BUNDESGERICHTSHOF

IM NAMEN DES VOLKES

URTEIL

III ZR 146/10

Verkündet am:
13. Januar 2011
K i e f e r
Justizangestellter
als Urkundsbeamter
der Geschäftsstelle

in dem Rechtsstreit

Nachschlagewerk: ja
BGHZ: nein
BGHR: ja

Speicherung dynamischer IP-Adressen

TKG § 97 Abs. 1 Satz 1, Abs. 2 Nr. 1, § 100 Abs. 1

a) 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.

b) 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.

BGH, Urteil vom 13. Januar 2011 - III ZR 146/10 - OLG Frankfurt am Main
LG Darmstadt

Der III. Zivilsenat des Bundesgerichtshofs hat auf die mündliche Verhandlung vom 13. Januar 2011 durch den Vizepräsidenten Schlick, die Richter Dörr und Dr. Herrmann, die Richterin Caliebe und den Richter Tombrink

für Recht erkannt:

Auf die Revision des Klägers wird das Urteil des 13. Zivilsenats in Darmstadt des Oberlandesgerichts Frankfurt am Main vom 16. Juni 2010 aufgehoben.

Die Sache wird zur neuen Verhandlung und Entscheidung, auch über die Kosten des Revisionsrechtszugs, an das Berufungsgericht zurückverwiesen.

Von Rechts wegen

Tatbestand

1 Die Beklagte bietet Telekommunikationsleistungen an. Der Kläger ist Inhaber eines von ihr bereitgestellten DSL-Anschlusses. Hierfür haben er und die Rechtsvorgängerin der Beklagten den "T. flat"-Tarif vereinbart. Dieser beinhaltet ein zeit- und volumenunabhängiges Pauschalentgelt, soweit der Kunde für die Einwahl in das Internet den von der Beklagten zur Verfügung gestellten DSL-Anschluss nutzt. Der Kunde kann sich mit seinen Zugangsdaten (Kennung und Passwort) jedoch auch über andere Telekommunikationsanschlüsse (zum Beispiel über Mobiltelefone, Anschlüsse von Wettbewerbern der

Beklagten im Inland oder aus dem Ausland) oder mittels anderer Zugangstechniken (z.B. Analog-, ISDN- oder GSM-Verbindungen) in die Dienste der Beklagten einwählen. In diesem Fall werden zeitabhängige Nutzungsentgelte berechnet. Ferner kann der Kunde Zugriff auf kostenpflichtige Dienste nehmen, die entsprechend der individuellen Nutzung gesondert und unabhängig von den angebotenen Zugangstarifen von der Beklagten in Rechnung gestellt werden.

2 Die Beklagte weist dem Rechner, den der Kunde zur Einwahl in das Internet nutzt, für die Dauer der einzelnen Verbindung eine IP-Adresse zu, die sie einem ihr zugeteilten Großkontingent entnimmt. Diese Adresse besteht aus einer mit einer Telefonnummer vergleichbaren, aus vier Blöcken gebildeten Ziffernfolge, die die Kommunikation vernetzter Geräte (z.B. Web-Server, E-Mail-Server oder Privatrechner) ermöglicht. Nach Beendigung der Verbindung wird die jeweilige IP-Adresse wieder freigegeben und steht den Kunden der Beklagten zur Einwahl in das Internet erneut zur Verfügung. Aufgrund dieses Verfahrens erhält der einzelne Nutzer für jede Einwahl in das Internet in aller Regel eine unterschiedliche IP-Nummer (dynamische IP-Adresse).

3 Die Beklagte speichert nach Beendigung der jeweiligen Verbindung unter anderem die hierfür verwendete IP-Adresse für einen gewissen Zeitraum. Diesen hat sie während des laufenden Rechtsstreits auf sieben Tage begrenzt. Zuvor hatte sie für die Speicherung eine längere Zeitspanne in Anspruch genommen. Der Kläger meint, die Beklagte sei verpflichtet, die IP-Adressen sofort nach dem Ende der einzelnen Internetsitzungen zu löschen. Die Beklagte ist demgegenüber der Auffassung, sie sei gemäß § 96 Abs. 1 Satz 2 i.V.m. § 97 Abs. 1 Satz 1, Abs. 2 Nr. 1 und § 100 Abs. 1 TKG zu einer vorübergehenden Speicherung der IP-Adressen berechtigt.

Hinweis: Auch Teile der Urteilssammlung sind als Datenbank nach §§ 87a ff. UrhG geschützt.

JLaw – Gesetze und Urteile (mobile App)
Kostenlos
Über 200 Gesetze
Über 100.000 Urteile
JLaw – für Android
JLaw – für iOS

4 Neben Löschungs- und Unterlassungsansprüchen hinsichtlich weiterer Daten hat der Kläger die Verurteilung der Beklagten zur sofortigen Löschung der seinem Rechner zugeteilten IP-Adressen nach dem jeweiligen Ende der Internetverbindungen verfolgt. Das Landgericht hat den Anträgen teilweise stattgegeben, hinsichtlich der IP-Adressen die Beklagte jedoch nur verurteilt, diese sieben Tage nach dem jeweiligen Ende der Internetverbindungen zu löschen. Die hiergegen gerichtete Berufung des Klägers ist erfolglos geblieben. Mit seiner vom Berufungsgericht zugelassenen Revision verfolgt er sein auf die Verpflichtung der Beklagten zur sofortigen Löschung der IP-Adressen gerichtetes Begehren weiter.

Entscheidungsgründe

5 Die zulässige Revision ist begründet. Sie führt zur Aufhebung des angefochtenen Berufungsurteils und zur Zurückverweisung der Sache an die Vorinstanz.

I.

6 Das Berufungsgericht hat in seiner Entscheidung (MMR 2010, 645) ausgeführt, die Beklagte sei zur Speicherung der IP-Adressen während des vom Landgericht ausgeurteilten Zeitraums berechtigt, da diese Daten zur Ermittlung des Entgelts und zur Abrechnung sowie zum Erkennen, Eingrenzen und Beseitigen von Störungen oder Fehlern an ihren Telekommunikationsanlagen erforderlich seien.

7 Der mit der Beklagten vereinbarte Tarif sehe nicht eine reine zeit- und volumenunabhängige Pauschale vor. Vielmehr seien für einzelne Nutzungen gesondert abzurechnende Entgelte zu zahlen. Die IP-Adressen seien zu deren Abrechnung erforderlich. Bei der Einwahl in das Internet würden auf dem dafür benötigten Radiusserver der Beklagten lediglich die jeweilige Kennung, das hinterlegte Passwort des Teilnehmers sowie die der einzelnen Internetverbindung zugeordnete IP-Adresse gespeichert, nicht aber das von dem jeweiligen Teilnehmer gewählte Tarifmodell. Der Radiusserver übertrage deshalb die IP-Adressen und die diesen jeweils zugeordneten Sessionsdaten an einen Computer des Abrechnungssystems der Beklagten. Ohne die IP-Nummern sei eine Entgeltberechnung nicht möglich. Dass die Beklagte gleichwohl über technische Mittel verfüge, die es ihr ermöglichten, auch ohne die zeitweise Speicherung von IP-Adressen die Abrechnungen zu erstellen, sei nicht zu erkennen und sei vom Kläger auch nicht einmal ansatzweise schlüssig dargetan worden. Er habe gegenüber den detaillierten Darlegungen der Beklagten lediglich eingewandt, es gebe "Log-Dateien". Es sei jedoch nicht ersichtlich, dass diese Dateien es ohne die IP-Adressen ermöglichten, die Abrechnung vorzunehmen. Dies ergebe sich auch nicht aus dem vom Landgericht eingeholten Sachverständigengutachten. Überdies könne dem Kläger nach § 44 Abs. 1, § 96 Abs. 1 Satz 3, § 97 Abs. 3 TKG allenfalls ein Anspruch auf "unverzügliche" und nicht etwa auf "sofortige" Löschung zustehen.

8 Auch die Voraussetzungen des in § 96 Abs. 1 Satz 2, § 100 Abs. 1 TKG geregelten Erlaubnistatbestands für die Speicherung der IP-Adressen seien für einen Zeitraum von sieben Tagen erfüllt. Aufgrund der plausiblen und im wesentlichen unstreitig gebliebenen Darlegungen der Beklagten könne davon ausgegangen werden, dass es dieser bei einer "sofortigen" Löschung der IP-Adressen derzeit praktisch unmöglich wäre, einen relevanten Teil von Störun-

gen und Fehlern an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. § 100 Abs. 1 TKG setze für die Speicherung von Verkehrsdaten im Gegensatz zu § 100 Abs. 3 TKG keine im "Einzelfall" bereits feststehende Störung voraus. Vielmehr müsse die Beklagte in die Lage versetzt werden, regelmäßig erst nach einigen Tagen eingehenden Störungsmitteilungen auf den Grund zu gehen. Hierfür seien in der Regel die IP-Adressen notwendig. Bei der Versendung von "Schrottmails" (Spam), Hackerangriffen, der Verbreitung von Viren und Trojanern, und bei massenweisen Zugriffen auf bestimmte Webseiten (Denial-of-Service-Attacken) seien die Störungen nur zu beseitigen, wenn die IP-Adressen der (gegebenenfalls zuvor infizierten) Rechner bekannt seien, von denen die Attacken ausgingen. Anderenfalls seien die betroffenen Computer nicht identifizierbar. Wenn eine an einem Angriff beteiligte IP-Adresse aus dem Kontingent eines bestimmten Internetproviders, etwa der Beklagten, stamme, wendeten sich die Betroffenen oder deren Internetprovider an denjenigen, dessen Bereich die betreffende Adresse zuzuordnen sei, um Angriffe stoppen zu lassen beziehungsweise zumindest hierauf hinzuweisen. Die Beklagte müsse durch die Speicherung der IP-Adressen in der Lage sein, derartige Störungen abzustellen. Anderenfalls sei auch ihre eigene Infrastruktur gefährdet. Es sei nachvollziehbar und allgemein bekannt, dass, wenn ein Internetprovider nicht gegen Versender von Spams, Schadsoftware und dergleichen vorgehe, dies zur Sperrung bestimmter IP-Adressenkontingente, von denen die Störungen ausgegangen seien, durch andere Internetdienstleister und -provider führe. Diese Adressenbereiche seien dann nicht mehr erreichbar und könnten von der Beklagten und deren Kunden nicht mehr genutzt werden.

9 Der Kläger habe sich demgegenüber bis zuletzt lediglich pauschal und ohne nähere Details darauf berufen, dass es "zumutbare technische Mittel zur unwiederbringlichen Anonymisierung von Datenbeständen (gebe), deren Ein-

satz gleichwohl die Nutzbarkeit der Daten" im Sinne einer Netzsicherheit gewährleisten könnte. Dem entsprechenden Beweisangebot, ein Sachverständigengutachten einzuholen, sei nicht nachzugehen gewesen, weil es einer im Zivilprozess unstatthaften Erhebung eines Ausforschungsbeweises gleichgekommen wäre.

II.

10 Dies hält der rechtlichen Nachprüfung nicht in allen Punkten stand. Nach dem derzeitigen Sach- und Streitstand ist es nicht auszuschließen, dass die Beklagte zu einer vorübergehenden Speicherung der dem Rechner des Klägers jeweils zugeteilten dynamischen IP-Adressen nach Beendigung der Internetverbindungen nicht berechtigt ist, so dass dieser gemäß § 44 Abs. 1 Satz 1 i.V.m. § 96 Abs. 1 Satz 3 TKG die unverzügliche Löschung verlangen kann. Sofern für die Speicherung der IP-Adressen keine Rechtsgrundlage besteht, kann dieser Anspruch je nach den technischen Möglichkeiten auch auf eine "sofortige" Löschung hinauslaufen. Die tatsächlichen Voraussetzungen für die Befugnis der Beklagten zur Erhebung und Verwendung dieser Daten gemäß § 96 Abs. 1 Satz 2 i.V.m. § 97 Abs. 1 Satz 1, Abs. 2 Nr. 1, § 100 Abs. 1 TKG hat das Berufungsgericht, wie die Revision zutreffend rügt, nicht frei von Rechtsfehlern festgestellt.

11 1. Die Vorinstanz hätte nicht ohne Beweisaufnahme davon ausgehen dürfen, die Beklagte sei berechtigt, die IP-Adressen zum Zweck der Entgeltermittlung und Abrechnung zu erheben und zu verwenden (§ 97 Abs. 1 Satz 1, Abs. 2 Nr. 1 TKG), weil diese Daten hierfür erforderlich seien.

12 a) Die Beklagte ist entgegen der Ansicht der Revisionserwiderung für die tatsächlichen Voraussetzungen ihrer Berechtigung, die streitgegenständlichen Daten zu speichern, darlegungs- und beweisbelastet. Aus §§ 95 bis 98 TKG ergibt sich, dass der Diensteanbieter keine Daten seiner Kunden erheben und verwenden darf, es sei denn, das Gesetz räumt ihm eine Befugnis hierzu ein. Da sich die Beklagte damit auf einen Erlaubnistatbestand beruft (vgl. Begründung der Bundesregierung zum Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes, BT-Drs. 16/11967 S. 17), der eine Ausnahme von ihrer grundsätzlichen Löschungspflicht (Büttgen in Scheurle/Mayen, TKG, 2. Aufl., § 96 Rn. 10; Klesczewski in Berliner Kommentar zum TKG, 2. Aufl., § 96 Rn. 13) darstellt, trifft sie für die ihm zugrunde liegenden Tatsachen die Darlegungs- und Beweislast (vgl. z.B. BGH, Urteile vom 21. April 2010 - XII ZR 134/08, FamRZ 2010, 1050 Rn. 52; vom 14. Oktober 2009 - XII ZR 146/08, FamRZ 2009, 1990 Rn. 18 jew. m.w.N.; vom 3. Juli 2009 - V ZR 182/08, ZOV 2009, 237 Rn. 32; Beschluss vom 5. Februar 2007 - II ZR 51/06, WM 2007, 1465 Rn. 4).

13 Entgegen der Ansicht der Vorinstanz folgt aus dem unstreitig gebliebenen Parteivorbringen nicht, dass die Voraussetzungen des Erlaubnistatbestands des § 97 Abs. 1 Satz 1, Abs. 2 Nr. 1 TKG erfüllt sind. Als unstreitig hat das Berufungsgericht lediglich die bei der Beklagten praktizierten Abläufe der Entgeltermittlung und Abrechnung und insbesondere die Verwendung der IP-Adressen, und nicht der Kundenkennung, für diese Zwecke festgestellt. Hieraus folgt indessen nicht, dass die Speicherung der IP-Adressen im Sinne des § 97 Abs. 1 Satz 1 TKG für diese Zwecke "benötigt" wird. Dies richtet sich nicht allein nach der vom Diensteanbieter angewandten Abrechnungstechnik. In dem Erfordernis, dass die jeweiligen Verkehrsdaten für diese Zwecke "benötigt" werden, kommt vielmehr der bei der gebotenen Abwägung der Datenschutzbelan-

ge des Kunden mit den berechtigten Interessen des Diensteanbieters zu beachtende Verhältnismäßigkeitsgrundsatz zum Ausdruck (siehe hierzu näher unten Nummer 2 Buchst. b cc). Bei dem in § 97 Abs. 1 Satz 1 TKG verwendeten Wort "benötigt" handelt es sich demnach um einen unbestimmten Rechtsbegriff des Inhalts, dass für die in dieser Vorschrift geregelten Zwecke kein weniger eingriffsintensives Mittel zur Verfügung steht, als die Erhebung und Verwendung der jeweils in Rede stehenden Verkehrsdaten.

14 Der Sachverständige Dipl.-Ing. X hat in diesem Zusammenhang in seinem Gutachten die Behauptung der Beklagten, die IP-Adressen seien zur Entgeltermittlung und Abrechnung erforderlich, nicht bestätigt und ausgeführt, bereits die so genannten Log-Dateien, die auf dem Radiusserver gespeichert würden, ermöglichten ohne Rückgriff auf die IP-Adressen die Zuordnung der jeweiligen Internetsitzung zu den einzelnen Kunden und damit auch die Abrechnung. Dem ist die Beklagte zwar ausführlich entgegengetreten und hat insbesondere geltend gemacht, in den vom Gutachter möglicherweise mit dem Begriff "Log-Dateien" gemeinten Sessionsdaten seien die IP-Adressen enthalten. Der Kläger hat diesen Vortrag jedoch weiterhin in dem entscheidenden Punkt bestritten, dass die Abrechnung ohne die gespeicherten IP-Adressen nicht möglich sei. Ob dies der Fall ist und ob die anderen, ohnehin gespeicherten Daten zur Entgeltermittlung und Abrechnung genügen und mit deren Verwendung ein weniger intensiver Eingriff in die Rechte der Kunden der Beklagten verbunden ist, ist zu klären.

15 Die Revision beanstandet zu Recht, das Berufungsgericht hätte, sofern es die Beklagte nicht aufgrund der Ausführungen des Gutachters als beweisfällig ansehen wollte, seine Feststellungen zur Notwendigkeit, die streitgegenständlichen Daten zur Entgeltermittlung und Abrechnung zu speichern, nicht

treffen dürfen, ohne den erstinstanzlich herangezogenen Gutachter anzuhören (§ 411 Abs. 3 ZPO), ihm eine neue Begutachtung aufzugeben (§ 412 Abs. 1, 1. Alt. ZPO) oder sich anderweitig sachverständig beraten zu lassen (§ 412 Abs. 1, 2. Alt. ZPO).

16 Es ist zwar grundsätzlich dem pflichtgemäßen Ermessen des Tatrichters überlassen, ob er seine eigene Sachkunde für ausreichend erachtet und deshalb von der Einholung eines Sachverständigengutachtens absieht. Die Grenze seines Ermessens hat das Berufungsgericht jedoch nicht eingehalten. Die Würdigung eines schwierigen technischen Sachverhalts, wie hier die Beurteilung, ob für die Zuordnung abrechnungsrelevanter Internetsessionsdaten zu den einzelnen Kunden der Beklagten die Speicherung der IP-Adressen erforderlich ist, setzt besondere technische Kenntnisse voraus und wird nicht schon durch die Beherrschung allgemeiner Erfahrungssätze ermöglicht. Der Tatrichter kann, wenn es um die Beurteilung einer Fachwissen voraussetzenden Frage geht, auf die Einholung eines Sachverständigengutachtens nur verzichten, wenn er entsprechende eigene besondere Sachkunde auszuweisen vermag und dies in einem vorherigen Hinweis an die Parteien dartut (vgl. zum Ganzen Senatsurteil vom 23. November 2006 - III ZR 65/06, NJW-RR 2007, 357 Rn. 14 m.w.N.).

17 b) Der Verfahrensmangel ist entscheidungserheblich, denn dem Berufungsgericht ist im Ausgangspunkt darin beizupflichten, dass die zwischen den Parteien bestehenden Tarifvereinbarungen eine Zuordnung der jeweiligen Sessionsdaten zu dem Kundenkonto des Klägers erfordern. Deshalb scheidet entgegen der Ansicht der Revision die Berechtigung der Beklagten zur Speicherung der zugeteilten dynamischen IP-Adressen gemäß § 97 Abs. 1 Satz 1, Abs. 2 Nr. 1 TKG nicht von vornherein aus. Zwar beinhaltet der Tarif ein zeit- und volumenunabhängiges Pauschalentgelt (Flatrate), soweit sich der Kläger

zur Herstellung einer Internetverbindung des von der Beklagten zur Verfügung gestellten DSL-Anschlusses bedient. Allerdings hat er auch die Möglichkeit, seine Zugangsdaten für andere Arten der Einwahl in das Internet und zur Inanspruchnahme von kostenpflichtigen Angeboten der Beklagten zu nutzen. In diesen Fällen entstehen zusätzliche Kosten. Dass der Kläger diese Möglichkeiten bislang nicht genutzt hat, schließt, wie das Berufungsgericht zutreffend ausgeführt hat, nicht aus, dass er künftig hiervon Gebrauch machen wird. Für diesen Fall muss die Beklagte in der Lage sein, anhand der Sessionsdaten und ihrer Zuordnung zum Kläger, diese Leistungen abzurechnen.

18 2. Ebenfalls nicht frei von Rechtsfehlern hat das Berufungsgericht die Feststellungen zu den Voraussetzungen des § 100 Abs. 1 TKG getroffen. Nach dieser Bestimmung darf der Diensteanbieter zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen unter anderem die Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden, soweit dies für diese Zwecke erforderlich ist.

19 a) Die Revision rügt insoweit zutreffend, das Berufungsgericht habe dem Kläger nicht entgegenhalten dürfen, er habe sich ohne Angabe näherer Details darauf berufen, es gebe entgegen den Behauptungen der Beklagten zumutbare technische Mittel, die Netzsicherheit zu gewährleisten, ohne auf die jeweils zugeteilten IP-Adressen zurückgreifen zu müssen. Der Kläger durfte sich auf ein einfaches Bestreiten der gegenteiligen Behauptungen der Beklagten beschränken. Diese ist, wie sich aus den Ausführungen zu 1 a ergibt, für die tatsächlichen Voraussetzungen ihrer Berechtigung, die streitgegenständlichen Daten in Ausnahme von § 96 Abs. 1 Satz 3 TKG zu speichern, darlegungs- und beweisbelastet.

20 Im Grundsatz hängt die Substantiierungslast des Bestreitenden davon ab, wie eingehend die darlegungspflichtige Gegenpartei vorgetragen hat (st. Rspr.; vgl. z.B. BGH, Urteile vom 15. Juni 2000 - I ZR 55/98, NJW-RR 2000, 1635, 1638; vom 3. Februar 1999 - VIII ZR 14/98, NJW 1999, 1404, 1405 f und vom 12. Oktober 1989 - IX ZR 184/88, BGHZ 109, 47, 55). In der Regel genügt aber gegenüber einer Tatsachenbehauptung der darlegungspflichtigen Partei ein einfaches Bestreiten des Gegners (BGH, Urteile vom 15. Juni 2000 und 3. Februar 1999 jew. aaO; vom 11. Juli 1995 - X ZR 42/93, NJW 1995, 3311, 3312 und vom 23. März 1993 - VI ZR 176/92, NJW 1993, 1782, 1783). Eine darüber hinausgehende Substantiierungslast trifft die nicht darlegungsbelastete Partei im Regelfall nur dann, wenn der darlegungspflichtige Gegner außerhalb des von ihm darzulegenden Geschehensablaufs steht und die maßgeblichen Tatsachen nicht kennt, während sie der anderen Partei bekannt und ihr ergänzende Angaben zuzumuten sind (z.B. BGH, Urteile vom 15. Juni 2000 aaO; vom 19. April 1999 - II ZR 331/97, NJW-RR 1999, 1152; vom 3. Februar 1999 aaO; vom 7. Dezember 1998 - II ZR 266/97, BGHZ 140, 156, 158; vom 17. Oktober 1996 - IX ZR 293/95, NJW 1997, 128 , 129 und vom 11. Juni 1990 - II ZR 159/89, NJW 1990, 3151 f).

21 Die Voraussetzungen für die Notwendigkeit eines qualifizierten Bestreitens liegen im Streitfall nicht vor. Der Kläger hat keine der Beklagten überlegenen technischen Erkenntnismöglichkeiten und steht den maßgeblichen Geschehensabläufen nicht näher als diese. Vielmehr ist das Gegenteil der Fall. Angesichts der Komplexität der maßgeblichen technischen Zusammenhänge kann ungeachtet der ausführlichen Darlegungen der Beklagten auch nicht davon ausgegangen werden, dass jeglicher Anhaltspunkt für die Möglichkeit der objektiven Unrichtigkeit ihrer Behauptungen zur Notwendigkeit fehlt, die IP-Adressen zu den in § 100 Abs. 1 TKG aufgeführten Zwecken kurzzeitig zu speichern. Dies gilt umso mehr, als auch das erstinstanzlich eingeholte Sachverständigengutachten nur die Geeignetheit der Speicherung der IP-Adressen für diese Zwecke, nicht aber die Erforderlichkeit bestätigt hat. Das Berufungsgericht durfte deshalb den diesbezüglichen Sachvortrag der Beklagten nicht als unstreitig behandeln. Eine etwaige Beweisaufnahme wäre entgegen der Ansicht der Vorinstanz auch nicht auf eine Ausforschung über die unsubstantiierten Erklärungen des Klägers hinausgelaufen. Vielmehr wäre Beweis über die Richtigkeit der detaillierten Angaben der Beklagten zu erheben gewesen.

22 b) Dieser Verfahrensfehler ist entscheidungserheblich. Dem Berufungsgericht ist im Ergebnis darin zu folgen, dass, sofern die Speicherung der dynamischen IP-Adressen notwendig ist, um unter anderem der Versendung von Spam-Mails und Denial-of-Service-Attacken entgegen zu wirken, die Beklagte nicht vor Ablauf von sieben Tagen zur sofortigen Löschung verpflichtet ist. Der Senat schließt sich insoweit der von dem Bundesbeauftragten für den Datenschutz und Informationsfreiheit (offener Brief des Bundesbeauftragten vom 16. März 2007, im Internet abrufbar unter http://web10.ub.uni-rostock.de/uploads/sima-nowski/ma/schaar2007.htm; so auch AG Bonn MMR 2008, 203, 204) vertretenen Auffassung an.

23 aa) Zu den Verkehrsdaten, die nach § 100 Abs. 1 TKG erhoben und verwendet werden dürfen, gehören grundsätzlich auch die jeweils genutzten IP-Adressen (Begründung der Bundesregierung des Entwurfs eines Telekommunikationsgesetzes, BT-Drucks. 15/2316 S. 90; Wittern in Beck' scher TKG-Kommentar, 2006, § 100 Rn. 3; vgl. auch BVerfG NJW 2010, 833 Rn. 254).

24 bb) Keinen rechtlichen Bedenken unterliegt weiter die auch von der Revision nicht gerügte Auffassung des Berufungsgerichts, dass eine abzuwehrende Störung im Sinne des § 100 Abs. 1 TKG unter anderem vorliegt, wenn Internetdienstleister bestimmte IP-Adressbereiche eines anderen Internetanbieters - hier der Beklagten - sperren, weil von ihnen Schadprogramme oder massenweise so genannte Spam-Mails versandt werden oder "Denial-of-Service-Attacken" ausgehen. Der Begriff der Störung ist umfassend zu verstehen als jede vom Diensteanbieter nicht gewollte Veränderung der von ihm für sein Telekommunikationsangebot genutzten technischen Einrichtungen (vgl. Begründung der Bundesregierung zum Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes, durch den eine mit § 100 Abs. 1 TKG fast wortgleiche Bestimmung an § 15 des Telemediengesetzes angefügt werden sollte, BT-Drs. 16/11967 S. 17). Der Begriff der Telekommunikationsanlagen in § 100 Abs. 1 TKG schließt überdies nach der Legaldefinition des § 3 Nr. 23 TKG neben den technischen Einrichtungen auch das gesamte System ein. Die Sperrung der von dem Diensteanbieter vorgehaltenen IP-Adressenkontingente stellt damit auch eine Veränderung der Telekommunikationsanlagen dar, die sodann nicht mehr nutzbar sind.

25 cc) Entgegen der Auffassung der Revision (so wohl auch Bundesrat, Stellungnahme zum Entwurf eines Gesetzes zur Stärkung der Sicherheit in der

Informationstechnik des Bundes, BR-Drs. 62/09 Beschluss S. 9 f, kritisch auch Breyer RDV 2004, 147 f) setzt die in § 100 Abs. 1 TKG geregelte Befugnis zur Erhebung und Verwendung von Daten auch unter Berücksichtigung des Fernmeldegeheimnisses (Art. 10 Abs. 1 GG, § 88 TKG) und des Grundrechts auf informationelle Selbstbestimmung (Art. 1 Abs. 1, Art. 2 Abs. 1 GG) nicht voraus, dass im Einzelfall bereits Anhaltspunkte für eine Störung oder einen Fehler an den Telekommunikationsanlagen vorliegen (Eckhardt CR 2003, 805, 809; Kannenberg in Scheurle/Mayen, aaO, § 100 Rn. 10; Klesczewski aaO, § 100 Rn. 8; Wittern aaO Rn. 2). 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.

26 (1) Dies ergibt sich aus dem Vergleich von § 100 Abs. 1 TKG mit seiner Vorgängerregelung, dem § 9 Abs. 1 Nr. 1 der Telekommunikations-Datenschutzverordnung (TDSV) vom 18. Dezember 2000 (BGBl. I S. 1740), und mit § 100 Abs. 3 TKG. § 9 Abs. 1 TDSV setzte sowohl für die nunmehr in § 100 Abs. 1 TKG als auch für die in Absatz 3 dieser Bestimmung geregelten Fallgestaltungen voraus, dass die Datenerhebung und -verwendung im jeweiligen Einzelfall erforderlich war. Diese Bedingung ist im Gesetzestext nunmehr für die vormals in § 9 Abs. 1 Nr. 1 TDSV geregelten Fälle des § 100 Abs. 1 TKG (Störungen und Fehler an Telekommunikationsanlagen) entfallen. Demgegenüber ist sie in Absatz 3 für die früher § 9 Abs. 1 Nr. 2 TDSV zugrunde liegenden Sachverhalte der Leistungserschleichung und sonstigen missbräuchlichen Inanspruchnahme der Telekommunikationsnetze beibehalten worden. Dem ist zu entnehmen, dass für § 100 Abs. 1 TKG nicht mehr erforderlich ist, dass im Einzelfall Anhaltspunkte für eine Störung oder einen Fehler bestehen. Für den Verzicht auf dieses Erfordernis spricht im Übrigen, dass hierfür ein gesetzgeberi-

sches Bedürfnis bestand, da insbesondere zur Abwehr erheblichen Spam-Aufkommens und von so genannten Denial-of-service-Attacken generelle Abwehrmaßnahmen erforderlich sind, um die Funktionsfähigkeit des Telekommunikationsbetriebs zu gewährleisten (Wittern aaO). Die Beklagte ist nach § 109 Abs. 1 Nr. 2, Abs. 2 TKG verpflichtet, derartige präventive Schutzmaßnahmen gegen Störungen zu treffen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen können. Schließlich streitet dafür, dass eine abstrakte Gefahr für die Ermächtigung des § 100 Abs. 1 TKG genügt, dass der Diensteanbieter die Daten auch zum "Erkennen" von Störungen und Fehlern sammeln und verwerten darf (Wittern aaO Rn. 6). Das "Erkennen" von Störungen und Fehlern findet in der Regel in einem Stadium statt, in dem Anhaltspunkte hierfür erst gewonnen werden, also ein konkreter Verdacht noch nicht bestehen muss (Wittern aaO; enger: Gramlich in Manssen, Telekommunikations- und Multimediarecht, Stand August 2008, § 100 Rn. 18).

27 (2) Diese Auslegung begegnet auch keinen verfassungsrechtlichen Bedenken. § 100 TKG greift zwar, soweit er die Erhebung und Verwendung von Telekommunikationsdaten erlaubt, in den Anspruch des einzelnen Nutzers auf Wahrung des Fernmeldegeheimnisses (Art. 10 Abs. 1 GG, § 88 TKG) und seines Grundrechts auf informationelle Selbstbestimmung (Art. 1 Abs. 1, Art. 2 Abs. 1 GG) ein. Insbesondere Art. 10 Abs. 1 GG begründet nicht nur ein Abwehrrecht gegen den Staat, sondern auch einen Auftrag an diesen, Schutz insoweit vorzusehen, als Private sich Zugriff auf Kommunikationsdaten verschaffen (BVerfG NJW 2007, 3055 Rn. 13). Diese Rechte können und müssen aber mit den berechtigten Belangen der Telekommunikationsunternehmen, öffentlichen Interessen und den übrigen Interessen der Kunden abgewogen werden (vgl. BVerfG aaO Rn. 14). § 100 TKG bringt die Rechte der Nutzer aus Art. 1 Abs. 1, Art. 2 Abs. 1 und Art. 10 Abs. 1 GG mit den gleichfalls grundrechtlich

geschützten Rechten des Diensteanbieters aus Art. 12 Abs. 1 und Art. 14 Abs. 1 GG sowie mit dem legitimen Interesse der Nutzer und dem öffentlichen Interesse (§ 109 Abs. 1 Nr. 2, Abs. 2 TKG) an der Funktions- und Leistungsfähigkeit des Telekommunikationssystems zum Ausgleich. Die präventive Erhebung und Verwertung von Daten wird hierbei nicht unbegrenzt erlaubt, auch wenn eine abstrakte Gefahr von Störungen und Fehlern an Telekommunikationsanlagen genügt. Vielmehr werden die Befugnisse des Diensteanbieters durch den Verhältnismäßigkeitsgrundsatz strikt begrenzt (Wittern aaO Rn. 7).

28 Die anlasslose, jedoch auf sieben Tage begrenzte Speicherung der jeweils genutzten IP-Adressen wahrt - ihre technische Erforderlichkeit für die Zwecke des § 100 Abs. 1 TKG vorausgesetzt - die Verhältnismäßigkeit. Die bloße Speicherung der IP-Adressen stellt noch keinen schwerwiegenden Eingriff in die Grundrechte der Nutzer dar (vgl. BVerfGE 121, 1, 20; vgl. ferner BVerfG NJW 2010, 833 Rn. 254). 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 (BVerfGE 120, 378, 402). Die Identität des jeweiligen Nutzers ist aus der IP-Nummer selbst nicht erkennbar und wird erst durch die Zusammenführung mit weiteren Angaben ermittelbar. Diese findet jedoch - nach dem bisherigen Sach- und Streitstand - für die Zwecke des § 100 Abs. 1 TKG nur bei dem konkreten Verdacht einer Störung oder eines Fehlers an den Telekommunikationsanlagen statt. Überdies ist die Speicherung auf einen sehr kurzen Zeitraum begrenzt.

29 Allerdings können bei einer, wie im vorliegenden Sachverhalt, anlasslosen Speicherung von Daten erhöhte Anforderungen an die Verhältnismäßigkeit der Maßnahme zu stellen sein. Informationserhebungen gegenüber Personen,

die den Eingriff durch ihr Verhalten nicht veranlasst haben, sind grundsätzlich von höherer Eingriffsintensität als anlassbezogene. Werden Personen, die keinen Erhebungsanlass gegeben haben, in großer Zahl in den Wirkungsbereich einer Maßnahme einbezogen, können von ihr auch allgemeine Einschüchterungseffekte ausgehen, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen können. Die Unbefangenheit des Verhaltens wird insbesondere gefährdet, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen (BVerfG aaO m.w.N.). Diese zu strafprozessualen, präventiv-polizeilichen und geheimdienstlichen Eingriffen entwickelte Rechtsprechung ist aber nicht ohne Abstriche auf die vorliegende Fallgestaltung zu übertragen. Die Intensität des Eingriffs für den Grundrechtsträger wird maßgeblich davon beeinflusst, welche Nachteile ihm über die Informationserhebung hinaus drohen oder von ihm nicht ohne Grund befürchtet werden (BVerfG aaO S. 403). Die kurzzeitige Speicherung der dynamischen IP-Adressen durch die Beklagte zum Zweck des Erkennens, des Eingrenzens und der Beseitigung von Störungen und Fehlern und damit des Schutzes ebenfalls teilweise grundrechtlich geschützter Rechte und öffentlicher Interessen zielt nicht auf Maßnahmen hoheitlicher Repression oder Verhaltensüberwachung ab. Eine Identifizierung des Anschlusses, dem die IP-Adresse zugeteilt wurde, findet für die Zwecke des § 100 Abs. 1 TKG überdies erst bei einem konkreten Anlass statt. Die IP-Adressenspeicherung ist daher, wenn überhaupt, lediglich in sehr geringem Maß geeignet, einzuschüchtern oder auch nur die Unbefangenheit des Kunden bei der Nutzung des Internets zu beeinträchtigen.

30 Demgegenüber sind die Interessen, denen die Datenspeicherung dient, von erheblichem Gewicht, selbst wenn, wie der Kläger geltend macht, nur ein sehr geringer Teil der gespeicherten IP-Adressen für die in § 100 Abs. 1 TKG

aufgeführten Zwecke verwendet wird. Sofern die IP-Nummern zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern notwendig sind, würde der Verzicht auf die Speicherung angesichts der gerichtsbekannten Häufigkeit der Versendung von Spam-Mails, Schad- und Spionageprogrammen und der "Denial-of-Service-Attacken" auf Dauer - zum Schaden der Beklagten und aller ihrer Nutzer - zu einer schwerwiegenden und nachhaltigen Beeinträchtigung der Kommunikationsinfrastruktur führen.

31 Insgesamt ist der mit der streitgegenständlichen Speicherung verbundene Eingriff in die Rechte der Nutzer vergleichsweise gering und überwiegt die legitimen, teilweise ebenfalls grundrechtlich abgesicherten Interessen der Beklagten und ihrer Kunden sowie die öffentlichen Interessen an der Funktionstüchtigkeit und Leistungsfähigkeit der Telekommunikationsinfrastruktur nicht.

32 (3) § 100 Abs. 1 TKG ist in dieser Auslegung auch mit dem europäischen Recht vereinbar.

33 (a) Gemäß Art. 15 Abs. 1 der maßgeblichen Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (ABl. L 201 vom 31. Juli 2002 S. 37 - im Folgenden: RL) können die Mitgliedstaaten Rechtsvorschriften erlassen, nach denen Verkehrsdaten im Sinne des Art. 6 Abs. 1 RL, zu denen auch die IP-Adressen gehören, unter anderem dann gespeichert werden dürfen, wenn dies "zur Verhütung, Ermittlung, Feststellung ... des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist". Zu einem unzulässigen Gebrauch elektronischer Kommunikationssysteme gehört auch der Missbrauch des Inter-

nets durch die Versendung von Spam-Mails, Schad- und Spionageprogrammen sowie durch Denial-of-Service-Attacken. Die Speicherung der IP-Adressen für sieben Tage nach Beendigung der jeweiligen Verbindung ist, ihre technische Notwendigkeit zur Abwehr oder zur Beseitigung derartiger Missbräuche vorausgesetzt, damit vom Wortlaut des Art. 15 Abs. 1 RL gedeckt. Eine solche Speicherung ist aus den vorgenannten Gründen nach den Maßstäben des Grundgesetzes verhältnismäßig. Da nichts dafür ersichtlich ist, dass Art. 15 Abs. 1 RL insoweit weitergehende Anforderungen enthält, ist sie auch "notwendig, angemessen und verhältnismäßig" im Sinne dieser Bestimmung.

34 Dies gilt auch, soweit die Speicherung der IP-Adressen einen im Einzelfall bestehenden Anhaltspunkt für einen unzulässigen Gebrauch des Internets nicht voraussetzt. Zwar hat die Generalanwältin des Gerichtshofs der Europäischen Union Kokott in ihren Schlussanträgen in der Rechtssache "Promusicae" (C-275/06) Zweifel daran geäußert, ob die Speicherung von Verkehrsdaten aller Nutzer ohne einen konkreten Verdacht gemäß Art. 15 Abs. 1 RL, wie sie im dortigen Fall zur Durchsetzung von Urheberrechten für allerdings erheblich längere Dauer in Rede stand, mit Grundrechten vereinbar" sei (Slg. 2008 S. I-271, 296 Rn. 82). Der Gerichtshof hat diese Bedenken in seinem Urteil zu jener Sache jedoch nicht aufgegriffen. Vielmehr hat er lediglich ausgeführt, die Richtlinie 2002/58/EG gebiete zur Wahrung der Art. 7 und 8 der Charta der Grundrechte der Europäischen Union (Achtung des Privatlebens und Schutz personenbezogener Daten) die Herstellung eines angemessenen Gleichgewichts zwischen diesen Rechten einerseits und den Rechten und Interessen, denen die Datenerhebung und -verarbeitung dienen soll, andererseits (aaO S. I-271, 344 ff, Rn. 64 ff). Dabei komme den Mitgliedstaaten ein Beurteilungsspielraum beim Erlass der Umsetzungsmaßnahmen zu, die an die verschiedenen denkbaren Sachverhalte angepasst werden könnten (aaO S. 345, Rn. 67).

Hieraus ergibt sich, dass der Gerichtshof eine anlasslose "Vorratsdatenspeicherung" nicht per se für unzulässig hält, sie vielmehr unter der Voraussetzung einer - dem Beurteilungsermessen der Mitgliedstaaten überlassenen und hier aus den oben dargestellten Gründen gegebenen - angemessenen Abwägung der betroffenen Belange für (europa-)rechtlich möglich hält.

35 (b) Einer Vorlage der Sache an den Gerichtshof der Europäischen Union (Art. 267 Abs. 2, 3 AEUV) bedarf es trotz der hohen Hürden für den Verzicht auf diese Maßnahme (vgl. hierzu BGH, Beschluss vom 26. November 2007 - NotZ 23/07, BGHZ 174, 273 Rn. 34 m.w.N.) nicht. Die vorstehenden Schlussfolgerungen ergeben sich ohne weiteres aus dem eindeutigen Wortlaut des Art. 15 Abs. 1 RL und der zitierten Entscheidung des Gerichtshofs. Hinsichtlich der Abwägung zwischen dem Fernmeldegeheimnis sowie dem Recht der Internetnutzer auf informationeile Selbstbestimmung einerseits und den Belangen der Beklagten sowie der übrigen Nutzer und den öffentlichen Interessen an der Funktionstüchtigkeit der Telekommunikationssystems andererseits ist insbesondere zu berücksichtigen, dass die Richtlinie den Mitgliedstaaten bei der Gewichtung der widerstreitenden Interessen einen Beurteilungsspielraum eröffnet (EuGH aaO). Ein solcher ist nur bei offensichtlich unverhältnismäßigen nationalen Maßnahmen überschritten (vgl. BGH aaO Rn. 37 m.w.N.). Dass die der Auslegung des Senats von § 100 Abs. 1 TKG zugrunde liegende Abwägung der wechselseitigen Belange nicht offensichtlich unverhältnismäßig ist, liegt auf der Hand. Aus diesen Gründen ist die richtige Anwendung des Unionsrechts derart offenkundig, dass für einen vernünftigen Zweifel kein Raum mehr verbleibt und eine Vorlage nach Art. 267 Abs. 2, 3 AEUV damit nicht geboten ist (acte clair, vgl. BGH aaO Rn. 34; Urteil vom 6. November 2008 - III ZR 279/07, BGHZ 178, 243 Rn. 31).

36 3. Da noch Feststellungen nachzuholen sind, ist die Sache nicht zur Endentscheidung reif und deshalb unter Aufhebung des angefochtenen Berufungsurteils an die Vorinstanz zurückzuverweisen (§ 563 Abs. 1, 3 ZPO).

Schlick Dörr Herrmann

Caliebe Tombrink

Vorinstanzen:
LG Darmstadt, Entscheidung vom 06.06.2007 - 10 O 562/03 -
OLG Frankfurt in Darmstadt, Entscheidung vom 16.06.2010 - 13 U 105/07 -