WENDLER TREMML

RECHTSANWÄLTE

Beglaubigte Abschrift

WENDLER TREMML · Fasanenstraße 61 · D - 10719 Berlin

Vorab via Telefax: 9023-2223
Landgericht Berlin
ZK 57

10174 Berlin

BERLIN
Dr. Ralf Grote
Norman Müller
Markus Schmidt
Carsten Gerlach
Raimund E. Walch[3]

DÜSSELDORF
Michael Wendler
Kai F. Sturmfels, LL.M.[3]
Dr. Jutta Walther
Beata Kosny

MÜNCHEN
Dr. Bernd Tremml, M.C.J.[1]
Dr. Dr. Georg Scholz †
Dr. Michael Bihler
Wolf D. Schenk[2]
Dr. Michael Karger[4]
Dr. Andreas Stadler
Stefan Sandrock
Dr. Matthias von Oppen

BRÜSSEL
Sophie Melchinger
Dr. Michael Bihler
Kai F. Sturmfels, LL.M.[3]

1 Fachanwalt für Verwaltungsrecht
2 Fachanwalt für Arbeitsrecht
3 Fachanwalt für Bau- u. Architektenrecht
4 Fachanwalt für IT-Recht

www.law-wt.de

Berlin, den 22. März 2010
Unser Zeichen:172/00123-08/vb/ka

In dem Rechtsstreit
Patrick Breyer ./. Bundesrepublik Deutschland
- 57 S 87/08 -

nehmen wir zu der gerichtlichen Verfügung vom 11. Februar 2010 wie folgt Stellung:

A. Unzulässigkeit des Rechtswegs

Die Beklagte hält die Rüge der Unzulässigkeit des Rechtswegs weiter aufrecht.

Vorliegend handelt es sich nicht um eine bürgerlich-rechtliche Streitigkeit, sondern um eine öffentlich-rechtliche Streitigkeit, für die der Verwaltungsrechtsweg nach § 40 VwGO eröffnet ist. Bei der rechtlichen Einordnung von Realakten der Verwaltung - wie beim hier streitigen Betrieb von Telemedien und der

BERLIN
Fasanenstraße 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
Martiusstraße 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 2/739 63 54
Fax 0032 2/736 05 71
bruxelles@law-wt.de

HypoVereinsbank Berlin (BLZ 100 208 90) Konto-Nr. 354 971 577
IBAN: DE96 1002 0890 0354 9715 77 – SWIFT: HYVEDEMM488
USt-IdNr. DE814047461 - Steuernummer: 24/319/63777

Speicherung von IP-Adressen durch die Beklagte - ist auf den Sach- bzw. Funktionszusammenhang abzustellen.

Realakte der Verwaltung sind immer öffentlich-rechtlich zu qualifizieren, sofern sie nicht in einem engen inneren und äußeren Zusammenhang mit der Wahrnehmung privatrechtlich zu erfüllender Aufgaben stehen (Schoch/Schmidt-Aßmann/Pietzner, VwGO, 18. Aufl. 2009, § 40 Rn. 393).

Soweit der Betrieb der Telemedien mit dem elektronischen Angebot von Verwaltungsdienstleistungen im Zusammenhang steht (so z.B. die Möglichkeit der elektronischen Markenrecherche auf dem Server des Deutschen Patent- und Markenamtes), liegt der öffentlich-rechtliche Funktionszusammenhang auf der Hand. Vorliegend besteht zwischen der Beklagten und dem Kläger als Nutzer von Informationsangeboten ein öffentlich-rechtlich determiniertes Rechtsverhältnis, da die Beklagte mit den entsprechenden Informationsangeboten ihrer jeweiligen öffentlich-rechtlichen Informationspflicht nachkommt. Der Rechtsschutz kann in diesem Zusammenhang daher nur mittels öffentlich-rechtlichen Leistungs- bzw. Unterlassungsansprüchen über den Verwaltungsrechtsweg geltend gemacht werden.

B. sachliche Unzuständigkeit

Die Beklagte hält ebenfalls an ihrem Einwand der sachlichen Unzuständigkeit des Amtsgerichtes Mitte in erster Instanz bzw. des Landgerichtes Berlin in der Berufungsinstanz fest.

1. Sowohl in den Hinweisen vom 19. Dezember 2008 als auch im Beschluss der Kammer vom 1. April 2008 – 57 T 14/08 – sind nach hiesiger Ansicht nicht alle für die Bemessung des Streitwerts relevanten Faktoren ausreichend berücksichtigt worden.

Bei der Streitwertbemessung nach § 48 Abs. 2 GKG sind alle Umstände einzubeziehen, die einen sachlichen Bezug zum Streitgegenstand haben. Dazu gehören auch die tatsächlichen und wirtschaftlichen Folgen der Entscheidung für die Parteien (Binz/Dörndorfer/Petzold/Zimmermann, § 48 GKG Rn. 11; Hartmann, § 48 GKG Rn. 27).

2. Dabei ist insbesondere als werterhöhender Faktor zu berücksichtigen, dass ein Rechtsstreit als Musterprozess geführt wird (Binz/Dörndorfer/Petzold/Zimmermann, § 48 GKG Rn. 11; Hartmann, § 48 GKG Rn. 27).

Wie bereits das AG Tiergarten in seiner Entscheidung vom 13. August 2008 ausgeführt hat, besteht das Interesse des Klägers vorliegend keineswegs allein in dem rein privaten, ideellen Interesse an einer Unterlassung der Speicherung seiner Daten. Vielmehr führt er das Verfahren als Musterprozess im Rahmen seines öffentlichen Engagements gegen Datenspeicherung.

Der Kläger ist in Vereinigungen und Initiativen aktiv, die sich gegen eine Datenspeicherung einsetzen, unter anderem im „Arbeitskreis Vorratsdatenspeicherung" und der Kampagne „Wir speichern nicht". Er betreibt die Website „www.daten-speicherung.de", auf der er über rechtliche Aspekte der Datenspeicherung und des Datenschutzes informiert und für eine Minimierung der Datenspeicherung eintritt. In diesem Zusammenhang ist er auch in zahlreichen Veröffentlichungen, Interviews und Reden öffentlich in Erscheinung getreten.

Beweis: Verzeichnis der Veröffentlichungen, Interviews und Reden des Klägers auf seiner Website www.daten-speicherung.de, **Anlage BB 1**

Bereits eine vorangegangene Klage des Klägers gegen das Bundesministerium der Justiz vor dem Amtsgericht Mitte mit inhaltlich identischem Klageantrag (Urt. v. 27. März 2007, Az.: 5 C 314/06) wurde von ihm augenscheinlich als

Musterprozess im Zusammenhang mit seinem öffentlichen Engagement geführt.

In einem Pressebericht des Branchen-Nachrichtendienstes Heise online heißt es zu dem Verfahren vor dem AG Mitte unter Berufung auf Aussagen des Klägers:

> *„Für den Kläger, den im Arbeitskreis Vorratsdatenspeicherung aktiven Juristen Patrick Breyer, hat die inzwischen rechtskräftige Entscheidung Signalwirkung für die gesamte Internetbranche […] "Selbst der Deutsche Bundestag protokolliert gegenwärtig das Verhalten der Nutzer seines Internetportals auf Vorrat – unter Verstoß gegen seine eigenen Gesetze", moniert Breyer. Er forderte zunächst alle öffentlichen Stellen des Bundes und der Länder auf, die "rechtswidrige Vorratsspeicherung" spätestens bis zum Jahresende abzustellen. Andernfalls müssten weitere Gerichtsverfahren eingeleitet werden." Der Jurist hat auf seiner Website eine Musterklage zur Verfügung gestellt.“*

Der Kläger veröffentlichte auf seiner Internet-Seite „www.daten-speicherung.de“ eine Musterklage, in der er unter Verweis auf das Urteil des AG Mitte zu Klagen gegen die Speicherung von Verbindungsdaten aufrief. Die Musterklage ist zwischenzeitlich – vermutlich in Hinblick auf das vorliegende Verfahren – wieder von der Website entfernt worden, aber im Internet-Archiv www.archive.org auffindbar.

Beweis: Ausdruck der Seite „Musterklage Internetportale“ aus der Website „www.daten-speicherung.de“, entnommen aus dem Internet-Archiv archive.org, Stand November 2007, **Anlage BB 2**

In einem Interview des Onlinemagazins Telepolis mit dem Kläger heißt es:

> *„Mehr Erfolg hatte die Bürgerrechtsbewegung auf dem Rechtswege, wo das Amtsgericht Berlin Mitte die Speicherung von personenbezogenen Daten beim Besuch von Webseiten untersagte.“*

Beweis: Interview vom 2. Oktober 2007, **Anlage BB 3**

Es ist somit offensichtlich, dass der Kläger mit der Klage nicht ausschließlich eigene, persönliche Interessen verfolgt. Vielmehr will er im Rahmen eines Musterverfahrens und im Zusammenhang mit seinem öffentlichen Engagement gegen Datenspeicherung vermeintlich grundsätzliche Interessen der Allgemeinheit wahrnehmen und klären. Es ist zu erwarten, dass der Kläger auch das vorliegende Verfahren im Falle des Obsiegens als Anlass nehmen wird, eine Muster-Klageschrift zu veröffentlichen und diese durch Veröffentlichungen und Interviews publik zu machen.

Der übergeordnete Mustercharakter der Klage für den Kläger wird auch an dem umfassenden Inhalt der Klageanträge deutlich. Der Kläger behauptet selbst nicht einmal alle Webangebote der Beklagten zu nutzen und damit alle Web-Server der Beklagten zu besuchen. Nach seinem Vortrag beschränkt sich vielmehr sein eigenes Interesse durchaus auf im Verhältnis zur Gesamtzahl der von der Beklagten betriebenen Web-Server wenige Web-Server. Dieser Widerspruch wird nur unter Berücksichtigung des vom Kläger angestrebten Mustercharakters der Klage erklärlich.

Dieser Mustercharakter des Verfahrens ist streitwerterhöhend zu berücksichtigen. Das Landgericht hat diesen Faktor in seinen Hinweisen vom 19. Dezember 2008 bislang nicht erwähnt.

3. Wie ebenfalls vom AG Tiergarten ausgeführt, erstreckt sich das Interesse des Klägers zudem nicht nur auf ein einziges Internetportal, sondern auf sämtliche Internet-Angebote der Bundesverwaltung. Die Gesamtzahl von Servern, die der Beklagten zuzuordnen sind, ist praktisch nicht ermittelbar. Nach Schätzung der Beklagten bestehen jedoch bereits mindestens 500 Systeme, die allein im Regierungsnetz IVBB (Informationsverbund Berlin Bonn) in der Lage sind, IP-Adressen zu speichern.

Dies führt bei objektiver Betrachtung aus Sicht des Klägers zu einer Ausweitung der von ihm befürchteten Auswirkungen des beanstandeten Verhaltens der Beklagten.

Zum einen ist das Risiko der vom Kläger behaupteten – diesseits bestrittenen – möglichen Folgen einer Speicherung von IP-Adressen naturgemäß umso größer, je mehr Server derartige Daten speichern. Bereits das persönliche ideelle Interesse des Klägers ist somit aus seiner Sicht gegenüber einer Klage auf Unterlassung der Speicherung in nur einem Internet-Portal deutlich erhöht.

Zum anderen ist zu berücksichtigen, dass der Kläger mit seinem (Muster-) Verfahren aus seiner Sicht auch ideelle Interessen der Allgemeinheit verfolgt. Dieses Interesse verkörpert sich in der vorliegenden Klage bezüglich der Internet-Angebote der gesamten Bundesverwaltung wesentlich stärker als in einer Klage gegen nur ein Internet-Angebot. Auch das ideelle Interesse des Klägers an einem Datenschutz-Musterverfahren ist somit deutlich stärker.

Der Umfang der Gefahr einer Rechtsverletzung, wie sie vom Kläger behauptet wird, hängt zudem maßgeblich auch von der Anzahl der von der Beklagten betriebenen Telemedien ab. Je mehr Angebote die Beklagte hier unterbreitet, desto höher ist die abstrakte Gefahr, dass die IP-Adresse des Klägers als, wie er selbst ausführt, intensivem Internetnutzer von der Beklagten gespeichert wird. Das Unterlassungsinteresse des Klägers ist also umso höher, je mehr Internetportale Gegenstand seines Unterlassungsbegehrens sind. Der Kläger hat es insoweit selbst in der Hand den Wert dieses Interesses durch einen generellen Antrag, wie von ihm in diesem Verfahren gestellt, oder durch einen auf einzelne Telemedienangebote der Beklagten beschränkten Antrag zu bestimmen.

Die Gesamtzahl der Server, auf die sich das Unterlassungsbegehren des Klägers bezieht, ist somit bei der Bemessung des Streitwertes als erhöhender Fak-

tor angemessen zu berücksichtigen. Auch wenn keine schlichte Multiplikation des vom AG Mitte angenommenen Streitwerts von 600,- Euro in Bezug auf einen einzigen Server mit der Gesamtzahl der betroffenen Server vorzunehmen ist, erscheint doch ein Streitwert von 4.000,- Euro angesichts einer Gesamtzahl von ca. 500 Systemen, die allein im Regierungsnetz IVBB (Informationsverbund Berlin Bonn) in der Lage sind, IP-Adressen zu speichern, unangemessen niedrig und dem ideellen Interesse der Parteien am Ausgang des Verfahrens nicht angemessen.

4. Bei der Streitwertbemessung nach § 48 Abs. 2 GKG sind im Übrigen auch die wirtschaftlichen Auswirkungen des Streitgegenstandes auf die Parteien zu berücksichtigen (Hartmann, § 48 GKG Rn. 27; LAG Mecklenburg-Vorpommern, NZA-RR 2001, 551). Alleine die Umstellung aller oben genannten ca. 500 Systeme im IVBB bedeutet einen äußerst hohen technischen und administrativen Aufwand für die Beklagte mit geschätzten Minimalkosten in Höhe von ca. 1,2 Mio Euro.

Beweis: Sachverständigengutachten

Bei diesen Kosten noch völlig unberücksichtigt sind Kosten für die Entwicklung alternativer Maßnahmen zur Schadprogrammabwehr, die jedoch erforderlich wären, um einen sicheren Betrieb der entsprechenden Systeme der Beklagten zu gewährleisten. Zur Vermeidung von Wiederholungen dürfen wir zur Notwendigkeit entsprechender Abwehrmaßnahmen auf unsere Ausführungen im Schriftsatz vom 3. Juli 2008 verweisen.

Dieser unverhältnismäßig hohe Kostenaufwand ist bei der Bemessung des Streitwertes ebenfalls angemessen zu berücksichtigen.

Wir weisen in diesem Zusammenhang ausdrücklich darauf hin, dass der Bundesgerichtshof hinsichtlich des Gegenstandswertes der Klage keine Entschei-

dung in der Sache getroffen hat, sondern vielmehr die Rechtsbeschwerde der Beklagten als formal unzulässig zurückgewiesen hat.

C. Übernahme durch das Berufungsgericht

Die Beklagte schließt sich hiermit dem Antrag des Klägers vom 14. Januar 2010 an und beantragt gemäß § 526 Abs. 2 S. 1 Nr. 2 ZPO,
den Rechtsstreit dem Berufungsgericht zur Entscheidung über eine Übernahme vorzulegen.

Vorsorglich möchten wir darauf hinweisen, dass aus der Entscheidung vom 11. Februar 2010, nunmehr in der Berufungsinstanz auch über die Begründetheit der Klage zu entscheiden, eine Änderung der Prozesslage folgt, die sowohl zu einer besonderen rechtlichen Schwierigkeit als auch zu einer grundsätzlichen Bedeutung der Rechtssache führt. Die grundsätzliche Bedeutung der Rechtssache des vorliegenden Verfahrens ist bereits durch Beschluss des Landgerichts vom 7. April 2009 festgestellt worden. Die Sache ist damit schon gemäß § 526 Abs. 2 S. 1 Nr. 1 ZPO dem Berufungsgericht zur Entscheidung über eine Übernahme vorzulegen. Gemäß § 526 Abs. 2 S. 2, Abs. 1 Nrn. 2 und 3 ZPO ist der Rechtsstreit durch das Berufungsgericht zu übernehmen.

D. IP-Adressen sind keine personenbezogenen Daten

In Hinblick auf die anstehende Entscheidung zur Sache möchten wir nachfolgend noch einmal die bisherige Argumentation zusammenfassen.

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.

Die Rechtsauffassung der Beklagten ist zwischenzeitlich vom Amtsgericht München in einer Entscheidung vom 30. September 2008 (Az: 133 C 5677/08 = CR 2009, 59) bestätigt worden.

Bei einer IP-Adresse handelt es sich ausschließlich um die technische Adresse eines Internetanschlusses/Computers. Die IP-Adresse ist kein Identifizierungs- oder gar Authentifizierungsmerkmal für den jeweiligen Nutzer des Computers. Welche natürliche Person über den jeweiligen Computer den Internetanschluss tatsächlich 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 zugeteilt 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

Von diesem Zusammenhang geht auch das Bundesverfassungsgericht in seinem Urteil zur Vorratsdatenspeicherung vom 2. März 2010 (1 BvR 256/08) aus. Um aus einer IP-Adresse den jeweiligen Anschlussinhaber zu ermitteln, muss auf die Telekommunikationsverkehrsdaten des Zugangsanbieters zurückgegriffen werden (Absatz 255). Erst nach einer solchen Auskunftserteilung – die nach dem Urteil des Bundesverfassungsgerichts nur in engen Grenzen zulässig ist – kann die IP-Adresse „individualisiert", d.h. einem konkreten Anschlussinhaber zugeordnet werden (Absatz 258). Das Bundesverfassungsgericht hat daher an diese „Individualisierung" von IP-Adressen durch die Zugangsanbieter hohe Voraussetzungen geknüpft.

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; Hornung, DuD 2004, 429, 430; Eckhardt, K&R 2007, 602; Moos, K&R 2008, 137, 139). 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 stehenden Hilfsmitteln und ohne unverhältnismäßigen Aufwand durchführen können (Gola/Schomerus, § 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 denjenigen, 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).

Die Rechtsauffassung des Klägers würde letztlich zu einer vollständigen Aufgabe der Relativität des Personenbezugs führen. Dies wird z.B. in dem vom Kläger angeführten Aufsatz von Pahlen-Brandt, K&R 2008, S. 288, 290 auch ausdrücklich ausgesprochen:

> *„Die relative Sicht der Personenbezogenheit von Daten führt zu ungewollten Datenschutzlücken; ihr kann daher nicht gefolgt werden. […] Bei der Beurteilung des Schutzes ist illegales Handeln mit zu bedenken.“*

Dies würde jedoch entgegen dem Willen des Gesetzgebers und sachlich ohne Grund 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/Damman, § 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/Damman, § 3 Rn. 31). Müsste bei der Beurteilung des Personenbezugs jede noch so unwahrscheinliche, ggf. sogar illegale Handlung zur Herstellung eines möglichen Personenbezugs berücksichtigt werden, wäre das Kriterium des „Personenbezugs" nutzlos. Alle nur denkbaren Daten würden dem Datenschutzrecht unterfallen.

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.

(1) **Keine Kenntnis der Zugangsdaten der Zugangsanbieter (Provider)**

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).

In Hinblick auf das Fernmeldegeheimnis hat das Bundesverfassungsgericht im Urteil vom 2. März 2010 zur Vorratsdatenspeicherung gerade hohe Anforderungen an die gesetzliche Regelung derartiger Auskunftsansprüche aufgestellt. Die Zusammenführung von IP-Adressen und Zugangsdaten der Zugangsanbieter ist in Hinblick auf die **erst dann erfolgende** Individualisierung der IP-Adressen nicht ohne weiteres und nur unter besonderen Voraussetzungen möglich. Bei der Herausgabe der personenbezogenen Zugangsdaten durch den Zugangsanbieter sind die vom Bundesverfassungsgericht gezogenen Grenzen unter Berücksichtigung des Fernmeldegeheimnisses und des Datenschutzrechts selbstverständlich zu beachten.

Eine Vorverlagerung des Schutzes und eine uferlose Ausdehnung des Begriffs der personenbezogenen Daten in den Bereich der Speicherung der anonymen IP-Adressen ist nicht erforderlich, um Datenschutz und Fernmeldegeheimnis zu sichern (so auch Eckhardt, K&R 2007, 602, 604).

(2) Keine schrankenlose Übermittlung von IP-Adressen zulässig

Entgegen der Auffassung des AG Mitte ist es auch nicht zutreffend, dass 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). Wegen der Unzulässigkeit einer derartigen Übermittlung wäre der Kläger gerade nicht datenschutzrechtlich „völlig schutzlos". 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 (Gola/Schomerus, § 3 Rn. 10; Eckhardt, K&R 2007, 602, 603). 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 (Köcher, MMR 2007, 799, 801; Eckhardt, K&R 2007, 602, 603).

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 TMG, 3 Abs. 1 BDSG.

(3) Bestätigung durch Amtsgericht München

Das Amtsgericht München hat deshalb in einer Entscheidung vom 30. September 2008 (Az: 133 C 5677/08 = CR 2009, 59) den relativen Personenbezug dynamischer IP-Adressen ausdrücklich bestätigt. In der Entscheidung führt das AG München aus:

> *„Anders als vom Amtsgericht Berlin entschieden, sind nach hiesiger Auffassung dynamische IP-Adresse keine personenbezogenen Daten im Sinne des § 3 Abs. 1 Bundesdatenschutzgesetz. Damit fehlt es an einer Voraussetzung für den Unterlassungsanspruch.*
>
> *Nach diesseitiger Auffassung stellen die IP-Adressen deswegen keine personenbezogenen Daten dar, weil ihnen die notwendige Bestimmbarkeit fehlt. Bestimmbarkeit ist dann gegeben, wenn die datenspeichernde Stelle die hinter der Einzelangabe stehende Person mit den ihr normalerweise zur Verfügung stehenden Kenntnissen und Hilfsmitteln und ohne unverhältnismäßigen Aufwand bestimmen kann (vgl. Gola/Schomerus, BDSG, § 3 Rdnr. 10).*
>
> *IP-Adressen werden durch den von der Beklagten verschiedenen sogenannten Access Provider zeitlich begrenzt an Kunden vergeben, der Access Provider kann über die Bestandsdaten auch später den entsprechenden Nutzer ermitteln.*
>
> *Diese Möglichkeit steht der Beklagten nicht ohne weiteres zu. Die Beklagte könnte den Nutzer nur mit Hilfe des Access Providers ermitteln, der aber mangels Rechtsgrundlage den Betreiber eines Internetportals diese Angaben nicht zur Verfügung stellen darf.* ***Die theoretisch mögliche, aber illegale Möglichkeit einer Identifikation des Nutzers durch den Access Provider und Weitergabe der Daten an die Beklagte als Portalbetreiber kann vorgeschilderter Definition der Bestimmbarkeit der personenbezogenen Daten nicht entsprechen. Eine solch illegale Handlung kann kaum als normalerweise und ohne großen Aufwand durchzuführende Methode angesehen werden.“***

Dynamische IP-Adressen können daher für einen Betreiber eines Internetportals keine personenbezogenen Daten darstellen."

Anderes ergibt sich auch nicht aus den vom Kläger zitierten Urteilen des Schweizer Bundesverwaltungsgerichts und des Oberverwaltungsgerichts Stockholm. Beide Entscheidungen betonen vielmehr, dass die IP-Adresse für sich genommen nicht personenbezogen ist und ein Personenbezug erst durch Kenntnis der Daten des Zugangsanbieters hergestellt werden kann. Mit der rechtlichen Relevanz dieser Relativität des Personenbezugs setzen sich beide Entscheidungen jedoch nicht näher auseinander.

4. Keine Verletzung des Grundsatzes der Datensparsamkeit

Entgegen der Auffassung des Klägers führt der vom Bundesverfassungsgericht im Urteil vom 2. März 2010 zur Vorratsdatenspeicherung erwähnte Grundsatz der Datensparsamkeit nicht zu einer anderen Beurteilung der Rechtslage. Der Argumentation des Klägers liegt ein Zirkelschluss zugrunde.

Der Grundsatz der Datensparsamkeit bezieht sich nur auf personenbezogene Daten: die Speicherung personenbezogener Daten soll nach Möglichkeit vermieden und im Umfang beschränkt werden. Dies ist in § 3a BDSG ausdrücklich normiert.

Die vorliegend streitige Frage des (relativen) Personenbezugs von IP-Adressen ist somit gerade Voraussetzung sowohl für die Anwendbarkeit des Grundsatzes der Datensparsamkeit als auch des § 15 TMG. Es kann daher nicht im Wege eines Zirkelschlusses vom Grundsatz der Datensparsamkeit auf den Personenbezug und damit auf die Unzulässigkeit der Speicherung von IP-Adressen geschlossen werden.

Das Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung bezieht sich in dem vom Kläger daraus angeführten Absatz 270 zur Datensparsamkeit ausschließlich auf die Speicherung von IP-Adressen durch Telekommunikationsunternehmen bzw. Zugangsanbieter. Für die Zugangsanbieter sind die IP-Adressen aber - wie oben ausgeführt - unstreitig personenbezogene Daten. Die Frage des relativen Personenbezugs stellt sich in diesem Zusammenhang nicht und wurde daher auch vom Bundesverfassungsgericht nicht näher betrachtet.

5. Keine Verletzung eines „Rechts auf Anonymität"

Die Speicherung von IP-Adressen widerspricht auch nicht einem – wie auch immer gearteten – „Recht auf Anonymität". Das vom Kläger in diesem Zusammenhang behauptete „gesetzliche Aufzeichnungsverbot" existiert nicht.

Wie bereits mehrfach ausgeführt, ist der Beklagten allein aufgrund der IP-Adressen keine Individualisierung, d.h. kein Rückschluss auf konkrete Anschlussinhaber möglich. Es ist daher schon sachlich unzutreffend, dass bei einer Speicherung von IP-Adressen die Anonymität von Nutzungsvorgängen aufgehoben wird. Eine Personalisierung des Nutzers ist der Beklagten aufgrund der IP-Adresse nicht möglich (s. dazu oben). Die Personalisierung und Individualisierung durch die Zugangsprovider ist nur unter den vom Bundesverfassungsgericht gerade verschärften Voraussetzungen möglich. Für die Zugangsprovider sind die IP-Adressen ihrer Kunden deshalb auch unstreitig personenbezogene Daten.

Der vom Kläger in diesem Zusammenhang angeführte Vorlagenbeschluss des Verwaltungsgerichts Wiesbaden enthält insoweit keinerlei weiterführende Argumentation, sondern verweist schlicht ohne nähere Begründung auf die bereits oben zitierte Entscheidung des Amtsgerichts Mitte.

6. 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-Methode "POST"[1] an eine „hinter" dem For-

[1] HTTP-POST: Übertragung der Daten mit einer speziell dazu vorgesehenen Anfrageart in den HTTP-Kopfdaten, so dass diese in der URL nicht sichtbar sind und daher auch nicht in der Protokolldatei gespeichert werden

mular 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 Carsten Hein, 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 Carsten Hein, zu laden über die Beklagte

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

Beweis: 1. Zeugnis des Herrn Carsten Hein, 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.endlager-asse.de
www.behindertenbeauftragte.de
www.alle-inklusive.behindertenbeauftragte.de
www.bafin.de
www.bamf.de
www.integration-in-deutschland.de
www.baua.de
www.dasa-dortmund.de
www.gda-portal.de

www.reach-clp-helpdesk.de
www.biozid-portal.de
www.portal-produktsicherheit.de
www.zivildienst.de
www.bba.bund.de
www.bbk.bund.de
www.bdbos.bund.de
www.bescha.bund.de
www.gtai.de
www.bfarm.de
www.bfdi.bund.de
www.bfel.de
www.bundesjustizamt.de
www.bundesgerichtshof.de
www.bgr.bund.de
www.bib-demographie.de
www.bisp.de
www.bit.bund.de
www.ble.de
www.in-form.de
www.bmelv.de
www.bmg.bund.de
www.leben-hat-gewicht.de
www.neuegrippe.bund.de
www.bmg.bund.de
www.bevoelkerungsschutz-portal.de
www.bmi.bund.de
www.verwaltung-innovativ.de
www.zuwanderung.de
www.bnd.bund.de
www.bundespolizei.de
www.bundesrat.de
intranet.bundesrat.de
www.bsg.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de
www.bstu.bund.de
www.bund.de
www.bundesversicherungsamt.de
www.bvl.bund.de
www.aktionsplan-allergien.de
www.bevoelkerungsschutz.de
www.caf-netzwerk.de
www.ciec-deutschland.de
www.cio.bund.de
www.perspektive-it.de

www.d115.de
www.dehst.de
www.fn.de-mail.de
www.deutsche-islam-konferenz.de
www.dienstleistungszentrum.de
www.einfach-teilhaben.de
www.e-trade-center.de
www.freiheit-und-einheit.de
www.eu2007.bmi.bund.de
www.evergabe-online.info
www.favorit.de
www.government-site-builder.de
www.gsb-sl.bva.bund.de
www.intranet.bund.de
www.ixpos.de
www.portal21.de
www.kdb.bund.de
www.endlager-konrad.de
www.orghandbuch.de
www.pei.de
www.rki.de
www.umweltrat.de
www.thw.bund.de
www.anpassung.net
www.vertreter-des-bundesinteresses.de
www.vsz.bund.de
www.auslandsschulwesen.de
www.bva.bund.de

Beweis: Zeugnis des Herrn Carsten Hein, 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: Sachverständigengutachten

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 einer 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 Internetcafe oder einer Bibliothek oder irgendeinem anderen Internetanschluss zugeordnet war, ist nicht erkennbar. Hinzu kommt, dass es gerade bei Privatanschlüssen, 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 Carsten Hein, zu laden über die Beklagte

E. 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. Dass es ein legitimes Anliegen darstellen kann, Kommunikationsverbindungen im Internet zum Rechtsgüterschutz und zur Wahrung der Rechtsordnung den jeweiligen Akteuren zuordnen zu können, anerkennt das Urteil des BVerfG zur Vorratsdatenspeicherung vom 2. März 2010 in seinen Randziffern 260/261.

1. Konkrete Angriffszenarien und Sicherheitsmaßnahmen

Dies sei nachfolgend anhand diverser Angriffsszenarien und konkreter Sicherheitsmaßnahmen der Beklagten exemplarisch dargestellt, aus denen sichtbar ist, dass mit der zunehmenden Bedeutung des Internets auch die Gefahr seiner Nutzung für Straftaten und Rechtsverletzungen vielfältiger Art zunimmt.

a) Zur Erkennung und Abwehr von sogenannten DOS-Angriffen („denial of service", d. h. ein „Lahmlegen" der TK-Infrastruktur durch gezieltes und koordiniertes Fluten einzelner Webserver mit einer Vielzahl von Anfragen) wird ein Anomalieerkennungssystem (z. B. McAfee IntruShield Network Security Platform) 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 Dr. Dirk Häger, 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 Webservers 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 CERT[2] 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.

[2] „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.

Beweis: wie vor

d) Eine Bundesbehörde betreibt einen Webserver. Ein Angreifer versucht, einen nur ihm bekannten Fehler des Webservers 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.

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 Webservers genutzt wird (eventuell auch als Teil eines Bot-Netzes). 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 geschenen 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

F. 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 und stellt diese ihren Behörden und Dienststellen zur Nutzung zur Verfügung. 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 Dr. Dirk Häger, 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 – als Betreiberin der Netze des Bundes – 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 unstreitig 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 Telekommunikationsanlagen 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).

G. Zulässigkeit der Speicherung nach § 5 BSI-Gesetz

Eine Speicherung der IP-Adressen ist unabhängig von deren Personenbezug auch unter den Voraussetzungen des § 5 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) zulässig. Nach § 5 Abs. 1 Nr. 1 BSIG darf das Bundesamt für Sicherheit in der Informationstechnik (BSI) Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die IT-Technik des Bundes erforderlich ist.

Protokolldaten umfassen nach § 2 Abs. 8 BSIG Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind. IP-Adressen sind Steuerdaten im Sinne dieser Regelung, die bei der Internet-gestützten Kommunikation anfallen und zum Datenaustausch zwischen den beteiligten Systemen zwingend erforderlich sind.

Beweis: Sachverständigengutachten

Protokolldaten können nach § 2 Abs. 8 S. 2 BSIG auch Nutzungsdaten gemäß § 15 Abs. 1 TMG umfassen. Es kommt somit für die Zulässigkeit der Speicherung von IP-Adressen nach dem BSI-Gesetz nicht auf den Personenbezug der IP-Adressen an. Die Klage wäre jedenfalls insoweit abzuweisen, als eine Speicherung der Daten nach sondergesetzlichen Vorschriften, insbesondere nach § 5 BSIG, zulässig ist.

H. Zulassung der Revision

Das Landgericht hat bereits in seinem Beschluss vom 1. April 2009 zum Geschäftszeichen 57 T 62/08 die grundsätzliche Bedeutung der Rechtssache festgestellt. Dies gilt nicht nur für die Frage des Gegenstandswertes, sondern auch für die hier zentrale materiell-rechtlichen Rechtsfragen, insbesondere in wie weit es sich bei der streitgegenständlichen IP-Adresse um für die Beklagte personenbezogene Daten handelt. Die bisherige Rechtsprechung der Gerichte hierzu ist höchst uneinheitlich. Es liegen somit beide Fallgruppen für die Zulassung der Revision gemäß § 543 Abs. 2 Satz 1 ZPO vor.

Wir beantragen daher, für den Fall dass das Berufungsgericht die Entscheidung des Amtsgerichtes aufheben und der Klage stattgeben sollte,

die Revision zuzulassen.

Wir stellen zu.

[redacted]

Rechtsanwalt