Patrick Breyer

[anonymisiert]

[anonymisiert]

Patrick Breyer • [anonymisiert] • [anonymisiert]

Amtsgericht Tiergarten
Turmstraße 91
10559 Berlin

[anonymisiert], 06.07.2008

- nur per Fax -

Az. 2 C 6/08

In dem Verfahren Breyer ./. Bundesrepublik

weise ich vorab darauf hin, dass Herr Rechtsanwalt Starostik zur Wahrnehmung des Verhandlungstermins und der in diesem Zusammenhang erforderlichen Handlungen bevollmächtigt ist, nicht aber zur Verfahrensvertretung. Ich bitte daher, den Schriftverkehr weiterhin über mich zu führen.

Auf die Klageerwiderung der Gegenseite vom 03.07.2008 repliziere ich wie folgt, wobei ich dem Aufbau der Klageerwiderung folge:

a) Rechtsweg

Der Rechtsweg zur ordentlichen Gerichtsbarkeit ist gegeben. Dies hat bereits das Amtsgericht Mitte mit Beschluss vom 23.11.2006 im Vorprozess (Az. 5 C 314/06) entschieden. In diesem Beschluss heißt es zutreffend:

> „*Die Parteien werden gemäß § 139 Abs. 2 ZPO darauf hingewiesen, dass die Zuständigkeit der Zivilgerichte für die seitens des Klägers geltend gemachten Ansprüche, soweit diese auf die Vorschriften des Tele-*

> *dienstedatenschutzgesetzes (TDDSG) in Verbindung mit §§ 823, 1004 BGB gestützt werden, als gegeben erachtet wird.*“

Zwar dienen die Telemedien der Beklagten öffentlichen Zwecken. Dies sagt jedoch nichts darüber aus, ob hier eine privatrechtliche oder öffentlich-rechtliche Streitigkeit gegeben ist. Es ist anerkannt, dass Verwaltungshandeln auch dem Privatrecht unterworfen sein kann, selbst wenn es öffentlichen Zwecken dient (z.B. fiskalisches Handeln).

Entscheidend für den Rechtsweg ist die Frage, ob die streitentscheidende Norm privatrechtlich oder öffentlich-rechtlich ist, so die herrschende Meinung. Streitentscheidend sind hier die Regelungen des Telemediengesetzes, auf die die Klageschrift Bezug nimmt, insbesondere § 15 TMG, der die Zulässigkeit der streitgegenständlichen Datenspeicherung regelt.

§ 15 TMG ist eine privatrechtliche Norm. Er gilt nämlich unterschiedslos für private und für öffentliche Stellen. Dies ergibt sich aus § 1 Abs. 1 S. 2 TMG:

> „*Dieses Gesetz gilt für alle Anbieter einschließlich der öffentlichen Stellen [...]*“

Demnach hat der Gesetzgeber das Angebot von Telemedien einheitlich dem Privatrecht unterstellt. Daran muss sich die Beklagte festhalten lassen, wenn sie allgemein zugängliche Internetportale betreibt.

Die Klage ist außerdem auf § 1004 BGB, ebenfalls eine eindeutig privatrechtliche Norm, gestützt. Insofern kann ich den Rechtsschutz der ordentlichen Gerichtsbarkeit in Anspruch nehmen.

Eine öffentlich-rechtliche Streitigkeit im Sinne des § 40 VwGO liegt nicht vor, weil zwischen den Parteien weder ein öffentlich-rechtliches Rechtsverhältnis besteht noch eine öffentlich-rechtliche Norm den eigentlichen, streitentscheidenden Gegenstand des Rechtsstreits bildet.

b) Ermittlungspraxis des Bundeskriminalamts

Zu der Ermittlungspraxis des Bundeskriminalamts wird auf Seite 12 der Klageschrift ausgeführt, dass das Bundeskriminalamt aufgrund der streitgegenständlichen Zugriffsprotokolle Ermittlungen gegen Nutzer des Portals www.bka.de einleitet, die mit „signifikanter Zugriffsfrequenz“ Informationen über bestimmte kriminel-

le oder terroristische Vereinigungen von ihrem Portal abrufen. Insbesondere werden die entsprechenden Nutzer über § 113 TKG identifiziert und mit verschiedenen Datenbanken abgeglichen. Die aufgezeigte Verfahrensweise hat die Beklagte selbst auf parlamentarische Anfragen öffentlich bestätigt. [1] Es mag sein, dass „weitere Maßnahmen“ nur in wenigen Fällen vorgenommen wurden. Identifizierung und Datenbankabgleich wurden aber nach unbestrittenen Presseinformationen bei einer dreistelligen Anzahl von Personen durchgeführt, die in keinerlei Verbindung mit irgend einer Straftat stehen. In dem Pressebericht heißt es:[2]

> „*Ursprünglich hatte das BKA die Identität von 417 Personen feststellen wollen. Dabei handelte es sich nicht um Tatverdächtigte, sondern offenbar um alle Personen, die sich zwischen dem 28. März und dem 18. April diesen Jahres auf den Internetseiten des Bundeskriminalamtes über die „Militante Gruppe“ informieren wollten. Weil aber ein großer Teil der IP-Adressen von Providern stammte, die diese nur kurze Zeit speichern, wurde die Identifizierung von „nur“ rund 120 Telekom-Kunden beantragt. Das BKA habe „einen weiteren Teil“ der IP-Adressen „Presseorganen bzw. einzelnen Firmen oder Universitäten“ zugeordnet, heißt es. „Anhand dieser Daten werden weiterführende polizeiliche Ermittlungen wie unter anderem die Identifizierung weiterer Mitglieder der „militanten gruppe“ (mg) ermöglicht“, begründen die Beamten ihren Antrag.*“

I. Sachliche Zuständigkeit

Zur sachlichen Zuständigkeit ist bereits vorgetragen worden. Nach der Entscheidung des Landgerichts ist die Frage geklärt.

II. Bestimmtheit, Rechtsschutzbedürfnis

1. Bestimmtheit

Der Klageantrag ist hinreichend bestimmt im Sinne des § 253 ZPO. § 253 ZPO verlangt, den Klageantrag so bestimmt zu formulieren, dass er zur Vollstreckung geeignet ist (BGH, NJW 1981, 1056). Im Fall eines Unterlassungsanspruchs erfolgt die Zwangsvollstreckung durch das Prozessgericht im Wege des § 890 ZPO.

---

1 BT-Prot. 16/117, 22; BT-Drs. 16/6938.

2 Tagesspiegel vom 30.09.2007, http://www.tagesspiegel.de/politik/deutschland/BKA-Datenschutz;art122,2390884.

Der Klageantrag ist vorliegend so bestimmt bezeichnet, dass das Gericht prüfen kann, ob eine Zuwiderhandlung gegen das Urteil vorliegt oder nicht. Der Begriff des Telemediums ist im Telemediengesetz definiert (§ 1 TMG). Ob ein Telemedium von der Beklagten angeboten wird, kann unschwer anhand des Impressums des fraglichen Angebots nachvollzogen werden, zu dessen Führung jeder Anbieter verpflichtet ist (§ 55 Rundfunkstaatsvertrag). Ist im Impressum die Beklagte oder eine ihrer Behörden als Verantwortliche genannt, so liegt ein Telemedium der Beklagten vor. Es ist daher hinreichend bestimmt, die Unterlassung hinsichtlich aller „öffentlich zugänglicher Telemedien der Beklagten im Internet“ zu beantragen.

2. Rechtsschutzbedürfnis

Die Beklagte meint, meiner Klage fehle das Rechtsschutzbedürfnis, weil ich niemals sämtliche Telemedien der Beklagten nutzen würde. Dies ist richtigerweise keine Frage des Rechtsschutzbedürfnisses, sondern der Begehungsgefahr im Rahmen des § 1004 BGB. Diese ist aus den folgenden Gründen hinsichtlich sämtlicher Telemedien der Beklagten gegeben:

a) Vermutung der Wiederholungsgefahr

Die von § 1004 Abs. 1 S. 2 BGB geforderte Begehungsgefahr wird vermutet, da die Beklagte bereits in der Vergangenheit jeden meiner Besuche ihrer entsprechenden Telemedien in Verletzung meiner Persönlichkeitsrechte rechtswidrig aufgezeichnet hat. Da die Beklagte diese rechtswidrige Aufzeichnung bei den meisten ihrer Telemedien praktiziert, begründet ihr voran gegangenes Verhalten die Vermutung, dass sie auch meine Besuche neuer Seiten und Portale aufzeichnen wird.

Dass frühere Verletzungen Wiederholungen in der Zukunft vermuten lassen, ist allgemein anerkannt (BGHZ 140, 1, 10).

Dass die Beklagte meine IP-Adresse auf den meisten ihrer Angebote erfasst, ergibt sich aus der Stellungnahme des Bundesinnenministeriums vom 30.10.2007:[3]

> „*Die überwiegende Zahl der Ressorts und soweit dies in der Kürze der Zeit ermittelt werden konnte, deren nachgeordnete Behörden speichern die einem PC zugeordnete IP-Adresse, von denen aus ihre Internetseiten*

3 BT-Drs. 16/6884, 3.

besucht werden bzw. lassen dies durch beauftragte Unternehmen speichern.“

Der auf eine Wiederholungsgefahr begründete Unterlassungsanspruch ist nicht nur auf die Unterlassung einer identischen Rechtsverletzung gerichtet, sondern umfasst auch solche Beeinträchtigungsformen, die den Kern der Störung inhaltsgleich wiederholen (Bamberger/Roth-Fritzsche, § 1004, Rn. 93 m.w.N.). Eine solche im Kern gleiche Rechtsverletzung liegt vor, wenn die Beklagte auf von mir zuvor noch nicht besuchten Internetseiten nunmehr ebenfalls mein Nutzungsverhalten registriert. Es liegt insoweit keine vorbeugende Unterlassungsklage vor. Vielmehr hat die Beklagte bei vielen Gelegenheiten bereits in der Vergangenheit rechtswidrig mein Informationsverhalten personenbeziehbar protokolliert.

Der Unterlassungsanspruch kann nicht auf bereits besuchte Portale der Beklagten beschränkt sein. Die Beklagte ist für sämtliche ihre Angebote verantwortlich. Der Sachverhalt ist mit einem Zeitungsverlag oder einer Rundfunkanstalt vergleichbar, die zur Unterlassung einer bestimmten Tatsachenbehauptung verurteilt werden. Es wäre widersinnig, hier eine Beschränkung auf die konkrete Zeitung oder Sendung zu fordern, in deren Rahmen die Rechtsverletzung begangen wurde. Die Rechtsprechung tut dies zutreffend nicht, weil eine Verurteilung in diesem Fall schlichtweg dadurch umgangen werden könnte, dass die Behauptung in anderem Rahmen weiter verbreitet wird. Ebenso droht eine Umgehung auf Seiten der Beklagten, würde die Verurteilung auf einzelne Portale beschränkt.

Eine Beschränkung auf einzelne Portale wäre mir auch nicht zumutbar. Würde die Verurteilung im vorliegenden Fall auf bereits besuchte Angebote beschränkt, müsste ich ständig neue Klagen wegen neuerlich besuchter, weiterer Telemedien der Beklagten einreichen. Dies wäre mit dem Gebot des effektiven Rechtsschutzes (Art. 19 Abs. 4 GG) und mit dem Gedanken der Prozessökonomie nicht vereinbar. Die Beklagte hat durch ihr Verhalten nach dem Vorprozess gezeigt, dass sie zur Einhaltung des Gesetzes immer nur insoweit bereit ist, wie sie gerichtlich dazu verurteilt worden ist.

b) Erstbegehungsgefahr

Selbst wenn man die Vermutung der Wiederholungsgefahr nicht auf andere Angebote der Beklagten beziehen wollte, ist jedenfalls eine Erstbegehungsgefahr hinsichtlich sämtlicher Angebote der Beklagten gegeben: Ich bin intensiver Internetnutzer und nutze das Internet etwa 20 Stunden pro Woche. Dabei suche ich oft

mithilfe von Suchmaschinen nach bestimmten Informationen. Unter den „Treffern“ werden immer wieder auch Telemedien der Beklagten angezeigt, die ich sodann abrufe. Auf diese Weise ist es jederzeit möglich, dass ich auf jedes Telemedium der Beklagten gelange und dort in meinen Persönlichkeitsrechten verletzt werde, indem mein Informationsverhalten rechtswidrig erfasst wird.

III. Passivlegitimation, Vertretungsbefugnis

Der Beklagtenvertreter meint, das Bundesinnenministerium sei nicht passiv legitimiert in Bezug auf Telemedien außerhalb seines Geschäftsbereichs. Bezüglich anderer Geschäftsbereiche und Verfassungsorgane verfüge das Ministerium über keine Weisungsbefugnis, um ein Unterlassungsurteil durchzusetzen.

Dem ist entgegen zu treten. Die Beklagte vermengt unzulässig die Fragen der Passivlegitimation, Vertretungsmacht, Vertretungsbefugnis und des Weisungsrechts.

1. Passivlegitimation

Die Beklagte ist passiv legitimiert. Der geltend gemachte Unterlassungsanspruch richtet sich gegen sie. Sie ist für alle ihre Telemedien verantwortlich. Die Frage nach der Passivlegitimation des Bundesinnenministeriums stellt sich bereits deshalb nicht, weil dieses nicht verklagt ist.

Unrichtig ist auch die Theorie der Beklagten, die Verurteilung einer juristischen Person könne sich nur auf diejenigen Organe und Stellen erstrecken, hinsichtlich derer der Prozessvertreter weisungsbefugt ist. Die Beklagte kann bezeichnenderweise keine einzige gesetzliche Vorschrift oder Rechtsprechung anführen, aus der sich derartiges ergeben sollte. Wird beispielsweise eine privatrechtliche Gesellschaft von einem ihrer Geschäftsführer vor Gericht vertreten, so kann sie selbstverständlich insgesamt verurteilt werden. An die Verurteilung ist dann auch ein anderer Geschäftsführer gebunden, selbst wenn Geschäftsführer untereinander nicht weisungsbefugt sind.

Ebenso sind alle Stellen und Organe der Beklagten kraft Art. 20 GG in eigener Verantwortung gehalten, Recht und Gesetz – und damit auch eine gerichtliche Verurteilung – zu beachten. Es obliegt nicht dem Bundesinnenministerium, die Beachtung der Verurteilung durch Weisungen durchzusetzen. Die Weisungskompetenz des Ministeriums ist daher für die Passivlegitimation der Beklagten unerheblich.

Dementsprechend hat etwa das OVG Nordrhein-Westfalen mit Urteil vom 18.12.1985 (Az. 5 A 1125/84) die Beklagte, vertreten durch das Familienministerium, zur Unterlassung bestimmter Äußerungen verurteilt. Auch in diesem Verfahren war die Verurteilung nicht auf den Geschäftsbereich des Familienministeriums beschränkt, sondern band jede Stelle der Beklagten.

2. Vertretung der Beklagten

Das Bundesministerium des Innern kann die Beklagte im vorliegenden Verfahren auch vollumfassend vertreten.

a) Die von der Beklagten angeführte innere Organisation des Bundesrepublik nach Organen und Ministerien mit verschiedenen Geschäftsbereichen betrifft nur die Frage der internen Vertretungsberechtigung des Bundesinnenministeriums im Verhältnis zu den anderen Organen. Das Bundesinnenministerium soll intern nur im Rahmen seines Geschäftsbereichs tätig werden.

Im Rechtsverkehr hingegen kann das Bundesinnenministerium die Beklagte vollumfänglich vertreten und verpflichten. Die Vertretungsmacht des Ministeriums ist nach außen unbeschränkt.

Würde die Auffassung der Beklagten hinsichtlich der nach außen gespaltenen Vertretungsmacht zutreffen, so wären beispielsweise auch bei Klagen gegen die Beklagte auf Unterlassung bestimmter Äußerungen stets alle Ministerien gesetzliche Vertreter der Beklagten, weil der Unterlassungstitel ihre sämtlichen Ministerien bindet. Dass dies nicht zutreffen kann, liegt auf der Hand. Die entgegen gesetzte Entscheidung des OVG Nordrhein-Westfalen wurde bereits angeführt. Ebenso ist es übliche Praxis, dass das Bundesjustizministerium die Beklagte in justiziellen Fragen gerichtlich vertritt, selbst wenn das Urteil die Beklagte insgesamt – also alle Organe und Ressorts – bindet.

b) Ohne dass es im vorliegenden Verfahren darauf ankäme, ist das Bundesinnenministerium im Übrigen auch im Innenverhältnis zur Vertretung der Beklagten im vorliegenden Rechtsstreit berechtigt. Das Ministerium ist nach dem Organisationserlass des Bundeskanzlers (vgl. § 9 Geschäftsordnung der Bundesregierung) zuständig für den Bereich des Datenschutzes. Daraus ist die Befugnis zur umfassenden Vertretung der Beklagten in entsprechenden Rechtsstreitigkeiten abzuleiten.

c) Sollte das Gericht von der mangelnden Vertretungsmacht des Bundesinnenministeriums ausgehen, so beantrage ich

die Beklagte im Wege des Teilversäumnisurteils zu verurteilen, soweit nicht Telemedien des Bundesinnenministeriums betroffen sind.

Wäre das Bundesinnenministerium nämlich teilweise nicht zur Vertretung der Beklagten in der Lage, so würde insoweit keine wirksame Verteidigungsanzeige der Beklagten vorliegen. Auch der vom Bundesinnenministerium beauftragte Beklagtenvertreter wäre hinsichtlich der Telemedien anderer Ressorts und Organe nicht wirksam zur Vertretung bevollmächtigt.

Vor diesem Hintergrund des drohenden Versäumnisurteils mag der Beklagtenvertreter überdenken, ob er sich weiterhin darauf berufen will, dass er nur teilweise zur Vertretung der Beklagten in der Lage sei. In diesem Fall hätte es der Beklagten kraft ihrer eigenen Organisation oblegen, durch Mitwirkung sämtlicher Organe und Ministerien für eine ordnungsgemäße Vertretung im vorliegenden Rechtsstreit zu sorgen, um einem Versäumnisurteil zu entgehen.

d) Wirksam zugestellt ist die Klage in jedem Fall, denn § 170 Abs. 3 ZPO lässt die Zustellung an einen beliebigen gesetzlichen Vertreter – unabhängig vom Umfang dessen Vertretungsmacht – genügen. Mit der Aushändigung an das Bundesinnenministerium ist die Zustellung an einen gesetzlichen Vertreter der Beklagten erfolgt.

IV. Personenbezug

a) Vorab ist es traurig, dass sich die Beklagte entschlossen hat, sämtliche Argumente aus dem Vorprozess wieder aufzurollen, mit denen sie bereits damals keinen Erfolg hatte. Dabei hatte die Beklagte im Vorprozess noch Einsicht gezeigt und ihre Unterlassungsverpflichtung mit der Berufung nicht mehr angegriffen. Es widerspricht Art. 20 Abs. 3 GG, dass die Beklagte das Telemediengesetz stets nur insoweit einhält, wie sie gerichtlich dazu gezwungen wird. Sollte das Leugnen der Beklagten hingegen nur taktisch motiviert sein und der Zeitgewinnung dienen, bin ich bereit, der Beklagten im Vergleichswege eine angemessene Übergangszeit einzuräumen, wenn sie die Klage im Gegenzug anerkennt.

b) In der Sache führt die Beklagte an, dass sich eine IP-Adresse stets nur auf einen Internetanschluss beziehe und sich der jeweilige Nutzer des Anschlusses nicht bestimmen lasse. Dies trifft zu, lässt den Personenbezug des Datums aber

nicht entfallen. Die IP-Adresse ist nämlich auf die Person des Anschlussinhabers bezogen. Dies genügt § 3 BDSG. Die Internetprotokolle der Beklagten erlauben es, die Nutzung ihrer Telemedien über meinen Anschluss nachzuvollziehen. Damit ist ein Bezug zu meiner Person gegeben, ob ich selbst Nutzer bin oder nicht.

Im Übrigen habe ich bereits in der Klageschrift aufgeführt, dass ich selbst Inhaber des von mir genutzten Internetanschlusses bin. Ich benutze diesen auch ausschließlich. Keine andere Person hat Zugang zu meinem Anschluss.

1. Mittelbare Bestimmbarkeit des Nutzers anhand dynamischer IP-Adressen

Die Ausführungen der Beklagten zur Bestimmbarkeit des Nutzers einer zeitweise (dynamisch) vergebenen IP-Adresse widersprechen in Teilen der Klageschrift; insoweit werden sie bestritten. Namentlich kann die Zuordnung einer IP-Adresse zu einer Person nicht nur mithilfe einer Auskunft des Internet-Zugangsanbieters erfolgen, sondern auch auf anderem Wege:

- Eine Zuordnung ist dem Telemedienanbieter schon aufgrund eigener Daten möglich, wenn der Nutzer seine Identität offenbart, etwa im Rahmen einer Bestellung.

- Eine Identifizierung kann im Zusammenwirken mit Dritten möglich sein, die ihrerseits die Identität des Nutzers kennen. Angenommen, ich klicke in einem von mir genutzten E-Mail-Dienst auf einen Link zu einem Internetangebot der Beklagten. Die Beklagte speichert nun bei einigen ihrer Portale die vom Nutzer zuletzt – extern – besuchte Seite.[4] Dadurch kann sie bei meinem E-Mail-Anbieter anfragen, welcher seiner Kunden zum maßgeblichen Zeitpunkt meine IP-Adresse genutzt hat. Mein E-Mail-Anbieter kennt meine Identität. In ähnlicher Weise kann eine Identifizierung über die Anbieter von Internetforen, von Suchmaschinen usw. erfolgen, bei denen ich namentlich gemeldet bin.

2. Mittelbarer Personenbezug nicht nur durch IP-Adresse und Zeitangabe

Die Beklagte vertritt die Auffassung, eine IP-Adresse sei für sich genommen nicht personenbezogen, sondern nur in Verbindung mit Datum und Uhrzeit des jeweiligen Nutzungsvorgangs. Ein Anspruch auf Unterlassen der isolierten Speicherung von IP-Adressen bestehe nicht.

4 Etwa auf dem Portal www.bfn.de: „Daten über die Seite, von der aus die Datei angefordert wurde“.

Die Beklagte verkennt, dass die zur Rückverfolgung dynamischer IP-Adressen erforderliche Zeitangabe nicht notwendig dem Zugriffsprotokoll zu entnehmen sein muss. Protokolliert die Beklagte etwa allein IP-Adressen in der Weise, dass stündlich eine eigene Protokolldatei erstellt wird, so kann sich bereits aus dem automatisch gespeicherten Erstellungszeitpunkt der Protokolldatei eindeutig auf den Inhaber einer IP-Adresse schließen lassen, wenn dieser nämlich über die gesamte Stunde hinweg die maßgebliche IP-Adresse genutzt hat.

Auch auf andere Weise kann eine Identifizierung möglich sein. Ist auf ein Telemedium der Beklagten vor und nach dem gesuchten Zugriff mit der IP-Adresse A auch mit der IP-Adresse B zugegriffen worden und wurde der Zugriff über die IP-Adresse B nebst Zeitzuordnung auf Seiten des Nutzers protokolliert – wie es etwa bei Behörden und Unternehmen nicht selten ist – so kann auch der Zugriff mit der IP-Adresse A zeitlich hinreichend eingegrenzt werden, um eine eindeutige Identifizierung zu ermöglichen.

Dementsprechend hat auch das Landgericht Berlin im Vorprozess die Beklagte einschränkungslos verurteilt, die Speicherung der IP-Adresse zu unterlassen (Urteil vom 06.09.2007, Az. 23 S 3/07). An dieser Verurteilung habe ich den Klageantrag ausgerichtet.

Für den Fall, dass das Hohe Gericht im vorliegenden Verfahren die Bedenken der Beklagten gleichwohl teilen sollte, beantrage ich hilfsweise,

> **die Beklagte zu verurteilen, es zu unterlassen, die Internetprotokolladresse (IP-Adresse) des zugreifenden Hostsystems des Klägers, die im Zusammenhang mit der Nutzung öffentlich zugänglicher Telemedien der Beklagten im Internet – mit Ausnahme des Internetportals „http://www.bmj.bund.de“ – übertragen wird, nebst dem Zeitpunkt des jeweiligen Nutzungsvorgangs 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.**

3. Bestimmbarkeit meiner Person anhand der IP-Adresse

a) Keine Relativität des Personenbezugs

aa) Die Beklagte beruft sich auf eine ältere Minderauffassung, wonach ein Datum nur personenbezogen sei, wenn gerade die jeweils speichernde Stelle den Nutzer identifizieren könne.[5] Der Personenbezug soll nach dieser Auffassung „relativ" sein: Ein und dasselbe Datum könne personenbezogen oder „anonym" sein – je nach dem, wer über das Datum verfüge. Nach dieser Meinung soll das Datenschutzrecht auf „relativ personenbezogene" Daten grundsätzlich nicht anwendbar sein, insbesondere nicht auf ihre Speicherung. Anzuwenden sei das Datenschutzrecht erst, wenn die Daten an eine Stelle übermittelt werden sollen, die den Betroffenen mit eigenen Mitteln identifizieren kann. Dieser Übermittlungsvorgang und die anschließende Verarbeitung seien dann nur nach den Regelungen des Datenschutzrechts zulässig.[6]

Die Theorie eines „relativen Personenbezugs" entspricht nicht dem geltenden Recht, wie im Folgenden zu zeigen sein wird.

Nach § 3 Abs. 1 Bundesdatenschutzgesetz sind personenbezogene Daten „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person". Es genügt danach, wenn die Person des Betroffenen „bestimmbar" ist. Keineswegs fordert das Gesetz, dass der Betroffene gerade durch die speichernde Stelle bestimmbar sein muss. Das Datenschutzrecht soll auch davor schützen, dass eine Identifizierung erst durch die Zusammenführung mit weiteren Daten erfolgt, wie sie etwa im Fall von IP-Adressen bei dem Internet-Zugangsanbieter vorhanden sind. Auch ohne Auskunftsanspruch des Inhalteanbieters gegen den Zugangsanbieter kann es zu einer solchen Zusammenführung kommen, nämlich indem der Internet-Zugangsanbieter oder aber der Inhalteanbieter freiwillig die entsprechenden Daten an die jeweils andere Stelle übermittelt.

Ein personenbezogenes Datum liegt danach schon dann vor, wenn die Herstellung des Personenbezugs einer beliebigen Person möglich ist. Diese Auslegung ist auch europarechtlich geboten. § 3 Abs. 1 BDSG ist insoweit richtlinienkonform auszulegen. Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten bestimmt ausdrücklich:

---

5 Gola/Schomerus, BDSG, § 3, Rn. 9.

6 Gola/Schomerus, BDSG, § 3 Rdnr. 10 und 44a.

> „*26. Die Schutzprinzipien müssen für alle Informationen über eine bestimmte oder bestimmbare Person gelten. Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen.*“

Zu berücksichtigen sind also auch die Daten, die Dritten zur Verfügung stehen, etwa dem Internet-Zugangsanbieter.

Falsch ist auch die Auffassung, eine Bestimmbarkeit des Betroffenen liege nur vor, wenn der Betroffene mit legalen Mitteln identifiziert werden könne. Das Datenschutzrecht soll gerade vor dem Missbrauch von Daten schützen (§ 1 Abs. 1 BDSG), wie er in der Praxis leider tagtäglich vorkommt. Man braucht nur die Tätigkeitsberichte der Datenschutzbeauftragten zu lesen, um festzustellen, dass Staat und Wirtschaft immer wieder unter Verstoß gegen Datenschutzrecht Daten übermitteln. Der Einzelne wäre schutzlos gestellt, würde man eine unbeschränkte Speicherung seiner Daten mit dem Argument zulassen, seine Person könne von der momentan speichernden Stelle mit legalen Mitteln nicht bestimmt werden.

Die relativierende Auffassung würde ein Eldorado für Kreditauskunfteien, Detekteien, Werbeunternehmen usw. eröffnen. Diese könnten dann nämlich unbegrenzt sensible Daten über jegliche Personen ansammeln und weitergeben, solange sie nicht den Namen der Betroffenen, sondern nur deren Personalausweisnummer, Kundennummer, Kontonummer o.ä. speicherten. Sie könnten sich dann darauf berufen, dass sie selbst die Betroffenen mit legalen Mitteln nicht bestimmen könnten. Dies wäre mit dem Grundrecht auf informationelle Selbstbestimmung offensichtlich unvereinbar.

Bei der Auslegung des Begriffs der Bestimmbarkeit darf das Risiko einer unbefugten Bestimmung des Betroffenen nicht unbeachtet bleiben. Das Datenschutzrecht und die dort vorgesehenen Löschungspflichten dienen gerade dazu, dieses Missbrauchsrisiko von vornherein auszuschließen. Das Bundesverfassungsgericht stellt in seinem Beschluss vom 27.10.2006 (Az. 1 BvR 1811/99) ausdrücklich auf die Möglichkeit eines rechtswidrigen Datenmissbrauchs durch Dritte ab, wenn es ausführt:

> „*Auch das Risiko eines Missbrauchs der Verkehrsdaten durch das Telekommunikationsunternehmen oder durch Dritte, die sich unbefugt Zugang zu ihnen verschaffen, ist nicht völlig auszuschließen.*“

Die relativierende Auffassung findet dementsprechend auch keinen Anhaltspunkt im Gesetz. § 3 Abs. 1 BDSG stellt – bewusst – weder darauf ab, ob der Betroffene gerade von der speichernden Stelle bestimmbar ist, noch schränkt er die Beurteilung der Bestimmbarkeit auf legale Mittel ein. Vielmehr heißt es in der EG-Datenschutzrichtlinie ausdrücklich, es müssten „alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten“. Dies ist die zutreffende und verbindliche Definition der Bestimmbarkeit im Sinne des Datenschutzrechts.

Schließlich vergessen die Vertreter der relativierenden Auffassung den praxisrelevantesten, legalen Fall, in dem „relativ“ personenbezogene Daten der Person eines Nutzers zugeordnet werden können. Möglich ist dies nämlich stets staatlichen Stellen, die über entsprechende Zwangsbefugnisse verfügen. Im Internet ermöglicht § 113 TKG die Identifizierung von Internetnutzern: Besteht der Verdacht einer Ordnungswidrigkeit, einer Straftat, einer Gefahr oder halten die Geheimdienste dies für erforderlich, so hat der Internet-Zugangsanbieter jeder zuständigen Stelle unverzüglich Auskunft über den Namen des Nutzers einer IP-Adresse zu erteilen (§ 113 Telekommunikationsgesetz; dazu LG Stuttgart, MMR 2005, 628 ff.; MMR 2005, 624 ff.; LG Hamburg, MMR 2005, 711; LG Würzburg, NStZ-RR 2006, 46).

Konsequenz der Verneinung des Personenbezugs von Internet-Nutzungsprotokollen wäre, dass das Internet-Nutzungsverhalten inhaltlich und zeitlich unbegrenzt protokolliert werden dürfte. Die Löschungspflichten in § 15 des Telemediengesetzes wären praktisch bedeutungslos. Schon die Befürchtung eines Missbrauchs dieser Datenhalden würde die Informations- und Meinungsfreiheit im Internet unangemessen beeinträchtigen. Im Volkszählungsurteil hat das Bundesverfassungsgericht zutreffend ausgeführt (BVerfGE 1, 43):

> „*Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare*

Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“

Auch im Internet wäre eine unbefangene Ausübung der Informations- und Meinungsäußerungsfreiheit unmöglich, wenn jeder Klick und jede Eingabe personenbeziehbar registriert werden dürfte.

Nicht nachvollziehbar ist zuletzt die Auffassung, das Datenschutzrecht gelte zwar nicht für die Speicherung, wohl aber für die Übermittlung „relativ“ personenbezogener Daten an eine Stelle mit Zusatzwissen. Die Vertreter der relativierenden Auffassung erkennen hier offenbar selbst, dass eine konsequente Anwendung ihrer Meinung, wonach kein Personenbezug gegeben sei, zu untragbaren Ergebnissen führte. Ihre in freier Rechtsschöpfung vorgenommene Einschränkung hinsichtlich der Datenübermittlung an Stellen mit Zusatzwissen findet jedoch ebenso wenig eine Stütze im Gesetz. Die gesetzlichen Regelungen sowohl der Datenspeicherung wie auch der Datenübermittlung beziehen sich gleichermaßen auf personenbezogene Daten. Es ist in sich widersprüchlich, dass ein und dasselbe Datum für ein und dieselbe Stelle personenbezogen sein soll, wenn es übermittelt werden soll, nicht aber, wenn es gespeichert werden soll.

Die These eines relativen Personenbezugs ist daher mit dem Gesetz nicht in Einklang zu bringen. Sie wird auch in der Rechtsprechung zurecht nicht heran gezogen.

bb) Laut Bundesdatenschutzgesetz sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 BDSG). „Bestimmbar“ bedeutet dabei „zuordnungsfähig“, „ermittelbar“, „feststellbar“.

Das Amtsgericht Mitte hat im Vorprozess (Az. 5 C 314/06) den Begriff der Bestimmbarkeit getreu seiner sprachlichen Bedeutung angewandt. Das Gericht hat entschieden, dass die von einem Internet-Zugangsanbieter temporär zugewiesene Internetkennung (dynamische IP-Adresse) nicht nur bei dem Internet-Zugangsanbieter, sondern auch bei Anbietern von Telemedien im Internet ein personenbezogenes Datum darstelle. Welcher Nutzer sich hinter einer IP-Adresse verbirgt, ist in der Tat auch im zuletzt genannten Fall bestimmbar – zwar nicht notwendig anhand der dem Inhalteanbieter vorliegenden Daten, aber jedenfalls mithilfe weiterer Daten, nämlich der Einwahlprotokolle des Internet-Zugangsanbieters.

Das Gericht hat seine Entscheidung wie folgt begründet:

> „*Dynamische IP-Adressen stellen in Verbindung mit den weiteren von der Beklagten ursprünglich gespeicherten Daten personenbezogene Daten im Sinne des § 15 TMG dar, da es sich um Einzelangaben über bestimmbare natürliche Personen im Sinne des § 3 Abs. 1 Bundesdatenschutzgesetz handelt. Die EG-Richtlinie 95/46/EG (Datenschutzrichtlinie-Erwägungsgründe) bestimmt unter Ziffer 26, dass bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden müssen, die vernünftiger Weise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden können, um die betreffende Person zu bestimmen. Nach zutreffender Ansicht des Hessischen Datenschutzbeauftragten (aaO) ist es durch die Zusammenführung der personenbezogenen Daten mit Hilfe Dritter bereits jetzt ohne großen Aufwand in den meisten Fällen möglich, Internetnutzer aufgrund ihrer IP-Adresse zu identifizieren. Eine Verneinung des Personenbezuges von dynamischen IP-Adressen mit der Folge der Nichtanwendbarkeit des TDDSG und TDSV, beziehungsweise jetzt des TMG und des TKG, hätte zur Folge, dass diese Daten ohne Restriktionen an Dritte z.B. den Access-Provider übermittelt werden könnten, die ihrerseits die Möglichkeit haben, den Nutzer aufgrund der IP-Adresse zu identifizieren, was mit dem Grundgedanken des Datenschutzrechts nicht vereinbar ist. Abgesehen davon wird die Rechtsauffassung der Beklagten insoweit nicht geteilt, als vorgetragen wird, dass eine Bestimmbarkeit der Person nur gegeben sei, wenn der Betroffene mit legalen Mitteln identifiziert werden könne. Zu Recht weist der Kläger darauf hin, dass das Datenschutzrecht gerade vor dem Missbrauch von Daten schützen soll, so dass eine derartige Einschränkung des Begriffs der Bestimmbarkeit von Personen seitens des Gerichts als nicht gerechtfertigt erachtet wird.*“

Die in Bezug genommene „Orientierungshilfe zum Umgang mit personenbezogenen Daten bei Internetdiensten“ [7] des Arbeitskreis Medien der deutschen Konferenz der Datenschutzbeauftragten des Bundes und der Länder führt unter Punkt 3.1 aus:

> „*Betrachtet man die Möglichkeiten anderer Anbieter (beispielsweise Inhalts-Anbieter) eine Identifikation anhand der IP-Adresse vorzunehmen,*

7 http://www.datenschutz.hessen.de/Tb31/K25P03.htm.

so sind hier die Möglichkeiten der Zusammenführung der personenbezogenen Daten im Internet zu berücksichtigen. Mit Hilfe Dritter ist es bereits jetzt ohne großen Aufwand in den meisten Fällen möglich, Internet-Nutzer und -Nutzerinnen aufgrund ihrer IP-Adresse zu identifizieren. Wenn z.B. für Inhalte-Anbieter der Personenbezug von IP-Adressen verneint und das TDDSG beziehungsweise die TDSV nicht für anwendbar erklärt werden, hätte dies nicht nur die mit dem Grundrechtsschutz unvereinbare Konsequenz, dass der Diensteanbieter die Daten unbegrenzt selbst verarbeiten oder nutzen könnte, sondern er dürfte diese Daten auch ohne Restriktionen an Dritte übermitteln, die ihrerseits die Möglichkeit hätten, den Nutzer aufgrund der IP-Adresse zu identifizieren. Es bedarf keiner näheren Begründung, dass dies dem Schutzgedanken des Datenschutzrechts diametral zuwiderlaufen würde. Dynamische IP-Adressen sind daher personenbezogene Daten, da sie durch Zusammenführung mit den dahinter stehenden Zuordnungstabellen den Rückschluss auf bestimmbare Personen zulassen (vgl. §§ 3 Abs. 1 BDSG, 1 Abs. 2 TDDSG).“

Auch die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) heraus gegebenen Handlungsempfehlungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder für E-Government-Angebote führen aus[8]:

„*Die Frage, ob IP-Nummern personenbezogen sind, ist von großer Bedeutung, weil an verschiedenen Stellen des Internets IP-Adressen – teilweise zusammen mit anderen Nutzungsdaten – protokolliert werden und durch Zusammenführen dieser Daten Profile über das Nutzungsverhalten erstellt werden können. Auf jeden Fall sind statische IP-Adressen personenbezogene Daten, da diese einen direkten und andauernden Bezug zu dem Nutzenden enthalten und auf diesen ohne weiteres rückschließen lassen. Mit Hilfe Dritter ist es darüber hinaus aber bereits jetzt in vielen Fällen möglich, Internet-Nutzer und -Nutzerinnen auch bei nicht-statischen IP-Adressen zu identifizieren. Dynamische IP-Adressen müssen daher ebenfalls als personenbezogene Daten behandelt werden, da sie durch Zusammenführung mit den dahinter stehenden Zuordnungstabellen den Rückschluss auf bestimmbare Personen zulassen (vgl. §§ 3 Abs. 1 BDSG, 1 Abs. 2 TDDSG). Als Folge dieser Zuordnung sind für das Erhe-*

8 http://www.bsi.de/fachthem/egov/download/2_Daten.pdf, 13.

> *ben, Verarbeiten, Nutzen und auch Löschen von IP-Adressen die Vorschriften für Verbindungs- bzw. Nutzungsdaten anzuwenden.*“

Im Ergebnis ebenso hat das Landgericht Frankenthal mit Beschluss vom 21.05.2008 (Az.: 6 O 156/08) entscheiden:

> „*Im Übrigen sind nach Ansicht der Kammer dynamische IP-Adressen auch personenbezogen i.S.d. personenbezogenen Berechtigungskennungen gemäß § 96 Abs. 1 Nr. 1 TKG. [...] Die Kammer sieht danach unter Berücksichtigung aller Umstände die dynamischen IP-Adressen als Verkehrsdaten i.S.d. § 3 Ziff. 30 TKG an, da diese Daten im Zusammenhang mit der Inanspruchnahme von Telekommunikationsdiensten stehen und sich so erkennen lassen.*“

Das Amtsgericht Wuppertal hat schon mit Urteil vom 03.04.2007 entschieden (NStZ 2008, 161):

> „*Nach der Legaldefinition des § 3 Abs. 1 BDSG sind Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Solche Daten fallen grundsätzlich auch bei IP-Adressen und Zugangsdaten an. Denn insbesondere die IP-Adresse kann jederzeit zurückverfolgt und einer bestimmten Person zugeordnet werden.*“

Dass bei Anbietern von Telediensten gespeicherte IP-Adressen personenbezogene Daten darstellen, hat das Landgericht Berlin bereits früher entschieden (Az. 27 O 616/05 vom 10.11.2005, CR 2006, 418). In Bezug auf einen Anbieter von Inhalten im Internet hat es ausgeführt:

> „*Bei den begehrten Daten Namen und Anschrift handelt es sich, anders als die dynamischen IP-Adressen, die als Nutzungsdaten anzusehen sind, auch um sogenannte Bestandsdaten (vgl. Spindler u.a., TDG, 2004, § 3 TDDSG, Rn. 5).*“

Das Gericht geht also ohne Weiteres davon aus, dass dynamisch vergebene IP-Adressen die Herstellung eines Personenbezugs ermöglichen und deswegen als Nutzungsdaten dem TDDSG – heute TMG – unterliegen. Nutzungsdaten im Sinne des Gesetzes sind nämlich nur personenbezogene Daten (§ 15 TMG).

Die Artikel 29-Gruppe der Datenschutzbeauftragten der Europäischen Union hat erstmals in ihrer Stellungnahme vom 21.11.2000 festgestellt:[9]

> „*Wie in diesem Arbeitspapier bereits erwähnt wurde, können Internet-Zugangsanbieter und Verwalter von lokalen Netzwerken ohne großen Aufwand Internet-Nutzer identifizieren, denen sie IP-Adressen zugewiesen haben, da sie in der Regel in Dateien systematisch Datum, Zeitpunkt, Dauer und die dem Internet-Nutzer zugeteilte dynamische IP-Adresse einfügen. Dasselbe lässt sich von den Internet-Diensteanbietern sagen, die in ihren HTTP-Servern Protokolle führen. In diesen Fällen besteht kein Zweifel, dass man von personenbezogenen Daten im Sinne von Artikel 2 Buchstabe a) der Richtlinie 95/46/EG reden kann.*“

In ihrer Stellungnahme 2/2002 vom 30.05.2002 hat die Gruppe erneut festgestellt:[10]

> „*Die Datenschutzgruppe möchte betonen, dass es sich bei IP-Adressen, die den Internetnutzern zugewiesen werden, um personenbezogene Daten handelt, die durch die Richtlinie 95/46/EG und 97/66/EG geschützt sind.*“

Zuletzt haben die EU-Datenschützer in ihrer Stellungnahme 4/2007 vom 20.06.2007 mit dem Titel „zum Begriff 'personenbezogene Daten'“ festgestellt:[11]

> „*Dynamische IP-Adressen*
>
> *Die Datenschutzgruppe hat IP-Adressen als Daten, die sich auf eine bestimmbare Person beziehen, eingestuft. In ihrer Begründung heißt es: '[…] können Internet-Zugangsanbieter und Verwalter von lokalen Netzwerken ohne großen Aufwand Internet-Nutzer identifizieren, denen sie IP-Adressen zugewiesen haben, da sie in der Regel in Dateien systematisch Datum, Zeitpunkt, Dauer und die dem Internet-Nutzer zugeteilte dynamische IP-Adresse einfügen. Dasselbe lässt sich von den Internet-Diensteanbietern sagen, die in ihren HTTP-Servern Protokolle führen. In diesen Fällen besteht kein Zweifel, dass man von personenbezogenen*

9 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37de.pdf, 17.
10http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp58_de.pdf, 3.
11http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf, 19.

Daten im Sinne von Artikel 2 Buchstabe a) der Richtlinie 95/46/EG reden kann."

b) Bestimmbarkeit der Person anhand der IP-Adresse

aa) Bestimmbarkeit im Sinne des § 3 BDSG

Wie oben dargelegt, ist anhand der von der Beklagten erstellten Zugriffsprotokolle bestimmbar, welche Zugriffe von mir stammen, welche Seiten ich betrachtet habe, welche Suchbegriffe ich eingegeben habe usw.

Die Beklagte speichert unstreitig unter anderem die IP-Adresse jedes „zugreifenden Hostsystems", also auch des Systems, das mir den Zugang zum Internet vermittelt. In meinem Fall handelte es sich um Rechner des Internet-Zugangsanbieters Hansenet. Hansenet speichert fünf Tage lang, welchem Internet-Zugangskunden welche IP-Adresse zu welchem Zeitpunkt zur Benutzung zugewiesen war. Kombiniert man die von der Beklagten gespeicherten Protokolle mit den Protokollen und Bestandsdaten von Hansenet, lässt sich meine Person ermitteln und lassen sich die einzelnen von mir auf den Portalen der Beklagten besuchten Seiten einschließlich meiner Sucheingaben (Suchwörter) nachvollziehen.

All dies bestreitet die Beklagte nicht. Die Beklagte vertritt lediglich die unzutreffende Auffassung, ihre Protokolldaten seien keine personenbezogenen Daten im Rechtssinne.

bb) Bestimmbarkeit für die Beklagte

Die Beklagte führt an, sie selbst könne meine Person anhand ihrer Protokolle nicht identifizieren. Hierauf kommt es nach dem Gesetz jedoch nicht an, weil nach § 3 BDSG und der Datenschutzrichtlinie 95/46/EG die Bestimmbarkeit durch Verknüpfung mit weiteren Daten genügt. Dass meine Person auf diese Weise bestimmbar ist, ist oben bereits ausgeführt worden.

Übrigens heißt es in der eigenen Datenschutzerklärung des Bundesinnenministeriums:[12]

„*Bei jedem Zugriff auf unsere Server werden Daten für statistische und Sicherungszwecke gespeichert. Wir erfassen hier lediglich für eine be-*

12http://www.bmi.bund.de/cln_012/nn_122688/Internet/Navigation/DE/Service/Impressum/ImpressumNode.html__nnn=true.

> *grenzte Zeit die IP-Adresse Ihres Internet Service Providers, Datum und Uhrzeit sowie die Website, die Sie bei uns besuchen. Diese Daten werden ausschließlich zur Verbesserung unseres Internetdienstes genutzt und nicht auf Sie zurückführbar ausgewertet. Wir behalten uns das Recht vor, im Falle von schweren Verstößen gegen unsere Nutzungsbedingungen und bei unzulässigen Zugriffen bzw. Zugriffsversuchen auf unsere Server unter Zuhilfenahme einzelner Datensätze eine Herleitung zu personenbezogenen Daten zu veranlassen.*“

Die Beklagte gesteht damit selbst ein, dass eine Bestimmung des Nutzers anhand ihrer Protokolldaten möglich ist.

4. Freiwillige Preisgabe des Personenbezugs

Die personenbezogene Nachverfolgung meines Nutzungsverhaltens anhand der IP-Adresse ist der Beklagten auch möglich, wo ich aufgrund einer Anmeldung oder Bestellung meine Person gegenüber der Beklagten offenlegen muss.

a) Entgegen der Auffassung der Beklagten berechtigt sie diese freiwillige Offenlegung – etwa zum Zweck einer Bestellung – nicht, auch mein gesamtes sonstiges Internet-Nutzungsverhalten personenbeziehbar zu speichern. Die Bestellung hat mit meinem Informationsverhalten auf ihren Portalen nichts zu tun. Nach der Argumentation der Beklagten wäre sie von dem gesamten Datenschutzrecht ausgenommen, weil die Benutzung ihrer Telemedien freiwillig ist. Dies entspricht dem Telemediengesetz nicht.

b) Die Beklagte meint weiter irrig, bestimmbar sei der Nutzer nur, wenn seine Formulareingaben zusammen mit der IP-Adresse erfasst und gespeichert würden.

aa) Dass dies nicht praktiziert werde, kann sie sodann nur für einen Teil ihrer Angebote behaupten. Unzutreffend ist dies jedenfalls bei anderen Angeboten der Beklagten. So heißt es in der Datenschutzerklärung des Portals bundestag.de:[13]

> „*Erfassung der IP-Adresse bei Verwendung des Kontaktformulars für Abgeordnete*
>
> *Aus Sicherheitsgründen wird dem Empfänger die IP-Adresse des Benutzers übermittelt. Dies ist zwingende Voraussetzung für die Verwendung des Kontaktformulars.*“

13http://www.bundestag.de/interakt/impressum/index.html.

bb) Schon die Ausgangsbehauptung der Beklagten, dass eine Identifizierung bei getrennter Speicherung der IP-Adresse nicht möglich sei, ist falsch:

Auch bei separater Speicherung von Formulardaten und IP-Adresse kann die Beklagte sehen, dass ich beispielsweise um 11:39:10 Uhr eine Bestellung unter meinem Namen aufgegeben habe. Sie kann dann in ihren separat gespeicherten Zugriffsprotokollen nachsehen, wer um 11:39:10 Uhr eine Bestellung abgesandt hat. In ihren Zugriffsprotokollen wird nämlich nicht nur der Abruf von Daten festgehalten („http-GET-request“), sondern auch das Absenden von Daten („http-POST-request“). Dies trägt die Beklagte selbst vor. Dass der Formularinhalt nicht in dem Zugriffsprotokoll festgehalten wird, ändert nichts daran, dass eine Verknüpfung der Daten auf die beschriebene Weise möglich ist.

Soweit die Beklagte vorträgt, bei Bestellungen würde der „genaue Zeitpunkt des Server Zugriffs“ nicht übermittelt, ist ihr Vortrag ungenau und nicht einlassungsfähig. Selbstverständlich wird bei der Übermittlung von Bestellungen per E-Mail stets automatisch die sekundengenaue Zeit übermittelt, zu welcher der Rechner die E-Mail versandt hat. Dieser E-Mail-Versand erfolgt unmittelbar nach Aufzeichnung des Bestellvorgangs im Zugriffsprotokoll der Beklagten. Da die Beklagte nicht jede Sekunde eine Bestellung erhält, ist eine eindeutige Zuordnung selbst im Fall einer geringfügigen Verzögerung möglich; in der Praxis ist vielleicht eine Verzögerung um eine Sekunde denkbar.

c) Anders als die Beklagte meint, kann sie sehr wohl ganz regelmäßig aus der Tatsache, dass ich mit einer IP-Adresse eine Bestellung abgegeben habe, darauf schließen, dass Zugriffe unmittelbar davor und danach mit derselben IP-Adresse ebenfalls von mir stammen. Nahe liegt dies beispielsweise bei den Seiten und Suchwörtern, mit deren Hilfe ich überhaupt erst auf die Bestellseite gelangen konnte, sowie bei thematisch verwandten Seiten.

Weiter erleichtert werden kann die Zuordnung, wo neben IP-Adresse, Zeitpunkt und Seitenbezeichnung auch das Feld „verwendeter Internet-Browser und Betriebssystem“ gespeichert wird, wie etwa auf dem Portal www.bmas.de. [14] Dieses Feld ermöglicht sehr detaillierte Rückschlüsse auf das eingesetzte System (z.B. „Mozilla/5.0 (Windows; U; Windows NT 5.0; de; rv:1.8.1.1) Gecko/20061204 Firefox/2.0.0.1“) und ist mit großer Wahrscheinlichkeit von Nutzer zu Nutzer verschieden. Wenn in zeitlichem Zusammenhang mit derselben IP-Adresse und demsel-

14http://www.bmas.de/coremedia/generator/17608/impressum.html.

ben System Seiten abgerufen werden, ist mit hoher Wahrscheinlichkeit der Rückschluss auf ein und dieselbe Person möglich.

Bei einigen Angeboten der Beklagten werden darüber hinaus sogenannte „Cookies“ eingesetzt, um die besuchten Seiten den einzelnen Nutzern eindeutig zuordnen zu können. So wird auf dem Portal www.bfn.de jedem Besucher eine eindeutige Sitzungskennung zugewiesen und im Rechner des Nutzers gespeichert. Diese Kennung protokolliert der Anbieter sodann bei jedem Seitenaufruf zusammen mit dem Namen der aufgerufenen Seite.[15] Ebenso erfolgt dies etwa bei den Portalen www.bmelv.de und www.bund.de. Auch dadurch lässt sich im Fall einer namentlichen Bestellung oder Anmeldung das gesamte Nutzungsverhalten personenbezogen nachvollziehen.

d) Die Beklagte verkennt, dass der Begriff der Bestimmbarkeit nicht erfordert, dass jeder Nutzer in jedem Einzelfall mit 100%-iger Sicherheit bestimmbar ist. Es genügt, wenn eine Identifizierung teilweise oder gar typischerweise möglich ist. Denn personenbeziehbar sind dann zumindest diejenigen Daten, die eine Identifizierung des Nutzers ermöglichen. Da die Beklagte aus ihrer Protokollierungspraxis personenbeziehbare Zugriffe nicht ausnehmen kann, muss sie für alle Zugriffe das Datenschutzrecht einhalten.

Die in der Artikel 29-Gruppe zusammen geschlossenen Datenschutzbeauftragten der EU-Mitgliedsstaaten haben dementsprechend festgestellt:[16]

> „*Es könnte argumentiert werden, dass die für die Nutzung von Computer X während eines bestimmten Zeitraums erfassten Daten keine Identifizierung des Nutzers unter Einsatz vernünftiger Mittel gestatten und daher nicht als personenbezogene Daten anzusehen sind. Hier ist jedoch anzumerken, dass die Internet-Diensteanbieter höchstwahrscheinlich nicht wissen, ob eine bestimmte IP-Adresse die Identifizierung ermöglicht oder nicht und daher die mit dieser IP-Adresse verknüpften Daten genauso verarbeiten wie Informationen, die mit IP-Adressen von ordnungsgemäß registrierten und bestimmbaren Benutzern verknüpft sind. Wenn der Internet-Diensteanbieter also nicht mit absoluter Sicherheit erkennen kann, dass die Daten zu nicht bestimmbaren Benutzern gehören, muss er sicherheitshalber alle IP-Informationen wie personenbezogene Daten behandeln.*“

15http://www.bfn.de/impressum.html.

16http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf, 20.

Schon das Amtsgericht Mitte hat es im Vorprozess zutreffend genügen lassen, dass es „in den meisten Fällen möglich [ist], Internetnutzer aufgrund ihrer IP-Adresse zu identifizieren."

e) Dass eine getrennte Speicherung der Formulareingaben die Identifizierung des Nutzers nicht ausschließt, ist bereits oben unter b) ausgeführt worden.

V. Keine Notwendigkeit der Aufzeichnung von IP-Adressen

1. „Angriffsszenarien und Sicherheitsmaßnahmen" der Beklagten

Die Beklagte macht geltend, zur Aufrechterhaltung der Funktionsfähigkeit ihrer Telemedien sei es erforderlich, eine personenbeziehbare, dauerhafte, verdachts- und anlasslose Aufzeichnung der gesamten Nutzung ihrer Telemedien vorzunehmen. Dies ist sowohl sachlich falsch (a) wie auch rechtlich unerheblich (b):

a) In sachlicher Hinsicht wird die Argumentation der Beklagten schon dadurch widerlegt, dass sie selbst unstreitig mehrere Portale ohne Aufzeichnung von IP-Adressen anbietet, ohne dass diese Angebote häufiger gestört oder sonst beeinträchtigt wären als ihre sonstigen Portale. Ohne Speicherung von IP-Adressen bietet die Beklagte etwa die Portale www.bmj.bund.de, inzwischen auch www.bfdi.bund.de, außerdem www.bundesrechnungshof.de, www.bmbf.de und – mit Ausnahme der beschriebenen Speicherpraxis hinsichtlich einzelner Seiten – das Portal des Bundeskriminalamts www.bka.de an. [17] Die Beklagte widerlegt also in ständiger Praxis ihre eigene Argumentation.

b) In rechtlicher Hinsicht nennt die Beklagte keine einzige Norm, aus der sich eine Zulässigkeit der verschiedenen von ihr praktizierten Auswertungen ergeben soll. Vielmehr untersagt § 15 TMG eindeutig die Speicherung von Nutzungsdaten über die Dauer des Nutzungsvorgangs hinaus.

Im Hinblick auf die sachliche Selbstwiderlegung und die rechtliche Unerheblichkeit verzichte ich darauf, auf die einzelnen Datennutzungen der Beklagten einzugehen und im Einzelnen zu widerlegen, dass anlasslos protokollierte IP-Adressen zur Aufrechterhaltung des Betriebs erforderlich seien. Sollte das Hohe Gericht die von der Beklagten beschriebenen „Angriffsszenarien und Sicherheitsmaßnahmen" hingegen für erheblich halten, so erbitte ich einen entsprechenden Hinweis, um dazu näher ausführen zu können.

17 Parl. Staatssekretär beim Bundesinnenministerium Peter Altmaier, BT-Prot. 16/118, 12277.

2. Stand der Technik

Die Behauptung der Beklagten, die personenbeziehbare Totalprotokollierung des Nutzungsverhaltens sämtlicher Nutzer entspreche dem Stand der Technik, ist sowohl sachlich falsch (a) wie auch rechtlich unerheblich (b).

a) Die von der Beklagten zitierten technischen Vorschriften sehen eine solche Totalprotokollierung für öffentlich zugängliche Telemedien nicht vor. Das Gegenteil ergibt sich aus den vom Bundesamt für Sicherheit in der Informationstechnik (BSI) heraus gegebenen Handlungsempfehlungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder für E-Government-Angebote.[18] In diesen Empfehlungen heißt es:

S. 33:

- *Bei reinen Informationsangeboten sollte auf eine vollständige Erfassung der IP-Adressen der Nutzer verzichtet werden, da diese für die Erbringung des Angebots und seine Abrechnung nicht erforderlich sind. Für die statistische Auswertung reichen gekürzte IP-Adressen aus.*

- *Bei E-Government-Dienstleistungen dürfen nur diejenigen Nutzungsvorgänge protokolliert werden, bei denen dies aufgrund gesetzlicher Vorgaben erforderlich ist (z. B. automatisierte Abrufverfahren). Darüber hinaus dürfen Daten dann gespeichert werden, wenn konkrete Anhaltspunkte für eine missbräuchliche Inanspruchnahme vorliegen und soweit die Daten zur Missbrauchsaufklärung erforderlich sind. Diese Daten dürfen nicht für andere Zwecke genutzt werden.*

S. 39:

> *Wenn die Nutzung eines Angebots die Erhebung personenbezogener Daten voraussetzt, sind die Nutzer über die Zweckbestimmung der Verarbeitung, für die die Daten bestimmt sind, zu unterrichten. Wenn Daten in Log-Dateien gespeichert werden, könnte eine Information folgendermaßen aussehen:*

18http://www.bsi.de/fachthem/egov/download/2_Daten.pdf.

Mit Ihrem Zugriff auf diese Seite werden die um die letzten drei Ziffern verkürzte IP-Adresse Ihres Rechners und weitere Angaben (Datum, Uhrzeit, betrachtete Seite) auf unserem Server für Zwecke der Datensicherheit für zwei Monate gespeichert. Die Daten werden außerdem für statistische Zwecke ausgewertet. Durch die Verkürzung der IP-Adresse ist der Bezug der gespeicherten Daten auf Ihre Person ausgeschlossen.

Wir verwenden keine Cookies, Java-Applets oder Active-X-Controls. Sollten Sie noch Fragen zum Datenschutz haben, wenden Sie sich bitte an: […]

S. 40 (Elektronischer Behördenwegweiser/Informationsangebote):

- *Elektronische Behördenwegweiser müssen so gestaltet werden, dass die Bürgerinnen und Bürger grundsätzlich ohne Nennung ihres Namens die erforderlichen Informationen erhalten.*

- *Eine personenbezogene Protokollierung der Abfragen hat zu unterbleiben.*

S. 49 (Protokollierungen der Nutzung):

Die Protokolldaten werden bei kostenfreier Nutzung des Online-Dienstes nach Ende der jeweiligen Nutzung gelöscht; bei kostenpflichtiger Nutzbarkeit sind die Protokolldaten spätestens nach Ablauf von sechs Monaten nach Versendung der Rechnung und des Einzelnachweises zu löschen, soweit es nicht zu Einwendungen gekommen ist oder nach bereichsspezifischen Regelungen besondere Aufbewahrungsfristen zu beachten sind.

Für die Telemedien der Beklagten entspricht es also umgekehrt dem Stand der Technik, eine personenbeziehbare Totalprotokollierung des Nutzungsverhaltens zu unterlassen.

b) Im Übrigen sind die von der Beklagten angeführten technischen Normwerke rechtlich unerheblich. Für die Beklagte verbindlich ist das deutsche Recht, namentlich § 15 TMG, und nicht technische Industrienormen.

VI. Keine Zulässigkeit der Speicherung nach § 100 TKG

Die Speicherung von IP-Adressen durch die Beklagte ist auch nicht nach § 100 TKG gerechtfertigt. Die Vorschrift ist nicht anwendbar (1.) und rechtfertigt ohnehin keine globale und pauschale Totalprotokollierung (2.).

1. Kein geschäftsmäßiges Erbringen von Telekommunikationsdiensten

Auf die streitgegenständlichen öffentlichen Telemedien der Beklagten findet § 100 TKG keine Anwendung. Vielmehr hat der Gesetzgeber die Zulässigkeit der Datenverarbeitung durch Anbieter von Telemedien im Telemediengesetz abschließend geregelt. Dies ergibt sich aus § 12 Abs. 1 TMG, der bestimmt:

> „*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.*“

§ 100 TKG ist weder Bestandteil des Telemediengesetzes, noch bezieht er sich ausdrücklich auf Telemedien.

Dass der Gesetzgeber die Verarbeitung von Nutzungsdaten im Telemediengesetz abschließend regeln und den Rückgriff auf andere Vorschriften gerade ausschließen wollte, ergibt sich auch aus der folgenden Passage in der Begründung des Gesetzentwurfs:[19]

> „*Gesetzliche Erlaubnistatbestände außerhalb des TMG greifen nur dann, wenn sie sich ausdrücklich auf Telemedien beziehen.*“

Der Gesetzgeber war sich dabei bewusst, dass das Angebot von Telemedien in technischer Hinsicht notwendig eine Übertragung per Telekommunikation voraus setzt. Dementsprechend heißt es in § 1 Abs. 1 S. 1 TMG:

> „*Dieses Gesetz gilt für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen [...] sind (Telemedien).*“

Der Gesetzgeber wollte aus dem Anwendungsbereich des Gesetzes also nur solche Dienste ausnehmen, die ausschließlich die Übertragung von Signalen zum Gegenstand haben. Dass die Angebote der Beklagten nicht ausschließlich eine

---

19 BT-Drs. 16/3078, 16.

Übertragungsleistung zum Gegenstand haben, sondern vielmehr hauptsächlich eine inhaltliche Informationsleistung, liegt auf der Hand.

Des weiteren hat der Gesetzgeber die Abgrenzung zu den Datenschutzregelungen des TKG in § 11 Abs. 3 TMG geregelt, in dem es heißt:

> „*Bei Telemedien, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, gelten für die Erhebung und Verwendung personenbezogener Daten der Nutzer nur § 12 Abs. 3, § 15 Abs. 8 und § 16 Abs. 2 Nr. 2 und 5.*“

Dazu heißt es in der Gesetzesbegründung:[20]

> „*In § 11 Abs. 3 erfolgt eine Ergänzung zum Geltungsbereich der Datenschutzbestimmungen bei Telemediendiensten, die zugleich dem TK-Datenschutz unterliegen. Für diese Telemedienanbieter (Internet-Access, E-Mail- Übertragung) gelten ohnehin die Datenschutzvorschriften des TKG.*“

Die Telemedien der Beklagten haben hingegen nicht überwiegend eine Übertragungsleistung zum Gegenstand, wie es bei Internetzugang und E-Mail der Fall ist. Vielmehr überwiegt bei den Telemedien der Beklagten eindeutig das Angebot von Inhalten, also von Informationen. In der Gesetzesbegründung heißt es:[21]

> „*Unter „Telemediendienste“ fallen alle übrigen Informations- und Kommunikationsdienste, die also nicht ausschließlich Telekommunikationsdienste oder Rundfunk sind. Diese erstrecken sich auf einen weiten Bereich von wirtschaftlichen Tätigkeiten, die – sei es über Abruf- oder Verteildienste – elektronisch in Form von Bild-, Text- oder Toninhalten zur Verfügung gestellt werden.*“

Die Telemedien der Beklagten stellen solche Dienste dar. Damit verdrängt das TMG das Telekommunikationsgesetz; § 100 TKG ist nicht anwendbar.

2. Keine gleichzeitige Anwendung von TKG und TMG

Mit den angeführten Regelungen hat der Gesetzgeber – außerhalb des § 11 Abs. 3 TMG – eine gleichzeitige Anwendung von TKG und TMG ausgeschlossen, wie sich aus der Gesetzesbegründung ergibt.

---

20 BT-Drs. 16/3078, 15 f.

21 BT-Drs. 16/3078, 13.

3. Unzulässigkeit der Speicherung nach § 100 Abs. 1 TKG

Dass § 100 TKG auch im Rahmen seines Anwendungsbereichs keine Totalprotokollierung personenbezogener Daten rechtfertigt, führt bereits die Klageschrift näher aus.

a) Keine Erforderlichkeit der Speicherung von IP-Adressen

Dass die Speicherung von IP-Adressen für das Angebot eines Telemediums nicht erforderlich ist, ist bereits in der Klageschrift näher ausgeführt und wird belegt durch die von der Beklagten selbst betriebenen Portale www.bmj.bund.de, www.bfdi.bund.de, www.bundesrechnungshof.de und www.bmbf.de.

Auch der Gesetzgeber hat mit § 100 TKG keineswegs eine Totalprotokollierung sämtlicher IP-Adressen legitimieren wollen. Vielmehr heißt es in der von der Beklagten angeführten Begründung des Gesetzentwurfs wörtlich:[22]

> „*Zur Verhinderung von Missbrauch und zur Datensicherheit können hiervon auch IP-Adressen erfasst sein, sofern sie der Erbringung von Telekommunikationsdiensten dienen.*“

Dass von § 100 TKG auch IP-Adressen erfasst sein können, ist unbestritten. Mit keinem Wort spricht die Gesetzesbegründung aber davon, dass eine anlasslose Totalprotokollierung sämtlicher IP-Adressen von § 100 TKG abgedeckt sein soll. Ermöglichen wollte der Gesetzgeber vielmehr eine einzelfallbezogene Protokollierung im Störungs- oder Missbrauchsfall.

b) Präventive Speicherung unzulässig

§ 100 TKG ist mit dem Landgericht Darmstadt zutreffend so auszulegen, dass er dem verfassungsrechtlichen Verbot der Speicherung personenbezogener Daten auf Vorrat Rechnung trägt. Dazu ist bereits im Einzelnen in der Klageschrift ausgeführt worden.

Das Merkmal des „Erkennens“ von Störungen macht auch in der genannten Auslegung des § 100 TKG Sinn. Denn § 100 TKG erlaubt nicht nur die Erhebung von Bestands- und Verkehrsdaten, sondern auch ihre Verwendung. Die Verwendung ohnehin zu Abrechnungszwecken gespeicherter Daten zum Erkennen von Störungen mag angehen. Die Erhebung weiterer Daten ist möglicherweise im Einzelfall

---

22 BT-Drs. 15/2316, 90.

und zeitlich befristet bei besonders störanfälligen Diensten erforderlich, um immer wieder kehrende Störungen erkennen und ihre Ursachen beseitigen zu können. Keinesfalls ist dem Wortlaut des § 100 TKG aber zu entnehmen, dass eine einzelfallunabhängige Aufzeichnung des gesamten Nutzerverhaltens zugelassen werden soll. Dies wäre mit dem Verhältnismäßigkeitsgebot des Grundgesetzes nicht in Einklang zu bringen und würde auch systematisch dem Grundsatz des § 96 Abs. 2 S. 2 TKG widersprechen, wonach „Verkehrsdaten vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen“ sind. Dieser Vorschrift hätte es nicht bedurft, wenn der Gesetzgeber mit § 100 TKG eine generelle Protokollierung hätte zulassen wollen.

Soweit die Beklagte die Kommentierung zu § 100 TKG im Beck'schen TKG-Kommentar anführt, ist darauf hinzuweisen, dass der Kommentator, Dr. Felix Wittern, von Beruf betrieblicher Datenschutzbeauftrager der Firma AOL Deutschland Medien GmbH ist. [23] Das Unternehmen AOL, das im Eigentum einer US-amerikanischen Muttergesellschaft steht, verdient sein Geld unter anderem als Anbieter von Internet-Zugangsdiensten. In den USA unterliegt AOL keinerlei Datenschutzgesetzen und praktiziert eine zeitlich unbegrenzte Speicherung des Nutzerverhaltens. Es liegt auf der Hand, dass der betriebliche Datenschutzbeauftragte von AOL ein berufliches Interesse daran hat, § 100 TKG eine möglichst weit gehende Zulässigkeit der Erhebung personenbezogener Daten auch in Deutschland zu entnehmen.

Was die Zitate der Beklagten von Gerichtsentscheidungen anbelangt, ist nur die Entscheidung des Amtsgerichts Bonn richtig und vollständig zitiert, wobei auch diese nur zu Internet-Zugangsanbieter betrifft.

Das Urteil des Landgerichts Darmstadt vom 06.06.2007 (Az. 10 O 562/03) stellt hingegen keineswegs eine Aufgabe der zutreffenden Rechtsprechung der 25. Zivilkammer desselben Gerichts dar (Urteil vom 25.01.2006, Az. 25 S 118/05). Vielmehr ist das Urteil der 10. Kammer in erster Instanz von einer Einzelrichterin gefällt worden und gegenwärtig beim Oberlandesgericht Frankfurt in der Berufungsinstanz anhängig. Die Beklagte beruft sich also auf ein Urteil, dass keine Rechtskraft entfaltet.

Das in der Klageschrift zitierte, in Kammerbesetzung gefällte Urteil der 25. Zivilkammer des Landgerichts Darmstadt (Urteil vom 25.01.2006, Az. 25 S 118/05)

23http://alice.aol.de/Portalkontakt-Datenschutz/Ansprechpartner-Thema-Datenschutz-AOL-1602562134-11.html.

ist demgegenüber rechtskräftig, nachdem der Bundesgerichtshof die dagegen eingelegte Revision nicht zugelassen hat (Beschluss vom 26.10.2006, Az. III ZR 40/06). In diesem Urteil des Landgerichts Darmstadt heißt es zutreffend:

> „*Nach § 100 Abs. 1 TKG darf der Diensteanbieter, soweit erforderlich, zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden. Nach Abs. 3 kann der Diensteanbieter bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte die Bestandsdaten und Verkehrsdaten erheben und verwenden, die zum Aufdecken sowie Unterbinden von Leistungserschleichungen und sonstigen rechtswidrigen Inanspruchnahmen der Telekommunikationsnetze und -dienste erforderlich sind.*
>
> *Es handelt sich bereits nach dem Wortlaut der Regelungen um vorfallsbezogene Maßnahmen, die die von der Beklagten durchgeführte generelle Speicherung aller Verkehrsdaten aller Kunden nicht erlaubt.*“

Unabhängig hiervon bleibt es dabei, dass § 100 TKG im vorliegenden Fall schon nicht anwendbar ist und sich auch die angeführten Urteile nur auf Internet-Zugangsanbieter beziehen. Die von der Beklagten angebotenen Telemedien sind nach dem Telemediengesetz zu beurteilen, das eine § 100 TKG entsprechende Vorschrift bewusst nicht enthält.

VII. Anträge

Die aktuellen Anträge werden nochmals wie folgt zusammen gefasst:

Es wird beantragt,

> **die Beklagte zu verurteilen, es zu unterlassen, die Internetprotokolladresse (IP-Adresse) des zugreifenden Hostsystems des Klägers, die im Zusammenhang mit der Nutzung öffentlich zugänglicher Telemedien der Beklagten im Internet – mit Ausnahme des Internetportals „http://www.bmj.bund.de“ – 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,**

hilfsweise:

> **die Beklagte zu verurteilen, es zu unterlassen, die Internetprotokolladresse (IP-Adresse) des zugreifenden Hostsystems des Klägers, die im Zusammenhang mit der Nutzung öffentlich zugänglicher Telemedien der Beklagten im Internet – mit Ausnahme des Internetportals „http://www.bmj.bund.de“ – übertragen wird, nebst dem Zeitpunkt des jeweiligen Nutzungsvorgangs 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.**

Vorsorglich wird daneben beantragt,

> **die Beklagte im Wege des Teilversäumnisurteils zu verurteilen, soweit nicht Telemedien des Bundesinnenministeriums betroffen sind.**

Eine Abschrift dieses Schriftsatzes wird gleichzeitig dem Beklagtenvertreter elektronisch übermittelt.

Patrick Breyer