Meinhard Starostik

Rechtsanwalt

Rechtsanwaltskanzlei:
Schillstr. 9 • 10785 Berlin
Tel.: 030 - 88 000 345
Fax: 030 - 88 000 346
email: Kanzlei@Starostik.de
USt-ID-Nr. DE165877648

RA Starostik, Schillstraße 9, 10785 Berlin

An das
Landgericht Berlin
Littenstraße 12 - 17
10179 Berlin

vorab per Fax: (030) 90 23 – 22 23

Kanzlei vereidigter Buchprüfer:
Schwarzenberger Str. 7 • 08280 Aue
Tel.: 03771-564 700

Berlin, den 26. März 2010

AZ: 45/08
(bitte stets angeben)

In dem Rechtsstreit
Breyer ./. Bundesrepublik Deutschland
Az.: 57 S 87/08

wird auf den Schriftsatz des Beklagtenvertreters vom 22.03.2010 wie folgt erwidert:

Der Schriftsatz des Beklagtenvertreters vom 22.03.2010 stellt größtenteils eine wortgleiche Wiedergabe der erstinstanzlichen Klageerwiderung der Beklagten dar. Um das Berufungsgericht nicht auch von Klägerseite mit Wiederholungen zu belasten, wird zur Erwiderung in erster Linie Bezug auf die Replik vom 06.07.2008 genommen, welche bereits die meisten Argumente des Beklagtenvertreters widerlegt. Nur soweit der Beklagtenvertreter neuen Vortrag anbringt, soll im Folgenden darauf ergänzend erwidert werden.

A. Rechtsweg

Ab Seite 1 der Replik vom 06.07.2008 ist bereits erläutert worden, weshalb der Rechtsweg zur Ordentlichen Gerichtsbarkeit eröffnet ist.

Der Beklagtenvertreter will der Kommentierung von Ehlers in Schoch/Schmidt-Aßmann/Pietzner das Gegenteil entnehmen. Dabei gibt er die dortige Kommentierung fehlerhaft wieder. Die Auffassung, Realakte der öffentlich-rechtlich organisierten Verwaltung seien immer öffentlich-rechtlich zu qualifizieren, sofern sie nicht in einem engen inneren und äußeren Zusammenhang mit der Wahrnehmung privatrechtlich zu erfüllender Aufgaben stehen, bezieht Ehlers ausdrücklich nur auf „die Zuordnung nicht normgeleiteter

Realakte".[1] Werden Realakte dagegen „in Vollziehung einer Rechtsnorm vorgenommen, teilen sie die Rechtsnatur dieser Norm".[2] Die Verarbeitung personenbezogener Nutzungsdaten durch die Beklagte erfolgt nach Maßgabe des § 15 TMG und teilt daher die privatrechtliche Rechtsnatur dieser Vorschrift.

Es entspricht der ständigen Rechtsprechung des Gemeinsamen Senats aller Obersten Bundesgerichte, dass sich der Rechtsweg in Ermangelung einer ausdrücklichen Regelung nach der Natur des Rechtsverhältnisses richtet, aus dem der Klageanspruch hergeleitet wird.[3] Dabei kommt es regelmäßig darauf an, ob die an der Streitigkeit Beteiligten zueinander in einem hoheitlichen Verhältnis der Über- und Unterordnung stehen und ob sich der Träger hoheitlicher Gewalt der besonderen, ihm zugeordneten Rechtssätze des öffentlichen Rechts bedient oder ob er sich den für jedermann geltenden zivilrechtlichen Regelungen unterstellt.[4] Der Kläger steht bei der Benutzung der Telemedien der Beklagten nicht in einem hoheitlichen Verhältnis der Über- und Unterordnung zu ihr. Auch bedient sich die Beklagte nicht besonderer, ihr zugeordneter Rechtssätze des öffentlichen Rechts. Vielmehr verarbeitet sie Nutzungsdaten nach „den für jedermann geltenden zivilrechtlichen Regelungen" des Telemediengesetzes, die – wie in der Replik vom 06.07.2008 näher ausgeführt – für öffentliche und nicht-öffentliche Stellen gleichermaßen gelten.

Zwar werden auch Gleichordnungsverhältnisse ausnahmsweise als öffentlich-rechtlich angesehen, wenn die das Rechtsverhältnis beherrschenden Rechtsnormen überwiegend den Interessen der Allgemeinheit dienen, wenn sie sich nur an Hoheitsträger wenden oder wenn der Sachverhalt einem Sonderrecht der Träger öffentlicher Aufgaben unterworfen ist und nicht Rechtssätzen, die für jedermann gelten.[5] Das Rechtsverhältnis zwischen Internetnutzer und Telemedienanbieter und insbesondere die Normen, die den Schutz der personenbezogenen Daten des Nutzers gewährleisten, dienen aber nicht überwiegend Interessen der Allgemeinheit, sondern gewährleisten das Grundrecht auf informationelle Selbstbestimmung des einzelnen Internetnutzers. Auch wendet sich das Telemediengesetz nicht nur an Hoheitsträger. Der Sachverhalt ist schließlich auch nicht einem Sonderrecht der Träger öffentlicher Aufgaben unterworfen, sondern Rechtssätzen, die für jedermann gelten, nämlich den Vorschriften des Telemedienrechts.

Der Kommentierung in Schoch/Schmidt-Aßmann/Pietzner zufolge ist ein Rechtsschutzbegehren nur dann öffentlich-rechtlicher Art im Sinne des § 40 VwGO, wenn es aus einer Regelung des öffentlichen Rechts hergeleitet werden kann[6] und die streitentscheidenden Normen dem öffentlichen Recht angehören.[7] Dass die §§ 15 TMG, 1004 BGB dem öffentlichen Recht zuzurechnen seien, behauptet selbst der Beklagtenvertreter nicht. Es handelt sich unzweifelhaft um privatrechtliche Normen.

---

[1] Ehlers in Schoch/Schmidt-Aßmann/Pietzner, § 40 VwGO, Rn. 392 f.

[2] Ehlers in Schoch/Schmidt-Aßmann/Pietzner, § 40 VwGO, Rn. 392.

[3] GmS-OGB, NJW 1988, 2295 m.w.N.

[4] GmS-OGB, NJW 1988, 2295 m.w.N.

[5] GmS-OGB, NJW 1990, 1527 m.w.N.

[6] Ehlers in Schoch/Schmidt-Aßmann/Pietzner, § 40 VwGO, Rn. 213.

[7] Ehlers in Schoch/Schmidt-Aßmann/Pietzner, § 40 VwGO, Rn. 215.

Dementsprechend richtet sich die Verarbeitung personenbezogener Nutzerdaten auch dann nach dem Telemediengesetz, wenn die Beklagte ein Internetportal zur Recherche von Markenbezeichnungen oder zum Angebot sonstiger Verwaltungsdienstleistungen anbietet. In der Replik vom 06.07.2008 ist bereits erläutert worden, dass die Verfolgung öffentlicher Zwecke die Anwendbarkeit des Privatrechts auf staatliches Handeln nicht hindert.

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

Prozessual gibt die Rechtswegrüge des Beklagtenvertreters **keinen Anlass, die Zulässigkeit des beschrittenen Rechtswegs vorab auszusprechen**. Nach der ständigen Rechtsprechung des Bundesgerichtshofs braucht ein Berufungsgericht dann nicht über die Zulässigkeit des beschrittenen Rechtswegs vorweg durch Beschluss zu entscheiden, wenn es die Zulässigkeit des Rechtswegs bejaht und im Falle der Entscheidung durch Beschluss keinen Anlass hätte, die Beschwerde nach § 17a Abs. 6 Satz 5 GVG zuzulassen.[1] Dieser Fall ist hier gegeben: Die Zulässigkeit des Rechtswegs ist gegeben und es besteht keinen Anlass, die Beschwerde nach § 17a Abs. 6 Satz 5 GVG zuzulassen. Weder ist die von Beklagtenseite aufgeworfene Rechtswegfrage von grundsätzlicher Bedeutung, noch weicht die Zulassung des Rechtswegs gar von der Entscheidung eines obersten Gerichtshofes des Bundes oder des Gemeinsamen Senats der obersten Gerichtshöfe des Bundes ab.

Eine gleichwohl erfolgende Vorabentscheidung würde dazu führen, dass das Verfahren ein weiteres Mal über Monate ausgesetzt werden müsste. Die Beklagte könnte über weitere Monate hinweg die Rechte des Klägers verletzen und die notwendigen Veränderungen für eine gesetzeskonforme Einrichtung ihrer Informationstechnik hinauszögern. Wie mit Schriftsatz vom 14.01.2010 bereits ausführlich erläutert und vom Berufungsgericht mit Beschluss vom 11.02.2010 anerkannt, gebietet die bisherige Verfahrensdauer eine zeitnahe Sachentscheidung. Dementsprechend bittet der Kläger, von einer Vorabentscheidung über die Zulässigkeit des Rechtswegs abzusehen.

B. Sachliche Zuständigkeit

Mit der Beklagten weiter über die sachliche Zuständigkeit zu streiten, ist müßig, nachdem das Berufungsgericht den Streitwert rechtskräftig auf 4.000 Euro festgesetzt hat. Die Beklagte kann auch mit einer Revision nicht geltend machen, das Landgericht habe zu Unrecht die Zuständigkeit des Amtsgerichts – und damit auch seine eigene Zuständigkeit – angenommen.[2] Die abweichende Rechtsauffassung des Beklagtenvertreters zur sachlichen Zuständigkeit ist bereits in der Berufungsbegründung und mit weiterem Schriftsatz vom Februar 2009 widerlegt worden, so dass sich weiterer Vortrag dazu erübrigt.

---

[1] BGHZ 132, 245; BGHZ 131, 169.

[2] Vgl. BGH, NJW 2003, 2917.

D. Personenbezug von IP-Adressen

Entgegen der Angabe des Beklagtenvertreters sind dessen Ausführungen unter dieser Überschrift keine „Zusammenfassung" des bisherigen Vorbringens, sondern größtenteils eine wortgleiche Übernahme der Klageerwiderung. Dementsprechend kann größtenteils anstelle einer Erwiderung auf die erstinstanzliche Replik des Klägers vom 06.07.2008 Bezug genommen werden.

1. Mittelbare Bestimmbarkeit des Nutzers anhand dynamischer IP-Adressen

Falsch ist die Darstellung des Beklagtenvertreters, das Bundesverfassungsgericht habe mit Urteil vom 02.03.2010 die Identifizierung von Internetnutzern nach § 113 TKG an hohe Voraussetzungen geknüpft.

Die Entscheidung des Bundesverfassungsgerichts bezieht sich von vornherein nur auf die Identifizierung von Internetnutzern mithilfe anlasslos auf Vorrat gespeicherter Daten (§§ 113b, 113 TKG).[1] Auf die sonstige Identifizierung von Internetnutzern gemäß § 113 TKG bezieht sich die Entscheidung nicht.

Selbst für die mittelbare Nutzung von Vorratsdaten zur Identifizierung von Internetnutzern hat das Bundesverfassungsgericht keine hohen Voraussetzungen aufgestellt. Umgekehrt hat es bestätigt, dass die Beklagte Internetnutzer ohne richterliche Anordnung für die Verfolgung jeglicher Straftat und sogar bestimmter Ordnungswidrigkeiten, zur Abwehr jeder Gefahr für die öffentliche Sicherheit oder Ordnung und für die Erfüllung jeder gesetzlichen Aufgabe der Nachrichtendienste identifizieren lassen dürfe.[2] Voraussetzung sei nur der Verdacht einer beliebigen Straftat wie etwa einer Beleidigung im Internet oder eine konkrete Gefahr für ein beliebiges Rechtsgut. Die Identifizierung ist nicht auf Tatverdächtige oder Störer beschränkt, sondern im Rahmen der „Erforderlichkeit" zu den in § 113 TKG genannten Zwecken darf die Beklagte jeden Internetnutzer identifizieren lassen.

Die unzureichende Eingriffsschwelle des § 113 TKG führt dazu, dass alleine die Deutsche Telekom AG schon im Jahr 2006 täglich mehr als 500 Internetnutzer gegenüber Behörden der Beklagten und der Länder namhaft machen musste.[3] Selbstverständlich erweist sich der Verdacht einer Straftat nicht selten als unbegründet, so dass zu einem großen Teil auch Unschuldige betroffen sind. Dass dies etwa bei der „Homepageüberwachung" durch das Bundeskriminalamt der Fall war, ist bereits vorgetragen worden.

---

[1] BVerfG, 1 BvR 256/08 vom 2.3.2010, Abs. 254 ff.

[2] BVerfG, 1 BvR 256/08 vom 2.3.2010, Abs. 254 ff.

[3] Köbele, Deutsche Telekom AG, https://www.datenschutzzentrum.de/sommerakademie/2007/sak2007-koebele-wirtschaftsunternehmen-verlaengerter-arm-der-sicherheitsbehoerden.pdf.

Vor diesem Hintergrund ist die Behauptung des Beklagtenvertreters abwegig, die Identifizierung von Internetnutzern durch die Beklagte sei nach sozial üblichen Maßstäben auszuschließen. Der Beklagtenvertreter räumt auf Seite 30 seines Schriftsatzes umgekehrt selbst ein, dass die Beklagte die von ihr gespeicherten Internet-Nutzungsdaten zur „Tätermittlung" – richtig: zur Identifizierung von Internetnutzern zur Aufklärung des Verdachts einer Straftat oder Ordnungswidrigkeit sowie für Zwecke der Gefahrenabwehr oder der Nachrichtendienste – nutzt. Damit gesteht auch der Beklagtenvertreter ein, dass die Beklagte die Nutzer ihrer Internetportale über § 113 TKG identifizieren kann.

3. a) Vermeintliche Relativität des Personenbezugs

In einem Teil der überkommenen Kommentarliteratur zum Bundesdatenschutzgesetz wird die Auffassung vertreten, Daten seien nur dann personenbezogen, wenn die jeweils speichernde Stelle selbst den Betroffenen identifizieren könne.[1] Diese Kommentatoren haben die Einführung der Richtlinie 95/46/EG nicht zum Anlass genommen, ihre zum frühen Bundesdatenschutzgesetz verfasste Kommentierung zu überdenken. Die „datenschutzrechtliche Relativitätstheorie" stammt aus einer Zeit, zu welcher der Begriff des Personenbezugs noch nicht europarechtlich vorgegeben war.

Die inzwischen ganz herrschende Meinung folgt diesen Stimmen zu Recht nicht: Europaweit ist man sich inzwischen einig, dass IP-Adressen unter Geltung der Datenschutzrichtlinie 95/46/EG allgemein als personenbezogene Daten einzuordnen sind. Die entsprechenden Entscheidungen und Stellungnahmen des Amtsgerichts Berlin-Mitte, des Verwaltungsgerichts Wiesbaden, des schweizerischen Bundesverwaltungsgerichts, des obersten schwedischen Verwaltungsgerichts sowie der Datenschutzbeauftragten aller EU-Staaten und des Bundesjustizministeriums sind bereits zitiert worden. Dieser Liste hinzuzufügen ist nun auch das Urteil des Französischen Verfassungsgerichtshofs vom 10.06.2009 zur Erhebung der IP-Adressen von Tauschbörsennutzern durch Rechteinhaber, in dem ausgeführt wird, „dass gleichwohl die Ermächtigung von Privatpersonen, Daten zu erheben, die indirekt die Identifizierung der Inhaber von Zugängen zu öffentlichen Online-Kommunikationsdiensten ermöglichen, dazu führt, dass diese Privatpersonen personenbezogene Daten über Vergehen verarbeiten".[2]

Falsch ist die Darstellung des Beklagtenvertreters, die vom Kläger wiedergegebene Rechtslage würde „zu einer vollständigen Aufgabe der Relativität des Personenbezugs führen". Der Begriff des Personenbezugs war nie relativ, so dass auch keine „Aufgabe der Relativität" vorliegen kann.

---

[1] Gola/Schomerus, BDSG, § 3, Rn. 9.

[2] Conseil Constitutionnel, Entscheidung vom 10.06.2009, Az. 2009-580 DC, Abs. 27, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html.

Soweit der Beklagtenvertreter weiter behauptet, die zutreffende, in der Richtlinie 95/46/EG verankerte Definition des Personenbezugs widerspreche dem Willen des Gesetzgebers, bleibt er für diese Behauptung jeden Nachweis schuldig.

Falsch ist zuletzt die Darstellung des Beklagtenvertreters, dass letztlich „alle Daten in einer bestimmten Kombination und mit geeignetem Zusatzwissen wieder auf bestimmte Personen zurückbezogen werden" könnten und dass bei zutreffender Auslegung des Merkmals der Bestimmbarkeit „alle nur denkbaren Daten dem Datenschutzrecht unterfallen" würden. Anonyme Daten einschließlich anonymer Internet-Nutzungsprotokolle sind nicht personenbezogen und unterliegen nicht dem Datenschutzrecht. Dementsprechend haben die Datenschutz-Aufsichtsbehörden in ihrem Beschluss vom 26./27.11.2009 nicht jede Aufzeichnung von IP-Adressen als unzulässig bezeichnet, sondern die hinreichend verkürzte Aufzeichnung von IP-Adressen für zulässig erachtet.[1] Wird eine IP-Adresse etwa durch Verkürzung um zwei Byte wirksam anonymisiert, so unterfällt sie dem Datenschutzrecht ebenso wenig wie sonstige anonyme Daten über das Internet-Nutzungsverhalten. Da die vorliegende Klage darauf gerichtet ist, der Beklagten die Aufzeichnung der IP-Adresse des Klägers zu untersagen, bleibt der Beklagten die Aufzeichnung eines hinreichend verkürzten Teils dieser Adresse unbenommen. Ein solches Teildatum stellt nämlich nicht die IP-Adresse des Klägers im Sinne der Klageanträge dar.

Im Übrigen ist der Streit über den Begriff des Personenbezugs für den vorliegenden Rechtsstreit ohne Bedeutung, weil hier die Speicherung von IP-Adressen durch den Staat in Rede steht. Speichert der Staat IP-Adressen von Internetnutzern, so ist die Bestimmbarkeit des Betroffenen auch nach der „datenschutzrechtlichen Relativitätstheorie" anzunehmen, weil der Beklagten das zur Identifizierung erforderliche Zusatzwissen über § 113 TKG legal zugänglich ist und die Beklagte von § 113 TKG auch regen Gebrauch macht. Im Hinblick darauf sind die von der Beklagten gesammelten Internet-Nutzungsdaten selbst nach der vom Beklagtenvertreter herangezogenen Minderauffassung personenbezogen.

(3) Urteil des Amtsgerichts München

Neben die europaweit einhellige Rechtsprechung zur Auslegung des Begriffs des Personenbezugs tritt nun in der Tat ein vereinzeltes Urteil des Amtsgerichts München, in dem eine abweichende Auffassung geäußert wurde. Dieser Auffassung zufolge seien zeitweilig (dynamisch) vergebene IP-Adressen für private Anbieter von Internetdiensten nicht personenbezogen und dürften von diesen daher unbegrenzt auf Vorrat gespeichert werden.[2] Hierzu ist erstens zu bemerken, dass die diesbezüglichen Erwägungen des Amtsgerichts für dessen Entscheidung nicht tragend waren und lediglich als obiter dictum geäußert wurden („Nur ergänzend soll darauf hingewiesen werden [...]"). Zweitens

[1] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26./27.11.2009, http://www.datenschutz-mv.de/dschutz/beschlue/Analyse.pdf.

[2] AG München, MMR 2008, 860.

behauptet die Beklagte selbst nicht, dass das Urteil rechtkräftig sei. Drittens setzt sich das obiter dictum mit keinem Wort mit der europarechtlich vorgegebenen Definition des Personenbezugs in der Richtlinie 95/46/EG auseinander. Schließlich ist das Urteil auf die Beklagte nicht anwendbar. Es betraf die Speicherung einer IP-Adresse durch eine Privatperson. Demgegenüber steht der Beklagten – wie bereits ausgeführt – die Identifizierungsmöglichkeit des § 113 TKG zu Gebote, so dass vorliegend auch nach der vom Amtsgericht München vertretenen „Relativitätstheorie" ein Personenbezug gegeben ist.

4. Grundsatz der Datensparsamkeit

Offenkundig falsch ist die Behauptung des Beklagtenvertreters, das Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung beziehe sich in Absatz 270 „ausschließlich auf die Speicherung von IP-Adressen durch Telekommunikationsunternehmen bzw. Zugangsanbieter." Richtig ist, dass das Bundesverfassungsgericht in diesem Absatz ausdrücklich auf „Diensteanbieter nach dem Telemediengesetz" Bezug nimmt und ausführt:

> „Ebenfalls lässt sich zum gegenwärtigen Zeitpunkt nicht feststellen, dass die Regelung im Zusammenwirken mit anderen Vorschriften darauf zielt oder hinausläuft, eine allgemein umfassende Datensammlung zur weitestmöglichen Rekonstruierbarkeit jedweder Aktivitäten der Bürger zu schaffen. Von Bedeutung sind insoweit die Geltung des das Datenschutzrecht sonst weithin durchziehenden Grundsatzes der Datensparsamkeit sowie zahlreiche Löschungspflichten, mit denen der Gesetzgeber das Entstehen vermeidbarer Datensammlungen grundsätzlich zu verhindern sucht. Maßgeblich für diese Beurteilung sind insoweit insbesondere etwa die §§ 11 ff. TMG, die die Diensteanbieter nach dem Telemediengesetz grundsätzlich zur Löschung von nicht für die Abrechnung erforderlichen Daten verpflichten (vgl. § 13 Abs. 4 Nr. 2, § 15 TMG) und so auch gegenüber privatwirtschaftlichen Anreizen verhindern, dass die Internetnutzung inhaltlich in allgemeinen kommerziellen Datensammlungen festgehalten wird und damit rekonstruierbar bleibt."

Wenn das Bundesverfassungsgericht ausführt, die Löschungspflichten der §§ 13 Abs. 4 Nr. 2, 15 TMG verhinderten, dass die Internetnutzung der Bürger „rekonstruierbar bleibt", so erkennt es damit die Bestimmbarkeit des Bürgers anhand seiner Telemedien-Nutzungsdaten an.

Wenn der Beklagtenvertreter in dem Urteil des Bundesverfassungsgerichts vom 02.03.2010 Ausführungen zur vermeintlichen Relativität des Personenbezugs vermisst, so beruht das Fehlen solcher Ausführungen darauf, dass der verfassungs- und einfachrechtliche Begriff des Personenbezugs eines Datums nicht relativ ist. Nach der Rechtsprechung des Bundesverfassungsgerichts liegt ein persönlicher Lebenssachverhalt bereits dann vor, wenn die Verknüpfung des Lebenssachverhalts mit der zugehörigen Person „möglich" ist.[1]

---

1 BVerfGE 65, 1 (42 und 49); BVerfGE 67, 100 (143); BVerfGE 77, 1 (46); BVerfGE 103, 21 (33); zu Art. 10: BVerfGE 100, 313 (366).

5. Recht auf Anonymität

Die Argumente des Beklagtenvertreters zum Recht von Internetnutzern auf Anonymität werden bereits durch die Ausführungen auf Seite 6 f. des Schriftsatzes vom 20.11.2009 widerlegt, auf die Bezug genommen wird.

6. Preisgabe des Personenbezugs durch den Kläger

Da das Gesetz die Identifizierbarkeit des Klägers gerade durch die Beklagte nicht fordert und diese Identifizierbarkeit im Übrigen durch § 113 TKG gegeben ist, ist es müßig, mit dem Beklagtenvertreter über weitere Identifizierungsmöglichkeiten zu streiten. Es bleibt daher bei den diesbezüglichen Ausführungen in der Replik vom 06.07.2008.

V. Vermeintliche Notwendigkeit der Speicherung von IP-Adressen

Während der Beklagtenvertreter unter dieser Überschrift behauptet, die Speicherung von IP-Adressen über die Dauer des Nutzungsvorgangs hinaus sei notwendig, räumt er auf Seite 8 desselben Schriftsatzes – wie schon zuvor mit Schriftsatz vom 27.01.2009 – ausdrücklich ein, dass die Beklagte „alternative Maßnahmen zur Schadprogrammabwehr" einsetzen kann, „um einen sicheren Betrieb der entsprechenden Systeme der Beklagten zu gewährleisten", dass also ein sicherer Betrieb der Systeme der Beklagten auch ohne die rechtswidrige Protokollierung des Surfverhaltens samt IP-Adressen möglich ist. Der Vortrag der Beklagten zur vermeintlichen Notwendigkeit der Speicherung von IP-Adressen ist mithin in sich widersprüchlich und deshalb unbeachtlich.

Die Beklagte widerlegt die Behauptungen ihres Prozessbevollmächtigten unter dieser Überschrift im Übrigen dadurch, dass sie selbst eine Vielzahl von Internet-Portalen 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 bieten etwa die folgenden Ministerien und Behörden der Beklagten Internetportale an:

- Bundesjustizministerium
- Bundesdatenschutzbeauftragter
- Bundesrechnungshof
- Bundesforschungsministerium
- Bundeskriminalamt
- Bundesversicherungsamt
- Bundesanstalt für Arbeitsschutz
- Bundesanstalt für Wasserbau
- Kraftfahr-Bundesamt
- Bundeseisenbahnvermögen
- Bundesstelle für Seeschiffahrt und Hydrographie
- Bundesanstalt für Gewässerkunde
- Bundesfinanzministerium

Der hypothetische Fall, dass die Speicherung von IP-Adressen einmal zur Wiederherstellung der Verfügbarkeit eines Telemediums erforderlich sein könnte, ist von vornherein dem Streit entzogen, indem er vom Klageantrag ausgenommen worden ist.

In rechtlicher Hinsicht nennt der Beklagtenvertreter keine einzige Norm, aus der sich eine Zulässigkeit der verschiedenen insbesondere vom Bundesverwaltungsamt praktizierten Auswertungen ergeben soll. Vielmehr untersagt § 15 TMG eindeutig die Speicherung personenbezogener Nutzungsdaten über die Dauer des Nutzungsvorgangs hinaus.

Im Hinblick auf das Eingeständnis der Beklagten zu Alternativmöglichkeiten, die sachliche Selbstwiderlegung des Beklagtenvortrags durch ihre eigene Praxis und die rechtliche Unerheblichkeit verzichte ich darauf, auf die einzelnen Datennutzungen des Bundesverwaltungsamts einzugehen und im Einzelnen zu widerlegen, dass anlasslos protokollierte IP-Adressen zur Aufrechterhaltung des Betriebs oder der Systemsicherheit 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.

2. Stand der Technik

Soweit die Beklagte durch eine Vorratsspeicherung des Internet-Nutzungsverhaltens Strafverfolgung betreiben und dadurch von Straftaten abschrecken will, ist eine Vorratsspeicherung von Internet-Nutzungsdaten zu Strafverfolgungszwecken illegal. Dies wird schon auf Seite 7 f. der Klageschrift im Einzelnen erläutert. Ergänzend ist aus historischer Sicht anzuführen, dass der Bundestag einen Vorschlag des Bundesrats, eine Vorratsspeicherung von Telemedien-Nutzungsdaten für Strafverfolgungszwecke einzuführen,[1] nie behandelt hat und verfallen ließ.[2]

Eine Vorratsspeicherung des Internet-Nutzungsverhaltens für Strafverfolgungszwecke ist nicht nur einfachgesetzlich, sondern auch verfassungsrechtlich unzulässig, wie das Bundesverfassungsgericht mit Urteil vom 02.03.2010 festgestellt hat. Das Bundesverfassungsgericht hat die europarechtlich vorgegebene Vorratsspeicherung von Telekommunikations-Verkehrsdaten nur als „Ausnahme" und nur unter mehreren Voraussetzungen für verfassungskonform erachtet:[3] So dürfe die Vorratsspeicherung nicht direkt durch staatliche Stellen erfolgen.[4] Außerdem dürften die Internetseiten oder Diensteanbieter, die ein Nutzer im Internet kontaktiert hat, nicht gespeichert werden.[5] Mit diesen Grundsätzen ist die Praxis etwa des Bundesverwaltungsamts unvereinbar, weil dessen Vorratsdatenspeicherung direkt durch eine staatliche Stelle erfolgt und außerdem auch die aufgerufenen Internetseiten und genutzten Internetportale erfasst.

---

[1] Entwurf eines Gesetzes zur Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Missbrauchs von Kindern und der Vollstreckung freiheitsentziehender Sanktionen, BR-Drs. 275/02 (Beschluss) vom 31.05.2002.

[2] Gesetzesdokumentation XIV/1145, http://dipbt.bundestag.de/doc/gm/41/41145.pdf.

[3] BVerfG, 1 BvR 256/08 vom 2.3.2010, Abs. 218.

[4] BVerfG, 1 BvR 256/08 vom 2.3.2010, Abs. 218.

[5] BVerfG, 1 BvR 256/08 vom 2.3.2010, Abs. 270.

Soweit die Beklagte durch eine Vorratsspeicherung des Internet-Nutzungsverhaltens Angriffe auf ihre Infrastruktur abwehren will, legte die Bundesregierung im Jahr 2009 auf Initiative des Bundesinnenministeriums einen Gesetzentwurf vor, demzufolge § 15 TMG um die folgende Bestimmung ergänzt werden sollte:

> „Soweit erforderlich, darf der Diensteanbieter Nutzungsdaten zum Erkennen, Eingrenzen oder Beseitigen von Störungen seiner für Zwecke seines Dienstes genutzten technischen Einrichtungen erheben und verwenden."[1]

Der Deutsche Bundestag hat diese Bestimmung im Verlauf des Gesetzgebungsverfahrens ausdrücklich und ersatzlos aus dem Gesetzentwurf gestrichen und das Gesetz ohne Änderung des Telemediengesetzes verabschiedet.[2] Damit hat der Gesetzgeber erneut seinen Willen bekräftigt, dass unser Internet-Nutzungsverhalten nicht personenbeziehbar aufgezeichnet werden darf, auch nicht im Hinblick auf etwaige „Störungen" technischer Anlagen.

Wenn der Beklagtenvertreter die Auffassung vertritt, die veralteten BSI-Maßnahmenkataloge „konkretisierten" die ISO-Norm 27001 oder stellten den Stand der Technik dar, so ist dies falsch, aber auch unerheblich. Für die Beklagte verbindlich ist das deutsche Recht, namentlich § 15 TMG, und nicht technische Industrienormen oder Maßnahmenkataloge, die der demokratisch gewählte Gesetzgeber nicht beschlossen hat. Im Übrigen ist bereits mit der Replik vom 06.07.2008 ausgeführt worden, dass die vom Bundesamt für Sicherheit in der Informationstechnik herausgegebenen Handlungsempfehlungen für E-Government-Angebote ausdrücklich den Verzicht auf eine Aufzeichnung von IP-Adressen vorsehen.

b) Präventive Speicherung

Das weiterhin nicht rechtskräftige, erstinstanzliche Urteil des Landgerichts Darmstadt vom 25.01.2006 ist bereits mit der Replik vom 06.07.2008 zutreffend eingeordnet worden. Inzwischen hat auch der Bundesrat dieses Urteil wie folgt kommentiert:

> „Die Ermächtigungsgrundlage muss daneben hinreichend normenklar und -bestimmt sein sowie dem verfassungsrechtlichen Gebot der Verhältnismäßigkeit genügen. Hiermit nicht vereinbar sind anlasslose oder flächendeckend durchgeführte Speicherungen sämtlicher Nutzungsdaten; es müssen vielmehr Anhaltspunkte für eine konkrete Störung vorliegen (vgl. BVerfG, Urteil vom 11.03.2008 - 1 BvR 2074/05 u. a. -, MMR 2008, 308). [...]

---

[1] Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes, BR-Drs. 62/09.

[2] Gesetz vom 14.08.2009 – BGBl. I 2009 Nr. 54 vom 19.08.2009, 2821.

> Dies erscheint insbesondere deshalb veranlasst, weil die zu § 100 Absatz 1 TKG ergangene Rechtsprechung in verfassungsrechtlich bedenklicher Weise die vorbeugende Speicherung von IP-Adressen zur Störungseingrenzung und -beseitigung zulässt, ohne dass tatsächliche Anhaltspunkte bei einem bestimmten Nutzer vorliegen (vgl. LG Darmstadt, Urteil vom 06.06.2007 - 10 O 562/03 -, CR 2007, 574)."[1]

G. § 5 BSIG

Der Begründetheit der Klage steht der nach Klageerhebung in Kraft getretene § 5 BSIG nicht entgegen.

I. Unanwendbarkeit auf andere Bundesbehörden als das BSI

Zunächst einmal ermächtigt die Vorschrift einzig das Bundesamt für Sicherheit in der Informationstechnik zur Verarbeitung von Protokolldaten. Die Speicherung durch die übrigen Behörden der Beklagten bleibt also in jedem Fall illegal. § 5 BSIG lässt sich im Umkehrschluss entnehmen, dass andere Behörden als das Bundesamt für Sicherheit in der Informationstechnik von vornherein nicht zur Verarbeitung von Protokolldaten zu „Sicherheitszwecken" ermächtigt werden sollten.

II. Begründetheit der Klage auch bezüglich des BSI

§ 5 BSIG ermächtigt das Bundesamt für Sicherheit in der Informationstechnik nicht dazu, die Internetprotokolladresse (IP-Adresse) des zugreifenden Hostsystems des Klägers, die im Zusammenhang mit der Nutzung öffentlich zugänglicher Telemedien der Beklagten im Internet übertragen wird, nebst dem Zeitpunkt des jeweiligen Nutzungsvorgangs über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern, soweit die Speicherung nicht im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich ist.

Die Beklagte trägt dazu zwar vor, dass IP-Adressen Protokolldaten im Sinne des § 5 BSIG seien. Sie legt aber nicht dar, dass auch der Zeitpunkt des jeweiligen Nutzungsvorgangs ein Protokolldatum sei, zu dessen Verarbeitung § 5 BSIG ermächtige. Tatsächlich enthält etwa das Internetprotokoll (IP Protocol) keine Zeitangabe. Eine solche Zeitangabe ist auch bei dem für Telemediendienste typischen Hypertextprotokoll (HTTP Protocol) nicht „zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig", wie es § 2 Abs. 8 BSIG verlangt. Auch die Bundesregierung ordnet Datum und Uhrzeit nicht als „Steuerdatum" im Sinne des § 2 Abs. 8 BSIG ein.[2] Dementsprechend bleibt die Klage mit dem Hilfsantrag selbst auf der Grundlage des Vortrags der Beklagten begründet.

---

[1] BR-Drs. 62/09, 9 f.

[2] BT-Drs. 16/11967, 12.

§ 5 Abs. 1 BSIG ermächtigt das BSIG außerdem nur zu einer „unverzüglichen" Verarbeitung und anschließenden Löschung von Protokolldaten, etwa um laufende Angriffe festzustellen. Die vorliegende Klage richtet sich gegen eine Aufbewahrung der IP-Adresse „über das Ende des jeweiligen Nutzungsvorgangs hinaus". Zu einer solchen Aufbewahrung ermächtigt § 5 Abs. 1 BSIG nicht. § 5 Abs. 2 BSIG sieht zwar unter bestimmten Voraussetzungen eine dreimonatige Vorratsspeicherung von Protokolldaten vor. Die Beklagte legt jedoch selbst nicht dar, dass die Voraussetzungen des § 5 Abs. 2 BSIG gegeben seien.

Allgemein stehen sämtliche Ermächtigungen des § 5 Abs.1 und 2 BSIG unter dem Vorbehalt der Erforderlichkeit. Dass eine Vorratsspeicherung von IP-Adressen zur Abwehr von Störungen, Fehlern, Angriffen oder Schadprogrammen nicht erforderlich ist, weil alternative Schutzmaßnahmen existieren, gesteht die Beklagte selbst zu. Auch aus diesem Grund rechtfertigt § 5 BSIG keine personenbezogene Vorratsspeicherung des Internet-Nutzungsverhaltens.

Nicht erforderlich für die in § 5 BSIG genannten Zwecke ist insbesondere die Speicherung der dem Kläger zugewiesenen IP-Adressen. Unstreitig gehen vom Internetzugang des Klägers keinerlei Gefahren für die Kommunikationstechnik des Bundes aus.

III. Mögliche Verfassungswidrigkeit des § 5 BSIG

Sollte § 5 BSIG hingegen dahin auszulegen sein, dass er das Bundesamt für Sicherheit in der Informationstechnik zur personenbezogenen Vorratsspeicherung der Telemediennutzung des Klägers über das Ende des Nutzungsvorgangs hinaus ermächtigte, so ist die Vorschrift verfassungswidrig und nichtig.

Die Anlehnung des § 5 BSIG an § 100 TKG, der seinerseits mit der Verfassung nicht im Einklang steht[1] und von den Gerichten notdürftig einschränkend ausgelegt und angewandt wird,[2] übersieht, dass Nutzungsdaten nicht nur über die näheren Umstände von Individualkommunikation, sondern über den Inhalt der abgerufenen und eingegebenen Informationen (z.B. Internetseiten, Suchwörter) Aufschluss geben und damit weit reichende Rückschlüsse auf die Persönlichkeit des Nutzers zulassen, wie sie bei sonstigen Medien undenkbar wären.

§ 5 BSIG wird in einer Auslegung als Ermächtigung zur Vorratsdatenspeicherung den verfassungsrechtlichen Mindestanforderungen und dem Verhältnismäßigkeitsgebot nicht gerecht. Insbesondere die von § 5 BSIG in dieser Auslegung gestattete anlasslose grundrechtseingreifende Aufzeichnung und Auswertung aller Daten „ins Blaue hinein" lässt die Verfassung nicht zu.[3] Nach der Rechtsprechung des Bundesverfassungsgerichts darf eine automatisierte Datenerfassung „nicht anlasslos erfolgen oder flächendeckend

[1] Breyer, RDV 2004, 147; vgl. auch Bundesrat, BR-Drs. 62/09, 10.

[2] LG Darmstadt, MMR 2006, 330.

[3] Bundesrat, BR-Drs. 62/09 (Beschluss), 6.

durchgeführt werden".[1] Begriffe wie „erforderlich" oder „sachdienlich" stellen keine hinreichende Eingrenzung dar.[2] Das „strikte Verbot der Sammlung personenbezogener Daten auf Vorrat" ist zu gewährleisten.[3]

In seiner Stellungnahme vom 06.03.2009 äußerte der Bundesrat dementsprechend „erhebliche Bedenken", ob der mit § 5 BSIG verbundene Grundrechtseingriff „verfassungsrechtlich zu rechtfertigen ist."[4] Die Ermächtigung könne „zu allgemeinen Einschüchterungseffekten bei den Nutzern dieser Kommunikationstechnik führen und Beeinträchtigungen bei der Ausübung von Grundrechten bedingen". Insbesondere die von § 5 Abs. 1 BSIG gestattete anlasslose grundrechtseingreifende Auswertung aller Daten „ins Blaue hinein" sei mit der Verfassung nicht vereinbar.[5]

Im April 2009 kritisierte auch der Deutsche Anwaltverein, § 5 BSIG fehle es an der verfassungsrechtlich gebotenen Anlassbezogenheit der Überwachung.[6] Die vollständige Überwachung sei „der falsche Ansatz zur Erhöhung der IT-Sicherheit". Stattdessen seien Sicherheitslücken in der eingesetzten IT-Infrastruktur und Software zu schließen, „welche Schadprogrammen das Eindringen erst ermöglichen." Die informationelle Selbstbestimmung der Nutzer sei „ein höheres Schutzgut als die technische Unversehrtheit von IT-Infrastrukturen." Wörtlich schrieb der Verein weiter:

> „Die Erhöhung der IT-Sicherheit darf sodann nicht um den Preis der anlasslosen und permanenten Verletzung des Fernmeldegeheimnisses erfolgen. Nach § 5 soll eine ständige verdachts- und anlasslose vollständige Überwachung von Verbindungsdaten und Inhalten erfolgen, die mit Bundesbehörden in Verbindung treten. Unabhängig davon, ob die Mittel zur vollständigen Überwachung überhaupt tauglich sind, ist eine solche vollständige Überwachung jeglicher Kommunikation unter Sicherheitsaspekten nicht angezeigt (s. dazu oben 1. a) und damit im Hinblick auf die Grundrechte auf informationelle Selbstbestimmung und das Fernmeldegeheimnis nicht verfassungsmäßig."[7]

Inzwischen hat auch das Bundesverfassungsgericht entschieden, dass die Zulässigkeit der vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten aufgrund der EG-Richtlinie zur Vorratsdatenspeicherung eine Ausnahme bleiben muss.[8] Maßgeblich für die Rechtfertigungsfähigkeit der Verbindungsdatenspeicherung sei insbesondere, dass sie nicht direkt durch staatliche Stellen erfolge, dass sie nicht auch die Kommunikationsinhalte erfasse und dass auch die Speicherung der aufgerufenen Internetseiten grundsätzlich untersagt sei.[9] Diese Rechtfertigungsvoraussetzungen erfüllt § 5 BSIG in einer Auslegung als Ermächtigung zur Vorratsdatenspeicherung nicht: Die dort vorgesehene

---

[1] BVerfG, MMR 2008, 308, 308; BVerfG, NVwZ 2007, 688, 691.
[2] BVerfG, MMR 2007, 93, 94; BVerfG, NVwZ 2007, 688, 691.
[3] BVerfG, MMR 2006, 531.
[4] BR-Drs. 62/09 (Beschluss), 5.
[5] BR-Drs. 62/09 (Beschluss), 5.
[6] DAV, Stellungnahme 2009-31 vom April 2009, 3.
[7] DAV, Stellungnahme 2009-31 vom April 2009, 3.
[8] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 218.
[9] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 218.

Speicherung erfolgt direkt durch eine staatliche Stelle und umfasst gerade auch die Speicherung jeder aufgerufenen Internetseite. In seiner Entscheidung vom 2.3.2010 hat das Bundesverfassungsgericht maßgeblich darauf abgestellt, dass die §§ 11 ff. TMG die Diensteanbieter nach dem Telemediengesetz grundsätzlich zur Löschung von nicht für die Abrechnung erforderlichen Daten verpflichteten (vgl. § 13 Abs. 4 Nr. 2, § 15 TMG) und so verhinderten, dass die Internetnutzung inhaltlich festgehalten werde und damit rekonstruierbar bleibe.[1] Im Bereich der vielen Telemedien des Bundes beseitigte § 5 BSIG im Falle einer weiten Auslegung diese Löschungspflichten des TMG und zielte umgekehrt darauf ab, dass die Internetnutzung inhaltlich festgehalten wird und damit rekonstruierbar gemacht wird. Dies würde den grundrechtlichen Vorgaben nicht genügen.

Sollte das Hohe Gericht § 5 BSIG daher – selbst in möglichst grundrechtskonformer Auslegung – eine Ermächtigung zu einer personenbezogenen Vorratsspeicherung des Internet-Nutzungsverhaltens des Klägers entnehmen, so wird beantragt, die Beklagte zunächst durch Teilurteil „mit Ausnahme des Bundesamts für Sicherheit in der Informationstechnik" zu verurteilen und den Rechtsstreit im Übrigen dem Bundesverfassungsgericht nach Art. 100 GG zur Entscheidung über die Vereinbarkeit des § 5 BSIG mit dem Grundrecht auf Informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) vorzulegen.

IV. Weitere sondergesetzliche Vorschriften

Soweit die Beklagte allgemein nur unter dem Vorbehalt „sondergesetzlicher Vorschriften" verurteilt werden will, nennt sie mit Ausnahme des § 5 BSIG keine „sondergesetzlichen Vorschriften", die eine solche Einschränkung rechtfertigen sollen. Umgekehrt regelt § 15 TMG spezialgesetzlich und abschließend den Umgang mit den Internet-Nutzungsdaten des Klägers bei der Nutzung der Telemedien der Beklagten. Dementsprechend ist die Klage entgegen der Auffassung des Beklagtenvertreters nicht „insoweit abzuweisen, als eine Speicherung der Daten nach sondergesetzlichen Vorschriften" zulässig sei.

Beglaubigte und einfache Abschrift anbei.

[redacted]
Meinhard Starostik
- Rechtsanwalt -

[1] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 270.