Gericht:	OLG Frankfurt 13. Zivilsenat
Entscheidungsdatum:	16.06.2010
Aktenzeichen:	13 U 105/07
Dokumenttyp:	Urteil
Quelle:	Juris
Normen:	§ 113a TKG, § 113b TKG

Kein Anspruch gegen den Provider auf sofortige Löschung von IP-Adressen

Orientierungssatz

Der Kunde der Telekom AG kann nicht verlangen, dass die zur Aufnahme einer Internetverbindung vergebenen "dynamischen" IP-Adressen sofort nach Beendigung der Verbindung gelöscht werden. In der Regel handelt die Telekom AG ohne schuldhaftes Zögern, wenn sie die Löchung erst nach sieben Tagen vornimmt.

Tenor

Die Berufung des Klägers gegen das Urteil der 10. Zivilkammer – Einzelrichterin – des Landgerichts Darmstadt vom 6.06.2007 wird zurückgewiesen.

Der Kläger hat die Kosten des zweiten Rechtszuges zu tragen.

Das Urteil ist vorläufig vollstreckbar.

Der Kläger darf die Vollstreckung durch Sicherheitsleistung oder Hinterlegung von 115 % des auf Grund des Urteils vollstreckbaren Betrages abwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 115 % des jeweils zu vollstreckenden Betrages leistet.

Die Revision wird zugelassen.

Gründe

I.

1 Der Kläger erstrebt die Verurteilung der Beklagten dergestalt, dass diese nach dem jeweiligen Abbruch einer Internetverbindung die zum Zwecke des Aufbaus der Internetverbindung vergebenen dynamischen IP-Adressen jeweils „sofort“ zu löschen hat.

2 Der Kläger ist als Versicherungskaufmann in einem Angestelltenverhältnis tätig. Freiberuflich betätigt er sich überdies als Informatiker.

3 Die Beklagte ist mit über 10,5 Millionen Kunden einer der größten …- Dienstleister Deutschlands.

4 Neben reinen Verbindungen stellt die Beklagte im Rahmen eines einheitlichen Leistungsangebots weitere Dienste zur Verfügung. Dazu gehören E-Mail-Dienste, Chat & Foren, ein Nachrichtenmagazin, Online-Banking, ein elektronischer Terminkalender (WebOrganizer) und SMS- sowie Nachrichtendienste über das Internet (X-Messenger). Dabei bietet die Beklagte den Zugang zu ihren Online-Diensten über analoge, ISDN-, GSM- oder DSL-Verbindungen an. Ihre Dienste sind auch über Telekommunikationsnetze anderer Unternehmer – auch aus dem Ausland – zu erreichen.

5 Die Kunden der Beklagten können bei Abschluss eines Internetzugangsvertrages zwischen verschiedenen Tarifen wählen. Die Tarife werden meist nach Dauer und Tageszeit der Dienstnutzung abgerechnet (X Eco, X by day, X by night). Außerdem gibt es Tarife, bei denen eine bestimmte Nutzungsdauer pauschal zu vergüten ist und erst darüber hinaus eine minutenbezogene Abrechnung beginnt (X surftime 30 bzw. 60, 90 oder 120). Außerdem bie-

tet die Beklagte eine sogenannte Flatrate an, worunter man im allgemeinen Sprachgebrauch einen zeit- und volumen*un*abhängigen Pauschaltarif für den Internetzugang versteht.

6 Bei der sogenannten „X dsl flat“ handelt es sich um eine Kombination von Dienstleistungen, die es dem jeweiligen Kunden ermöglicht, einen ...-Anschluss zu verwenden und sich über das Telekommunikationsnetz der Beklagten einzuwählen. Der jeweilige Kunde erhält einen Zugang für einen Pauschalvertrag, wenn er eine ...-Verbindung für die Einwahl verwendet. Die pauschale Vergütung über die sogenannte Flatrate gilt für den Internetzugang nur dann, wenn der Kunde den bereitgestellten ...-Anschluss nutzt, um sich einzuwählen. Ein ...-Kunde kann sich mit seinen Zugangsdaten (Kennung und Passwort) aber auch über andere Telekommunikationsanschlüsse (z. B. über Mobiltelefone, aus dem Ausland oder über Wettbewerber der Beklagten im Inland) sowie über beliebige Zugangstechniken (analoge, ISDN- oder GSM-Verbindungen, W-Lan) in den Dienst der Beklagten einwählen. In diesem Fall werden zeitabhängige Nutzungsentgelte für die erbrachten Leistungen fällig. Auch für die Nutzung weiterer Sonderdienste, z. B. den Zugriff auf kostenpflichtige Inhalte anderer Anbieter oder SMS-Dienste, werden entsprechend der individuellen Nutzung gesondert und unabhängig von den angebotenen Zugangstarifen in Rechnung gestellt. Weiterhin entstehen zusätzliche Kosten für die Einrichtung von Mitbenutzern; und zwar pro Mitbenutzer und unabhängig von der gewählten Zugangsart ein bestimmter Satz pro Minute und je Kennung pro Monat.

7 Die Beklagte betreibt in Deutschland an 80 Standorten Einwahlknoten für Breitbandzugänge (z. B. DSL) und mehr als 200 weitere Standorte für Schmalbandverbindungen (z. B. die Einwahl über ein Modem). Dieser Einwahlknotenpunkt wird „Point of Presence“ (POP) genannt und stellt einen Knotenpunkt dar, an dem die Leistungen der Nutzer konzentriert werden, um den Zugang ins Internet zu ermöglichen. An dieser Stelle befindet sich ein so genannter Radius-Server der Beklagten, auf dem die Kunden-Kennungen und das jeweils dazu gehörende Passwort für alle berechtigten Nutzer gespeichert sind. Funktionsbedingt sind auf dem Radius-Server keine weiteren Daten über den Nutzer hinterlegt, weshalb der Radius-Server auch das von dem jeweiligen Kunden gewählte Tarifmodell nicht kennt.

8 Mittels des Radius-Servers und anhand der dort gespeicherten Kennung sowie dem hinterlegten Passwort wird in jedem Fall der Einwahl eines Kunden dessen Nutzungsberechtigung geprüft. Nach der erfolgten Authentifizierung erhält der jeweilige Teilnehmer / Kunde eine sogenannte „dynamische IP- Adresse“ zugeteilt, die sich von der „statischen IP-Adresse“, die einem bestimmten Computer dauerhaft zugeordnet wird, dadurch unterscheidet, dass sie dem Teilnehmer ausschließlich für die gesamte Dauer des Nutzungsvorgangs (Session) zugeteilt wird und bleibt. Dabei wird diese IP-Adresse in einem standardisierten Verfahren aus einem Nummernpool entnommen. Es handelt sich um eine aus vier Ziffernblöcken zusammengesetzte Zahlenreihe, die nach der Beendigung des Nutzungsvorgangs wieder als freie IP-Adresse in den Nummernpool, also den Nummern-Bestand der Beklagten genommen wird und so für andere Nutzungsvorgänge verwendet werden kann. Die Vergabe der dynamischen IP-Adresse hat zur Folge, dass der jeweilige Teilnehmer sich im Internet gegenüber anderen Internetteilnehmern und Serverbetreibern frei und unerkannt, mithin anonym bewegen kann.

9 Die Zuteilung dieser dynamischen IP-Adresse ist für den Verbindungsaufbau zwingend nötig und ermöglicht erst den Zugang zum Internet und zu anderen Telediensten der Beklagten. Kein Internet-Dienst kommt ohne die Verwendung dieser IP-Adressen aus, die als Kommunikationsadresse dient und den Verbindungsaufbau erst ermöglicht. Im Internet kann daher ohne IP-Adresse weder gemailt oder gesurft noch gechattet werden.

10 Erst nach der Zuteilung der IP-Adresse beginnt der abrechnungsrelevante Zeitraum. Dabei erfolgt die Abrechnung nicht etwa über den Radius-Server, der nicht einmal das von dem jeweiligen Kunden gewählte Tarifmodell kennt. Zur Ermöglichung einer Abrechnung überträgt der Radius-Server der Beklagten vielmehr die jeweiligen IP-Adressen und die diesen jeweils zugeordneten Session-Daten, nämlich unter anderem den verwendeten Zugangsweg und den Beginn und das Ende der Nutzung. Dies geschieht bei der Beklagten systembedingt nicht unverzüglich nach Beendigung der einzelnen Nutzung, sondern in festgelegten und wenige Tage betragenden Übertragungs-Intervallen. Die Daten werden sodann durch die so-

genannte „OC-Plattform“ für das dezentrale Abrechnungssystem aufbereitet und letztlich dorthin übergeben. Auf die OC-Plattform können Dritte nicht zugreifen. Zeitlich nach der Verarbeitung der Daten durch die OC-Plattform werden die entgeltlichen und die unentgeltlichen Datenbestandteile voneinander getrennt, sofern in diesem Verarbeitungsschritt die Tarifinformationen vorliegen.

11 Die Beklagte hat die in der vorbeschriebenen Weise genutzten dynamischen IP-Adressen in der Vergangenheit nach dem Rechnungsversand noch 80 Tage lang gespeichert; und zwar in Kombination mit abrechnungsrelevanten Nutzungsdaten / Session-Daten wie den Anfang und das Ende der Verbindung, die Menge der empfangenen und übertragenen Daten, Breitband – oder Schmalbandeinwahl und den Netzvermittlungspunkt. Im Jahr 2007 – und damit im Laufe des vorliegenden und seit 3.05.2003 rechtshängigen Verfahrens – hat die Beklagten diese Speicherzeit auf sieben Tage reduziert. Sie löscht dann die IP-Adresse und die zugeordneten ein- und ausgegangenen Datenmengen, mit der Folge, dass eine Identifikation des Nutzers nicht mehr möglich ist. Diese neue Speicherpraxis entspricht einer Absprache mit dem Bundesbeauftragten für Datenschutz, der diese Praxis ausdrücklich für rechtlich zulässig hält und keinen Anlass zu datenschutzrechtlichen Beanstandungen sieht. Insoweit wird auf das veröffentlichte Schreiben des Bundesbeauftragten für Datenschutz vom 16.03.2007 an die Arbeitsgemeinschaft Vorratsdatenspeicherung verwiesen (vgl. Blatt 387 d. A.).

12 Mit dem Kläger hat die Beklagte unter der Vertragsnummer … vor Jahren einen nach wie vor bestehenden Internet-Zugangsvertrag nach dem sogenannten „X dsl flat“-Tarif abgeschlossen. Im Rahmen dieses Vertragsverhältnisses erhält der Kläger für die Telefon-Nutzung zwar einen ausführlichen Einzelverbindungsnachweis, nicht aber für die Internetnutzung. Wegen der dem Vertrag zu Grunde liegenden Leistungsbeschreibung wird auf Blatt 362 f d. A. Bezug genommen.

13 Spätestens über sein außergerichtliches Schreiben vom 10.03.2003 (vgl. Blatt 5 f d. A.) hat der Kläger eine Einwilligung zur Speicherung von dynamischen IP-Adressen widerrufen.

14 Der Kläger hat im ersten Rechtszug die Auffassung vertreten, sein Vertragsverhältnis mit der Beklagten sei als reiner Flatrate-Zugangsvertrag einzustufen, bei dem es für die Beklagte auf Grund des pauschalisierten Entgeltes keinerlei Anlass gebe, die IP-Adresse nach der Beendigung des Nutzungsvorgangs zu speichern.

15 Der Kläger hat gemeint, im Interesse des Datenschutzes und zum Schutz seiner Privatsphäre müsse die Beklagte die – den Nutzungsvorgängen des Klägers jeweils zugeordneten – IP-Adresse sofort nach Abschluss des jeweiligen Nutzungsvorgangs löschen; dies deshalb, weil über die auch für Dritte sichtbare IP-Adresse die Möglichkeit bestehe, das Nutzerverhalten auszuspähen und daraus Rückschlüsse auf die Persönlichkeit des jeweiligen Teilnehmers zu ziehen.

Der Kläger hat ein berechtigtes Interesse der Beklagten an der Speicherung der jeweiligen IP-Adresse in Abrede gestellt. Er hat geltend gemacht, sie benötige die IP-Adresse weder zu Abrechnungszwecken noch müsse sie auf diese Daten zum Schutz ihres Systems und / oder zum Schutz anderer Nutzer / Teilnehmer zurückgreifen.

16 Im Rahmen der Abrechnung, so hat der Kläger weiter vorgebracht, sei zwischen reinen Flatrates und zeit- bzw. volumenabhängigen Tarifen zu unterscheiden. Bei Flatrates bestehe bereits deshalb kein Speicherbedürfnis, weil lediglich eine pauschale Vergütung abgerechnet werde. Bei zeit- und volumenunabhängigen Tarifen, und um einen solchen handele es sich hier, könne die Beklagte für die Abrechnung auf sogenannte Log-Dateien zurückgreifen, die sie neben den IP-Adressen speichere. Die Beklagte verwechsle im Übrigen die Begriffe 'Geeignetheit' und 'Erforderlichkeit'. Lediglich auf die 'Erforderlichkeit' komme es bei der Speicherung von derartigen Daten aber an. Abgesehen davon sei dem Gesetz zu entnehmen, dass sich die Darlegungs- und Beweislast dann ändere, wenn die Beklagte Daten auf Grund gesetzlicher Bestimmungen gelöscht habe.

17 Der Kläger hat sich zudem darauf berufen, dass die Beklagte auch bei der Vermeidung von Störungen / Angriffen gegen ihr System bzw. bei Eingriffen in die Rechte ihrer Nutzer ohne

eine Speicherung der IP-Adressen auskomme. Die Speicherung von IP-Adressen erleichtere vielleicht das Auffinden und Zurückverfolgen von technischen Störungen. Sie sei dafür aber nicht erforderlich, wie sich bereits daraus ergebe, dass die A GmbH ohne eine solche Speicherung auskomme. Aus § 100 TKG ergebe sich ohnehin, dass die Beklagte die IP-Adressen nicht ohne eine(n) konkreten Anlass/Vorfall/Störung speichern dürfe. Die verdachtsunabhängige Speicherung auf Vorrat sei verfassungswidrig. Auch § 101 I TKG setze eine konkrete Störung voraus.

18 Der Kläger hat im ersten Rechtszug zuletzt beantragt,

19 1. Die Beklagte wird verurteilt, die IP-Adressen, welche sie den von dem Kläger genutzten Internet-Rechnern zuweist, sofort nach dem jeweiligen Ende der Internetverbindungen zu löschen.

2. Die Beklagte wird verurteilt, es zu unterlassen, die bei der Nutzung des Internetzugangs durch den Kläger im Rahmen des zwischen den Parteien bestehenden Vertragsverhältnisses nach dem Tarif X dsl flat bekannt gewordenen Anfangs- und Endzeitpunkte der Internetverbindungen zu erheben und zu speichern.

3. Die Beklagte wird verurteilt, es zu unterlassen, die bei der Nutzung des Internetzugangs durch den Kläger im Rahmen des zwischen den Parteien bestehenden Vertragsverhältnisses nach dem Tarif X dsl flat bekannt gewordenen Volumen der übertragenen Daten zu erheben und zu speichern.

4. Die Beklagte wird verurteilt, die ihr bei der Nutzung des Internetzugangs durch den Kläger im Rahmen des zwischen den Parteien bestehenden Vertragsverhältnisses nach dem Tarif X dsl flat bereits bekannt gewordenen IP-Adressen, Anfangs- und Endzeitpunkte der Internetverbindungen sowie Volumen der übertragenen Daten unverzüglich zu löschen.

5. Der Beklagten wird für jeden Fall der Zuwiderhandlung gegen Ziffer 2 oder 3 ein Ordnungsgeld von bis zu 100.000,– Euro, ersatzweise Ordnungshaft, zu vollziehen an den Vorstandsmitgliedern, angedroht.

6. Die Beklagte wird verurteilt, an den Kläger in jedem Fall der Zuwiderhandlung gegen 1, 2 oder 3 einen Schadensersatz in angemessener Höhe, vorschlagsweise fünf Euro zu zahlen.

20 Die Beklagte hat im ersten Rechtszug beantragt,

21 die Klage abzuweisen.

22 Die Beklagte hat im ersten Rechtszug die Auffassung vertreten, ihre Speicherpraxis, der zufolge dynamischen IP-Adressen zunächst bis zum Ablauf von 80 Tagen und seit 2007 bis zum Ablauf von sieben Tagen gespeichert werden, sei nicht nur zulässig, sondern auch notwendig.

23 Die Beklagte hat behauptet, sogenannte Log-Dateien, auf Grund derer sie auch ohne Rückgriff auf die IP-Adressen eine Abrechnung vollziehen könne, stünden ihr nicht zur Verfügung. Die Verwendung derartiger Dateien erhöhe sogar zum Nachteil ihrer Teilnehmer das Missbrauchsrisiko.

24 Zwar könne, nachdem die Kennung und das Passwort des jeweiligen Teilnehmers in Kombination mit der IP-Adresse über den Radius-Server in ihr Abrechnungssystem übergeleitet worden seien, eine Aufteilung in abrechnungspflichtige und abrechnungsfreie Nutzungswege und Zeiten erfolgen. Zur Vermeidung von Abrechnungsschwierigkeiten, zur Gewährleistung einer Prüfbarkeit sowie zum Nachweis der Richtigkeit der Abrechnungen sei es jedoch notwendig, die IP-Adressen weiter zu speichern, um Einwendungen der Nutzer hinsichtlich der Nutzung des Internets begegnen zu können und nachweisen zu können, dass die in Rechnung gestellten Beträge ordnungsgemäß abgerechnet worden seien. Die IP-Adresse sei auch nötig, um die tatsächliche Verfügbarkeit / Nutzbarkeit ihrer Dienste belegen zu können, etwa wenn der Teilnehmer diesbezügliche Einwände erhebe und Kürzungen des Entgeltes

vornehme. So wie ein Versandhändler zu einzelnen Bestellungen eine Verfahrensnummer speichere, so wie jede Autovermietung einem Mieter das Kfz-Kennzeichen zuordne und wie jedes Gericht zu einem anhängigen Verfahren ein Aktenzeichen vergebe, so müsse es auch der Beklagten möglich sein, eine Zuordnung zu ermöglichen. Die IP-Adresse stelle eine vergleichbare Verfahrens- bzw. Referenznummer dar.

25 Die Beklagte hat die Auffassung vertreten, es handele sich bei dem mit dem Kläger bestehenden Vertragsverhältnis nicht um eine reine Flatrate. Je nach Zugangsart (etwa über einen mobilen Anschluss), bei der Nutzung von Inhalten (z. B. Videos), die zum Leistungsangebot der Beklagten gehören, und / oder der Einrichtung eines Mitbenutzers bedürfe es einer Abrechnung anhand der Anfangs- und Enddaten der jeweiligen Nutzung.

26 Die Speicherung sei darüber hinaus, so hat die Beklagte weiter geltend gemacht, auch deshalb notwendig, weil es – was allgemein und damit gerichtsbekannt sei – relativ häufig zu Störungen / Missbrauchsfällen komme, denen nur mithilfe der IP-Adressen entgegen gewirkt werden könne. Die Beklagte sei auf Grund ihres Systems in der Lage, die bei ihr gespeicherten Nutzerdaten effektiv vor Angriffen Dritter – seien es Missbrauchsversuche durch SPAM und „Bot-Netze“, durch Viren, Würmer bzw. Trojaner oder durch die inzwischen häufig eingesetzte Methode des „Phishing“ bzw. DDoS-Angriffe etc. – zu schützen (vgl. insoweit die detaillierten Darlegungen der Beklagten im Schriftsatz vom 17.11.2006, Blatt 303 ff d. A.). Auch die eigene Infrastruktur der Beklagten müsse geschützt werden. Dabei dürfe nicht außer Betracht gelassen werden, dass die Beklagte von den vorstehend Störungen regelmäßig erst Kenntnis erlange, wenn sich Nutzer beschwerten. Keinesfalls sei davon auszugehen, dass Angriffe regelmäßig sofort entdeckt werden könnten. Auf Grund dieser vielfältigen und ständig akuten Störungen sei die Beklagte nach § 100 I TKG berechtigt, die IP-Adressen, bei denen es sich um sogenannte „Verkehrsdaten“ in einem zeitlichen Rahmen von sieben Tagen zu speichern, um sie zur Erkennung und Analyse von Angriffsmustern zu nutzen. § 100 I TKG setze, anders als § 100 III TKG, nicht mehr voraus, das im Einzelfall eine tatsächliche Störung und / oder ein Fehler vorliege. Zulässig sei die streitgegenständliche Datenerhebung, um Fehlern unverzüglich entgegenwirken zu können. Es handele sich dabei auch keineswegs um eine verdachtsunabhängige Vorratsspeicherung; vielmehr seien die Störungen durch SPAM, Schadsoftware etc. ständig und anhaltend präsent und könnten jederzeit dazu führen, dass die eigene Infrastruktur der Beklagten tangiert sei, weil andere Dienstanbieter ihre IP-Adressbereiche im Störungsfalle sperrten, wie es in der Vergangenheit bereits vorgekommen sei. So habe „C“ in den USA auf Grund einer Virenwelle, die viele mitteleuropäische Nutzer betroffen hätten, ihre Mailserver für einige IP-Adressbereiche der Beklagten zeitweise komplett gesperrt, mit der Folge, dass Millionen von Kunden der Beklagten nicht mehr in der Lage gewesen seien, ihre E-Mails an „C“ zu verschicken. „C“ habe die Aufhebung der Sperre davon abhängig gemacht, dass die Beklagte ihre betroffenen Kunden informiere. Dazu sei die Beklagte nur auf Grund einer Auswertung ihrer IP-Adressen möglich gewesen, wobei der Vorgang über einen Monat in Anspruch genommen habe. In einem anderen Fall habe das US Patent- und Markenamt einen Teilbereich der IP-Adressen der Beklagten komplett gesperrt, um in erster Linie seine eigene Infrastruktur zu schützen. Dies habe zur Folge gehabt, dass eine Kommunikation mit den Webservern und den Mailservern aus diesem Bereich nicht mehr möglich gewesen sei. Mehr als einer Million der Teilnehmer der Beklagten, zu denen auch gewerbliche Teilnehmer gehörten, sei damit ein Zugang zu diesen Seiten verwehrt gewesen. Erst sechs bis sieben Wochen später habe sich herausgestellt, dass eine handvoll Computer durch einen Wurm infiziert gewesen seien, die das US-Patent- und Markenamt mit ständigen Anfragen bombardiert hätten. Erst nachdem der Beklagten die betroffenen IP-Adressen bezeichnet worden seien, habe sie mit deren Hilfe die wenigen verseuchten Computer ausfindig machen und die Teilnehmer informieren können.

27 Soweit der Kläger geltend mache, dass die A GmbH ohne die Speicherung von IP-Adressen auskomme, sei klarzustellen, dass dieses Unternehmen keine mit den von der Beklagten erbrachten Leistungen vergleichbare Dienste erbringe.

28 Schließlich sei eine Speicherung unter Berücksichtigung des § 9 BDSG erforderlich, damit die Beklagte ihrer gesetzlichen Pflicht gerecht werde, die Datensicherheit insgesamt zu gewährleisten.

29 Auch die staatlichen Sicherheitsbehörden seien im Rahmen der Strafverfolgung auf die gespeicherten Daten angewiesen. Ein sachgerechter Schutz von Urheberrechten sei nur auf Grund gespeicherter IP-Adressen erreichbar. Seit der Umstellung auf eine Speicherzeit von (nur) sieben Tagen könnten Störungen / Fehler zwar nicht mehr so umfassend wie früher erfasst und eingegrenzt werden, bei einem wesentlichen Teil der Störungen gelinge dies aber nach wie vor. Der zeitliche Rahmen der Speicherung dürfe daher keinesfalls verkürzt werden.

30 Von einer Verfassungswidrigkeit der Speicherpraxis sei schon deshalb nicht auszugehen, weil die anonymisierte IP-Adresse für sich gesehen keinerlei Rückschluss auf den jeweiligen Nutzer / Teilnehmer zulasse. In diesem Zusammenhang hat die Beklagte klargestellt, dass lediglich ein kleiner, eingegrenzter Personenkreis Zugriff auf diejenigen Daten habe, mittels derer über die IP-Adressen ein Zusammenhang zu einem bestimmten Kunden hergestellt werden könne. Außerdem sei durch die standardisierte und intervallartige Verlagerung der Daten vom Radius-Server auf die OC-Plattform gewährleistet, dass Dritte keinerlei Zugriff auf die Daten hätten.

31 Vor diesem Hintergrund halte nicht nur der Regierungspräsident Darmstadt die Speicherpraxis der Beklagten für rechtmäßig, wie aus dessen veröffentlichtem Schreiben vom 14.01.2003 (vgl. Blatt 7 f d. A.) zu entnehmen sei.

32 Auch der Bundesbeauftragte für Datenschutz gehe ausweislich seines veröffentlichten Schreibens vom 16.03.2007 (vgl. Blatt 387 d. A.) von der Zulässigkeit der Speicherpraxis der Beklagten aus.

33 Aus einer Presseerklärung der Europäischen Kommission zur Bekämpfung von SPAM vom 15.11.2006 (KOM(2006)688, vgl. Blatt 323 – 325, 336 ff d. A.) sei zu entnehmen, dass die Europäische Kommission auf Grund massiver Verbreitung von SPAM, Späh- und Schadsoftware ein verstärktes Vorgehen gegen illegale Online-Aktivitäten für zwingend erforderlich halte, wozu die Internet-Access-Provider aufgerufen seinen.

34 Wegen weiterer Details des erstinstanzlichen Vorbringens beider Parteien wird auf die Schriftsätze des Klägers vom 15.04.2003, 7.05.2003, 16.05.2003, 30.06.2003, 26.08.2003, 26.09.2003, 14.01.2004, 20./21.09.2006, 11.12.2006, 21.12.2006, 26.01.2007, 7.03.2007 21.05.2007 und 22./23.05.2007 nebst den jeweiligen Anlagen (vgl. Blatt 1 – 27, 29 – 39, 42 – 46, 80 – 82, 142 – 150, 151 – 154, 178 – 179, 273 – 294, 315 – 318, 340, 368 – 369, 370 – 372, 412 – 414 und 419 – 422 d. A.) und auf die Schriftsätze der Beklagten vom 10.06.2003, 6.08.2003, 22.01.2004, 17.11.2006, 14.12.2006, 16.01.2007, 9.05.2007, 16.05.2007 und 31.05.2007 nebst den jeweiligen Anlagen (vgl. Blatt 58 – 76, 87 – 141, 180 – 192, 299 – 313, 319 – 338, 354 – 364, 374 – 387, 393 – 411 und 424 – 425 d. A.) verwiesen.

35 Gemäß Beweisbeschluss vom 16.03.2004 (vgl. Blatt 196 - 198 d. A.) hat das Landgericht Darmstadt Beweis erhoben durch Einholung eines schriftlichen Gutachtens des Dipl. Ing. SV1. Wegen des Wortlauts des Gutachtens vom 20.06.2006 wird auf die Akten Bezug genommen. Der Sachverständige hat eine ergänzende Stellungnahme vom 14.09.2006 abgegeben (vgl. Blatt 271 – 272 d. A.).

36 Mit Urteil vom 6.06.2007 hat die 10. Zivilkammer – Einzelrichterin – des Landgerichts Darmstadt der Klage nur zum Teil stattgegeben und die Beklagte unter anderem auf den Klageantrag zu 1) verurteilt, „die IP-Adressen, welche sie den von dem Kläger genutzten Internet-Rechnern zuweist, sieben Tage nach dem jeweiligen Ende der Internetverbindung zu löschen."

37 Zur Begründung, wegen deren Einzelheiten auf Blatt 427 – 440 d. A. verwiesen wird, hat das Landgericht im Kern ausgeführt, der Kläger habe gegen die Beklagte nur insoweit einen Anspruch auf Nichterhebung bzw. Löschung der im Streit stehenden Daten (unabhängig von der rechtlichen Qualifizierung der Dienstleistungen als Telekommunikationsdienstleistungen oder Teledienste), soweit die Speicherung dieser Daten über das Ende der Internetverbindung hinaus nicht zu Abrechnungszwecken oder zur Behebung von Störungen erforderlich – und damit gesetzlich erlaubt – ist.

38 Soweit es den – im zweiten Rechtszug allein noch streitgegenständlichen Klageantrag zu 1) betrifft – hat das Landgericht dargelegt, der Anspruch auf Löschung der IP-Adresse bestehe insoweit als der Kläger sich gegen die Speicherung der IP-Adressen nach Ablauf von sieben Tagen nach Beendigung der Internetverbindung wende; der darüber hinaus verfolgte Anspruch auf *sofortige* Löschung bestehe nicht.

39 Das Landgericht hat die Auffassung vertreten, die Speicherung der IP-Adresse für den Zeitraum von sieben Tagen nach dem Ende der jeweiligen Internetverbindung sei jedenfalls zur Behebung von Störungen erforderlich. Bei den fraglichen Dienstleistungen der Beklagten handele es sich (im wesentlichen) um Telekommunikationsdienstleistungen i. S. d. § 3 Nr. 24 TKG. Aus Gründen des Datenschutzes und der Datensicherheit sei die Beklagte zunächst berechtigt, die Nutzerdaten von den Verbindungsdaten getrennt zu halten, auch wenn dies zur Konsequenz habe, dass die Verbindungsdaten einschließlich der IP-Adresse nicht unmittelbar nach dem Ende der Internetverbindung gelöscht werden, da sie noch ausgewertet und mit den Nutzerdaten sowie den Tarifbedingungen abgeglichen werden müssten. Dies gelte allerdings nur unter der Voraussetzung, dass diese Auswertung der Daten binnen kurzer Frist erfolge. Nach diesem Zeitraum sei die Speicherung unter diesem Aspekt nicht mehr erforderlich; vielmehr sei es dem Dienstanbieter zumutbar, innerhalb dieser Frist die Daten auszuwerten und etwa entgeltpflichtige Sonderleistungen zu erfassen und abzurechnen.

40 Ob eine Speicherung der IP-Adresse darüber hinaus – auch bei sogenannten Flatrate-Verträgen – zu Abrechnungszwecken erforderlich und zulässig sei, etwa um die Verfügbarkeit der Dienstleistung (insbesondere des Zugangs) in diesem Zeitraum und die Richtigkeit der Abrechnung nachweisen zu können, sei fraglich, habe aber offen bleiben können.

41 Die Beklagte habe hierzu dargelegt, dass die Speicherung der IP-Adressen nicht nur dem Nachweis diene, dass die Dienste der Beklagten in Anspruch genommen worden seien und damit zur Verfügung standen (etwa wenn ein Kunde mit Flatrate die Pauschale wegen einer behaupteten Leistungsstörung kürzen wolle), sondern auch erforderlich sei, um die tatsächlich stattgefundenen Verbindungen bei Inanspruchnahme von gesondert vergütungspflichtigen Diensten nachweisen zu können.

42 Dies erscheine zwar zunächst plausibel, begründe allerdings lediglich eine mögliche Geeignetheit, nicht hingegen eine *Erforderlichkeit* der Speicherung zu diesen Zwecken. Die Beklagte habe insoweit nicht substantiiert dargelegt, dass ihr kein anderes geeignetes (und weniger belastendes) Mittel zur Erreichung dieser Zwecke zur Verfügung stehe. Durch die bloße Nennung zusätzlicher Daten im Falle eines Streites dürfe sich die Nachweismöglichkeit und Beweislage nicht wesentlich verändern.

43 Die Frage einer Erforderlichkeit der Speicherung der Daten zu Abrechnungszwecken habe jedoch im Hinblick auf die Zulässigkeit der Speicherung nach § 100 I TKG dahingestellt bleiben können, weshalb es letztlich auch nicht auf das im Laufe des Rechtsstreits eingeholte Gutachten zur Frage der Erforderlichkeit zu Abrechnungszwecken ankomme. Die Beklagte habe nach Einholung des Gutachtens substantiierten Vortrag zur Frage der Erforderlichkeit der Speicherung zur Behebung von Störungen gehalten. Demgegenüber sei ihr Vortrag zur Erforderlichkeit zu Abrechnungszwecken teilweise nicht ausreichend substantiiert geblieben.

44 Die Speicherung der IP-Adresse sei, so hat das Landgericht weiter ausgeführt, jedenfalls für die Dauer von sieben Tagen nach dem Ende der jeweiligen Internetverbindung zur Behebung von Störungen im Sinne des § 100 I TKG erforderlich und zulässig.

45 Die Beklagte benötige die IP-Adresse zur Erkennung, Eingrenzung und Beseitigung von Störungen oder Fehlern ihrer Telekommunikationsanlagen. Es sei nachvollziehbar und allgemein bekannt, dass es nach dem Ende einer Internetverbindung einige Zeit dauern könne, bis eine Störung entdeckt oder eine Fehlermeldung durch andere Service Provider erfolge. Dies gelte auch für Mitteilungen betreffend Spam-Angriffe. Es sei im Übrigen auch allgemein bekannt, dass es verschiedene Missbrauchsarten gebe, die die Sicherheit der Nutzer der Beklagten und die Sicherheit der Telekommunikationsanlagen der Beklagten bedrohten.

46 Dem sei der Kläger auch nicht entgegengetreten; er habe sich darauf beschränkt, die Erforderlichkeit der Speicherung gerade dieser Daten zu diesem Zweck zu bestreiten.

47 Zu den häufigsten Störungen des Telekommunikationsnetzes der Beklagten gehöre zunächst die Versendung von belästigenden Nachrichten per E-Mail (sog. Spam-E-Mails). Dies sei nicht nur eine Belästigung, sondern stelle für die Nutzer und die Beklagte eine direkte Bedrohung der Infrastruktur dar, weil diese in erheblichem Ausmaß durch Spam in Anspruch genommen würden und diese Kapazitäten der regulären Inanspruchnahme durch die Nutzer nicht zur Verfügung stünden. Außerdem würden Spam häufig durch mit Schadsoftware infizierte Rechner ohne Wissen des Inhabers und unter Missbrauch seines Internetzugangs versendet. Dies zu unterbinden sei in Anbetracht der Beeinträchtigungen durch Spam nicht nur im Interesse des betroffenen Nutzers, sondern auch im Interesse der Beklagten selbst sowie der Gesamtheit ihrer Nutzer.

48 Die Identifikation eines solchen infizierten Rechners sowie eines Spam-Versenders könne nach dem substantiierten und nachvollziehbaren Vortrag der Beklagten nur anhand der IP-Adresse, die nicht gefälscht werden könne, sowie des dazugehörigen Datums nebst Uhrzeit stattfinden. Der Kläger habe dies nicht substantiiert in Abrede gestellt.

49 Mit den genannten Informationen könne der Internetprovider nach Erhalt einer entsprechenden Information durch den Empfänger einer Spam-Nachricht oder durch andere Internetprovider das jeweilige Nutzerkonto ermitteln, von dem aus die fragliche E-Mail versandt worden sei; ggf. könnten auch Rechner ermittelt werden, die unbemerkt mit Schadprogrammen infiziert worden seien.

50 Der Internetprovider – hier also die Beklagte – könne dann dem betroffenen Nutzer mitteilen, dass sein Computer von Dritten missbraucht werde; er könne auch Maßnahmen ergreifen, um den Spam-Versand zu unterbinden.

51 Der diesbezüglich ins Detail gehende Vortrag der Beklagten, wonach – insbesondere in Anbetracht der Anzahl ihrer Nutzer – einzig die IP-Adresse geeignet sei, nach dem Ende einer Internetverbindung eine Identifizierung eines einzelnen Nutzers zu ermöglichen, sei nachvollziehbar und vom Kläger nicht hinreichend bestritten. Die Behauptung des Klägers, die IP-Adresse sei zur Identifikation nicht erforderlich, da weitere Datensammlungen bestünden, sei zu pauschal und überdies von der Beklagten in Abrede gestellt worden.

52 Auch bei der Verbreitung von Schadprogrammen (u. a. Viren, Würmer, Trojaner), die ebenfalls häufig über Spam-Nachrichten erfolge, könne der Absender und dessen Nutzer-Account nur über die IP-Adresse (nebst Datum und Uhrzeit des Versandes) ermittelt werden. Dadurch sei es möglich, Nutzer eines infizierten Rechners zu warnen und mögliche Schäden zu reduzieren.

53 Das Vorgenannte gelte im Prinzip auch bei sog. Phishing-Emails.

54 Eine weitere Störung bestehe darin, dass Angriffe auf einzelne Computer durch Zusammenschlüsse vieler infizierter Rechner dann erfolgen könnten, wenn von den infizierten Computern in einer gleichzeitigen und gesteuerten Aktion die Infrastruktur eines Unternehmens oder Webdienstes angegriffen werde, indem auf dem angegriffenen Computer ständig Informationen/Dienstleistungen abgefragt würden, bis er bzw. der entsprechende Webserver abstürze. Hierbei zeichneten die angegriffenen Computer zwar meist die IP-Adresse, das Datum und die Uhrzeit des Angriffs auf. Die angegriffenen Computer könnten die betreffenden Angreifer bzw. Nutzer der entsprechend infizierten Computer jedoch nicht identifizieren und die Angriffe durch infizierte Computern auch nicht selbst stoppen. Wenn eine am Angriff beteiligte IP-Adresse aus dem Adressbereich eines anderen Internetproviders, etwa der Beklagten, stamme, könnten sich die Betroffenen bzw. deren Internetprovider an die Beklagte wenden. Die Beklagte selbst könne nach deren substantiierten Vorbringen derartige Angriffe nur stoppen bzw. den Kunde mit dem betroffenen Rechner informieren, wenn die IP-Adresse (nebst Datum und Uhrzeit) noch in den bei ihr gespeicherten Daten vorhanden sei. Bei einer sofortigen Löschung der IP-Adresse könnten diese Störungs- und Missbrauchsszenarien in Kun-

dennetzen nicht mehr bekämpft und die Nutzer unwissentlich infizierter Rechner nicht mehr gewarnt und informiert werden.

55 Darüber hinaus hat das Landgericht die Ansicht vertreten, die Beklagte sei auch berechtigt, ihre eigene Infrastruktur gegen rechtswidrige Inanspruchnahme zu schützen. Es sei nachvollziehbar und allgemein bekannt, dass dann, wenn ein Internetprovider nicht gegen Spam-Versender und Versender von Schadsoftware vorgehe, dies dazu führe, dass bestimmte IP-Adressbereiche, von denen in der Vergangenheit Störungen ausgegangen seien, von anderen Internetdienstleistern und Internetprovidern gesperrt würden. Diese Adressbereiche seien dann nicht mehr erreichbar und könnten von der Beklagten und deren Nutzern nicht mehr genutzt werden.

56 Auch dies rechtfertige – zur Abwehr von Störungen – die Speicherung der IP-Adresse sowie des Datums und des Zeitraums der jeweiligen Nutzung zumindest so lange bis entsprechende Rückmeldungen wegen Störungen erfahrungsgemäß erfolgten. Der Provider erhalte in den vorgenannten Fällen häufig erst im Nachhinein Kenntnis von den Störungen, so dass die Störungsquelle auch erst im Nachhinein ermittelt werden könne (und müsse).

57 Bei einer unverzüglichen Löschung der IP-Adresse und des Zeitpunktes ihrer Nutzung durch einen konkreten Nutzer sei eine nachträgliche Ermittlung der Störungsquelle jedoch nicht mehr möglich, was die Beklagte im Einzelnen und detailreich dargelegt habe. Der Kläger habe dies nicht substantiiert bestritten.

58 Eine solche – praktisch vorbeugende – Speicherung der IP-Adresse zur Eingrenzung und Behebung von Störungen ohne konkrete tatsächliche Anhaltspunkte bei einem bestimmten Benutzer lasse § 100 I TKG seit einer entsprechenden Gesetzesänderung auch ausdrücklich zu. Es sei daher nicht erforderlich, dass im Einzelfall tatsächlich Störungen und Fehler oder konkrete Anhaltspunkte dafür vorlägen. Ausreichend sei es, dass mit hinreichender Wahrscheinlichkeit von dem weiteren Auftreten solcher Störungen auszugehen sei, was auf Grund der Lebenserfahrung zu bejahen sei.

59 Mangels gegenteiliger Anhaltspunkte und aufgrund allgemeiner Lebenserfahrung gehe das Gericht davon aus, dass solche Rückmeldungen durch andere Internetprovider und betroffene Nutzer im Regelfall zeitnah, jedenfalls binnen sieben Tagen, erfolgen, so dass die Speicherung der IP-Adresse (und des Anfangs- und Endzeitpunktes der betreffenden Verbindung) grundsätzlich nur für diesen Zeitraum zur Verhinderung und Behebung von Störungen nach § 100 I TKG erforderlich und damit zulässig sei.

60 Gegen das dem Kläger am 11.06.2007 zugestellte landgerichtliche Urteil wendet sich der Kläger mit seiner am 22.06.2007 eingelegten und begründeten Berufung.

61 Er verfolgt seinen ursprünglichen Klageantrag zu 1) unverändert weiter und erstrebt eine Abänderung des Urteils dahingehend, dass die Beklagte verurteilt wird, die den Rechnern des Klägers zugewiesenen IP-Adresse *sofort* nach der Beendigung der jeweiligen Internetverbindung zu löschen.

62 Der Kläger wiederholt und vertieft sein erstinstanzliches Vorbringen und macht – unter Hinweis auf die Entscheidung des Bundesverfassungsgerichts vom 27.06.2006 zum Aktz. 1 BvR 1811/99 (abgedruckt in NJW-2007, 3055 = MMR 2007, 308), die sich mit der Speicherung von Verkehrsdaten befasst, die nach der Nutzung eines mittels einer Prepaid-Karte genutzten Mobiltelefons gespeichert wurden – geltend, die sofortige Löschung der IP-Adresse sei für die Beklagte sowohl technisch möglich als auch praktikabel. Fünfzehn andere Zugangsanbieter löschten die IP-Adresse jedenfalls sofort. Wegen der detaillierten Bezeichnung dieser Anbieter und wegen weiterer Einzelheiten wird auf die Ausführungen im Schriftsatz des Klägers vom verwiesen (vgl. Blatt 463, 478- 480 d. A.).

63 Der Kläger meint, § 100 TKG erlaube nur die gezielte Ermittlung von IP-Adressen auf Grund konkreter Störungen bzw. Fehlern oder bei tatsächlichen Anhaltspunkten für Missbrauch. Dadurch habe sich auch durch die Neufassung des § 100 TKG und damit den Wegfall der

Worte „im Einzelfall“ nichts geändert. Bei verdachtsunabhängiger Vorratsdatenspeicherung seien „zu dokumentierende tatsächliche Anhaltspunkte“ nicht ersichtlich.

64 Spams, ein Virenversand, Botnetze und DDos-Angriffe stellten keine Störungen im Sinne des § 100 I TKG dar, da sie die Funktionsfähigkeit der TK-Anlagen nicht beeinträchtigten, wie die tägliche Praxis der Beklagten und anderer Anbieter belege. Spams seien nur im Zusammenhang mit der Kapazität und im Sinne einer höheren Auslastung von Relevanz. Kapazitäten könnten aber erweitert werden, weshalb eine Belastung nicht mit einer Störung im Sinne des § 100 TKG verbunden sei. Die Infrastruktur der Beklagten werde dadurch nicht bedroht. Dass die Beklagte anhand von IP-Adressen den Störer ermitteln könne, müsse bestritten werden. Die Beklagte bleibe hinreichende Darlegungen und Belege schuldig. Außerdem existiere, was in der einschlägigen Literatur regelmäßig diskutiert werde, spezielle Anonymisierungssoftware, die die Rückverfolgung anhand von IP-Adressen vereiteln könne.

65 Die IP-Adressen des Klägers müssten bereits deshalb nicht gespeichert werden, weil der Kläger keine Spam versende und den Internet-Zugang auch nicht missbrauche. Nutzer unwissentlich infizierter Rechner würden von der Beklagten auch keineswegs gewarnt oder informiert.

66 Die Speicherung sämtlicher Nutzerdaten über sieben Tage hinweg, nur weil die Daten eines kleinen Bruchteils der Nutzer einmal benötigt werden könnten, sei unverhältnismäßig und verfassungswidrig. Die Beklagte selbst habe in einem internen Papier einmal ausgerechnet, dass nur 0,004 % der gespeicherten IP-Adressen jemals störungsrelevant würden. Wenn aber von 250.000 Kunden nur ein einziger Kunde rechtswidrig handele, sei es unverhältnismäßig alle Kunden unter „Generalverdacht“ zu stellen.

67 Der Kläger, der mit Rücksicht auf die im Laufe des vorliegenden Rechtsstreits eingeführten §§ 113 a, 113 b TKG zunächst angekündigt hatte, hilfsweise auch einen Feststellungsantrag zu stellen, wonach die Beklagte bis zum 31.12.2007 verpflichtet gewesen sei, die IP-Adressen sofort nach dem jeweiligen Ende der Internetverbindungen zu löschen, verfolgt diesen Hilfs-Antrag nicht mehr weiter.

68 Der Kläger beantragt,

69 das Urteil der 10. Zivilkammer – Einzelrichterin – des Landgerichts Darmstadt vom 6.06.2007 abzuändern und die Beklagte zu verurteilen, die IP-Adressen, welche sie den von dem Kläger genutzten Internet-Rechnern zuweist, sofort nach dem jeweiligen Ende der Internetverbindungen zu löschen.

70 Die Beklagte beantragt,

71 die Berufung zurückzuweisen.

72 Die Beklagte verteidigt das angefochtene Urteil, das ihrer Meinung nach auf der zutreffenden Würdigung des wechselseitigen Parteivorbringens, auf dem Ergebnis der mündlichen Verhandlung und auf den eigenen Erkenntnissen des Landgerichts basiere.

73 Die Beklagte hält an ihrer Rechtsauffassung fest, sie sei nach §§ 97 II Nr. 1 TKG, 100 I TKG berechtigt, die IP-Adressen insbesondere zur Erkennung, Eingrenzung und Beseitigung von Fehlern und Störungen an Telekommunikationsanlagen sowie zu Zwecken der Abrechnung zu erheben und zu verwenden.

74 Die Beklagte wiederholt und vertieft ihr Vorbringen erster Instanz und macht geltend, bei Störungen der Telekommunikationsanlage und bei Störungen ihres Abrech-nungssystems sei sie auf die gespeicherten IP-Adressen angewiesen, weil sie ansonsten nach Abbruch des Nutzungsvorgangs nicht mehr erkennen könne, welchem Account die in Anspruch genommenen Dienste zu berechnen oder Fehler und Störungen zuzuordnen seien. Entsprechendes gelte auch für eine weitere Verkürzung des Speicherzeitraumes, der zur Folge habe, dass eine zuverlässige und korrekte Abrechnung nicht möglich sei. Dies gelte auch für den Fall eines einzelnen Kunden, bei dem sie auf Grund einer entsprechenden Verurteilung mit Hilfe

einer speziell dafür entwickelten Software eine schnellere Löschung der IP-Adressen bewirke. Einerseits erlaube es die dafür entwickelte Technik nicht, die IP-Daten für eine Vielzahl von Kunden unmittelbar nach der Beendigung der Session zu löschen; andererseits sei bei diesem Verfahren eine hundertprozentig korrekte Abrechnung nicht gewährleistet.

75 Viele Störungen und Fehler seien, so macht die Beklagte weiter geltend, nur über die IP-Adresse zu erkennen, einzugrenzen und zu beseitigen. Die IP-Adresse sei erforderlich, um zu klären, von wo die Störung und / oder der Fehler ausgehe. Tatsächlich könne es, wie das Landgericht zutreffend festgestellt habe, nach dem Ende der Internetverbindung einige Zeit dauern, bis die Störung überhaupt entdeckt werde oder eine Fehlermeldung von anderen Service-Providern erfolge. Betroffene oder deren Internetprovider wendeten sich dann an die Beklagte, damit die Angriffe gestoppt werden können. Dies gelte nicht nur für Spam-Angriffe, sondern auch für andere Störungs- bzw. Fehlerarten (wird näher ausgeführt, vgl. Blatt 643 - 649 d. A.), die die Beklagte bereits im ersten Rechtszug ausführlich beschrieben habe und die deshalb im landgerichtlichen Urteil zutreffend als unstreitig beschrieben worden seien. Wirkungsvoll könne die Beklagte regelmäßig erst dann gegen Störungen vorgehen, wenn eine Beschwerde vorliege. So sei das Landgericht zu Recht auch davon ausgegangen, dass die Beklagte diejenigen Teilnehmer benachrichtige, deren Computer erkennbar von Späh- und Schadsoftware infiziert worden ist.

76 Die Beklagte macht weiter geltend, Angriffe könnten die gesamte Infrastruktur eines Unternehmens oder eines Internetdienstes derart belasten, dass es zum Absturz komme. Der Schutz der Teilnehmer der Beklagten sei auch deshalb erforderlich, weil die Beklagte nur so die eigene Infrastruktur schützen könne. Immerhin zähle zur Infrastruktur nicht nur die Computer-Hardware, sondern auch der IP-Adressbereich, auf den sie im Rahmen der Verteilung der IP-Adressen zurückgreifen müsse. Dieser Adressbereich sei ein wesentlicher Bestandteil ihrer Produkte. Eine Einschränkung der Nutzbarkeit der IP-Adressen stelle mithin eine Störung ihrer Telekommunikationsanlage dar. In einem idealen Netzwerk könne von jeder IP-Adresse auf jede andere IP-Adresse zurückgegriffen werden. Da es aber im Zusammenhang mit den beschriebenen Störungen und Fehlern dazu kommen könne, dass Internetdienstleister ihre Dienste für bestimmte Adressbereiche komplett sperrten („sogenanntes „Blacklisting“), wenn von diesen in der Vergangenheit Störungen ausgegangen seien (sei es dass sie von einem bestimmten Adressbereich von Spam überflutet würden oder konkreten Angriffen ausgesetzt seien), müsse die Beklagte ihren IP-Adressbereich schützen und Störungsquellen beheben. Denn sobald der IP-Adressbereich der Beklagten in eine solche „Blacklist“ aufgenommen sei, könnten ihre Nutzer auf eine Vielzahl von Internetdiensten nicht mehr zugreifen. Die Funktionsfähigkeit ihrer Computer wäre ansonsten beeinträchtigt. Allein die Sperrung der IP-Adresse eines einzelnen sendenden Computers, eines sogenannten „Mailservers“ (Beispiel „C“ sowie US-Patent- und Markenamt) betreffe meist mehrere 100.000 Teilnehmer der Beklagten.

77 Dass infolge der zeitweisen Speicherung der IP-Adresse auch der (rechtmäßige) Zugriff der Strafverfolgungsbehörden ermöglicht werde, sei dabei ein Nebeneffekt, wobei eine Speicherzeit von nur sieben Tagen für die Staatsanwaltschaft regelmäßig nicht für Ermittlungen ausreiche.

78 Soweit der Kläger geltend mache, dass reine Internetzugangsanbieter, also sogenannte Internetprovider, die nicht wie die Beklagte zahlreiche zusätzliche Dienstangebote vorhielten, IP-Adressen nicht speicherten, sei zu berücksichtigen, dass diese sich in Regel der Beklagten als „Vorleister“ bedienten. Es sei dann der Vorleister, der über die entscheidende Infrastruktur verfüge und diejenigen Daten speichere, die zur Erkennung, Eingrenzung und Beseitigung von Störungen erforderlich seien. Durch eine Speicherung von (nur) sieben Tagen lasse sich ein wesentlicher Teil der Störungsfälle erkennen und eingrenzen. Andere, gleich effektive Mittel zur Erkennung, Eingrenzung und Beseitigung der beschriebenen Störungen existierten nicht. Die Speicherung der IP-Adresse sei das mildeste Mittel; sie sei auch zwingend erforderlich.

Eben deshalb halte der Bundesbeauftragte für Datenschutz die siebentägige Speicherung der Beklagten für zulässig und praxisgerecht, wie entsprechenden Presseveröffentlichungen zu entnehmen sei. Die automatisierte Löschung der IP-Adressen nach sieben Tagen sei das

Ergebnis einer Abwägung zwischen dem Fernmeldegeheimnis der Teilnehmer, also auch des Klägers, und den Belangen der Beklagten; sie werde den in der vom Kläger zitierten Entscheidung des Bundesverfassungsgerichts vom 27.10.2006 (vgl. NJW-2007, 3055 = MMR 2007) gerecht.

79 Es dürfe, so führt die Beklagte weiter an, auch nicht unberücksichtigt bleiben, dass die Europäische Kommission in den dargestellten Angriffen ebenfalls eine ernsthafte Störungen der Telekommunikation und einen Angriff auf die Privatsphäre sehe.

80 Die Beklagte ist der Ansicht, ihre Speicherpraxis verstoße weder gegen das TKG noch gegen Datenbestimmungen. Dabei bilde § 100 I TKG, der nach seiner Novellierung im Unterschied zu § 100 III TKG keinen konkreten Störungsfall voraussetze, die Rechtsgrundlage. In der Entscheidung des Bundesverfassungsgerichts vom 2.03.2010 zum Aktz. 1 BvR 256/08 (vgl. NJW 2010, 833 ff) werde unter der Randnummer 227 ausdrücklich klargestellt, dass die Vorratsspeicherung von Verkehrsdaten im Interesse des Staates an anderen (engeren) Kriterien zu messen sei als die Speicherung durch einen Dienstanbieter. Auch sei nach der genannten Entscheidung davon auszugehen, dass eine staatlichen Interessen folgende Speicherung derartiger Daten nicht schlechthin unverhältnismäßig sei, dass die Nichtigkeit der §§ 113 a, 113 b TKG letztlich nur aus der fehlenden konkreten Ausgestaltung der Überwachungsmaßnahmen und Kontrollmechanismen resultiere.

81 Wegen weiterer Details des wechselseitigen Parteivorbringens im zweiten Rechtszug wird auf die Schriftsätze des Klägers vom 22.06.2007, 20.08.2007, 30.10.2007, 4.06.2008, 3.07.2008, 28.07.2008, 27.10.2008, 10.02.2009, 10.03.2009, 24.03.2009, 3.03.2010, 19.05.2010, 20.05.2010, 24.05.2010 und 25.05.2010 nebst den jeweiligen Anlagen (vgl. Blatt 462 – 486, 499 – 524, 729 – 733, 740 – 760, 761 – 762, 796 – 797, 798 - 799, 800 – 804, 900 – 901, 902 – 914, 923, 962, 964, 967 - 968 und 975 – 980 d. A.) und die Schriftsätze der Beklagten vom 18.10.2007, 22.07.2008, 17.02.2009, 22.03.2010 und 20.05.2010) und 08.06.2010 nebst den jeweiligen Anlagen (vgl. Blatt 630 – 726, 780 – 795, 847 – 888, 929 – 931, 942 – 960 und 994-999 d. A.) verwiesen.

82 Mit Rücksicht auf die mit Wirkung zum 1.01.2008 in Kraft getretenen §§ 113 a, 113 b TKG hat der Senat den Rechtsstreit nach Gewährung rechtlichen Gehörs bis zur Erledigung des Verfahrens vor dem Bundesverfassungsgericht mit dem Aktz. 1 BvR 256/08 ausgesetzt (vgl. den Beschluss vom 24.02.2009, Blatt 893 – 896 d. A.).

83 Der Aussetzungsgrund ist mit der Entscheidung des Verfassungsgerichts vom 2.03.2010 (abgedruckt in NJW 2010, 833 ff) entfallen.

II.

84 Die Berufung des Klägers ist zulässig.

85 Das Rechtsmittel ist nicht nur statthaft, da bereits angesichts der Bedeutung der im Raume stehenden und durch die siebentägige Speicherung der IP-Adresse möglichen, grundrechtsrelevanten Eingriffe in die Privatsphäre des Klägers die Beschwerdesumme von 600,00 € (§ 511 II Nr. 1 ZPO) überschritten ist.

86 Es bestehen auch keine sonstigen Zulässigkeitsbedenken.

87 Die Berufung ist form- und fristgerecht eingelegt und begründet worden.

88 Es ist berufungsrechtlich auch nicht zu beanstanden, dass der Kläger sein Rechtsmittel auf den Urteilsausspruch zu 1.) beschränkt hat; denn zwischen den Parteien besteht kein Streit darüber, dass die IP-Adressen von den Anfangs- und Endzeitpunkten sowie vom Volumen der jeweils übertragenen Daten getrennt werden können, mit der prozessualen Folge, dass der Urteilsausspruch zu 1) von den Urteilsaussprüchen zu 2) – 4) eindeutig abgegrenzt werden kann.

89 In der Sache selbst bleibt der Berufung allerdings der Erfolg versagt.

90 Der angefochtene Teil des Urteils der 10. Zivilkammer des Landgerichts Darmstadt vom 6.06.2007, wonach die Beklagte im Verhältnis zum Kläger verpflichtet ist, „die IP-Adressen, welche sie den von dem Kläger genutzten Internet-Rechnern zuweist, sieben Tage nach dem jeweiligen Ende der Internetverbindung zu löschen“, bedarf keiner Korrektur.

91 Der Kläger hat gegenüber der Beklagten keinen Anspruch darauf, dass die seinen Nutzungsvorgängen jeweils zugeteilten IP-Adressen „sofort“ nach der Beendigung der jeweiligen Internetverbindung (Session) gelöscht werden.

92 Dabei sind für den Senat – auf der Grundlage der im vorliegenden Zivilprozess maßgeblichen wechselseitigen Darlegungen der Parteien – die nachstehenden Erwägungen maßgeblich.

93 Der Kläger kann zwar im Rahmen seines Vertragsverhältnisses zur Beklagten, welches unter anderem durch die Bestimmungen des Telekommunikationsgesetzes (TKG) eine besondere Ausgestaltung erfährt, verlangen, dass die Beklagte sich bei der Erfüllung ihrer vertraglichen Pflichten an die gesetzlichen Vorgaben hält.

94 Nach § 44 TKG ist die Beklagte dem Kläger daher insbesondere „zur Beseitigung und bei Wiederholungsgefahr zur Unterlassung verpflichtet“, wenn sie „gegen dieses Gesetz, eine auf Grund dieses Gesetzes erlassene Rechtsverordnung, eine auf Grund dieses Gesetzes in einer Zuteilung auferlegte Verpflichtung oder eine Verfügung der Bundesnetzagentur verstößt“.

95 Die Regelung des – ab dem 1.04.2010 neu gefassten – § 35 II Ziffer 1 BDSG, wonach personenbezogene Daten zu löschen sind, wenn ihre Speicherung unzulässig ist, ist neben den Spezialnormen des TKG subsidiär (vgl. Klesczewski in Berliner Kommentar, 2006, § 100 TKG, Rd. 10; Gramlich in Manssen, Telekommunikations- und Multimediarecht, lose Blattsammlung, Stand 6/2007, § 91 TKG, Rd. 34; Robert in Beck’scher TKG-Kommentar, 3. Auflage, 2006, § 91 TKG, Rd. 4;); denn in § 1 III S. 1 BDSG ist bestimmt, dass dann, wenn andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, diese dem BDSG vorgehen.

96 Vor diesem Hintergrund stellt sich, da die Parteien nicht auf spezielle, individualvertraglichen Regelungen rekurrieren und den streitgegenständlichen Vertrag auch nicht vorgelegt haben, vorliegend die Frage, ob die Beklagte dem Kläger qua Gesetz nach der jeweiligen Beendigung einer Internetverbindung bezüglich der sogenannten IP-Adresse eine „sofortige“ Löschung schuldet, oder ob die Beklagte im Gegenteil auf Grund eines Erlaubnistatbestandes zu einer zeitweisen Speicherung dieser Daten berechtigt / verpflichtet ist.

1.)

97 Ein Grund zu der Annahme, ein Anspruch auf „sofortige“ Löschung der IP-Adressen könne sich unmittelbar aus der Verfassung ergeben, besteht aus Sicht des Senats nicht.

98 Das Bundesverfassungsgericht hat im Gegenteil mit dem zum Aktz. 1 BvR 256/08 ergangenen Urteil vom 2.03.2010 (abgedruckt in NJW 2010, 833 ff; vgl. z. B. Rd. 227, 254, 278, 300 der Entscheidung) nicht einmal ansatzweise in Zweifel gezogen, dass es rechtmäßig ist, dass „Diensteanbieter in Abhängigkeit von den jeweiligen betrieblichen und vertraglichen Umständen – von den Kunden teilweise beeinflussbar – nach § 96 TKG“ solche Daten, die im Zusammenhang mit dem Telekommunikationsverkehr gewonnenen worden sind „speichern dürfen“.

99 Die Senat hat keinen Anlass, an der Verfassungsmäßigkeit der vorliegend relevanten Bestimmungen in §§ 97 III, 96 I 3 TKG und §§ 96 I 3, 100 I TKG zu zweifeln.

100 2.) Mit dem Kläger ist inzwischen davon auszugehen, dass sich eine Verpflichtung der Beklagten zur Speicherung der IP-Adressen jedenfalls nicht aus den §§ 113 a, 113 b TKG ergibt.

101 Auf Grund der unter anderem zum Aktenzeichen 1 BvR 256/08 ergangenen Entscheidung des Bundesverfassungsgerichts vom 2.03.2010 (abgedruckt in NJW 2010, 833 ff) steht vielmehr fest, dass die mit Wirkung zum 1.01.2008 in Kraft getretenen §§ 113 a, 113 b TKG, die im staatlichen Interesse unter anderem eine auch die Beklagte verpflichtende Regelung zur Vorratsspeicherung für sechs Monate enthalten, gegen die Verfassung der Bundesrepublik Deutschland verstoßen und nichtig sind. Die Beklagte ist folglich nicht etwa im Interesse des Staates gehalten, die vorliegend streitgegenständlichen IP-Adressen für sechs Monate zu speichern.

102 3.) Der Kläger kann sich im Zusammenhang mit dem von ihm verfolgten Anspruch auf „sofortige“ Löschung der seinen Rechnern für die einzelnen Internetverbindungen jeweils zugeteilten IP-Adressen *nicht* auf §§ 97 III, 96 I 3 TKG berufen.

103 Nach § 97 I 1 TKG (in der ab dem 1.01.2008 gültigen Fassung) dürfen Diensteanbieter die in § 96 Abs. 1 TKG (in der ab dem 23.02.2010 gültigen Fassung) aufgeführten „Verkehrsdaten“ verwenden, soweit die Daten zur Ermittlung des Entgelts und zur Abrechnung mit ihren Teilnehmern benötigt werden. Nach § 97 II Ziffer 1 TKG dürfen die Diensteanbieter zur ordnungsgemäßen Ermittlung und Abrechnung der Entgelte für ihre Telekommunikationsdienste und zum Nachweis der Richtigkeit derselben neben sonstigen für die Entgeltabrechnung erheblichen Umstände unter anderem die „Verkehrsdaten“ nach § 96 Abs. 1 TKG erheben und verwenden; und zwar nach der Maßgabe der Absätze 3 bis 6 des § 97 TKG. Das hat gemäß § 97 III TKG zur Folge, dass Diensteanbieter „nach Beendigung der Verbindung aus den „Verkehrsdaten“ nach § 96 Abs. 1 Nr. 1 bis 3 und 5 TKG unverzüglich die für die Berechnung des Entgelts erforderlichen Daten zu ermitteln“ und zu trennen haben. Die in diesem Sinne erforderlichen Daten – und nur diese – dürfen nach dem gesetzlichen Erlaubnistatbestand bis zu sechs Monate nach der Versendung der Rechnung gespeichert werden. Demgegenüber sind die für „die Abrechnung nicht erforderliche Daten unverzüglich zu löschen, soweit sie nicht nach § 113 a TKG“ (etwa in einer zukünftige und verfassungsgemäßen Fassung) „zu speichern sind.“

104 Davon, dass es sich bei den streitgegenständlichen IP-Adressen um „Verkehrsdaten“ im Sinne der genannten Bestimmungen handelt, geht nicht nur das Verfassungsgericht in seiner vielbeachteten Entscheidung vom 2.03.2010 (abgedruckt in NJW 2010, 833 ff; vgl. dort Rd. 168, 189, 211) ohne Weiteres aus. Dies darf inzwischen auch als allgemein anerkannt bezeichnet werden (vgl.: EuGH in GRUR 2009, 579; OGH Wien in NJOZ 2010, 675; OLG Karlsruhe in MMR 2009, 412 sowie in GRUR-RR 2009, 379; OLG Köln in GRUR-RR 2009, 9; OLG Zweibrücken in GRUR-RR 2009, 12; Hanseat. OLG Hamburg, Urteil vom 17.02.2010 zum Aktz. 5 U 60/09, veröffentlich in juris, Das Rechtsportal; LG Frankenthal in MMR 2008, 687; LG München in MMR 2010, 111 m. w. N.; Landgericht Hamburg in MMR 2009, 570; die als Blatt 384 ff zu den Akten genommene Stellungnahme des Bundesbeauftragten für Datenschutz vom 7.04.2005; vgl. ferner Nr. 15 der Erwägungen sowie Art 2 b und Art 6 der Richtlinie 2002/58/EG des Europäischen Parlamentes und Rates vom 12.07.2002; Lünenbürger in TKG-Kommentar von Scheuerle und Mayen, 2. Auflage, 2008, § 3 TKG, Rd. 81; Gramlich in Manssen, Telekommunikations- und Multimediarecht, lose Blattsammlung, Stand 6/2007, § 96 TKG, Rd. 30;). Was der Gesetzgeber unter „Verkehrsdaten“ verstanden wissen will, erschließt sich nicht zuletzt auch aus (der für nichtig erklärten) Bestimmung des § 113 a I, IV Ziffer 1 TKG a. F., in dem als ein zu speicherndes Verkehrsdatum die „Internetprotokoll-Adressen“ ausdrücklich erwähnt wird. Jede andere Würdigung würde auch den Definitionen der Begriffe „Bestandsdaten“ und „Verkehrsdaten“ in § 3 Ziffern 3 und 30 TKG sowie an der Tatsache vorbeigehen, dass nach § 96 I Ziffer 5 TKG unter „Verkehrsdaten“ auch die „zum Aufbau und zur Aufrechterhaltung der Telekommunikation … notwendigen Daten“ zu verstehen sind.

105 Auch vom Kläger ist diese rechtliche Einordnung der Internet-Protokoll-Adressen daher nicht ernsthaft in Zweifel gezogen.

106 a.) Soweit der Kläger die Auffassung vertritt, die seinen Rechnern jeweils zugeteilten IP-Adressen seinen in Anbetracht dieser gesetzlichen Regelung schon deshalb „sofort“ zu löschen, weil er mit der Beklagten einen Flatrate-Vertrag abgeschlossen habe, bei dem ein

pauschaliertes Entgelt zu entrichten sei, verkennt der Kläger bereits die Vielschichtigkeit seines Vertragsverhältnisses mit der Beklagten.

107 Immerhin ist zwischen den Parteien unstreitig geblieben, dass es sich bei Verträgen nach dem sogenannten „X dsl flat"-Tarif – und einen solchen hat der Kläger unstreitig mit der Beklagten abgeschlossen – um eine Kombination von Dienstleistungen handelt, die es dem jeweiligen Kunden ermöglicht, einen ...-Anschluss zu verwenden und sich über das Telekommunikationsnetz der Beklagten einzuwählen. Der jeweilige Kunde erhält dabei zwar einen Zugang für einen *Pauschalvertrag, wenn er eine ...-Verbindung für die Einwahl verwendet* . Die pauschale Vergütung über die sogenannte Flatrate gilt für den Internetzugang aber nur dann, wenn der Kunde den bereitgestellten ...-Anschluss nutzt, um sich einzuwählen. Ein ...-Kunde kann sich mit seinen Zugangsdaten (Kennung und Passwort) jedoch unstreitig auch über andere Telekommunikationsanschlüsse (z. B. über Mobiltelefone, aus dem Ausland oder über Wettbewerber der Beklagten im Inland) sowie über beliebige Zugangstechniken (analoge, ISDN- oder GSM-Verbindungen, W-Lan) in den Dienst der Beklagten einwählen. In diesem Fall werden besondere Nutzungsentgelte für die erbrachten Leistungen fällig. Auch für die Nutzung weiterer Sonderdienste, z. B. den Zugriff auf kostenpflichtige Inhalte anderer Anbieter oder SMS-Dienste, werden entsprechend der individuellen Nutzung gesondert und unabhängig von den angebotenen Zugangstarifen in Rechnung gestellt. Weiterhin können zusätzliche Kosten für die Einrichtung von Mitbenutzern entstehen; und zwar pro Mitbenutzer und unabhängig von der gewählten Zugangsart ein bestimmter Satz pro Minute und je Kennung pro Monat.

108 Bei diesen dem Kläger eröffneten Nutzungsmöglichkeiten ist es mithin möglich, dass sich im Einzelfall neben dem pauschalen Flatrate-Entgelt ein Anspruch der Beklagten auf ein Zusatzentgelt ergibt, welches die Beklagte folglich ermitteln können muss.

109 Die bisherige Nicht-Inanspruchnahme von entgeltpflichtigen Zusatzleistungen durch den Kläger und die von ihm zum Ausdruck gebrachte Absicht, diese Zusatzmöglichkeiten auch weiterhin nicht in Anspruch zu nehmen, rechtfertigt keine andere rechtliche Würdigung. Die Beklagte ist verpflichtet, dem Kläger die vertraglich geschuldeten Leistungen jederzeit umfassend zur Verfügung zu stellen. Der Kläger kann seine bisherige Handhabung und seine bisherige Absicht jederzeit aufgeben und sein vertragliches Recht in Anspruch nehmen. Die Beklagte muss daher im Rahmen des streitgegenständlichen X dsl flat"-Tarifs – wie gegenüber allen anderen Kunden mit solchen Verträgen – die auf Grund des Massengeschäftes notwendiger Weise automatisierte Möglichkeit haben, die Inanspruchnahme solcher Zusatzleistungen zu erfassen.

110 b) Der Kläger geht auch fehl in der Annahme, bei den dynamischen IP-Adressen handele es sich nicht um für die „Berechnung des Entgelts *erforderliche* Daten" im Sinne der §§ 96 I, 97 II Ziffer 1 TKG, weshalb sie nach der jeweiligen Beendigung der Internetverbindung „sofort" zu löschen seien.

111 Es ist zwischen den Parteien unstreitig geblieben, dass die für den Verbindungsaufbau zwingend nötige IP-Adresse den Zugang zum Internet und zu anderen Telediensten der Beklagten überhaupt erst ermöglicht. Es besteht zwischen den Parteien ferner kein Streit darüber, dass auf dem Radius-Server der Beklagten lediglich die jeweilige Kennung sowie das hinterlegte Passwort der einzelnen Teilnehmer und die der einzelnen Internetverbindung zugeordnete IP-Adresse gespeichert wird. Die Abrechnung erfolgt nicht etwa über den Radius-Server, der nicht einmal das von dem jeweiligen Teilnehmer gewählte Tarifmodell kennt. Zur Vorbereitung einer Abrechnung überträgt der Radius-Server der Beklagten deshalb die jeweiligen IP-Adressen und die diesen jeweils zugeordneten Session-Daten, nämlich unter anderem den verwendeten Zugangsweg und den Beginn und das Ende der Nutzung, in automatisierten Vorgängen und intervallmäßig auf eine sogenannte „OC-Plattform", wo die Daten – und zwar ohne dass Dritte eine Zugriffsmöglichkeit hätten – für das dezentrale Abrechnungssystem aufbereitet werden müssen. Erst danach werden die Daten an das dezentrale Abrechnungssystem übergeben.

112 Schon aus dieser unstreitigen Abfolge ergibt sich zwangsläufig, dass bei einer Löschung der IP-Adressen „sofort" nach der jeweiligen Beendigung der Internetverbindung eine Abrech-

nung überhaupt nicht möglich wäre. Demnach ist davon auszugehen, dass die Voraussetzungen des Erlaubnistatbestandes für eine zeitweise Speicherung gegeben sind.

113 Dass die Beklagte gleichwohl über technische Mittel verfügt, die es ihr ermöglichen könnten, auch ohne die zeitweise Speicherung von IP-Adresse abzurechnen, ist nicht zu erkennen und vom Kläger auch nicht einmal ansatzweise schlüssig dargelegt worden.

114 Die Behauptung des Klägers, die Beklagte verfüge über sogenannte „Log-Dateien", auf Grund derer sie auch ohne Rückgriff auf die IP-Adressen eine Abrechnung vollziehen könne, hat die Beklagte über ihre Schriftsätze vom 10.06.2003, 6.08.2003, 17.11.2006, 9.05.2007 und 31.05.2007 (vgl. Blatt 61 ff, 90 f, 301 ff, 376 f und 424 d. A.) und über ihre Ausführungen im Verhandlungstermin vom 16.05.2007 (Blatt 390 d. A.) nachvollziehbar und unter ausführlicher Beschreibung ihres Systems in Abrede gestellt. Der Kläger hat aus Anlass des genannten Verhandlungstermins vom 16.05.2007 zwar ausgeführt, er bestreite, dass es solchen Log-Dateien nicht gebe, er habe vielmehr „anderweitig erfahren" dass es sie gebe (Blatt 390 d. A.). Sein dahingehendes Vorbringen hat er allerdings nicht weiter vertieft. Mit Schriftsatz vom 21.05.2007 (vgl. Blatt 412 d. A.) hat der Kläger vielmehr nur geltend gemacht, die Existenz solcher „Log-Dateien" (wie auch immer der Kläger den Begriff definieren mag) „dürfte gerichtsbekannt sein", was aber gerade nicht der Fall ist.

115 Die Existenz von Log-Dateien, in denen über die sogenannten Session-Daten hinaus auch die Teilnehmer-Kennung abgespeichert wird, ergibt sich auch nicht etwa aus dem in erster Instanz eingeholten Gutachten des Dipl. Ing. SV1 vom 20.06.2006, der unter „log-Daten" nicht mehr und nicht weniger als Informationen über das Nutzerverhalten „in Form des mitgeschriebenen Ein- und Ausloggens" sieht und dies mit der „Herstellung einer Telefonverbindung" vergleicht (vgl. dort Seite 18). Solche Daten gibt es bei der Beklagten zweifelsohne, sie sind notwendige Bestandteile der sogenannten Session-Daten, ohne die eine Abrechnung nach dem jeweiligen Tarif letztlich nicht möglich ist. Es ist aber nach dem unwidersprochen gebliebenen Vorbringen der Beklagten gerade die streitgegenständliche IP-Adresse und nicht etwa die Kundenkennung, die die Beklagte in datenmäßiger Verknüpfung zusammen mit den Session-Daten speichert. Es ist nicht ersichtlich, dass es im System der Beklagten eine weitere Datensammlung, eine andersartige Log-Datei, gibt.

116 Wollte man die Beklagte also verpflichten, nach dem Ende der Internetverbindung die IP-Adresse „sofort" von den übrigen Session-Daten zu trennen und zu löschen, dann wäre eine Abrechnung für die Beklagte überhaupt nicht mehr möglich, weil keine sonstigen – auf den jeweiligen Teilnehmer bezogenen – Zuordnungsmöglichkeiten vorhanden wären.

117 Von daher ist es nicht zu beanstanden, dass die Beklagte die IP-Adressen nicht „sofort" löscht, sondern die entgeltlichen und die unentgeltlichen Datenbestandteile erst nach einer Verarbeitung der Daten durch die sogenannte OC-Plattform voneinander trennt.

118 Gegen diese Würdigung streitet auch nicht etwa das umstrittene Vorbringen des Klägers, etwa fünfzehn Internetzugangsanbieter (Internetprovider) löschten die IP-Adressen jeweils nach Beendigung der Session. Denn nach den unangegriffen gebliebenen Darlegungen der Beklagten ist davon auszugehen, dass diese Internetprovider, anders als die Beklagte, keine zusätzliche Dienstangebote vorhalten und sich in der Regel eines Telekommunikationsanbieters als Vorleister bedienen.

119 c.) Der Kläger verkennt überdies, dass ihm nach §§ 44 I, 96 I, 97 III TKG – wenn überhaupt – allenfalls ein Anspruch auf „ *unverzügliche* " Löschung und nicht etwa auf „ *sofortige* " Löschung zustehen könnte.

120 Dass der Gesetzgeber den Rechtsbegriff „unverzüglich" im Sinne von „ohne schuldhaftes Zögern" (vgl. § 121 BGB) verstanden und nicht mit „sofort" gleichgesetzt wissen will, ist allgemein anerkannt (vgl. statt vieler: Gramlich in Manssen, Telekommunikations- und Multimediarecht, lose Blattsammlung, Stand 6/2007, § 96 TKG, Rd. 38; Büttgen in TKG-Kommentar von Scheuerle und Mayen, 2. Auflage, 2008, § 96 TKG, Rd. 9; Eckhard in Recht der Medien, 2008, § 96 TKG, Rd. 6 – jeweils m. w. N.). Der streitgegenständliche Löschungsanspruch steht und fällt mithin mit der Frage, ob die Beklagte die Löschung schuldhaft verzögert.

121 Es hätte daher näherer Darlegungen des Klägers dazu bedurft, dass es der Beklagten bei entsprechendem technischen und wirtschaftlich verhältnismäßigen Aufwand überhaupt möglich ist, die IP-Adresse schneller zu löschen, dass sie also zum Zwecke einer sachgerechten Fakturierung und zur Vermeidung eines Datenverlustes nicht einmal für den inzwischen auf sieben Tage reduzierten Zeitraum auf die IP-Adresse zurückgreifen können muss. Diesbezügliche Anhaltspunkte sind dem Vorbringen des Klägers nicht zu entnehmen; er beruft sich vielmehr nur pauschal und ohne nähere Details darauf, die Beklagte müsse lediglich die Software abändern, um schneller löschen zu können.

122 Der Kläger ist insoweit auch darlegungs- und beweisbelastet, weil nach vorstehenden Ausführungen die Voraussetzungen eines Erlaubnistatbestandes gegeben sind. Wenn der Kläger der Auffassung ist, die Beklagte habe die Grenzen des Erlaubnistatbestandes überschritten und zögere schuldhaft bei der Löschung der Daten, dann ist er es, der dies schlüssig zu erläutern hat, damit seine Behauptung überhaupt einer Beweisaufnahme zugänglich wird.

123 Vor diesem Hintergrund kann dahingestellt bleiben, ob der nach vorstehenden Ausführungen unsubstanziierte Vorwurf eines „schuldhaften Zögerns“ auch deshalb unbegründet sein könnte, weil die Beklagte – im Sinne des den Datenschutz weithin durchziehenden Grundsatzes der Datensparsamkeit – bei der Datenverarbeitung zum Zwecke der Abrechnung nicht nur Schnelligkeit an den Tag legen muss.

124 Immerhin handelt sich bei der Beklagten vorgehaltenen Infrastruktur nicht nur um ausgesprochen komplexe Mechanismen; der Beklagten obliegt es im Sinne aller ihrer Teilnehmer nach § 109 TKG auch, „angemessene technische Vorkehrungen oder sonstige Maßnahmen“ zu treffen, die dem „Schutze des Fernmeldegeheimnisses und personenbezogener Daten“ sowie dem Schutz „der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe“ dienen. Die Beklagte muss mithin nicht nur einen möglichst umfangreichen Schutz der Zugangsmöglichkeiten und des Datenschutzes gewährleisten, sondern zugleich Schnelligkeitsanforderungen genügen. In Anbetracht dessen dürfte eine isolierte und von den übrigen Anforderungen losgelöste Betrachtung allein der Abrechnungsmechanismen kaum in Betracht kommen. Im Zweifel dürfte mithin nicht unberücksichtigt bleiben, dass die Beklagte auch bei der Einrichtung und Unterhaltung ihres Abrechnungssystems die Sicherheitsbedürfnisse der Gesamtheit ihrer Teilnehmer zu berücksichtigen hat. Die Beklagte hat insoweit unwidersprochen dargelegt, dass sie – wenn sie die IP-Adresse nicht mit den Session-Daten verknüpfen dürfte – die Benutzerkennung selbst mit den Session-Daten verknüpfen müsste, was mit einem ungleich größeren Eingriff in den Datenschutz der Teilnehmer verbunden wäre. Abgesehen davon muss es der Beklagten auch möglich sein, in geeigneter Weise ihre eigene Infrastruktur zu schützen.

125 Dass es bei der Prüfung der Berechtigung des Vorwurfs eines „schuldhaften Zögerns“ bei der Löschung von im Zusammenhang mit der Abrechnung erhobene Daten auch auf die Belange der Allgemeinheit der Teilnehmer und der Infrastruktur der Beklagten ankommen, liegt auch in Anbetracht der im Internet veröffentlichten Stellungnahme des Bundesbeauftragten für Datenschutz vom 16.03.2007 (vgl. Blatt 387 d. A.), des Bundeskriminalamtes in Wiesbaden aus dem Jahr 2003 (vgl. Blatt 98 ff d. A.), des Hessischen Landtages vom 11.12.2003 (vgl. Blatt 183 ff d. A.) und des Regierungspräsidenten in Darmstadt vom 14.01.2003 (vgl. Blatt 7 f d. A.) – mögen sie auch nicht in allen Einzelheiten nachvollziehbar sein – nicht fern.

126 Nicht zuletzt aus den Richtlinien 95/46/EG und 2002/58/EG des Europäischen Parlaments vom 24.10.1995 bzw.12.07.2002 (letztere in der Fassung der Änderungen vom 15.03.2006 und 25.11.2009) ergibt sich mit besonderer Deutlichkeit, dass die Dienstanbieter in Zusammenarbeit mit den Netzbetreibern geeignete Maßnahmen zu ergreifen haben, um den Datenschutz und die Netzsicherheit zu fördern.

127 Aus alldem folgt, dass der Kläger aus §§ 44 I, 96 I, 97 III TKG einen Anspruch auf „sofortige“ Löschung der IP-Adressen nicht ableiten kann.

128 Dabei verkennt der Senat nicht, dass sich die Basis der vorliegenden Entscheidung durch technische Entwicklungen, d. h. durch eine Verbesserung der technischen Möglichkeiten verändern kann. Der vorliegende Rechtstreit kann jedoch nur auf Grund der derzeitigen Stan-

dards und – was an dieser Stelle ebenfalls hervorzuheben ist – auf der Grundlage des wechselseitigen Vorbringens der Parteien des vorliegenden Rechtsstreits und nach dem im Zivilprozess geltenden Grundsatz der Parteimaxime und nicht etwa nach dem Grundsatz der Amtsermittlung entschieden werden.

129 4.) Darüber, dass sich eine Berechtigung der Beklagten zur automatisierten Speicherung von IP-Adressen für sieben Tage nach der Beendigung der Internetverbindung nicht aus § 96 I 3 TKG in Verbindung mit § 100 III TKG (in der ab dem 24.02.2007 gültigen Fassung) ergibt, besteht zwischen den Parteien zu Recht kein Streit.

130 Der Gesetzgeber hat die Anforderungen an die Erhebung und Verwendung von Verkehrsdaten zum Zwecke der Erkennung, Eingrenzung und Beseitigung von Störungen und Fehlern an Telekommunikationsanlagen (§ 100 I TKG) bzw. zum „Aufdecken sowie Unterbinden von Leistungserschleichungen und sonstigen rechtswidrigen Inanspruchnahmen der Telekommunikationsnetze und -dienste“ (§ 100 III TKG) im Rahmen der der Novellierung des § 100 TKG unterschiedlich ausgestaltet. Darauf, dass die strengeren Voraussetzungen einer Erhebung und Verwendung nach § 100 III TKG („bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte“) erfüllt sind, hat die Beklagte sich nicht berufen.

131 5.) Demgegenüber sind auch die Voraussetzungen des in §§ 96 I 3, 100 I TKG geregelten Erlaubnistatbestandes gegeben.

132 Danach darf der Diensteanbieter Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden, soweit dies „zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern der Telekommunikationsanlagen“ „erforderlich“ ist.

133 a.) Auf Grund der plausiblen und im Wesentlichen unstreitig gebliebenen Darlegungen der Beklagten kann davon ausgegangen werden, dass es der Beklagten bei einer „sofortigen“ Löschung der IP-Adressen derzeit praktisch unmöglich wäre, einen relevanten Teil von Störungen und Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen.

134 Gemeinsamer Zweck der einem Anbieter nach § 100 I TKG gestatteten datenschutzrechtlich relevanten Maßnahmen ist eine angemessene Reaktion und (so weit wie möglich) Abhilfe, um seine Dienste (weiter bzw. wieder) ordnungsgemäß erbringen zu können. Vor der eigentlichen Reaktion, der „Beseitigung“ von Störungen und Fehlern, müssen diese (und ihre Ursachen) erst einmal lokalisiert werden. Dies erfolgt regelmäßig in zwei (zusammenhängenden) Schritten; nämlich zunächst dem „Erkennen“, dass eine Anlage nicht (ordnungsgemäß) funktioniert, sodann dem „Eingrenzen“ der möglichen Ursachen auf bestimmte, und ggf. eine einzige (und damit verbundenen der Ausschluss zunächst ebenfalls in Betracht gezogener anderer Ursachen als irrelevant). Alle drei Maßnahmen-Schritte liegen im Interesse und in der Sphäre des Diensteanbieters. Dieser wird dabei tatsächlich oft auf eine Information oder auch Mitwirkung von Teilnehmern / Nutzern angewiesen sein, um überhaupt von Problemen zu erfahren (vgl. dazu Gramlich in Manssen, Telekommunikations- und Multimediarecht, lose Blattsammlung, Stand 6/2007, § 100 TKG, Rd. 18).

135 Der Dienstanbieter wird gleichwohl nicht generell ermächtigt, Daten zu erheben und zu verwenden. Das Gesetz gestattet ihm dies nur insoweit als dies zur Zielerreichung „erforderlich“ ist.

136 Was unter dem unbestimmten Rechtsbegriff „erforderlich“ zu verstehen ist, ist nach der einschlägigen Literatur und Rechtsprechung noch nicht abschließend geklärt. Der Senat schließt sich insoweit der Auffassung von Graf im Beck’schen Online-Kommentar (Stand 1.10.2009, zu § 100 TKG) an, der auf die im vorliegenden Verfahren ergangene landgerichtliche Entscheidung verweist und eine Speicherung von IP-Adressen für den Zeitraum von sieben Tagen für zulässig hält.

137 Darauf, dass die Phase des „Erkennens“ von Störungen und Fehlern nicht erst einsetzen darf, wenn sich Fehlfunktionen bereits eingestellt haben, hat Gramlich (in Manssen, Telekommunikations- und Multimediarecht, lose Blattsammlung, Stand 6/2007, § 100 TKG, Rd.

18) überzeugend hingewiesen. In der Phase des „Erkennens“ soll auch und gerade geklärt werden, ob sich eine Störungs- / und Fehleranzeige bestätigt (Gramlich a. a. O.). Selbst unter Berücksichtigung der unbestreitbaren Tatsache, dass § 100 I TKG nicht als Generalermächtigung zur Erhebung von Daten aufzufassen ist, kann doch in Anbetracht des unbestrittenen und plausiblen Vorbringens der Beklagten, wonach es teilweise mehrere Tage dauert, bis Störungsmitteilungen einzelner Teilnehmer bei ihr eingehen und verarbeitet werden können, eine „sofortige“ Löschung der IP-Adresse nicht in Betracht kommen. Sie würde es der Beklagten in Anbetracht der derzeitigen technischen Möglichkeiten schlechthin unmöglich machen, Störungsmeldungen auf den Grund zu gehen.

138 Da § 100 I TKG, anders als § 100 IV TKG, gerade keine im „Einzelfall“ feststehende Störung voraussetzt, und da sich aus den Erwägungen zur Richtlinie 2002/58/EG (vgl. dort Nr. 29) ergibt, dass „Verkehrsdaten“ in Bezug auf Teilnehmer und Nutzer in Einzelfällen verarbeitet“ werden dürfen, „um technische Versehen oder Fehler bei der Übertragung von Nachrichten zu ermitteln“, muss auch eine Zuordnung zu einzelnen Teilnehmern für einen überschaubaren Zeitraum möglich sein.

139 Dass diese Sichtweise sachgerecht ist, vertreten auch Wittern (in Beck’scher TKG-Kommentar, 2006, § 100 TKG, Rd. 2, 3) und Klesczewski (in Berliner Kommentar, 2006, § 100 TKG, Rd. 8 -10), weil beispielsweise bei sogenannten Denial of Services-Attacken oder erheblichem Spam-Aufkommen generelle Abwehrmechanismen erforderlich sind.

140 Die Beklagte hat weitere Störungen und Fehler beschrieben, die zu einschneidenden Funktionsbeeinträchtigungen bis hin zur totalen Sperre von einzelnen Nummernbereichen (vgl. die von der Beklagten beschriebenen Sperrungen im „C-Fall“ und durch das US-Patent- und Markenamt) führen können. Insoweit hat das Landgericht zutreffend ausgeführt, dass die Beklagte nachvollziehbar dargelegt hat, dass die Erkennung, Eingrenzung und Beseitigung dieser Störungen ohne die IP-Adresse und die dadurch überhaupt erst mögliche Zuordnung nicht denkbar wäre. Der Senat erlaubt sich zur Vermeidung von Wiederholungen die Bezugnahme auf die diesbezüglichen Ausführungen im angefochtenen Urteil (vgl. Blatt 433 ff d. A.).

141 Vor diesem Hintergrund kommt es letztlich nicht entscheidend auf die Frage an, ob in diesem Zusammenhang nicht auch potentielle Störungen in dem Fakturierungssystem der Beklagten, welches von den Radius-Servern der Beklagten getrennt ist, berücksichtigungsfähig sein könnten. Nur am Rande sei daher erwähnt, dass der Begriff der “Telekommunikationsanlagen“ in § 3 Ziffer 23 TKG zwar als „technische Einrichtungen oder Systeme“ definiert werden, „die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können“. Gleichwohl erscheint es zumindest nicht fern liegend, in dem Fakturierungssystem der Beklagten ein von der Telekommunikation untrennbares Annex-System zu sehen und dieses auch unter den Begriff der Telekommunikationsanlagen im Sinne des § 100 TKG zu subsumieren.

142 b.) Soweit es die Frage anbelangt, wann die Beklagte die nach vorstehenden Ausführungen berechtigter Weise erhobenen Verkehrsdaten wieder zu löschen hat, bedarf es auch hier der zwingend notwendigen Unterscheidung zwischen der vom Kläger vorliegend begehrten „sofortigen“ Löschung und der nach dem Gesetz bei fehlendem Bedürfnis „unverzüglichen“ vorzunehmenden Löschung. Hier gelten die vorstehenden Erwägungen entsprechend.

143 Auf Grund des wechselseitigen Vorbringens der Parteien ist nicht einmal ansatzweise zu erkennen, dass die Beklagte die in Absprache mit dem Bundesbeauftragten für Datenschutz für einen Zeitraum von sieben Tagen gespeicherten IP-Adressen bei gehöriger Anstrengung schneller löschen könnte und dann auch müsste. Ein schuldhaftes Zögern der Beklagten lässt sich im Rahmen des vorliegenden Zivilprozesses unter Zugrundelegung der Prozessmaxime nicht feststellen. Der Kläger, der sich freiberuflich als Informatiker betätigt, hat sich bis zuletzt (vgl. auch die Ausführungen im Schriftsatz vom 24.05.2010, Blatt 967 f d. A.) lediglich pauschal und ohne nähere Details darauf berufen, dass es „zumutbare technische Mittel zur unwiederbringlichen Anonymisierung von Datenbeständen (gebe), deren Einsatz gleichwohl die Nutzbarkeit der Daten“ im Sinne einer Netzsicherheit gewährleisten könnten. Dem entsprechenden Beweisangebot (Einholung eines Sachverständigengutachtens) war

nicht nachzugehen, weil es einer im Zivilprozess unstatthaften Erhebung eines Ausforschungsbeweises gleichkäme.

144 Nichts anderes ergibt aus dem umstrittenen Vorbringen des Klägers, etwa fünfzehn Internetzugangsanbieter (Internetprovider) löschten die IP-Adressen jeweils nach Beendigung der Session. Denn nach den unangegriffen gebliebenen Darlegungen der Beklagten halten diese Internetprovider, anders als die Beklagte, keine zusätzlichen Dienstangebote vor und bedienen sich in der Regel eines Telekommunikationsanbieters als Vorleister. Es ist die Beklagte, die für die meisten Internetzugangsanbieter in Deutschland als Vorleister tätig ist und als solcher auch über die wesentliche technische Infrastruktur verfügt, um Störungen oder Fehler zu erkennen, einzugrenzen und zu beseitigen. Es ist somit auch die Beklagte, die zu diesen Zwecken in den hier streitgegenständlichen Zeiträumen Daten speichern muss.

145 Nach Schluss der mündlichen Verhandlungen vom 26.05.2010 hat der Kläger einen Schriftsatz vom 27.05.2010 eingereicht, wegen dessen Wortlaut auf Blatt 986 – 987 der Akten verwiesen wird. Im Wesentlichen hat er darin einzelne Passagen aus einem Urteil des Amtsgerichts Darmstadt vom 30.06.2005 (Aktz. 300 C 397 / 04) und einem Urteil des Landgerichts Darmstadt vom 25.01.2006 (Aktz. 25 S 118 / 2005) wiedergegeben und geltend gemacht, die Sachverhalte deckten sich mit dem hier vorliegenden, was der Senat bei seiner Entscheidung bedenken möge. Unabhängig davon hat der Kläger geltend gemacht, in den X-AGB stehe nicht, dass der Gegenstand des Internetzugangs auch die Möglichkeit beinhalte, entgeltliche Telemediendienste in Anspruch zu nehmen; hierfür sei der Abschluss eines gesonderten Vertrages (Premium-Content) erforderlich.

146 Die zitierten Entscheidungen des Amtsgerichts Darmstadt vom 30.06.2005 und des Landgerichts Darmstadt vom 25.01.2006 hat der Senat bei seiner Entscheidungsfindung berücksichtigt. Sie rechtfertigen keine andere Würdigung. Der im Schriftsatz vom 27.05.2010 enthaltene Hinweis auf die X-AGB war nach § 156 ZPO nicht mehr zu berücksichtigen. Der Senat hat die mündliche Verhandlung am 26.05.2010 nach ausführlicher Erörterung des Sach- und Streitstandes geschlossen. Verfahrensfehler des Gerichts im Sinne des § 156 II Ziffer 1 ZPO sind nicht ersichtlich und werden auch nicht gerügt. Der Kläger, der in der mündlichen Verhandlung keinen Schriftsatznachlass beantragt hat, hat auch keinen Wiederaufnahmegrund im Sinne der §§ 156 II Ziffer 2, 579, 580 ZPO vorgetragen.

147 Unabhängig davon sind die X-AGB (anders als die unstreitige Leistungsbeschreibung Blatt 362 f d. A.) von den Parteien auch zu keinem Zeitpunkt zum Bestandteil der Akten gemacht worden; und zwar obwohl das Landgericht um Vorlage der Vertragsunterlagen gebeten hatte (siehe Seite 3 des angefochtenen Urteils und Seite 2 des Verhandlungsprotokolls vom 16.05.2007, vgl. Blatt 429 und Blatt 389 d. A.).

148 Nach alldem ist die teilweise Zurückweisung des Klageantrages zu 1) durch das Landgericht nicht zu beanstanden und die Berufung mit der sich aus § 97 I ZPO ergebenden Kostenfolge zurückzuweisen.

149 Die Entscheidung zur vorläufigen Vollstreckbarkeit findet ihre Rechtsgrundlage in §§ 708 Ziffer 11, 711, 709 S. 2 ZPO.

150 Der Senat hat die Revision zugelassen, weil die vorliegende Entscheidung (zumindest solange die für verfassungswidrig erklärten Regelungen der §§ 113 a, 113 b TKG nicht durch verfassungsgemäße Bestimmungen ersetzt worden sind) nicht nur von rechtspolitischer Bedeutung, sondern auch von grundsätzlicher Bedeutung im Sinne des § 543 II Ziffer 1 ZPO ist. Der Umfang und die Voraussetzungen eines datenschutzrechtlichen Unterlassungsanspruchs der vorliegenden Art sind bisher höchstrichterlich noch nicht geklärt.