BUNDESGERICHTSHOF

BESCHLUSS

VI ZR 135/13

vom

28. Oktober 2014

in dem Rechtsstreit

Nachschlagewerk: ja

BGHZ: nein

BGHR: ja

Richtlinie 95/46/EG (Datenschutz-Richtlinie) Art. 2 a, Art. 7 f; TMG §§ 12, 15

Dem Gerichtshof der Europäischen Union werden gemäß Art. 267 AEUV folgende Fragen zur Auslegung des Unionsrechts vorgelegt:

1. Ist Art. 2 Buchstabe a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Abl. EG 1995, L 281/31) Datenschutz-Richtlinie - dahin auszulegen, dass eine Internetprotokoll-Adresse (IP-Adresse), die ein Diensteanbieter im Zusammenhang mit einem Zugriff auf seine Internetseite speichert, für diesen schon dann ein personenbezogenes Datum darstellt, wenn ein Dritter (hier: Zugangsanbieter) über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt?

2. Steht Art. 7 Buchstabe f der Datenschutz-Richtlinie einer Vorschrift des nationalen Rechts entgegen, wonach der Diensteanbieter personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben und verwenden darf, soweit dies erforderlich ist, um die konkrete Inanspruchnahme des Telemediums durch den jeweiligen Nutzer zu ermöglichen und abzurechnen, und wonach der Zweck, die generelle Funktionsfähigkeit des Telemediums zu gewährleisten, die Verwendung nicht über das Ende des jeweiligen Nutzungsvorgangs hinaus rechtfertigen kann?

BGH, Beschluss vom 28. Oktober 2014 - VI ZR 135/13 - LG Berlin
AG Berlin-Mitte

Der VI. Zivilsenat des Bundesgerichtshofs hat am 28. Oktober 2014 durch den Vorsitzenden Richter Galke, die Richter Wellner, Stöhr und Offenloch und die Richterin Dr. Oehler

beschlossen:

I. Das Verfahren wird ausgesetzt.

II. Dem Gerichtshof der Europäischen Union werden gemäß Art. 267 AEUV folgende Fragen zur Auslegung des Unionsrechts vorgelegt:

1. Ist Art. 2 Buchstabe a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Abl. EG 1995, L 281/31) - Datenschutz-Richtlinie - dahin auszulegen, dass eine Internetprotokoll-Adresse (IP-Adresse), die ein Diensteanbieter im Zusammenhang mit einem Zugriff auf seine Internetseite speichert, für diesen schon dann ein personenbezogenes Datum darstellt, wenn ein Dritter (hier: Zugangsanbieter) über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt?

2. Steht Art. 7 Buchstabe f der Datenschutz-Richtlinie einer Vorschrift des nationalen Rechts entgegen, wonach der Diensteanbieter personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben und verwenden darf, soweit dies erforderlich ist, um die konkrete Inanspruchnahme des Telemediums durch den jeweiligen Nutzer zu ermöglichen und abzu-

rechnen, und wonach der Zweck, die generelle Funktionsfähigkeit des Telemediums zu gewährleisten, die Verwendung nicht über das Ende des jeweiligen Nutzungsvorgangs hinaus rechtfertigen kann?

Gründe:

A.

1 Der Kläger macht gegen die beklagte Bundesrepublik Deutschland einen Unterlassungsanspruch wegen der Speicherung von Internetprotokoll-Adressen (im Folgenden: IP-Adressen) geltend. IP-Adressen sind Ziffernfolgen, die vernetzten Computern zugewiesen werden, um deren Kommunikation im Internet zu ermöglichen. Beim Abruf einer Internetseite wird die IP-Adresse des abrufenden Computers an den Server übermittelt, auf dem die abgerufene Seite gespeichert ist. Dies ist erforderlich, um die abgerufenen Daten an den richtigen Empfänger zu übertragen.

2 Zahlreiche Einrichtungen des Bundes betreiben allgemein zugängliche Internetportale, auf denen sie aktuelle Informationen bereitstellen. Mit dem Ziel, Angriffe abzuwehren und die strafrechtliche Verfolgung von Angreifern zu ermöglichen, werden bei den meisten dieser Portale alle Zugriffe in Protokolldateien festgehalten. Darin werden jeweils der Name der abgerufenen Datei bzw. Seite, in Suchfelder eingegebene Begriffe, der Zeitpunkt des Abrufs, die übertragene Datenmenge, die Meldung, ob der Abruf erfolgreich war, und die IP-

Adresse des zugreifenden Rechners über das Ende des jeweiligen Nutzungsvorgangs hinaus gespeichert.

3 Der Kläger rief in der Vergangenheit verschiedene solcher Internetseiten auf. Mit seiner Klage begehrt er, die Beklagte zu verurteilen, es zu unterlassen, die IP-Adresse des zugreifenden Hostsystems des Klägers, die im Zusammenhang mit der Nutzung öffentlich zugänglicher Telemedien der Beklagten im Internet - mit Ausnahme eines bestimmten Portals, für das der Kläger bereits einen Unterlassungstitel erwirkt hat - übertragen wird, über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern oder durch Dritte speichern zu lassen, soweit die Speicherung nicht im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich ist. Das Amtsgericht hat die Klage abgewiesen. Auf die Berufung des Klägers hat das Berufungsgericht das erstinstanzliche Urteil unter Zurückweisung des weitergehenden Rechtsmittels teilweise abgeändert und die Beklagte verurteilt, es zu unterlassen, die IP-Adresse des zugreifenden Hostsystems des Klägers, die im Zusammenhang mit der Nutzung öffentlich zugänglicher Telemedien der Beklagten im Internet - mit Ausnahme eines Internetportals - übertragen wird, in Verbindung mit dem Zeitpunkt des jeweiligen Nutzungsvorgangs über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern oder durch Dritte speichern zu lassen, sofern der Kläger während eines Nutzungsvorgangs seine Personalien, auch in Form einer die Personalien ausweisenden E-Mail-Anschrift, angibt und soweit die Speicherung nicht im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich ist.

4 Gegen dieses Urteil haben beide Parteien die vom Berufungsgericht zugelassene Revision eingelegt. Der Kläger begehrt die Verurteilung der Beklagten ohne die vom Berufungsgericht ausgesprochenen Beschränkungen. Mit der

Revision verfolgt die Beklagte ihren Antrag auf vollständige Klageabweisung weiter.

B.

5 Die für die Entscheidung des Rechtsstreits maßgebenden Bestimmungen des deutschen Rechts lauten:

§ 12 Telemediengesetz (TMG)

6 (1) Der Diensteanbieter darf personenbezogene Daten zur Bereitstellung von Telemedien nur erheben und verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.

7 (2) Der Diensteanbieter darf für die Bereitstellung von Telemedien erhobene personenbezogene Daten für andere Zwecke nur verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.

8 (3) Soweit nichts anderes bestimmt ist, sind die jeweils geltenden Vorschriften für den Schutz personenbezogener Daten anzuwenden, auch wenn die Daten nicht automatisiert verarbeitet werden.

§ 15 Telemediengesetz (TMG)

9 (1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind insbesondere

1. Merkmale zur Identifikation des Nutzers,

2. Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und

3. Angaben über die vom Nutzer in Anspruch genommenen Telemedien.

10 (2) Der Diensteanbieter darf Nutzungsdaten eines Nutzers über die Inanspruchnahme verschiedener Telemedien zusammenführen, soweit dies für Abrechnungszwecke mit dem Nutzer erforderlich ist.

11 (3) Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

12 (4) Der Diensteanbieter darf Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verwenden, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind (Abrechnungsdaten). Zur Erfüllung bestehender gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen darf der Diensteanbieter die Daten sperren. ...

§ 3 Bundesdatenschutzgesetz (BDSG)

13 (1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). ...

C.

14 Das Berufungsgericht, dessen Urteil unter anderem in ZD 2013, 618 veröffentlicht ist, hat im Wesentlichen ausgeführt, analog § 1004 Abs. 1 Satz 2 BGB und gemäß § 823 BGB, Art. 1 Abs. 1, Art. 2 Abs. 1 GG, § 4 Abs. 1 BDSG, § 12 Abs. 1 TMG bestehe der geltend gemachte Unterlassungsanspruch nur insoweit, als er Speicherungen von IP-Adressen in Verbindung mit dem Zeitpunkt des jeweiligen Nutzungsvorgangs betreffe und der Kläger während eines Nutzungsvorgangs seine Personalien angebe.

15 In diesem Fall sei die dynamische IP-Adresse des Klägers in Verbindung mit dem Zeitpunkt des Nutzungsvorgangs ein personenbezogenes Datum. Die dazu erforderliche Bestimmbarkeit des Betroffenen sei relativ zu verstehen. Die Bestimmung der Person müsse gerade für die verarbeitende Stelle technisch und rechtlich möglich sein und dürfe keinen Aufwand erfordern, der außer Verhältnis zu dem Nutzen der Information für diese Stelle stehe. Danach sei in Fällen, in denen der Nutzer seinen Klarnamen offen lege, ein Personenbezug dynamischer IP-Adressen zu bejahen, weil die Beklagte den Klarnamen mit der IP-Adresse verknüpfen könne.

16 Die Verwendung des Datums über das Ende des Nutzungsvorgangs hinaus sei nach § 12 Abs. 1 TMG unzulässig, da nicht von einer Einwilligung des Klägers auszugehen sei und ein Erlaubnistatbestand nicht vorliege. § 15 Abs. 1 TMG greife jedenfalls deshalb nicht, weil die Speicherung der IP-Adresse über das Ende des Nutzungsvorgangs hinaus für die Ermöglichung des Angebots (für den jeweiligen Nutzer) nicht erforderlich sei. Der Begriff der Erforderlichkeit sei eng auszulegen und umfasse nicht den *sicheren* Betrieb der Seite. Ansonsten wäre die von der Bundesregierung zunächst beabsichtigte Einführung eines Erlaubnistatbestandes zwecks Abwehr von Angriffen zum Schutz der Systeme nicht erforderlich gewesen. § 5 BSIG sei nicht einschlägig, da die Beklagte die

Internetseiten nicht betreibe, um den Nutzern zur Kommunikation mit den jeweiligen Behörden zu dienen.

17 Ein weitergehender Unterlassungsanspruch bestehe nicht. Soweit der Kläger seinen Klarnamen nicht angebe, könne nur der Zugangsanbieter die IP-Adresse einem bestimmten Anschlussinhaber zuordnen. In den Händen der Beklagten sei die IP-Adresse hingegen - auch in Verbindung mit dem Zeitpunkt des Zugriffs - kein personenbezogenes Datum, weil der Anschlussinhaber bzw. Nutzer für die Beklagte nicht bestimmbar sei. Maßgeblich sei, dass der Zugangsanbieter die IP-Adressen nur für einen begrenzten Zeitraum speichern und nur in bestimmten Fällen an Dritte übermitteln dürfe. Dass die Beklagte im Zusammenhang mit einem strafrechtlichen Ermittlungsverfahren oder der Verfolgung von Urheberrechtsverletzungen unter bestimmten Voraussetzungen an die für die Herstellung des Personenbezugs erforderlichen Informationen gelangen könnte, sei unerheblich, weil das Interesse an der Verfolgung von Straftaten und Urheberrechtsverletzungen das Persönlichkeitsrecht des Betroffenen regelmäßig überwiege. Es komme auch nicht auf die theoretische Möglichkeit an, dass der Zugangsanbieter der Beklagten unbefugt Auskunft erteile. Denn eine illegale Handlung könne nicht als normalerweise und ohne großen Aufwand durchzuführende Methode angesehen werden.

D.

18 Gemäß Art. 267 Abs. 1 Buchstabe b und Abs. 3 AEUV ist von Amts wegen eine Vorabentscheidung des Gerichtshofs der Europäischen Union über die Auslegung des Art. 2 Buchstabe a und des Art. 7 Buchstabe f der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Da-

ten und zum freien Datenverkehr (Abl. EG 1995, L 281/31) - Datenschutz-Richtlinie - einzuholen, da davon der Erfolg bzw. Misserfolg der Revisionen der Parteien abhängt.

19 Der Kläger könnte von der Beklagten beanspruchen, es zu unterlassen, die für den Abruf ihrer Internetseiten durch den Kläger übermittelten IP-Adressen in Verbindung mit der Zeit des jeweiligen Abrufs über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern oder durch Dritte speichern zu lassen (mit Ausnahme eines Störfalles zur Wiederherstellung der Verfügbarkeit des Telemediums). Das setzt voraus, dass es sich bei dem Speichern der (hier allein in Frage stehenden dynamischen) IP-Adresse um einen nach dem Datenschutzrecht unzulässigen Eingriff in das allgemeine Persönlichkeitsrecht - in seiner Ausprägung als Recht auf informationelle Selbstbestimmung - des Klägers handelte (§ 1004 Abs. 1, § 823 Abs. 1 BGB i. V. mit Artt. 1 und 2 GG). Davon wäre auszugehen, wenn die IP-Adresse - jedenfalls zusammen mit dem Zeitpunkt des Zugriffs auf eine Internetseite - zu den "personenbezogenen Daten" im Sinne von Art. 2 Buchstabe a in Verbindung mit Erwägungsgrund 26 Satz 2 der Datenschutz-Richtlinie bzw. § 12 Abs. 1 und 3 TMG i. V. mit § 3 Abs. 1 BDSG zählte (I.) und ein Erlaubnistatbestand im Sinne von Art. 7 Buchstabe f der Datenschutz-Richtlinie bzw. § 12 Abs. 1 und 3, § 15 Abs. 1 und 4 TMG nicht vorläge (II.).

20 I. Zur Vorlagefrage II. 1.

21 1. Nach § 12 Abs. 1 TMG darf "der Diensteanbieter […] personenbezogene Daten zur Bereitstellung von Telemedien nur erheben und verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat." Diese Vorschrift ist anwendbar, da die in Rede stehenden Portale als Telemedien (§ 1

Abs. 1 Satz 1 TMG), die Beklagte als Diensteanbieter (§ 2 Satz 1 Nr. 1 TMG) und der Kläger als Nutzer (§ 11 Abs. 2 TMG) anzusehen sind.

22 2. Personenbezogene Daten sind nach der auch für das Telemediengesetz maßgeblichen (KG, K&R 2011, 418; Moos in Taeger/Gabel, BDSG, 2. Aufl., § 12 TMG Rn. 5) Legaldefinition in § 3 Abs. 1 BDSG "Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)." Die von der Beklagten gespeicherten dynamischen IP-Adressen sind jedenfalls im Kontext mit den weiteren in den Protokolldateien gespeicherten Daten als Einzelangaben über sachliche Verhältnisse anzusehen, da die Daten Aufschluss darüber gaben, dass zu bestimmten Zeitpunkten bestimmte Seiten bzw. Dateien über das Internet abgerufen wurden (vgl. Simitis/Dammann, BDSG, 8. Aufl., § 3 Rn. 10; Sachs, CR 2010, 547, 548). Diese sachlichen Verhältnisse waren solche des Klägers; denn er war Inhaber des Anschlusses, dem die IP-Adressen zugewiesen waren (vgl. BGH, Urteil vom 12. Mai 2010 - I ZR 121/08, BGHZ 185, 330 Rn. 15), und hat die Internetseiten im Übrigen auch selbst aufgerufen. Da die gespeicherten Daten aber aus sich heraus keinen unmittelbaren Rückschluss auf die Identität des Klägers zuließen, war dieser nicht "bestimmt" im Sinne des § 3 Abs. 1 BDSG (vgl. Schulz in Roßnagel, BeckRTD-Komm., § 11 TMG Rn. 22; Gola/Schomerus, BDSG, 11. Aufl., § 3 Rn. 10). Für den Personenbezug kommt es deshalb darauf an, ob er "bestimmbar" war.

23 a) Die Bestimmbarkeit einer Person setzt voraus, dass grundsätzlich die Möglichkeit besteht, ihre Identität festzustellen (Buchner in Taeger/Gabel, BDSG, 2. Aufl., § 3 Rn. 11; Plath/Schreiber in Plath, BDSG, § 3 Rn. 13). Umstritten ist, ob bei der Prüfung der Bestimmbarkeit ein objektiver oder ein relativer Maßstab anzulegen ist.

24 aa) Nach einer Auffassung kommt es auf die individuellen Verhältnisse der verantwortlichen Stelle nicht an (so etwa Pahlen-Brandt, K&R 2008, 286, 289; dies., DuD 2008, 34 ff.; Karg, MMR 2011, 345, 346; Schaar, Datenschutz im Internet, Kap. 3 Rn. 153, 174 f.; ähnlich Weichert in Däubler/Klebe/Wedde/ders., BDSG, 4. Aufl., § 3 Rn. 13, 15; vgl. auch Schweizer BVG, Urteil vom 27. Mai 2009 - A-3144/2008 - BeckRS 2009, 22471 unter J.2.2.1). Danach kann ein Personenbezug auch dann anzunehmen sein, wenn ausschließlich ein Dritter in der Lage ist, die Identität des Betroffenen festzustellen.

25 bb) Die überwiegende Auffassung vertritt demgegenüber einen relativen Ansatz. Ein Personenbezug ist danach zu verneinen, wenn die Bestimmung des Betroffenen gerade für die verantwortliche Stelle mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft verbunden ist, so dass das Risiko einer Identifizierung als praktisch irrelevant erscheint. Dies wird, da das Gesetz die Begriffe des Personenbezugs und des Anonymisierens komplementär verwendet, aus § 3 Abs. 6 BDSG hergeleitet (Simitis/Dammann, BDSG, 8. Aufl., § 3 Rn. 23, 196; Weichert in Däubler/Klebe/Wedde/ders., BDSG, 4. Aufl., § 3 Rn. 13; Moos in: Taeger/Gabel, BDSG, 2. Aufl., § 12 TMG Rn. 8; Mantz, ZD 2013, 625). Dies könnte bei einer entsprechenden Auslegung in Einklang stehen mit der Datenschutz-Richtlinie, nach deren Erwägungsgrund 26 bei der Beurteilung der Bestimmbarkeit alle Mittel berücksichtigt werden sollten, die "vernünftigerweise" eingesetzt werden könnten, um die betreffende Person zu bestimmen (Artikel-29-Datenschutzgruppe, WP 136 S. 15, www.ec.europa.eu/justice/data-protection/article-29; Buchner in Taeger/Gabel, aaO, § 3 BDSG Rn. 12; Simitis/Dammann, aaO Rn. 24).

26 cc) Stellte man mit dem relativen Ansatz auf die Kenntnisse, Mittel und Möglichkeiten der die IP-Adressen speichernden Stelle ab, könnten dieselben

Daten für eine Stelle - etwa für den Zugangsanbieter (vgl. EuGH, Slg. 2011, I-12006 Rn. 51 - Scarlet Extended) - personenbezogen und für eine andere Stelle - etwa für den Anbieter einer Internetseite (hier: die Beklagte) - nicht personenbezogen sein (so etwa LG Frankenthal, MMR 2008, 687, 689; LG Wuppertal, K&R 2010, 838, 839; AG München, K&R 2008, 767 m. zust. Anm. Eckhardt; ders., CR 2011, 339, 342 ff.; Meyerdierks, MMR 2009, 8, 10 ff.; Krüger/Maucher, MMR 2011, 433, 436 ff.; Simitis/Dammann, BDSG, 8. Aufl., § 3 Rn. 32 f.; Plath/Schreiber in Plath, BDSG, § 3 Rn. 14 f.; Gola/Schomerus, BDSG, 11. Aufl., § 3 Rn. 10; Bergmann/Möhrle/Herb, Datenschutzrecht, § 3 BDSG Rn. 32 [Stand: Januar 2012]; Spindler/Nink in Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl., § 11 TMG Rn. 5b; Moos in: Taeger/Gabel, BDSG, 2. Aufl., § 12 TMG Rn. 8; Schulz in Roßnagel, BeckRTD-Komm., § 11 TMG Rn. 23; Bizer/Hornung, ebd., § 12 TMG Rn. 44; Müller-Broich, TMG, § 11 Rn. 5; Schmitz in Hoeren/Sieber/Holznagel, Hdb. Multimedia-Recht, Kap. 16.2 Rn. 76 [Stand: Dezember 2009]; Härting, Internetrecht, 5. Aufl., Kap. B Rn. 276).

27 b) Für die Auslegung des nationalen Rechts (§ 12 Abs. 1 TMG) ist maßgebend, wie der Personenbezug in Art. 2 Buchstabe a der - diesen Bereich betreffenden - Datenschutz-Richtlinie zu verstehen ist.

28 aa) Der Wortlaut der Richtlinienbestimmung scheint nicht eindeutig zu sein. Nach dem Erwägungsgrund 26 Satz 2 der Richtlinie sollen bei der Entscheidung, ob eine Person bestimmbar ist, auch Mittel berücksichtigt werden, die "von einem Dritten" eingesetzt werden könnten, um die betreffende Person zu bestimmen. Das könnte so zu verstehen sein, dass der Personenbezug auch für einen Verantwortlichen, der eine Information lediglich speichert, schon dann zu bejahen ist, wenn ausschließlich ein Dritter, läge diesem die Information vor, den Betroffenen ohne unverhältnismäßigen Aufwand identifizieren könnte; je-

denfalls könnte ein Personenbezug dann anzunehmen sein, wenn vernünftigerweise nicht auszuschließen ist, dass die Information zukünftig an den Dritten übermittelt wird (vgl. Pahlen-Brandt, DuD 2008, 34, 38; Sachs, CR 2010, 547, 550 f.). Andererseits könnte ein solches Verständnis des Erwägungsgrundes nicht zwingend sein. Berücksichtigt man bei der Beurteilung der Bestimmbarkeit nur Mittel, die "vernünftigerweise" eingesetzt werden könnten, um die betreffende Person zu bestimmen (Artikel-29-Datenschutzgruppe, WP 136 S. 15, www.ec.europa.eu/justice/data-protection/article-29; Buchner in Taeger/Gabel, BDSG, 2. Aufl., § 3 BDSG Rn. 12; Simitis/Dammann, BDSG, 8. Aufl., § 3 Rn. 24), wäre auch ein relatives Verständnis der Bestimmbarkeit und damit des Personenbezugs möglich.

29 3. Die Frage ist im Streitfall entscheidungserheblich.

30 a) Folgt man dem objektiven Ansatz, so waren die dem Anschluss des Klägers zugewiesenen und von der Beklagten gespeicherten dynamischen IP-Adressen auch über das Ende der einzelnen Nutzungsvorgänge hinaus personenbezogen. Denn das Berufungsgericht hat angenommen, dass der Zugangsanbieter des Klägers die für dessen Identifizierung anhand der IP-Adressen erforderlichen Daten über das Ende der einzelnen Internetverbindungen hinaus gespeichert hat (zur Befugnis des Anbieters vgl. BGH, Urteile vom 13. Januar 2011 - III ZR 146/10, NJW 2011, 1509 und vom 3. Juli 2014 - VI ZR 391/13, NJW 2014, 2500). Mit diesem Zusatzwissen hätten die von der Beklagten gespeicherten Daten ohne unverhältnismäßigen Aufwand dem Kläger als Anschlussinhaber zugeordnet werden können.

31 b) Folgt man demgegenüber dem relativen Ansatz, so ist der Personenbezug im Streitfall zu verneinen. Denn die Stellen der Beklagten, die die IP-Adressen des Klägers gespeichert haben, hätten den Kläger nicht ohne unverhältnismäßigen Aufwand identifizieren können. Nach den getroffenen Feststel-

lungen ist davon auszugehen, dass ihnen - die Nichtangabe der Personalien vorausgesetzt - keine Informationen vorlagen, die dies ermöglicht hätten. Anders als es bei statischen IP-Adressen der Fall sein kann, lässt sich die Zuordnung dynamischer IP-Adressen zu bestimmten Anschlüssen keiner allgemein zugänglichen Datei entnehmen (Gerlach, CR 2013, 478, 480).

32 c) Der Zugangsanbieter des Klägers durfte den Stellen der Beklagten, welche die IP-Adressen speichern (sog. verantwortliche Stellen), keine Auskunft über dessen Identität erteilen, weil es dafür keine gesetzliche Grundlage gibt (§ 95 Abs. 1 Satz 3 TKG). Alleine die Befugnisse der zuständigen Stellen nach § 113 TKG (etwa die Staatsanwaltschaft im Rahmen eines Ermittlungsverfahrens) rechtfertigen es noch nicht, die auf Grund dieser Befugnisse beschaffbaren Informationen auch für andere staatliche Stellen (etwa die Stellen der Beklagten, welche die IP-Adressen speichern), an die diese Informationen nicht weitergegeben werden dürfen, als zugänglich anzusehen. Illegale Handlungen können - erst recht bei staatlichen Stellen - nicht als Mittel der Informationsbeschaffung angesehen werden.

33 II. Zur Vorlagefrage II. 2.

34 Wäre davon auszugehen, dass es sich bei der IP-Adresse im Zusammenhang mit den Daten des Zugriffs um personenbezogene Daten handelte, wäre die Speicherung über den Zugriff hinaus nach § 12 Abs. 1 TMG nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat. Eine solche Einwilligung liegt hier nicht vor. Es kommt aber eine Erlaubnis nach § 15 Abs. 1 TMG in Betracht. Auch insoweit ist eine Vorabentscheidung des Gerichtshofs der Europäischen Union über die Auslegung des Art. 7 Buchstabe f der Datenschutz-Richtlinie einzuholen.

35 1. Nach § 15 Abs. 1 TMG darf der Diensteanbieter personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind dabei insbesondere Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien.

36 a) Für die rechtliche Prüfung ist nach dem Vortrag der Beklagten davon auszugehen, dass die Speicherung der IP-Adressen zur Gewährleistung und Aufrechterhaltung der Sicherheit und Funktionsfähigkeit ihrer Telemedien erforderlich ist. Dies gilt insbesondere für die Erkennung und Abwehr häufig auftretender "Denial-of-Service"-Attacken, bei denen die TK-Infrastruktur durch gezieltes und koordiniertes Fluten einzelner Webserver mit einer Vielzahl von Anfragen lahm gelegt wird.

37 b) Fraglich ist, ob dadurch die Voraussetzungen des § 15 Abs. 1 TMG erfüllt sein können. Eine solche Auslegung wäre mit dem Wortlaut der Vorschrift vereinbar. Denn die behaupteten "Denial-of-Service"-Attacken führen dazu, dass das Telemedium nicht mehr erreichbar und seine Inanspruchnahme somit nicht mehr möglich ist. Wenn und soweit Maßnahmen des Diensteanbieters erforderlich sind, um solche Angriffe abzuwehren, könnten die Maßnahmen deshalb als erforderlich angesehen werden, "um die Inanspruchnahme von Telemedien zu ermöglichen" (vgl. Meyerdierks/Gendelev, ZD 2013, 626, 627).

38 c) In der Literatur wird allerdings überwiegend die Auffassung vertreten, dass die Datenerhebung und -verwendung nur erlaubt ist, um ein konkretes Nutzungsverhältnis zu ermöglichen und die Daten, soweit sie nicht für Abrechnungszwecke benötigt werden, mit dem Ende des jeweiligen Nutzungsvorgangs zu löschen sind. Dafür spricht insbesondere § 15 Abs. 4 Satz 1 TMG, der eine

Verwendung der Daten zu Abrechnungszwecken auch über das Ende des Nutzungsvorgangs hinaus ausdrücklich erlaubt und der im Fall einer weiten Auslegung des § 15 Abs. 1 TMG nur klarstellende Bedeutung hätte (vgl. Zscherpe in Taeger/Gabel, BDSG, 2. Aufl., § 15 TMG Rn. 32, 40; jurisPK-Internetrecht/Heckmann, 4. Aufl., Kap. 9 Rn. 362; Schmitz in Hoeren/Sieber/Holznagel, Hdb. Multimedia-Recht, Kap. 16.2 Rn. 204 [Stand: Dezember 2009]). Dieses Verständnis des § 15 Abs. 1 TMG würde einer Erlaubnis zur Speicherung der IP-Adressen zur (generellen) Gewährleistung und Aufrechterhaltung der Sicherheit und Funktionsfähigkeit von Telemedien entgegenstehen.

39 2. Da für das Verständnis des § 15 Abs. 1 TMG der diesen Bereich regelnde Art. 7 Buchstabe f der Datenschutz-Richtlinie maßgebend ist, stellt sich die Frage, wie diese Richtlinienbestimmung auszulegen ist.

40 a) Nach Art. 7 Buchstabe f der Datenschutz-Richtlinie ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie erforderlich ist zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Art. 1 Abs. 1 der Richtlinie geschützt sind, überwiegen. Nach dem Urteil des Europäischen Gerichtshofs vom 24. November 2011 in Sachen ASNEF und FECEMD (Slg. 2011, I-12181 Rn. 29 ff.) führt die Datenschutz-Richtlinie zu einer grundsätzlich umfassenden Harmonisierung der nationalen Rechtsvorschriften. Deshalb steht Art. 7 Buchstabe f der Datenschutz-Richtlinie hinsichtlich der Verarbeitung personenbezogener Daten jeder nationalen Regelung entgegen, die bei Fehlen der Einwilligung der betroffenen Person neben den beiden in der Vorschrift genannten kumulativen Voraussetzungen zusätzliche Erfordernisse aufstellt. Zwar dürfen

die Mitgliedstaaten in der Ausübung ihres Ermessens gemäß Art. 5 der Datenschutz-Richtlinie Leitlinien für die geforderte Abwägung aufstellen. Eine nationale Regelung darf jedoch nicht die Verarbeitung bestimmter Kategorien personenbezogener Daten ausschließen, indem sie für diese Kategorien das Ergebnis der Abwägung abschließend vorschreibt, ohne Raum für ein Ergebnis zu lassen, das auf Grund besonderer Umstände des Einzelfalls anders ausfällt (EuGH, aaO).

41 b) Nach diesen Maßstäben könnte das vom Berufungsgericht befürwortete enge Verständnis des § 15 Abs. 1 TMG nicht in Einklang mit Art. 7 Buchstabe f der Datenschutz-Richtlinie stehen (Drewes, ZD 2012, 115, 118; vgl. auch Meyerdierks/Gendelev, ZD 2013, 626, 627 und BGH, Urteil vom 4. Juni 2013 - 1 StR 32/13, BGHSt 58, 268 Rn. 70 ff.). Denn nach dieser Auslegung dürfte der Diensteanbieter personenbezogene Daten des Nutzers ohne dessen Einwilligung über das Ende des jeweiligen Nutzungsvorgangs hinaus nur zu einem bestimmten Zweck, nämlich dem der Abrechnung, verwenden; für andere Zwecke dürften die Daten nach Ende des Nutzungsvorgangs unabhängig von einer Abwägung der im Einzelfall berührten Interessen nicht verwendet werden.

42 c) Danach stellt sich die Frage, ob § 15 Abs. 1 TMG richtlinienkonform dahin ausgelegt werden muss, dass auch der von dem Diensteanbieter verfolgte Zweck, die Funktionsfähigkeit des Telemediums zu gewährleisten, die Verwendung personenbezogener Daten des Nutzers auch über das Ende des jeweiligen Nutzungsvorgangs hinaus rechtfertigen kann, wenn, soweit und solange die Verwendung zu diesem Zweck erforderlich ist.

43 3. Die Frage ist auch entscheidungserheblich.

44 Wenn nach der Entscheidung des Gerichtshofs zu Art. 2 Buchstabe a der Datenschutz-Richtlinie der Personenbezug der gespeicherten IP-Adressen zu bejahen sein sollte, könnte der Anspruch des Klägers gleichwohl entfallen, wenn der Erlaubnistatbestand des § 15 Abs. 1 TMG - bei einem von der Datenschutz-Richtlinie geforderten weiteren Verständnis - eingriffe.

Galke Wellner Stöhr

Offenloch Oehler

Vorinstanzen:
AG Berlin-Mitte, Entscheidung vom 13.08.2008 - 2 C 6/08 -
LG Berlin, Entscheidung vom 31.01.2013 - 57 S 87/08 -