenen. Das Erheben besteht in einer Aktivität, durch die die erhebende Stelle entweder Kenntnis von den betreffenden Daten erhält oder Verfügung über diese begründet.[76] Zusätzlich muss ein willensgetragenes aktives Handeln der handelnden Personen (Mitarbeiter des Providers)[77] gegeben sein, um die Verfügung über personenbezogene Daten zu begründen.[78] Die Alternative der Kenntnisnahme ist beim Einsatz von DPI-Technologie nicht einschlägig, jedoch liegt ein aktives und willentliches Begründen der Verfügung über personenbezogene Daten vor, indem die Datenströme vom Provider willentlich abgezweigt und gezielt und ohne technische Notwendigkeit durch die Application Layer Firewalls (sprich die DPI-Hard- und Software) hindurch geleitet und vollumfänglich gegen die Listen geprüft werden. Dieses durchleuchten mittels DPI-Technologie ist auch für die eigentliche Provideraufgabe der Weiterleitung nicht notwendig. Der Umstand, dass die personenbezogenen Daten nach dem Abgleich mit den Listen unangetastet weitergeleitet werden, ist für die Begründung der Verfügung irrelevant. Im Gegensatz zur Nutzung (siehe sogleich) ist auch die personenbezogene Verwendung keine Voraussetzung der Erhebung. Ebenso irrelevant sind der Anlass der Datenbeschaffung, ihr Zweck und die beabsichtigte oder tatsächliche Verwendung der Informationen.[79] Unerheblich ist es außerdem, ob die beschaffte Information zur Kenntnis genommen oder sonst inhaltlich genutzt werden soll. Es genügt, wenn die Möglichkeit dazu besteht.[80] Providermitarbeiter sind jederzeit in der Lage die zu filternden und die herausgefilterten Daten einzusehen oder inhaltlich zu nutzen.

---

[74] Spindler/Schuster/*Zimmermann/Stender-Vorwachs*, TMG § 8 Rn. 62; BT-Drs. 14/6098, S. 24.

[75] Spindler/Schuster/*Hoffmann*, TMG § 9 Rn. 17.

[76] Simitis/*Dammann*, BDSG, 6. Auflage 2006, § 3 Rn. 102.

[77] Soweit nachfolgend vom „Provider“ oder „Unternehmen“ als Handelnden die Rede ist, sind die gesetzlichen Vertreter oder handelnde Mitarbeiter gemeint.

[78] Simitis/*Dammann*, BDSG, § 3 Rn. 102.

[79] Simitis/*Dammann*, BDSG, § 3 Rn. 105.

[80] Simitis/*Dammann*, BDSG, § 3 Rn. 106.

Hingegen kommt eine datenschutzrechtliche Verarbeitung nicht in Betracht, da die durchlaufenden personenbezogenen Daten nicht den fünf Phasen des § 3 Abs. 4 BDSG unterliegen. Insbesondere liegt durch die Entfernung des Schadcodes keine Veränderung nach § 3 Abs. 4 BDSG Nr. 2 vor, weil die personenbezogenen Daten nicht inhaltlich umgestaltet werden, da sich ihr Informationsgehalt nicht verändert.[81] Im Übrigen sind sie auch nie gespeichert (§ 3 Abs. 4 Nr. 1 BDSG). Auch für eine Nutzung im Sinne des § 3 Abs. 5 BDSG reicht es nicht aus, dass die „vorbeifließenden" personenbezogenen Daten maschinenintern mit den Listen abgeglichen werden. Zum einen stellt dies einen bloßen recheninternen Vorgang dar und zum anderen muss sich die Nutzung auf den Personenbezug erstrecken,[82] was hier eindeutig nicht der Fall ist, da zum einen die zu filternden Schadroutinen keine personenbezogenen Daten darstellen und zum anderen hinsichtlich der „vorbeifließenden" personenbezogenen Daten keine Nutzung des innewohnenden Informationsgehalts erfolgt. Folglich ist auch das Ergebnis, nämlich das Ausfiltern der Routinen, nicht personenbezogen.[83]

Die oben bejahte Erhebung ist aber über § 28 Abs. 1 Nr. 2 BDSG zulässig. Das Interesse des Providers an der Aufrechterhaltung der Netzwerksicherheit durch das Ausfiltern der Malware ist ein überwiegendes berechtigtes Interesse. § 109 Abs. 1 Nr. 2 TKG sieht zudem vor, dass Provider Vorkehrungen treffen müssen, um unerlaubte Zugriffe auf die Providersysteme zu verhindern. Falls Malware auf diese Systeme übergreift, ist die Gefahr der unerlaubten Zugriffe gegeben.

4.2.2 STRAFRECHT

4.2.2.1 § 202A STGB

Die Anwendung des § 202a StGB scheitert an dem Fehlen der Überwindung einer besonderen Sicherung. Soweit eine Datenübermittlung verschlüsselt abläuft, können und wollen die Provider keine Daten abfangen oder verändern, so dass es schon an der Tathandlung fehlt. Der Versuch ist nicht strafbar.[84] Unverschlüsselte Datenübertragung ist nicht von § 202a StGB umfasst, so dass das Ausspähen von unverschlüsselter Kommunikation nach dieser Vorschrift straflos bleibt.

4.2.2.2 § 202B STGB

Es könnte jedoch ein Abfangen von Daten nach § 202b StGB vorliegen. Es müsste sich um ein Verschaffen von Daten aus einer nichtöffentlichen Datenübermittlung unter Anwendung von technischen Hilfsmitteln handeln.

4.2.2.2.1 DATEN

Es ist vorab zu klären, ob Schadcode und Malware Daten im Sinne des § 202a Abs. 2 StGB darstellen. Daten werden als kodierte Informationen verstanden, die für den Menschen nicht unmittelbar wahrnehmbar sind.[85] Diese Informationen werden durch Programmiersprachen wieder wahrnehmbar gemacht, wobei sich die Sprachen über eine festgelegte Zeichenfolge definieren. Die Verwendung solcher sprachlicher Regelwerke

[81] Zum Begriff der Veränderung siehe Simitis/*Dammann*, BDSG, § 3 Rn. 129.

[82] Simitis/*Dammann*, BDSG, § 3 Rn. 189 und 191.

[83] Simitis/*Dammann*, BDSG, § 3 Rn. 191.

[84] Dölling/Duttge/Rössner/*Tag*, Gesamtes Strafrecht, 2008, § 202a Rn. 13; BT-Drs. 16/3656, S. 10.

[85] *Schultz*, MIR 2006, Dok. 180, Rn. 8, mit weiteren Nachweisen.

ermöglicht es, Informationen in Daten zu kodieren und bei Bedarf wieder zu dekodieren.[86] „Malware“ ist ein Kunstwort aus „malicious“ und „Software“. Software besteht immer aus kodierten Informationen, die über Programmiersprachen wahrnehmbar gemacht werden können. Letzterer Wortbestandteil zeigt also, dass alle Formen von Malware Software und damit Daten in diesem Sinne sind. Außerdem kann man auch am Begriff des „*Daten*pakets“ anknüpfen. Bereits der Header eines solchen Pakets enthält Daten, nämlich sogenannte Metadaten, in Form von Ziel- oder Quelladressen, wie man oben sehen konnte. Erst Recht sind also Nutzdaten Daten im Sinne des § 202a Abs. 2 StGB.

Auf die schädliche oder unerwünschte Zielrichtung der Malware kommt es beim Datenbegriff nicht an. Sehr oft werden erst die Kombination von gewissen Informationen und die Wechselwirkung mit den Zielsystemen zu nachteiligen Auswirkungen führen. Die Nachteile beim Provider sind meistens mittelbarer Natur, beispielsweise wenn durch infizierte Kundenrechner (sogenannten „Bots“) übermäßig viel Traffic, zum Beispiel durch Distributed-Denial-of-Service-Angriffe oder übermäßige Versendung von Spammails, generiert wird und dadurch die Funktionsfähigkeit und Nutzbarkeit des Providernetzes beeinträchtigt wird. Im schlimmsten Fall ist jedoch eine unmittelbare Betroffenheit gegeben, wenn die Systeme des Providers mit Malware infiziert werden und er deswegen zur Leistungserbringung nicht mehr oder nur sehr eingeschränkt in der Lage ist.

4.2.2.2.2 (SICH)VERSCHAFFEN

Eine weitere Frage ist, ob ein Herausfiltern, sprich das Nichtweiterleiten des schädlichen Codes zum Kunden, ein (Sich)Verschaffen im Sinne der Vorschrift darstellt. „(Sich)Verschaffen“ suggeriert, dass der Provider die Daten mitschneiden[87] und damit abspeichern müsste. In der Praxis hat er aber kein Interesse am Inhalt der Schadroutinen, da er diese zwingenderweise vorher kennt und außerdem den herausgefilterten Schadcode auch nicht aufzubewahren braucht. Es ist für § 202b StGB indes auch nicht erforderlich, dass er die Daten aufzeichnet oder abspeichert, es reicht nämlich aus, dass er die Herrschaft über die Daten oder die Möglichkeit zur Kenntnisnahme hat.[88] Das ist durch die (wenn auch kurzzeitige) Durchleitung durch die DPI-Hardware und vor allem durch das darauf folgende Herausfiltern mittels einer ALF der Fall. Auch ohne die Verwendung von DPI-Hardware hat der Provider aufgrund der Durchleitung über die eigene Infrastruktur Herrschaft über die Daten, jedoch manifestiert sich durch die Filterung und Verwerfung diese Herrschaft besonders deutlich, da hierdurch dem Kunden aufgrund des gezielten und gewollten Eingreifens des Providers gewisse Daten vorenthalten werden. Ein Mitarbeiter des Providers entscheidet welche Daten gefiltert und verworfen werden und hat – wie oben schon erwähnt – auch die Möglichkeit die herausgefilterten Daten bei Bedarf einzusehen und zu vergleichen, ob die Filterung entsprechend den Vorgaben erfolgt. Die Daten werden demzufolge klassisch „abgefangen“,[89] sprich es wird verhindert, dass sie ihr Ziel erreichen, so wie es die Überschrift des § 202b StGB ausdrückt.

4.2.2.2.3 NICHTÖFFENTLICHE DATENÜBERMITTLUNG

Eine Datenübermittlung, sprich Übertragung von Daten, ist unproblematisch gegeben, schließlich ist dies die ureigene Aufgabe eines Providers.[90] Auslegungsbedürftig ist das Tatbestandsmerkmal der Nichtöffentlichkeit.

---

[86] *Schultz*, MIR 2006, Dok. 180, Rn. 8.

[87] *Schultz*, MIR 2006, Dok. 180, Rn. 22.

[88] *Vassilaki*, CR 2008, 133; *Schumann*, NStZ 2007, 677; BT-Drs 16/3565, 11; *Fischer,* 56. Auflage, StGB § 202b Rn. 5; BeckOK v.Heintschel-Heinegg/*Weidemann,* Stand: 01.03.2009, StGB § 202b Rn. 9.

[89] http://de.thefreedictionary.com/Abfangen.

[90] Vgl. oben.

Dieses ist so zu verstehen, dass an die Allgemeinheit (Broadcast) oder einen größeren Rezipientenkreis gerichtete Datenkommunikation (Multicast), beispielsweise Streams, öffentliche Datenübermittlungen sind, während einzelne bestimmte und gezielte Ende-zu-Ende-Verbindungen nichtöffentlich im Sinne der Vorschrift sind. Es kommt mithin darauf an, ob der Absender die übermittelten Daten für einen erkennbar eingeschränkten Empfängerkreis bestimmt hat.[91] Bei individueller Internetkommunikation ist dies üblicherweise der Fall. Auf die Verschlüsselung der Übertragung kommt es im Übrigen nicht an, da ansonsten vom Gesetzgeber ein dem § 202a StGB ähnlicher Wortlaut gewählt worden wäre („besonders gesichert").[92]

4.2.2.2.4 UNBEFUGT

Der Täter muss unbefugt handeln. Der Begriff weist auf das allgemeine Rechtswidrigkeitsmerkmal hin.[93] Denkbar ist, dass der Provider oder das filternde Unternehmen neben der Funktionsfähigkeit seines Netzes, auch die Kunden vor Schäden durch die Malware bewahren will, so dass eine mutmaßliche Einwilligung zur Filterung in Betracht kommt, soweit nicht bereits über die Zustimmung zu den AGB eine ausdrückliche Einwilligung gegeben ist. Ein Nutzer wird die Malware in den seltensten Fällen willentlich anfordern, sondern eher darauf vertrauen, dass die Daten ohne versteckte Schadsoftware bei ihm ankommen. Gleiches gilt für das Interesse des Kunden an der Nutzung eines funktionstüchtigen Zugangs. Eine mutmaßliche Einwilligung in die Filterung wird also im Regelfall anzunehmen sein, so dass es an der Rechtswidrigkeit fehlt. Ausnahmen sind Nutzer, die gezielt und gewollt Malware und deren Verbreitung analysieren wollen, sprich darauf angewiesen sind, dass die angeforderten Daten mitsamt der Malware übermittelt werden.[94] Allerdings wird dies der große Ausnahmefall sein. Eine spezielle Befugnis zum Ausfiltern von Schadsoftware ergibt sich, wie oben dargestellt, mittelbar aus § 109 Abs. 1 Nr. 2 TKG, soweit die Gefahr besteht, dass die Malware auf die Providersysteme übergreift und dadurch unerlaubte Zugriffe auf die Providersysteme ermöglicht werden.

4.2.2.3 § 303A STGB

Daneben könnte auch § 303a StGB einschlägig sein. Es ist umstritten, ob § 303a StGB nur für physische Datenträger[95] oder auch für Datenübermittlungen gilt. Der Wortlaut enthält keinerlei Beschränkung auf stoffliche Datenträger. Im Gegenteil wird durch den Verweis auf den Datenbegriff in § 202a Abs. 2 StGB auch die dort enthaltene Datenübermittlung in den Tatbestand des § 303a eingeführt. Erfasst werden demzufolge auch Daten in der Übermittlungsphase.[96]

---

[91] BeckOK v.Heintschel-Heinegg/*Weidemann,* StGB § 202b Rn. 6; *Vassilaki,* CR 2008, 132; *Ernst*, NJW 2007, 2662; *Schumann,* NStZ 2007, 677; *Gröseling/Höfinger*, MMR 2007, 552.

[92] BeckOK v.Heintschel-Heinegg/*Weidemann,* StGB § 202b Rn. 6; *Fischer*, StGB § 202b Rn. 4; *Marberth-Kubicki,* ITRB 2008, 17.

[93] *Fischer*, StGB § 202b Rn. 7; *Vassilaki*, CR 2008, 133; ebenso Schönke/Schröder/*Stree*, StGB, 27. Auflage 2006, für das gleichlautende Merkmal in § 202a, dort die Kommentierung zu § 202a Rn. 11.

[94] Denkbar ist, dass ein Nutzer seine lokale Firewall oder Antivirussoftware auf Funktionsfähigkeit testen möchte oder ein Unternehmen das solche Software entwickelt Sammlungen von Signaturen von aktuell umlaufender Malware erstellen will.

[95] So *Fischer*, StGB § 303a Rn. 3.

[96] Ausdrücklich *Lackner/Kühl*, StGB § 303a Rn. 2; *Ernst* NJW 2003, 3237; NK-StGB/*Zaczyk*, 2001, § 303a Rn. 6; Wessels/*Hettinger*, Straftaten gegen Vermögenswerte, Teil 2, 2009, S. 28.

§ 303a StGB pönalisiert in Absatz 1 das Löschen, Unterdrücken, Unbrauchbarmachen und Verändern von Daten. Das Herausfiltern der Malware müsste also unter eine dieser vier Alternativen fallen. Gelöscht werden Daten, wenn sie vollständig und unwiederbringlich unkenntlich gemacht werden, sich also nicht mehr rekonstruieren lassen und damit für immer gänzlich verloren sind.[97] Die Tathandlung entspricht dem Zerstören nach § 303 Abs. 1 StGB.[98] Herausfiltern und Nichtweiterleiten der Daten führt auch dazu, dass sie unkenntlich gemacht werden. Sie kommen niemals beim Berechtigten an und können so auch nicht von diesem zur Kenntnis genommen werden.

In Betracht kommt auch ein Unterdrücken. Unterdrücken bedeutet die Daten dauernd oder auch nur vorübergehend dem Zugriff des Berechtigten zu entziehen und dadurch ihre Verwendbarkeit auszuschließen, wobei auch das Verhindern des Zugangs der Daten erfasst ist.[99] Das Herausfiltern und Nichtweiterleiten der Daten ist eine klassische Verhinderung des Datenzugangs.[100]

Problematisch ist indes, wie oben bereits ausgeführt, dass der verfügungsberechtigte Nutzer die Übermittlung der Malware nicht angefordert hat und die Löschung oder Unterdrückung derselben für ihn zu keinerlei Beeinträchtigung führt. Im Gegenteil, der Normalnutzer wird vor potentiellen Schäden bewahrt. Geschützt ist in § 303a StGB das Interesse des Verfügungsberechtigten an der unversehrten Verwendbarkeit der in den Daten enthaltenen Informationen.[101] An Malware und den für ihn potentiell schädlichen Informationen hat ein Normalnutzer aber kein Interesse. Eine Beeinträchtigung kommt nur in Frage, wenn es Nutzer gibt, die die Malware analysieren wollen. Für die ganz überwiegende Mehrheit der Nutzer dürfte die Filterung folglich eine erwünschte Maßnahme darstellen, so dass es auf die wenigen hypothetischen Ausnahmen der Malwareanalyse nicht mehr ankommt und demzufolge schon an der Tatbestandsmäßigkeit fehlt.

4.2.2.4 § 206 StGB

Folgt man einem Teil der Literatur, so ist auch § 206 Abs. 2 Nr. 2 StGB, das Unterdrücken einer Sendung, einschlägig. Sendungen in diesem Sinne sind nicht nur körperliche Gegenstände, sondern auch Telekommunikation.[102] Ein Unterdrücken ist durch Eingriffe in den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten mittels Telekommunikationsanlagen (vgl. § 3 Nr. 22 TKG) möglich, dies mit dem Ergebnis, dass die zu sendende Nachricht ihr Ziel nicht oder nur noch verstümmelt oder unvollständig erreicht.[103] Das ist – wie oben festgestellt – der Fall. Fraglich ist jedoch, ob die Malware als „Nachricht“ einzuordnen ist. Zwar nimmt die Kommentarliteratur auf die Definition in § 3 Nr. 22 TKG Bezug, ersetzt aber das Wort „Signale“ durch „Nachricht“[104], was angesichts des geschützten Fernmeldegeheimnisses

[97] Schönke/Schröder/*Stree*, StGB § 303a Rn. 4.

[98] BeckOK v.Heintschel-Heinegg/*Weidemann,* StGB § 303a Rn. 8; *Lackner/Kühl*, StGB § 303a Rn. 3.

[99] *Lackner/Kühl*, StGB § 303a Rn. 3; *Hilgendorf*, JuS 1997, 325.

[100] So ist beispielsweise das Filtern von Spammails schon länger als „Unterdrücken“ anerkannt, Wessels/*Hettinger*, S. 28; *Schmidl*, MMR 2005, 346; *Heidrich/Tschoepe*, MMR 2004, 79; *Hoeren*, MMR 2004, 3515.

[101] Wessels/*Hettinger*, S. 27.

[102] Schönke/Schröder/*Lenckner*, StGB § 206 Rn. 20; MünchKommStGB/*Altenhain*, StGB, 1. Auflage 2003, § 206 Rn. 52; *Fischer*, StGB § 206 Rn. 15.

[103] Schönke/Schröder/*Lenckner*, StGB § 206 Rn. 20.

[104] Schönke/Schröder/*Lenckner*, StGB § 206 Rn. 20.

konsequent ist. Letztlich kann die Entscheidung der Frage aber dahinstehen, da in § 206 Abs. 2 ebenfalls die fehlende Befugnis vorausgesetzt wird.

4.3 NETZWERKMANAGEMENT

4.3.1 DATENSCHUTZRECHT

Die Ermittlung der Art des übertragenen Traffic ist datenschutzrechtlich zulässig, soweit die verhaltensbasierte Methode angewendet wird. Sobald Signaturen von Anwendungen mit dem durchlaufenden Traffic und ganz besonders intensiv mit Webtraffic über Port 80[105] gegengeprüft werden, liegt eine datenschutzrechtliche Erhebung vor, weil ebenso wie im Fall der Filterung von Malware über „vorbeifließende" personenbezogene Daten kurzzeitig verfügt wird. Für diesen Abgleich müsste der Provider die Erlaubnis der Betroffenen einholen, was insbesondere bei personenbezogenen Daten Dritter faktisch gar nicht möglich ist. § 28 BDSG scheidet ebenso aus, da die Drosselung zum einen für die Erfüllung des Geschäftszwecks eines Internetproviders nicht notwendig ist und zum anderen die Nr. 1 - 3 nicht einschlägig sind. Das schutzwürdige Interesse (Nr. 2) der Kunden oder Dritter an einem unbeeinflussten Weiterleiten der personenbezogenen Daten ohne automatisierten Abgleich überwiegt das Interesse des Providers den Traffic mit dem Ziel des Einbremsens zu analysieren.

4.3.2 STRAFRECHT

Abhängig vom eingesetzten Drosselungsverfahren liegt möglicherweise eine Strafbarkeit vor.

4.3.2.1 BANDBREITENLIMITIERUNG

Eine Limitierung der Bandbreite allgemein, für gewisse Ports oder bestimmte Dienste, indem der maximal mögliche Datendurchsatz über einen gewissen Zeitraum gezielt gedeckelt wird, ist weder ein Abfangen noch ein Verändern von Daten im Sinne der §§ 202b, 303a StGB oder ein Unterdrücken gemäß § 206 Abs. 2 StGB. Dies allerdings nur unter der Voraussetzung, dass alle Verbindungsversuche erlaubt und die jeweiligen Daten auch tatsächlich durch- und weitergeleitet werden. Die Übertragung erfolgt dann zwar verlangsamt, jedoch bleiben die konkret übertragenen Daten unangetastet. Ein Unterdrücken im Sinne der obigen Definitionen liegt nicht vor, da die Inhalte den Empfänger vollständig erreichen. Bei extremer Drosselung und entsprechend überlanger Dauer des Übermittlungsvorgangs könnte man an eine vorübergehende Entziehung denken, wenn dem Nutzer nicht zumutbar ist tagelang auf den Zugang der Daten zu warten, der ansonsten nur Minuten oder Sekunden dauern würde. Es käme zu einer faktischen Sperrung der Inhalte. Ab welchem zeitlichen Ausmaß oder ab welcher Bandbreiten- oder Geschwindigkeitsreduzierung eine solche faktische Blockade anzusehen ist, ist schwer zu beantworten und eine Frage des Einzelfalls. Insbesondere wäre ein solcher Eingriff vom Nutzer nur schwer zu beweisen, da neben gezielten Geschwindigkeitseingriffen auch die Geschwindigkeit der sendenden Server oder Peers, die Auslastung auf Routen oder physikalische Effekte (Einstrahlungen und Übersprechen) Einfluss haben können. Einige Provider verschleiern daher ihre Eingriffe, indem sie zeitlich und örtlich scheinbar zufällig, tatsächlich aber in Zeiten hoher Auslastung, die Bandbreite reduzieren.

Wird die beim Nutzer verfügbare Bandbreite so stark reduziert, dass angeforderte oder verschickte Daten überhaupt nicht mehr durchgeleitet werden und im Ergebnis eine echte Sperrung entsteht, so ist ein Unterdrücken unproblematisch gegeben.[106]

[105] Vgl. die technische Beschreibung der Anwendungserkennung mittels Signatur.

[106] Dazu unten mehr.

4.3.2.2 GEFÄLSCHTE TCP-RESET-PAKETE („COMCASTMETHODE“)

Die Methode, gefälschte TCP-Resetpakete einzusetzen, ist dagegen anders zu beurteilen.

4.3.2.2.1 § 202B STGB

Ein Verschaffen von Daten liegt nicht vor, da der Provider keine fremden Daten abfängt, sondern eigene gefälschte RST-Pakete an die providerfremden Anschlüsse schickt, die (wie im Fall Comcast über Torrentsoftware) Daten austauschen. Auch die Kenntnisnahme welche konkreten IP-Adressen aus dem jeweiligen Nutzerpool zum aktuellen Zeitpunkt am Filesharing beteiligt sind, ist für § 202b StGB irrelevant, da dieser Umstand providereigene, also für ihn bestimmte, Daten (eigene Nutzer, eigene IP-Adressen) betrifft. Auch die IP-Adressen der providerfremden Nutzer sind für den Provider bestimmte Daten, da er prinzipbedingt nur so die Inhaltsdaten übermitteln kann.

4.3.2.2.2 § 303A STGB

Es liegt jedoch eine Strafbarkeit nach § 303a vor. Als Tathandlungen kommen Unterdrücken, Unbrauchbarmachen und Verändern in Betracht. Durch den Abbruch des Übermittlungsvorgangs aufgrund der gefälschten Resetpakete wird den beteiligten Anschlüssen die vollständige Übersendung der Daten unmöglich gemacht, was ein Unterdrücken darstellt. Wurde nur ein Teil der Daten übertragen, was regelmäßig der Fall ist, da der Reset kurz nach Verbindungsaufbau initiiert wird,[107] liegt auch regelmäßig ein Unbrauchbarmachen von Daten vor, weil die nur teilweise übertragenen Dateien nicht genutzt oder ausgeführt werden können. Unbrauchbar gemacht sind Daten nämlich dann, wenn sie durch zusätzliche Einfügungen oder andere Manipulationen so in ihrer Verwendungsfähigkeit beeinträchtigt sind, dass sie den mit ihnen verbundenen Zweck nicht mehr ordnungsgemäß erfüllen können.[108] Ein Verändern liegt vor, wenn die Teildaten zwar lesbar sind,[109] aber durch die unvollständige Übertragung deren Informationsgehalt oder Aussagewert beeinträchtigt wird.[110]

4.3.2.2.3 § 303B STGB

Falls durch die Eingriffe die Funktionstüchtigkeit der Datenverarbeitung bei einem Wirtschaftsunternehmen oder einer Behörde beeinträchtigt wird, so ist durch die Erfüllung des § 303a StGB auch eine Strafbarkeit nach § 303b Abs. 1 Nr. 1 StGB denkbar. Meist wird es jedoch am hierzu erforderlichen Vorsatz fehlen.

4.3.2.2.4 § 206 STGB

Außerdem liegt ein vorsätzliches Unterdrücken einer Sendung gemäß § 206 Abs. 2 Nr. 2 StGB vor. Die von den Nutzern angeforderten und nur teilweise übertragenen Daten haben einen eigenen Informationsgehalt, so dass sie folglich als „Nachrichten“ einzustufen sind. Zur Verwirklichung des Tatbestands reicht es aus, dass die

[107] Näheres siehe im technischen Teil.

[108] Wessels/*Hettinger*, S. 28.

[109] Beispielsweise einfache unkomprimierte Textdateien.

[110] Wessels/*Hettinger*, S. 28; Schönke/Schröder/*Stree*, StGB § 303a Rn. 4.

Nachricht ihr Ziel nicht oder nur noch verstümmelt oder unvollständig erreicht.[111] Das ist im Fall des TCP-Resets der Fall.

4.4 CONTENTFILTERUNG UND BLOCKIERUNG VON WEBSEITEN

4.4.1 DATENSCHUTZRECHT

Contentfilter arbeiten ebenso wie die Malwarefilter mit Blacklists, so dass ebenfalls alle übermittelten Inhalte automatisiert mit diesen Listen gegengeprüft werden müssen. Es handelt sich mithin um eine Erhebung im obigen Sinne, für die eine Einwilligung notwendig ist.[112]

4.4.2 STRAFRECHT

4.4.2.1 § 202B STGB

Genau wie bei der Malwarefilterung ist das allgemeine Ausfiltern von Daten tatbestandsmäßig. Entscheidend für eine Strafbarkeit ist wiederum das Rechtswidrigkeitsmerkmal der Befugnis. Soweit die Provider im Auftrag Dritter tätig werden, so tun sie dies aufgrund eines Gesetzes, gerichtlichen Urteils oder aufgrund eines Auftrags der Rechteinhaber, so dass hieraus die Befugnis abzuleiten ist. Soweit sie im Eigeninteresse tätig werden, was insbesondere die Fallgruppe der Sperrung von Diensten betrifft, so sollte sich die Befugnis aus dem Vertrag mit dem Kunden ergeben, in dem die Sperrung von gewissen Diensten ausgewiesen ist. Ansonsten wäre eine Strafbarkeit gegeben.

4.4.2.2 § 206 STGB

Gleiches gilt für § 206. Es liegt zwar ein Unterdrücken einer Sendung vor, jedoch ist dieses gerechtfertigt oder rechtfertigbar.

4.4.2.3 § 303A STGB

In Betracht kommt erneut das Unterdrücken von Daten. Wie oben bereits ausgeführt, bedeutet Unterdrücken, dass die Daten dauernd oder vorübergehend dem Zugriff des Berechtigten entzogen werden und dadurch ihre Verwendbarkeit ausgeschlossen wird, wobei auch das Verhindern des Zugangs der Daten erfasst ist.[113] Berechtigter in diesem Sinne ist der Datenabrufende. Wie oben erwähnt, wird durch die Vorschrift das Interesse an der unversehrten Verwendbarkeit der Daten geschützt.[114] Nach herrschender Meinung muss der Berechtigte an den Daten ein unmittelbares Nutzungs- oder Verfügungsrecht haben.[115] Die unmittelbare Nutzungsbefugnis an den Daten ergibt sich zunächst aus dem Vertrag mit dem Provider. Der Provider muss dem Kunden die angeforderten Daten zuleiten. Diese Nutzungsbefugnis des Kunden erstreckt sich jedoch nicht

[111] Schönke/Schröder/*Lenckner*, StGB § 206 Rn. 20; ähnlich, aber nur bei vollständigem Zurückhalten, MünchKommStGB/*Altenhain*, StGB § 206 Rn. 56.

[112] Vergleiche oben die rechtlichen Ausführungen zum Filtern von Malware.

[113] *Lackner/Kühl*, StGB § 303a Rn. 3; *Hilgendorf*, JuS 1997, 325.

[114] Wessels/*Hettinger*, S. 27; MünchKommStGB/*Wieck-Noodt*, StGB § 303a Rn. 2.

[115] MünchKommStGB/*Wieck-Noodt*, StGB § 303a Rn. 3.

auf Daten an denen Dritte (ausschließliche) Rechte haben, so dass das Ausfiltern von rechtlich geschützten Daten (zum Beispiel aus Urheberrecht oder dem Recht am eigenen Bild) schon gar nicht tatbestandsmäßig ist und es folglich auf die Klärung der Frage, ob das Merkmal der Rechtswidrigkeit als Tatbestandsmerkmal[116] oder als allgemeines Deliktsmerkmal[117] anzusehen ist, nicht mehr ankommt.

4.5 UMLEITUNGEN

4.5.1 DATENSCHUTZRECHT

Da keine personenbezogenen Daten, sondern Domains, URLs und Webserver-IP-Adressen übertragen werden und nicht mit dem restlichen Traffic abgeglichen werden, ist dieser Vorgang datenschutzrechtlich unbedenklich.

4.5.2 STRAFRECHT

4.5.2.1 § 202B STGB

Problematisch ist das Tatbestandsmerkmal des (Sich)Verschaffens. Ein (Sich)Verschaffen liegt unter anderem auch vor, wenn übermittelte Daten auf den Rechner des Täters umgeleitet werden.[118] Der Provider erhält die aufzulösende oder nichtexistente Domain, sprich die Daten, in den drei ersten Alternativen, aber freiwillig vom Kunden. Die daran anschließende richtige Vorgehensweise des Providers ist die, Domains mit der richtigen IP-Adresse aufzulösen oder eine Fehlermeldung (bei Nichterreichbarkeit) auszugeben.[119] Gibt der Nameserver dennoch statt der Fehlermeldung oder der richtigen IP-Adresse eine IP des Providers mit einer Suchseite, Stoppschildseite oder Seite mit Einstellungen aus,[120] so geschieht dies innerhalb des Nameservers (Resolvers), so dass es nicht zu einem neuen Verschaffensvorgang kommt.

Anders ist jedoch die Lage in der vierten Alternative. Hierbei werden die DNS-Anfragen, die für den (vom Nutzer eingestellten) providerfremden DNS-Server bestimmt sind, durch den Provider abgefangen und zwecks Beantwortung auf die eigenen DNS-Server des Providers umgeleitet. Nach obiger Definition wird dadurch das Tatbestandsmerkmal des (Sich)Verschaffens erfüllt. Dies geschieht auch mit technischen Mitteln (DPI-Technologie). Problematisch ist indes das Merkmal der Nichtöffentlichkeit. Zwar werden die Domainzuordnungen über DNS-Rootserver der Öffentlichkeit verfügbar gemacht, dennoch ist die individuelle DNS-Abfrage durch einen bestimmten Nutzer als nichtöffentlich anzusehen. Eine Befugnis zur Umleitung ist derzeit (später jedoch möglicherweise aus dem Zugangserschwerungsgesetz) nicht ersichtlich, so dass dieses Vorgehen nach § 202b strafbar ist.

---

[116] *Lackner/Kühl*, StGB § 303a Rn. 4; NK-StGB/*Zaczyk*, 2001, § 303a Rn. 12; Dölling/Duttge/Rössner/*Weiler*, § 303a, Rn. 9; *Hilgendorf*, JuS 1996, 892.

[117] Schönke/Schröder/*Stree*, StGB § 303a Rn. 6; *Fischer*, StGB, § 303a Rn. 13.

[118] *Fischer*, StGB § 202b Rn. 5.

[119] http://tools.ietf.org/html/rfc1034.

[120] Vgl. obige Beispiele.

4.5.2.2 § 303A STGB

Bezüglich der beiden ersten Varianten fehlt es möglicherweise an einer Strafbarkeit nach § 303a StGB wenn man lediglich die einzelnen Übertragungen, die bei einer DNS-Abfrage vorkommen, betrachtet. Die vom Nutzer übermittelten Daten (URLs inklusive der Domains) kommen unverändert an ihrem Ziel, nämlich beim Providernameserver, an. Fraglich ist jedoch, ob die zurückgelieferten (falschen) IP-Adressen oder der Umstand, dass überhaupt eine IP (IP der Suchseite mit Werbung) zurückgeliefert wird, wenn tatsächlich keine Domain existiert, von § 303a umfasst ist. Die Vorschrift erfasst nur existierende Daten. Die Antwortdaten werden jedoch vom Provider erst mit der Beantwortung der Anfrage generiert. Zwar hat der Nutzer ein Interesse an einer wahrheitsgemäßen Beantwortung, jedoch existieren diese „richtigen" Daten nie, so dass sie auch nicht verändert worden sein können. Die generierten Antwortdaten hingegen sind zwar inhaltlich falsch, aber unverändert.

Stellt man hinsichtlich der zweiten Alternative jedoch auf den Gesamtzusammenhang ab, so ist an ein Unbrauchbarmachen der gesendeten Daten zu denken. Unbrauchbarmachen ist gegeben, wenn die Daten in ihrer Gebrauchsfähigkeit derart beeinträchtigt werden, dass sie für ihren bestimmungsgemäßen Zweck nicht mehr genutzt werden können.[121] Die URL samt Domain wird vom Nutzer übermittelt, um mittels der zugewiesenen IP auf die entsprechende Webseite zu gelangen. Dieser Zweck wird vereitelt wenn die Daten nicht zur Auflösung der eigentlichen Ziel-IP verwendet werden, sondern faktisch verworfen werden und stattdessen beim ersten Aufruf immer die IP der Einstellungsseite zurückgegeben wird. Gleiches gilt für die Umleitung der Anfragedaten in der vierten Alternative. Zweck der Abfrage war die Beantwortung durch die providerfremden DNS-Server. Die Erfüllung dieses Zwecks wird durch das Abfangen vereitelt. Die vom Nutzer übermittelten DNS-Anfragedaten werden folglich in ihrer Gebrauchsfähigkeit beeinträchtigt.

Für die erste Alternative ist der Zweck der Weiterleitung kein tauglicher Anknüpfungspunkt. Die falsch eingetippte Webseite existiert nicht, so dass auch kein Interesse an einer ordnungsgemäßen Weiterleitung beeinträchtigt sein kann. Der bestimmungsgemäße „Zweck" der Eingabe nichtexistenter Domains besteht jedoch darin eine Fehlermeldung auszugeben. So stehen auch im RFC 1034[122], der als Standard klassifiziert ist, in Unterpunkt 3.7 die drei möglichen Behandlungsmethoden einer Anfrage: „The response by the name server either answers the question posed in the query, refers the requester to another set of name servers, or signals some error condition". Die Fehlerausgabe ist somit als dritter Punkt ausdrücklich erwähnt. Zwar ist nicht definiert wie ein solcher Fehler auszusehen hat, jedoch dürfte eine mit Werbebannern gefüllte Suchseite dem Kriterium der Fehlersignalisierung nur schwerlich genügen.

In der dritten Variante ist die Datenveränderung klarer. Hierbei werden die IP-Adressen der „gesperrten" Webseiten im Providernameserver gelöscht (§ 303a Abs. 1 Alt. 1 StGB) und durch die IP-Adresse der Stoppseite ersetzt.

4.5.2.3 § 303B STGB

Durch die Erfüllung des § 303a StGB ist ebenfalls eine Strafbarkeit nach § 303b Abs. 1 Nr. 1 StGB denkbar, beispielsweise indem Zweigstellen von Unternehmen nicht mehr im Internet erreichbar sind oder die E-Mail-

[121] BeckOK v.Heintschel-Heinegg/*Weidemann,* StGB § 303a Rn. 11.

[122] http://tools.ietf.org/html/rfc1034.

oder VOIP-Kommunikation durch die DNS-Manipulationen nicht mehr richtig funktioniert.[123] Angesichts der Bekanntheit dieser Folgen ist im Einzelfall zu prüfen, ob bedingter Vorsatz gegeben ist.

4.5.2.4 § 206 STGB

Während in den drei ersten Alternativen die DNS-Anfragen den Provider erreichen und folglich die „Sendungen" ihr Ziel erreichen, wird in der vierten Alternative die Anfrage an den fremden DNS-Server nicht weitergeleitet. Dies stellt unproblematisch ein vorsätzliches Unterdrücken dar. Dieses ist nur gerechtfertigt, wenn ein Gesetz das Vorgehen in der Form vorschreibt.[124] Der ausdrückliche Wille des Nutzers besteht gerade darin, den fremden DNS-Server nutzen zu wollen, so dass auch keine mutmaßliche Einwilligung in die Beantwortung durch einen Providerserver möglich ist.

4.5.2.5 §§ 263, 13 STGB

Ein Betrug durch Unterlassen im Fall der Nichtunterrichtung der Umleitung auf providereigene Suchseiten und der damit einhergehenden Erzeugung von kostenpflichtigem Traffic bei Volumentarifen scheitert jedoch bereits an der hierzu erforderlichen Garantenstellung. Zwar stehen Kunde und Provider in einem Vertragsverhältnis, jedoch reicht dieses alleine nicht aus. Es bedarf eines besonderen Vertrauensverhältnisses. Es müssen besondere vertrauensbildende Umstände hinzukommen, beispielsweise, wenn die Nichtaufklärung einen erheblichen Schaden verursacht oder es einem Vertragspartner erkennbar auf einen Umstand ankommt.[125] Das ist jedoch bei der heutigen Tarifstruktur (im Gegensatz zu früher) und den sich daraus ergebenden geringen Mehrkosten nicht der Fall. Auch wird es einem Kunden darauf nicht ankommen, da er sich ohne negative Vorerfahrungen darüber selten Gedanken machen wird.

4.6 WERBEEINBLENDUNGEN

4.6.1 DATENSCHUTZRECHT

4.6.1.1 PROFILBILDUNG DURCH DAS WERBEUNTERNEHMEN

Das Einblenden von nutzerspezifischer Werbung ist, je nach Ausgestaltung, datenschutzrechtlich[126] relevant. Bei Phorms „Webwise" ist angedacht die Zuordnung der Daten zu einer identifizierbaren Person durch „Anonymisierung" (sog. „Random Digit Number"[127]) zu kappen. Damit würde es am Merkmal der Einzelangaben (§ 3 Abs. 1 BDSG) fehlen. Keine Einzelangaben im Sinne des Gesetzes sind nämlich Angaben, die

123 http://www.zdnet.de/news/digitale_wirtschaft_internet_ebusiness_icann_sicherheitskomitee_verurteilt_dns_sperren_story-39002364-41005634-1.htm.

124 Möglicherweise später im Zugangserschwerungsgesetz.

125 http://www.jurawelt.com/studenten/skripten/strafr/1841.

126 Es wird hierbei unterstellt, dass ein deutscher Provider mit einem Werbeunternehmen kooperiert.

127 Phorm spricht zwar von „random", jedoch ist nur die Erstgenerierung zufällig; die einmal zugeteilte Nummer bleibt für die Zukunft bestehen und wird in einem speziellen Cookie gespeichert, da ansonsten das System nicht funktionieren würde.

sich zwar auf eine einzelne Person beziehen, die jedoch nicht identifizierbar ist.[128] Dem Unternehmen kommt es auch nicht darauf an, dass eine identifizierbare Person gewisse Interessen hat, sondern, dass über den Verlauf mehrerer Surfsessions hinaus bei einer nicht identifizierbaren, aber immer gleichen Person die passende Werbung eingeblendet wird, indem die besuchten Seiten zu vorgegebenen Interessenkategorien zugeordnet werden.[129] Die Profilbildung wäre nach dieser Methode datenschutzrechtlich nicht zu beanstanden, solange sich Provider und Werbeunternehmen an diese Vorgehensweise halten. Man muss sich nämlich immer im Klaren sein, dass das Werbeunternehmen prinzipbedingt vollen Zugriff auf die Inhaltsdaten hat und bei einem Missbrauch derselben faktisch immer einen Personenbezug ohne größeren Aufwand herstellen könnte, so dass auch keine Anonymisierung im Sinne des § 3 Abs. 6 BDSG vorliegt. Für eine Identifizierung reicht es beispielsweise aus, dass ein Nutzer einmalig unverschlüsselt eine E-Mail mit seinem Namen über einen Webmaildienst versendet oder abruft. Durch die fortwährende Speicherung der „Random Digit Number" gilt dies nicht nur für eine einzelne Websession, sondern für den gesamten Zeitraum der Zuteilung der Nummer. Bei, mit Phorm kooperierenden, Providern folglich für die gesamte Zeit des Vertragsverhältnisses.

Soweit es durch die Banner und deren Code zu einer Veränderung der Webseite im Sinne des § 3 Abs. 4 Satz 2 Nr. 2 BDSG kommt, ist diese nur relevant, wenn die Daten der Webseite als personenbezogene Daten anzusehen sind und deren Informationsgehalt durch das inhaltliche Umgestalten geändert wird.

4.6.1.2 WEITERLEITUNG DER DATEN VOM PROVIDER ZUM WERBEUNTERNEHMEN

Hinsichtlich der Weiterleitung der Datenströme durch den Provider an das Werbeunternehmen liegt eine erlaubnispflichtige Übermittlung im Sinne des § 3 Abs. 4 Satz 2 Nr. 3 BDSG (Bekanntgabe der Informationen durch Weitergeben), die auch nicht über § 28 BDSG gerechtfertigt ist, da es hierbei nicht um eine Weiterleitung zwecks Erbringung der eigentlichen Providerleistung (Kunden den Zugang zum Internet zu ermöglichen) geht und auch keine Interessen des Werbeunternehmens schützenswert sind (§ 28 Abs. 2 Nr. 2 BDSG). Hinsichtlich dieser vom Vertragszweck abweichenden Übermittlung müsste der Provider demzufolge die Erlaubnis der Betroffenen einholen.

4.6.2 STRAFRECHT

4.6.2.1 ERFÜLLUNG VON § 202B STGB DURCH DEN PROVIDER

Wegen der Weitergabe der Daten und der Erlaubnis die Daten durch ein Werbeunternehmen zu nutzen liegt das Merkmal des Verschaffens für Dritte vor. Soweit der Kunde nicht hierzu eingewilligt hat, erfolgt dies auch ohne Befugnis.

4.6.2.2 ERFÜLLUNG VON § 202B STGB DURCH DAS WERBEUNTERNEHMEN

Gleiches gilt für das Werbeunternehmen. Das Tatbestandsmerkmal des (Sich)Verschaffens ist erfüllt. Insbesondere reicht es nicht aus, dass der Provider dem Unternehmen die Nutzung der Daten erlaubt, da er nicht berechtigt ist über die von den Kunden übertragenen Daten zu verfügen, soweit diese nicht in die Nutzung und Weitergabe eingewilligt haben.

---

[128] *Gola/Schomerus*, BDSG, § 11 Rn. 9.

[129] Zur genauen Funktionsweise siehe die Animation unter http://www.phorm.com/technology/index.html.

4.6.2.3 § 303A STGB HINSICHTLICH DER VERÄNDERUNG DER WEBSEITEN

Durch die Einfügung von Werbung in den Datenstrom werden im Ergebnis Webseiten ohne Zustimmung der Webseitenbetreiber in ihrem Aussehen verändert. Fraglich ist, ob diese Einfügung von Bannern oder Werbelayern den Sinn- und Informationsgehalt (Aussagewert) der Webseiten verändern und dadurch der ursprüngliche Verwendungszweck beeinträchtigt wird.[130] Eine direkte Änderung des Codes auf dem Server des Webseitenbetreibers erfolgt nicht. Jedoch werden die Daten während der Übertragung zum Abrufenden durch den Provider unter Beteiligung des Werbeunternehmens um den Werbebannercode ergänzt. Für eine Veränderung reicht es aus, wenn es zum Hinzufügen von Daten kommt.[131] Der Informationsgehalt der ursprünglichen Webseite wird dadurch auch geändert, da hierdurch der Eindruck entsteht der Betreiber hätte die Werbung geschaltet, was auch rechtliche Relevanz (Haftung und Informationspflichten) entwickeln kann. Insbesondere können Inhalte ihren Sinngehalt verlieren, wenn gewisse Banner eine Voreingenommenheit (beispielsweise Sponsoring durch eine bestimmte Firma, während sich der Webseitenautor kritisch mit einem Konkurrenzprodukt auseinandersetzt) des Betreibers suggerieren. Nutzt der Webseitenbetreiber nicht zufällig gerade den die Werbung einfügenden Internetprovider, wird er womöglich auch nie von der Manipulation seiner Seite erfahren. Ursprünglich war beispielsweise auch lediglich ein Opt-Out-Verfahren für Webseitenbetreiber durch Phorm angedacht, so dass ein Großteil der Webseitenbetreiber womöglich niemals von der Manipulation erfahren hätte.[132] Ein solches Verändern von Webseiten ist auch rechtswidrig, so dass die daran Beteiligten strafbar sind.

4.6.2.4 § 303B STGB HINSICHTLICH DER VERÄNDERUNG DER WEBSEITEN

Durch die überdeckenden Banner oder Layer kann zum Beispiel der Onlineshop eines Unternehmens beeinträchtigt werden, indem Eingabemasken überdeckt werden oder Hinweise nicht mehr erkennbar sind. Eventualvorsatz bei den Provider- bzw. Werbeunternehmensverantwortlichen ist für eine Strafbarkeit ausreichend.

4.6.3 URHEBERRECHT

Soweit eine Webseite oder Teile davon Werkqualität haben, ist durch die aufgezwungene Einfügung der Werbung an eine Entstellung oder Beeinträchtigung gemäß § 14 UrhG zu denken. Problematisch ist jedoch, dass das Werk an sich auf dem Server des Webseitenanbieters unangetastet bleibt. Die Vorschrift erfasst jedoch über das Merkmal der Beeinträchtigung auch Umfeldeinwirkungen auf das Werk, die es herabsetzen, ohne es selbst zu ändern.[133] Beeinträchtigen bedeutet etwas in seiner Wirkung hemmen, behindern, einschränken sowie etwas schmälern.[134] Durch die Überlagerung mit Werbelayern wird beispielsweise die Sicht auf das Werk erschwert, so dass es zu einer nicht intendierten Wirkung des Werkes kommt und dieser Umstand geeignet ist eine Interessengefährdung im Sinne des § 14 UrhG herbeizuführen.

---

[130] Schönke/Schröder/*Stree*, StGB § 303a Rn. 4.

[131] BeckOK v.Heintschel-Heinegg/*Weidemann,* StGB § 303a Rn. 13; MünchKommStGB/*Wieck-Noodt*, StGB § 303a Rn. 15; Schönke/Schröder/*Stree*, StGB § 303a Rn. 4.

[132] http://blog.pregos.info/2009/04/17/phorm-opt-out-fuer-websitebetreiber, http://www.golem.de/0904/66503.html, http://www.golem.de/0904/66530.html.

[133] Wandtke/Bullinger/*Bullinger*, Urheberrecht 3. Auflage 2009, § 14 Rn. 1.

[134] Wandtke/Bullinger/*Bullinger*, Urheberrecht § 14 Rn. 3.

4.7 MANIPULATION VON WEBINHALTEN ZWECKS EFFIZIENTERER ÜBERTRAGUNG

4.7.1 DATENSCHUTZRECHT

In dieser Konstellation liegt – soweit personenbezogene Daten manipuliert werden – ein Erheben im Sinne des § 3 Abs. 3 BDSG vor, weil durch die Umwandlung im Proxy eine willentliche Verfügung des Providers über die Daten begründet wird, so dass eine Einwilligung der Betroffenen nötig ist. So ist die Kompression eines Bildes, das gleichzeitig ein personenbezogenes Datum darstellt, ein Verfügen hierüber. Durch die optionale Zwischenspeicherung (Caching) ist auch eine Verarbeitung im Sinne einer Speicherung denkbar. Ansonsten ist keine der weiteren Verarbeitungsphasen gemäß § 3 Abs. 4 BDSG einschlägig. Die Nutzung nach Abs. 5 scheitert erneut am Erfordernis der Nutzung mit Personenbezug. Die Daten werden nicht wegen ihres identifizierenden Informationsgehalts genutzt.

Soweit das Interesse des Providers die Kompression einzusetzen das Interesse des Betroffenen am Schutz seiner Daten überwiegt, beispielsweise weil technisch bedingt nur mittels Kompression gewisse Webangebote überhaupt für Kunden einigermaßen nutzbar gemacht werden (beispielsweise der Abruf normaler, vom Anbieter nicht für den Mobilbereich optimierter, Webseiten über GPRS), so kommt erneut § 28 BDSG in Frage. Diese Ermöglichung der Nutzbarkeit und die Reduktion des Datenvolumens (oft einhergehend mit einer Kostenreduktion, falls ein Volumentarif genutzt wird) liegen auch im Interesse des Kunden, was bei der Interessenabwägung ebenfalls einzubeziehen ist.

4.7.2 STRAFRECHT

4.7.2.1 § 202B STGB

Problematisch ist wieder das Merkmal des (Sich)Verschaffens. Nach obiger Definition reicht es aus, dass der Täter eine Kenntnisnahmemöglichkeit hat oder die Herrschaft über die Daten erlangt. Mitarbeiter haben durch den zusätzlichen Proxy eine leichtere Möglichkeit an die Daten zu gelangen. Indes wird im Gegensatz zur Filterung von Malware oder Content nie ein Mitarbeiter Daten überprüfen müssen, so dass zwar eine zusätzliche Möglichkeit zur Kenntnisnahme gegeben ist, eine Kenntnisnahme aber technikbedingt nicht angedacht ist. Die Daten werden automatisiert umgewandelt. Jedoch hat der Provider für die Zeit der Umwandlung – wie oben bereits geschildert – eine zum Normalfall der bloßen Durchleitung erweiterte Herrschaft über die Daten. Soweit nicht eine Befugnis durch Einwilligung des Kunden besteht, ist die Strafbarkeit gemäß § 202b StGB gegeben.

4.7.2.2 § 303A STGB

In Betracht kommt nur die Alternative der Veränderung von Daten. Verändert werden Daten nach obigen Ausführungen, wenn sie einen anderen Informationsgehalt (Aussagewert) erhalten und dadurch der ursprüngliche Verwendungszweck beeinträchtigt wird.[135] Jedoch ändert sich meist nichts am Informationsgehalt und Verwendungszweck der Daten, da diese – wenn auch komprimiert – inhaltlich vollständig übertragen werden. Falls die Kompression den Informationsgehalt ausnahmsweise beeinflusst (zum Beispiel bei den oben erwähnten Ajax-Anwendungen), wird die Tatbestandsmäßigkeit jedoch meist am fehlenden Vorsatz des Providers scheitern. Ein denkbarer Eventualvorsatz wäre zudem nur schwer nachweisbar.

[135] Schönke/Schröder/*Stree*, StGB § 303a Rn. 4.

4.7.2.3 § 206 STGB

In Betracht kommt erneut nur die Tatbestandsalternative des Unterdrückens. Die realen Webseiteninhalte werden durch den Proxyserver zurückgehalten und durch neuzusammengesetzte und komprimierte Inhalte ersetzt. Indes müsste für ein Unterdrücken der Informationsgehalt beeinträchtigt sein. Soweit der Proxy ordnungsgemäß funktioniert, werden die auf der Webseite enthaltenen Informationen möglicherweise in ästhetisch minderer Qualität, aber dennoch vollständig ausgeliefert. Problematisch wird es für den Provider nur, wenn die Informationen nicht beim Kunden ankommen, wie im eben genannten Beispiel der Ajax-Anwendungen. Es stellt sich dann wiederum das eben thematisierte Problem des (Eventual)Vorsatzes.

4.7.3 URHEBERRECHT

4.7.3.1 § 14 URHG

Durch zu starke Kompression von Bilddateien und die teilweise auftretende falsche Zusammensetzung der Webseitenelemente ist erneut eine Entstellung oder Beeinträchtigung denkbar.

4.7.3.2 §§ 16, 106 URHG

Außerdem ist eine unzulässige Vervielfältigung eines Werkes durch die Zwischenschaltung des Proxyservers in Betracht zu ziehen. Fraglich ist insbesondere, ob die Schranke des § 44a UrhG greift. Zwar handelt es sich um eine flüchtige und begleitende Vervielfältigung, jedoch ist ein Performance Enhancing Proxy gerade kein klassischer Cachingproxy. Die Zwischenspeicherung dient in diesem Fall primär der Veränderung der Webseiten. Diese Veränderung ist auch ein wesentlicher Teil eines technischen Verfahrens. Als Zweck der Vervielfältigung kommt die Alternative der Ermöglichung der Übertragung durch einen Vermittler (hier der Provider) in Betracht. Indes wird durch den Proxy die Übermittlung nicht erst ermöglicht, da diese auch ohne Proxy funktioniert. Es soll aber ausreichen das effiziente Funktionieren von Übertragungssystemen zu ermöglichen.[136] Das ist hier der Fall, da durch die Kompression und das Weglassen von Code Bandbreite eingespart wird. Eine Privilegierung greift aber nur, wenn Informationen nicht verändert werden.[137] Allerdings wird in der Literatur darauf hingewiesen, dass Änderungen gecachter Informationen nicht zur Folge haben können, dass der Vorgang als erlaubnispflichtige Vervielfältigung eingeordnet wird.[138] Andererseits soll das Herausfiltern von Werbung, ein Fall, der mit dem hier thematisierten automatisierten Verändern eher vergleichbar ist als mit dem Caching, eine Vervielfältigung nach § 16 darstellen. Vervielfältigungen ohne eigene schöpferische Leistung fallen nämlich unter § 16 und nicht unter § 23 UrhG.[139] Eine unzulässige Vervielfältigung ist somit durch den Einsatz des Proxyservers gegeben. Diese ist gemäß § 106 Abs. 1 UrhG strafbar.

[136] Wandtke/Bullinger/*von Welser*, Urheberrecht § 44a Rn. 9; Erwägungsgrund 33 iVm Art. 5 Abs. 1 Multimedia-Richtlinie.

[137] Wandtke/Bullinger/*von Welser*, Urheberrecht § 44a Rn. 10.

[138] *Hoeren*, MMR 2000, 516; Wandtke/Bullinger/*von Welser*, Urheberrecht § 44a Rn. 11.

[139] Wandtke/Bullinger/*von Welser*, Urheberrecht § 44a Rn. 12.

4.8 BEREITSTELLUNG VON STAATLICHER ÜBERWACHUNGS- UND ZENSURINFRASTRUKTUR

Soweit deutsche Polizeibehörden oder Geheimdienste staatlicherseits mit Hilfe der Provider in den Datenstrom eingreifen, so tun sie dies hoffentlich nur aufgrund eines Gesetzes. So überwachen die deutschen Geheimdienste BND, MAD und Bundes- sowie Landesverfassungsschutzbehörden beispielsweise aufgrund des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G10) unter gewissen speziellen Voraussetzungen den Datenverkehr.[140] Eine zukünftige generelle Überwachung des Internetdatenverkehrs durch den Staat wird von den Regierungsparteien im Koalitionsvertrag abgelehnt.[141]

5 FAZIT

Die Ergebnisse zeigen, dass die geltende Rechtslage kaum mit der technischen Entwicklung Schritt gehalten hat. So sind ungewollte Auswüchse in der Providerbranche nur bedingt rechtlich klar handhab- oder sanktionierbar. Das geltende Recht behandelt derzeit überwiegend die Manipulation von längerfristig aufbewahrten Daten. Dass Daten quasi „on-the-fly“ während einer Übertragung inhaltlich manipuliert werden können, war für den Gesetzgeber jedoch auch nicht unbedingt absehbar.

Auffällig ist außerdem, dass den Kunden durch die Internetprovider entweder gar keine (zum Beispiel beim Netzwerkmanagement) oder nur durch deren aktives Zutun und oft nur im Nachhinein die Wahl gelassen wird, ob sie die angeblichen Verbesserungen implementiert haben wollen. Hier ist zu fordern, dass Provider solche Methoden erst nach der Einholung der Einwilligung einsetzen und vor Abschluss eines Vertrages auf deren Einsatz hinweisen. Zwar sind die deutschen Provider noch nicht so weit gegangen, insbesondere was die verhaltensbasierte Werbung anbelangt, wie die Provider in Nordamerika oder Großbritannien, jedoch ist es sicher nur eine Frage der Zeit, bis auch hierzulande ähnliche Werbefirmen Partner unter den Providern finden. Das Beispiel Phorm zeigt aber auch sehr anschaulich, dass auf Druck der Kunden und nicht zuletzt der EU-Kommission, die Behavioral-Targeting-Technologie mit dem Aufbranden des Protests datenschutzfreundlich ausgestaltet wurde und schließlich der Regelbetrieb aufgrund der fortgesetzten Ablehnung[142] – zumindest vorerst – ausgesetzt wurde.

Für den deutschen und europäischen Gesetzgeber besteht die Notwendigkeit die Regeln der Netzneutralität[143] und des Verbraucher- und Datenschutzes zum einen überhaupt als geltendes Recht auszugestalten und zum anderen vorhandenes Recht, insbesondere den einfachgesetzlichen Schutz des Fernmeldegeheimnisses, zügig an die fortschreitende Technikentwicklung und insbesondere an die bereits vorhandenen höchst intransparenten Echtzeitmanipulationsmöglichkeiten anzupassen. Soweit der Kunde nicht ausdrücklich

[140] Siehe hierzu auch die Einleitung.

[141] http://www.spiegel.de/netzwelt/netzpolitik/0,1518,657486-4,00.html.

[142] Repräsentative Umfragen in den USA zeigen, dass 66% (und nach einer Erklärung der Technologie 86 %) der US-Bevölkerung DPI und personalisierte Werbung ablehnen; siehe hierzu http://www.telecomtv.com/comspace_newsDetail.aspx?n=45633&id=e9381817-0593-417a-8639-c4c53e2a2a10 mit weiteren aufschlussreichen Umfrageergebnissen.

[143] http://www.heise.de/newsticker/meldung/Union-und-FDP-setzen-auf-offene-Standards-und-Open-Source-834219.html; http://www.spiegel.de/netzwelt/netzpolitik/0,1518,657486,00.html; vgl. auch oben das Thema „Netzneutralität“.

zustimmt, sollte der Gesetzgeber durch entsprechende Vorschriften und Sanktionen klarstellen, dass sich Internetprovider auf ihre klassische Aufgabe zu beschränken haben, nämlich die diskriminierungs- und analysefreie Weiterleitung von Datenpaketen. Innerhalb der Datenpakete haben Provider und von diesen beauftragte Drittfirmen – im wahrsten Sinne der Worte – „nichts zu suchen“.