WILDE BEUGER SOLMECKE
RECHTSANWÄLTE

WILDE BEUGER SOLMECKE Kaiser-Wilhelm-Ring 27 -29, 50672 Köln

Rafaela Wilde
Michael Beuger
Christian Solmecke LL.M.
Nicola Simon
Fachanwältin f. Arbeitsrecht
Otto Freiherr Grote
Kilian Kost
Frank Fischer
Jennifer Hannemann
Matthias Besenthal LL.M.
Dr. Eva-Maria Brus
Agnieszka Slusarczyk

Steganos Software GmbH
Herrn Gabriel Yoran
Monbijouplatz 5
10178 Berlin

Per Email: gabriel.yoran@steganos.com

Köln, 24.05.2012

Aktenzeichen:	3076/12 sd	Rechtsanwalt:	Kilian Kost
Sekretariat:	Sabrina Daßler	Telefon:	0221 951563-58

Gutachten

1. Aktueller Stand der Vorratsdatenspeicherung (rechtlich / politisch) in Deutschland / auf EU-Ebene. Wie ist der diesbezügliche Stand in der Schweiz, in Dubai, Malta sowie den Seychellen?

EU-Ebene:

Auf EU-Ebene wurde am 15. 3. 2006 die Richtlinie zur Vorratsdatenspeicherung (2006/24/EG) erlassen. Danach sind IP-Adressen für eine Dauer von mindestens 6 Monaten anlasslos zu speichern. Die EU-Kommission hat letztes Jahr aufgrund der Nichtumsetzung der Richtlinie die ersten Stufen eines Vertragsverletzungsverfahrens gegen Deutschland eingeleitet. Eine Klage gegen Deutschland vor dem EuGH wird noch in diesem Monat erwartet. Allerdings wird es, wie jetzt bekannt wurde, keine pauschalen Strafzahlungen für die Vergangenheit geben. Hierdurch wird der

Postfach 19 04 23
50501 Köln

Gerichtsfach K 1581

Tel. 0221 951563-0
Fax 0221 67789727
www.wbs-law.de
info@wbs-law.de

Druck auf die Bundesregierung, möglichst schnell eine Neuregelung des Gesetzes herbeizuführen, erheblich abgeschwächt. Beobachter rechnen nicht damit, dass die Vorratsdatenspeicherung noch in dieser Legislaturperiode beschlossen wird.

Die Richtlinie zur Vorratsdatenspeicherung ist auch auf EU-Ebene umstritten. Derzeit wird an einer Reform gearbeitet, die jedoch inhaltlich kaum Änderungen bringen dürfte. Auch der EuGH prüft auf Veranlassung des höchsten irischen Gerichts die Vereinbarkeit der Richtlinie mit der EU-Grundrechte Charta.

Deutschland:

Das Gesetz zur Regelung der Vorratsdatenspeicherung (§§ 113 a, b TKG; § 100 g StPO) wurde vom Bundesverfassungsgericht (Urteil vom 2. 3. 2010 - 1 BvR 256/08) für verfassungswidrig erklärt. Somit ist auch die Regelung des § 113 a Abs. 6 TKG, der die Speicherungspflicht von Anonymisierungsdiensten regelt, nichtig. Das BVerfG hält die Vorratsdatenspeicherung in der Ausgestaltung, wie sie von der EU-Richtlinie vorgegeben ist, jedoch nicht per se für mit dem Grundgesetz unvereinbar. Daher bemüht sich der Gesetzgeber jetzt, die Vorratsdatenspeicherung so umzusetzen, dass sie sowohl den Vorgaben des BVerfG als auch denen der EU-Richtlinie genügt.
In der Koalition herrscht derzeit noch Streit darüber, wie eine solche Umsetzung aussehen soll. Bundesinnenminister Friedrich spricht sich für eine 1:1 Umsetzung der EU-Richtlinie aus. Falls die Richtlinie nach der Umsetzung in deutsches Recht geändert wird, will er eine sofortige Anpassung des deutschen Rechts vornehmen. Bundesjustizministerin Leutheusser-Schnarrenberger spricht sich dagegen für das sog. „Quick-Freeze-Modell" aus. Danach sollen die Daten auf einer ersten Stufe bei konkretem Verdacht einer Straftat eingefroren werden. Auf der zweiten Stufe wird ein Zugriff auf die Daten nach richterlicher Anordnung möglich.

Aufgrund der bestehenden Uneinigkeit über die konkrete Ausgestaltung und der Abschwächung des Zeitdrucks aus Brüssel ist das Thema Vorratsdatenspeicherung voraussichtlich bis September 2013 vom Tisch.

Schweiz:

In der Schweiz gibt es seit 2002 ein Gesetz zur Vorratsdatenspeicherung (Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)). Danach müssen die Daten 6 Monate gespeichert werden. Insofern ist die Schweiz als Standort nicht attraktiv.

Dubai:

Soweit bekannt und ersichtlich, besteht hier keine gesetzliche Regelung zur Vorratsdatenspeicherung.

Malta:

In Malta besteht eine 12-monatige Speicherfrist. Als Standort daher auch unattraktiv.

Seychellen:

Soweit bekannt und ersichtlich, besteht hier keine gesetzliche Regelung zur Vorratsdatenspeicherung.

2. Ist unsere Mandantin mit den von ihr hier angebotenen Produkten Access- oder Contentprovider?

a. Einordnung des Dienstes als Telekommunikations- oder Telemediendienstes

Diese Frage stellt sich nur, wenn der Dienst überhaupt als Telemediendienst i.S.d. TMG zu qualifizieren ist. An dieser Stelle ist eine Abgrenzung zu Telekommunikationsdiensten erforderlich.

Teilweise wird eine Schwerpunktbetrachtung vorgenommen und auf den überwiegenden Leistungsteil des Anonymisierungsdienstes abgestellt. Dies führt zu dem Ergebnis, dass Anonymisierungsdienste als Telekommunikationsdienste einzuordnen sind (Schmitz, in: Hoeren/Sieber, Multimedia-Recht, Teil 16 Rn. 69; Spindler/Nink, in: Spindler Schuster, Recht der elektronischen Medien, § 13 TMG Rn. 14a). Grund dafür ist, dass die maßgebliche Funktion eines Anonymisierungsdienstes darin liegt, Informationen durchzuleiten. Inhaltsbezogene Dienste werden durch den Anbieter selbst nicht erbracht.

Überwiegend werden Anonymisierungsdienste jedoch als Dienste mit Doppelnatur bezeichnet (Redeker, IT-Recht, Teil D, Rn. 1186; BT-Drucksache 16/5846, S. 72; ähnlich auch Schmitz, in: Hoeren/Sieber, Multimedia-Recht, Teil 16 Rn. 68). Dabei wird eine technisch-funktionale Abgrenzung zwischen den Regelungsbereichen des TKG und denen des TMG vorgenommen (Rau/Behrens, K&R 2009, 766, 768; Raabe, CR 2003, 268). Die Durchleitung der Information wird dabei als Telekommunikation, die Anonymisierungsfunktion selbst als Telemedium eingeordnet (BT-Drucksache 16/5846, S. 72).

Diese Auslegung kommt auch in den Gesetzesbegründung der für verfassungswidrig erklärten Regelung des § 113 a Abs. 6 TKG zum Ausdruck. Zwar spricht das Gesetz an dieser Stelle nur von Telekommunikationsdiensten (*„Wer Telekommunikationsdienste erbringt und hierbei die nach Maßgabe dieser Vorschrift zu speichernden Angaben verändert…“*), jedoch können auch Dienste mit Doppelnatur hierunter fallen. In der Gesetzesbegründung heißt es an dieser Stelle:

> *„Soweit eine Speicherungsverpflichtung danach auch für die Anbieter von Anonymisierungsdiensten begründet wird, ist zu berücksichtigen,*

dass auch diese Anbieter öffentlich zugängliche Telekommunikationsdienste erbringen. (…)

Nach § 3 Nr. 24 TKG fallen darunter die „reinen" Telekommunikationsdienste (also Dienste, die ausschließlich in der Übertragung von Signalen über Telekommunikationsnetze bestehen) sowie Dienste mit Doppelnatur, die zwar auch unter den Rechtsrahmen für Telemedien fallen, aber zugleich Telekommunikationsdienste nach § 3 Nr. 24 TKG sind, weil sie überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen. Dies sind in erster Linie diejenigen Dienste, die sowohl der Bereitstellung eines Internetzugangs als auch der Übertragung elektronischer Post dienen. Auch Anonymisierungsdienste weisen allerdings eine solche Doppelnatur auf, da ihre Tätigkeit sowohl in der Durchleitung der Nachricht als auch in der Ersetzung der Ausgangskennung des Telekommunikationsnutzers besteht. Diese Dienste sind daher sowohl Telemedien als auch – im Hinblick auf ihre Transportfunktion – Telekommunikationsdienste für die Öffentlichkeit"

Es ist daher davon auszugehen, dass die Übermittlung der Informationen als Telekommunikation, die Anonymisierungsfunktion selbst als Telemedium zu qualifizieren ist.

b. Einordnung als Content- oder Accesprovider

Soweit man davon ausgeht, dass im Hinblick auf die Anonymisierungsfunktion das TMG zur Anwendung gelangt, stellt sich die Frage, welchem Providertyp der angebotene Dienst zuzuordnen ist.

Unter § 8 TMG ist ein Diensteanbieter dann zu subsumieren, wenn er fremde Informationen in einem Kommunikationsnetz übermittelt oder den Zugang zur Nutzung dieser Informationen vermittelt. Ein Contentprovider

i.S.d. § 7 Abs. 1 S. 1 TMG hält dagegen eigene Informationen zur Nutzung bereit.

Der Dienst Internet Anonym und der geplante Dienst zur Umgehung von Proxy-/Geo-Sperren sind danach unter § 8 TMG zu subsumieren. Es werden zu keinem Zeitpunkt eigene Informationen zur Nutzung bereitgehalten. Vielmehr steuern die Produkte den Weg der Datenpakete vom Absender zum Empfänger, sodass eine Übermittlung fremder Informationen in einem Kommunikationsnetz vorliegt (Rau/Behrens, K&R 2009, 766, 769). Soweit die Dienste als Telemedien i.S.d. § 2 Abs. 1 Nr. 1 TMG einzuordnen sind (s.o. 2./a.), unterfallen sie daher der Regelung des § 8 TMG.

3. Inwiefern ist das Umgehen von GeoServer-/Proxy-Sperren sowie das Anonymisieren von IP-Adressen nach deutschem Recht strafbar? Macht sich unsere Mandantschaft ggf. wegen Beihilfe strafbar, wenn Dritte mithilfe ihrer Produkte Straftaten, wie z.B. Filesharing, begehen?

a. Strafbarkeit der Nutzer des Dienstes wegen Nutzung der Dienste an sich

Das Anonymisieren von IP-Adressen ist nicht strafbar oder verboten. § 13 Abs. 6 TMG statuiert sogar eine Pflicht der Diensteanbieter, die anonyme oder pseudonyme Nutzung von Telemedien anzubieten, soweit dies technisch möglich und zumutbar ist.

Die Umgehung einer „Geo-Sperre" könnte einen Verstoß gegen das Verbot der Umgehung technischer Schutzmaßnahmen nach § 95a UrhG darstellen, der nach § 108 b Abs. 1 Nr. 1 UrhG strafbar ist. Durch die Verwendung der „Geo-Sperre" als technische Schutzmaßnahme verhindert der Anbieter, dass Nutzer mit bestimmten IP-Adressen auf einen Inhalt zugreifen können. § 95a UrhG setzt jedoch auch voraus, dass die technische Schutzmaßnahme gerade von demjenigen eingesetzt wird, der die Rechte an dem betroffenen Werk hat (§ 95 a Abs. 2 S. 2 UrhG). Wird der Dienst z.B. dazu genutzt, in

Deutschland gesperrte Youtube-Videos abzurufen, liegt kein Verstoß gegen § 95 a UrhG vor, da Youtube nicht die Rechte an den gesperrten Videos innehat (Mittsdörfer/Gutfleisch, MMR 2009, 731, 735).

Außerdem ist zweifelhaft, ob eine Geo-Sperre tatsächlich eine wirksame technische Schutzmaßnahme darstellt. Ziel dieser Maßnahme ist es, Nutzer mit (im Fall von Youtube) deutschen IP-Adressen auszusperren. Durch die Zwischenschaltung eines VPN wird dieses Schutzziel jedoch nicht umgangen oder manipuliert, da eine Geo-Sperre gerade nicht die echte Ziel-IP identifizieren kann. Die Geo-Sperre stellt somit keine wirksame technische Schutzmaßnahme i.S.d. § 95 a UrhG dar (Mittsdörfer/Gutfleisch, MMR 2009, 731, 735). Der Nutzer eines Dienstes, der eine solche Sperre umgeht macht sich daher weder strafbar noch kann er zivilrechtlich belangt werden.

b. Strafbarkeit von Steganos wegen Beihilfe zu von Nutzern begangenen Straftaten

Denkbar ist, dass Nutzer den Anonymisierungsdienst nutzen, um Straftaten zu begehen. Dass sich Steganos durch den Verkauf der Dienstleistungen wegen Beihilfe zu einer solchen Tat strafbar macht, kann jedoch nicht angenommen werden.

Die Strafbarkeit wegen Beihilfe setzt voraus, dass der Gehilfe hinsichtlich der Tat des Haupttäters Vorsatz hat. Bei neutralen Handlungen wie dem Verkauf einer zu legalen Zwecken nutzbaren Dienstleistung, kann ein Vorsatz des Gehilfen nur angenommen werden, wenn der Haupttäter die Dienstleistung ausschließlich in Anspruch nehmen will, um damit Straftaten zu begehen und der Gehilfe dies weiß. Dass die Begehung einer Straftat lediglich für möglich gehalten wird, ist nicht ausreichend, um einen Beihilfevorsatz anzunehmen.

Das Wissen, dass der Kunde die Dienstleistung zu einem illegalen Zweck in Anspruch nehmen will, wird man Steganos nicht unterstellen können, insbesondere da in aller Regel kein vorheriger Kontakt zum Kunden erfolgt.

Steganos kann daher gar keine Kenntnis davon haben, zu welchen Zwecken der Kunde die Software nutzen will.

Eine Strafbarkeit wegen Beihilfe zu einer Straftat eines Nutzers scheidet daher im Regelfall aus.

Anders sieht es höchstens dann aus, wenn sich ein erkennbar tatgeneigter Nutzer (vgl. BGH NStZ-RR 1999, 184, 186) an Steganos wendet, z.B. um zu erfahren, ob er mit Hilfe der Dienstleistung tatsächlich anonym kinderpornographisches Material verbreiten kann. Erfolgt in Kenntnis dieses Zwecks ein Verkauf an den Nutzer, käme eine Beihilfe zu einer von diesem begangenen Straftat in Betracht.

c. Zivilrechtliche Verantwortlichkeit

Aufgrund der Einordnung als Diensteanbieter i.S.d. § 8 TMG (s.o. unter 2./b.) gelangt Steganos im Hinblick auf Schadensersatzansprüche in den Genuss einer Haftungsprivilegierung. Nach § 8 TMG besteht keine Verantwortlichkeit des Diensteanbieters, wenn dieser (1.) die Übermittlung nicht veranlasst hat, (2.) den Adressaten der übermittelten Informationen nicht ausgewählt und (3.) die übermittelten Informationen nicht ausgewählt oder verändert hat. Diese Voraussetzungen treffen hier zu, sodass selbst bei Kenntnis einer Rechtsverletzung keine Schadensersatzpflicht besteht (Rau/Behrens K&R 2009, 766, 769).

Im Hinblick auf Unterlassungs- und Beseitigungsansprüche greift dagegen keine Haftungsprivilegierung ein. Die §§ 7 ff. TMG sind nach Ansicht des BGH nicht auf Unterlassungsansprüche anwendbar (BGH MMR 2007, 507 m.w.N.). Daher kommt bei Kenntnis einer Rechtsverletzung des Nutzers eine Störerhaftung in Betracht. Die Inanspruchnahme als Störer setzt jedoch die Verletzung von Prüfungspflichten voraus, deren Umfang sich danach richtet, inwieweit dem Betroffenen eine Prüfung möglich und zumutbar ist. Ohne konkreten Anlass gibt es keine Verpflichtung, nach Rechtsverletzungen zu suchen (§ 7 Abs. 2 S. 1 TMG). Die Nutzung des Anonymisierungsdienstes

allein kann nicht als hinreichender Anhaltspunkt für eine drohende Rechtsverletzung durch den Nutzer gesehen werden (Rau/Behrens K&R 2009, 766, 770). Es ist einem Anonymisierungsdienst jedoch zumutbar, Filtermechanismen anzuwenden, die ein wiederholtes Durchleiten von rechtswidrigen Informationen verhindern, z.B. durch Sperrung des Zugriffs auf bestimmte Hosts (Rau/Behrens K&R 2009, 766, 771). Vor Kenntniserlangung besteht jedoch zu solchen Maßnahmen keine Veranlassung.

4. Im US-Strafrecht besteht unter dem Titel „piercing the corporate veil" eine Doktrin, die unter bestimmten Voraussetzung eine Durchgriffshaftung auf den Gesellschafter für Handlungen der Gesellschaft ermöglicht. Ergeben sich hieraus Auswirkungen für die Mandantin?

Ein Haftungsdurchgriff auf die Gesellschafter nach der „piercing the corporate veil-Doktrin" besteht grds. nur bei U.S.-amerikanischen Gesellschaftsformen wie der U.S. Corporation und der Limited Liability Company (LLC). Auch dann kommt ein Durchgriff nur in Ausnahmefällen in Betracht, etwa wenn gesellschaftsrechtliche Formen missachtet, keine getrennten Bücher geführt oder die Gesellschaft bewusst unterkapitalisiert gehalten wurde.

Für die von der Mandantin geplante Gesellschaftskonstruktion bestehen keine Anhaltspunkte dafür, die einen Gerichtsstand in den USA begründen würden, sodass eine ohnehin unwahrscheinliche Haftung nach der vorbezeichneten Doktrin ausscheidet.

5. Inwieweit stellt sich das Bewerben der vorbezeichneten Dienste / Produkte als problematisch dar (unabhängig von einer konkreten Werbemaßnahme)? Können hierdurch bereits Straftatbestände und/oder zivil-, wettbewerbsrechtliche Unterlassungs- und/oder Schadensersatzansprüche ausgelöst werden?

Das Bewerben der Dienste kann dann problematisch sein, wenn die Werbung darauf abzielt, die Möglichkeit der Begehung von Rechtsverletzungen in den Vordergrund zu stellen. So hat das OLG Hamburg (MMR 2009, 405) im Fall eines Usenet Anbieters entschieden, dass dieser verschärft haftet, wenn er seinen Dienst mit Internettauschbörsen wie eMule oder eDonkey vergleicht, diese aber als „rechtlich sehr unsicher" einstuft und dabei betont, dass im Usenet Dateien heruntergeladen werden können, ohne dass dies dem Nutzer „nachzuweisen" ist (auszugsweiser Wortlaut der streitgegenständlichen Werbung: *„Wenn Sie Filesharingprogramme benutzen ist es für die Staatsanwaltschaft kein Problem, Ihnen nachzuweisen, was Sie heruntergeladen haben. Vermeiden Sie dieses unnötige Risiko!"*).

Von einem so offensichtlichen Herausstellen der illegalen Nutzungsmöglichkeiten kann bei der gegenwärtigen Produktdarstellung von Internet Anonym (http://www.steganos.com/de/produkte/anonym-surfen/internet-anonym/uebersicht/) nach unserer Ansicht nicht ausgegangen werden. Zwar werden auch hier Tauschbörsen erwähnt *(„Denn ob Sie sich informieren, einkaufen oder Tauschbörsen nutzen geht niemanden etwas an.")*, jedoch nur als eine unter vielen anderen (legalen) Nutzungsmöglichkeiten. Im Vordergrund steht der Schutz vor Bedrohungen durch andere Internetnutzer. Darüber hinaus ist die Nutzung von Tauschbörsen nicht per se illegal. Auch unter Berücksichtigung der urheberfreundlichen Rechtsprechung des OLG Hamburg wird daher eine Bewerbung der Dienste unter Bezugnahme auf Tauschbörsen voraussichtlich nicht zu einer Haftungsverschärfung führen. Falls Sie dieses Risiko jedoch nicht in Kauf nehmen wollen, wäre auch in Erwägung zu ziehen, auf den Begriff „Tauschbörse" komplett zu verzichten. Jedenfalls ist es im Falle eines Rechtsstreits vorteilhaft, wenn die Werbung die legalen Nutzungsmöglichkeiten der Dienste in den Vordergrund stellt.

Im Übrigen gelten die allgemeinen wettbewerbsrechtlichen Vorgaben. Die Werbung darf insbesondere nicht hinsichtlich der

Verwendungsmöglichkeiten und Zwecktauglichkeit der Produkte irreführen (§ 5 Abs. 1 Nr. 1 UWG).

Kilian Kost
Rechtsanwalt