- erschienen in MMR 2015, 8 -

Reto Mantz[*]

Freund oder Feind auf meiner Leitung?

Zur (Un-)Zulässigkeit des Eingriffs in den Datenstrom durch TK-Anbieter mittels Deep Packet Injection

(Internet-)Zugangsanbieter versorgen ihre Kunden mit dem Zugang ins Internet. Der Datenstrom der Nutzer fließt daher zwangsläufig durch ihre Anlagen und Netzwerke. Diese strategisch günstige Stellung wollen manche Anbieter für neue Geschäftsmodelle nutzen. Eine Möglichkeit ist der Eingriff in den Datenstrom der Kunden, u.a. um hier Werbung zu platzieren. Der folgende Beitrag betrachtet die (zivil- und strafrechtliche) Zulässigkeit und Rechtsfolgen solcher Eingriffe in den Datenstrom.[1] Dabei sollen zunächst der technische Hintergrund solcher Eingriffe (II.) und die wegen dieses Vorgehens angestrengten Verfahren gegen die Anbieter (III.) dargestellt werden. Daran schließt sich die rechtliche Analyse insbesondere zur Frage der Haftung des TK-Anbieters (IV.) an.

I. Einleitung

Telekommunikationsdiensteanbieter, die ihren Kunden den Zugang zum Internet verschaffen (im folgenden „TK-Anbieter“ bzw. „Access Provider), sind Vermittler zwischen ihren Kunden und dem Internet. Als Folge der technologischen und ökonomischen Entwicklungen der letzten Jahre bieten sich TK-Anbietern durch ihre Mittlerrolle neue Geschäftsfelder, die ihnen quasi als Nebenprodukt zum Internetzugang zufallen.

So wurde Ende 2012 bekannt, dass der TK-Anbieter Telefónica plante, in Deutschland Standortdaten der eigenen Kunden zu sammeln, zu aggregieren und für Werbezwecke an Dritte zu verkaufen.[2] Während dieses Modell in England bereits in die Tat umgesetzt wurde, nahm Telefónica aufgrund der öffentlichen Entrüstung – und wohl auch, weil dieses Vorgehen wahrscheinlich unzulässig ist – hiervon Abstand.[3]

Ein weiteres Beispiel ist die Praxis einiger TK-Anbieter in den USA, Brasilien und möglicherweise auch Großbritannien, mittels „Deep Packet Injection“[4] in den Datenstrom ihrer Kunden aktiv einzugreifen und dadurch bei ihren Kunden Werbung zu schalten oder Cookies zu platzieren und nebenbei das Surfverhalten ihrer Kunden zu analysieren.[5] Dabei schalteten die TK-Anbieter die Werbung nicht zwangsläufig selbst, sondern arbeiteten hierfür mit Werbenetzwerken oder anderen Unternehmen zusammen. Erst 2014 wurde bekannt, dass auch der amerikanische Access Provider ComCast Hinweise und Werbung in den Datenstrom der Nutzer seiner „XFinity“-WLAN-Hotspots einspeist.[6] Im Zusammenhang mit diesen Eingriffen in den Datenstrom kam es in den USA, Großbritannien und Brasilien zu Verfahren gegen die betroffenen TK-Anbieter. Nicht bekannt ist bisher, ob deutsche TK-Anbieter bereits

---

[*] Dr. jur. Reto Mantz, Dipl.-Inf., Richter, Landgericht Frankfurt am Main.

[1] Alle in den Fußnoten enthaltenen Links wurden am 26.9.2014 zuletzt abgerufen.
[2] Eingehend dazu Mantz, K&R 2013, 7.
[3] Pressemitteilung von Telefónica v. 1.11.2012, http://blog.telefonica.de/2012/11/information-zur-diskussion-rund-um-das-produkt-smart-step.
[4] Zum Begriff unten 2. und 3.
[5] S. dazu *Costa*, Consent in European Data Protection Law, 2013, 288; *Clayton*, The Phorm „Webwise“ System, http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf.
[6] ArsTechnica v. 8.9.2014, http://arstechnica.com/tech-policy/2014/09/why-comcasts-javascript-ad-injections-threaten-security-net-neutrality.

heute ähnlich vorgehen, oder ob sie dies planen. Im Ergebnis kann davon allerdings nur abgeraten werden.

II. (Technischer) Hintergrund

Was war passiert? Verschiedene Nutzer von TK-Anbietern wunderten sich im Jahre 2008, dass beim Surfen im Internet Werbung auf Webseiten angezeigt wurde, auf denen sie diese nicht vermutet hätten, beispielsweise auf den eigentlich werbefreien Produktseiten verschiedener Anbieter. Als sie testweise statt über den eigenen Kabelanschluss die Webseiten über ihr Mobiltelefon abriefen, war die Werbung hingegen nicht zu sehen. Ähnliches passierte im Jahr 2014 Nutzern der „XFinity"-WLAN-Hotspots des amerikanischen Anbieters ComCast.

Zum Verständnis des Vorgangs soll zunächst (vereinfacht) dargestellt werden, wie der Zugang ins Internet üblicherweise hergestellt wird, und welche Rolle der TK-Anbieter hierbei übernimmt.

1. IP und WWW

a. TK-Anbieter als Vermittler

Das Internet wie wir es heute kennen ist ein Netzwerk aus miteinander verbundenen Geräten, die auf Basis verschiedener Protokolle miteinander kommunizieren. Die meisten Geräte sind dabei über Netzwerkkabel miteinander verbunden. Über diese Kabel werden Anfragen und Antworten gesendet. Das dabei am meisten verwendete Protokoll ist TCP/IP. Der wohl am häufigsten genutzte Dienst ist das allgemein bekannte WWW.

Über WWW werden Webseiten im Internet bereitgehalten und können abgefragt werden. So sendet das Endgerät des Nutzers beispielsweise beim Abruf einer Webseite mittels eines Browsers eine Anfrage an einen Server im Internet. Diese Anfrage wird vom Endgerät des Nutzers (i.d.R. über das im Haus liegende Kabel) zu den Anlagen des TK-Anbieters transportiert, der sie „ins Internet" weiterreicht. Dort wird die Anfrage erneut so lange weitergereicht, bis sie beim betroffenen Server ankommt. Der Server antwortet anschließend, indem er die angefragte Webseite, meist eine Datei im sogenannten HTML-Format,[7] an den anfragenden Nutzer „durch das Internet" zurück zum TK-Anbieter und von dort wieder zum Endgerät des Kunden transportiert. Das Endgerät des Kunden zeigt dann die erhaltene Datei im Browser an.

Tatsächlich werden die über das Internet übertragenen Daten i.d.R. jeweils in kleine Pakete aufgeteilt, die sogenannten IP-Pakete. Dabei besteht jedes IP-Paket aus einem sogenannten Header (Kopf), der u.a. Daten zur Adressierung (Absender, Empfänger) enthält, und dem Inhalt (auch „Nutzdaten" oder „Payload" genannt). Ein IP-Paket kann man sich daher ähnlich wie einen Brief vorstellen, wobei der Header den Briefumschlag darstellt. Die oben als Beispiel genannte HTML-Datei wird daher in der Regel auf eine Mehrzahl von IP-Paketen verteilt und auf dem Endgerät des anfordernden Nutzers wieder zusammengesetzt. Die Gesamtheit der von und zum Endgerät bzw. Endnutzer übertragenen Daten wird als „Datenstrom" bezeichnet.

b. Bilder, Werbung und Skripte in Webseiten

[7] Hypertext Markup Language, s. http://de.wikipedia.org/wiki/Html.

Eine Webseite besteht aber i.d.R. nicht nur aus einem HTML-Dokument, sondern enthält z.B. auch Grafiken oder lädt aufgrund von in der Webseite enthaltenen Skripten Inhalte nach. Im Rahmen der Darstellung der vom Webserver übermittelten Webseite fordert der Browser daher diese weiteren Inhalte beim Webserver an. Der oben dargestellte Kommunikationsverlauf wird also – für die weiteren Inhalte – wiederholt. Zu beachten ist, dass solche in die Webseite integrierten anderen Daten nicht zwingend auf demselben Webserver liegen müssen. Sie können auch auf anderen Servern z.B. von Dritten gespeichert sein, wobei der Browser des Endgeräts dann mit diesen Servern bei Dritten eine Verbindung aufbaut.[8]

Werbebanner und Cookies werden sogar in der Regel nicht auf dem Webserver vorgehalten, auf dem die Webseite liegt. Vielmehr enthält die HTML-Datei Anweisungen zum Nachladen von Bannern oder Cookies von einem Werbeanbieter, üblicherweise einem Werbenetzwerk, das auf Basis von bestimmten Algorithmen Werbung z.B. in Form eines Bildes für den Kunden auswählt und überträgt.

Weiter ist wichtig sich zu vergewärtigen, dass immer, wenn ein Dokument von einem Webserver angefordert wird, bestimmte Informationen an den Webserver übertragen werden, nämlich insbesondere die IP-Adresse des anfordernden Endgeräts, Informationen zum System und der sogenannte „Referrer“, also die Adresse derjenigen Seite, von der aus die Seite aufgerufen wurde, oder die auf den angeforderten Inhalt Bezug genommen hat.

2. Deep Packet Inspection

Für die Erfüllung des Zugangsdienstes durch den TK-Anbieter ist es ausreichend, wenn seine Anlagen auf den Header zugreifen. Der Inhalt eines Paketes, der „Payload“, ist hierfür unbedeutend. Man spricht auch davon, dass die Übertragung mittels des Protokolls TCP/IP „inhaltsneutral“ ist.[9] Allerdings sind TK-Anlagen heutzutage so leistungsfähig, dass es ohne Weiteres möglich ist, beim Datentransport auch den Inhalt aller TCP/IP-Pakete zu analysieren. Dieses Verfahren wird „Deep Packet Inspection“ (DPI) genannt. DPI kann beispielsweise genutzt werden, um bestimmte Inhalte zu blockieren oder priorisiert zu behandeln. Beispielsweise haben verschiedene Anbieter in ihren Mobilfunknetzen DPI verwendet, um TCP/IP-basierte Telefongespräche z.B. über Skype zu blockieren, da die Kunden den kostenpflichten Telefondienst des Anbieters nutzen sollten, statt die Gespräche über das Internet abzuwickeln.[10] Es wird zudem vermutet, dass die chinesische Internetzensur mittels auf DPI realisiert wird.[11] Eine solche Verwendung von DPI für Blockaden oder Priorisierungen anhand des Inhalts der Pakete wird teilweise als Verletzung der Netzneutralität angesehen.[12] Dies ist jedoch nicht Gegenstand dieses Beitrages.

3. Eingriff des TK-Anbieters in den Datenstrom = Deep Packet Injection

Bereits im Jahr 2008 wurde bekannt, dass amerikanische und britische TK-Anbieter in den Datenstrom ihrer Kunden eingriffen, indem sie in den Datenstrom des Abrufs einer Webseite zusätzlichen Inhalt einfügt, nämlich Werbebanner oder Cookies eines großen Werbenetzwerks, in den Datenstrom, mit dem eine HTML-Seite transportiert wurde, am Ende ein weiteres Paket mit einem „<script>“-Tag eingefügt wurde, das den Browser des Endnutzers wie oben dargestellt veranlasste, den eingefügten Code auszuführen.[13] Dadurch

---

[8] Eingehend dazu ULD, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook v. 19.8.2011, S. 7 f., https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf.
[9] *Frevert*, MMR 2012, 510, 511; *Görisch*, EuZW 2012, 494, 495 m.w.N.
[10] *Spies/Ufer*, MMR 2010, 13, 16; *Körber*, MMR 2011, 215, 220; *Görisch*, EuZW 2012, 494.
[11] ZD-Aktuell 2012, 03265.
[12] Übersicht der Positionen bei *Frevert*, MMR 2012, 510, 511 ff.
[13] Technische Darstellung und Analyse bei *Topolski*, NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking v. 18.6.2008, http://www.freepress.net/sites/default/files/fp-legacy/NebuAd_Report.pdf.

lud der Browser des Endnutzers entweder weitere Inhalte, z.B. in Form von Bildern oder Werbebannern, oder führte in die HTML-Datei enthaltene Skripte lokal aus. Hierfür werden Werbebanner oder Cookies vom Server des Werbenetzwerks abgerufen. Der Nutzer erhält dadurch Inhalte die gar nicht in die Ursprungswebseite gehörten. Dies ist für den Kunden weder ohne Weiteres erkennbar noch nachvollziehbar oder zu verhindern. Zusätzlich erhält der Server des Werbenetzwerks Informationen über das Endgerät des Nutzers, insbesondere IP-Adresse, Informationen über das Endgerät, aber auch die gerade abgerufene Webseite in Form des „Referrers". Mittels dieser Informationen konnten die Werbeanbieter das Verhalten der Kunden des TK-Anbieters beobachten und analysieren.

Außerdem ist es ohne Weiteres möglich, durch „Deep Packet Injection" unbemerkt auch Schadcode in die HTML-Datei einzufügen, z.B. in Form eines Scripts, das eine Sicherheitslücke des Browsers ausnutzt. Auch wenn man den Werbeanbietern eine solche Absicht nicht unterstellen will, ist festzuhalten, dass die entsprechenden Anlagen beim TK-Anbieter oder beim Werbeanbieter ein attraktives Ziel für Hackerangriffe darstellen, da hier passgenau und praktisch ohne wirksames Gegenmittel des Nutzers Schadcode eingefügt werden kann.[14]

Einzige praktisch wirksame Gegenmaßnahme gegen das dargestellte Verfahren ist die Verschlüsselung des Datenverkehrs, da so dem TK-Anbieter die Einspeisung zusätzlicher Inhalte in den Datenstrom unmöglich gemacht bzw. erheblich erschwert wird. Ob der Server einer angeforderten Webseite allerdings überhaupt verschlüsselten Datenverkehr unterstützt, steht nicht im Einwirkungsbereich des Nutzers. Ruft der Nutzer Webseiten auf, die vom Server nicht verschlüsselt angeboten werden, ist er der „Deep Packet Injection" seines TK-Anbieters schutzlos ausgesetzt.

III. Verfahren gegen TK-Anbieter wegen „Deep Packet Injection"

In den USA sind wegen des oben dargestellten Vorgehens verschiedene Prozesse eingeleitet worden. Klagen gegen den Werbeanbieter NebuAd[15] (sowie die beteiligten TK-Anbieter) endeten mit einem Vergleich zwischen den Klägern und NebuAd[16] und einer Abweisung der Klagen gegen die TK-Anbieter.[17] Als Begründung für die Abweisung wurde angeführt, dass die TK-Anbieter selbst keine Kenntnis von den Daten genommen hätten.[18]
In Großbritannien setzte die British Telecom in den Jahren 2006 und 2007 ein ähnliches Verfahren unter der Bezeichnung „Phorm"[19] ein, ohne seine Nutzer zu informieren oder die entsprechende

[14] Vgl. *Johnson*, The Guardian v. 25.9.2009, http://www.theguardian.com/technology/2009/sep/25/malvertising; Bericht über Werbung auf der Seite der New York Times v. 14.9.2009, http://www.dailyfinance.com/2009/09/14/malvertising-hits-the-new-york-times; hierfür hat sich der Begriff „Malvertising" (zusammengesetzt aus „Malware" und „Advertising") gebildet, s. https://en.wikipedia.org/wiki/Malvertising.
[15] Erläuterung des Verfahrens durch CEO Bob Dyke, http://www.imediaconnection.com/content/18668.asp.
[16] Die zugehörigen Gerichtsdokumente können unter http://www.nebuadsettlement.com/content.aspx?c=4747&sh=1 eingesehen werden.
[17] Technology & Marketing Law Blog v. 19.8.2011, http://blog.ericgoldman.org/archives/2011/08/deep_packet_ins_1.htm.
[18] *Davis*, MediaPost, 30.9.2013, http://www.mediapost.com/publications/article/210309/nebuad-partner-wow-defeats-wiretapping-lawsuit.html.
[19] Eingehend zum technischen Hintergrund von "Phorm" *Clayton*, The Phorm „Webwise" System, http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf.

Einwilligung einzuholen.[20] Verschiedene Beschwerden nahm die EU-Kommission zum Anlass, im Jahr 2009 ein Vertragsverletzungsverfahren gegen Großbritannien wegen unzureichender Umsetzung der EU-Datenschutzrichtlinien 95/46/EG und 2002/58/EG einzuleiten, da das britische Recht den Eingriff in die Kommunikation der Nutzer ohne deren explizite Einwilligung gestattete.[21] Im Jahr 2010 erhob die EU-Kommission Klage vor dem EuGH.[22] Großbritannien änderte in der Folge den „*Regulation of Investigatory Powers Act 2000*" (RIPA) ab und gestaltete das britische Recht insoweit richtlinienkonform. Mit Entscheidung vom 26.1.2012 schloss die EU-Kommission daraufhin das Verfahren.[23]
Das brasilianische Justizministerium wiederum verhängte im Jahr 2014 eine Strafe von 1,6 Mio USD gegen den brasilianischen TK-Anbieter „*Oi*", weil er das Surfverhalten seiner Kunden mittels Deep Packet Injection überwacht und die Daten an die Phorm Inc. verkauft habe.[24]

IV. Rechtliche Analyse

Auch nach deutschem Recht dürfte die oben dargestellte Praxis unter verschiedenen Gesichtspunkten problematisch sein.

Im der folgenden Analyse wird davon ausgegangen, dass das oben dargestellte Verfahren durch TK-Anbieter – wie in den oben dargestellten Fällen „NebuAd" (USA) und „Phorm" (UK, Brasilien) – ohne Wissen und insbesondere ohne explizite Einwilligung des Nutzers durchgeführt wird.[25]

1. Vorüberlegung 1: Schutzbereich von Fernmeldegeheimnis und TK-Datenschutz

§ 88 TKG enthält eine einfachgesetzliche Regelung des in Art. 10 GG geregelten Fernmeldegeheimnisses. Gemäß § 88 Abs. 1 TKG unterliegen dem Fernmeldegeheimnis der Inhalt der Telekommunikation und ihre näheren Umstände. § 88 Abs. 3 TKG verbietet einerseits, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Andererseits stellt § 88 Abs. 3 S. 2 TKG eine strenge Zweckbindung auf.

§§ 91 ff. TKG wiederum enthalten spezielle Regelungen zum Datenschutz in der Telekommunikation.

2. Vorüberlegung 2: Persönlicher Anwendungsbereich

Dem Fernmeldegeheimnis unterliegen nach § 88 Abs. 2 TKG Diensteanbieter, legaldefiniert in § 3 Nr. 6 TKG. Dazu gehören auch Access Provider.[26] Der TK-Datenschutz der §§ 91 ff. TKG findet nach § 91 Abs. 1 TKG Anwendung auf „*Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste in Telekommunikationsnetzen ... erbringen oder an deren Erbringung mitwirken*." Dies trifft hier auf den Anbieter von Internetzugängen ohne Weiteres zu. Die insoweit subsidiären Regelungen des BDSG sind nicht anzuwenden.

---

[20] *Costa*, Consent in European Data Protection Law, 2013, 288.
[21] EU-Kommission, Pressemitteilung v. 14.4.2009 – IP/09/570, http://europa.eu/rapid/press-release_IP-09-570_de.htm.
[22] EU-Kommission, Pressemitteilung v. 30.9.2010 – IP/10/1215, http://europa.eu/rapid/press-release_IP-10-1215_de.htm.
[23] EU-Kommission, Pressemitteilung v. 26.1.2012 – IP 12/60, http://europa.eu/rapid/press-release_IP-12-60_de.htm.
[24] Bloomberg v. 29.7.2014, http://www.bna.com/brazilian-web-provider-n17179893228.
[25] Jedenfalls im Hinblick auf straf-, datenschutz- und vertragsrechtliche Ansprüche könnte die informierte Einwilligung des Nutzers einen hinreichenden Rechtfertigungsgrund darstellen.
[26] BeckTKG-*Geppert/Schütz*, 4. Aufl. 2013, § 88 Rn. 22.

Der in das Verfahren involvierte Werbeanbieter hingegen erbringt weder selbst TK-Dienste, noch wirkt er daran mit. Auf ihn finden daher unmittelbar weder §§ 88 ff., 91 ff. TKG oder § 206 StGB Anwendung. Er unterliegt jedoch den allgemeinen datenschutzrechtlichen Regeln des BDSG.

Im Ergebnis ist daher zu differenzieren zwischen der Haftung des TK-Anbieters auf der einen und der Haftung des Werbeanbieters auf der anderen Seite. Der vorliegende Beitrag beschränkt die Analyse auf die Haftung des TK-Anbieters.

3. Haftung des TK-Anbieters

a. Verletzung des Fernmeldegeheimnisses (§ 206 StGB)

Verletzungen des Fernmeldegeheimnisses aus § 88 TKG sind strafrechtlich nach § 206 StGB sanktioniert. Danach macht sich strafbar, wer als geschäftsmäßiger Anbieter von TK-Diensten unbefugt einer anderen Person Mitteilung über Tatsachen macht, die dem Fernmeldegeheimnis unterliegen.

Wie oben dargestellt, kann die vom TK-Anbieter durchgeführte Deep Packet Injection dazu verwendet werden, dass der Computer des Kunden eine Verbindung zum Server des Werbetreibenden aufbaut. Der Werbetreibende erhält damit Informationen über die Computerausstattung des Kunden, dessen IP-Adresse sowie über die von ihm abgerufene Webseite. Er erhält damit Informationen mindestens über die Umstände der Telekommunikation gemäß § 206 Abs. 5 S. 2 StGB.

Zu beachten ist dabei, dass der TK-Anbieter, sofern er nicht zusätzlich die ihm über den Kunden vorliegenden Daten direkt an den Werbetreibenden übermittelt, im dargestellten Verfahren nicht unmittelbar Mitteilung über dem Fernmeldegeheimnis unterliegende Tatsachen macht. Allerdings veranlasst er durch die Deep Packet Injection den Kunden, dem Werbetreibenden diese Daten (unwissentlich) selbst zur Verfügung zu stellen, indem der Browser eine Verbindung mit dem Server des Werbeanbieters aufbaut. Der Kunde ist dadurch ein unwissendes Werkzeug gegen sich selbst. Die Strafbarkeit der Verantwortlichen des TK-Anbieters ergibt sich daher aus §§ 206 Abs. 1, 25 Abs. 1 S. 2 StGB.

b. Verletzung des TK-Datenschutzes (§§ 91 ff. TKG)

Durch die oben dargestellte technische Konstellation kommt ein Verstoß gegen § 96 Abs. 2 TKG durch unzulässige Erhebung und Verwendung von Verkehrsdaten in Betracht, der nach § 149 Abs. 1 Nr. 16 TKG mit Geldbuße bis zu € 300.000 belegt werden kann. Soweit der TK-Anbieter selbst Daten über das Surfverhalten des Nutzers erhebt, ist ein solcher Verstoß ohne Weiteres gegeben. Aber auch, wenn nur der Werbeanbieter Verkehrsdaten aus der Verbindung erhebt, handelt der TK-Anbieter ordnungswidrig. Denn der TK-Anbieter leistet mit der Durchführung der Deep Packet Injection einen mindestens fördernden Beitrag[27] zur Kenntniserlangung beim Werbeanbieter. Beim TK-Anbieter liegt auch Vorsatz i.S.d. des OWiG bezüglich seiner Mitwirkungshandlung sowie der Erlangung des Werbeanbieters von Verkehrsdaten vor.[28] Nach § 14 Abs. 1 S. 2 OWiG (als Ausdruck des Einheitstäterbegriffs) ist es auch ausreichend, wenn besondere persönliche Merkmale – hier die TK-Anbietereigenschaft – nur bei einem Beteiligten vorliegen.

Eine Übermittlung von Bestandsdaten wie Name, Adresse etc. über den Nutzer an den Werbeanbieter wäre nach § 95 Abs. 1 TKG ebenfalls unzulässig, da sie nicht zur Erfüllung des Vertrages mit dem Nutzer erforderlich ist.

c. Beteiligung an datenschutzrechtlichen Verletzungen des Werbeanbieters

[27] Vgl. BGH NStZ 1985, 165.
[28] Vgl. KK-*Rengier*, OWiG, 4. Aufl. 2014, § 14 Rn. 30 ff.

Wie oben dargestellt, findet das TKG auf den Werbeanbieter keine Anwendung, da er selbst nicht TK-Anbieter ist. Für ihn gelten vielmehr die Regelungen

- 11 -

des BDSG und insbesondere des TMG, da die Schaltung von Werbung im Internet einen Telemediendienst i.S.v. § 1 Abs. 1 TMG darstellt.

Problematisch könnte in diesem Zusammenhang bereits sein, ob der Werbeanbieter überhaupt personenbezogene Daten erhebt. Personenbezogen sind Daten nach § 3 Abs. 1 BDSG, wenn es sich um solche einer bestimmten oder bestimmbaren Person handelt. Bestimmbar ist eine Person, wenn die Daten sich – auch unter Rückgriff auf vorhandenes oder allgemein verfügbares Zusatzwissen – mit nicht unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten Person zuordnen lassen.[29] Diesbezüglich ist seit Jahren im Streit, ob das erforderliche Zusatzwissen irgendjemandem (absoluter Personenbezug) oder der verarbeitenden Stelle selbst (relativer Personenbezug) zur Verfügung stehen muss,[30] wobei erstere Auffassung von den Aufsichtsbehörden vertreten wird,[31] letztere Auffassung aber im Vordringen begriffen ist. Auf den Streit soll hier nicht näher eingegangen werden.

Schließt man sich der – für TK- und Werbeanbieter hier günstigen – Ansicht eines relativen Personenbezuges an, lässt sich die Frage der datenschutzrechtlichen Zulässigkeit letztendlich nicht generell beantworten, da unklar ist, über welche Daten der jeweilige Werbeanbieter im Einzelfall verfügt. In den oben dargestellten Fällen[32] sind durch die TK-Anbieter wohl teilweise auch identifizierende Daten über die Kunden an den Werbeanbieter übermittelt worden, so dass dort ein Personenbezug vorlag. Zu beachten ist weiter, dass sich aus den auflaufenden Verkehrsdaten – ggf. in Verbindung mit allgemein zugänglichem Zusatzwissen – möglicherweise mit aktuellen Datenverarbeitungsmethoden (Stichwort „Big Data“) auf die Person des Nutzers schließen lassen kann. Dabei bietet die IP-Adresse des Nutzers aufgrund des sog. „Geo-Tagging“ bereits einen groben Anhalt für den Standort des Nutzers. Weitere Informationen können ggf. eine engere Eingrenzung und Identifizierung ermöglichen. Ein Personenbezug ist daher abhängig vom Einzelfall zumindest nicht ausgeschlossen. Für den TK-Anbieter bedeutet dies ein erhebliches Risiko, dass die Daten doch dem BDSG unterfallen.[33]

Geht man von einem Personenbezug aus, könnte man an eine Rechtfertigung der Erhebung von Daten durch den Werbeanbieter nach § 15 Abs. 1 TMG denken. Diese ist im Ergebnis aber ausgeschlossen. Nach § 15 Abs. 1 TMG darf der TM-Anbieter personenbezogene Daten erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen. In der vorliegenden Konstellation ist es allerdings äußerst fraglich, ob sich der Werbeanbieter überhaupt auf § 15 Abs. 1 TMG berufen kann. Denn er ist dem Nutzer völlig unbekannt. Es ist dem Nutzer zudem auch unbekannt, dass er überhaupt

---

[29] Simitis-*Dammann*, BDSG, 8. Aufl. 2014, § 3 Rn. 24.
[30] Eingehend LG Berlin ZD 2013, 618; Simitis-*Dammann*, BDSG, 8. Aufl. 2014, § 3 Rn. 32 ff.; zur Auslegung *Breyer*, ZD 2014, 400.
[31] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26./27. 11. 2009 in Stralsund, 1, abrufbar unter: http://www.bfdi.bund.de/ SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/Nov09Reichweitenmessung.pdf?__blob=publicationFile; Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. 28.1.2011, https://www.daten- schutzzentrum.de/ip-adressen; Orientierungshilfe des hessischen Arbeitskreis Medien, Ziff. 3.1, http://www.datenschutz.hessen.de/_old_content/tb31/ k25p03.htm.
[32] Oben III.
[33] Vgl. Simitis-*Dammann*, BDSG, 8. Aufl. 2014, § 3 Rn. 37 f.

den Telemediendienst des Werbeanbieters in Anspruch nimmt. Daher ist schon der Telemediendienst an sich nicht erforderlich. Es ist zwar bei Werbung auch auf normalen Webseiten eher die Ausnahme denn die Regel, dass der Nutzer einsehen kann, zu welchen Werbenetzwerken er Kontakt aufnimmt, er hat aber jedenfalls die Kontrolle darüber, ob er eine Webseite mit Werbung überhaupt ansteuern möchte. Dies ist in der vorliegenden Konstellation nicht der Fall.

Nach § 15 Abs. 3 TMG ist vor diesem Hintergrund auch die Erstellung von Nutzungsprofilen durch den Werbeanbieter unzulässig. Zwar können TM-Anbieter grundsätzlich u.a. zu Zwecken der Werbung Nutzerprofile erstellen, wenn der Nutzer nicht widerspricht und zuvor auf sein Widerspruchsrecht hingewiesen worden ist. Mangels Kenntnis des Nutzers von der Existenz des Werbeanbieters und mangels Hinweises auf das Widerspruchsrecht greift diese Rechtfertigung aber nicht.

Handelt es sich demnach bei den vom Werbeanbieter erhobenen Informationen um personenbezogene Daten, was jedenfalls bei einer seriösen anwaltlichen Beratung nicht ausgeschlossen werden kann, stellt die Erhebung durch den Werbeanbieter ebenso wie die Erstellung von Nutzerprofilen eine Ordnungswidrigkeit nach § 16 Abs. 2 Nr. 4 BDSG dar, die mit Geldbuße bis € 50.000,- geahndet werden kann. An dieser ist der TK-Anbieter unter Zugrundelegung des Einheitstäterbegriffs des § 14 Abs. 1 OWiG beteiligt.

d. Ergebnis

Im Ergebnis besteht für den TK-Anbieter ein erhebliches straf- und ordnungswidrigkeitsrechtliches Risiko.

4. Ansprüche der Wettbewerber

Auf Seiten der Wettbewerber und der durch die Deep Packet Injection betroffenen Webseitenbetreiber kommen insbesondere Ansprüche nach § 44 TKG in Betracht. Denn § 44 TKG schützt nach seinem Wortlaut auch den Wettbewerb.[34]

Wettbewerber i.S.v. § 44 TKG sind Unternehmen, die ihrerseits TK-Dienstleistungen anbieten,[35] wobei hiervon auch Unternehmen erfasst sind, die Telekommunikationsleistungen in irgendeiner Form anbieten.[36] Betroffen ist der Wettbewerber, wenn er TK-Dienstleistungen gleicher oder ähnlicher Art anbietet und dadurch ein wenigstens abstraktes Wettbewerbsverhältnis zum verletzenden Unternehmen besteht.[37] Problematisch könnte jedoch die persönliche Betroffenheit des Wettbewerbers in Form eines Eingriffs in den eingerichteten und ausgeübten Gewerbebetrieb sein. Ausreichend hierfür ist allerdings schon die Möglichkeit eines Wettbewerbsnachteils. Da der TK-Anbieter, ggf. zusammen mit dem Werbetreibenden, u.a. unter Verstoß gegen das Fernmeldegeheimnis Informationen über das (Surf-)Verhalten seiner Kunden erhält, die er analysieren und für weitere (werbliche) Handlungen verwenden kann, ist ein Wettbewerbsvorteil aufgrund überlegenen Wissens jedenfalls möglich.

Inhaltlich muss dem TK-Anbieter die Zuwiderhandlung gegen den Bestimmungskatalog des § 44 Abs. 1 S. 1 TKG vorzuwerfen sein. Dabei ist es ausreichend, wenn er die Zuwiderhandlung nicht selbst durchführt, sondern durch einen Dritten durchführen lässt, oder die Handlung eines Dritten fördert.[38] Dies ist bei der oben dargestellten Verfahrensweise der

---

[34] BeckTKG-*Ditscheid/Rudloff*, 4. Aufl. 2013, § 44 Rn. 4.
[35] BerlinTKG-*Rugullis*, 3. Aufl. 2013, § 44 Rn. 13; BeckTKG-*Ditscheid/Rudloff*, 4. Aufl. 2013, § 44 Rn. 18.
[36] BeckTKG-*Ditscheid/Rudloff*, 4. Aufl. 2013, § 44 Rn. 20.
[37] Arndt/Fetzer/Scherer-*Kessel*, TKG, 2008, § 44 Rn. 13; BeckTKG-*Ditscheid/Rudloff*, 4. Aufl. 2013, § 44 Rn. 19.
[38] BeckTKG-*Ditscheid/Rudloff*, 4. Aufl. 2013, § 44 Rn. 14 m.w.N.

Fall, da ein Verstoß gegen §§ 88, 91 ff. TKG vorliegt. Ausreichend ist im Übrigen auch, wenn eine solche Zuwiderhandlung nur droht, § 44 Abs. 1 S. 2 TKG. Dies könnte bspw. bereits der Fall sein, wenn einer der in Deutschland tätigen Anbieter die Einrichtung einer „Deep Packet Injection“ ernsthaft ankündigt.[39]

Als Rechtsfolge sieht § 44 Abs. 1 TKG zunächst Beseitigung und Unterlassung vor. Der TK-Anbieter müsste dementsprechend

- 12 -

die Deep Packet Injection einstellen. Dabei kann der Wettbewerber auch im Wege des einstweiligen Rechtsschutzes gegen den TK-Anbieter vorgehen.

Entsprechend § 44 Abs. 1 S. 4 TKG ist der TK-Anbieter zusätzlich zu Schadensersatz verpflichtet, wenn ihm schuldhaftes Verhalten vorzuwerfen ist. Letzteres ist bei „Deep Packet Injection“ der Fall. Problematisch ist diesbezüglich allerdings die Bezifferung des konkreten Schadens beim Wettbewerber. Auch der Vortrag von Schätzgrundlagen i.S.v. § 287 ZPO dürfte den Wettbewerber vor Schwierigkeiten stellen.

Neben § 44 TKG können Wettbewerber Ansprüche auf Beseitigung, Unterlassung und Schadensersatz auch nach §§ 8, 9, 4 Nr. 11 UWG geltend machen. Diese Ansprüche stehen neben § 44 TKG.[40] Die hier in Rede stehenden Normen des TKG dürften auch Marktverhaltensregeln darstellen, wobei auf den Streit, ob Datenschutzbestimmungen generell als Marktverhaltensregeln einzustufen sind, hier nicht eingegangen werden soll.[41]

5. Ansprüche der Endnutzer

Auch Endnutzer können Ansprüche gegen den TK-Anbieter erheben.

a. § 44 TKG

Zunächst können Endnutzer nach § 44 Abs. 1, 2 TKG Beseitigung, Unterlassung und Schadensersatz verlangen. Dabei sind die Endnutzer durch den unzulässigen Eingriff in ihren Datenstrom jedenfalls beeinträchtigt gemäß § 44 Abs. 1 S. 3 TKG und damit Betroffene i.S.d. Norm.

An Schadensersatz ist insbesondere aufgrund des Eingriffs in das allgemeine Persönlichkeitsrecht der Endnutzer insbesondere durch Erhebung und ggf. Analyse der Umstände der Telekommunikation, speziell der Adressen der angesurften Webseiten, zu denken. Die Rechtsprechung erkennt für Verletzungen des allgemeinen Persönlichkeitsrechts grundsätzlich auch Schadensersatz zu.[42] Bei der Bemessung der Höhe eines Schadensersatz kann hier insbesondere Berücksichtigung finden, wie lange der TK- bzw. Werbeanbieter Daten erhoben hat, da sich die Intensität bei der Überwachung des Surfverhaltens mit zunehmender Dauer steigert.

Sollte z.B. durch eine Sicherheitslücke beim Werbeanbieter Schadcode auf dem Endgerät des Kunden ausgeführt worden sein, wären jedenfalls Reparatur- bzw. Behebungskosten

---

[39] Vgl. Arndt/Fetzer/Scherer-*Kessel*, TKG, 2008, § 44 Rn. 41.

[40] OLG Düsseldorf GRUR-RR 2014, 311 (314); BeckTKG-*Ditscheid/Rudloff*, 4. Aufl. 2013, § 44 Rn. 4; BerlinTKG-*Rugullis*, 3. Aufl. 2013, § 44 Rn. 39; Arndt/Fetzer/Scherer-*Kessel*, TKG, 2008, § 44 Rn. 41; a.A. Ohly/Sosnitza-*Ohly*, UWG, 6. Aufl. 2014, § 4 Rn. 11/10; Köhler/Bornkamm-*Köhler*, 32. Aufl. 2014, § 4 Rn 11.14a.

[41] Dazu OLG Karlsruhe NJW 2012, 3312; OLG Hamburg ZD 2013, 511; OLG Köln NJW 2014, 1820; Köhler/Bornkamm-*Köhler*, UWG, 32. Aufl. 2014, § 4 Rn. 11.42 m.w.N.

[42] Vgl. Palandt-*Grüneberg*, BGB, 73. Aufl. 2014, § 253 Rn. 10 m.w.N.

ersatzfähig. Aufgrund der Darlegungs- und Beweislast des Endnutzers wird hier allerdings der Nachweis der Kausalität schwer fallen.[43]

b. Vertragsrechtliche Ansprüche der Nutzer

„Deep Packet Injection" stellt auch eine Verletzung des als Dienstvertrag nach § 611 BGB einzuordnenden[44] Vertrages seitens des Anbieters dar. Denn die Achtung des Fernmeldegeheimnisses durch den TK-Anbieter dürfte auch wesentlicher Gegenstand des Vertrages sein. Dementsprechend kann der Nutzer vertragliche Ansprüche geltend machen. Er kann dementsprechend den Vertrag kündigen, die Vergütung mindern und Schadensersatz verlangen.

c. Deliktische Ansprüche, § 1004 BGB

Aufgrund der Verletzung seines allgemeinen Persönlichkeitsrechts kann der Endnutzer nach § 823 Abs. 1 BGB, wegen der Verletzung von Schutzgesetzen, insbesondere § 206 StGB und §§ 91 ff. TKG, auch nach § 823 Abs. 2 BGB Schadensersatz verlangen. Ferner kann er nach § 1004 BGB Unterlassung fordern.

d. Auskunft

Letztlich stehen dem Endnutzer Ansprüche auf Auskunft aus Vertrag sowie aus § 34 BDSG zu. Dabei ist § 34 BDSG gemäß § 93 Abs. 1 S. 4 TKG ausdrücklich nicht gesperrt.

6. Ansprüche der Webseitenbetreiber

Betroffen von der „Deep Packet Injection" sind neben den Endnutzern auch die Betreiber derjenigen Webseiten, die durch die Nutzer des TK-Anbieters angesurft wurden, und in deren Webseite Code injiziert wurde.

Die Injektion von Daten in den Datenstrom (und damit implizit die Webseite) ist als Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb des Webseitenbetreibers anzusehen. Denn die eingespielten Inhalte oder Codes werden aus Sicht des Endnutzers jedenfalls dem Webseitenbetreiber zugerechnet. Handelt es sich bei dem injizierten Code um Werbung, wird zudem in das Recht des Webseitenbetreibers eingegriffen, auf seiner Webseite allein zu entscheiden, ob und welche Werbung geschaltet werden soll. Der Webseitenbetreiber kann daher nach §§ 823 Abs. 1, 1004 BGB Schadensersatz und Unterlassung verlangen.

Handelt es sich bei dem eingespeisten Code um Werbung, können Ansprüche auch auf §§ 8, 9, 4 Nr. 10 UWG gestützt werden. Denn durch die Einspeisung von Werbung in die Webseite wird die vom Webseitenbetreiber möglicherweise selbst geschaltete Werbung in ihrer Effektivität beeinträchtigt. Auch wenn der Webseitenbetreiber keine Werbung schaltet, fällt die eingespeiste Werbung auf ihn zurück und setzt die Attraktivität und Effektivität seiner Webseite herab. Im Ergebnis liegt eine Wettbewerbsbehinderung i.S.v. § 4 Nr. 10 UWG vor. Problematisch könnte lediglich sein, die eigene Betroffenheit darzulegen und zu beweisen. Denn die lediglich theoretische Möglichkeit, dass die eigene Webseite von einem Kunden des Anspruchsgegners angesurft wird, dürfte nicht ausreichen. Allerdings dürfte es für den Webseitenbetreiber nicht allzu schwer sein, eine konkrete Verletzung (ähnlich einem Lockvogelkauf) durch einen Kunden des TK-Anbieters festzustellen, zu dokumentieren und konkret darzulegen.

---

[43] Zur Frage eines eventuellen Mitverschuldens bei fehlendem Selbstschutz gegen Viren etc. *Mantz*, K&R 2007, 566.

[44] BGH NJW 2005, 2076.

Auf § 44 TKG können Ansprüche hingegen nicht gestützt werden, da die Webseitenanbieter keine Wettbewerber i.S.d. § 44 Abs. 1 TKG sind.[45] Das Angebot einer Webseite für sich ist ein Telemedien- und kein Telekommunikationsdienst.

Auch Ansprüche nach § 823 Abs. 2 BGB dürften nicht gegeben sein. Zwar stellen die hier verletzten Gesetze des StGB und des TKG Schutzgesetze i.S.d. § 823 Abs. 2 BGB dar,[46] Rechtsgutinhaber ist hier jedoch jeweils der Endnutzer, nicht der Webseitenbetreiber.

7. Ansprüche der Verbraucherschutzverbände

Nach § 44 Abs. 2 TKG können auch die nach § 3 UKlaG berechtigten Stellen Ansprüche gegen den TK-Anbieter erheben. Dabei

- 13 -

stellen §§ 88 ff. und §§ 91 ff. TKG auch verbraucherschützende Vorschriften i.S.d. § 44 Abs. 2 S. 1 TKG dar.[47]

V. Einwilligung als Rechtfertigung

Grundsätzlich kann der Endnutzer in Eingriffe nach § 206 StGB, §§ 88 ff., 91 ff. TKG einwilligen.[48] Erforderlich ist jedenfalls – wie bei § 4a BDSG – eine informierte Einwilligung.[49] In Anbetracht der erheblichen Intensität des Eingriffs und dessen starken Überraschungsfaktors ist allerdings äußerst fraglich, ob eine solche Einwilligung mittels AGB oder Datenschutzrichtlinie erteilt werden kann. Zusätzlich dürfte die Einwilligung des Endkunden allein kaum reichen, da nach wohl h.M. alle an der Kommunikation beteiligten Personen ihre Einwilligung erteilen müssen.[50] Dementsprechend wäre auch die Einwilligung der Webseitenbetreiber als Gegenstationen der Kommunikationsvorgänge erforderlich.

Selbst wenn man davon ausgeht, dass allein die Einwilligung des Endnutzers ausreichend sein sollte, sieht sich der TK-Anbieter dennoch den oben dargestellten Ansprüchen der Wettbewerber aufgrund des Eingriffs in deren eingerichteten und ausgeübten Gewerbebetrieb ausgesetzt. In diese Verletzungen können die Endnutzer nicht wirksam einwilligen.

VI. Fazit

Das Ergebnis könnte eindeutiger kaum sein: Deep Packet Injection stellt ohne wirksame Einwilligung einen eindeutig unzulässigen Eingriff in das Fernmeldegeheimnis dar, der für die Verantwortlichen strafrechtliche Folgen haben kann. Da durch die Deep Packet Injection jedenfalls Verkehrsdaten erhoben werden, liegt auch ein Verstoß gegen die Regelungen des TK-Datenschutzes vor. In Betracht kommen zusätzlich Verstöße gegen die Datenschutzvorschriften des TMG, wenn die Daten beim Werbeanbieter Personenbezug aufweisen. Für die Datenschutzverletzungen ist der TK-Anbieter ordnungswidrigkeitsrechtlich verantwortlich und muss mit der Auferlegung entsprechender Strafen durch die Bundesnetzagentur rechnen.

---

[45] Anderes gilt natürlich für Webseiten von TK-Anbietern, die auch ohne Berücksichtigung ihrer Webseite als Wettbewerber anzusehen sind, für diese s. unter IV.4.
[46] Zu Datenschutzrechtsnormen als Schutzgesetz OLG Hamburg GRUR-RR 2012, 40; LG Gera MMR 2011, 282.
[47] BeckTKG-*Ditscheid/Rudloff*, 4. Aufl. 2013, § 44 Rn. 62.
[48] Schönke/Schröder-Lenckner/Eisele, KK-StGB, 29. Aufl. 2014, § 206 Rn. 11; BeckTKG-*Bock*, 4. Aufl. 2013, § 88 Rn. 44.
[49] BeckTKG-*Bock*, 4. Aufl. 2013, § 88 Rn. 44.
[50] BeckTKG-*Bock*, 4. Aufl. 2013, § 88 Rn. 44 m.w.N.

Zusätzlich sieht sich der TK-Anbieter Ansprüchen seiner Kunden und Wettbewerber sowie der Verbraucherschutzverbände auf Beseitigung, Unterlassung und Schadensersatz ausgesetzt. Auch betroffene Webseitenbetreiber können erfolgreich Ansprüche erheben.

Von solchen Eingriffen in den Datenstrom ist daher aus rechtlichen Gründen insgesamt dringend abzuraten. Auch unter Berücksichtigung der öffentlichen Meinung ist der Einsatz von Deep Packet Injection keine gute Idee, wie die öffentlichen Diskussion um den Verkauf von TK-Daten an Werbeanbieter im Jahr 2012 nachdrücklich gezeigt haben. Da bisher Versuche, Deep Packet Injection einzusetzen noch nicht bekannt geworden sind, haben die hiesigen TK-Anbieter möglicherweise bereits erkannt, dass nicht alles, was wirtschaftlich sinnvoll erscheinen mag, auch erlaubt und empfehlenswert ist. Interessant ist dennoch, dass die strenge gesetzliche Regulierung im TKG neuen technischen Bedrohungen wie der Deep Packet Injection gut und effektiv entgegen zu wirken vermag.