BUNDESGERICHTSHOF

IM NAMEN DES VOLKES

URTEIL

III ZR 391/13

Verkündet am:
3. Juli 2014
K i e f e r
Justizangestellter
als Urkundsbeamter
der Geschäftsstelle

in dem Rechtsstreit

Der III. Zivilsenat des Bundesgerichtshofs hat auf die mündliche Verhandlung vom 3. Juli 2014 durch den Vizepräsidenten Schlick und die Richter Dr. Herrmann, Wöstmann, Seiters und Reiter

für Recht erkannt:

Die Revision des Klägers gegen das Urteil des 13. Zivilsenats in Darmstadt des Oberlandesgerichts Frankfurt am Main vom 28. August 2013 wird zurückgewiesen.

Die Kosten des Revisionsrechtszugs hat der Kläger zu tragen.

Von Rechts wegen

Tatbestand

1 Die Beklagte bietet Telekommunikationsleistungen an. Der Kläger ist Inhaber eines von ihr bereitgestellten DSL-Anschlusses. Hierfür haben er und die Rechtsvorgängerin der Beklagten ein zeit- und volumenunabhängiges Pauschalentgelt vereinbart.

2 Die Beklagte weist dem Rechner, den der Kunde zur Einwahl in das Internet nutzt, für die Dauer der einzelnen Verbindung eine IP-Adresse zu, die sie einem ihr zugeteilten Großkontingent entnimmt. Diese Adresse besteht aus einer mit einer Telefonnummer vergleichbaren, aus vier Blöcken gebildeten Ziffernfolge, die die Kommunikation vernetzter Geräte (z.B. Web-Server, E-Mail-

Server oder Privatrechner) ermöglicht. Nach Beendigung der Verbindung wird die jeweilige IP-Adresse wieder freigegeben und steht den Kunden der Beklagten zur Einwahl in das Internet erneut zur Verfügung. Aufgrund dieses Verfahrens erhält der einzelne Nutzer für jede Einwahl in das Internet in aller Regel eine unterschiedliche IP-Nummer (dynamische IP-Adresse).

3 Die Beklagte speichert nach Beendigung der jeweiligen Verbindung unter anderem die hierfür verwendete IP-Adresse für sieben Tage. Zuvor hatte sie für die Speicherung eine längere Zeitspanne in Anspruch genommen. Der Kläger meint, die Beklagte sei verpflichtet, die IP-Adressen sofort nach dem Ende der einzelnen Internetsitzungen zu löschen. Die Beklagte ist demgegenüber der Auffassung, sie sei zur Abwehr von Störungen und Fehlern an Telekommunikationsanlagen (§ 96 Abs. 1 Satz 2 i.V. m. § 100 Abs. 1 TKG) zu einer vorübergehenden Speicherung der IP-Adressen berechtigt. Aufgrund einer Änderung der technischen Voraussetzungen beruft sich die Beklagte inzwischen nicht mehr darauf, sie sei auch zum Zweck der Entgeltermittlung und -abrechnung (§ 97 Abs. 1 Satz 1, Abs. 2 TKG) für die Inanspruchnahme von Diensten, die ungeachtet des Pauschaltarifs kostenpflichtig seien, zur Speicherung befugt.

4 Neben Löschungs- und Unterlassungsansprüchen hinsichtlich weiterer Daten hat der Kläger die Verurteilung der Beklagten zur sofortigen Löschung der seinem Rechner zugeteilten IP-Adressen nach dem jeweiligen Ende der Internetverbindungen verfolgt. Das Landgericht hat den Anträgen teilweise stattgegeben, hinsichtlich der IP-Adressen die Beklagte jedoch nur verurteilt, diese sieben Tage nach dem jeweiligen Ende der Internetverbindungen zu löschen. Die hiergegen gerichtete Berufung des Klägers hat das Oberlandesgericht in einem ersten Urteil zurückgewiesen. Auf die Revision des Klägers hat der Senat diese Entscheidung mit Urteil vom 13. Januar 2011 (III ZR 146/10,

NJW 2011, 1509), auf das wegen der Einzelheiten Bezug genommen wird, aufgehoben und die Sache an die Vorinstanz zurückverwiesen. Das Oberlandesgericht hat nach Durchführung einer Beweisaufnahme die Berufung des Klägers wiederum zurückgewiesen. Hiergegen richtet sich die vom Berufungsgericht zugelassene erneute Revision des Klägers.

Entscheidungsgründe

5 Die zulässige Revision hat in der Sache keinen Erfolg.

I.

6 Das Berufungsgericht hat ausgeführt, unter Berücksichtigung der rechtlichen Vorgaben des ersten Revisionsurteils und der Ergebnisse der im zweiten Berufungsverfahren durchgeführten Beweisaufnahme sei die Beklagte zur Speicherung der dem jeweiligen Nutzer zugeteilten dynamischen IP-Adressen für einen Zeitraum von sieben Tagen nach dem Ende der jeweiligen Internetverbindungen gemäß § 100 Abs. 1 TKG befugt. Die in Rede stehende Datenerhebung und –verwendung sei geeignet, erforderlich und im engeren Sinne verhältnismäßig, um Gefahren für die Funktionsfähigkeit des Telekommunikationsbetriebs entgegenzuwirken. Die Identität des jeweiligen Internetbenutzers sei aus der IP-Nummer selbst nicht zu entnehmen. Sie sei erst durch die Zusammenführung mit weiteren Angaben zu ermitteln. Dies finde nach dem wechselseitigen Sachvortrag der Parteien nur bei dem konkreten Verdacht einer Störung oder eines Fehlers an den Telekommunikationsanlagen statt. Die Speicherung sei zudem auf einen sehr kurzen Zeitraum begrenzt. Die Interessen, de-

nen die Datenspeicherung diene, seien von erheblichem Gewicht. Soweit die IP-Nummern zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern notwendig seien, würde der Verzicht auf die von der Beklagten praktizierte Speicherung angesichts der gerichtsbekannten Häufigkeit von "Denial-of-Service-Attacken" und der Versendung von Spam-Mails, Schad- und Spionageprogrammen zu einer schwerwiegenden und nachhaltigen Beeinträchtigung der Kommunikationsinfrastruktur führen, und zwar zum Schaden der Beklagten und aller ihrer Kunden.

7 Nach den überzeugenden Angaben des vom Gericht beauftragten Sachverständigen gebe es jedenfalls nach dem derzeitigen Stand der Technik keine anderen Möglichkeiten als die von der Beklagten praktizierte Speicherung, um Störungen der Telekommunikationsanlagen zu erkennen, einzugrenzen und notfalls zu beseitigen. Der Sachverständige habe nachvollziehbar dargelegt, dass bei der Beklagten monatlich mehr als 500.000 Missbrauchs-(Abuse-)Meldungen eingingen, von denen 162.000 im Zusammenhang mit Spams stünden. 164.000 hätten einen potentiell direkten Einfluss auf die Infrastruktur und die Dienste der Beklagten. Daneben gebe es Abusemeldungen zu anderen Arten von Missbräuchen (Schadcodes auf Webseiten, Hacking und dergleichen). Der Sachverständige habe in sich stimmig und nachvollziehbar erläutert, dass das von der Beklagten entwickelte System zur Abwehr dieser Beeinträchtigungen erforderlich sei und beibehalten werden müsse. Es habe auch dazu geführt, dass es kaum Fälle gegeben habe, in denen ein anderes Telekommunikationsunternehmen einen bestimmten Adressraum der Beklagten wegen von dort massenhaft ausgehender Spams mit der Folge gesperrt habe, dass aus dem Adressbereich kommende Nachrichten überhaupt nicht mehr angenommen worden seien.

8 Der gerichtlich bestellte Sachverständige habe neben der grundsätzlichen Sinnhaftigkeit der Verfahrensweise der Beklagten auch geprüft, ob Veränderungen denkbar seien, mit Hilfe derer die Speicherung der IP-Adressen für sieben Tage überflüssig werden könnte und ob entgegen der vom Bundesbeauftragten für Datenschutz und Informationsfreiheit geteilten Auffassung der Beklagten zumindest der Speicherzeitraum verkürzt werden könnte. Danach scheide aber insbesondere die vom Sachverständigen angesprochene und theoretisch bestehende Möglichkeit der sogenannten Pseudonymisierung, bei der die IP-Adresse nicht gespeichert würde, aus. Zwar wäre es bei diesem Verfahren möglich, die Kundenkennung nicht mit der IP-Adresse, sondern einer zusätzlichen Zeichenkette zu verknüpfen, die nicht automatisch einem bestimmten Kunden zuzuordnen wäre. Die Pseudonymisierung müsste aber in jedem einzelnen Fall des § 100 Abs. 1 TKG wieder aufgehoben werden, wozu eine vertrauenswürdige Stelle angerufen werden müsste. Der Sachverständige habe nachvollziehbar und unwidersprochen dargelegt, dass der damit verbundene Mehraufwand angesichts der Vielzahl der Fälle, die monatlich abzuwickeln seien, in der Praxis nicht vertretbar sei.

II.

9 Dies hält den Angriffen der Revision stand.

10 1. Gegen die auf der Grundlage der Ausführungen des Sachverständigen getroffenen tatsächlichen Feststellungen des Berufungsgerichts erhebt die Revision weder zum Verfahren noch in der Sache Rügen. Hierfür hätte auch keine Veranlassung bestanden.

11 2. Unbehelflich für den geltend gemachten Anspruch, die jeweils dem Kläger zugeteilte IP-Nummer nach Beendigung der einzelnen Verbindung in das Internet zu löschen, ist der Hinweis der Revision auf die vom Sachverständigen kursorisch angesprochene Möglichkeit der "Pseudonymisierung", die die Beklagte entgegen der Annahme des Berufungsgerichts nicht generell, sondern allein für den Kläger vornehmen könne.

12 Bei diesem Verfahren soll die Kundenkennung nicht mit der für die Internetverbindung genutzten IP-Adresse verknüpft werden, sondern mit einer anderen anonymen Zeichenfolge. Im Fall des Verdachts eines Missbrauchs würde die Zuordnung dieser Kennung zu den Daten des Nutzers - im Gegensatz zur Praxis der Beklagten - nicht automatisch, sondern durch eine neutrale Stelle erfolgen. Allerdings ist auch die - zudem dynamisch, das heißt ständig wechselnden Anschlüssen zugeteilte - IP-Nummer für sich genommen anonym, wie das Berufungsgericht vom Kläger unbeanstandet festgestellt hat. Ihre Zuordnung zu einem Kunden wird erst durch die Verknüpfung mit den Sessionsdaten des Nutzers ermöglicht. Insoweit unterscheidet sich das derzeitige Verfahren der Beklagten letztlich nicht von der vom Sachverständigen angeschnittenen "Pseudonymisierung". Der mit dieser bewirkte Gewinn an Datenschutz würde dementsprechend maßgeblich nicht infolge der Ersetzung der IP-Adresse durch eine andere Zeichenfolge bewirkt, sondern wäre darauf zurückzuführen, dass eine automatische Verknüpfung der anonymen Zeichenfolge (gleichgültig, ob IP-Adresse oder andere Kennung) durch die Beklagte selbst unterbleibt und stattdessen eine dritte Stelle zwischengeschaltet würde, die die Rückgängigmachung der Pseudonymisierung vornähme. Dies ist jedoch, wie das Berufungsgericht auf der Grundlage der Ausführungen des Sachverständigen von der Revision unbeanstandet festgestellt hat, angesichts der hohen Zahl der Vorfälle der Beklagten nicht zuzumuten. Der Kläger kann dem auch nicht mit Erfolg

entgegenhalten, die Einschaltung der dritten Stelle könne auf seine Person oder seinen Anschluss beschränkt werden. Die Beklagte wäre rechtlich allen anderen Kunden gegenüber verpflichtet, ebenso zu verfahren wie gegenüber dem Kläger.

13 3. Im Übrigen tritt die Revision der Rechtsauffassung des Senats in seinem ersten Revisionsurteil in dieser Sache vom 13. Januar 2011 (aaO) entgegen. Auch unter Berücksichtigung der vom Kläger vorgebrachten Angriffe hält der Senat nach Überprüfung jedoch an seinem Rechtsstandpunkt fest.

14 a) Zu Unrecht meint die Revision unter Bezugnahme auf Randnummer 24 des Urteils vom 13. Januar 2011, der Begriff der "Störung" an Telekommunikationsanlagen im Sinne des § 100 Abs. 1 TKG umfasse entgegen der Ansicht des Senats nicht die Sperrung einzelner IP-Adresskontingente der Beklagten durch andere Internetanbieter, wenn von diesen Bereichen aus Schadprogramme, sogenannte Spam-Mails oder "Denial-of-Service"-Attacken ausgingen. Sie meint, "System" im Sinne der Definition des Begriffs der Telekommunikationsanlagen in § 3 Nr. 23 TKG sei nur ein technisches System. Werde ein bestimmter IP-Adressbereich gesperrt, werde die Telekommunikationsanlage der Beklagten selbst nicht gestört. Das System laufe in diesem Fall unbeeinträchtigt weiter. Die betroffenen Adressenkontingente könnten an dem System weiter teilnehmen, nur nicht im Verhältnis zu dem sperrenden anderen Internetdienstleister, der sie infolge seiner geschäftspolitischen Entscheidung nicht mehr bedienen wolle.

15 Dies kann nicht überzeugen. Daraus, dass sich das Adjektiv "technische" in § 3 Nr. 23 TKG auch auf den Begriff des "Systems" bezieht, ist für die Rechtsposition des Klägers nichts herzuleiten. Wie die Revision selbst nicht

verkennt, kommt eine Störung des "technischen Systems" nach § 100 Abs. 1 TKG nicht nur in Betracht, wenn die physikalische Beschaffenheit der für die Telekommunikation verwendeten Gerätschaften verändert wird. Vielmehr liegt nach dem Zweck der Vorschrift eine Störung des Systems auch vor, wenn die eingesetzte Technik die ihr zugedachten Funktionen nicht mehr richtig oder vollständig erfüllen kann (Gramlich in Manssen, Telekommunikations- und Multimediarecht, C § 100 Rn. 16 [Stand: 8/08]; Kannenberg in Scheurle/Mayen, TKG, 2. Aufl., § 100 Rn. 6 f; Mozek in Säcker, TKG, 3. Aufl., § 100 Rn. 7). Entgegen der Ansicht der Revision tritt eine Funktionseinschränkung des technischen Systems der Beklagten auch dann ein, wenn einzelne ihrer IP-Nummernbereiche von anderen Internetdiensten gesperrt werden. In diesem Fall sind die von diesen Anbietern unterhaltenen Web- und Mailserver für die Kunden der Beklagten nicht mehr erreichbar. Damit können deren technischen Einrichtungen und Systeme nicht mehr ihre Aufgabe erfüllen, den Nutzern den uneingeschränkten Zugang zu sämtlichen öffentlichen Angeboten im Internet zu verschaffen, wozu sich die Beklagte gegenüber ihren Kunden verpflichtet. Unmaßgeblich ist, dass die bei der Versendung von Schadprogrammen, Spams und dergleichen aus dem Netz der Beklagten drohende Sperrung ihrer IP-Kontingente durch andere Anbieter auf deren autonomer Entscheidung beruht. Die Blockierung der Nummernbereiche wird in diesen Fällen durch die aus der technischen Sphäre der Beklagten stammenden Missbräuche des Internets herausgefordert und stellt in der Regel eine verständliche und angemessene Reaktion der anderen Dienstanbieter zum Schutz ihrer Anlagen und Nutzer dar.

16 b) Nicht zu folgen vermag der Senat der Revision auch, soweit sie sich die an dem Senatsurteil vom 13. Januar 2011 (aaO) geäußerte Kritik von Braun (Beck‘ scher TKG-Kommentar, 4. Aufl., § 100 Rn. 10 f mwN; siehe aber dem-

gegenüber z.B. auch Eckhardt, DSB 2011, 22, 23 f; Karg, MMR 2011, 345, 346) zu eigen macht.

17 In methodischer Hinsicht beanstandet er, die vom Senat in Randnummer 24 des Urteils zum Beleg für sein weites Verständnis des Störungsbegriffs des § 100 Abs. 1 TKG angeführte Begründung der Bundesregierung zur Ergänzung von § 15 TMG (BT-Drs. 16/11967, S. 17) sei nicht aussagekräftig, weil die vorgesehene Gesetzesänderung nicht erfolgt sei. Dies hat der Senat indessen berücksichtigt, wie in seiner Formulierung "durch den eine mit § 100 Abs. 1 TKG fast wortgleiche Bestimmung an § 15 des Telemediengesetzes angefügt werden sollte" zum Ausdruck kommt. Es ist kein Grund dafür ersichtlich, dass die Begründung der von der Bundesregierung vorgeschlagenen, aber letztlich nicht zustande gekommenen Änderung des Telemediengesetzes keine Aussagekraft für die Auslegung von § 100 Abs. 1 TKG haben kann. Diese Bestimmung und der von der Bundesregierung vorgeschlagene Absatz 9 von § 15 TMG haben fast denselben Wortlaut. Zudem sind die Störungsszenarien, die beiden Vorschriften zugrunde liegen, vergleichbar. Auch wenn die Anbieter von Telemedien in stärkerem Maße von Spams, Denial-of-Service-Attacken, Schadprogrammen und dergleichen unmittelbar betroffen sein mögen als ein Teilnehmernetzbetreiber, können solche Missbräuche aus den im Senatsurteil vom 13. Januar 2011 (aaO) und oben unter Buchstabe a ausgeführten Gründen auch zu Störungen der Anlagen der Beklagten führen. Überdies haben nach den von der Revision hingenommenen tatrichterlichen Feststellungen monatlich etwa 164.000 bei der Beklagten auflaufende Missbrauchsmeldungen Angriffe zum Gegenstand, die sich potentiell unmittelbar schädlich auf die Infrastruktur und die Dienste der Beklagten auswirken.

18 Weiter wird geltend gemacht (Braun aaO), der Erwägungsgrund 29 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (ABl. L 201 S. 37; nachfolgend: RL) spreche gegen die vom Senat für richtig gehaltene weite Auslegung des Begriffs der "Störung" im Sinne von § 100 Abs. 1 TKG. Zudem sehe der Erwägungsgrund 29 die Verarbeitung von Verkehrs- und Bestandsdaten nur in Einzelfällen, nicht aber anlasslos, vor. Daher müsse § 100 Abs. 1 TKG über eine unionsrechtskonforme Auslegung entsprechend verstanden werden (aaO Rn. 12).

19 Diese Kritik ist bereits deshalb unbegründet, weil der im vorliegenden Fall zu entscheidende Sachverhalt von demjenigen, der in Erwägungsgrund 29 der genannten Richtlinie behandelt wird, nicht erfasst ist. Der Erwägungsgrund befasst sich allein mit der Verarbeitung von Verkehrsdaten, die (nur) in Einzelfällen erfolgen soll, um technische Versehen oder Fehler bei der Übertragung von Nachrichten zu ermitteln. Vorliegend steht jedoch die Berechtigung der Beklagten im Streit, auch ohne konkreten Anlass die von ihren Kunden genutzten IP-Adressen zu speichern. Die Speicherung und die Verarbeitung von personenbezogenen Daten sind Vorgänge, die in der Richtlinie unterschieden werden. Dies gilt insbesondere für Art. 6 Abs. 1 RL, der - vorbehaltlich der hier einschlägigen Maßgaben des Art. 15 Abs. 1 RL - die grundsätzliche Pflicht zur Löschung oder Anonymisierung der Verkehrsdaten nach der Übertragung von Nachrichten vorschreibt (siehe auch Erwägungsgrund 7 und Art. 4 Abs. 1a, zweiter Spiegelstrich RL).

20 Aber auch dessen ungeachtet geht die Beanstandung von Braun (aaO) fehl. Wie der Senat in seinem Urteil vom 13. Januar 2011 (aaO Rn. 33) ausge-

führt hat, wird § 100 Abs. 1 TKG von Art. 15 Abs. 1 RL gedeckt. Danach können die Mitgliedstaaten Vorschriften erlassen, die die Rechte und Pflichten gemäß Art. 6 RL beschränken, wenn dies unter anderem zur Verhütung, Ermittlung, Feststellung und Verfolgung des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen notwendig, angemessen und verhältnismäßig ist. Technische Versehen oder Fehler bei der Übertragung von Nachrichten (Erwägungsgrund 29 RL) können zwar zwei von mehreren denkbaren Folgen eines solchen Missbrauchs sein, können aber auch eine Fülle anderer Ursachen haben. Die dem Erwägungsgrund 29 und Art. 15 Abs. 1 RL jeweils zugrunde liegenden Sachverhalte überlappen sich damit nur teilweise. Die Anwendungsbereiche unterscheiden sich aber im Übrigen weitgehend, wie sich deutlich aus dem Wortlaut des Erwägungsgrunds und der Vorschrift ergibt. Für die von der Revision der Sache nach befürwortete einschränkende Auslegung von Art. 15 Abs. 1 RL und damit des Störungsbegriffs von § 100 Abs. 1 TKG im Lichte des Erwägungsgrunds 29 RL ist deshalb kein Raum.

21 4. Unbehelflich ist weiter der Hinweis des Klägers in seinem die Revisionsbegründung ergänzenden Schriftsatz vom 31. März 2014, eine Störung gemäß § 100 Abs. 1 TKG sei nicht deckungsgleich mit der in Art. 15 Abs. 1 RL enthaltenen Voraussetzung für die Beschränkungen von Art. 6 Abs. 1 RL, dass diese notwendig sind für die Verhütung, Ermittlung, Feststellung und Verfolgung des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen. Dies ist zwar rein begrifflich betrachtet richtig. Hieraus kann der Kläger jedoch inhaltlich nichts für seine Rechtsposition herleiten. Wie der Senat in seinem ersten Urteil ausgeführt hat, stellen die Missbräuche des Internets, die in der Versendung von Spam-Mails, Schad- und Spionageprogrammen sowie in "Denial-of-Service-Attacken" und dergleichen bestehen, einen unzulässigen Gebrauch elektronischer Kommunikationssysteme gemäß Art. 15 Abs. 1 RL dar (aaO Rn. 33)

dar. Derartige Missbräuche haben aus den in Randnummer 24 seines Urteils vom 13. Januar 2011 und oben unter Nummer 3 ausgeführten Gründen vielfach Störungen der Telekommunikationsanlagen des Netzbetreibers gemäß § 100 Abs. 1 TKG zur Folge. Ist die Ausnahme von der Löschungspflicht nach Art. 6 Abs. 1 RL bereits zur Verhütung, Ermittlung, Feststellung und Verfolgung von Missbräuchen der Kommunikationssysteme zulässig, muss dies erst Recht zum Erkennen, Eingrenzen oder Beseitigen von hieraus resultierenden Störungen der Telekommunikationsanlagen des Netzbetreibers im Sinne des § 100 Abs. 1 TKG gelten, zumal beides in der Praxis kaum zu unterscheiden ist. Der von der Revision geltend gemachte inhaltliche Widerspruch zwischen Art. 15 Abs. 1 RL und § 100 Abs. 1 TKG besteht damit nicht.

22 5. Schließlich gibt auch das Urteil des Gerichtshofs der Europäischen Union vom 8. April 2014 (C-293/12 u.a. - Digital Rights Ireland Ltd. u.a., BeckRS 2014, 80686), mit dem die Ungültigkeit der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. Nr. L 105 S. 54) ausgesprochen wurde, dem Senat keinen Anlass, seinen im ersten Revisionsurteil vom 13. Januar 2011 (aaO) eingenommenen Rechtsstandpunkt zu revidieren. Maßgeblich für die Ungültigkeit dieser Richtlinie, die eine anlasslose Vorratsspeicherung von Verkehrs- und Bestandsdaten für mindestens sechs Monate vorsah, war nach der Entscheidung des Gerichtshofs das Fehlen eines objektiven Kriteriums, das es ermöglichte, den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung zwecks Verhütung und Verfolgung von Straftaten auf solche Delikte zu beschränken, die unter Berücksichtigung des Ausmaßes und der Schwere des Grundrechtseingriffs als hinrei-

chend schwer angesehen werden konnten, um den Eingriff zu rechtfertigen (aaO Rn. 60). Weiterhin monierte der Gerichtshof, dass die Richtlinie keine materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den gespeicherten Daten und deren spätere Nutzung enthielt. Es fehle eine ausdrückliche Bestimmung, dass sich der Zugang zu den und die spätere Nutzung der Daten strikt auf die Zwecke der Verhütung und der Verfolgung genau abgegrenzter schwerer Straftaten beschränke (aaO Rn. 61). Vor allem unterliege der Zugriff der nationalen Behörden zu den auf Vorrat gespeicherten Daten keiner vorherigen Kontrolle eines Gerichts oder einer anderen unabhängigen Stelle, deren Entscheidung die Wahrung der Verhältnismäßigkeit gewährleiste (aaO Rn. 62). Schließlich beanstandete der Gerichtshof, dass die Mindestspeicherfrist für sämtliche Datenkategorien sechs Monate betragen sollte, ohne dass die Festlegung auf objektiven Kriterien beruhte, die gewährleisteten, dass sie auf das absolut Notwendige beschränkt wurde (aaO Rn. 63 f).

23 Diese Erwägungen sind auf die hier im Streit befindliche siebentägige Speicherung von IP-Adressen zu den in § 100 Abs. 1 TKG bestimmten Zwecken nicht übertragbar. Die Speicherung erfolgt nicht für die Zwecke der Strafverfolgungsbehörden, sondern im Interesse des Netzbetreibers. Ein Zugriff von Polizei oder Staatsanwaltschaft auf die gespeicherten Daten ist in dieser Rechtsgrundlage nicht vorgesehen. Überdies ist die Speicherfrist von sieben Tagen nach den aufgrund sachverständiger Beratung getroffenen, nicht angegriffenen tatrichterlichen Feststellungen auf das zur Erreichung der legitimen Zwecke des § 100 Abs. 1 TKG notwendige Maß begrenzt. Sie ist auch ihrer absoluten Dauer nach nicht mit der in der genannten Richtlinie bestimmten Mindestfrist von sechs Monaten vergleichbar.

24 6. Eine Vorlage der Sache an den Gerichtshof der Europäischen Union gemäß Art. 267 Abs. 2, 3 AEUV ist auch weiterhin entbehrlich. Insoweit nimmt der Senat auf sein erstes Revisionsurteil in dieser Sache (aaO Rn. 35) Bezug. Die in der vorliegenden Entscheidung ergänzend angestellten Erwägungen zum europäischen Recht ergeben sich ebenfalls ohne weiteres mit der zur Anwendung der acte clair-Doktrin (siehe dazu Senatsurteil vom 13. Januar 2011 aaO mwN) erforderlichen Eindeutigkeit aus dem Wortlaut des Art. 15 Abs. 1 RL und des Erwägungsgrunds 29 RL sowie aus dem Urteil des Gerichtshofs vom 8. April 2014 (aaO).

Schlick Herrmann Wöstmann

Seiters Reiter

Vorinstanzen:
LG Darmstadt, Entscheidung vom 06.06.2007 - 10 O 562/03 -
OLG Frankfurt in Darmstadt, Entscheidung vom 28.08.2013 - 13 U 105/07 -