Gericht:	BGH 6. Zivilsenat	**Quelle:**	
Entscheidungsdatum:	16.05.2017		
Rechtskraft:	ja	**Normen:**	§ 12 Abs 1 TMG, § 12 Abs 2 TMG, § 15 Abs 1 TMG, § 3 Abs 1 BDSG, § 4 Abs 1 BDSG, Art 2 Buchst a EGRL 46/95, Art 7 Buchst f EGRL 46/95, § 823 Abs 1 BGB, Art 1 Abs 1 GG, Art 2 Abs 1 GG
Aktenzeichen:	VI ZR 135/13		
Dokumenttyp:	Urteil	**Zitiervorschlag:**	BGH, Urteil vom 16. Mai 2017 – VI ZR 135/13 –, juris

Datenschutz im Internet: Dynamische IP-Adresse als personenbezogenes Datum; Zulässigkeit der Erhebung von personenbezogenen Daten eines Nutzers durch einen Anbieter von Online-Mediendiensten

Leitsatz

1. Die dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Internetseite, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, stellt für den Anbieter ein personenbezogenes Datum im Sinne des § 12 Abs. 1 und 2 TMG in Verbindung mit § 3 Abs. 1 BDSG dar (Fortführung von EuGH, 19. Oktober 2016, C-582/14, NJW 2016, 3579).(Rn.25)

2. § 15 Abs. 1 TMG ist entsprechend Art. 7 Buchst. f der Richtlinie 95/46 EG dahin auszulegen, dass ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung auch über das Ende eines Nutzungsvorgangs hinaus dann erheben und verwenden darf, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die generelle Funktionsfähigkeit der Dienste zu gewährleisten, wobei es allerdings einer Abwägung mit dem Interesse und den Grundrechten und -freiheiten der Nutzer bedarf (Fortführung von EuGH, 19. Oktober 2016, C-582/14, NJW 2016, 3579).(Rn.35)

Fundstellen

NSW TMG § 12 (BGH-intern)
NSW TMG § 15 (BGH-intern)
NSW BDSG § 3 (BGH-intern)
NSW Datenschutzrichtlinie Art. 2 (BGH-intern)
NSW Datenschutzrichtlinie Art. 7 (BGH-intern)
WM 2017, 1320-1324 (Leitsatz und Gründe)
DB 2017, 1645-1648 (Leitsatz und Gründe)
VersR 2017, 955-959 (Leitsatz und Gründe)
K&R 2017, 501-505 (Leitsatz und Gründe)
NJW 2017, 2416-2419 (Leitsatz und Gründe)
MDR 2017, 942-943 (Leitsatz und Gründe)
WRP 2017, 1100-1104 (Leitsatz und Gründe)

weitere Fundstellen

GRURPrax 2017, 333 (red. Leitsatz, Kurzwiedergabe)

Verfahrensgang

vorgehend BGH 6. Zivilsenat, 28. Oktober 2014, Az: VI ZR 135/13, EuGH-Vorlage
vorgehend LG Berlin 57. Zivilkammer, 31. Januar 2013, Az: 57 S 87/08, Urteil
vorgehend AG Tiergarten, 13. August 2008, Az: 2 C 6/08

Diese Entscheidung zitiert

Rechtsprechung
Fortführung EuGH 2. Kammer, 19. Oktober 2016, Az: C-582/14

Tenor

Auf die Revisionen der Parteien wird das Urteil der 57. Zivilkammer des Landgerichts Berlin vom 31. Januar 2013 aufgehoben.

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

Von Rechts wegen

Tatbestand

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, Cyber-Angriffe abzuwehren und die strafrechtliche Verfolgung von Angreifern zu ermöglichen und dadurch eine Abschreckungswirkung zu erreichen, werden bei einer Vielzahl 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.

4 Das Amtsgericht hat die Klage abgewiesen. Auf die Berufung des Klägers hat das Berufungsgericht das erstinstanzliche Urteil unter Zurückweisung des weitergehenden Rechtsmittels teilweise abgeändert. Es hat 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.

5 Gegen dieses Urteil haben beide Parteien die vom Berufungsgericht zugelassene Revision eingelegt. Der Kläger begehrt die Verurteilung der Beklagten ohne die vom Berufungsgericht aus-

gesprochenen Beschränkungen. Die Beklagte verfolgt ihren Antrag auf vollständige Klageabweisung weiter.

Entscheidungsgründe

I.

6 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.

7 In diesem Fall sei die dynamische IP-Adresse des Klägers ein personenbezogenes Datum. 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.

8 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.

9 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.

II.

10 Die Beurteilung des Berufungsgerichts hält revisionsrechtlicher Überprüfung nicht stand.

11 A) Revision des Klägers

12 Die Revision des Klägers hat Erfolg.

13 Nach den vom Berufungsgericht bisher getroffenen Feststellungen kann nicht ausgeschlossen werden, dass der Kläger von der Beklagten nach § 1004 Abs. 1 BGB analog, § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1 und Art. 1 Abs. 1 GG, § 4 Abs. 1 BDSG, § 12 Abs. 1 TMG beanspruchen

kann, 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. Bei dem Speichern der (hier allein in Frage stehenden dynamischen) IP-Adresse kann es sich um einen nach dem Datenschutzrecht unzulässigen Eingriff in das allgemeine Persönlichkeitsrecht des Klägers in seiner Ausprägung als Recht auf informationelle Selbstbestimmung handeln. Hierzu wird das Berufungsgericht weitere Feststellungen zu treffen haben.

14 1. Ein Unterlassungsanspruch scheitert nicht daran, dass die gespeicherten (dynamischen) IP-Adressen mangels Bestimmbarkeit des Anschlussinhabers für die Beklagte keine personenbezogenen Daten im Sinne von § 12 Abs. 1 TMG darstellen.

15 a) 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.

16 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.

17 b) 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)".

18 Die von der Beklagten gespeicherten dynamischen IP-Adressen des Klägers sind jedenfalls im Kontext mit den weiteren in den Protokolldateien gespeicherten Daten als Einzelangaben über sachliche Verhältnisse anzusehen, da die Daten Aufschluss darüber geben, 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 er rief die Internetseiten im Übrigen auch selbst auf. Da die gespeicherten Daten aus sich heraus keinen unmittelbaren Rückschluss auf die Identität des Klägers zuließen, war dieser zwar nicht "bestimmt" im Sinne des § 3 Abs. 1 BDSG (vgl. Schulz in Roßnagel, BeckRTD-Komm., § 11 TMG Rn. 22; Gola/Schomerus, BDSG, 12. Aufl., § 3 Rn. 10), er war jedoch "bestimmbar".

19 c) 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, 2. Aufl., § 3 Rn. 13). Umstritten war, ob bei der Prüfung der Bestimmbarkeit ein objektiver oder ein relativer Maßstab anzulegen ist (vgl. zum damaligen Meinungsstand Senatsbeschluss vom 28. Oktober 2014 - VI ZR 135/13, VersR 2015, 370 Rn. 23 ff.).

20 aa) Der erkennende Senat hat daher mit dem vorgenannten Beschluss dem Gerichtshof der Europäischen Union (im Folgenden: Gerichtshof) gemäß Art. 267 AEUV unter anderem folgende Frage zur Auslegung des Unionsrechts vorgelegt:

21 "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?"

22 bb) Der Gerichtshof hat mit Urteil vom 19. Oktober 2016 - C-582/14, NJW 2016, 3579 die Frage wie folgt beantwortet:

23 "Art. 2 Buchst. 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 ist dahin auszulegen, dass eine dynamische Internetprotokoll-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen."

24 Zur Begründung hat der Gerichtshof im Wesentlichen ausgeführt (aaO, Rn. 40 ff.), bereits aus dem Wortlaut von Art. 2 Buchst. a der Richtlinie 95/46 EG gehe hervor, dass nicht nur eine direkt identifizierbare, sondern auch eine indirekt identifizierbare Person als bestimmbar angesehen werde. Die Verwendung des Begriffs "indirekt" durch den Unionsgesetzgeber deute darauf hin, dass es für die Einstufung einer Information als personenbezogenes Datum nicht erforderlich sei, dass die Information für sich genommen die Identifizierung der betreffenden Person ermögliche. Zudem heiße es im 26. Erwägungsgrund der Richtlinie 95/46 EG, dass bei der Entscheidung, ob eine Person bestimmbar sei, alle Mittel berücksichtigt werden sollten, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Da dieser Erwägungsgrund auf die Mittel Bezug nehme, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem "Dritten" eingesetzt werden könnten, sei sein Wortlaut ein Indiz dafür, dass es für die Einstufung eines Datums als "personenbezogenes Datum" im Sinne von Art. 2 Buchst. a der Richtlinie 95/46 EG nicht erforderlich sei, dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befänden. Dass über die zur Identifizierung des Nutzers einer Website erforderlichen Zusatzinformationen nicht der Anbieter von Online-Mediendiensten verfüge, sondern der Internetzugangsanbieter dieses Nutzers, vermöge daher nicht auszuschließen, dass die von einem Anbieter von Online-Mediendiensten gespeicherten dynamischen IP-Adressen für ihn personenbezogene Daten im Sinne von Art. 2 Buchst. a der Richtlinie 95/46 EG darstellten. Die Möglichkeit, eine dynamische IP-Adresse mit den Zusatzinformationen zu verknüpfen, über die der Internetzugangsanbieter verfüge, stelle ein Mittel dar, das vernünftigerweise zur Bestimmung der betreffenden Person eingesetzt werden könne. Das vorlegende Gericht weise in seiner Vorlageentscheidung zwar darauf hin, dass das deutsche Recht es dem Internetzugangsanbieter nicht erlaube, dem Anbieter von Online-Mediendiensten die zur Identifizierung der betreffenden Person erforderlichen Zusatzinformationen direkt zu übermitteln, doch gebe es offenbar - vorbehaltlich der vom vorlegenden Gericht insoweit vorzunehmenden Prüfungen - für den Anbieter von Online-Mediendiensten rechtliche Möglichkeiten, die es ihm erlaubten, sich insbesondere im Fall von Cyberattacken an die zuständige Behörde zu wenden, damit diese die nötigen Schritte unternehme, um die fraglichen Informationen vom Internetzugangsanbieter zu erlangen und die Strafverfolgung einzuleiten. Der Anbieter von Online-Mediendiensten verfüge somit offenbar über Mittel, die vernünftigerweise eingesetzt werden könnten, um mit Hilfe Dritter, und zwar der zuständigen Behörde und dem Internetzugangsanbieter, die betreffende Person anhand der gespeicherten IP-Adressen bestimmen zu lassen.

25 cc) Auf dieser Grundlage ist das Tatbestandsmerkmal "personenbezogene Daten" des § 12 Abs. 1 und 2 TMG in Verbindung mit § 3 Abs. 1 BDSG richtlinienkonform dahingehend auszulegen, dass eine dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Internetseite, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt.

26 Denn die Beklagte verfügt über rechtliche Mittel, die vernünftigerweise eingesetzt werden können, um mit Hilfe Dritter, und zwar der zuständigen Behörde und des Internetzugangsanbieters, die betreffende Person anhand der gespeicherten IP-Adressen bestimmen zu lassen (vgl.

Gerichtshof aaO Rn. 47). Die Beklagte kann - im Falle einer bereits eingetretenen Schädigung - Strafanzeige bei den Strafverfolgungsbehörden erstatten; im Falle der drohenden Schädigung kann sie die zur Gefahrenabwehr zuständigen Behörden einschalten. Nach § 100j Abs. 2 und 1 StPO, § 113 TKG (vgl. BVerfGE 130, 151) können die für die Verfolgung von Straftaten oder Ordnungswidrigkeiten zuständigen Behörden zu diesem Zweck von Internetzugangsanbietern bei Vorliegen bestimmter Voraussetzungen Auskunft verlangen, entsprechendes gilt für die für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Behörden, die Verfassungsschutzbehörden des Bundes und der Länder, den Militärischen Abschirmdienst und den Bundesnachrichtendienst zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der genannten Stellen. Die in eine Auskunft aufzunehmenden Daten dürfen auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse bestimmt werden. Dadurch können die gewonnenen Informationen zusammengeführt und der Nutzer bestimmt werden (vgl. Gerichtshof aaO Rn. 49 a.E.).

27 2. Auf der Grundlage der vom Berufungsgericht getroffenen Feststellungen lässt sich nicht beurteilen, ob zugunsten der Beklagten ein Erlaubnistatbestand im Sinne von § 15 Abs. 1 TMG eingreift.

28 a) Handelt es sich bei der IP-Adresse im Zusammenhang mit den Daten des Zugriffs um personenbezogene Daten, ist 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.

29 b) Eine Einwilligung des Nutzers liegt hier nicht vor. Es kommt aber eine Erlaubnis nach § 15 Abs. 1 TMG in Betracht. Danach 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.

30 c) Fraglich war, ob die Voraussetzungen des § 15 Abs. 1 TMG auch dadurch erfüllt sein können, dass die Maßnahmen des Diensteanbieters über den konkreten Nutzungsvorgang hinaus "erforderlich" sind, um Cyberangriffe ("Denial-of-Service"-Attacken) abzuwehren und damit die Inanspruchnahme von Telemedien (allgemein) zu ermöglichen. Eine solche Auslegung wäre mit dem Wortlaut der Vorschrift vereinbar gewesen. Denn die behaupteten "Denial-of-Service"-Attacken führen dazu, dass das Telemedium nicht mehr erreichbar und seine Inanspruchnahme somit nicht mehr möglich ist. Allerdings wurde in der Literatur überwiegend die (enge) Auffassung vertreten, dass die Datenerhebung und -verwendung nur erlaubt sei, um ein konkretes Nutzungsverhältnis zu ermöglichen und die Daten, soweit sie nicht für Abrechnungszwecke benötigt werden, mit dem Ende des jeweiligen Nutzungsvorgangs zu löschen seien (vgl. zum damaligen Meinungsstand Senatsbeschluss vom 28. Oktober 2014 - VI ZR 135/13, aaO Rn. 38). Dieses enge Verständnis des § 15 Abs. 1 TMG hätte einer Erlaubnis zur Speicherung der IP-Adressen zur (generellen) Gewährleistung und Aufrechterhaltung der Sicherheit und Funktionsfähigkeit von Telemedien entgegengestanden.

31 aa) Der erkennende Senat hat dem Gerichtshof der Europäischen Union gemäß Art. 267 AEUV deshalb folgende weitere Frage zur Auslegung des Unionsrechts vorgelegt:

32 "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?"

33 bb) Der Gerichtshof hat mit Urteil vom 19. Oktober 2016 - C-582/14, aaO die Frage wie folgt beantwortet:

34 "Art. 7 Buchst. f der Richtlinie 95/46 ist dahin auszulegen, dass er einer Regelung eines Mitgliedstaats entgegensteht, nach der ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung nur erheben und verwenden darf, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die konkrete Inanspruchnahme der Dienste durch den betreffenden Nutzer zu ermöglichen und abzurechnen, ohne dass der Zweck, die generelle Funktionsfähigkeit der Dienste zu gewährleisten, die Verwendung der Daten über das Ende eines Nutzungsvorgangs hinaus rechtfertigen kann."

35 cc) Danach wäre die Auslegung des § 15 Abs. 1 und 4 TMG in dem oben angesprochenen engen Sinne mit Art. 7 Buchst. f der Richtlinie 95/46 EG unvereinbar. § 15 Abs. 1 TMG ist entsprechend Art. 7 Buchst. f der Richtlinie 95/46 EG dahin auszulegen, dass ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung auch über das Ende eines Nutzungsvorgangs hinaus dann erheben und verwenden darf, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die generelle Funktionsfähigkeit der Dienste zu gewährleisten, wobei es allerdings einer Abwägung mit dem Interesse und den Grundrechten und -freiheiten der Nutzer bedarf.

36 Nach Art. 7 Buchst. f der Richtlinie 95/46 EG 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 Artikel 1 Absatz 1 [der Richtlinie] geschützt sind, überwiegen".

37 Art. 5 der Richtlinie 95/46 EG erlaubt den Mitgliedstaaten zwar, nach Maßgabe des Kapitels II und damit des Art. 7 die Voraussetzungen näher zu bestimmen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist, doch kann von dem Ermessen, über das die Mitgliedstaaten nach Art. 5 verfügen, nur im Einklang mit dem von der Richtlinie verfolgten Ziel der Wahrung eines Gleichgewichts zwischen dem freien Verkehr personenbezogener Daten und dem Schutz der Privatsphäre (vgl. Gerichtshof aaO Rn. 58) Gebrauch gemacht werden. Die Mitgliedstaaten dürfen nach Art. 5 der Richtlinie in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten keine anderen als die in Art. 7 der Richtlinie aufgezählten Grundsätze einführen und auch nicht durch zusätzliche Bedingungen die Tragweite der sechs in Art. 7 vorgesehenen Grundsätze verändern (vgl. in diesem Sinne EuGH Slg 2011, I - 12181 Rn. 33 ff. ASNEF und FECEMD).

38 Im vorliegenden Fall hätte § 15 TMG, wenn er in der angesprochenen engen Weise ausgelegt würde, eine geringere Tragweite als der in Art. 7 Buchst. f der Richtlinie 95/46 EG aufgestellte Grundsatz.

39 Während nämlich in Art. 7 Buchst. f der Richtlinie allgemein auf die "Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden", Bezug genommen wird, würde § 15 TMG dem Diensteanbieter die Erhebung und Verwendung personenbezogener Daten eines Nutzers nur gestatten, soweit dies erforderlich ist, um die konkrete Inanspruchnahme elektronischer Medien zu ermöglichen und abzurechnen. § 15 TMG stünde daher einer zur Gewährleistung der Inanspruchnahme von Online-Mediendiensten dienenden Speicherung personenbezogener Daten über das Ende eines Zugriffs auf diese Dienste hinaus allgemein entgegen. Andererseits haben die Einrichtungen des Bundes, die Online-Mediendienste anbieten, ein berechtigtes Interesse daran, die Aufrechterhaltung der Funktionsfähigkeit der von ihnen allgemein zugänglich gemachten Internetseiten über ihre konkrete Nutzung hinaus zu gewährleisten.

40 Der Gerichtshof weist weiter darauf hin, dass Art. 7 Buchst. f der Richtlinie 95/46 EG einen Mitgliedstaat daran hindert, kategorisch und ganz allgemein die Verarbeitung bestimmter Kategorien personenbezogener Daten auszuschließen, ohne Raum für eine Abwägung der im konkreten Einzelfall einander gegenüberstehenden Rechte und Interessen zu lassen. Ein Mitgliedstaat kann daher für diese Kategorien das Ergebnis der Abwägung der einander gegenüberstehenden Rechte und Interessen nicht abschließend vorschreiben, ohne Raum für ein Ergebnis zu lassen, das aufgrund besonderer Umstände des Einzelfalls anders ausfällt (vgl. in diesem Sinne EuGH Slg 2011, I - 12181 Rn. 47 ff. ASNEF und FECEMD).

41 d) Diese Abwägung kann im Streitfall auf der Grundlage der vom Berufungsgericht getroffenen Feststellungen nicht (abschließend) vorgenommen werden. Das Berufungsgericht hat keine hinreichenden Feststellungen dazu getroffen, ob die Speicherung der IP-Adressen des Klägers über das Ende eines Nutzungsvorgangs hinaus erforderlich ist, um im konkreten Fall die generelle Funktionsfähigkeit der jeweils in Anspruch genommenen Dienste zu gewährleisten. Die Beklagte verzichtet nach ihren eigenen Angaben bei einer Vielzahl der von ihr betriebenen Portale mangels eines "Angriffsdrucks" darauf, die jeweiligen IP-Adressen der Nutzer zu speichern. Demgegenüber fehlen entsprechende Feststellungen dazu, wie hoch das Gefahrenpotential bei den übrigen Online-Mediendiensten des Bundes ist, welche der Kläger in Anspruch nehmen will. Dazu gehören etwa Feststellungen zu Art, Umfang und Wirkung von bereits erfolgten und etwa drohenden Cyber-Angriffen wie "Denial-of-Service"-Attacken sowie zu der Bedeutung der betroffenen Telemedien.

42 Erst wenn entsprechende Feststellungen hierzu getroffen sind, wird das Berufungsgericht die nach dem Urteil des Gerichtshofs gebotene Abwägung zwischen dem Interesse der Beklagten an der Aufrechterhaltung der Funktionsfähigkeit ihrer Online-Mediendienste und dem Interesse oder den Grundrechten und Grundfreiheiten des Klägers nachzuholen haben. Dabei wird auch der Gesichtspunkt der Generalprävention gebührend zu berücksichtigen sein. Die Parteien werden dabei Gelegenheit haben, gegebenenfalls ergänzend vorzutragen.

43 Allerdings dürfte der mit der Speicherung der Daten eines Nutzers über das Ende eines Nutzungsvorgangs hinaus verbundene Eingriff in das allgemeine Persönlichkeitsrecht - in seiner Ausprägung als Recht auf informationelle Selbstbestimmung - nach den bisherigen Feststellungen eher gering wiegen. Denn die Stellen der Beklagten, die die IP-Adressen des Klägers gespeichert haben, hätten den Kläger nicht ohne Weiteres identifizieren können. Nach den bisher getroffenen Feststellungen 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 (vgl. Gerlach, CR 2013, 478, 480). 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). Die Befugnisse der zuständigen Stellen im Sinne des § 113 Abs. 3 TKG (etwa die Staatsanwaltschaft im Rahmen eines Ermittlungsverfahrens nach § 100j StPO) zur Feststellung der Identität sind an enge Voraussetzungen gebunden, bei deren Vorliegen das Interesse des Nutzers an der Wahrung seiner Anonymität zurücktreten könnte.

44 B) Revision der Beklagten

45 Die Revision der Beklagten hat ebenfalls Erfolg und führt auch insoweit zur Aufhebung des Berufungsurteils und zur Zurückverweisung der Sache an das Berufungsgericht.

46 1. Das Berufungsgericht ist zwar zutreffend davon ausgegangen, dass die dynamische IP-Adresse des Klägers in Verbindung mit dem Zeitpunkt des Nutzungsvorgangs (erst recht) ein personenbezogenes Datum im Sinne von § 12 Abs. 1 TMG darstellt, wenn der Kläger während eines

Nutzungsvorgangs seine Personalien angibt und die Beklagte den Klarnamen mit der IP-Adresse verknüpfen kann. Dies begegnet nach den vorstehenden Ausführungen keinerlei Zweifel.

47 2. Jedoch steht das vom Berufungsgericht befürwortete enge Verständnis des § 15 Abs. 1 TMG nicht in Einklang mit Art. 7 Buchstabe f der Datenschutz-Richtlinie. § 15 Abs. 1 TMG muss richtlinienkonform dahin ausgelegt werden, dass der von dem Diensteanbieter verfolgte Zweck, die generelle 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. Das Berufungsgericht wird auf der Grundlage der noch zu treffenden Feststellungen die erforderliche Abwägung auch für den Fall nachzuholen haben, in dem der Nutzer während eines Nutzungsvorgangs seine Personalien angibt.

Galke Wellner Oehler

Roloff Klein