Abschrift

VON GIERKE & ROHNKE

Rechtsanwälte beim Bundesgerichtshof

von Gierke & Rohnke · Postfach 110524 · 76055 Karlsruhe

An den
Bundesgerichtshof
VI. Zivilsenat

76133 Karlsruhe

Bundesgerichtshof
Eing. 05. März 2014
Anl. Doppel Bd.

Cornelie von Gierke
Prof. Dr. Christian Rohnke
Stephanienstraße 30
76133 Karlsruhe
Eingang Seminarstraße
Telefon: (0721) 205198
Telefax: (0721) 205199
info@vongierke-rohnke.de
www.vongierke-rohnke.de

04.03.2014 vG/cd

SCHULTZ • SCHOTT
07. März 2014
Rechtsanwälte
beim Bundesgerichtshof

Revisionserwiderung

VI ZR 135/13

In Sachen

Dr. Breyer

gegen

BRD

begründe ich den Antrag auf Zurückweisung der Revision des Klägers wie folgt:

I.

Der Kläger begehrt die Unterlassung der Speicherung seiner Internetprotokolladresse (= IP-Adresse) bei der Nutzung öffentlich zugänglicher Telemedien der Beklagten im Internet. Mit seiner Revision wendet er sich dagegen, dass das Berufungsgericht seinen Hauptantrag abgewiesen und seinem ersten Hilfsantrag nur teilweise stattgegeben hat. Er meint, er könne verlangen, dass die Beklagte die Speicherung seiner dynamischen IP-Adresse unterlässt, auch wenn sie nicht zusätzlich den Zeitpunkt des Zugriffs auf die Internetseite speichere und er während des Nutzungsvorgangs seinen Klarnamen nicht nenne.

Soweit das Berufungsgericht die Klage als unbegründet angesehen hat, hat es hierzu ausgeführt: Der Hauptantrag sei unbegründet, da der Kläger keinen Anspruch auf Unterlassung der Speicherung der IP-Adresse als solcher, das heißt ohne Zeitpunkt des Zugriffs habe. Der Kläger könne nur die Unterlassung der Speicherung der IP-Adresse in Verbindung mit dem Zeitpunkt des jeweiligen Nutzungsvorgangs verlangen. Soweit die Beklagte nur die IP-Adressen ohne den zugehörigen Zeitpunkt des Zugriffs speichere, stelle die IP-Adresse als solche kein personenbezogenes Datum im Sinne von § 12 TMG, § 3 BDSG dar. Denn ohne den Zeitpunkt des Zugriffs könne ein Bezug zwischen den unter Angabe der Personalien stattgefundenen Kontakten des Klägers mit der Beklagten und der jeweiligen IP-Adresse auch unter Ausschöpfung aller technischen Möglichkeiten nicht hergestellt werden (BU 19/20). Auch der erste Hilfsantrag sei nur teilweise, nämlich in dem tenorierten Umfang, begründet, da der Kläger keinen Unterlassungsanspruch als anonymer Surfer habe. Soweit der Kläger während eines Besuchs auf einem Internetportal der Beklagten seinen Klarnamen nicht angebe, könne nur der Zugangsanbieter die IP-Adresse einem bestimmten Anschlussinhaber zuordnen. Der Betreiber der Internetseite (Beklagte) selbst verfüge nicht über das dazu erforderliche Zusatzwissen. Er könne den Personenbezug nur durch Auskunftserteilung durch den Zugangsanbieter, welchem Anschlussinhaber zu welchem Zeitpunkt eine bestimmte IP-Adresse zugeordnet war, herstellen. In diesem Fall handle es sich bei der IP-Adresse des Klägers in Verbindung mit dem Zeitpunkt des Zugriffs in den Händen der Beklagten nicht um ein personenbezogenes Datum (BU 20 ff).

Der Kläger rügt mit seiner zugelassenen Revision, das Berufungsgericht sei zu Unrecht davon ausgegangen, dass die IP-Adresse nur dann ein personenbezogenes Datum im Sinn des § 15 Abs. 1 TMG sei, wenn zusätzlich der Zeitpunkt des Nutzungsvorgangs gespeichert werde. Da statische (d.h. einem Rechner fest zugeordnete) IP-Adressen personenbezogene Daten seien, müsse entsprechendes auch für dynamische IP-Adressen gelten, da beide Arten technisch nicht voneinander unterschieden werden könnten, bevor sie gespeichert würden (RB 4 f). Der Personenbezug dynamischer IP-Adressen ergebe sich auch aus mehreren gerichtlichen Entscheidungen sowie aus einer europarechtskonformen Auslegung des § 15 Abs. 1 TMG (Kl-RB 5 f). Darauf, ob die Person nur mit legalen Mitteln bestimmt werden könne, komme es nicht an (Kl-RB 6 f). Verneine man den Personenbezug dynamischer IP-Adressen, seien das TMG und das TKG auf diese Art von Daten nicht anwendbar, was mit dem Datenschutzrecht nicht vereinbar sei (Kl-RB 7 f). Auch die Artikel-29 Gruppe der Datenschutzbeauftragten der EU-Mitgliedstaaten stufe IP-Adressen als Daten ein, die sich auf eine bestimmbare Person bezögen (Kl-RB 8). Der Kläger sei anhand seiner IP-Adresse für die Beklagte auch auf legalem Wege, nämlich mittels eines Auskunftsersuchens nach § 113 TKG, ohne weiteres identifizierbar (Kl-RB 8 ff). Stellten dynamische IP-Adressen für sich genommen ein personenbezogenes Datum dar, sei deren Speicherung unabhängig davon datenschutzrechtlich unzulässig, ob auch der Zeitpunkt des Nutzungsvorgangs gespeichert werde oder der Nutzer seinen Klarnamen während des Nutzungsvorgangs preisgebe (Kl-RB 10 f).

II.

Das Berufungsurteil lässt insoweit, als zum Nachteil des Klägers entschieden worden ist, keine Rechtsfehler zu dessen Lasten erkennen. Die Revision des Klägers wird daher zurückzuweisen sein.

1. Entgegen der Auffassung des Klägers ist das Berufungsgericht zu Recht und mit zutreffender Begründung davon ausgegangen, dass die IP-Adresse allenfalls dann ein personenbezogenes Datum im Sinn

des § 15 Abs. 1 TMG sein kann, wenn zusätzlich der Zeitpunkt des Nutzungsvorgangs gespeichert wird (BU 11 bis 13 und BU 19/20).

a) Nach der Legaldefinition des § 3 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. „Bestimmbarkeit" in diesem Sinne wird angenommen, wenn die konkrete Person nicht allein durch die Daten identifiziert, jedoch mit Hilfe anderer Informationen und Zusatzwissen ein Personenbezug hergestellt werden kann (Krüger/Macher, MMR 2011, 433, 434; Bucher, in: Taeger/Gabel, BDSG, 2. Aufl. 2013, § 3 Rn 11). Die herrschende Meinung vertritt ein relatives Verständnis des Personenbezugs (AG München, Urt. 30.09.2008 – 133 C 5677/08, CR 2009, 59; Simitis/Dammann, in Simitis, BDSG, 7. Aufl. 2011, § 3 Rn 32; Plath/Schreiber, in: Plath, BDSG, 1. Aufl. 2013, § 3 Rn 15; Gola/Schomerus, BDSG, 11. Aufl. 2012, § 3 Rn 10; Eckhardt, CR 2011, 339, 344; Eckhardt, K&R 2007, 602 f; Meyerdierks, MMR 2009, 8 f; Krüger/Maucher, MMR 2011, 433, 436; Moos, K&R 2008, 137, 139). Danach gilt: Nur wenn die verarbeitende Stelle ein Datum mit den ihr üblicherweise zur Verfügung stehenden Mitteln und unter vernünftigem Aufwand einer Person zuordnen kann, ist es für sie personenbezogen. Diese Auffassung findet sich auch in Erwägungsgrund 26 der EU-Datenschutzrichtlinie 95/46/EG und in Erwägungsgrund 24 des Entwurfs der EU-Datenschutzgrund-verordnung vom 25.01.2012 wieder (vgl. Gerlach, CR 2013, 478, 479 liSp).

b) Das Berufungsgericht hat sich dem relativen Verständnis des Personenbezugs angeschlossen. Das absolute Verständnis führe zu einer uferlosen und unpraktikablen Ausdehnung des Datenschutzes, die vom Gesetzgeber nicht gewollt sei. Eine rein theoretische Möglichkeit der Bestimmbarkeit berühre nicht die schutzwürdigen Belange und das Recht auf informationelle Selbstbestimmung potentiell Betroffener (BU 13 oben). Das Berufungsgericht hat weitere konkretisierende Maßstäbe für die „Bestimmbarkeit" des Personenbezugs aufgestellt (BU 13): Danach muss die Bestimmung der Person für die verarbeitende Stelle technisch und rechtlich möglich sein. Die Person muss nicht nur theoretisch, sondern auch praktisch bestimmbar sein, d.h. mit einem Aufwand, der nicht außer Verhältnis zum Nutzen der Bestimmung der

Person aus Sicht der verarbeitenden Stelle steht. Es ist im Einzelfall abzuwägen, ob der Datenschutz erforderlich ist bzw. wie weit er reichen soll. Dabei ist u.a. zu berücksichtigen, welche Hürden bestehen, bevor die verarbeitende Stelle an die Zusatzinformationen herankommt, ob und welche Missbrauchsszenarien eine Rolle spielen und ob der Schutz des Betroffenen auch ohne das absolute Verständnis des Personenbezugs ausreichend ist. Unter Anwendung dieser Kriterien kommt das Berufungsgericht zu dem Ergebnis, dass die Personenbeziehbarkeit dynamischer IP-Adressen durch den Access-Provider für sich genommen nicht ausreicht, die Personenbeziehbarkeit auch für Dritte zu bejahen. Für Dritte – wie etwa Betreiber von Webservern – sind dynamische IP-Adressen nur personenbezogen, wenn sie über weitere Zusatzinformationen verfügen und insbesondere den Personenbezug mit eigenen Mitteln herstellen können (BU 19/20).

2. Die gegen diese Beurteilung gerichteten Angriffe der Revision des Klägers (Kl-RB 4 ff) sind unbegründet.

a) Entgegen der Auffassung des Klägers lässt sich aus dem Umstand, dass ein Teil des Schrifttums statische (d.h. einem Rechner fest zugeordnete) IP-Adressen als personenbezogene Daten qualifiziert, nicht der Schluss ziehen, dass entsprechendes auch für dynamische IP-Adressen gelten müsse, da beide Arten technisch nicht voneinander unterschieden werden könnten, bevor sie gespeichert würden (RB 4 f).

aa) Hierzu ist zunächst folgendes anzumerken: Selbst wenn die Beklagte bei der Speicherung von IP-Adressen nicht zwischen statischen und dynamischen IP-Adressen unterscheiden könnte und statische IP-Adressen tatsächlich immer personenbezogen wären, ergäbe sich daraus kein Unterlassungsanspruch des Klägers. Denn der Kläger wird durch die Speicherung personenbezogener statischer IP-Adressen nicht in seinen Rechten verletzt, da er unstreitig ausschließlich eine dynamische IP-Adresse verwendet. Sämtliche Überlegungen des Klägers zum Personenbezug statischer IP-Adressen sind daher irrelevant.

bb) Lediglich vorsorglich ist daher darauf hinzuweisen, dass der vom Kläger vorgenommene undifferenzierte Vergleich mit „statischen IP-Adressen" den Blick auf unterschiedliche Sachverhaltskonstellationen verstellt (vgl. Gerlach, CR 2013, 478, 480; Venzke, ZD 2011, 479, 483). Zur Beurteilung der Rechtslage muss geklärt werden, was überhaupt mit „statischen" IP-Adressen gemeint ist und in welchen Konstellationen eine Personenbeziehbarkeit von IP-Adressen vorliegt. Bei „statischen" IP-Adressen ist demnach wie folgt zu differenzieren (vgl. Gerlach, CR 2013, 478, 480):

(1) Die erste Konstellation lässt sich wie folgt skizzieren: Jede IP-Adresse ist über das RIPE NCC einem Inhaber zugeordnet. Der beim RIPE NCC registrierte Inhaber jeder IP-Adresse ist über die whois-Datenbank ermittelbar. Dabei handelt es sich nur in Ausnahmefällen um eine natürliche Person. Nur in diesem Fall ist die IP-Adresse für jeder-mann personenbeziehbar – nämlich einer natürlichen Person als Inhaber zuzuordnen. Dies hat mit der Art der Adressvergabe durch den Access-Provider (statisch oder dynamisch) jedoch nichts zu tun (Gerlach, CR 2013, 478, 480).

(2) Die zweite Konstellation lässt sich dahingehend umschreiben, dass Access-Provider ihren Kunden immer die gleiche IP-Adresse aus ihrem Adresspool zuweisen können („statische" statt „dynamischer" Zuweisung). Über die whois-Datenbank ist in diesem Fall nur der Access-Provider als Inhaber der IP-Adresse ermittelbar (Gerlach, CR 2013, 478, 480/481).

cc) Aus diesen unterschiedlichen Konstellationen ergeben sich folgende rechtliche Konsequenzen:

(1) Vom Access-Provider statisch vergebene IP-Adressen sind rechtlich wie dynamisch vergebene IP-Adressen zu behandeln. Auch hier kann ein Personenbezug nur vom Access-Provider ohne weiteres hergestellt werden. Insbesondere lässt sich der Anschlussinhaber der IP-Adresse nicht über die whois-Datenbank ermitteln. Als Inhaber der IP-Adresse ist beim RIPE NCC der jeweilige Access-Provider registriert (Gerlach, CR 2013, 478, 481).

(2) Im Ergebnis nichts anderes gilt für den zumindest theoretisch möglichen Fall, dass eine direkte Registrierung von IP-Adressen beim RIPE NCC durch natürliche Personen zu einer Personenbeziehbarkeit aller IP-Adressen führt. Es ist zwar theoretisch möglich, dass als Inhaber einer IP-Adresse über die whois-Datenbank eine natürliche Person ermittelt werden kann. Eine Personenbestimmung von Inhabern von IP-Adressen über die whois-Datenbank steht aber außer Verhältnis zum erwartbaren Nutzen. Die whois-Datenbank ist kein „vernünftigerweise" eingesetztes Zusatzwissen zur Herstellung von Personenbezug. Nach dem relativen Verständnis des Personenbezugs handelt es sich daher bei allen IP-Adressen – nicht nur bei dynamischen IP-Adressen – nur für den jeweiligen Access-Provider um personenbezogene Daten (Gerlach, CR 2013, 478, 481; vgl. auch Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 11 TMG Rn 8; Härting, Internetrecht, 4. Aufl. 2010, Teil A Rn 94).

b) Der Kläger kann seine Auffassung, wonach dynamische IP-Adressen nicht nur gegenüber Access-Providern, sondern auch gegenüber Dritten personenbezogene Daten darstellen sollen, auch nicht mit Erfolg auf die von ihm (RB 5) zitierten Gerichtsentscheidungen stützen.

aa) Richtig ist, dass das Amtsgericht und das Landgericht Berlin sowie das VG Wiesbaden in den vom Kläger (RB 5, 2. Abs.) zitierten Urteilen die Ansicht vertreten haben, bei einer dynamischen IP-Adresse handle es sich generell um ein personenbezogenes Datum im Sinne von § 15 TMG bzw. § 3 Abs. 1 BDSG (AG Berlin Mitte, Urt. 27.03.2007 – 5 C 314/06, ZUM 2008, 83 f, juris Rn 13 f; LG Berlin, Urt. 06.09.2007 – 23 S 3/07, MMR 2007, 799 f; VG Wiesbaden, Beschl. 27.02.2009 – 6 K 1045/08.WI, MMR 2009, 428 ff). Diese Auffassung ist aber schon deswegen abzulehnen, weil sich jede pauschale Bejahung oder Verneinung der Personenbeziehbarkeit eines bestimmten Datums verbietet. Denn die Bestimmbarkeit der Person, auf die sich die Information bezieht, ist relativ und hängt von den individuellen Kenntnissen, Mitteln und Möglichkeiten der jeweiligen Person ab (Gola/Schomerus, BDSG, 9. Aufl. 2007, § 3 Rn 10; Moos, K&R 2008, 137, 139). Auch für die Frage der Personenbeziehbarkeit von IP-Adressen ist deshalb danach zu differenzieren, für wen dieses Datum personenbeziehbar sein soll. Für den

Access-Provider gilt unstreitig Personenbezug (vgl. BU 12, 2. Abs. mwN). Dies ist insofern zutreffend, als der Access-Provider den Nutzern in der Regel selbst die IP-Nummern zuweist, so dass er leicht – unter Einblick in seine eigenen Systeme – herausfinden kann, welcher natürlichen Person eine bestimmte IP-Adresse zugeordnet war. Differenzierter ist aber der Personenbezug für den Telemedien-Diensteanbieter zu beurteilen. Dieser kann eine Zuordnung der IP-Adresse zu einer bestimmten Person ohne Rückgriff auf fremde Hilfsmittel nicht vornehmen. Es kommt deshalb darauf an, ob er mit den ihm normalerweise zur Verfügung stehenden Hilfsmitteln und ohne unverhältnismäßigen Aufwand den Personenbezug herstellen kann. Dies wird für den reinen Internet-Diensteanbieter von der herrschenden Meinung schon deswegen zu Recht verneint, weil es diesem unter anderem aus datenschutzrechtlichen Gründen regelmäßig versagt ist, den hinter einer IP-Adresse stehenden Namen des Nutzers einfach von dem Access-Provider zu erfragen (Moos, K&R 2008, 137, 139 reSp; Eckhardt, K&R 2007, 602).

bb) Der Kläger kann sich auf die in diesem Zusammenhang zitierte EuGH-Entscheidung „ASNEF" (Urt. 24.11.2011 – C-468/10 u.a.) schon deswegen nicht mit Erfolg berufen, weil diese Entscheidung, welche die Auslegung von Art. 7 Buchst. F der EGRL 46/95 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr betrifft, keine Aussage zu der hier streitigen Frage enthält, ob es sich bei dynamischen IP-Adressen für Internetseitenbetreiber um personenbezogene Daten im Sinne von § 3 BDSG bzw. von § 11 TMG handelt. Entsprechendes gilt auch für die vom Kläger in diesem Zusammenhang weiter zitierte BGH-Entscheidung vom 13.11.2011 (III ZR 146/10, NJW 2011, 1509 ff), mit welcher der BGH zu den Voraussetzungen für die Befugnis, dynamische IP-Adressen zum Zweck der Entgeltermittlung und Abrechnung gemäß § 97 Abs. 1 Satz 1, Abs. 2 Nr. 1 TKG zu speichern, Stellung genommen und hierzu folgenden Leitsatz aufgestellt hat:

> »Die Befugnis zur Speicherung von IP-Adressen zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen gemäß § 100 Abs. 1 TKG setzt nicht voraus, dass im Einzelfall bereits Anhaltspunkte für eine Störung

> oder einen Fehler vorliegen. Es genügt vielmehr, dass die in Rede stehende Datenerhebung und -verwendung geeignet, erforderlich und im engeren Sinn verhältnismäßig ist, um abstrakten Gefahren für die Funktionstüchtigkeit des Telekommunikationsbetriebs entgegenzuwirken.«

Weder in diesem Leitsatz noch in den Gründen dieser Entscheidung findet sich eine Aussage über den Personenbezug von IP-Adressen (vgl. auch Krüger/Maucher, MMR 2011, 433, 436 liSp). Allenfalls lässt sich eine Tendenz dahin erkennen, dass der BGH in dieser Entscheidung nicht etwa dem vom Kläger vertretenen absoluten Verständnis, sondern vielmehr dem vom Berufungsgericht und der herrschenden Auffassung vertretenen relativen Verständnis zuneigt: Nach der zitierten Entscheidung stellt die bloße Speicherung der dynamischen IP-Adressen noch keinen schwerwiegenden Eingriff in die Grundrechte der Nutzer dar (BGH, aaO, Rn 28). Dies gilt umso mehr, als von maßgebender Bedeutung für das Gewicht des Grundrechtseingriffs ist, welche Persönlichkeitsrelevanz die Informationen aufweisen, die von der informationsbezogenen Maßnahme erfasst werden. Die Identität des jeweiligen Nutzers ist aus der IP-Adresse selbst nicht erkennbar und wird erst durch die Zusammenführung mit weiteren Angaben ermittelbar (BGH, aaO, Rn 28). Ginge der BGH von der absoluten Bestimmbarkeit aus, hätte er der IP-Adresse als Information wohl ein größeres Gewicht beigemessen (vgl. Krüger/Maucher, MMR 2011, 433, 436 liSp).

cc) Soweit der Kläger (RB 5) in diesem Zusammenhang auch die BGH-Entscheidung „Sommer unseres Lebens“ (Urt. 12.05.2010 – I ZR 121/08, GRUR 2010, 633 ff) zitiert, räumt er zumindest indirekt („zwar hat ....“) selbst ein, dass diese Entscheidung nicht für einen absoluten, sondern für einen relativen Personenbezug von IP-Adressen spricht, da es in Randnummer 15 dieser Entscheidung heißt :

> »[15] Der IP-Adresse kommt keine mit einem eBay-Konto vergleichbare Identifikationsfunktion zu. Anders als letzteres ist sie keinem konkreten Nutzer zugeordnet, sondern nur einem Anschlussinhaber, der grundsätzlich dazu berechtigt ist, beliebigen Dritten Zugriff auf seinen Internetanschluss zu gestatten. Die IP-Adresse gibt deshalb bestimmungsgemäß keine zuverlässige Auskunft über die Person, die zu einem konkreten Zeitpunkt einen bestimmten Internetanschluss nutzt.«

c) Entgegen RB 6 spricht auch die europarechtskonforme Auslegung des § 15 Abs. 1 TMG anhand des 26. Erwägungsgrundes der EG-Datenschutzrichtlinie 95/46/EG nicht etwa für das vom Kläger vertretene absolute, sondern vielmehr für das vom Berufungsgericht vertretene relative Verständnis des Personenbezugs und damit gegen die Annahme, dass der Kläger einen Anspruch auf Unterlassung der Speicherung der IP-Adresse als solcher, das heißt ohne Zeitpunkt des Zugriffes hat.

aa) Gemäß Erwägungsgrund 26 der Datenschutzrichtlinie 95/46/EG sollen 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«.

Die Einbeziehung der Mittel Dritter bedeutet nicht, dass die Bestimmbarkeit absolut gefasst wird, also bereits dann besteht, wenn irgend jemand zu ihr in der Lage ist. Vielmehr wählt die Richtlinie mit dem Merkmal „vernünftigerweise" einen pragmatischen Ansatz, der inhaltlich dem BDSG-Kriterium des (nicht) unverhältnismäßigen Aufwands entspricht (Dammann, in: Simitis, BDSG, 7. Aufl. 2011, § 3 Rn 24). Auch aus Erwägungsgrund 26 der EG-Datenschutzrichtlinie 95/46/EG folgt mithin, dass die rein hypothetische Möglichkeit, eine Person zu bestimmen, nicht ausreicht, um diese Person als „bestimmbar" anzusehen, sondern dass es entscheidend darauf ankommt, ob es im Rahmen eines realistischen Aufwands an Zeit, Kosten und Arbeitskraft möglich ist, Informationen einer bestimmten Person zuzuordnen (Buchner, in: Taeger/Gabel, BDSG, 2. Aufl., § 3 Rn 12).

bb) Aus dem vorstehend Gesagten folgt zugleich, dass es – entgegen RB 6 ff – auch mit Blick auf Erwägungsgrund 26 der EG-Datenschutzrichtlinie 95/46/EG für die Beantwortung der Frage, ob dynamische IP-Adressen in Bezug auf einen Website-Betreiber personenbezogene Daten sind, sehr wohl auf dessen technische und rechtliche Möglichkeit ankommt, den Personenbezug herzustellen und damit auch darauf, ob die Person mit legalen Mitteln bestimmt werden kann oder nicht. Um insoweit eine interessengerechte Beurteilung vornehmen zu können, muss die Gefahr der Offenlegung des Personenbezugs

durch den Access-Provider untersucht werden. Es sprechen indes sowohl die strafrechtliche als auch die zivilrechtliche Sanktionierung dafür, dass eine Offenlegung durch den Access-Provider nicht zu erwarten ist:

(1) Die Access-Provider können den Personenbezug herstellen, werden diese Information an Dritte aber aus rechtlichen wie auch aus tatsächlichen Gründen und insbesondere unternehmerischen Gründen in aller Regel nicht weitergeben, sondern nur ausnahmsweise an autorisierte Stellen (Krüger/Maucher, MMR 2011, 433, 436; Eckhardt, K&R 2007, 602, 603; Moos, K&R 2008, 137, 139). Autorisiert sind zum einen staatliche Stellen, z.B. nach §§ 161, 163 StPO i.V.m. §§ 112 bzw. 113 TKG, sowie private Stellen, wenn die Voraussetzungen eines zivilrechtlichen Auskunftsanspruchs gegeben sind, z.B. nach § 101 Abs. 9 UrhG. Für die Auskunftserteilung müssen die jeweiligen gesetzlichen Voraussetzungen gegeben sein (Krüger/Maucher, MMR 2011, 433, 436; Meyerdierks, MMR 2009, 8, 12).

(2) Die Herausgabe an Private, die keinen zivilrechtlichen Auskunftsanspruch haben, ist demnach rechtlich ausgeschlossen. Würde der Access-Provider die Informationen an unbefugte Dritte herausgeben, würden sich die Verantwortlichen nach § 206 StGB strafbar machen. Eine unrechtmäßige Bekanntgabe an Dritte wäre zudem ein Verstoß gegen die Schutzpflichten aus dem Vertragsverhältnis gegenüber seinen Kunden, § 241 Abs. 2 BGB, und ein Verstoß gegen eigene gesetzliche Pflichten zur Wahrung des Datenschutzes (Krüger/Maucher, MMR 2011, 433, 436). Dass Internet-Access-Provider insbesondere durch das Datenschutzrecht und das Fernmeldegeheimnis (§ 88 TKG, § 206 StGB) rechtlich gehindert sind, dem Website-Betreiber den Namen des Nutzers der dynamischen IP-Adresse mitzuteilen, wird in der Praxis auch dadurch bestätigt, dass die Internet-Access-Provider sich regelmäßig weigern, zivilrechtliche Auskunftsansprüche bei Urheberrechtsverletzungen anzuerkennen (vgl. Eckhardt, K&R 2007, 602, 603). Die Tatsache, dass die Strafverfolgungsbehörden im Rahmen eines Ermittlungsverfahrens den Zusammenhang aufgrund von Auskunftsansprüchen herstellen können, stellt in Bezug auf den Website-Betreiber kei-

nen Personenbezug her. Für die Website-Betreiber ist damit die Herstellung eines Personenbezugs mittels der Kenntnis des Internet-Access-Providers ausgeschlossen (vgl. Eckhardt, K&R 2007, 602, 603).

(3) Auch das Argument, eine Verneinung des Personenbezugs von dynamischen IP-Adressen berge das Risiko, dass diese Daten an Dritte übermittelt würden, die ihrerseits die Möglichkeit hätten, den Nutzer zu identifizieren, was mit den Bestimmungen des Datenschutzrechts nicht vereinbar sei (so RB 7 unten), ist nach dem vorstehend Gesagten nicht stichhaltig: Dieses Argument ist der vom Kläger in diesem Zusammenhang erneut zitierten Entscheidung des AG Berlin-Mitte entnommen, wonach das Datenschutzrecht bereits für die Website-Betreiber gelten müsse, weil sie sonst die dynamische IP-Adresse an den Internet-Access-Provider frei von datenschutzrechtlichen Beschränkungen übermitteln dürften (AG Berlin-Mitte, Urt. 27.03.2007 - 5 C 314/06, ZUM 2008, 83 f, juris-Rn 14). Hier verkennt das AG-Berlin-Mitte und ihm folgend der Kläger aber, dass die Übermittlung von Daten auch dann dem Datenschutzrecht unterfällt, wenn die Daten zwar nicht für den Übermittelenden (hier: für die Beklagte oder für einen sonstigen Website-Betreiber), aber für den Empfänger (hier: für den Internet-Access-Provider) personenbezogene Daten sind bzw. werden (zutreffend: BU 23, 2. Abs.; vgl. auch Eckhardt, K&R 2007, 602, 603 reSp). Der Schutzbereich des Datenschutzrechts wäre mithin eröffnet, sobald das Datum an den Internet-Access-Provider übermittelt würde. Für den Internet-Access-Provider müssten die datenschutzrechtlichen Zulässigkeitsvoraussetzungen für eine Erhebung dieser Information vorliegen. Sind diese nicht gegeben darf er die Information vom Website-Betreiber – bildlich gesprochen – nicht annehmen. Die Befürchtung des Klägers, dass insoweit eine Schutzlücke bestehe, ist daher unbegründet (Eckhardt, K&R 2007, 602, 603 reSp).

cc) Der Kläger kann sich – entgegen RB 8, 2. Abs. – für das von ihm vertretene absolute Verständnis des Personenbezugs in § 3 Abs. 1 BDSG auch nicht etwa auf die Artikel-29-Gruppe der Datenschutzbeauftragten der EU-Mitgliedstaaten berufen. Denn in ihrer Stellungnahme 4/2007 vom 20.06.2007 über das Konzept der personenbezogenen Daten folgt die Artikel-29-Gruppe gerade nicht dem absoluten, sondern

vielmehr dem relativen Verständnis des Personenbezugs. Dies ergibt sich wortwörtlich aus den Ausführungen im zweiten Absatz der Seite 15 dieser Stellungnahme, wo es heißt:

> »Diese Aussage zeigt klar, dass der Grad, der für die Identifizierung als ausreichend beurteilt wird, vom Kontext der jeweiligen Situation abhängt.«

Deutlicher kann das relative Verständnis des Personenbezugs nicht zum Ausdruck gebracht werden. Dies ergibt sich auch aus den weiteren Ausführungen der Art.-29-Gruppe dazu, dass es sich bei dynamischen IP-Adressen für Internet Service-Provider per se um nicht personenbezogene Daten handle. Nur wenn und soweit eine Identifikation über Dritte (wie den Access-Provider) möglich sei und der Dienstanbieter nicht wisse, ob es sich im Einzelfall um eine dynamische oder eine statische IP-Adresse handle, unterliege die undifferenzierte Speicherung und Verwendung von IP-Adressen den datenschutzrechtlichen Vorschriften (vgl. Moos, K&R 2008, 137, 139 reSp).

d) Anders als der Kläger dies darzustellen versucht (RB 8 unten, RB 9), trifft es auch nicht zu, dass er anhand seiner IP-Adresse für die Beklagte auch auf legalem Wege, nämlich mittels eines Auskunftsersuchens nach § 113 TKG, ohne weiteres identifizierbar sei. Das Bundesverfassungsgericht hat mit Beschluss vom 24.01.2012 (BvR 1299/05 Rn 164 ff, Rn 174) entschieden, dass die Regelung des § 113 TKG a.F. verfassungskonform dahin auszulegen sei, dass sie für sich allein und ohne konkrete Abrufnorm noch keine Auskunftspflichten des Telekommunikationsunternehmens begründe und dass sie eine Zuordnung dynamischer IP-Adressen nicht (mehr) erlaube. § 113 TKG ist daraufhin mit Wirkung vom 01.07.2013 durch Gesetz vom 20.06.2013 (BGBl. I 2. 1602) neu gefasst worden. Nach § 113 Abs. 2 TKG n.F. darf Auskunft nach dieser Vor-schrift nur erteilt werden, soweit eine in Absatz 3 der Regelung genannte Stelle 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 Verfassungsschutzbehörden, des Militärischen Abschirmdienstes oder des Bundesnachrichtendienstes

unter Angabe einer gesetzlichen Bestimmung verlangt, die ihr eine Erhebung der entsprechenden Daten erlaubt. Nur an diese abschließend genannten Behörden darf die Übermittlung von Daten gemäß § 113 TKG erfolgen. Diese Behörden dürfen die Daten nicht an andere Behörden des Bundes weitergeben bzw. übermitteln. Insofern gilt nichts anderes als beim datenschutzrechtlichen Begriff der verantwortlichen Stelle.

e) Soweit der Kläger in tatsächlicher Hinsicht meint, er sei anhand der genutzten Adresse nicht nur dann identifizierbar, wenn die Beklagte die Adresse in Verbindung mit dem Zeitpunkt des jeweiligen Nutzungsvorgangs speichere (vgl. RB 10, lit. cc), trifft dies ebenfalls nicht zu: Wie die Beklagte vorinstanzlich mehrfach vorgetragen und unter Sachverständigenbeweis gestellt und wie dies auch das Berufungsgericht so festgestellt hat (BU 19/20), kann eine Zuordnung der IP-Adresse zu einem Internetanschluss und damit zu einem Anschlussinhaber als natürlicher Person – und nicht etwa zu einem mit dem Anschlussinhaber nicht notwendig identischen konkreten Nutzer, der noch nicht einmal vom Access-Provider eindeutig identifiziert werden kann – ausschließlich von dem Zugangsanbieter vorgenommen werden, zu dessen Adressbereich die fragliche IP-Adresse gehört. Nur dieser Zugangsanbieter weiß, welchem Kunden er eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugeteilt hat (SchrS 03.07.2008, S. 6, GA I 89; SchrS 22.03.2010, S. 11, GA II 113 jeweils mit 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. 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“ (SchrS 03.07.2008, S. 6, GA I 89; SchrS 22.03.2010, S. 11, GA II 113 jeweils mit Beweis: Sachverständigengutachten; vgl. auch AG Offenburg, Beschl. 20.07.2007 – 4 Gs 442/07, CR 2007, 676).

f) Aus den dargelegten Gründen kann ein Personenbezug der IP-Adresse für einen Website-Betreiber auch allenfalls dann entstehen, wenn der Nutzer seinen Klarnamen während des Nutzungsvorgangs

angibt und der Betreiber der Website den Klarnamen zusätzlich speichert (entgegen RB 10/11). Im Streitfall verhält es sich allerdings so, dass die Beklagte auch dann, wenn der Kläger auf einer Webseite in einem Formular seine Identität aktiv offenlegt (also z.B. Namen, Adresse etc. angibt), die IP-Adresse für die speichernde Stelle der Beklagten nur personenbeziehbar wäre, falls die Formulareingaben zusammen mit der IP-Adresse erfasst und gespeichert würden (SchrS 03.07.2008, S. 10, GA I 93 und SchrS 22.03.2010, S. 20, GA II 123, jeweils mit Beweis: Sachverständigengutachten). Da dies nicht der Fall ist, hätte das Berufungsgericht den vom Kläger geltend gemachten Unterlassungsanspruch auch nicht im tenorierten Umfang zusprechen dürfen. Hierzu wird auf die Revisionsbegründung der Beklagten verwiesen.

III.

Das angefochtene Urteil hält nach dem vorstehend Gesagten insoweit, als zum Nachteil des Klägers entschieden worden ist, der rechtlichen Nachprüfung stand. Es wird daher insoweit aufrecht zu erhalten sein.

[redacted]