

WENDLER TREMML

RECHTSANWÄLTE

Abschrift

WENDLER TREMML, Pasanenstraße 61 D - 10719 Berlin

Vorab per Fax 90146129 (21 Seiten)Amtsgericht Tiergarten
Lehrter Straße 60

10557 Berlin

BERLINDr. Ralf Grote
Norman Müller
Markus Schmidt
Carsten Gerlach
Raimund R. Walch**DÜSSELDORF**Michael Wendler
Kai P. Sturmfofs, LL.M.³
Dr. Jutta Walther
Catharina Eich
Theresa Steffens
Beata Kosny**MÜNCHEN**Dr. Bernd Tremml, M.C.J.¹
Dr. Dr. Georg Scholz²
Dr. Michael Bihler
Wolf D. Schenk²
Dr. Michael Karper¹
Dr. Andreas Stadler
Stefan Sandrock
Dr. Thomas Fischl**BRÜSSEL**Sophie Melchinger
Dr. Michael Bihler
Kai P. Sturmfofs, LL.M.³¹ Fachanwalt für Verwaltungsrecht² Fachanwalt für Arbeitsrecht³ Fachanwalt für Bau- u. Architektenrecht

www.law-wt.de

Berlin, den 03. Juli 2008

Unser Zeichen:172/00079-08/ms

In dem Rechtsstreit**Patrick Breyer ./ Bundesrepublik Deutschland****- 2 C 6/08 -**werden wir in der mündlichen Verhandlung **beantragen**,

1. die Klage abzuweisen
2. dem Kläger die Kosten des Rechtsstreits aufzuerlegen.

Begründung:

Die Klage ist aus mehreren Gründen bereits unzulässig. Es handelt sich um eine verwaltungsrechtliche Streitigkeit, für die der Zivilrechtsweg nicht eröffnet ist.

Selbst wenn es sich um eine zivilrechtliche Streitigkeit handeln sollte, ist das Amtsgericht Tiergarten sachlich unzuständig (dazu unten I).

- 2 -

BERLIN
Pasanenstraße 61
D - 10719 Berlin
Tel. 030/200 542-0
Fax 030/200 542-11
berlin@law-wt.de

DÜSSELDORF
Mörsenbroicher Weg 200
D - 40470 Düsseldorf
Tel. 0211/66 96 67-0
Fax 0211/66 96 67 66
dus@law-wt.de

MÜNCHEN
Marienstraße 5/II
D - 80802 München
Tel. 089/38 89 9-0
Fax 089/38 89 9-155
munich@law-wt.de

BRÜSSEL
Avenue de la Renaissance 1
B - 1000 Bruxelles
Tel. 0032 2/730 63 54
Fax 0032 2/730 05 71
bruxelles@law-wt.de

HypoVereinsbank Berlin (BLZ 100 208 90) Konto-Nr. 354 971 577
IBAN: DE96 1002 0890 0354 9713 77 – SWIFT: HYVHDE33
USt-IdNr. DE814047461 – Steuernummer: 24/512/63777

Aber auch materiell-rechtlich kann die Klage keinen Erfolg haben. Der Klageantrag ist zu unbestimmt, so dass dem Kläger bei diesem unbestimmten Umfang das erforderliche Rechtsschutzbedürfnis fehlt (dazu unten II). Die Beklagte ist für den vorliegenden Umfang des Klageantrages nicht passivlegitimiert (dazu unten III). Bei IP-Adressen handelt es sich für die Beklagte nicht um personenbezogene Daten. Ihre Speicherung ist schon deshalb uningeschränkt zulässig (dazu unten IV). Darüber hinaus ist die Speicherung auch gemäß § 100 Abs. 1 TKG zulässig, da sie aus technischen Gründen zur Erkennung, Eingrenzung und Beseitigung von Störungen an Telekommunikationsanlagen der Beklagten erforderlich ist (dazu unten V und VI).

Vorab wird ausdrücklich darauf hingewiesen, dass der Vortrag des Klägers zur angeblichen Ermittlungspraxis des Bundeskriminalamtes unzutreffend ist. Entgegen der Darstellung des Klägers, werden nicht automatisch Ermittlungen eingeleitet, sobald auf bestimmte Seiten der Homepage des Bundeskriminalamtes unter der Internetadresse www.bka.de zugegriffen wird. Nur in wenigen begründeten Ausnahmefällen wurden in bereits laufenden Ermittlungsverfahren mit staatsanwaltlichem Einverständnis weitere Maßnahmen auf der Grundlage strafprozessualer Befugnisnormen unternommen.

I. Fehlende sachliche Zuständigkeit

Zur sachlichen Zuständigkeit des Amtsgerichts verweisen wir nochmals auf unsere entsprechenden Ausführungen in unserem Schriftsatz vom 4. Juni 2008.

Bei der Festsetzung des Gegenstandswerts und der Bezifferung des ideellen Interesses des Klägers ist vorliegend zu berücksichtigen, dass die Untetlassung der Speicherung nicht in Bezug auf einen einzigen Server bzw. einen einzigen Anbieter, sondern in Bezug auf eine Vielzahl von Server – nämlich sämtliche Telemediendienste aller Behörden und Organe der Bundesrepublik Deutschland – beantragt wird. Der gesteigerten Tragweite des Klageantrags muss auch bei der Festsetzung des Gegenstandswerts angemessen Rechnung getragen werden.

Danach ist das Amtsgericht Tiergarten sachlich unzuständig zur Entscheidung dieses Rechtsstreits. Sachlich zuständig wäre vielmehr das Landgericht.

II. Fehlendes Rechtsschutzbedürfnis

Der Klageantrag entspricht nicht dem Bestimmtheitserfordernis gemäß § 253 Abs. 2 Nr. 2 ZPO. Der Kläger beantragt die Unterlassung der Speicherung im Zusammenhang „mit der Nutzung öffentlicher Telemedien der Beklagten im Internet“, ohne die jeweiligen Telemedien zu konkretisieren. Dies umfasst sämtliche Telemedien aller Organe und Behörden der Beklagten.

Das Rechtsschutzbedürfnis verlangt bei der vorbeugenden Unterlassungsklage eine sich konkret abzeichnende Verletzungsgefahr (ganz hM, vgl. nur BGH DB 1970, 629). Es ist jedoch praktisch ausgeschlossen, dass der Kläger jemals alle Telemedienangebote des Bundes nutzt bzw. deren Nutzung unmittelbar bevorsteht. Ein Rechtsschutzbedürfnis für den weiten, hinsichtlich der betroffenen Telemedienangebote nicht näher bestimmten Antrag des Klägers besteht somit nicht.

III. Fehlende Passivlegitimation

Grundsätzlich wirkt sich die Angabe zum Vertretungsberechtigten im Klagerubrum nicht auf die Frage der Passivlegitimation aus. Diesem Grundsatz liegt die Überlegung zu Grunde, dass der jeweils richtige Vertretungsberechtigte jederzeit in der Lage ist, für den Beklagten insgesamt rechtlich verbindlich aufzutreten und z.B. ein gerichtliches Unterlassungsurteil aufgrund seiner Vertretungsberechtigung und Organisationshoheit im Bereich des Beklagten durchzusetzen. Dieser Grundsatz trifft im vorliegenden Fall allerdings nicht zu.

Der Kläger verlangt die beantragte Unterlassung von der gesamten Bundesrepublik Deutschland. Dieser Antrag schließt nicht nur Telemedienangebote im Geschäftsbereich des Bundesministeriums des Innern ein, sondern auch die Geschäftsbereiche anderer Ministerien. Gemäß Art. 65 Abs. 1 S. 2 GG liegt die Vertretungskompetenz jedoch für den jeweiligen Geschäftsbereich bei den einzelnen Bundesministerien. Das Bundesministerium des Innern ist daher nur für die im Geschäftsbereich dieses Ministeriums angesiedelten Behörden, wie z.B.

das Bundeskriminalamt oder das Bundesamt für Sicherheit in der Informationstechnik weisungsbefugt, nicht aber für den Geschäftsbereich z.B. des Bundesministeriums der Justiz.

Noch deutlicher wird der Zusammenhang zur Passivlegitimation hinsichtlich der übrigen Verfassungsorgane, wie Bundestag, Bundesverfassungsgericht oder dem Bundespräsidenten. Bereits aus dem verfassungsrechtlichen Gebot der Gewaltenteilung folgt unzweifelhaft, dass das Bundesministerium des Innern und für dieses der Bundesminister des Innern als Vertreter der Beklagten nicht in der Lage ist und verfassungsrechtlich auch gar nicht in der Lage sein darf, gegenüber anderen Verfassungsorganen, wie z.B. dem Bundestag, Weisungen zu erteilen und damit ein mögliches Unterlassungsurteil um- und durchzusetzen.

Vor diesem besonderen verfassungsrechtlichen Hintergrund ist die Passivlegitimation unter dem Blickwinkel des in der Klage angegebenen Vertreters zu beurteilen. Auch wenn es sich bei der Bundesrepublik Deutschland um eine einheitliche juristische Person handelt, führen die verfassungsrechtlichen Erwägungen dazu, dass die Bundesrepublik Deutschland nicht einheitlich vertreten durch eine einzige Behörde mit Wirkung für und gegen alle ihre Behörden und Organe verklagt werden kann. Diese Behörde, hier also das Bundesministerium des Innern vertreten durch den Bundesminister des Innern ist rechtlich nicht in der Lage, im Falle eines in vollem Umfang Klage stattgebenden Urteils dieses umzusetzen. Fehlt jedoch eine solche Möglichkeit, kann eine Verurteilung auch nur insoweit erfolgen, als die Verringerungsbefugnis reicht. Im vorliegenden Fall ist der Klageantrag daher unbegründet, soweit er auf Telemedienangebote außerhalb des Geschäftsbereiches des Bundesministeriums des Innern gerichtet ist.

IV. Keine personenbezogenen Daten

Bei IP-Adressen handelt es sich für die Beklagte nicht um personenbezogene Daten im Sinne von § 3 Abs. 1 BDSG. Die Vorschrift des § 15 Abs. 1 TMG findet auf IP-Adressen daher keine Anwendung. Ihre Speicherung durch die Beklagte ist zulässig.

Vorab ist in diesem Zusammenhang zunächst allgemein darauf hinzuweisen, dass es sich bei einer IP-Adresse ausschließlich um die technische Adresse eines Internetanschlusses/Computers handelt. Die IP-Adresse ist dagegen kein Identifizierungs- oder gar Authentifizierungsmerkmal für den jeweiligen Nutzer des Computers. Welche natürliche Person über den jeweiligen Computer den Internetanschluss nutzt, lässt sich an Hand der IP-Adresse in keinem Fall ermitteln.

1. Mittelbare Bestimmbarkeit des Nutzers anhand dynamischer IP-Adressen

Personenbezogen sind Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Lässt sich aus den Daten ein unmittelbarer Bezug zu einer natürlichen Person nicht herstellen, sind die Daten nur dann personenbezogen, wenn der Betroffene bestimmbar ist (h.M., vgl. Gola/Schomerus, BDSG, 9. Aufl. 2007, § 3 Rn.10; Simitis/Dammann, BDSG, 6. Aufl. 2006, § 3 Rn. 22).

Die IP-Adresse als solche ist kein unmittelbar personenbezogenes Datum (AG Offenburg, Beschl. v. 20.7.2007 – 4 Gs 442/07 = CR 2007, 676; Köcher, MMR 2007, 799, 801). Ein Personenbezug kann allenfalls mittelbar unter Verwendung von Zusatzwissen hergestellt werden.

Beweis: Sachverständigengutachten

Die hier streitigen dynamischen IP-Adressen werden den Rechnern privater Internet-Benutzer von ihrem Zugangsanbieter (Internet-Provider, z.B. T-Online) temporär zugewiesen. Beendet der Kunde seine Internet-Verbindung, erhält er beim nächsten Zugangsversuch eine neue IP-Adresse aus dem Adressbereich des Zugangsanbieters zugeteilt. Auch wenn die Internet-Verbindung vom Kunden dauerhaft aufrechterhalten werden soll (z.B. durch geeignete Konfiguration eines Routers), trennt der Zugangsanbieter regelmäßig, mindestens jedoch alle 24 Stunden, die Verbindung automatisch. Wird die Verbindung unmittelbar nach der Trennung wieder aufgenommen, wird dabei dem Kunden auch wieder eine neue IP-Adresse zugewiesen.

Beweis: Sachverständigengutachten

Eine Zuordnung der IP Adresse zu einem Internetanschluss und damit zu einem Anschlussinhaber als natürlicher Person kann daher ausschließlich von dem Zugangsanbieter vorgenommen werden, zu dessen Adressbereich die fragliche IP-Adresse gehört (zum Ausnahmefall der freiwilligen Preisgabe des Personenbezugs durch den Kläger s.u.). Nur dieser Zugangsanbieter weiß, welchem Kunden er eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen hat.

Beweis: Sachverständigengutachten

Weder für die Beklagte noch für sonstige Dritte ist ohne Auskunft des Zugangsanbieters zu ermitteln, welcher Person (d.h., welchem Kunden des Zugangsanbieters) eine IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war.

Beweis: Sachverständigengutachten

Erst die Auskunft des Zugangsanbieters führt zu einer Individualisierung des Kunden bzw. Anschlussinhabers. Ohne diese Auskunft sind IP-Adressen „ein *technisches und rechtliches Nullum, mit dem niemand etwas anfangen kann*“ (AG Offenburg, Beschl. v. 20.7.2007 - 4 Gs 442/07 = CR 2007, 676).

Deshalb sind unter anderem auch die staatlichen Ermittlungsbehörden auf entsprechende Auskünfte der Zugangsanbieter angewiesen. Bei der Verfolgung netzgestützter Straftaten müssen die Staatsanwaltschaften regelmäßig Anfragen bei den Zugangsanbietern stellen, um die hinter einer bestimmten IP-Adresse stehende natürliche Person zu ermitteln.

Beweis: Sachverständigengutachten

Aus öffentlich zugänglichen Datenbanken kann lediglich ermittelt werden, dass die jeweilige IP-Adresse aus dem Adressbereich eines bestimmten Zugangsanbieters stammt.

Beweis: Sachverständigengutachten

2. Mittelbarer Personenbezug nur durch IP-Adresse und Zeitangabe

Aus oben stehendem folgt zugleich, dass eine IP-Adresse für sich genommen weder personenbezogen noch personenbeziehbar ist.

Erst in Zusammenhang mit einer Zeitangabe (Datum und Uhrzeit) kann der jeweilige Zugangsanbieter ermitteln, welchem seiner Kunden die IP-Adresse zu diesem Zeitpunkt zugeordnet war. Ohne Zeitangabe kann der Zugangsanbieter allenfalls bestätigen, dass die IP-Adresse aus seinem Adressbereich stammt. Ein Rückschluss auf einen konkreten Nutzer/Kunden oder eine sonstige natürliche Person ist ohne diese Zeitangabe objektiv unmöglich.

Beweis: Sachverständigengutachten

Die Klage ist daher schon aus diesem Grund abzuweisen, soweit die Unterlassung der isolierten Speicherung von IP-Adressen ohne Verknüpfung mit Datum und Uhrzeit beantragt wird.

3. Kein Personenbezug der IP-Adressen für die Beklagte

a) Relativität des Personenbezugs

Nach ganz herrschender Meinung ist der Begriff des „personenbezogenen Datums“ relativ (Simitis/Dammann, § 3 Rn. 33; Gola/Schomerus, § 3 Rn. 10; Hohnung, DuD 2004, 429, 430). Dieselben Daten können für den einen anonym und für den anderen einer natürlichen Person zuordenbar sein (Gola/Schomerus, § 3 Rn. 10).

IP-Adressen sind für die Beklagte dann personenbezogene Daten, wenn aus der IP-Adresse die Person des Klägers für die jeweils speichernde Behörde bestimmbar ist (vgl. Simitis/Dammann, § 3 Rn. 21; Gola/Schomerus, § 3 Rn. 10).

Für die Bestimmbarkeit kommt es auf die Kenntnisse, Mittel und Möglichkeiten nicht der Beklagten allgemein, sondern gemäß § 2 Abs. 1 BDSG der im konkreten Fall tätigen Behörde/Einrichtung der Beklagten als speichernden Stelle an (Gola/Schomerus, § 3 Rn. 10). Entscheidend ist, ob das Zusatzwissen, das zur Herstellung des Personenbezugs erforderlich ist, für die jeweils speichernde Stelle der Beklagten zugänglich ist (Simitis/Dammann, § 3 Rn. 39). Sie muss den Personenbezug mit den ihr normalerweise zur Verfügung ste-

henden Hilfsmitteln und ohne unverhältnismäßigen Aufwand durchführen können (Gola/Schormerus, § 3 Rn. 10). Dies ist z.B. dann der Fall, wenn das zur Identifikation der Person notwendige Zusatzwissen aus allgemein zugänglichen Quellen verfügbar ist (vgl. Simitis/Dammann, § 3 Rn. 36). Nur für diejenigen, der über das zur Identifikation benötigte Zusatzwissen verfügt, ist die Bezugsperson bestimmbar und das entsprechende Datum somit personenbezogen – für andere aber nicht (Simitis/Dammann, § 3 Rn. 33).

Eine andere Auffassung würde zu einer uferlosen Anwendung des Datenschutzrechts führen. Letztlich können alle Daten in einer bestimmten Kombination und mit geeignetem Zusatzwissen wieder auf bestimmte Personen zurückbezogen werden (Simitis/Dammann, § 3 Rn. 31). Eine solche unbeschränkte Anwendung des BDSG lag aber erkennbar nicht in der Absicht des Gesetzgebers und unterfällt nicht dem Schutzzweck der Datenschutzgesetze (Simitis/Dammann, § 3 Rn. 31).

b) Keine Bestimmbarkeit der Person für die Beklagte anhand der IP-Adresse

Unter Berücksichtigung dieser Grundsätze handelt es sich bei IP Adressen nicht um personenbezogene Daten für die jeweils speichernde Stelle der Beklagten, da die der jeweiligen Adresse zugeordnete natürliche Person für diese nicht bestimmbar ist.

Vorliegend ist die Rückführung einer IP-Adresse auf den jeweiligen Nutzer nur für den Zugangsanbieter möglich, nicht aber für sonstige Dritte wie die jeweils speichernde Stelle der Beklagten. Die zur Identifikation notwendigen Daten sind der Beklagten weder bekannt noch aus allgemein zugänglichen Quellen verfügbar.

Wie bereits oben ausgeführt, verfügen ausschließlich die Zugangsanbieter über die notwendigen Informationen, um den jeweiligen Kunden bzw. Anschlußinhaber anhand einer IP-Adresse und eines Zeitstempels zu identifizieren (vgl. auch Köcher, MMR 2007, 799, 801).

Beweis: Sachverständigengutachten

Diese Bestandsdaten der Zugangsanbieter sind weder allgemein noch öffentlich zugänglich noch sind sie der jeweils speichernden Stelle der Beklagten bekannt oder zugänglich.

Insbesondere kann das Bekanntwerden der zur Identifikation notwendigen Daten nach sozialüblichen Maßstäben ausgeschlossen werden (vgl. Simitis/Dammann, § 3 Rn. 37). Die jeweils speichernde Stelle der Beklagten kann nicht ohne weiteres und nach Belieben durch Nachfragen beim Zugangsanbieter einen Personenbezug der bei ihr gespeicherten IP-Adressen herstellen.

Die beim Zugangsanbieter gespeicherten Verbindungsdaten unterliegen nach § 88 TKG dem Fernmeldegeheimnis. Nach § 88 Abs. 3 Satz 3 TKG darf der Zugangsanbieter solche Daten nur an Dritte weitergeben, soweit das TKG oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Es fehlt daher für den Zugangsanbieter an einer Befugnis, die entsprechenden Daten ohne weiteres an eine speichernde Stelle der Beklagten zu übermitteln. Umgekehrt fehlt es für die speichernden Stellen der Beklagten an einer Befugnis, die beim Anbieter vorhandenen Daten nachzufragen, sofern nicht im Einzelfall gesetzliche Vorschriften dies erlauben (z.B. zu Zwecken der Strafverfolgung).

Entgegen der Auffassung des AG Mitte bedeutet dies nicht, dass die IP-Adressen „ohne Restriktionen an Dritte, z.B. den Access-Provider übermittelt werden könnten, die ihrerseits die Möglichkeit haben, den Nutzer aufgrund der IP-Adresse zu identifizieren“ (AG Mitte, Urt. v. 27.3.2007 – 5 C 314/06) und der Kläger damit völlig schutzlos gestellt wird. Die Relativität des Personenbezugs ist nämlich auch in diesem Fall zu berücksichtigen. Werden anonyme Daten an eine Stelle übermittelt, die in der Lage ist, den Personenbezug herzustellen, so ist nach ganz herrschender Meinung damit der Übermittlungstatbestand des BDSG erfüllt (Goja/Schomerus, § 3 Rn. 10). Bereits die Übermittlung der IP-Adressen durch eine speichernde Stelle der Beklagten an den Zugangsanbieter fällt somit unter den Anwendungsbereich der Datenschutzgesetze und bedarf entsprechender gesetzlicher Grundlagen (vgl. Köcher, MMR 2007, 799, 801).

Da die jeweils speichernde Stelle der Beklagten somit keine Kenntnis und – sofern nicht ausdrücklich im Einzelfall gesetzlich vorgesehen – keinen Zugriff auf die beim Zugangsanbieter gespeicherten Verkehrsdaten hat, ist ihr die Zuordnung einer IP-Adresse zu einer bestimmten Person nicht möglich. Für die speichernden Stellen der Beklagten handelte es sich demnach bei den bei ihr

gespeicherten dynamischen IP-Adressen des Klägers nicht um personenbezogene Daten im Sinne der §§ 15 Abs. 1 TMC, 3 Abs. 1 BDSG.

4. Freiwillige Preisgabe des Personenbezugs durch den Kläger

Der Kläger trägt weiter vor, dass ein unmittelbarer Personenbezug „seiner“ IP-Adresse für die Beklagte dann hergestellt wird, wenn er auf einer Webseite in einem Formular seine Identität aktiv offenlegt (also z.B. Namen, Adresse etc. angibt). In diesem Sonderfall werden die Formulareingaben unter der gerade aktuellen IP-Adresse des vom Kläger dafür genutzten Internetanschlusses/Computers an einen Web-Server der Beklagten übermittelt.

- a) Die Preisgabe der unmittelbar personenbezogenen Daten erfolgt in diesem Szenario freiwillig durch den Kläger und mit Einwilligung für die jeweilige Verwendung. Die Speicherung der Daten dürfte schon aus diesem Grund zulässig sein.
- b) Personenbeziehbar wird die IP-Adresse aber auch in diesem Fall für die speichernde Stelle der Beklagten nur dann, wenn die Formulareingaben zusammen mit der IP-Adresse erfasst und gespeichert würden.

Beweis: Sachverständigengutachten

Dies ist jedoch nicht der Fall. Jedenfalls auf den Webservern der Beklagten, die im Bundesverwaltungsamt gehostet werden, erfolgt eine solche Speicherung nicht. Formulareingaben und Server-Zugriffe werden getrennt erfasst, gespeichert und verarbeitet.

Insbesondere werden die im Formular eingegebenen Daten nicht in der Protokolldatei der Webserver gespeichert. Die Formulareingaben werden in der Regel durch Verwendung der http-POST Methode an eine „hinter“ dem Formular liegende Funktion weitergereicht, welche die Formulareingaben per E-Mail an eine interne Kontaktadresse (z.B. den jeweils zuständigen Sachbearbeiter) versendet. Eine Speicherung der Daten in einer Protokolldatei findet dabei nicht statt.

Beweis: 1. Zeugnis des Herrn [REDACTED], zu laden über die Beklagte
2. Sachverständigengutachten

Der Inhalt dieser E-Mail besteht ausschließlich aus den jeweiligen Nutzereingaben. Die IP-Adresse des Nutzers und der genaue Zeitpunkt des Server-Zugriffs werden nicht übermittelt.

Beweis: Zeugnis des Herrn [REDACTED], zu laden über die Beklagte

Einer nachträglichen Zusammenführung dieser Daten steht deshalb entgegen, dass kein eindeutiges Identifizierungsmerkmal existiert.

Beweis: 1. Zeugnis des Herrn [REDACTED], zu laden über die Beklagte
2. Sachverständigengutachten

Das beschriebene Verfahren zur Verarbeitung von Formulareingaben ist in dieser Form durchgehend beispielsweise auf sämtlichen Web-Servern umgesetzt, die vom Bundesverwaltungsamt für eine große Zahl von Einrichtungen des Bundes betrieben werden. Hierbei handelt es sich um folgende Internetauftritte:

www.bafin.de
www.bamf.de
www.zivildienst.de
www.jki.bund.de
www.bbk.bund.de
www.bdbos.bund.de
www.behindertenbeauftragte.de
www.evergabe-online.info
www.bescha.bund.de
www.bfa-fish.de
www.bfai.de
www.e-trade-center.com
www.ixpos.de
www.bfarm.de
www.bfdi.bund.de
www.mri.bund.de
www.bundesjustizamt.de
www.endlager-konrad.de
www.bgr.bund.de
www.bib-demographie.de
www.bisp.de
www.bka.de
www.ble.de
www.bmelv.de
www.bmgs.bund.de
www.leben-hat-gewicht.de
www.bmi.bund.de
www.verwaltung-innovativ.de
www.d115.de
www.zuwanderung.de
www.bnd.de
www.bundespolizei.de

www.bundesrat.de
www.deutsche-finanzagentur.de
www.hag.bund.de
www.bsi.bund.de
www.bstu.bund.de
www.bva.bund.de
www.bundesversicherungsamt.de
www.bvl.bund.de
www.aktionsplan-allergien.de
www.bevoelkerungsschutz.de
www.cicac-deutschland.de
www.dehst.de
www.gab-sl.bva.bund.de
www.vti.bund.de
www.intranet.bund.de
www.kbst.bund.de
www.pei.de
www.rki.de
www.thw.bund.de
www.anpassung.net
www.vertreterdesbundesinteresses.de
www.bsi.bund.de/certbund
www.bund.de

Beweis: Zeugnis des Herrn [REDACTED], zu laden über die Beklagte

- c) Selbst wenn eine Zusammenführung der Daten möglich wäre, würde die speichernde Stelle der Beklagten damit lediglich wissen, welche IP-Adresse dem vom Kläger zum Zeitpunkt der Formulareingabe genutzten Internetanschluss/Computer zugeordnet war. Dies verschafft der Beklagten aber keine Informationen, die über diese Tatsache hinausgehen.

Beweis: Sachverständigenutachten

Entgegen der Auffassung des Klägers kann eine speichernde Stelle der Beklagten damit insbesondere nicht nachvollziehen, welche sonstigen Seiten der Kläger auf ihrem Web-Server abgerufen hat. Aufgrund der oben beschriebenen temporären Natur dynamischer IP-Adressen kann die speichernde Stelle der Beklagten nämlich nicht wissen, ob die IP-Adresse, die dem Kläger zum Zeitpunkt der Formulareingabe zugeordnet war, dem Kläger auch bei früheren bzw. späteren Seitenabrufen zugeordnet war. So ist es denkbar, dass der Kläger zu einem bestimmten Zeitpunkt Formulareingaben unter eine bestimmten IP-Adresse tätigt, seine Internetverbindung beendet und unmittelbar darauf die gleiche IP-Adresse einer anderen Person zugewiesen wird, die weitere Seiten auf einem Web-Server der Beklagten besucht.

Beweis: Sachverständigengutachten

Auch in diesem Fall sind ein Personenbezug der IP-Adresse und damit ein Nachvollziehen des Nutzungsverhaltens des Klägers allenfalls dann möglich, wenn die IP-Adressen und die zugehörigen Zugriffszeiten mit den Daten des jeweiligen Zugangsanbieters abgeglichen werden. Nur die Zusammenführung zwischen IP-Adresse/Zeitstempel und den Kundendaten des Zugangsanbieters erlaubt die Herstellung eines Personenbezugs.

Beweis: Sachverständigengutachten

- d) Schließlich wäre es aufgrund der eingangs beschriebenen Funktion der IP-Adresse als lediglich technischer Adresse des jeweiligen Internetanschlusses/Computers für eine speichernde Stelle der Beklagten auch schlichtweg unmöglich zu schließen, welche im Zusammenhang mit einer IP-Adresse gespeicherten Zugriffe auf Web-Server der Beklagten von der natürlichen Person ausgeführt wurden, die unter Nutzung irgendeines Internetanschlusses/Computers mit dieser IP-Adresse ihre Identitätsdaten auf einem Formular der Beklagten angegeben hat. Ob die IP-Adresse im konkreten Zeitpunkt der Nutzung des Internetanschlusses/Computers für die Eingabe der Identitätsdaten irgendeinem Privatanschluss, einem öffentlich zugänglichen Internetanschluss etwa in einem Internetcafé oder einer Bibliothek oder irgendeinem anderen Internetanschluss zugeordnet war, ist nicht erkennbar. Hinzu kommt, dass es gerade bei Privatanlässen, wie dem des Klägers, keinesfalls ungewöhnlich ist, dass mehrere natürliche Personen über den gleichen Internetanschluss auf Internetangebote zugreifen.
- e) Selbst wenn anhand der freiwilligen Preisgabe von Identitätsdaten eine zeitweilige Zuordnung einer IP-Adresse zu einer natürlichen Person wie dem Kläger möglich wäre, dürfte dies nicht zu einer völligen Untersagung der Speicherung von IP-Adressen führen. Wie oben beschrieben, wäre es in diesem Falle ausreichend, dass die Formulareingaben derart getrennt von der IP-Adresse erfasst werden würden, dass eine Zusammenführung und damit ein Rückschluss von der IP-Adresse auf eine natürliche Person nicht möglich wäre.

Beweis: Sachverständigengutachten

Eine solche getrennte Erfassung ist problemlos möglich.

Beweis: Sachverständigengutachten

Sie wird, wie oben ausgeführt, von der Beklagten im Übrigen im Bundesverwaltungsamt bereits praktiziert.

Beweis: Zeugnis des Herrn [REDACTED], zu laden über die Beklagte

V. Notwendigkeit der Speicherung von IP-Adressen

Die Speicherung von IP-Adressen, die (auch) im Zusammenhang mit der Nutzung öffentlich zugänglicher Telemedien der Beklagten anfallen, ist zur Gewährleistung und Aufrechterhaltung der IT-Sicherheit und der Funktionsfähigkeit der Telemedien und Telekommunikationsnetze der Beklagten erforderlich.

1. Konkrete Angriffszenarien und Sicherheitsmaßnahmen

Dies sei nachfolgend anhand diverser Angriffsszenarien und konkreter Sicherheitsmaßnahmen der Beklagten exemplarisch dargestellt.

- a) Zur Erkennung und Abwehr von sogenannten DOS-Angriffen („denial of service“, d.h. ein „Lahtmlegen“ der TK-Infrastruktur durch gezieltes und koordiniertes Fluten einzelner Webserver mit einer Vielzahl von Anfragen) wird ein Anomalieerkennungssystem (z. B. McAfee IntruShield Network Security Plattform) eingesetzt, bei dem bestimmte Kennzahlen des normalen Datenverkehrs aufgezeichnet werden und Abweichungen als mögliche Angriffe eingestuft werden. DOS-Attacken sind ein gängiges Angriffs-Szenario und treten bei der Beklagten häufig auf.

Beweis: Zeugnis des Herrn [REDACTED], zu laden über die Beklagte
Sachverständigengutachten

Zur Anomalieerkennung müssen insbesondere auch die IP-Adressen über einen gewissen Zeitraum gespeichert und ausgewertet werden. Anomalien im Zugriffsverhalten lassen sich zwangsläufig erst in einer Rückschau erkennen, nicht aber durch Analyse eines einzigen Zugriffs.

Beweis: wie vor

- b) Beim Betrieb eines Webserver wird eine mögliche Anomalie der Zugriffe, d.h. ein möglicher Angriff erkannt. Die Angriffsmethode ist aber so komplex (z.B. mehrfach gepackter und verschlüsselter Schadcode, Ausnutzung von unbekannten Schwachstellen in verschiedenen Software-Produkten), dass die Analyse mehrere Wochen dauert. Bis zum Abschluss der Analyse muss die IP-Adresse des ursprünglichen Webserver-Zugriffs gespeichert werden. Die Systeme werden bei Bedarf bereinigt und die IP-Adresse auf eine Sperrliste gesetzt.

Die dargestellte Komplexität der Angriffe findet sich häufig (wöchentlich).

Beweis: wie vor

- c) Die Beklagte wird von einem CERT¹ darüber informiert, dass von einer bestimmten IP-Adresse (oder einem bestimmten IP-Adressen-Bereich, also z.B. aus dem Netz eines bestimmten Zugangsanbieters) in den letzten Wochen erfolgreiche Angriffe ausgingen. Die Beklagte muss in diesem Fall die gespeicherten Daten der letzten Monate analysieren und feststellen, welche Web-Server von dieser IP Adresse aus angegriffen wurden. Die Web-Server werden bei Bedarf bereinigt und die IP-Adresse ggf. auf eine Sperrliste gesetzt. Dieses Szenario tritt monatlich in der Bundesverwaltung auf.

Beweis: wie vor

- d) Eine Bundesbehörde betreibt einen Webserver. Ein Angreifer versucht, einen nur ihm bekannten Fehler des Webserver für einen Angriff auszunutzen. Bei solchen Angriffen ist es häufig notwendig, bestimmte Parameter des Angriffs in Abhängigkeit vom angegriffenen System geringfügig zu modifizieren. Das heißt, ein solcher Angriff ist in der Regel nicht sofort erfolgreich, sondern es sind mehrere Versuche erforderlich, bis die richtigen Parameter geraten werden. Ein automatisches Analysesystem erkennt den ersten Zugriffsversuch des Angreifers als ungültig, kann dies aber zunächst nicht als Angriff interpretieren, da es sich ja eventuell um eine zufällig fehlerhafte Eingabe handeln kann. Der Zugriffsversuch nebst IP-Adresse des Absenders wird gespeichert.

¹ „Computer Emergency Response Team“, Computersicherheitszentren, in Deutschland z.B. bei der Universität Stuttgart, beim Deutschen Forschungsnetz DFN und beim Bundesamt für Sicherheit in der Informationstechnik (BSI) angesiedelt.

Nach einem bestimmten Zeitraum startet der Angreifer mit geänderten Parametern einen weiteren Angriffsversuch, der erneut erfolglos ist und wiederum als ungültiger Zugriff registriert wird. Obwohl der Angreifer bei beiden Angriffsversuchen die gleiche Schwachstelle mit sehr ähnlichen Parametern attackiert, ermöglichen ihm die verwendeten Internet-Kommunikationsprotokolle, diese Zugriffsversuche sehr unterschiedlich aussehen zu lassen.

Da der zweite Zugriff anders kodiert ist und die Parameter etwas geändert sind, ist kein direkter Vergleich der Zugriffe möglich. Einzig die IP-Adresse des Absenders ist in beiden Fällen möglicherweise identisch, daher erfolgt eine Meldung des automatischen Analysesystems. Dieser setzt diese Adresse auf eine Warnliste, weitere Zugriffe von dort werden manuell analysiert. Ein Angriff ist bis zu diesem Zeitpunkt nicht erkennbar. Nach einer weiteren Zeitspanne erfolgt ein erneuter Versuch, der wiederum modifiziert ist. Die IP-Adresse wird auf eine Sperrliste gesetzt. Später erfährt die Behörde von der Lücke in ihrem Webserver und kann die fehlerhaften Zugriffe als Angriff einstufen. Der Fehler auf dem Webserver wird beseitigt und die protokollierte Absendeadresse der Strafverfolgung zugeführt.

Die geschilderten Angriffe treten regelmäßig (mindestens monatlich) auf.

Beweis: wie vor

- e) Ein Angreifer kann durch Ausnutzung einer Lücke im Betriebssystem eine Schadsoftware auf dem Webserver einer Bundesbehörde installieren, die sich ohne eine aufwendige forensische Analyse nicht erkennen lässt, keine offensichtlichen Schäden anrichtet, aber zur Weiterleitung von Angriffen auf weitere Server oder andere Nutzer des Webserver genutzt wird (eventuell auch als Teil eines Botnetzes). Gestartet und gestoppt wird die Schadfunktion durch eine zulässige, aber ungewöhnliche Abfrage im Internet, z. B. über DNS. Der erste Start erfolgt erst Wochen nach der Installation. Die Behörde beobachtet diesen ungewöhnlichen Verkehr und analysiert die gespeicherten IP-Adressen. Es wird eine Übereinstimmung zwischen dem aktuellen und früheren Datenverkehr festgestellt. Die Logdaten des früheren Datenverkehrs enthalten Informationen (URL), die das Einbringen des Schadprogramms erkennbar machen und eine Analyse der Schadfunktion ermöglichen.

Beweis: wie vor

2. Stand der Technik

Neben der Verwendung von IP-Adressen in den vorstehend beschriebenen unmittelbar wirksamen IT-Sicherheitsmaßnahmen bildet die Speicherung und Verwendung von IP-Adressen die unverzichtbare Grundlage für die mittelbar wirksame IT-Sicherheitsmaßnahme der Protokollierung.

Beweis: Sachverständigengutachten

Diese Protokollierung verfolgt drei zentrale Ziele:

- Unterstützung der Detektion und damit Abwehr von Angriffen (wie oben näher erläutert).
- Grundlage für die Strafverfolgbarkeit von Angriffen. IP-Adressen sind das wichtigste Indiz im Rahmen der Strafverfolgung. Die Identifikation eines Angreifers kann nur anhand der IP-Adresse sowie des dazugehörigen Datums nebst Uhrzeit stattfinden (vgl. LG Darmstadt, Urt. v. 6.6.2007 - 10 O 562/03 = CR 2007, 574).
- Abschreckungswirkung aufgrund der Strafverfolgbarkeit.

Protokolldaten dienen dann dem Zweck, nachträglich feststellen zu können, ob Sicherheitsverletzungen im IT-System stattgefunden haben oder ob ein Angriffsversuch unternommen wurde. Protokolldaten werden für die Optimierung, die Fehleranalyse im Schadensfall und zur Ursachenermittlung bzw. zur Integritätsprüfung genutzt. Die Protokollierung kann auch der Täterermittlung und damit auch der Abschreckung von potenziellen Tätern dienen. Durch regelmäßige Auswertung der Protokolldaten können vorsätzliche Angriffe auf ein IT-System unter Umständen frühzeitig erkannt werden.

Beweis: Sachverständigengutachten

Dabei entspricht die Protokollierung dem nationalen und internationalen Stand der Technik. So findet sich die Forderung der Protokollierung in einschlägigen Standards und Normen:

- ITIL (IT Infrastructure Library) (Quelle: ICT Infrastructure Management, Stationery Office (5. November 2002), ISBN-10: 0113309031)
- ISO/IEC 15408

- ISO 27001. Die ISO 27001 ist eine der wichtigsten Grundlagen für die Zertifizierung von Informationsmanagementsystemen.
- ISO 17799 / ISO 27002. Diese vertiefende Norm fordert die Protokollierung unter anderem in Control 10.10.1 "Audit logging".
- BSI-Standards 100-2 (IT-Grundschutz)
Die national als Stand der Technik gesehenen BSI-Standards konkretisieren die ISO-Norm 27001. In der Maßnahme "M 4.182 Überwachen des IIS-Systems" aus dem Baustein "B 5.10 Internet Information Server" wird als minimale Protokollierung die Aufzeichnung der folgenden Informationen gefordert: Datum, Zeit, Client IP-Adresse.

Beweis: Sachverständigengutachten

VI. Zulässigkeit der Speicherung nach § 100 Abs. 1 TKG

Selbst wenn es sich bei den IP-Adressen um personenbezogene Daten im Sinne des BDSG handeln würde, wäre ihre Speicherung durch die Beklagte gemäß § 100 Abs. 1 TKG zulässig.

1. Geschäftsmäßiges Erbringen von Telekommunikationsdiensten

Die Beklagte ist nicht nur Anbieterin von Telemedien (Web-Servern und Websites), sondern auch geschäftsmäßiger Anbieter von Telekommunikationsdiensten im Sinne des TKG. Auf den Betrieb dieser Telekommunikationsdienste findet § 100 Abs. 1 TKG Anwendung.

Unter anderem betreibt die Beklagte mit dem Informationsverbund Berlin-Bonn (IVBB) und dem Informationsverbund der Bundesverwaltung (IVBV) umfangreiche eigene Telekommunikationsnetze. In diesen Telekommunikationsnetzen sind zahlreiche Telemediendienste (z.B. Webserver) der Beklagten angesiedelt.

Beweis: Zeugnis des Herrn [REDACTED], zu laden über die Beklagte

Die Telekommunikationsnetze der Beklagten verfügen über Schnittstellen zum öffentlichen Internet. Wenn z.B. der Kläger auf die Website des Bundesministeriums des Inneren zugreift, nutzt er damit gleichzeitig die Telekommunikationsinfrastruktur der Beklagten, da der Webserver des Bundesministeriums des

Innern an den IVBB angeschlossen ist und die Datenpakete des Klägers damit zwangsläufig über die Telekommunikationsinfrastruktur der Beklagten laufen.

Beweis: wie vor

Die Beklagte ist somit Anbieter von Telekommunikationsdiensten im Sinne des § 3 Nr. 6 TKG (Beck'scher TKG-Kommentar, § 3 Rn. 19). Sie ist auch geschäftsmäßiger Anbieter von Telekommunikationsdiensten. Gemäß § 3 Nr. 10 TKG ist das geschäftsmäßiges Erbringen definiert als „das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht“. Es kommt daher nicht darauf an, ob der Telekommunikationsdienst gewerbsmäßig angeboten wird. Entscheidend ist allein, dass das Angebot des Telekommunikationsdienstes auf eine gewisse Dauer angelegt und nicht auf einen Einzelfall begrenzt ist (Beck'scher TKG-Kommentar, § 91 Rn. 9). Dabei ist die Anzahl der berechtigten Nutzer dieser Dienste unerheblich. Erforderlich ist eine gewisse Regelmäßigkeit aus Sicht des Anbieters. Dies dürfte in Hinblick auf den Betrieb der Kommunikationsinfrastruktur der Bundesverwaltung unstrittig sein.

Nach allgemeiner Auffassung unterfällt daher der Betrieb von Behördennetzen wie den von der Beklagten betriebenen Telekommunikationsnetze dem geschäftsmäßigen Betrieb von Telekommunikation im Sinne des TKG (Beck'scher TKG-Kommentar, § 91 Rn. 9).

2. Gleichzeitige Anwendung von TKG und TMG

Unerheblich ist in diesem Zusammenhang, dass die Beklagte gleichzeitig Telekommunikationsdienste und Telemediendienste anbietet. TKG und TMG stehen nicht in einem Ausschließlichkeitsverhältnis. Es gibt somit einen Überschneidungsbereich in der Anwendung beider Gesetze (vgl. Roßnagel, NVwZ 2007, 743, 745).

3. Zulässigkeit der Speicherung nach § 100 Abs. 1 TKG

Gemäß § 100 Abs. 1 TKG darf die Beklagte als Anbieter von Telekommunikationsdiensten zum Erkennen, Eingrenzen und Beseitigen von Störungen oder Fehlern an ihren TK-Anlagen die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden. Dies umfasst auch die Speicherung der IP-Adressen des Klägers.

a) **Erforderlichkeit der Speicherung**

Wie bereits oben dargestellt, ist die Speicherung der IP-Adressen im Rahmen eines ordnungsgemäßen Betriebs von IT-Infrastruktur und insbesondere von Telekommunikationseinrichtungen erforderlich, um Störungen – vor allem als Folge von Angriffen Dritter – zu erkennen, einzugrenzen und zu beseitigen. Nach dem Willen des Gesetzgebers ist daher auch die Speicherung von IP-Adressen insoweit zulässig (Regierungsentwurf zum TKG, BT-Drs. 15/2316, S. 90).

Dies ist von der Rechtsprechung bestätigt worden. So haben das Landgericht Darmstadt und das Amtsgericht Bonn entschieden, dass die präventive Speicherung von IP-Adressen generell geeignet ist, einen Missbrauch von Telekommunikationseinrichtungen aufzudecken und zu bekämpfen (AG Bonn, Urt. v. 5.7.2007 – 9 C 177/07 = MMR 2008, 203, 205; LG Darmstadt, Urt. v. 6.6.2007 - 10 O 562/03 = CR 2007, 574).

b) **Präventive Speicherung zulässig**

Dabei ist unerheblich, dass die Speicherung nicht angriffs- bzw. einzelfallbezogen, sondern präventiv geschieht. § 100 Abs. 1 TKG setzt im Unterschied zu der früher geltenden Norm des § 9 Abs. 1 TDSV 2000 nicht mehr voraus, dass im Einzelfall tatsächlich Störungen und Fehler oder konkrete Anhaltspunkte dafür vorliegen müssen.

Dies verkennt das Landgericht Darmstadt in dem vom Kläger zitierten Urteil vom 25.1.2006 – 25 S 118/05 (MMR 2006, 330). Der Gesetzgeber hat bewusst auf die Einschränkung einer Speicherung nur „im Einzelfall“ in § 100 Abs. 1 TKG verzichtet (Beck'scher TKG-Kommentar, § 100 Rdnr. 2). § 100 Abs. 1 TKG soll bewusst auch die Speicherung von Daten zur Abwehr von Störungen oder Fehlern erlauben, die bei einer größeren Anzahl von Teilnehmern oder Nutzern oder in einer Vielzahl von Fällen auftreten. Die Speicherung soll nach dem Wortlaut des § 100 Abs. 1 TKG auch der „Erkennung“ von Störungen und Fehlern dienen. Wäre aber ein konkreter und somit dem Anbieter bereits bekannter Vorfall als Grundlage der Speicherung notwendig, wäre die vom Gesetz gewollte Erkennung notwendigerweise unbekannter Fehler unmöglich. Diese Ausweitung ist auch sachgerecht, da beispielsweise zu einer Abwehr von Denial-of-Service-Attacken oder erheblichen Spam-Aufkommen generelle Abwehrmaßnahmen erforderlich sind, um den Betrieb der Telekommunikati-

onsanlagen fortzuführen (Beck'scher TKG-Kommentar, § 100 Rdnr. 2). Dazu haben wir oben unter II bereits ausführlich vorgetragen.

Die präventive Speicherung von IP-Adressen zur Erkennung von Fehlern oder Störungen ist deshalb nach allgemeiner Auffassung gemäß § 100 Abs. 1 TKG zulässig (AG Bonn, Urt. v. 5.7.2007 – 9 C 177/07 = MMR 2008, 203, 204; LG Darmstadt, Urt. v. 6.6.2007 – 10 O 562/03 = CR 2007, 574; Beck'scher TKG-Kommentar, § 100 Rdnr. 1).

Insbesondere hat das Landgericht Darmstadt in einer späteren Entscheidung vom 6.6.2007 seine frühere Auffassung revidiert und eine präventive Speicherung von IP-Adressen gemäß § 100 Abs. 1 TKG zu Zwecken der Störungs- und Fehlerbeseitigung ausdrücklich für zulässig erachtet (LG Darmstadt, Urt. v. 6.6.2007 – 10 O 562/03 = CR 2007, 574).

Die Klage ist somit aus formellen, wie auch aus materiell rechtlichen Gesichtspunkten unzulässig bzw. unbegründet und daher insgesamt abzuweisen.

Beglaubigte und einfache Abschrift anbei. Der Terminsvertreter des Klägers hat mit Telefax vom heutigen Tage eine Abschrift des Schriftsatzes erhalten.



Rechtsanwalt