Meinhard Starostik

Rechtsanwalt

Rechtsanwaltskanzlei:
Schillstr. 9 ◆ 10785 Berlin
Tel.: 030 - 88 000 345
Fax: 030 - 88 000 346
email: Kanzlei@Starostik.de
USt-ID-Nr. DE165877648

Kanzlei vereidigter Buchprüfer:
Schwarzenberger Str. 7 ◆ 08280 Aue
Tel.: 03771-290 999

RA Starostik, Schillstraße 9, 10785 Berlin

An das
Landgericht Berlin
Littenstr. 12-17
10179 Berlin

Berlin, den ??. September 2011

AZ: 45/08
(bitte stets angeben)

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

wird nunmehr seitens des Klägers beantragt,

das gem. § 148 ZPO ausgesetzte Verfahren wieder aufzunehmen.

Wir stellen

die Anträge zu a und b aus der Berufungsbegründung.

Der Antrag zu c aus der Berufungsbegründung wird zurückgenommen.

Mit einer Entscheidung ohne mündliche Verhandlung erklärt sich der Kläger einverstanden.

Begründung:

Nachdem der Bundesgerichtshof die Beschwerde der Beklagten verworfen hat, ist die Festsetzung des **Streitwerts** auf 4.000 Euro rechtskräftig. Damit kann das Berufungsverfahren wieder aufgenommen werden. Vorsorglich weise ich darauf hin, dass die Beklagte auch mit einer Revision nicht geltend machen könnte, das Landgericht habe zu Unrecht die Zuständigkeit des Amtsgerichts – und damit auch seine eigene Zuständigkeit – angenommen.[1]

An dem Antrag zu c aus der Berufungsbegründung, den Rechtsstreit gegebenenfalls nach § 538 Abs. 2 ZPO an das Amtsgericht **zurückzuverweisen**, hält der Kläger nicht fest. Nach diversen Fristverlängerungsanträgen und einer unzulässigen Beschwerde der Beklagten dauert das Verfahren nun schon annähernd zwei Jahre lang. Eine Zurückverweisung würde das Verfahren weiter verzögern, zumal die Beklagte gegen eine stattgebende Entscheidung des Amtsgerichts sicherlich wieder Rechtsmittel einlegen würde. Um eine angemessene Verfahrensdauer zu wahren, bittet der Kläger daher um eine Sachentscheidung durch das Berufungsgericht. Eine Zurückverweisung

[1] Vgl. BGH, NJW 2003, 2917.

wäre ohnehin nur zum Zweck einer Beweisaufnahme in Betracht gekommen, die hier nicht erforderlich sein dürfte, da nur Rechtsfragen im Streit stehen.

Der Rechtsstreit ist nach Auffassung des Klägers entscheidungsreif. Die Beklagte bringt gegen die **schlüssige Klage** weiterhin keine erheblichen Einwendungen vor, sondern beruft sich nur auf eine unzutreffende Rechtsauffassung (kein Personenbezug) und auf einen nicht anwendbaren Erlaubnistatbestand (§ 100 TKG). Insoweit wird auf die Berufungsbegründung und auf die erstinstanzlichen Ausführungen vollumfänglich Bezug genommen.

Zu ergänzen sind diese Ausführungen nur in den folgenden Punkten:

I. Personenbezug

Der Personenbezug von IP-Adressen ist im europäischen Ausland inzwischen höchstrichterlich bestätigt worden.

Das Bundesverwaltungsgericht der Schweiz hat mit Urteil vom 27.05.2009[2] entschieden:

> „2.2.1 Unter Personendaten (Daten) fallen nach Art. 3 Bst. a DSG **alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen.** Darunter ist jede Art von Information zu verstehen, die auf die Vermittlung oder die Aufbewahrung von Kenntnissen ausgerichtet ist, ungeachtet, ob es sich dabei um eine Tatsachenfeststellung oder um ein Werturteil handelt. Unerheblich ist auch, ob eine Aussage als Zeichen, Wort, Bild, Ton oder Kombinationen aus diesen auftritt und auf welcher Art von Datenträger die Informationen gespeichert sind. Entscheidend ist, dass sich die Angaben einer oder mehreren Personen zuordnen lassen (URS BELSER, in: Maurer-Lambrou/Vogt [Hrsg.], Datenschutzgesetz, Basler Kommentar, 2. Aufl., Basel 2006, Rz. 5 zu Art. 3 DSG).
>
> Eine Person ist dann bestimmt, wenn sich aus der Information selbst ergibt, dass es sich genau um diese Person handelt. Bestimmbar ist sie dann, wenn aus dem Kontext einer Information auf sie geschlossen werden kann. Für die Bestimmbarkeit genügt aber nicht jede theoretische Möglichkeit der Identifizierung. Ist der Aufwand für die Bestimmung der betroffenen Personen derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird, liegt keine Bestimmbarkeit vor (vgl. Botschaft des Bundesrates vom 23. März 1988 zum DSG, Bundesblatt [BBl] 1988 II, S. 444 f.). Ob eine Person bestimmbar ist, muss anhand objektiver Kriterien im konkreten Fall beurteilt werden, wobei insbesondere auch die Möglichkeiten der Technik, wie zum Beispiel die beim Internet verfügbaren Suchwerkzeuge, mitzuberücksichtigen sind. **Entscheidend ist nicht, ob derjenige, der die Daten bearbeitet, den für eine Identifizierung erforderlichen Aufwand betreiben kann oder will, sondern ob damit gerechnet werden muss, dass ein Dritter, der ein Interesse an diesen Angaben hat, bereit ist, eine Identifizierung vorzunehmen** (BELSER, a.a.O., Rz. 6 zu Art. 3 DSG; DAVID ROSENTHAL, in: Rosenthal/Jöhri, Handkommentar zum Datenschutzgesetz, Zürich 2008, Rz. 24 f. zu Art. 3 DSG). […]

[2] Az. A-3144/2008, http://relevancy.bger.ch/pdf/azabvger/2009/a_03144_2008_2009_05_27_t.pdf.

2.2.3 Hinsichtlich der Qualifikation von IP-Adressen als Personendaten rechtfertigt sich eine vergleichende Betrachtung der Rechtslage in der Europäischen Union: Die Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten (nachfolgend **Datenschutzgruppe**) wurde durch Art. 29 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 eingesetzt und ist ein unabhängiges EU-Beratungsgremium für Datenschutzfragen. In ihrer am 20. Juni 2007 angenommenen Stellungnahme 4/2007 zum Begriff ‚personenbezogene Daten' stuft die Datenschutzgruppe mit Verweis auf ein früheres Arbeitspapier (Arbeitsdokument WP 37, Privatsphäre im Internet – Ein integrierter EU-Ansatz zum Online-Datenschutz, angenommen am 21. November 2000, insbesondere S. 17) IP-Adressen als Daten ein, die sich auf eine bestimmbare Person beziehen. Internet-Zugangsanbieter und Verwalter von lokalen Netzwerken könnten ohne grossen Aufwand Internetnutzer identifizieren, denen sie IP-Adressen zugewiesen hätten, da sie in der Regel in Dateien systematisch Datum, Zeitpunkt, Dauer und die dem Internetnutzer zugeteilte dynamische IP-Adresse einfügen würden. Dasselbe lasse sich von den Internet-Dienstanbietern sagen, die in ihren HTTP-Servern Protokolle führen würden. In diesen Fällen bestehe kein Zweifel, dass man von personenbezogenen Daten im Sinne von Art. 2 Bst. a der Richtlinie 95/46/EG reden könne.

Weiter wird in der Stellungnahme zum Begriff ‚personenbezogene Daten' ausdrücklich auf jene Fälle hingewiesen, in denen der Zweck der Verarbeitung von IP-Adressen in der Identifizierung der Computernutzer besteht, beispielsweise durch Inhaber von Urheberrechten zur strafrechtlichen Verfolgung wegen Verletzung von Rechten an geistigem Eigentum. Vor allem in diesen Fällen gehe der für die Verarbeitung Verantwortliche vom Vorhandensein der Mittel aus, die zur Identifizierung der betreffenden Personen ‚vernünftigerweise eingesetzt werden könnten', zum Beispiel von den Gerichten, bei denen Beschwerde eingelegt worden sei. Andernfalls sei die Erhebung der Informationen nicht sinnvoll. Einen Sonderfall würden IP-Adressen bilden, die unter bestimmten Umständen aus verschiedenen technischen und organisatorischen Gründen keine Identifizierung des Nutzers gestatten würden, wie beispielsweise bei einem Computer in einem Internet-Café, in dem keine Identifizierung der Kunden gefordert werde. Es könne argumentiert werden, dass hier keine personenbezogenen Daten vorlägen, da der Nutzer unter Einsatz vernünftiger Mittel nicht identifiziert werden könne. In diesem Fall sei jedoch zu berücksichtigen, dass ein Internet-Dienstanbieter in der Regel nicht wissen könne, ob eine bestimmte IP-Adresse die Identifizierung ermögliche oder nicht. **Wenn der Internet-Dienstanbieter also nicht mit absoluter Sicherheit erkennen könne, dass die Daten zu nicht bestimmbaren Benutzern gehören würden, müsse er sicherheitshalber alle IP-Informationen wie personenbezogene Daten behandeln** (Stellungnahme, S. 19 f.).

2.2.4 Bei IP-Adressen handelt es sich um technische Informationen, die eine eindeutige Identifizierung eines Rechners zulassen. **Dabei können statische IP-Adressen, die einem Rechner fest zugeteilt sind, wie die Beklagte in ihrer Duplik selber darlegt, vergleichbar einer Telefonnummer als Personendaten qualifiziert werden. Im Ergebnis muss dasselbe aber auch für dynamische IP-Adressen gelten:** Zwar können weder die Beklagte

> noch die Urheberrechtsinhaber selber die hinter einer IP-Adresse stehende Person bestimmen. Der Provider muss diese Information nur im Zusammenhang mit der Verfolgung von Straftaten und nur gegenüber Behörden offenlegen. Die Person ist daher lediglich anhand der IP-Adresse nicht bestimmbar (ROSENTHAL, a.a.O., Rz. 27 zu Art. 3 DSG). Wird jedoch eine Straftat verübt, ändert sich die Situation. Nicht nur steigt das Interesse an der Bestimmung der Person hinter der IP-Adresse, mit der Einleitung einer Strafuntersuchung erhält der Urheberrechtsinhaber auch indirekt das Mittel in die Hand, die Person zu identifizieren. Dadurch werden die betreffenden Aufzeichnungen automatisch zu Personendaten auch bezüglich der so ermittelbaren bzw. ermittelten Person und nicht mehr nur des registrierten Inhabers der IP-Adresse (ROSENTHAL, a.a.O., Rz. 27 zu Art. 3 DSG). Wie die Praxis zeigt, sind gerade Urheberrechtsinhaber bereit, strafrechtlich vorzugehen, um die Identifizierung der Daten von Internetnutzern zu erwirken. Sie können, objektiv betrachtet, ein konkretes Interesse an der entsprechenden Information für sich beanspruchen. Daher ist auch damit zu rechnen, dass ein in seinen Rechten verletzter Urheberrechtsinhaber den nötigen Aufwand auf sich nimmt, diese Daten zu identifizieren. Ob sodann ein Strafverfahren zum gewünschten Erfolg führt oder allenfalls im konkreten Fall vorzeitig eingestellt wird, ändert dagegen nichts an der grundsätzlichen Bestimmbarkeit der Daten. In diesem Sinne erachtet auch die Datenschutzgruppe der Europäischen Union dynamische IP-Adressen als personenbezogene Daten gemäss Art. 2 Bst. a der Richtlinie 95/46/EG, deren Definition von Personendaten sehr ähnlich ist mit derjenigen in Art. 3 Bst. a DSG.
>
> **IP-Adressen sind folglich entgegen der Ansicht der Beklagten als Personendaten im Sinne des DSG anzusehen.**“

Diesen Ausführungen ist im Grunde nichts hinzuzufügen.

Das **Oberverwaltungsgericht (Kammarrätt) Stockholm** hat bereits am 8. Juni 2007 entschieden, dass IP-Adressen allgemein personenbezogene Daten im Sinne der EG-Datenschutzrichtlinie 95/46/EG sind.[3] Es hat diese Entscheidung zusammenfassend wie folgt begründet:

Da das schwedische Datenschutzgesetz der Umsetzung der **Richtlinie 95/46/EG** diene, sei es in deren Licht auszulegen. Nach Art. 2 finde die Richtlinie 95/46/EG Anwendung auf personenbezogene Daten. Personenbezogene Daten seien danach „alle Informationen über eine bestimmte oder bestimmbare natürliche Person (‚betroffene Person‘); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind“. Erwägungsgrund 26 der Richtlinie 95/46/EG besage, bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Die Schutzprinzipien finden keine Anwendung auf Daten, die derart anonymisiert sind, dass die betroffene Person nicht mehr identifizierbar ist.

[3] Az. 285-07, http://arkiv.idg.se/it24/SthlmRRejpt_3978_07.pdf.

In Verbindung mit den Daten des Internet-**Zugangsanbieters könne die Person ermittelt werden**, über deren Internetanschluss die Nutzung erfolgt sei. Der Anschlussinhaber könne eine natürliche Person sein. Dass sich nicht ermitteln lässt, wer diesen Internetzugang tatsächlich genutzt hat, ändere an dem Personenbezug nichts, weil die IP-Adresse jedenfalls auf die Person des Anschlussinhabers rückschließen lasse. Dass der Kläger – das schwedische „Anti-Piracy-Office" – die Rückführung der von ihm gespeicherten IP-Adresse auf die Person des Anschlussinhabers nicht selbst auf legale Weise vornehmen könne, sei nach dem Erwägungsgrund 26 der Richtlinie unerheblich. Im Übrigen sammele der Kläger die IP-Adressen von Tauschbörsenteilnehmern gerade zu dem Zweck, die Teilnehmer identifizieren zu lassen. IP-Adressen seien auch nicht anonymisiert in einer Weise, in der die betroffene Person nicht mehr identifizierbar sei.

Am 16. Juni 2009 hat das **oberste schwedische Verwaltungsgericht** – der dem Bundesverwaltungsgericht vergleichbare „Regeringsrätten" – das eingelegte Rechtsmittel gegen die Entscheidung zurückgewiesen,[4] so dass das Urteil rechtskräftig ist.

Dass der Personenbezug dadurch entfalle, dass die zur Identifizierung erforderlichen Daten **bei verschiedenen Stellen gespeichert** und Zusammenführungen verboten seien, widerlegt jetzt auch Ott überzeugend in einem Aufsatz. Er führt ein systematisches Argument an, welches an § 15 Abs. 3 TMG anknüpft:[5]

> „Schon die Regelung zur Pseudonymisierung zeigt, dass bei der Bestimmung des Personenbezugs die **Kombinationsmöglichkeiten** mit Daten eigener anderer Dienste zu berücksichtigen sind. Würde die getrennte Speicherung von Identifikationsmerkmal und pseudonymisierten Daten, deren Zusammenführung sogar [unter Bußgeldandrohung] gesetzlich verboten ist (§ 15 Abs. 3 S. 3 TMG), dazu führen, dass der Personenbezug entfällt, würde dadurch der Anwendungsbereich des Datenschutzrechts entfallen und die Regelung zur Pseudonymisierung leer laufen, weil die getrennte Speicherung von Name und eigentlichen Informationen dann keiner Ermächtigungsgrundlage mehr bedürfte."

Abschließend nehme ich Bezug auf den ausführlichen Aufsatz **von Pahlen-Brandt** in K&R 2008, 288, den ich diesem Schriftsatz als Anlage beifüge.

II. Gesetzliches Aufzeichnungsverbot für die Internetnutzung

In der Entscheidung zum Internet-Bewertungsportal www.spickmich.de hat sich der **Bundesgerichtshof** erstmals zum Anspruch auf spurenlose Nutzung von Telemedien geäußert und ausgeführt:[6]

> „Die **anonyme Nutzung ist dem Internet immanent** (vgl. Senatsurteil vom 27. März 2007 - VI ZR 101/06 - VersR 2007, 1004, 1005). Dementsprechende Regelungen zum Schutz der Nutzerdaten gegenüber dem Diensteanbieter finden sich in den §§ 12 ff. TMG, den Nachfolgeregelungen zu § 4 Abs. 4 Nr. 10 TDG. Eine Beschränkung der **Meinungsäußerungsfreiheit** auf Äußerungen, die einem bestimmten Individuum zugeordnet werden können,

[4] Az. 3978-07.

[5] Ott, KuR 2009, 308 (311).

[6] Urteil vom 23.06.2009, Az. VI ZR 196/08, NJW 2009, 2888.

> ist mit Art. 5 Abs. 1 Satz 1 GG nicht vereinbar. Die Verpflichtung, sich namentlich zu einer bestimmten Meinung zu bekennen, würde nicht nur im schulischen Bereich, um den es im Streitfall geht, die Gefahr begründen, **dass der Einzelne aus Furcht vor Repressalien oder sonstigen negativen Auswirkungen sich dahingehend entscheidet, seine Meinung nicht zu äußern.** Dieser Gefahr der Selbstzensur soll durch das Grundrecht auf freie Meinungsäußerung entgegen gewirkt werden (vgl. Ballhausen/Roggenkamp K&R 2008, 403, 406).
>
> [...] Für Datenabfragen aus Bewertungsforen führt mithin die wortgetreue Anwendung der Vorschriften in § 29 Abs. 2 Nr. 1 a und 2 BDSG zu keinem Widerspruch zu dem sich aus Art. 5 Abs. 1 GG ergebenden **Recht auf uneingeschränkte Kommunikationsfreiheit**. Sie ist auch nicht vereinbar mit dem bis 28. Februar 2007 in § 4 Abs. 6 Teledienstedatenschutzgesetz und seit 1. März 2007 in den §§ 12 ff. TMG gewährleisteten **Recht des Internetnutzers auf Anonymität**. [...]"

Der Bundesgerichtshof hat damit bestätigt, dass Internetnutzer ein „**Recht auf Anonymität**" haben und dass dieses Recht einfachgesetzlich in den §§ 12 ff. TMG gewährleistet ist.

Zweitens hat der Bundesgerichtshof bestätigt, dass es mit der in Art. 5 Abs. 2 S. 1 GG grundrechtlich geschützten **Meinungsfreiheit** unvereinbar wäre, wenn man seine Meinung im Internet nicht anonym äußern könnte. Eben dies ist aber die Folge der beklagtenseits praktizierten Protokollierung sämtlicher Serverzugriffe, etwa wo die Beklagte Internet-Meinungsforen anbietet.[7] In solchen Foren kann man seine Meinung wegen der Protokollierung von Nutzungsdaten nicht anonym äußern.

Art. 5 Abs. 2 S. 1 GG schützt indes nicht nur „das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten", sondern ebenso das Recht, „sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten". Die **Informationsfreiheit** steht in der grundgesetzlichen Ordnung gleichwertig neben der Meinungs- und Pressefreiheit.[8] Beide Rechte beschränken sich nicht auf Werturteile, sondern erfassen grundsätzlich auch Tatsachenmitteilungen.[9] Denn die Kenntnis von Tatsachen ist die Voraussetzung dafür, dass man sich eine Meinung zu einer Frage überhaupt bilden kann. [10]

Besteht aber ein Recht zur anonymen Meinungsäußerung, so muss auch ein **Recht auf anonyme Information** über Meinungen und Tatsachendarstellungen bestehen. Ebenso wie die Identifizierbarkeit jedes Bürgers, der im Internet seine Meinung äußert, Art. 5 GG verletzt, verletzt die personenbeziehbare Protokollierung jedes Informationsabrufs – und damit die Protokollierungspraxis der Beklagten – das Grundrecht aus Art. 5 Abs. 1 S. 1 GG. Denn auch eine Aufzeichnung des Informationsverhaltens würde – in den Worten des Bundesgerichtshofs – „die Gefahr begründen, dass der Einzelne aus Furcht vor Repressalien oder sonstigen negativen Auswirkungen sich dahingehend entscheidet", von dem Abruf öffentlich zugänglicher Informationen abzusehen. Diese Gefahr besteht etwa dort, wo aus dem Seitenabruf wegen des Inhalts der Seite oder des Telemediums auf politische Meinungen, religiöse

[7] Beispielsweise http://www.bmg.bund.de/bmg_forum/ und http://www.cio.bund.de/kbst_forum/, wo ausdrücklich auch die IP-Adressen der Nutzer festgehalten werden.
[8] BVerfGE 27, 71 (81).
[9] BVerfGE 85, 1 (15).
[10] BVerfGE 85, 1 (15).

Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben des Internetnutzers geschlossen werden kann.

Die abschreckende Wirkung einer Speicherung **schadet mittelbar auch der Meinungsfreiheit und unserem Gemeinwesen überhaupt**. Denn nur umfassende Informationen, die man ungehindert und unbefangen zur Kenntnis nehmen kann, ermöglichen eine freie Meinungsbildung und -äußerung für den Einzelnen wie für die Gemeinschaft.[11] Nur auf der Grundlage eines freien und unbefangenen Informationszugangs kann der Bürger informiert politische Entscheidungen treffen und am freiheitlichen demokratischen Gemeinwesen mitwirken. Ein registrierungsfreier Informationszugang ist heutzutage elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens.

In zwei Beschlüssen vom 27.02.2009[12], die das von der Beklagten betriebene Internetportal www.agrar-fischerei-zahlungen.de betreffen, hat das **Verwaltungsgericht Wiesbaden** inzwischen bestätigt:

> „Der Anwendungsbereich der Datenschutzrichtlinie 95/46/EG und des deutschen Datenschutzrechts einschließlich § 15 TMG hängt davon ab, ob es sich dabei um ein **personenbezogenes Datum** handelt, weil eine Zuordnung zu einer bestimmbaren Person möglich ist, gleichwohl, ob es sich um eine statische oder dynamische IP-Adresse handelt.
>
> Die IP-Adresse ist ein numerisches Adressformat, welches die Kommunikation vernetzter Geräte (Server oder Privatcomputer) im Internet ermöglicht. Bei Abruf einer Seite wird dem Server, auf dem die Seite gespeichert ist, die Adresse des abrufenden Computers mitgeteilt, so dass die Daten über das Internet von dem einen an den anderen Rechner geleitet wird en können. Für die Verbindung von Privatanwendern mit dem Internet können **feste IP-Adressen** vergeben werden. Dabei handelt es sich nach Ansicht des Gerichts ohne weiteres um ein personenbezogenes Datum. Üblicherweise werden dynamische IP-Adressen verwendet. Dabei weist der Anbieter des Zugangs dem Kunden bei jedem Zugang eine Adresse aus seinem Adresskontingent zu. Aus der Adresse kann der Einwahlstandort des Benutzers abgelesen werden.
>
> In der Rechtssache Promusicae/Telefonica hat die Generalanwältin die Ansicht vertreten, dass eine dynamischen IP-Adresse personenbezogene Daten enthält (vgl. Schlussanträge Promusicae/Telefonica, a.a.O., Rn. 61 und die Nachweise in Fußnote 31). In seinem Urteil vom 29.01.2008 in dieser Rechtssache hat sich der Gerichtshof ausdrücklich mit dieser Frage aber nicht beschäftigt. Das Amtsgericht Berlin-Mitte hat einer Klage eines Benutzers der Internetseite des Bundesministeriums der Justiz gegen die Speicherung seiner IP-Adresse stattgegeben, weil über die dynamische IP-Adresse der Benutzer identifiziert werden könne (Urteil vom 27.03.2007, 5 C 314/06, zitiert nach juris). Das Amtsgericht Berlin-Mitte stützte sich maßgeblich auf die 26. Begründungserwägung der Richtlinie 95/46/EG. Danach sollten bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die

[11] Vgl. BVerfGE 27, 71 (81).

[12] Az. 6 K 1045/08WI, MMR 2009, 428; Az. 6 K 1352/08WI, NVwZ 2009, 1183.

> betreffende Person zu bestimmen. Die Berufung der Beklagten erstreckte sich nur auf die Reichweite der Unterlassungsverpflichtung. Der Rechtstreit ist rechtskräftig abgeschlossen (vgl. Landgericht Berlin, Urteil vom 06.09.2007, 23 S 3/07, zitiert nach juris). In der deutschen Literatur wurde dieser Rechtsprechung widersprochen. Das Gericht ist aber der Auffassung, dass auch eine **dynamische IP-Adresse ein personenbezogenes Datum** ist. Davon geht auch die Artikel 29-Datenschutzgruppe in ihrem Arbeitsdokument WP 104 vom 18.01.2005 aus (Nr. III. 3., S. 19 ff., 01248/07/DE); bekräftigend in der Stellungnahme WP 150 vom 15.05.2008 (Nr. 3b, S. 8, 00989/08/DE). **Da die Speicherung der IP-Adresse nicht erforderlich ist, steht die Richtlinie 95/46/EG ihr entgegen.**
>
> Nach den Angaben des Sachverständigen B sollen in Zukunft bei den Internetseiten hessischer Behörden die IP-Adressen zu statistischen Zwecken anonymisiert werden, aus Gründen der Datensicherheit aber ungekürzt gespeichert werden. Die Speicherfristen für die vollständig gespeicherten IP-Adressen durfte er auf Nachfrage des Gerichts aus Geheimhaltungsgründen nicht angeben. Da die Beigeladene ihre Seite im Auftrag auch des Landes Hessen betreibt, geht das Gericht davon aus, dass eine Speicherung nach der Praxis hessischer Behörden stattfindet. Diese wäre **mangels einer gesetzlichen Grundlage** im hessischen Landesrecht nur zulässig, wenn es sich bei einer IP-Adresse nicht um ein personenbezogenes Datum handelt."

Das Verwaltungsgericht Wiesbaden hat also nicht nur den Personenbezug der beklagtenseits erstellten Nutzungsprotokolle bestätigt, sondern auch die **Unzulässigkeit** dieser Protokolle.

Ebenso schreibt der **Bundesdatenschutzbeauftragte** in seinem neuesten Tätigkeitsbericht:[13]

> „Das Telemediengesetz setzt dem Anbieter einer Website für die Verwendbarkeit der technischen Nutzungsdaten (Protokolldaten), die der Nutzer beim Besuch eines Internet-Angebots hinterlässt, enge Grenzen. Erlaubt ist ihm danach die Verarbeitung für die technische Durchführung des Dienstes und für Abrechnungszwecke. Darüber hinaus dürfen die Nutzungsdaten im Einzelfall nur dann verwendet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte für eine Leistungserschleichung vorliegen. **Eine Verarbeitungsbefugnis für Datensicherheitszwecke oder – vorsorglich – für Strafverfolgungszwecke besteht nicht.** Ebenso wenig zulässig ist die von einer Vielzahl der Website-Anbieter durchgeführte statistische Auswertung der Nutzungsdaten, da hierbei die IP-Adressen der Besucher, die als personenbezogene Daten anzusehen sind, verwendet werden.
>
> Die Praxis vieler Anbieter steht im Widerspruch zu diesen strengen gesetzlichen Vorgaben. So speichern und verwenden manche Anbieter Nutzungsdaten zu Datensicherheitszwecken und für statistische Auswertungen. Vorschläge, das Problem dadurch zu lösen, dass man IP-Adressen kurzerhand zu nicht personenbezogenen Daten erklärt, was dann für die gesamten Nutzungsdaten gelten würde, hätte fatale datenschutzrechtliche Konsequenzen. Damit wäre jede beliebige Verwendung der Nutzungsdaten unabhängig von der Zweckbestimmung für den Anbieter

[13] Bundesbeauftragter für den Datenschutz, Tätigkeitsbericht 2007/2008, http://twiturl.de/TB0708, 96.

> und letztlich sogar für jedermann möglich (vgl. Nr. 7.11). Unter Verwendung der beim Zugangsprovider vorhandenen Informationen ist jedoch immer ein Personenbezug herstellbar. Ebenso, wenn von einem Internet-Anbieter formularmäßig auch persönliche Daten, z. B. bei einer Bestellung, erhoben werden. **Allein schon aus diesen Gründen sind IP-Adressen im Regelfall als personenbezogene Daten anzusehen.** Dafür spricht aber vor allem, dass Strafverfolgungsbehörden gerade die IP-Adressen, die bei Internet-Anbietern anfallen, dazu verwenden, die Identität mutmaßlicher Täter zu ermitteln (s. u. Nr. 7.10)."

Auch der Bundesdatenschutzbeauftragte bestätigt mithin Personenbezug und **Protokollierungsverbot**.

Ausweislich eines **Schreibens des Bundesjustizministeriums** vom 02.02.2009[14] über das Internetportal www.bundeskriminalamt.de ist inzwischen sogar die Beklagte selbst zu der folgenden Einsicht gelangt:

> „Das Bundesministerium des Innern und das Bundesministerium der Justiz haben Fragen der Zulässigkeit der Homepageüberwachung geprüft und sind hierbei zu dem Ergebnis gelangt, dass die Homepageüberwachung **durchgreifenden Bedenken** begegnet. Die wesentlichen Gesichtspunkte hierbei sind:
>
> Die Homepageüberwachung führt zu einer **Speicherung und Verwendung personenbeziehbarer und damit personenbezogener Daten im Sinne des § 3 Abs. 1 BDSG**, mithin zu einem Eingriff in das Grundrecht auf informationelle Selbstbestimmung, der dem Gesetzesvorbehalt unterliegt. Darüber hinaus erscheint auch das durch Art. 5 Abs. 2 Satz 1 GG geschützte Recht, sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten, beeinträchtigt. [...]
>
> Das Betreiben der (Fahndungs)Webseite ist ein Telemediendienst im Sinne des § 1 Abs. 1 TMG. Nach § 15 Abs. 1 Satz 1 TMG dürfen personenbezogene Daten eines Nutzers (Nutzungsdaten) nur erhoben und gespeichert werden, soweit dies erforderlich ist, um die Inanspruchnahme des Telemediendienstes zu ermöglichen und abzurechnen. **Nutzungsdaten sind nach § 15 Abs. 1 Satz 2 TMG insbesondere Merkmale zur Identifikation des Nutzers, wie z. B. die IP-Adresse**, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung (Zeitpunkte des Besuchs der Fahndungswebseite) und Angaben über die vom Nutzer in Anspruch genommenen Telemedien (Fahndungsseite).
>
> Zur Inanspruchname des Dienstes müssen diese Daten vorliegend nicht über den Zeitraum der Inanspruchnahme (Besuch der Webseite) hinaus gespeichert oder verwendet werden. Auch eine Abrechnung im Sinne des § 15 Abs. 1 Satz 1 TMG kommt bei unentgeltlich betriebenen Fahndungswebseiten nicht in Betracht. Da auch eine nach § 12 TMG grundsätzlich mögliche, nach § 13 TMG indessen an mehrere Voraussetzungen geknüpfte Einwilligung der Nutzer in die Erhebung und Verwendung der Daten regelmäßig nicht vorliegen wird, **ist die Verwendung der vorgenannten Daten gemäß § 15 Abs. 4 TMG über das Ende des Nutzungsvorgangs hinaus nicht zulässig.**"

[14] Az. RB3 -zu 4104/8 – 1 – R5 39/2008, http://www.daten-speicherung.de/data/bmj_2009-02-02.pdf.

Von dem Hintergrund dieses Schreibens muss man es als Skandal bezeichnen, dass die Beklagte ihre Surfprotokollierung auf anderen Portalen gleichwohl fortsetzt, damit **wissentlich Recht und Gesetz verletzt** und vor Gericht eine Auffassung vorträgt, die in Wahrheit nicht die ihre ist.

Dass die Beklagte wider besseres Wissen handelt, ergibt sich auch aus einer Angabe der Bundesnetzagentur gegenüber dem Bundesdatenschutzbeauftragten. Auf die Frage, auf welcher **Rechtsgrundlage** die Bundesnetzagentur IP-Adresse, Datum/Uhrzeit, URL, Referrer und Browser jedes Nutzers ihres Bürgerportals aufzeichnet, antwortete die Bundesnetzagentur: „nicht erkennbar". Das Bundespresseamt, welches die Internetseite des Bundeskanzleramts betreibt, gab als Rechtsgrundlage seiner Surfprotokollierung an: „nach Urteil Berlin: Lücke". Das Auswärtige Amt antwortete auf die Frage nach der Rechtsgrundlage immerhin: „da es keine gibt, zukünftig keine Speicherung der IP-Adressen". Es ist beschämend für einen Rechtsstaat, dass sich nicht alle Behörden der Beklagten so einsichtig verhalten und dass sich insbesondere das Bundesinnenministerium wider besseren Wissens weigert, die vorliegende Klage anzuerkennen und das geltende Recht umzusetzen.

In dieser Situation bleibt dem Kläger nur die vorliegende Klage, um die Beklagte zu zwingen, die **rechtswidrige Aufzeichnung des Internet-Nutzungsverhaltens** des Klägers einzustellen.

Beglaubigte und einfache Abschrift anbei.

Meinhard Starostik
Rechtsanwalt