

SCHULTZ · SCHOTT
Rechtsanwälte beim Bundesgerichtshof

SCHULTZ · SCHOTT · Stephaniensstraße 57 · 76133 Karlsruhe

An den
BUNDESGERICHTSHOF
- VI. Zivilsenat -

KARLSRUHE

Dr. Ekkehart Schott
Dr. Michael Schultz

Prof. Dr. Rudolf Nirk (bis 2010)

Stephaniensstraße 57
76133 Karlsruhe

Telefon: +49 (0) 721 / 18 31 53 0
Telefax: +49 (0) 721 / 18 31 53 19
E-Mail: kanzlei@bgh-schultz-schott.de
Internet: <http://www.bgh-schultz-schott.de>

10.12.2013 / H

REVISIONSBEGRÜNDUNG

in Sachen

Breyer

./.
Bundesrepublik Deutschland

- VI ZR 135/13 -

Für den Kläger werde ich beantragen,

das angefochtene Urteil aufzuheben, soweit es den Kläger
beschwert, und

insoweit nach den Schlußanträgen des Klägers in der
Berufungsinstanz zu erkennen,

hilfsweise

insoweit die Sache zu neuer Verhandlung und
Entscheidung an das Berufungsgericht
zurückzuverweisen.

Revisionsgründe

Der Kläger begehrt die Unterlassung der Speicherung seiner Internetprotokolladresse bei der Nutzung öffentlich zugänglicher Telemedien der Beklagten im Internet. Das Amtsgericht hat die Klage wegen sachlicher Unzuständigkeit abgewiesen, das Landgericht hat ihr teilweise stattgegeben.

I.

Die Beklagte betrieb eine Vielzahl allgemein zugänglicher Internetportale (BU 2). „Bei den meisten“ dieser Portale hielt die Beklagte jeden Zugriff auf ihre Informationsangebote in Protokolldateien fest (BU 3). In diesen Protokolldateien speicherte die Beklagte über das Ende des jeweiligen Nutzungsvorgangs hinaus unter anderem die Internetprotokolladresse (IP-Adresse) des zugreifenden Hostsystems (BU 3). Der Kläger rief verschiedene Internetportale der Beklagten auf; die Beklagte und ihre Behörden speicherten die dem Kläger jeweils zugewiesene IP-Adresse über das Ende des jeweiligen Nutzungsvorgangs hinaus (BU 4).

Der Kläger hat beantragt, die Beklagte zu verurteilen, es zu unterlassen, die IP-Adresse des zugreifenden Hostsystems des Klägers, die bei der Nutzung öffentlich zugänglicher Telemedien der Beklagten im Internet übertragen werde, über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern oder speichern zu lassen, soweit die Speicherung nicht im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich sei. Hilfsweise hat er unter anderem beantragt, die Beklagte zu verurteilen es zu unterlassen, die IP-Adresse „in Verbindung mit dem Zeitpunkt des jeweiligen Nutzungsvorgangs“ über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern, weil die Speicherung der ihm jeweils zugewiesenen IP-Adresse über den Nutzungsvorgang hinaus gegen § 15 Abs. 4 TMG verstoße. Der Beklagten sei es nicht erlaubt, Nutzungsdaten – zu denen nach § 15 Abs. 1 TMG auch die personenbezogenen Daten eines Nutzers gehörten – über das Ende des Nutzungsvorgangs hinaus zu verwenden. Er, der Kläger, ist der Ansicht, dass es sich bei den ihm von seinem Zugangsanbieter beim Aufruf von Webseiten jeweils zugewiesenen IP-Adressen um personenbezogene Daten im Sinne von § 15 Abs. 1 TMG und § 3 Abs. 1 BDSG handele. Die Speicherung der Daten sei nicht ausnahmsweise zulässig, insbesondere nicht gemäß § 15 Abs. 4 TMG.

Dem ist die Beklagte entgegengetreten. Sie hat unter anderem vorgetragen, dynamische IP-Adressen seien keine personenbezogenen Daten. Nur der Access-Provider des Klägers könne zusammen mit einer Zeitangabe eine IP-Adresse einem seiner Kunden zuordnen, ihr – der Beklagten – sei es dagegen nicht möglich, mit den ihr zur Verfügung stehenden Mitteln die verwendete IP-Adresse zu individualisieren. Gegen die Qualifizierung von dynamischen IP-Adressen als personenbezogene Daten spreche ferner, dass der Access-Provider nicht ohne weiteres berechtigt sei, die gespeicherten Daten weiterzugeben.

Das Amtsgericht hat die Klage als unzulässig abgewiesen, da der Zuständigkeitsstreitwert 5.000,00 EUR bei weitem übersteige (AU 4).

Mit seiner dagegen gerichteten Berufung hat der Kläger seine erstinstanzlichen Anträge weiter verfolgt. Das Berufungsgericht hat dem ersten Hilfsantrag des Klägers stattgegeben. Der Kläger könne von der Beklagten gemäß §§ 1004 Abs. 1 Satz 2 BGB analog, 823 Abs. 1, Abs. 2 BGB i.V.m Art. 1, 2 Abs. 1 GG, §§ 4 Abs. 1 BDSG, 12 TMG nur verlangen, „es zu unterlassen die Internetprotokolladresse des zugreifenden Hostsystems des Klägers, die im Zusammenhang mit der Nutzung öffentlich zugänglicher Telemedien der Beklagten im Internet (...) übertragen wird, in Verbindung mit dem Zeitpunkt des jeweiligen Nutzungsvorgangs über das Ende des jeweiligen Nutzungsvorgangs zu speichern oder speichern zu lassen, sofern der Kläger während eines Nutzungsvorgangs selbst seine Personalien (...) angebe“ (BU 10). Die Revision gegen sein Urteil hat es zugelassen.

II.

Das angefochtene Urteil hält revisionsrechtlicher Prüfung nicht stand. Der Kläger kann verlangen, dass die Beklagte die Speicherung seiner dynamischen IP-Adresse unterlässt, auch wenn sie nicht zusätzlich den Zeitpunkt des Zugriffs auf die Internetseite speichert (dazu unten unter 2.a)). Die Unterlassung der Speicherung der dynamischen IP-Adresse kann der Kläger nicht nur dann verlangen, wenn er während des Nutzungsvorgangs seinen Klarnamen nennt (dazu unten unter 2.b)).

1. Das Berufungsgericht hat seine gegenteilige Auffassung wie folgt begründet:

Nach der Legaldefinition des § 3 BDSG seien personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer

bestimmten oder bestimmbaren natürlichen Person (BU 11). Bestimmbarkeit sei zu bejahen, wenn sich die Daten direkt auf eine bestimmte Person beziehen würde, wenn sie einen unmittelbaren Rückschluss auf die Identität der Person zuließen (BU 11) oder wenn die Person nicht allein durch die Daten identifiziert, jedoch mit Hilfe anderer Informationen und Zusatzwissen ein Personenbezug hergestellt werden könne (BU 12 oben). Ob die IP-Adresse für den Internetseitenbetreiber ein personenbezogenes Datum sei, richte sich nach der Auslegung des Begriffs der Bestimmbarkeit (BU 12). Insoweit sei dem relativen Ansatz zu folgen (BU 13); es komme darauf an, ob die Bestimmung der Person technisch und rechtlich möglich sei. Zudem dürfe für die Bestimmbarkeit kein Aufwand erforderlich sein, der außer Verhältnis zum Nutzen der Information für die verarbeitende Stelle stehe (BU 13). Die rein theoretische Möglichkeit der Bestimmbarkeit berühre die schutzwürdigen Belange der Person nicht (BU 13). Der Kläger habe daher keinen Anspruch auf Unterlassung der Speicherung der IP-Adresse, wenn nicht zusätzlich der Zeitpunkt seines Zugriffs auf die Seiten der Beklagten gespeichert werde (BU 19). Ein Personenbezug der dynamischen IP-Adresse sei auch nur dann zu bejahen, wenn der Nutzer zusätzlich seinen Klarnamen offen lege, da erst dann das Kriterium der Bestimmbarkeit erfüllt sei (BU 13).

2. Diese Begründung hält revisionsrechtlicher Prüfung in zweierlei Hinsicht nicht stand:

α) Zu Unrecht hat das Berufungsgericht gemeint, dass die IP-Adresse nur dann ein personenbezogenes Datum im Sinn des § 15 Abs. 1 TMG ist, wenn zusätzlich der Zeitpunkt des Nutzungsvorgangs gespeichert werde.

αα) Statische IP-Adressen, die einem Rechner fest zugeordnet sind, sind als personenbezogene Daten zu qualifizieren (vgl. VG Wiesbaden, Beschluss vom 27.02.2009 – 6 K 1045/08.WI, MMR 2009, 428 bis 432, juris-Dokument, Rn. 38; Buchner in Taeger/Gabel, 2. Aufl. § 3 BDSG, Rn. 17; Schulz in Roßnagel, 1. Aufl., § 11 TMG, Rn. 26; Dammann in Simitis, 6. Aufl., § 3 BDSG, Rn. 63; Roßnagel, Handbuch Datenschutzrecht, S. 1298, Rn. 56; Steidle/Pordes, Im Netz von Google. Web-Tracking und Datenschutz, DuD 2008, 324, 326; Gabriel/Cornels, MMR 2008, Heft 11, S. XIV, XV m.w.N; Arbeitskreis Medien, Orientierungshilfe zum Umgang mit personenbezogenen Daten bei Internetdiensten, 3.1.). Wenn für die statischen IP-Adressen ein Personenbezug anzunehmen ist, muss er auch für die dynamischen IP-Adressen gelten; beide Arten können technisch nicht voneinander unterschieden werden, bevor sie gespeichert werden

(Roßnagel, Handbuch Datenschutzrecht, S. 1299, Rn. 140, Gabriel/Cornels, a.a.O., m.w.N.).

bb) Zu Recht hat auch das Berufungsgericht angenommen (BU 25), dass gegenüber den Access-Providern ein Personenbezug der dynamischen IP-Adresse anzunehmen ist, da die Access-Provider – unabhängig davon, ob es sich um eine statische oder dynamische IP-Adresse handelt, – über das Zusatzwissen verfügen, um den Nutzer hinter der IP-Adresse zu bestimmen (Buchner, a.a.O.; Schulz in Roßnagel, 1. Aufl., § 11 TMG, Rn. 25; Steidle/Pordesch, a.a.O., m.w.N.).

Auch gegenüber Dritten – wie dem Betreiber einer Internetseite – stellt die dynamische IP-Adresse – entgegen der Ansicht des Berufungsgerichts – ein personenbezogenes Datum im Sinne des Telemediengesetzes dar, da sie eine Einzelangabe über eine bestimmbare natürliche Person darstellt. (AG Berlin-Mitte, Urteil vom 27.03.2007 – 5 C 314/06, ZUM 2008, 83 f, juris-Dokument, Rn. 13 f; VG Wiesbaden, Beschluss vom 27.02.2009 – 6 K 1045/08.WI, MMR 2009, 428 bis 432, juris-Dokument, Rn. 39, vgl. auch LG Berlin, Urteil vom 06.09.2007 – 23 S 3/07, MMR 2007, 799 f, juris-Dokument, 2. Orientierungssatz; LG Darmstadt, Urteil vom 25.01.2006 – 25 S 118/2005, 25 S 118/05, MMR 2006, 330 bis 332, juris-Dokument, 2. Leitsatz; vgl. auch das Urteil des EuGH vom 24.11.2011 – C 70/10, MMR 2012, 174 bis 176, in dem der EuGH allgemein von einer Personenbezogenheit der IP-Adresse ausgeht).

(1) Zwar ist der I. Zivilsenat in seiner „Sommer unserer Lebens“-Entscheidung (Urteil vom 12.05.2010 – I ZR 121/08, BGHZ 185, 330 bis 341, juris-Dokument, Rn. 15) davon ausgegangen ist, dass der dynamischen IP-Adresse keine – einem eBay-Konto vergleichbare – Identifikationsfunktion zukomme, da sie keinem konkreten Nutzer zuzuordnen sei, sondern „nur“ einem Anschlussinhaber. Auch auf den Anschlussinhaber bezogene Daten sind aber personenbezogene Daten. Der III. Zivilsenat geht zu Recht davon aus (Urteil vom 13.01.2011 – III ZR 146/10, K&R 2011, 178 bis 182, juris-Dokument, Rn. 27), dass § 100 TKG, soweit er die Erhebung und Speicherung der Telekommunikationsdaten, also auch die Speicherung der IP-Adresse erlaubt, in den Schutzbereich des Fernmeldegeheimnis gemäß Art. 10 Abs. 1 GG sowie in das Recht auf informationelle Selbstbestimmung gemäß Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG eingreife.

Dann ist die Folgerung unabweisbar, dass der dynamischen IP-Adresse ein Personenbezug inne wohnt und sie daher ein personenbezogenes Datum im Sinne des § 15 Abs. 1 TMG ist. Bestünde kein Personenbezug

der IP-Adresse, könnte das Grundrecht auf informationelle Selbstbestimmung durch die Speicherung nicht betroffen sein (vgl. Karg, MMR 2011, 345). Ferner hat der III. Senat in der zitierten Entscheidung IP-Adressen als Bestands- und Verkehrsdaten im Sinne des TKG behandelt. Die Regelungen des TKG, auf die sich der III. Senat bezog (§§ 96 Abs. 1, 100 Abs. 1 TKG), erfassen ausschließlich personenbezogene Daten, wie die Gesetzessystematik des TKG zeigt. Denn die Normen, auf die sich der Senat bezog, gehören zu Abschnitt 2 des TKG „Datenschutz“ (§ 91 Abs. 1 Satz 1 TKG). Die Qualifizierung von IP-Adressen als Verkehrsdaten im Sinne der §§ 96 Abs. 1, 100 Abs. 1 TKG impliziert somit, dass es sich bei diesen Daten um personenbezogene Daten handelt (vgl. Lorenz, Datenschutzrechtliche Einordnung der IP-Adresse, Anmerkung zum Urteil vom 13.01.2011 – III ZR 146/10, jurisPR-ITR 15/2011 Anm.2).

(2) Dass es sich bei einer dynamischen IP-Adresse um ein personenbezogenes Datum handelt, ergibt sich durch eine europarechtskonforme Auslegung des Begriffs der „personenbezogenen Daten“ im Sinn des § 15 Abs. 1 TMG anhand des 26. Erwägungsgrundes der EG-Datenschutzrichtlinie 95/46/EG (vgl. AG Berlin-Mitte, a.a.O.). Nach der 26. Begründungserwägung der Datenschutzrichtlinie 95/46/EG sollen nämlich 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 können, um die betreffende Person zu bestimmen.

Für die Antwort auf die Frage, ob dynamische IP-Adressen personenbezogene Daten sind, ist daher maßgeblich, ob die Person anhand der dynamischen IP-Adresse bestimmbar ist und bestimmt werden kann. Für die Bestimmbarkeit ist allein der Inhalt der Daten entscheidend und nicht – wie die Gegenansicht meint (vgl. Roßnagel in Handbuch Datenschutzrecht, 1. Aufl., S. 1298, Rn. 56; Eckhardt, K&R 2007, 602; 603; Meyerdierks, Sind IP-Adressen personenbezogene Daten?, MMR 2008, 8, 9) – die technische und rechtliche Möglichkeit der datenverarbeitenden Stelle, den Personenbezug herzustellen (vgl. Pahlen-Brandt, Zur Personenbezogenheit von IP-Adressen, K&R 2008, 288), denn darauf, ob, die Person nur mit legalen Mitteln bestimmt werden kann, kommt es nicht an (AG Berlin-Mitte, a.a.O.). Also hängt der Personenbezug der IP-Adresse nicht davon ab, ob die datenverarbeitende Stelle den Personenbezug tatsächlich herstellen kann, sondern nur davon, ob die Informationen, die die Daten liefern, für sich genommen geeignet sind, die hinter den Daten stehende Person zu bestimmen.

Falls ein Personenbezug der dynamischen IP-Adresse nur mit illegalen Mitteln herstellbar ist, ist sie geeignet, einen Personenbezug herzustellen. Das Schutzbedürfnis der Personen, die die Daten betreffen, endet nicht dort, wo Dritte nicht mehr mit erlaubten Mitteln auf die Daten zugreifen und die Person identifizieren können. Durch die Zusammenführung der personenbezogenen Daten mit Hilfe Dritter ist es bereits jetzt ohne großen Aufwand in den meisten Fällen technisch möglich, Internetnutzer aufgrund ihrer IP-Adresse zu identifizieren (AG Berlin-Mitte, a.a.O., Rn. 14), denn durch die Zusammenführung dynamischer IP-Adressen mit den dahinter stehenden Zuordnungstabellen, können Rückschlüsse auf bestimmte Personen gezogen werden (Arbeitskreis Medien, Orientierungshilfe zum Umgang mit personenbezogenen Daten bei Internetdiensten, 3.1.). Der Betreiber einer Website kann daher in Erfahrung bringen, welcher Nutzer sich hinter einer IP-Adresse verbirgt, wenn die Daten des Access-Providers, der stets weiß, welcher Nutzer sich hinter einer IP-Adresse verbirgt, zu den Daten des Betreibers der Website hinzugefügt werden. Darauf, ob der Access-Provider zur Weitergabe seiner Daten rechtlich befugt ist oder diese illegal weiter gibt, kommt es, wie gesagt, nicht an; es genügt vielmehr, dass die Möglichkeit dazu besteht.

Die Lebenserfahrung und die Berichte der Aufsichtsbehörden zeigen indes, dass Datenschutzverstöße an der Tagesordnung sind und vernünftigerweise in Betracht gezogen werden müssen. Auch die Sanktionsbewehrung durch den Gesetzgeber zeigt, dass dieser Rechtsverletzungen für (nicht nur theoretisch) möglich hält. In § 3 Abs. 6 BDSG stellt der Gesetzgeber für die Frage der Identifizierbarkeit eines Datums ausschließlich auf den damit verbundenen „Aufwand an Zeit, Kosten und Arbeitskraft“ ab und nicht auf die Frage der rechtlichen Zulässigkeit. Ferner erhebt der Gesetzgeber in § 3a BDSG das Gebot der Datensparsamkeit und Datenvermeidung zum ersten, übergeordneten Gebot des Datenschutzes. Dies zeigt, dass der Gesetzgeber das Risiko von Rechtsverletzungen minimieren und es nicht als vermeintlich vernachlässigbar hinnehmen will.

(3) Eine Verneinung des Personenbezugs von dynamischen IP-Adressen hätte zur Folge, dass sowohl das Telemediengesetz als auch das Telekommunikationsgesetz auf diese Art von Daten nicht anwendbar sind; damit besteht das Risiko, dass diese Daten an Dritte übermittelt werden können, die ihrerseits die Möglichkeit haben, den Nutzer aufgrund der IP-Adresse zu identifizieren, was mit den Bestimmungen des Datenschutzrechts nicht vereinbar ist (AG Berlin-Mitte, a.a.O., Rn. 14).

Eine Bestimmbarkeit im Sinne des § 3 BDSG ist nicht nur dann gegeben, wenn der Betroffene nur mit legalen Mitteln identifiziert werden kann. Das Datenschutzrecht soll gerade vor dem Missbrauch von Daten schützen, so dass eine derartige Einschränkung des Begriffs der Bestimmbarkeit von Personen nicht gerechtfertigt ist (AG Berlin-Mitte, a.a.O.). Das Argument der Gegenansicht, das gesetzliche Verbot, anonyme Daten an eine Stelle zu übermitteln, die in der Lage ist, den Personenbezug herzustellen, würde ausreichend Schutz gewähren (vgl. Eckhardt, K&R 2007, 602, 603), vermag hingegen nicht zu überzeugen, da allein die Existenz von Regelungen nicht ihre Einhaltung garantiert (Pahlen-Brandt, Zur Personenbezogenheit von IP-Adressen, K&R 2008, 288, 290). Dynamische IP-Adressen bedürfen daher auch des Schutzes durch das Datenschutzrecht, wenn eine datenverarbeitende Stelle über sie verfügt, der selbst die Möglichkeiten zur Identifizierung fehlen. Ansonsten besteht die Gefahr, dass der Betreiber der Website die Daten an einen Käufer verkauft, der ihm zwar glaubhaft, aber wahrheitswidrig versichert, dass er die Daten nur datenschutzgemäß verarbeiten werde (Pahlen-Brandt, a.a.O.). Der Schutz des informationellen Selbstbestimmungsrechts wäre in solchen Fällen nicht ausreichend gewährleistet.

(4) Auch die Artikel-29-Gruppe der Datenschutzbeauftragten der EU-Mitgliedsstaaten stuft IP-Adressen als Daten ein, die sich auf eine bestimmbare Person beziehen. Access-Provider 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-Diensteanbietern 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 a) der Datenschutzrichtlinie 95/46/EG reden könne (vgl. Stellungnahme 4/2007 der Artikel-29-Gruppe der Datenschutzbeauftragten der EU-Mitgliedstaaten vom 20.06.2007 zum Begriff „personenbezogene Daten“, S. 19). Auch das Bundesministerium der Justiz, der Düsseldorfer Kreis sowie der Arbeitskreis der Medien der Datenschutzbeauftragten von Bund und Ländern sehen IP-Adressen als personenbezogene Daten an und ordnen daher die Zulässigkeit ihrer Erhebung und Verwendung stets dem Regime des Datenschutzrechts unter (vgl. Hullen/Roggenkamp in Plath, 1. Aufl., § 12 TMG, Rn. 14).

(5) Der Kläger ist anhand seiner IP-Adresse selbst dann bestimmbar, wenn man nur die der Beklagten selbst legalerweise zur Verfügung

stehenden Mittel berücksichtigen wollte. Die Beklagte kann den Kläger mithilfe von Auskunftersuchen an dessen Internet-Zugangsanbieter legal identifizieren, und zwar nach § 113 TKG in Verbindung mit diversen fachgerichtlichen Erhebungsbefugnissen. Rechtlich zulässig ist die Identifizierung des Klägers für die Beklagte immer dann, wenn dies „im Einzelfall zum Zweck der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben“ der Nachrichtendienste erforderlich ist. Entgegen der Auffassung des Berufungsgerichts müssen weder die Voraussetzungen des § 100g StPO vorliegen noch ist eine richterliche Anordnung vorausgesetzt.

Die Fälle des § 113 TKG, die der Beklagten eine Identifizierung eröffnen, sind nicht nur theoretisch denkbar, sondern treten praktisch häufig auf. Im Rahmen der sogenannten „Homepageüberwachung“ identifizieren Strafverfolgungsbehörden beispielsweise alle Nutzer, die sich für amtliche Informationen über bestimmte Straftaten interessieren – in der Hoffnung, auf diese Weise die Täter feststellen zu können. In erster Linie werden so die IP-Adressen Unbeteiligter identifiziert.

Im Rahmen der Prüfung der Zulässigkeit einer Verfassungsbeschwerde des Klägers gegen § 113 TKG hat das Bundesverfassungsgericht die Darlegung gefordert, „mit einiger Wahrscheinlichkeit von solchen Maßnahmen berührt zu werden“. Das Bundesverfassungsgericht hat dies für den Kläger mit der Begründung angenommen, „dass die durch § 112 Abs. 2 und § 113 Abs. 1 TKG ermöglichten Auskünfte eine große Streubreite haben und Dritte auch zufällig erfassen können“ (BVerfGE 130, 151 Abs. 102). Damit steht fest, dass der Kläger mit einiger Wahrscheinlichkeit von einer IP-Zuordnung nach § 113 TKG betroffen sein kann und § 113 TKG folglich bei der Frage der Bestimmbarkeit des Klägers „vernünftigerweise“ in Betracht zu ziehen ist.

Das Bundesverfassungsgericht hat ausgesprochen, dass der Gesetzgeber mit dem Telemediengesetz „das Entstehen vermeidbarer Datensammlungen grundsätzlich zu verhindern sucht“. Der Gesetzgeber würde „die Diensteanbieter nach dem Telemediengesetz grundsätzlich zur Löschung von nicht für die Abrechnung erforderlichen Daten verpflichten (vgl. § 13 Abs. 4 Nr. 2, § 15 TMG) und so auch gegenüber privatwirtschaftlichen Anreizen verhindern, dass die Internetnutzung inhaltlich in allgemeinen kommerziellen Datensammlungen festgehalten wird und damit rekonstruierbar bleibt“ (BVerfGE 125, 260, 348 Abs. 270).

Nur die Annahme des Personenbezugs der steitgegenständlichen Daten verhindert, dass die Internetnutzung des Klägers bei der Beklagten „rekonstruierbar bleibt“, selbst wenn man nur das legale Mittel von Auskünften nach § 113 TKG berücksichtigen wollte.

cc) Stellen dynamische IP-Adressen für sich genommen ein personenbezogenes Datum dar, hat der Kläger einen Anspruch darauf, dass die Beklagte die Speicherung dieser Daten unabhängig davon unterläßt, ob auch der Zeitpunkt des Nutzungsvorgangs gespeichert wird.

Im Übrigen ist der Kläger anhand der genutzten IP-Adresse nicht nur dann identifizierbar, wenn die Beklagte die Adresse „in Verbindung mit dem Zeitpunkt des jeweiligen Nutzungsvorgangs“ speichert. Die Beklagte hat zwar behauptet, die Zuordnung einer IP-Adresse durch den Zugangsanbieter könne nur aufgrund einer konkreten Zeitangabe (Datum und Uhrzeit) erfolgen. Sie ist aber dem Vortrag des Klägers nicht entgegengetreten (Rüge auch aus § 286 ZPO), wonach diese Zeitangabe nicht notwendig dem Zugriffsprotokoll selbst zu entnehmen sein muss. Der Kläger hat in den Tatsacheninstanzen erläutert, wie sonst eine hinreichende zeitliche Eingrenzung möglich ist (Schriftsatz vom 06.07.2008 S. 9 ff, GA I 115 ff). Obwohl diese Ausführungen unbestritten geblieben sind, hat sie das Berufungsgericht rechtsfehlerhaft übergangen. Eine Befugnis der Beklagten zur Protokollierung aller Nutzungsdaten mit Ausnahme des Zugriffszeitpunkts eröffnete der Beklagten zu viele Identifizierungsmöglichkeiten, so dass die bloß eingeschränkte Verurteilung nach dem Hilfsantrag des Klägers nicht hingenommen werden kann.

b) Entgegen der Ansicht des Berufungsgerichts hängt die datenschutzrechtliche Unzulässigkeit der Speicherung der dynamischen IP-Adresse auch nicht davon ab, dass der Nutzer zusätzlich seinen Klarnamen während des Nutzungsvorgangs preisgibt.

Da die dynamische IP-Adresse – wie dargestellt – für sich genommen ein personenbezogenes Datum ist, entsteht ein Personenbezug nicht erst dann, wenn der Nutzer seinen Klarnamen während des Nutzungsvorgangs angibt und der Betreiber der Website den Klarnamen des Nutzers zusätzlich speichert. Da eine Identifizierung des Nutzers auch

ohne den Klarnamen möglich ist, ist der Nutzer auch schutzbedürftig,
wenn er seinen Klarnamen nicht nennt.

