[redacted]

[redacted]

Landgericht Darmstadt
- 10. Zivilkammer -

64278 DARMSTADT

per Fax: 06151-125917

10.07.2004

Az. 10 O 562/03 - [redacted] ./. T-Online AG

Hohes Gericht,

wie unzählige andere Internetnutzer bin auch ich von der Datenspeicherpraxis der T-Online International AG betroffen, deren Zulässigkeit Gegenstand des vorbezeichneten Verfahrens ist. Da die deutsche Zivilprozessordnung für solche Fälle keine besondere Mitwirkungsmöglichkeit vorsieht, andererseits aber auch die Anstrengung von Parallelverfahren nicht sinnvoll ist, möchte ich auf das Rechtsinstitut des *amicus curiae* zurückgreifen, um das Gericht auf einige wichtige Umstände hinzuweisen, die für den o.g. Rechtsstreit entscheidungserheblich sind. Die ZPO lässt die Verwertung von gerichts- und allgemeinkundigen Tatsachen sowie Rechtsmeinungen unabhängig vom Vortrag der Parteien zu; außerdem können sich die Parteien Vorbringen in einem *amicus curiae*-Schriftsatz zu eigen machen.

Wegen der zentralen Bedeutung der in dem Verfahren zu klärenden Rechtsfrage für die Bedeutung des Datenschutzes auf dem Gebiet der Telekommunikation rege ich die Berücksichtigung der folgenden Gesichtspunkte durch das Gericht sowie die Übersendung dieses Schriftstücks an die Parteien an:

Inhaltsübersicht

A. Hintergrund

Zur Bedeutung und zum technischen Hintergrund von IP-Adressen ist zunächst auf folgendes hinzuweisen:

Die Bedeutung der von der Beklagten gespeicherten IP-Adressen gibt es am ehesten wieder, wenn man diese als eine Art Postfachnummer ansieht. Wenn ein Kunde der Beklagten eine Internetverbindung herstellt, dann wird ihm für die Dauer des Nutzungsvorgangs ein „Postfach“ zugewiesen. Diese Zuweisung ist aus technischen Gründen erforderlich, denn wenn der Internetnutzer Daten von anderen Computersystemen anfordert, müssen diese wissen, an wen die Daten gesendet werden sollen. Dazu dient die IP-Adresse.

Daraus ergibt sich zugleich die besondere Gefahr, die mit einer Speicherung von IP-Adressen über das Ende eines Nutzungsvorgangs hinaus verbunden ist. Die Betreiber derjenigen Computersysteme, von denen der Internetnutzer Daten anfordert (insbesondere Anbieter von Diensten im Internet), kennen aus technischen Gründen stets die IP-Adresse des Nutzers. Sie können daher speichern, über welche IP-Adresse welche Daten im einzelnen abgerufen werden.

In der Praxis werden solche „Logfiles“ verbreitet erstellt und gespeichert, z.B. um Statistiken über die Benutzung des Dienstes erstellen zu können. Die Speicherung von Logfiles erlaubt es jedoch auch, nachzuvollziehen, welche Emails

ein Nutzer gelesen oder verschickt hat, mit wem er kommuniziert und welche öffentlich zugänglichen Informationen er gelesen hat (sogenannte WWW-Seiten). Daraus lässt sich ableiten, für welche Themen er sich interessiert, unter Umständen auch, welche politische Meinung er hat, unter welchen Krankheiten er leidet, welcher Religion er zugehört, ob er Gewerkschaftsmitglied ist oder welche sexuellen Vorlieben er hat.

Solange den Betreibern eines Dienstes im Internet nur die IP-Adresse des Nutzers bekannt ist, ist die Gefahr, dass ein Personenbezug hergestellt wird, gering. Speichern Internet-Zugangsanbieter wie die Beklagte aber, welchem Nutzer eine IP-Adresse zu welchem Zeitpunkt zugeordnet war, dann lässt sich ein Personenbezug herstellen und genau nachvollziehen, welche Aktivitäten bestimmte Personen im Internet entfaltet haben.

Im wirklichen Leben ist eine derart lückenlose Überwachung der Bevölkerung unmöglich. Im Internet ist sie technisch ohne Weiteres machbar. Beim Abholen eines Formulars einer Behörde, beim Betreten eines Buchladens oder beim Betrachten eines Schaufensters im „wirklichen Leben“ bleibt man anonym. Es gibt keinen Grund, warum dies im virtuellen Leben anders sein sollte.

Eine Vorratsspeicherung von IP-Adressen, wie sie die Beklagte vornimmt, ist ähnlich zu beurteilen, wie wenn der Bäcker beim Brötchenkauf die Vorlage des Personalausweises fordert, der dann kopiert und registriert wird. Dass in den Telekommunikationsnetzen Straftaten begangen werden, stellt keine Besonderheit dar. Auch auf der Straße oder in Wohnungen geschehen Straftaten, ohne dass dies dort eine Totalüberwachung legitimiert. Niemand muss beim Absenden eines Briefes seinen Personalausweis vorlegen oder in einer öffentlichen Bibliothek registrieren lassen, welche Seite er in welchem Buch aufschlägt. Eine vergleichbar umfassende Kontrolle entsprechender Online-Aktivitäten (E-Mail-Versand, Nutzung des World Wide Web) ist ebenso wenig hinnehmbar[1].

Dass die Herstellung von Persönlichkeitsprofilen verboten sein und daher in der Praxis nicht oft vorkommen mag, mag sein. Bei Entscheidungen über die Zulässigkeit der Speicherung personenbezogener Daten zu berücksichtigen sind aber schon solche Gefahren und Nachteile, die der Einzelne nicht ohne Grund befürchtet[2]. Schon die Flugdatenaffäre um deutsche Abgeordnete zeigte, dass es allen Vertraulichkeitsvorschriften zum Trotz zur Offenlegung personenbezo-

---

[1] DSB-Konferenz, Datenschutzbeauftragte des Bundes und der Länder: Entschließung zur systematischen verdachtslosen Datenspeicherung in der Telekommunikation und im Internet der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25.10.2002, BT-Drs. 15/888, 199.
[2] BVerfGE 100, 313 (376).

gener Daten mit schwerwiegenden Folgen kommen kann. Den einzig wirksamen Schutz hiergegen stellt es dar, wenn Daten erst gar nicht gespeichert oder frühestmöglich gelöscht werden (so auch § 3a BDSG, Grundsatz der Datensparsamkeit).

B. Rechtliche Bewertung

Internet-Zugangsanbieter wie die Beklagte dürfen die jeweils dynamisch zugewiesene IP-Adresse während der Dauer eines Nutzungsvorgangs speichern, weil dies technisch erforderlich ist, um die Internetnutzung zu ermöglichen. Ihre Speicherung über das Ende des Nutzungsvorgangs hinaus ist jedoch unzulässig. Dies ergibt sich ohne weiteres aus dem Gesetz.

Rechtlich umstritten ist, ob sich die Zulässigkeit der Speicherung von Daten über die Nutzung von Internetzugängen nach dem Teledienstdatenschutzgesetz (TDDSG) oder dem Telekommunikationsgesetz (TKG) richtet. Diese Frage kann vorliegend jedoch offen bleiben, weil die Speicherung der genannten Daten mit keinem der beiden Gesetze vereinbar ist.

I. Rechtslage nach dem TDDSG

Da für Internet-Zugangsanbieter wie die Beklagte überwiegend von einer Anwendbarkeit des TDDSG ausgegangen wird[3] und auch der Wortlaut des § 2 Nr. 3 TDG[4] für eine Anwendung des TDDSG spricht, wird die Rechtslage bei Anwendung dieses Gesetzes zuerst dargestellt.

§ 6 Abs. 1 S. 1 TDDSG bestimmt, dass der Diensteanbieter personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben, verarbeiten oder nutzen darf, soweit dies erforderlich ist, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen (Nutzungsdaten). Nach § 6 Abs. 4 TDDSG darf der Diensteanbieter Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus nur verarbeiten (also auch speichern, vgl. § 3 Abs. 4 BDSG) und nutzen, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind.

---

[3] Davon geht etwa der Bundesbeauftragte für Datenschutz (siehe 18. Tätigkeitsbericht, Kapitel 11, Punkt 8) und die zuständigen Stellen der Länder aus. Ebenso die Bundesregierung in BT-Drs. 14/1191, 7 f. Auch die Beklagte geht hiervon aus.

[4] „Teledienste im Sinne von Absatz 1 sind insbesondere [...] Angebote zur Nutzung des Internets“.

IP-Adressen sind Nutzungsdaten im Sinne des TDDSG[5], weil es sich um personenbezogene Daten eines Nutzers handelt. Sie geben Auskunft darüber, welche IP-Adresse einem Nutzer zugewiesen war.

1. Erforderlichkeit der Speicherung zur Abrechnung?

Nach § 6 Abs. 4 TDDSG darf der Diensteanbieter Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus nur verarbeiten (also auch speichern, vgl. § 3 Abs. 4 BDSG) und nutzen, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind.

Da die Höhe der Nutzungsentgelte in keinem Tarif des Beklagten von der zugewiesenen IP-Adresse abhängt[6], ist die Speicherung dieser Daten nicht erforderlich, um den jeweiligen Dienst mit dem Nutzer abzurechnen[7]. Dies hat die Beklagte außerprozessual auch nicht bestritten[8]. Ist als Nutzungsentgelt eine Pauschale vereinbart, so genügt bereits der bloße Zeitablauf zur Abrechnung. Richtet sich die Höhe der Nutzungsentgelte dagegen nach der Nutzungszeit, so genügt es zur Abrechnung, wenn die Beklagte speichert, wie lange ein Nutzer den Dienst während eines Abrechnungszeitraums insgesamt in Anspruch genommen hat[9]. Die Nutzungszeit wird dann mit dem Minutenpreis multipliziert und dem Nutzer in Rechnung gestellt. Eine Speicherung von IP-Adressen ist nicht erforderlich.

2. Erforderlichkeit für Nachweiszwecke?

Die Beklagte hat außerprozessual die Auffassung vertreten (Anlage) dass es nicht darauf ankomme, ob die Daten tatsächlich für die Abrechnung verwendet würden; es reiche aus, wenn sie der Durchsetzbarkeit des Entgeltanspruchs in Zweifelsfällen dienten. Dieser Auffassung steht der klare Wortlaut des § 6 Abs. 4 TDDSG entgegen, mit dem der Gesetzgeber eindeutig zum Ausdruck gebracht hat, dass nur die zur Abrechnung unerlässlichen Daten gespeichert wer-

---

[5] Bundesregierung in BT-Drs. 14/1191, 15.

[6] Für dynamisch vergebene IP-Adressen vgl. nur Schmitz in Hoeren/Sieber, Handbuch Multimediarecht, 16.4, Rn. 96.

[7] Schmitz, MMR 2003, 214 (216).

[8] Auch das Regierungspräsidium Darmstadt, MMR 2003, 213 (213) lässt es ausdrücklich offen, „ob man diese Speicherung der IP-Adresse [...] unter dem Aspekt der ‚Erforderlichkeit für Abrechnungszwecke' i.S.d. § 6 Abs. 4 TDDSG einordnen kann"; es stützt seine Auffassung vielmehr alleine auf § 9 BDSG.

[9] Schmitz in Hoeren/Sieber, Handbuch Multimediarecht, 16.4, Rn. 128: nur die jeweilige aggregierte Gesamtnutzungszeit darf gespeichert werden. Die Speicherung auch der einzelnen Einwahlzeiten lassen zu Dix/Schaar in: Roßnagel, Recht der Multimedia-Dienste, § 3 TDDSG, Rn. 119; Roßnagel, Handbuch Datenschutzrecht, 7.9, Rn. 79.

den sollen. Dies beruht auf der hohen Sensibilität von Teledienst-Nutzungsdaten[10], die auch der Gesetzgeber erkannt hat. Dementsprechend wird die Auffassung der Beklagten auch in der Literatur an keiner Stelle geteilt.

Schon die Sensibilität von Telekommunikationsverkehrsdaten nach dem TKG hat der Gesetzgeber erkannt und deswegen angeordnet, dass nur die entgeltrelevanten Verkehrsdaten gespeichert werden dürfen (§ 94 Abs. 2 S. 2 TKG). Der Gesetzgeber des TDDSG war eindeutig der Auffassung, dass Teledienst-Nutzungsdaten sensibler sind als Telekommunikationsverkehrsdaten, weil sie eine Vielzahl von Rückschlüssen auf das Kommunikationsverhalten der Nutzer ermöglichen. Schon aus dem Vergleich mit dem TKG ergibt sich daher, dass im Anwendungsbereich des TDDSG keine weiter gehenden Speicherungsrechte bestehen können.

Auch aus § 4 Abs. 6 TDDSG ergibt sich, dass Diensteanbieter dem Nutzer die Inanspruchnahme von Telediensten insoweit anonym zu ermöglichen haben, wie es ihnen technisch möglich und zumutbar ist. Der Beklagten ist es ohne weiteres möglich und zumutbar, ihre Dienste ohne Speicherung anderer Daten als der Nutzungsdauer anzubieten. Dass dem so ist, zeigt die Vielzahl von Internet-Zugangsanbietern, die dies so handhaben, etwa Arcor, QSC, T-Link[11] und Titan[12].

Die Speicherung von Nutzungsdaten kann daher nicht damit rechtfertigt werden, dass die Nutzung des Dienstes im Streitfall mit den gespeicherten Daten plausibel gemacht oder nachgewiesen werden kann. Mit diesem Argument wäre auch etwa die Speicherung der einzelnen Internetseiten, die der Nutzer aufruft, zulässig. Auch damit könnte nämlich im Einzelfall nachgewiesen werden, dass ein Nutzer den Dienst benutzt hat (z.B. wenn er die gleichen Internetseiten aufgerufen hat wie sonst auch). Selbst eine Speicherung von Inhaltsdaten könnte mit diesem Argument gerechtfertigt werden. Telefonunternehmen dürften dann also beispielsweise alle Telefongespräche aufnehmen, um anhand der Stimme nachweisen zu können, wer ihre Dienste in Anspruch genommen hat. Die bloße Eignung eines Datums zu Beweiszwecken kann dessen Speicherung jedoch noch nicht legitimieren. Ansonsten wäre praktisch das gesamte Datenschutzrecht sinnlos, weil sich bei keinem Datum ausschließen lässt, dass es einmal zu Beweiszwecken benötigt werden könnte.

Das weitgehende Verbot der Datenspeicherung durch den Gesetzgeber ist den Diensteanbietern auch zumutbar. Wenn sie ihre Forderung gegen den Kunden einklagen, trifft sie nämlich keine Beweislast bezüglich der Daten, die sie we-

---

[10] Siehe Seiten 2-4 oben.
[11] c't 19/2002, 124 (125).
[12] Siehe http://www.titan-dsl.de/highlight.htm.

gen des TDDSG nicht erfassen durften oder löschen mussten[13]. Dies ergibt sich aus einer analogen Anwendung des § 16 Abs. 2 der Telekommunikations-Kundenschutzverordnung (TKV), der für Telekommunikationsdienste bestimmt: „Soweit [...] gespeicherte Verbindungsdaten [...] auf Grund rechtlicher Verpflichtung gelöscht wurden, trifft den Anbieter keine Nachweispflicht für die Einzelverbindungen, wenn der Kunde in der Rechnung auf die nach den gesetzlichen Bestimmungen geltenden Fristen für die Löschung gespeicherter Verbindungsdaten in drucktechnisch deutlich gestalteter Form hingewiesen wurde."

Bestreitet ein Kunde der Beklagten, dass ihre Forderung berechtigt sei, so braucht die Beklagte die dem Kunden zugewiesenen IP-Adressen nicht vorzulegen. Sie muss lediglich nachweisen, dass sie einen Vertrag mit dem Kunden geschlossen hat und dass sie dem Kunden eine Kennung (sogenannte T-Online-Nummer) und eine Geheimzahl (sogenanntes Passwort) zugeteilt hat. Handelt es sich um einen zeitabhängig abgerechneten Tarif, so muss die Beklagte weiterhin beweisen, dass ihr Abrechnungssystem ordnungsgemäß funktioniert, dass es zu Lasten der Kunden also nur diejenigen Nutzungsvorgänge abrechnet, die unter Verwendung der jeweils zugeteilten Kennung und Geheimzahl stattgefunden haben (technische Prüfung, vgl. § 16 Abs. 3 TKV). Erbringt die Beklagte diese Nachweise, was sie ohne die streitgegenständlichen Daten kann, dann spricht zumindest der Beweis des ersten Anscheins für die Richtigkeit ihrer Entgeltforderung[14]. Wenn der Kunde geltend macht, seine Kennung und Geheimzahl seien in von ihm nicht zu vertretendem Umfang genutzt worden, so trägt er die volle Beweislast[15] (§ 16 Abs. 3 S. 3 Var. 1 TKV analog). Das gleiche gilt, wenn der Kunde Manipulationen Dritter behauptet (§ 16 Abs. 3 S. 3 Var. 2 TKV analog).

Nur in einer verschwindend geringen Zahl von Fällen (vermutlich bei weit unter 0,1% der Forderungen) kommt es überhaupt zu Streitigkeiten über Entgeltforderungen. Selbst wenn die Beklagte wegen der beschriebenen Rechtslage in ein oder zwei Fällen pro Jahr nicht in der Lage sein sollte, eine berechtigte Forderung zu realisieren, dann ist ihr das zumutbar, weil sie diesen Ausfall ohne Weiteres auf den Preis umlegen kann. Die Entscheidung des Gesetzgebers bezüglich der Risikozuweisung ist zu respektieren.

Auch den Kunden ist die beschriebene Beweislastverteilung zuzumuten. Sie haben es in der Hand, ihre Kennung und ihr Passwort geheim zu halten. Nach den AGB der Beklagten (Ziff. 6.1.3) sind sie hierzu sogar verpflichtet. Sie können Dritte von der unberechtigten Nutzung ihres Computers ausschließen. An-

---

[13] Schmitz in Hoeren/Sieber, Handbuch Multimediarecht, 16.4, Rn. 97.
[14] St. Rspr., vgl. nur OLG Koblenz, NJW-RR 2000, 930; OLG Stuttgart, ZIP 1999, 1217.
[15] LG Mainz, CR 2003, 589 (590).

sonsten können sie sich durch eine technische Prüfung der Anlagen der Beklagten versichern, dass diese korrekt abrechnen.

Wie sich aus § 6 Abs. 6-7 TDDSG ergibt, können die Kunden nicht im Nachhinein die Vorlage eines Einzelnachweises verlangen[16]. § 6 Abs. 6-7 TDDSG regeln abschließend, in welchem Fall Nutzungsdaten „verarbeitet" (also auch gespeichert, vgl. § 3 Abs. 4 BDSG) werden dürfen, bis etwa erhobene „Einwendungen abschließend geklärt sind oder die Entgeltforderung beglichen ist", nämlich nur „auf Verlangen des Nutzers". Verlangt der Nutzer keinen Einzelnachweis, was seiner freien Entscheidung obliegt, so gehen eventuell entstehende Beweisschwierigkeiten in Zweifelsfällen zu seinen Lasten. Diese Regelung ist sachgerecht und entspricht der sonstigen Beweislastverteilung im Wirtschaftsleben für automatisierte Vorgänge (z.B. müssen Kunden beim Kauf von Waren regelmäßig einen Kassenzettel verlangen und aufbewahren, um Gewährleistungsansprüche durchsetzen zu können).

Die Beklagte benötigt die streitgegenständlichen Daten auch nicht zur Abrechnung kostenpflichtiger Inhalte. Diese Abrechnung lässt sich ohne Weiteres über die vergebene Benutzerkennung und das Kennwort vornehmen. Dies ergibt sich schon aus der eigenen Aussage der Beklagten: „Wenn Sie bei T-Online kostenpflichtige Leistungen, z.B. Premium Content, beziehen, speichern wir die Informationen über den Inhalt der kostenpflichtigen Leistung und den Zeitpunkt der Lieferung als Abrechnungsdatum maximal 80 Tage nach Rechnungsversand."[17] An dieser Aussage wird deutlich, dass die Beklagte IP-Adressen gerade nicht speichern muss, um kostenpflichtige Dienste abzurechnen. Dies gilt erst recht, wenn ein Nutzer kostenpflichtige Dienste gar nicht in Anspruch nimmt.

Aufzeichnungen über die vergebenen IP-Adressen benötigt die Beklagte somit weder zur Abrechnung noch zur Durchsetzung ihrer Forderungen; IP-Adressen sind nicht „für Zwecke der Abrechnung mit dem Nutzer erforderlich" (§ 6 Abs. 4 TDDSG).

> Für den Fall, dass das Gericht trotz allem die Speicherung von Nutzungsdaten zu Nachweiszwecken für gesetzmäßig erachtet, ist auf folgendes hinzuweisen: Kunden können der Beklagten gegenüber ausdrücklich oder konkludent erklären, dass sie bei Streitigkeiten über das zu entrichtende Entgelt auf den Nachweis von Nutzungsdaten verzichten. Damit erklären sie sich einverstanden, dass die Beklagte im Streitfall auch ohne Speicherung der zugewiesenen IP-Adressen so behandelt wird, wie wenn sie diese Daten vorlegen würde. Eine entsprechende Beweislastvereinbarung ist zulässig und wirk-

---

[16] Vgl. Schmitz in Hoeren/Sieber, Handbuch Multimediarecht, 16.4, Rn. 97.
[17] Siehe http://www2.service.t-online.de/dyn/c/07/62/62/762620.html.

sam. Damit ist die Speicherung von IP-Adressen zumindest solcher Kunden keinesfalls mehr zu Nachweiszwecken erforderlich[18].

Für den Fall, dass das Gericht auch diesen Aspekt nicht für durchgreifend erachtet, wird auf folgendes hingewiesen:

Die streitgegenständlichen Daten sind zum Nachweis der Berechtigung oder der Nichtberechtigung der Entgeltforderungen der Beklagten nicht geeignet. Unabhängig davon, welche IP-Adresse zugewiesen wurde, kann eine Forderung der Beklagten gleichermaßen berechtigt oder unberechtigt sein. Die IP-Adresse sagt über die Berechtigung von Forderungen der Beklagten nichts aus.

Soweit sich die Beklagte auf die Möglichkeit einer Fehlfunktion ihrer Anlagen beruft, so sagen die genannten Daten darüber nichts aus[19]. Dass dem Kunden eine IP-Adresse zugewiesen wurde, schließt Fehlfunktionen bei der Bereitstellung des Dienstes der Beklagten weder aus noch macht es dies weniger wahrscheinlich. So mag das System der Beklagten durchaus die Vergabe einer IP-Adresse registrieren, aber dennoch keine Daten aus dem Internet übertragen. Umgekehrt kann das System der Beklagten keine Vergabe einer IP-Adresse registrieren, dies aber dennoch ordnungsgemäß tun.

Zur Aufdeckung von Fehlfunktionen ist statt der flächendeckenden Aufzeichnung personenbezogener Daten eine regelmäßige Überprüfung der Anlagen der Beklagten erforderlich. Im Streitfall kann eine Überprüfung durch einen Sachverständigen erfolgen. Es ist zudem praktisch ausgeschlossen, dass ein Fehler der Anlagen nur in einem einzelnen Fall auftritt. Wäre die Anlage fehlerhaft, würden sich die Kundenbeschwerden häufen, was im Streitfall als Indiz für einen Anlagenfehler gelten könnte.

Soweit die Beklagte geltend macht, eine Entgeltforderung könne darauf beruhen, dass ein Dritter die Kennung und das Passwort eines Nutzers missbraucht habe, ist zu beachten, dass die Beklagte diesbezüglich keine

---

[18] Vgl. auch § 16 Abs. 2 TKV: „Soweit [...] auf Wunsch des Kunden keine Verbindungsdaten gespeichert oder gespeicherte Verbindungsdaten auf Wunsch des Kunden [...] gelöscht wurden, trifft den Anbieter keine Nachweispflicht für die Einzelverbindungen, wenn der Kunde in der Rechnung auf die nach den gesetzlichen Bestimmungen geltenden Fristen für die Löschung gespeicherter Verbindungsdaten in drucktechnisch deutlich gestalteter Form hingewiesen wurde."

[19] Vgl. nur Wüstenberg, TKMR 2003, 105 (109); Schmitz, MMR 2003, 214 (216); irrig und ohne Begründung a.A. Regierungspräsidium Darmstadt, MMR 2003, 213 (213).

Beweislast trifft[20]. Es wird in solchen Fällen vermutet, dass der Kunde die fremde Nutzung zu vertreten und die Forderung daher zu begleichen hat. IP-Adressen sagen nichts darüber aus, ob der Kunde die Nutzung zu vertreten hat oder nicht[21]. Dies beantwortet auch die Frage, welche die Beklagte aufwirft, wenn sie geltend macht, die Kennung und das Passwort eines Nutzers könnten von mehreren Anschlüssen zugleich genutzt werden, was ein Hinweis auf eine unberechtigte Nutzung sein könnte. Auch hier sagt eine Speicherung der streitgegenständlichen Daten nichts darüber aus, ob die zeitgleiche Nutzung tatsächlich unberechtigt ist oder nicht mit Einwilligung des Kunden erfolgte. Im Übrigen kann die Beklagte eine zeitgleiche Nutzung schon an der gleichzeitig verwendeten Kennung und dem Passwort eines Nutzers feststellen. Die streitgegenständlichen Daten helfen ihr hierbei nicht.

Die Beklagte verdient Anerkennung in ihrem vorprozessualen Bemühen, hypothetische Einzelfälle zu konstruieren, in denen etwas anderes gelten könnte. Ihr ist zuzugeben, dass sich nicht ganz ausschließen lässt, dass eine IP-Adresse im Rahmen einer Beweisaufnahme irgendwann einmal die Rolle eines Indizes bezüglich der Berechtigung einer Forderung spielen könnte. Dasselbe gilt aber für alle anderen Nutzungsdaten einschließlich der abgerufenen Inhalte und im Übrigen auch für jegliches sonstige personenbezogene Datum über einen Nutzer. Aus jedem auf seine Person bezogenen Datum können sich im Einzelfall einmal Schlüsse bezüglich der Berechtigung einer Forderung der Beklagten ihm gegenüber ergeben. Das gesamte Datenschutzrecht beruht indes auf dem Gedanken, dass nicht bereits die bloße Möglichkeit, dass ein Datum irgendwann in der Zukunft einmal gebraucht werden könnte, dessen Speicherung rechtfertigt, weil ansonsten sämtliche personenbezogene Daten unbegrenzt auf Vorrat gespeichert werden dürften. Dies aber wäre eine unverhältnismäßige und unangemessene Beeinträchtigung des Persönlichkeitsrechts des Betroffenen, dem aus der Aufbewahrung personenbezogener Daten schwere Nachteile entstehen können[22]. Wegen der bloßen entfernten Möglichkeit einer Indizeignung der streitgegenständlichen Daten ist deren Aufbewahrung daher nicht gerechtfertigt[23].

Für den Fall, dass das Gericht auch diesen Umstand nicht für durchgreifend erachtet, wird darauf hingewiesen, dass die Berechtigung von Entgeltforderungen jedenfalls nicht die Speicherung der zugewiesenen

---

[20] Siehe Seite 7 oben.
[21] Vgl. nur Wüstenberg, TKMR 2003, 105 (109).
[22] Siehe Seiten 2-4 oben.
[23] Ebenso Schmitz, MMR 2003, 214 (216).

IP-Adresse selbst erforderlich macht. Ebenso potenziell beweisgeeignet ist die Speicherung der Tatsache, ob überhaupt eine IP-Adresse vergeben wurde. Die Speicherung des Datums, welche IP-Adresse im einzelnen zugewiesen wurde, ist dagegen nicht erforderlich.

Ließe man selbst dies nicht genügen, so käme jedenfalls eine Verkürzung der IP-Adressen um einige Stellen in Betracht (vgl. § 97 Abs. 4 S. 1 Nr. 1 TKG).

Schließlich wird darauf hingewiesen, dass die Beklagte die an einen Kunden vergebenen IP-Adressen selbst für solche Zeiträume speichert, für die dieser das in Rechnung gestellte Nutzungsentgelt vorbehaltlos beglichen hat. Wenn ein Kunde nach Begleichen einer Rechnung Entgelte nach § 812 BGB zurück fordern würde, würde er in jedem Fall die Beweislast für das Fehlen eines rechtlichen Grundes, also für die Nichtberechtigung der Forderung der Beklagten, tragen. Die Speicherung von Nutzungsdaten nach Begleichen einer Rechnung ist daher in keinem Fall gerechtfertigt. Genau dies tut die Beklagte aber, und zwar ohne dass eine zeitliche Grenze erkennbar ist.

3. Erforderlichkeit zur Missbrauchsbekämpfung?

Mit § 6 Abs. 8 TDDSG wurde eine abschließende Regelung über die Datenspeicherung zur Missbrauchsbekämpfung getroffen[24]. Würde man daneben noch die allgemeinen Regelungen anwenden, wäre die Vorschrift überflüssig. Aus § 6 Abs. 8 TDDSG ergibt sich, dass Leistungserschleichungen nur in Fällen eines konkreten Missbrauchsverdachts eine Datenspeicherung rechtfertigen können, keinesfalls generell[25]. Selbst wenn ein konkreter Verdacht vorliegt, dürfen nur die Daten von konkret Verdächtigen gespeichert werden, nicht die Daten aller Kunden.

Aus § 6 Abs. 8 TDDSG ergibt sich auch, dass die Möglichkeit der missbräuchlichen Inanspruchnahme eines Teledienstes zur Begehung von Straftaten usw. nicht genügt, um eine allgemeine Vorratsdatenspeicherung zu rechtfertigen. Die Norm lässt eine Datenspeicherung nur in Fällen von Leistungserschleichung zu. Was der Kunde mit ordnungsgemäß bezahlten Leistungen anfängt, geht die Beklagte ebensowenig an wie der Verkäufer einer gefährlichen Sache kontrollieren darf, was der Käufer damit anfängt. Dies ist auch sachgerecht, weil die

---

[24] Schaar, Datenschutz im Internet, Rn. 460 f.: kein Rückgriff auf § 9 BDSG.

[25] Schaar, Datenschutz im Internet, Rn. 460; Roßnagel, Handbuch Datenschutzrecht, 7.9, Rn. 82.

Beklagte von der Haftung für Handlungen ihrer Kunden gesetzlich freigestellt ist (§ 9 TDG).

Auch aus § 6 Abs. 5 S. 5 TDDSG[26] ergibt sich, dass für Zwecke der Strafverfolgung nur Auskunft über ohnehin gespeicherte Daten erteilt werden darf. Die generelle Speicherung von Nutzungsdaten alleine zur Erleichterung der Bekämpfung möglicher Missbrauchsfälle ist unzulässig.

Ob die dynamisch zugewiesene IP-Adresse ein Pseudonym darstellt, wie die Beklagte behauptet, kann offen bleiben, weil auch dies keine zusätzliche Datenspeicherung nach Ende des Nutzungsvorgangs rechtfertigen würde. Ein zusätzlicher Erlaubnistatbestand für die Speicherung von Pseudonymen ist nicht vorhanden. Nach § 3 Abs. 6a BDSG ist Pseudonymisieren ohnehin „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren“. Die Speicherung der streitgegenständlichen Daten erfolgt aber gerade zu dem Zweck, die Bestimmung des Betroffenen zu ermöglichen, nicht, um sie zu erschweren. Es wäre daher geradezu eine Verkehrung des Zwecks der Pseudonymisierung, diese zur Rechtfertigung einer Datenspeicherung heranzuziehen.

4. Erforderlichkeit nach § 9 BDSG?

Das Gleiche gilt für die Ansicht der Beklagten, eine Speicherung von Nutzungsdaten sei nach § 9 BDSG geboten, und zwar in Verbindung mit den Nrn. 3 und 5 der Anlage zu dieser Vorschrift. § 9 BDSG dient dem Zweck, die bei einer Stelle gespeicherten personenbezogenen Daten vor unberechtigten Zugriffen zu schützen, um die Betroffenen vor Nachteilen zu schützen. Man würde diesen Zweck in sein genaues Gegenteil verkehren, wenn man aus § 9 BDSG die Befugnis zur Speicherung weiterer personenbezogener Daten über die Kunden der Beklagten ableiten würde. Eine solche Mehrspeicherung würde nämlich noch weitere Daten über den Betroffenen der Gefahr missbräuchlicher Zugriffe aussetzen[27]. Gerade aus diesem Grund ist das Datenschutzrecht vom Grundsatz der Datensparsamkeit (§ 3a BDSG, § 4 Abs. 6 TDDSG) geprägt. Den besten Schutz vor missbräuchlichen Zugriffen auf persönliche Daten stellt es dar, wenn diese Daten erst gar nicht gespeichert werden. In diesem Fall ist es nämlich überflüssig, Vorkehrungen zu ihrem Schutz zu treffen, wie es die Beklagte vorgeblich beabsichtigt.

---

[26] „Nach Maßgabe der hierfür geltenden Bestimmungen darf der Diensteanbieter Auskunft an Strafverfolgungsbehörden und Gerichte für Zwecke der Strafverfolgung erteilen.“

[27] Siehe Seiten 2-4 oben.

Die Auffassung der Beklagten, § 9 BDSG gebiete die Speicherung der streitgegenständlichen Daten, ist schon deswegen unzutreffend, weil § 9 BDSG keine Ermächtigungsgrundlage für die Erhebung oder Speicherung von Teledienst-Nutzungsdaten darstellt. Nutzungsdaten dürfen nämlich nach § 6 Abs. 1 S. 1 TDDSG nur erhoben, verarbeitet oder genutzt werden, „soweit dies erforderlich ist, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen". Gegenüber dem BDSG handelt es sich dabei um eine abschließende Spezialregelung[28]. Dementsprechend führt die Begründung der TDDSG-Novelle von 2001 aus[29]: „Die jeweils geltenden Vorschriften für den Schutz personenbezogener Daten – insbesondere das BDSG – finden Anwendung, soweit das TDDSG nichts anderes bestimmt. Spezialregelungen des TDDSG sind die besonderen Grundsätze, Pflichten und Erlaubnistatbestände für Anbieter von Telediensten. Aus dem Verhältnis der Spezialität zwischen BDSG und TDDSG folgt, dass die Erlaubnistatbestände des TDDSG abschließend sind. Dienstean-bieter können sich demzufolge nicht auf allgemeine Erlaubnistatbestände des BDSG (z. B. § 28) berufen, wenn die Voraussetzungen für eine gesetzliche Erlaubnis hinsichtlich des Umgangs mit personenbezogenen Daten der Nutzer nach dem TDDSG nicht gegeben sind." Der Wille des Gesetzgebers ist eindeutig.

Hinzu kommt folgendes: In der Anlage zu § 9 BDSG ist eindeutig festgelegt, dass die Vorschrift nur Maßnahmen mit dem Ziel vorschreibt, „die innerbehördliche oder innerbetriebliche Organisation [datenschutzgerecht] zu gestalten" (S. 1 der Anlage zu § 9 BDSG). Wenn eine Stelle Daten über ihre Kunden speichert, dann handelt es sich um keine Maßnahme der „innerbetrieblichen Organisation", so dass die Anlage zu § 9 BDSG zur Speicherung von Kundendaten nicht ermächtigt.

Im Übrigen gilt Nr. 3 des Anlage zu § 9 BDSG ausdrücklich nur für „die zur Benutzung eines Datenverarbeitungssystems Berechtigten". Kunden der Beklagten haben keine Zugriffsberechtigung für das Datenverarbeitungssystem der Beklagten. Dies steht auch einer Anwendung der Nr. 5 entgegen. Die hypothetische Zugriffsmöglichkeit etwa von Hackern kann keine pauschale Datensammlung seitens der Beklagten rechtfertigen, zumal ein unbefugtes Eindringen durch Kunden der Beklagten nicht wahrscheinlicher ist als ein Eindringen durch Personen, die andere Internetzugänge verwenden und deren Daten die Beklagte folglich nicht speichern kann. Dass Kunden der Beklagten unbefugt auf bei der Beklagten gespeicherte personenbezogene Daten zugreifen könn-

---

[28] Engel-Flechsig in: Beck'scher IuKDG-Kommentar, § 6 TDDSG, Rn. 1; Schmitz, MMR 2003, 214 (216).

[29] BT-Drs. 14/6098, 14.

ten, ist ohnehin ganz regelmäßig schon aus technischen Gründen ausgeschlossen.

Was die Möglichkeit angeht, dass Kunden der Beklagten den Internetzugang nutzen könnten, um unbefugt auf bei anderen Stellen gespeicherte personenbezogene Daten zuzugreifen, ist folgendes festzustellen: Jede verantwortliche Stelle ist nur für diejenigen Daten verantwortlich, die sie selbst verarbeitet. Keine Stelle darf oder muss dafür Vorsorge treffen, dass ihre Mitarbeiter oder gar Kunden unbefugt auf persönliche Daten zugreifen, für deren Sicherheit eine andere Stelle verantwortlich ist. Dies ergibt sich daraus, dass § 9 BDSG und die Anlage dazu nur für Stellen gilt, die Daten verarbeiten. Diese Anknüpfung bedeutet, dass die Vorschrift ausschließlich auf den Schutz derjenigen Daten zielt, die eine Stelle selbst verarbeitet oder nutzt. Wenn eine allgemeine Überwachungspflicht zur Verhinderung des Missbrauchs personenbezogener Daten gewollt wäre, dann würde es keinen Sinn machen, solche Unternehmen von ihr auszunehmen, die selbst keine Daten verarbeiten.

Die entgegengesetzte Ansicht des Beklagten in Bezug auf § 9 BDSG führt zu absurden Ergebnissen: Jede datenverarbeitende Stelle wäre jederzeit und zeitlich unbegrenzt verpflichtet, alle verfügbaren personenbezogenen Daten über ihre Kunden zu erheben und vorzuhalten, nur weil der Zugriff auf die Daten vielleicht irgendwann einmal erforderlich sein könnte, um einen unbefugten Datenzugriff durch die Kunden nachvollziehen zu können. Nach dieser Auslegung des § 9 BDSG müssten sämtliche Kundendaten erfasst und aufbewahrt werden. Die Fluggesellschaften müssten z.B. ihre Business-Class-Sitze überwachen für den Fall, dass ein Passagier unbefugt in die Geschäftsunterlagen seines Nachbarn sieht. Mit dieser Auslegung könnte man praktisch das gesamte Datenschutzrecht ad acta legen[30]. Auch die Beklagte will wohl nicht ernsthaft behaupten, dass Internet-Zugangsanbieter zu einer Speicherung von IP-Adressen verpflichtet seien, wie es aus einer Anwendung des § 9 BDSG folgen würde. Es geht in der datenschutzrechtlichen Diskussion doch stets nur um ein Recht von Internet-Zugangsanbietern zur Speicherung dieser Daten. Ein solches Recht lässt sich aus § 9 BDSG schon deswegen nicht herleiten, weil diese Norm verantwortliche Stellen zu angemessenen Vorkehrungen verpflichtet und nicht nur berechtigt.

5. Ergebnis

§ 3 Abs. 1 TDDSG bestimmt: „Personenbezogene Daten dürfen vom Diensteanbieter zur Durchführung von Telediensten nur erhoben, verarbeitet und ge-

---

[30] So auch Schmitz, MMR 2003, 214 (216): „Die Begründung des RegPräs i.R.d. § 9 BDSG [...] würde § 9 BDSG zu einer Art ‚Generalerlaubnis' der Datenverarbeitung machen."

nutzt werden, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.“ Wie gezeigt, besteht für die Speicherung von IP-Adressen durch die Beklagte weder eine gesetzliche Erlaubnis, noch willigen ihre Kunden darin ein. Die Speicherung dieser Daten durch die Beklagte ist damit unzulässig.

II. Rechtslage nach dem TKG

§ 96 Abs. 2 TKG bestimmt, dass gespeicherte Verkehrsdaten über das Ende der Verbindung hinaus nur verarbeitet oder genutzt werden dürfen, soweit sie zum Aufbau weiterer Verbindungen oder für die in den §§ 97, 99, 100 und 101 TKG genannten Zwecke erforderlich sind. Im übrigen sind Verkehrsdaten vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen (§ 96 Abs. 2 S. 2 TKG).

Verkehrsdaten sind nach § 3 Nr. 30 TKG „Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden“. Ordnet man die Vergabe von IP-Adressen als Telekommunikationsdienst ein, so handelt es sich dabei um Verkehrsdaten, denn die jeweils einem Nutzer zugewiesene IP-Adresse wird bei der Bereitstellung des Internetzugangs durch die Beklagte verarbeitet und genutzt. Es handelt sich nicht um Bestandsdaten (§ 3 Nr. 3 TKG), weil Bestandsdaten während des Bestands des Vertragsverhältnisses unveränderlich bleiben, während die zugewiesene IP-Adresse von Verbindung zu Verbindung unterschiedlich ist.

1. Erforderlichkeit der Speicherung zur Abrechnung?

Nach § 95 Abs. 3 TKG hat der Diensteanbieter „nach Beendigung der Verbindung aus den Verkehrsdaten nach § 94 Abs. 1 Nr. 1 bis 3 und 5 unverzüglich die für die Berechnung des Entgelts erforderlichen Daten zu ermitteln. Nicht erforderliche Daten sind unverzüglich zu löschen. Die Verkehrsdaten dürfen – vorbehaltlich des Absatzes 4 Satz 1 Nr. 2 – höchstens sechs Monate nach Versendung der Rechnung gespeichert werden. Hat der Teilnehmer gegen die Höhe der in Rechnung gestellten Verbindungsentgelte vor Ablauf der Frist nach Satz 3 Einwendungen erhoben, dürfen die Verkehrsdaten gespeichert werden, bis die Einwendungen abschließend geklärt sind.“

Dass die streitgegenständlichen Daten für die Berechnung des Entgelts durch die Beklagte irrelevant sind, wurde bereits ausgeführt (siehe Punkt B.I.1, Seite 5).

2. Erforderlichkeit für Nachweiszwecke?

Wenn § 95 Abs. 3 S. 3 TKG bestimmt, dass „die Verkehrsdaten“ zu Beweiszwecken aufbewahrt werden dürften, dann nimmt er auf § 95 Abs. 3 S. 1 TKG Bezug. § 95 Abs. 3 S. 1 TKG spricht von denjenigen Verkehrsdaten, die für die

Berechnung des Entgelts erforderlich sind. Aus diesem Grund erlaubt § 95 Abs. 3 S. 3 TKG nur die Aufbewahrung derjenigen Verkehrsdaten, die für die Berechnung des Entgelts erforderlich sind. Würde man § 95 Abs. 3 S. 3 TKG auch auf diejenigen Verkehrsdaten anwenden, die für die Berechnung des Entgelts nicht erforderlich sind, dann hätte § 95 Abs. 3 S. 2 TKG keine eigenständige Bedeutung mehr und wäre überflüssig. Dies kann der Gesetzgeber nicht gewollt haben.

§ 95 Abs. 3 S. 3 TKG rechtfertigt mithin nur die Aufbewahrung derjenigen Verkehrsdaten, die für die Berechnung des Entgelts erforderlich sind[31]. Da IP-Adressen nicht für die Berechnung des Entgelts erforderlich sind[32], kann § 95 Abs. 3 S. 3 TKG ihre Speicherung nicht rechtfertigen.

Auch aus § 3a BDSG ergibt sich, dass sich Diensteanbieter „an dem Ziel auszurichten [haben], keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen." Der Beklagten ist es ohne weiteres möglich und zumutbar, ihre Dienste ohne Speicherung von IP-Adressen anzubieten. Dass dem so ist, zeigt die Vielzahl von Internet-Zugangsanbietern, die dies so handhaben[33].

Die Speicherung von Verkehrsdaten kann nicht damit rechtfertigt werden, dass die Nutzung des Dienstes im Streitfall mit den gespeicherten Daten plausibel gemacht oder nachgewiesen werden kann. Mit diesem Argument wäre auch etwa die Speicherung der einzelnen Internetseiten, die der Nutzer aufruft, zulässig. Auch damit könnte nämlich im Einzelfall nachgewiesen werden, dass ein Nutzer den Dienst benutzt hat (z.B. wenn er die gleichen Internetseiten besucht hat wie sonst auch). Selbst eine Speicherung von Inhaltsdaten könnte mit diesem Argument gerechtfertigt werden. Telefonunternehmen dürften dann also beispielsweise alle Telefongespräche aufnehmen, um anhand der Stimme nachweisen zu können, wer telefoniert hat. Die bloße Eignung eines Datums zu Beweiszwecken kann dessen Speicherung jedoch noch nicht legitimieren. Ansonsten wäre praktisch das gesamte Datenschutzrecht sinnlos.

Das in § 95 Abs. 3 TKG festgelegte Verbot der Speicherung nicht zur Abrechnung erforderlicher Daten ist für die Beteiligten auch sachgerecht. Insoweit gilt die oben (Punkt B.I.2, Seite 5 ff.) skizzierte Beweislastverteilung, die bei Anwendung des TKG unmittelbar aus der TKV folgt. Auch im Übrigen gelten die unter Punkt B.I.2 gemachten Ausführungen sinngemäß, wenn man das TKG anwendet.

---

[31] BeckTKG-Büchner, § 6 TDSV Anh. § 89, Rn. 2.
[32] Siehe Seite 5 oben.
[33] Siehe Seite 6 oben.

3. Erforderlichkeit zur Erstellung eines Einzelverbindungsnachweises?

Die Aufbewahrung der streitgegenständlichen Daten durch die Beklagte ist auch nicht zur Erstellung von Einzelverbindungsnachweisen erforderlich. § 99 TKG ermächtigt zur Speicherung von Verkehrsdaten für diesen Zweck nur dann, wenn der Kunde „vor dem maßgeblichen Abrechnungszeitraum schriftlich eine aufgeschlüsselte Rechnung verlangt hat (Einzelverbindungsnachweis)." Dies tun Nutzer der Beklagten jedoch nicht.

4. Erforderlichkeit zur Störungs- und Missbrauchsbekämpfung?

Mit § 100 TKG wurde eine abschließende Regelung über die Datenspeicherung zur Störungs- und Missbrauchsbekämpfung getroffen. Würde man daneben noch die allgemeinen Regelungen anwenden, wäre die Vorschrift überflüssig.

Zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen der Beklagten (§ 100 Abs. 1 TKG) ist die Speicherung von IP-Adressen nicht geeignet. Allenfalls, wenn im Einzelfall Anhaltspunkte für eine Störung diesbezüglich vorliegen, kommt die probeweise Speicherung einzelner IP-Adressen in Betracht. Aber auch in diesem Fall ist keine personenbezogene Speicherung erforderlich, schon gar nicht die personenbezogene Speicherung aller IP-Adressen, die an Kunden der Beklagten vergeben werden.

Was die Speicherung zur Missbrauchsbekämpfung angeht, so bestimmt § 100 Abs. 3 TKG ausdrücklich, dass die Speicherung von Verkehrsdaten zu diesem Zweck nur „bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte" zulässig ist, keinesfalls generell. Ansonsten wären auch die differenzierten Löschungsregelungen in § 97 TKG überflüssig. Dementsprechend weisen die Datenschutzbeauftragten des Bundes und der Länder auf folgendes hin: „Das grundgesetzlich garantierte Fernmeldegeheimnis lässt eine Speicherung von Daten über die Nutzung öffentlicher Telekommunikationsnetze (insbesondere auch des Internets) außer für betriebliche Zwecke nur zu, wenn ein konkreter Verdacht für eine Straftat von erheblicher Bedeutung besteht."[34]

Aus den §§ 112, 113 TKG und den §§ 100g, 100h StPO ergibt sich im Übrigen, dass auch für Zwecke der Strafverfolgung nur im Einzelfall Auskunft über gespeicherte Daten erteilt oder Verkehrsdaten erhoben werden dürfen. Die generelle Speicherung von Nutzungsdaten allein zur Erleichterung der Bekämpfung möglicher Missbrauchsfälle ist unzulässig.

---

[34] Erklärung der Datenschutzbeauftragten des Bundes und der Länder vom 25. Juni 2004, http://www.lda.brandenburg.de/sixcms/detail.php?id=161413&template=aktuell_d1.

5. Erforderlichkeit nach §§ 96 oder 101 TKG?

Die Speicherung der streitgegenständlichen Daten ist auch nicht zum Aufbau weiterer Verbindungen erforderlich (§ 96 Abs. 2 TKG). Ebensowenig liegt ein Fall des § 101 TKG vor, in dem ein Verfahren zur Bekämpfung bedrohender oder belästigender Anrufe geregelt ist.

6. Erforderlichkeit nach § 9 BDSG?

Auch auf der Basis des TKG stellt § 9 BDSG keine Ermächtigungsgrundlage für die Erhebung oder Speicherung von Verkehrsdaten dar. Verkehrsdaten dürfen nämlich nach § 96 Abs. 2 S. 1 TKG „über das Ende der Verbindung hinaus nur verwendet“ (also auch gespeichert, vgl. § 3 Abs. 5 und 4 BDSG) „werden, soweit sie zum Aufbau weiterer Verbindungen oder für die in den §§ 97, 99, 100 und 101 genannten Zwecke erforderlich sind.“ Gegenüber dem BDSG handelt es sich dabei um eine abschließende Spezialregelung.

> Für den Fall, dass das Gericht anderer Auffassung ist, wird auf die Ausführungen unter Punkt B.I.4 (Seite 12 ff.) verwiesen, die bei Anwendung des TKG entsprechend gelten.
>
> Da § 109 TKG eine spezielle Ausprägung des § 9 BDSG für Telekommunikationsdienste darstellt, gilt all das zu § 9 BDSG Ausgeführte entsprechend für § 109 TKG. Auch auf § 109 TKG lässt sich die Speicherung der streitgegenständlichen Daten daher nicht stützen.

7. Ergebnis

Verkehrsdaten dürfen nach § 96 Abs. 2 TKG „über das Ende der Verbindung hinaus nur verwendet [also auch gespeichert, vgl. § 3 Abs. 5 und 4 BDSG] werden, soweit sie zum Aufbau weiterer Verbindungen oder für die in den §§ 97, 99, 100 und 101 genannten Zwecke erforderlich sind. Im Übrigen sind Verkehrsdaten vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen.“ Wie gezeigt, fehlt es an einer Erforderlichkeit im Sinne des § 96 Abs. 2 S. 1 TKG. Die Speicherung ist auch weder aufgrund anderer Rechtsvorschriften zulässig, noch haben Kunden der Beklagten darin eingewilligt. Die Speicherung der streitgegenständlichen Daten durch die Beklagte ist damit auch auf Basis des TKG unzulässig.

Wegen der zentralen Bedeutung der in dem Verfahren zu klärenden Rechtsfrage für die Bedeutung des Datenschutzes auf dem Gebiet der Telekommunikation hoffe ich, dass das Gericht die Speicherpraxis der Beklagten für unzulässig erklären und dem Persönlichkeitsrecht der deutschen Internetnutzer in diesem entscheidenden Punkt zur Durchsetzung verhelfen wird.

Mit freundlichen Grüßen,

[redacted]

[redacted]

[redacted]