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
Littenstr. 12-17
10179 Berlin

Kanzlei vereidigter Buchprüfer:
Schwarzenberger Str. 7 ◆ 08280 Aue
Tel.: 03771-290 999

Berlin, den **1. Oktober 2010**

AZ: 45/08
(bitte stets angeben)

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

nehme ich zum Schriftsatz des Beklagtenvertreters vom 28.06.2010 wie folgt Stellung:

1. Person des Sachverständigen

Da der diesseits als Sachverständiger vorgeschlagene **Prof. Dr. Andreas Pfitzmann** zwischenzeitlich leider verstorben ist, benenne ich an seiner Stelle:

2a) **Prof. Dr. Hannes Federrath**, [*... anonymisiert ...*]. Prof. Dr. Federrath ist Informatiker und seit 2003 Inhaber eines wirtschaftsinformatischen Lehrstuhls für „Management der Informationssicherheit“ an der Universität Regensburg. Der von ihm betreute Studienschwerpunkt Informationssicherheit beschäftigt sich mit Sicherheit in verteilten Systemen und der Beherrschbarkeit großer IT-Systeme. Zu seinen Forschungsschwerpunkten zählt die Sicherheit im Internet. Prof. Dr. Federrath war unter anderem schon für den Deutschen Bundestag als Sachverständiger tätig.

2b) **Prof. Dr. Rüdiger Grimm**, [*... anonymisiert ...*]. Prof. Dr. Grimm ist Informatiker und seit 2005 Leiter der Professur IT-Risk-Management im Fachbereich Informatik der Universität Koblenz. Er ist auch als Berater des Fraunhofer Instituts für Sichere Informationstechnologie (SIT) in Darmstadt tätig. Prof. Dr. Grimm ist Mitglied des Leitungsgremiums des Fachbereichs „Sicherheit – Schutz und Zuverlässigkeit“ der Gesellschaft für Informatik e.V. und Sprecher deren Fachgruppe „E-Commerce, E-Government und Sicherheit“.

Die **weiteren Vorschläge** von Frau Dr. Kurz, Herrn Dr. Weichert und Herrn Schaar als mögliche Sachverständige bleiben aufrecht erhalten. Die beklagtenseits gegen diese Personen vorgebrachten Einwände greifen nicht durch. Bei der Benennung ist angegeben worden, weshalb diese Personen qualifiziert und in der Lage sind, die Beweisfrage zu beantworten. Insbesondere verfügen sie über Erfahrung in dem sicheren Betrieb von Webservern.

Die **beklagtenseits genannten Personen** kommen als Sachverständige demgegenüber nicht in Betracht, weil ihre Tätigkeit den Anschein erweckt, dass sie zu einer unvoreingenommenen Beantwortung der Beweisfragen nicht in der Lage wären.

Die Beklagte hat offenbar ausschließlich „anerkannte Mitglieder der nationalen und weltweiten Sicherheits-Community“ vorgeschlagen, zu der sich offenbar auch das Bundesinnenministerium rechnet. Alleine diese Verflechtung mit dem Lager der Beklagten rechtfertigt die Besorgnis der Befangenheit. Im Übrigen hat die Beklagte trotz ausdrücklicher Nachfrage nicht dazu vorgetragen, ob die von ihr benannten Personen gegen Entgelt für das Bundesinnenministerium oder eine nachgeordnete Behörde tätig sind oder waren, was zu befürchten ist.

Im Einzelnen ist zu den beklagtenseits vorgeschlagenen Personen zu sagen:

Prof. Dr. Bernhard Hämmerli ist ein studierter Elektroingenieur und kein ausgebildeter Informatiker. Er arbeitete in der Vergangenheit unter anderem für das US-amerikanische Unternehmen IBM, welches Sicherheitssysteme herstellt, und verfolgte ein entsprechendes wirtschaftliches Interesse. Noch heute ist er als Beirat der „European Homeland Security Association“ tätig, einer Lobbyorganisation der Verteidigungs- und Sicherheitsindustrie. Aufgrund dieser persönlichen Verflechtung besteht keine Gewähr für eine unvoreingenommene Beurteilung der Beweisfrage. Auch ist nicht ersichtlich, dass der Betrieb von Webservern in das Fachgebiet von Prof. Dr. Hämmerli fiele.

Hinzu kommt, dass Prof. Dr. Hämmerli **in der Schweiz** wohnt und wohl kein deutscher Staatsbürger ist. Fachlich ist zweifelhaft, ob sich Prof. Dr. Hämmerli als Schweizer zu der Beweisfrage nach dem nationalen – also deutschen – Stand der Technik äußern kann. Prozessual kann ein deutsches Gericht die Tätigkeit eines Sachverständigen nicht wie in § 404a ZPO vorgesehen leiten, wenn sich der Sachverständige außerhalb des deutschen Hoheitsgebiets befindet. Erstattet ein ausländischer Sachverständiger z.B. ein Gutachten nicht, so lassen sich die in § 411 ZPO vorgesehenen Ordnungsmittel kaum durchsetzen, zumal die Schweiz nicht EU-Mitgliedsstaat ist. Wenn der ausländische Sachverständige die Gerichtsakte nicht zurückgibt, ist sie zwangsweise kaum zurückzuerlangen (vgl. § 407a Abs. 4 ZPO). Überhaupt sind ausländische Sachverständige nicht durchsetzbar an das deutsche Prozess- und Datenschutzrecht gebunden. Die Verpflichtung eines ausländischen Staatsbürgers als Sachverständiger vor einem deutschen Gericht wird nach alledem nur ausnahmsweise in Betracht kommen, wenn in ganz Deutschland kein geeigneter Sachverständiger vorhanden wäre, was hier nicht der Fall ist.

Dem Vorschlag von Herrn **Christoph Fischer** ist entgegen zu halten, dass Herr Fischer studierter Elektrotechniker und nicht Informatiker ist. Eine wissenschaftliche Qualifikation ist nicht ersichtlich. Herr Fischer war in der Vergangenheit bei der Luftwaffe tätig und bestreitet seinen Lebensunterhalt seit 18 Jahren mit der Beratung unter anderem staatlicher Stellen zu den Themenbereichen Computersicherheit, Emergency Response, Forensik und „Information Warfare“. Vor diesem Hintergrund ist davon auszugehen, dass Herr Fischer bereits wiederholt für das Bundesinnenministerium oder nachgeordnete Stellen tätig war und wirtschaftlich von entsprechenden Aufträgen abhängig, jedenfalls stark daran interessiert ist. Nach eigenen Angaben arbeitet Herr Fischer häufig im Auftrag von Strafverfolgungsbehörden. Sein Unternehmen BFK edv-consulting GmbH bietet Dritten unter anderem „Ermittlungsarbeit in Notfällen“ sowie „Überwachung und Analyse ihrer Systemprotokolle“[1] im Rahmen des Dienstes „Logwatch“ an. Diese Dienste setzen die Existenz der streitgegenständichen Aufzeichnungen („Logfiles“) voraus. Offensichtlich bestreitet Herr Fischer seinen Lebensunterhalt also mit den auch vom Bundesverwaltungsamt eingesetzten Verfahren, deren Erforderlichkeit und Zulässigkeit

[1] BFK edv-consulting GmbH, Dienstleistungen, http://www.bfk.de/bfk_dienstleistung.html.

gerade Gegenstand des Beweisbeschlusses und des vorliegenden Prozesses sind. Bei einem derart starken eigenen wirtschaftlichen Interesse am Ausgang der Beweisaufnahme und des Prozesses kann von Herrn Fischer eine unvoreingenommene Beantwortung der Beweisfrage nicht erwartet werden.

Dem Vorschlag von Herrn **Udo Schweigert** ist entgegen zu halten, dass er – wie die Beklagte selbst angibt – „angesehenes Mitglied der Sicherheits-Community" ist, zu der sich offensichtlich auch das Bundesinnenministerium rechnet. Inwieweit er oder sein Unternehmen von Aufträgen des Ministeriums profitiert oder davon abhängig ist, legt die Beklagte wiederum nicht offen. Jedenfalls wird das Siemens-CERT, das Herr Schweigert leitet, neben Siemens selbst auch für Dritte tätig und bietet insbesondere Logfileanalyse an.[2] Diese Geschäftstätigkeit setzt die Existenz der streitgegenständlichen Aufzeichnungen voraus, deren Erforderlichkeit und Zulässigkeit gerade erst im Wege der Beweiserhebung und im Rahmen des vorliegenden Prozesses geprüft werden soll. Überdies verantwortet Herr Schweigert den Einsatz von „Einbruchserkennungsvorrichtungen" bei Siemens, deren Verwendung durch das Bundesverwaltungsamt in diesem Prozess streitgegenständlich ist. Insgesamt kann wegen dieses beruflichen Eigeninteresses auch von Herrn Schweigert eine unvoreingenommene Beantwortung der Beweisfrage nicht erwartet werden. Im Übrigen ist eine wissenschaftliche Qualifikation von Herrn Schweigert nicht ersichtlich.

Insgesamt führt schon der **Grundansatz der Beklagten** bei der Auswahl der von ihr vorgeschlagenen Personen dazu, dass die Personen nicht als Sachverständige in Betracht kommen. Um eine unvoreingenommene Beurteilung der Beweisfrage zu gewährleisten, können Personen, deren berufliche und wirtschaftliche Tätigkeit selbst speziell die zu beurteilende Protokollierung zum Gegenstand hat, nicht als Sachverständige heran gezogen werden, weil der Sachverständige sonst die Erforderlichkeit und letztlich Zulässigkeit seiner eigenen beruflichen und wirtschaftlichen Tätigkeit beurteilen müsste. Der Sachverständige muss die Beweisfrage fachlich beurteilen können, ohne jedoch ein eigenes berufliches oder wirtschaftliches Interesse an dem Ausgang der Beweisaufnahme zu haben. Diese Voraussetzung erfüllen nur die klägerseits vorgeschlagenen Personen.

2. Gesetzliche Regelung

Mit Schriftsatz vom 09.06.2010 ist erläutert worden, weshalb **die von der Beklagten gegebenen Begründungen** für ihre Aufzeichnungspraxis rechtlich unerheblich sind und die Aufzeichnung beliebiger Internetkennungen nicht zu rechtfertigen vermögen. Die dagegen vorgebrachten Einwendungen des Beklagtenvertreters greifen nicht durch:

Dass die Beklagte **personenbezogene Daten** verarbeitet, hat das Hohe Gericht seinem Beweisbeschluss zu Recht zugrunde gelegt. Am 08.09.2010 hat nun auch das oberste Gericht der Schweiz, das Schweizerische Bundesgericht, entschieden, dass die IP-Adresse eines Internetnutzers in der Hand einer vom Zugangsanbieter verschiedenen Stelle ein personenbezogenes Datum darstellt (Az. 1C_285/2009).

Zur Rechtfertigung der Beklagtenpraxis führt der Beklagtenvertreter jetzt **§ 904 BGB** an. Der Beklagtenvertreter zeigt aber weder auf, dass die Voraussetzungen des § 904 BGB im vorliegenden Fall gegeben seien, noch wie § 904 BGB von seiner Rechtsfolge

[2] Siemens CERT, http://www.siemens.com/innovation/de/ueber_funde/corp_technology/research_technology/technologieabteilung/info/cert.htm; Siemens, Sicherheit – Datennetze, http://www.siemens.com/innovation/de/publikationen/zeitschriften_pictures_of_the_future/pof_fruehjahr_2003/sicherheit/datennetze.htm.

her eine von einer konkreten, „gegenwärtigen Gefahr“ unabhängige Dauerprotokollierung rechtfertigen soll. Der Beklagtenvertreter verkennt vor allem, dass Diensteanbieter für die Bereitstellung von Telemedien erhobene personenbezogene Daten für andere Zwecke nur verwenden dürfen, „soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat“ (§ 12 Abs. 2 TMG). § 904 BGB bezieht sich nicht „ausdrücklich auf Telemedien“. Die bewusste Entscheidung des Gesetzgebers, Durchbrechungen der Spurenlosigkeit der Internetnutzung im Telemediengesetz speziell und abschließend zu regeln (*lex specialis*), kann nicht durch Rückgriff auf allgemeine Vorschriften des Bürgerlichen Rechts umgangen werden. Duldungspflichten im Sinne des § 1004 Abs. 2 BGB, wollte man § 1004 BGB denn als Anspruchsgrundlage heran ziehen, können sich daher allein aus dem Telemediengesetz selbst ergeben. Richtigerweise ist § 15 TMG als eigenständige Anspruchsgrundlage anzuerkennen, weil die Norm einen von der Allgemeinheit verschiedenen, abgrenzbaren Personenkreis – die Nutzer eines Telemediendienstes – faktisch begünstigt und gerade deren Persönlichkeitsinteressen schützen soll (Schutznorm).[3] Es kann nicht Absicht des Gesetzgebers gewesen sein, den Schutz der Nutzerdaten im Telemediengesetz zu regeln und mit einer Bußgeldandrohung zu bewehren, dem Nutzer aber kein Recht auf Durchsetzung seines gesetzlichen Schutzes einzuräumen. Jedenfalls folgt der Unterlassungsanspruch des Klägers auch aus § 35 Abs. 2 Nr. 1 BDSG, welcher anerkanntermaßen eine eigenständige Anspruchsgrundlage darstellt[4] und keine zusätzlichen Rechtsfertigungsmöglichkeiten eröffnet.

Der Beklagtenvertreter meint, um die Inanspruchnahme von Telemedien zu ermöglichen, sei all das **erforderlich i.S.d. § 15 Abs. 1 TMG**, was notwendig sei, „um einen nach dem Stand der Technik sicheren Betrieb zu gewährleisten“. Diese Definition ist als mit Wortlaut und Zweck des § 15 Abs. 1 TMG unvereinbar abzulehnen. Mit Schriftsatz vom 09.06.2010 ist ausgeführt worden, dass analog § 14 BImSchG allenfalls diejenigen Eingriffe in Nutzerrechte als zur Ermöglichung der „Inanspruchnahme von Telemedien“ erforderlich angesehen werden können, ohne welche die Bereitstellung des Telemediums „nach dem Stand der Technik nicht durchführbar oder wirtschaftlich nicht vertretbar“ wäre. Dass die Bereitstellung der Telemedien der Beklagten ohne Nutzerprotokollierung „nicht durchführbar oder wirtschaftlich nicht vertretbar“ wäre, behauptet die Beklagte selbst nicht. Umgekehrt stellen verschiedene Ministerien der Beklagten Telemedien ohne Nutzerprotokollierung bereit.

Der Beklagtenvertreter räumt jetzt erfreulicherweise ein, dass „die **technischen Mindestanforderungen** für das Bereithalten und Abrufen von Telemedien im Internet“ eine Nutzerprotokollierung nicht erfordern. Das Gebot der Datensparsamkeit (§ 3a BDSG) fordert gerade, „so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen“. Soweit der Beklagtenvertreter meint, die technischen Anforderungen an die Bereitstellung von Telemedien entsprächen nicht den „üblichen Sicherheitsstandards“, so ist dies bereits in den vergangenen Schriftsätzen unter Anführung verschiedener Standards und Empfehlungen widerlegt worden. Im Übrigen setzt eine möglicherweise „übliche“ Praxis kein Recht, sondern muss sich umgekehrt an dem demokratisch gesetzten Recht messen lassen. Um dies anschaulich zu machen: In manchen extremistischen Kreisen mag das Mitführen von Waffen als „üblicher Sicherheitsstandard“ gelten, ohne dass dies aber etwas an der Gesetzwidrigkeit dieser Praxis änderte. Dass das Prinzip der Datensparsamkeit

[3] Vgl. BeckOK, § 823 BGB, Rn. 155 m.w.N.

[4] BGHZ 181, 328; BGH, NJW 1984, 1889; st. Rspr.

„Sicherheitsinteressen und damit Rechtsgüter der Beklagten und Dritter gefährdet“, wie der Beklagtenvertreter behauptet, stellt die wahren Verhältnisse auf den Kopf: Die Datensammelwut der Beklagten ist es, welche Datensicherheitsinteressen und die Rechtsgüter unzähliger Internetnutzer gefährdet, wie die immer wiederkehrenden Datenpannen, Datenskandale und Datenmissbräuche zeigen, die durch vermeidbare Datensammlungen erst ermöglicht werden.

In jedem Fall ist das Merkmal der Erforderlichkeit in § 15 Abs. 1 TMG entsprechend dem rechtsstaatlichen **Verhältnismäßigkeitsgebot** grundrechtskonform auszulegen:[5] Als zur Bereitstellung von Telemedien erforderlich können nur diejenigen Eingriffe in Nutzerrechte angesehen werden, die zur wirtschaftlich vertretbaren Bereitstellung von Telemedien geeignet, erforderlich und verhältnismäßig sind. Eine Nutzerprotokollierung über das Ende des Nutzungsvorgangs hinaus ist zur Bereitstellung von Telemedien bereits deshalb nicht geeignet, weil Telemedien dem Nutzer nach Nutzungsende nicht mehr bereitgestellt werden müssen. Jedenfalls aber ist eine flächendeckende, permanente Aufzeichnung der Identität und des Verhaltens beliebiger Internetnutzer völlig unverhältnismäßig.

Mit Schriftsatz vom 09.06.2010 sind zahlreiche **Telemedien der Beklagten** genannt worden, die nach eigenen Angaben keine IP-Nutzerkennungen in personenbeziehbarer Form speichern. Der Beklagtenvertreter wendet ein, dass in Fällen der Nichtspeicherung durch den jeweiligen Anbieter „sehr wohl durch den Betreiber des Webservers eine Speicherung in Logfiles vorgenommen werden kann.“ Diese Möglichkeit besteht zwar grundsätzlich. Von ihr wird aber bei den meisten der vom Kläger genannten speicherfreien Telemedien der Beklagten keinen Gebrauch gemacht. Die Aufzählung speicherfreier Telemedien der Beklagten beruht unter anderem auf einer Umfrage[6] des Bundesdatenschutzbeauftragten, welche ausdrücklich auch die etwaige Einschaltung externer Dienstleister zum Gegenstand hatte. Wenn Behörden der Beklagten dort gleichwohl angaben, keine IP-Adressen „werden erhoben/gespeichert“, so bezog sich diese Angabe auch auf etwaige externe Dienstleister. Der Beklagtenvertreter behauptet mit Ausnahme des Bundeskriminalamtsportals selbst nicht konkret, dass bei den vom Kläger genannten Telemedien externe Anbieter Nutzer-IP-Adressen erfassten. Im Hinblick darauf, dass nur die Beklagte Einblick in ihre Speicherpraxis hat, kann es ihr prozessual nicht gestattet sein, ins Blaue hinein die Behauptung aufzustellen, dass eine anderweitige Speicherung „vorgenommen werden kann.“ Hier trifft die Beklagte eine sekundäre Darlegungslast. Mehrere der genannten Anbieter haben in der Umfrage ausdrücklich erklärt, keinen externen Serverbetreiber einzuschalten.[7] Auch andere Telemedien, deren Benutzung laut Datenschutzerklärung ausdrücklich keine Speicherung von IP-Adressen mit sich bringt (z.B. Bundesjustizministerium, Bundesdatenschutzbeauftragter, Bundesforschungsministerium, Bundesfinanzministerium), werden ohne externe Datenspeicherung bereit gestellt. Der Beklagtenvertreter will sicherlich selbst nicht behaupten, dass die Beklagte entgegen § 13 Abs. 1 TMG falsche Datenschutzerklärungen veröffentlichte, zumal der Betreiber eines Telemediums für eine etwaige Datenspeicherung durch externe Auftragnehmer einzustehen hat (§ 11 BDSG).

[5] Vgl. MüKo-Säcker, Einl., Rn. 132 m.w.N.

[6] Bundesdatenschutzbeauftragter, Abfrage der Bundesbehörden zur Praxis bei der Speicherung von Nutzungsdaten (März 2008), http://daten-speicherung.de/data/bfdi_umfrage_surfprotokollierung.pdf.

[7] Bundesdatenschutzbeauftragter, Abfrage der Bundesbehörden zur Praxis bei der Speicherung von Nutzungsdaten (März 2008), http://daten-speicherung.de/data/bfdi_umfrage_surfprotokollierung.pdf.

3. Beweisfragen

Mit Schriftsatz vom 09.06.2010 haben wir eine Präzisierung der Beweisfragen angeregt, wie in dem **Beweisbeschluss** vorbehalten. Dies ist weiterhin sinnvoll. Für den Fall, dass das Gericht eine Präzisierung der Beweisfragen nicht mehr vornehmen sollte, geht der Kläger davon aus, dass der Beweisbeschluss allein die Behauptungen der Beklagten wiedergibt und nicht die Beurteilung vorweg nimmt, inwieweit diese Behauptungen überhaupt von rechtlicher Bedeutung sind.

Unabhängig von der Rechtserheblichkeit soll im Folgenden zu den Beweisbehauptungen der Beklagten laut Beweisbeschluss Stellung genommen werden:

Die Beklagte behauptet, zur Gewährleistung **und Aufrechterhaltung der IT-Sicherheit** und der Funktionsfähigkeit der von ihr betriebenen und verwendeten Telemedien und Telekommunikationsnetze sei die Speicherung und spätere Verwendung von IP-Adressen des zugreifenden Hostsystems ihrer Nutzer erforderlich. Der Begriff der IT-Sicherheit ist in § 2 Abs. 2 BSIG definiert als die Verfügbarkeit, Unversehrtheit und Vertraulichkeit von Informationen. Die Anforderung der Verfügbarkeit umfasst damit bereits die Funktionsfähigkeit des Systems.

Unter Anwendung des aus dem **Rechtsstaatsprinzip** folgenden Verhältnismäßigkeitsgebots ist die Speicherung und spätere Verwendung von Nutzer-IP-Adressen zur Gewährleistung und Aufrechterhaltung der IT-Sicherheit erforderlich, wenn sie 1. geeignet ist, die Verfügbarkeit, Unversehrtheit und Vertraulichkeit von Informationen zu erhöhen, wenn 2. diese Erhöhung nicht durch mildere Mittel zu erreichen ist und wenn 3. das Maß an Erhöhung der IT-Sicherheit nicht außer Verhältnis zur Schwere des Eingriffs steht.

Im Rahmen der zweiten Frage nach der Erforderlichkeit sind als **mildere Mittel** alle Sicherheitsmaßnahmen in die Betrachtung einzubeziehen, welche technisch machbar, wirtschaftlich vertretbar und nicht mit Übergriffen in die Rechte unbeteiligter Nutzer verbunden sind. Maßstab muss also das sichere, fachgerecht eingerichtete, unterhaltene und verwendete IT-System sein, denn fachgerechte Vorsorge gegen Sicherheitsverletzungen greift weniger in Nutzerrechte ein als eine globale Aufzeichnung des Nutzerverhaltens. Es ist bereits darauf hingewiesen worden, dass zur fachgerechten Vorsorge eine sichere Abschottung von Webservern gehört und dass dann Risiken für von der Beklagten verwendete Telemedien Dritter oder für ihre Telekommunikationsnetze von vornherein nicht bestehen. Als milderes Mittel kommt auch die Bereitstellung des Telemedienangebots der Beklagten über externe Auftragnehmer und deren IT-Systeme in Betracht, wodurch Sicherheitsrisiken für die Beklagte ebenfalls praktisch ausgeschlossen werden können.

Nur wenn die Internet-Vorratsdatenspeicherung geeignet wäre, bei **sicher eingerichteten Webservern** die Verfügbarkeit, Unversehrtheit und Vertraulichkeit von Informationen weiter zu erhöhen, könnte sie als erforderlich angesehen werden. Selbst wenn die Erforderlichkeit nach diesem Maßstab zu bejahen wäre, wäre als milderes Mittel noch eine bloß eingeschränkte, anlassbezogene IP-Protokollierung in Betracht zu ziehen, um unbeteiligte Nutzer wie den Kläger möglichst vor einer unnötigen Erfassung seines Nutzungsverhaltens zu schützen.

Im Rahmen der dritten Frage nach der **Verhältnismäßigkeit** ist zu berücksichtigen, dass eine anlasslose und flächendeckende staatliche Erfassung des Internet-

Informations- und Kommunikationsverhaltens völlig unschuldiger und rechtschaffener Bürger das permanente Risiko einer Aufhebung der Vertraulichkeit der vertraulichen Internetnutzung durch etwaige Pannen oder Missbrauch schafft und die von diesem Risiko ausgehende abschreckende Wirkung die Informations- und Meinungsfreiheit der Bürger unzumutbar einschränkt. Es ist dementsprechend bereits umfassend unter Heranziehung der einschlägigen Rechtsprechung belegt worden, dass die beklagtenseits teils praktizierte pauschale und globale Internetaufzeichnung *per se* – also unabhängig von ihrem vorgeblichen Nutzen – unverhältnismäßig und mit den Grundrechten unvereinbar ist. Vor dem Hintergrund der Tiefe und Tragweite des Eingriffs kann keinesfalls jede Erhöhung der IT-Sicherheit eine Internet-Vorratsdatenspeicherung rechtfertigen. Selbst ein in der Praxis nachweislich und erheblich sicherer Betrieb von IT-Systemen durch eine flächendeckende IP-Protokollierung genügte zur Rechtfertigung nicht. Selbst wenn Webserver also gerade aufgrund einer flächendeckenden IP-Protokollierung erheblich weniger Verletzungen von Verfügbarkeit, Vertraulichkeit oder Integrität hinnehmen müssten als fachgerecht eingerichtete und eingesetzte Webserver ohne eine solche Protokollierung – was empirisch nicht auch nur ansatzweise belegt ist –, könnte die Verhältnismäßigkeit der Maßnahme noch nicht angenommen werden. Nur als notwendige, aber nicht hinreichende Voraussetzung der Verhältnismäßigkeit einer globalen und pauschalen Internet-Vorratsdatenspeicherung käme in Betracht, wenn empirisch gesichert wäre, dass entsprechende Systeme letztlich erheblich weniger Verletzungen von Verfügbarkeit, Vertraulichkeit oder Integrität hinnehmen müssten als fachgerecht eingerichtete und eingesetzte Webserver ohne eine solche Protokollierung. Die Beklagte mag bezeichnenderweise nicht einen empirischen Nachweis dieser Art anführen und betreibt umgekehrt selbst diverse Webserver ohne Protokollierung. Ungeachtet dessen ist daran festzuhalten, dass selbst eine empirisch nachweisbare, erhebliche Erhöhung der IT-Sicherheit eine anlasslose und flächendeckende staatliche Erfassung des Internet-Informations- und Kommunikationsverhaltens völlig unschuldiger und rechtschaffener Bürger vor den Grundrechten und dem Verhältnismäßigkeitsgebot nicht zu rechtfertigen vermag. Verhältnismäßig wäre eine Internet-Vorratsdatenspeicherung allenfalls, wenn das Telemedienangebot der Beklagten ohne diese Praxis „nach dem Stand der Technik nicht durchführbar oder wirtschaftlich nicht vertretbar“ wäre (§ 14 BImSchG analog).

Die Beklagte behauptet, eine Vorratsspeicherung von IP-Adressen entspreche dem nationalen und internationalen **Stand der Technik**. Es ist demgegenüber bereits darauf hingewiesen worden, dass der Stand der Technik lediglich die Summe aller technischen Möglichkeiten zu einem Zeitpunkt bezeichnet; technisch möglich ist die Vorratsspeicherung jeglicher IP-Adressen fraglos. Von rechtlicher Bedeutung kann hingegen allenfalls sein, ob eine IP-Protokollierung zu den (allgemein) „anerkannten Regeln der Technik“ bei dem Betrieb eines Webservers zu zählen ist. Die anerkannten Regeln der Technik unterscheiden sich vom Stand der Technik dadurch, dass sich letzterer in der Praxis noch nicht bewährt haben muss.[8] Anerkannte Regeln der Technik sind nur solche Regeln, die in der Wissenschaft keinem Meinungsstreit ausgesetzt und damit als theoretisch richtig anerkannt sind und feststehen sowie insbesondere in dem Kreise der für die Anwendung der betreffenden Regeln maßgeblichen, nach dem neuesten Erkenntnisstand vorgebildeten Techniker durchweg bekannt und auf Grund fortdauernder praktischer Erfahrung als technisch geeignet, angemessen und notwendig anerkannt sind.[9] Die allgemein anerkannten Regeln der Technik sind nicht identisch mit geschriebenen Regelwerken. Die in Regelwerken

[8] MüKo-Busche, § 633 BGB, Rn. 19.
[9] RGSt 44, 76.

zusammengefassten Normen können zwar allgemein anerkannte Regeln der Technik sein, sie brauchen es aber nicht zu sein.[10]

Von Bedeutung kann mithin allenfalls sein, ob die von der Beklagten praktizierte Vorratsdatenspeicherung in der Wissenschaft keinem Meinungsstreit ausgesetzt und damit als theoretisch richtige Maßnahme zur Gewährleistung der IT-Sicherheit **anerkannt** ist und feststeht sowie Informatikern durchweg bekannt und auf Grund fortdauernder praktischer Erfahrung als technisch geeignet, angemessen und notwendig zur Gewährleistung der Verfügbarkeit, Vertraulichkeit und Integrität von Informationen anerkannt ist. Nach Überzeugung des Klägers kann von einer solchen allgemeinen Anerkennung und praktischen Bewährung einer nicht-anonymisierten Protokollierung der Webserver-Nutzung keine Rede sein, zumal bedeutende Telemedien dauerhaft ohne solche Protokollierung angeboten werden. Viele Betreiber verzichten schon aus Gründen der Leistungsfähigkeit (Performance) auf solche Protokolle. Der Hersteller des verbreiteten Webservers Apache erklärt: „Eines der oftgenannten Argumente gegen eine Protokollierung ist die erforderliche Rechenkapazität. Dies ist ein legitimer Einwand, weil selbst mittelgroße Anwendungen Tausende von Protokollierungsanfragen auslösen können.“[11] Auch der zweitgrößte Hersteller von Webserver-Software Microsoft empfiehlt zum „Optimieren der Webserverleistung“: „Deaktivieren Sie die Protokollierung für Websites, virtuelle Verzeichnisse oder Dateien und Ordner, sofern diese nicht unbedingt erforderlich ist.“[12]

Im Übrigen weist die Rechtsprechung zutreffend darauf hin, dass selbst anerkennte Regeln der Technik **für sich genommen keine rechtliche Bedeutung** zukommt; ausschlaggebend ist allein, ob ein Verfahren zwangsläufig den angestrebten Erfolg beeinträchtigt.[13] Überhaupt wendet die Rechtsprechung die anerkennten Regeln der Technik nur im Vertragsrecht und wo gesetzlich gefordert an, nicht aber als eigene Rechtfertigung für Grundrechtseingriffe. Es muss nochmals deutlich darauf hingewiesen werden, dass das deutsche Recht und die Grundrechte im Kollisionsfall Vorrang auch vor etwa anerkannten Regeln der Technik haben und deren Anwendung Grenzen setzen.

4. Vermeintliche Notwendigkeit der Speicherung von IP-Adressen

Mit Schriftsatz vom 09.06.2010 ist darauf hingewiesen worden, dass im vorliegenden Rechtsstreit alleine die Sicherheit sogenannter Webserver der Beklagten in Rede steht, also von Systemen zur Bereitstellung von Telemedien. Auf Webservern dürfen laut BSI **andere Anwendungen nicht vorhanden** sein.[14] Der Beklagtenvertreter wendet ein, viele Telemedien erforderten eine Verbindung zu einer Datenbankapplikation. Dies trifft zu („dynamische Webseiten“), ändert aber nichts daran, dass sich eine solche Datenbankapplikation auf den abgeschotteten Webservern befinden muss. Auf Webservern dürfen keine Anwendungen vorhanden sein, die nicht eigens zur Bereitstellung des Telemediums erforderlich sind. Wird diese einfache Sicherheitsgrundregel beachtet, können Telemedien ohne Risiko für sonstige Systeme der Beklagten bereit gestellt werden. Ein Risiko besteht dann allenfalls für die Verfügbarkeit, Vertraulichkeit und Integrität des Telemediums selbst. Soweit der

[10] BGH, NJW 2007, 2983; BGH, NJW 2005, 1115; BGH, NJW 1998, 2814.

[11] Apache, log4net Manual (2007), http://logging.apache.org/log4net/release/manual/internals.html.

[12] Microsoft, Optimieren der Webserverleistung in Windows 2000, http://support.microsoft.com/kb/308186; ebenso Microsoft, Optimize Web Server Performance in Windows Server 2003, http://support.microsoft.com/kb/816517/en-us; vgl. auch Microsoft, IIS Optimization, http://technet.microsoft.com/en-us/library/bb727104.aspx.

[13] BGH, NJW-RR 1995, 472.

[14] BSI, IT-Grundschutzkatalog „M4 Hardware und Software“, M 4.97: „Ein Dienst pro Server“, https://www.bsi.bund.de/cln_174/ContentBSI/grundschutz/kataloge/m/m04/m04097.html.

Beklagtenvertreter ausführt, Angriffe dienten häufig dazu, die Abschottung von Webservern zu durchbrechen, so kann dieses Risiko durch eine physische Trennung von sonstigen Systemen ausgeschlossen werden.

Der Beklagtenvertreter führt zutreffend aus, dass Sicherungsmaßnahmen das Risiko von Einbrüchen **nie ganz ausschließen** können. Zum Einen wird aber bestritten, dass es bei fachgerecht eingerichteten und eingesetzten Webservern der Beklagten je zu einem erfolgreichen Einbruch gekommen ist oder kommen wird. Zum Anderen wird bestritten, dass fachgerecht eingerichtete und eingesetzte Webserver der Beklagten gerade im Fall einer Protokollierung beliebiger IP-Adressen insgesamt weniger Verletzungen von Verfügbarkeit, Vertraulichkeit oder Integrität hinnehmen müssten als fachgerecht eingerichtete und eingesetzte Webserver ohne eine solche Protokollierung. Hat die Protokollierung beliebiger IP-Adressen aber letztlich keine empirisch nachweisbare Auswirkung auf die IT-Sicherheit fachgerecht eingerichteter und eingesetzter Webserver, so kann sie auch nicht als erforderlich angesehen werden.

Die **Möglichkeit einer Analyse und Rückverfolgung von IP-Adressen** erhöht die Verfügbarkeit, Vertraulichkeit und Integrität fachgerecht eingerichteter und eingesetzter Webserver nicht in empirisch nachzuweisendem Maß, zumal sich ernsthafte Angriffe regelmäßig nicht weiter als zu einem russischen oder chinesischen Server rückverfolgen lassen, was nutzlos ist. Es ist bereits Prof. Dr. Hartmut Pohl mit den Worten zitiert worden: „Das ist auch der Stand der Technik in Unternehmen, die sich nicht dazu verleiten lassen zu protokollieren, wer greift auf unsere Systeme wann zu und sendet etwas, sondern, wenn ein Angriff stattgefunden hat, wird nicht eruiert, wer der Täter ist, es wird eruiert, wo liegt die Sicherheitslücke, und die wird geschlossen." In einer Umfrage unter 320 Unternehmen gaben 70% an, nach Einbrüchen Sicherheitslücken geschlossen zu haben, während nur 20% den Vorfall an Strafverfolgungsbehörden zur Weiterverfolgung meldeten.[15]

Der Beklagtenvertreter führt an, Anomalieerkennungssysteme könnten Datenveränderungen erkennen. Es ist indes schon ausgeführt worden, dass sich solche Veränderungen auch ohne Speicherung von IP-Adressen mit der vom BSI empfohlenen „**regelmäßigen Integritätsprüfung**"[16] erkennen lassen. Soweit der Beklagtenvertreter einwendet, dadurch lasse sich keine Vorsorge gegen zukünftige Angriffe treffen, ist dies mittels der Speicherung von IP-Adressen ebensowenig möglich. Vorsorge gegen zukünftige Angriffe lässt sich nur durch das Schließen von Sicherheitslücken treffen. Technisch falsch ist die Behauptung des Beklagtenvertreters, eine regelmäßige Integritätsprüfung habe bei dynamischen Telemedien „keinerlei Wirkung mehr". Im Wege der Integritätsprüfung können auch Veränderungen von Datenbanken erkannt werden. Eine regelmäßige Integritätsprüfung ist zu Recht im aktuellen IT-Grundschutzhandbuch des BSI vorgesehen. Es ist nicht ersichtlich, was den Beklagtenvertreter besser zur Beurteilung dieser Frage qualifizieren sollte als das Bundesamt für Sicherheit in der Informationstechnik.

Der Beklagtenvertreter beharrt darauf, dass auch **erfolglose Angriffsversuche** erkannt werden müssten. Er vermag aber nicht schlüssig darzulegen, wozu solche Kenntnis von Nutzen sein soll. Sicherheitslücken müssen ohnehin laufend geschlossen werden. Dass das Blockieren einzelner IP-Adressen wirkungslos ist, ist bereits im letzten Schriftsatz ausgeführt worden.

---

[15] CSI/FBI Computer Crime and Security Survey 2005, http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf, 20.

[16] BSI, IT-Grundschutzkatalog „M4 Hardware und Software", M 4.93: „Regelmäßige Integritätsprüfung", https://www.bsi.bund.de/cln_174/ContentBSI/grundschutz/kataloge/m/m04/m04093.html.

Soweit der Beklagtenvertreter sich **verändernde Angriffstechniken** mit mutierenden Grippeviren vergleicht, ist darauf hinzuweisen, dass sich fachgerecht eingerichtete und eingesetzte Webserver ungeachtet allfälliger Angriffsversuche in der Praxis auch ohne IP-Protokollierung gut betreiben lassen, nicht anders als die Menschheit mit der Existenz von Grippeviren leben kann und muss. Der Beklagtenvertreter würde wohl kaum fordern wollen, jeden Kontakt zwischen zwei Menschen aufzuzeichnen, nur weil man dadurch die Verbreitung von Krankheitserregern besser nachverfolgen könnte? Dazu würde das im vorliegenden Prozess vertretene maßlose Sicherheitsverständnis der Gegenseite aber letztlich führen.

Die Behauptung der Beklagten, die zitierten Aussagen des Bundesamts für Sicherheit in der Informationstechnik seien **veraltet**, ist falsch. Die zitierten Informationen werden aktuell auf dem Internetportal des BSI veröffentlicht. Sie gelten auch unter den Bedingungen dynamischer Telemedien. Dasselbe gilt für die Aussagen von Herrn Fox.

Anomalieerkennung unter Verwendung auf Vorrat gespeicherter IP-Adressen gehört nicht zum Sicherheitsstandard; der Beklagtenvertreter vermag keinen einzigen Beleg für seine entsprechende Behauptung anzuführen. Umgekehrt zeigen diverse Telemedien der Beklagten, dass eine Bereitstellung ohne IP-Protokollierung machbar und üblich ist.

Sperrlisten bleiben auch dann wirkungslos, wenn die Beklagte 47.000.000 von 4.200.000.000 IP-Adressen sperrt, weil dann noch immer weitere 4.153.000.000 IP-Adressen für Angriffe zur Verfügung stehen. Im Zeitalter von IPv6 werden es bereits 340 Mrd. Mrd. Mrd. Mrd. IP-Adressen sein (2^{128} oder 340.282.366.920.938.000.000.000.000.000.000.000 Adressen).[17] Bei diesen Zahlen ist offensichtlich, dass die Sperrung einzelner IP-Adressen wirkungslos ist. Im Übrigen ist bereits darauf hingewiesen worden, dass der Einsatz von Sperrlisten keine eigene IP-Protokollierung erfordert.

Dass „umfangreiche **Hackingangriffe**“ nur mithilfe von IP-Adressen abgewehrt werden könnten, ist falsch. Die verfügbaren milderen Mittel sind im letzten Schriftsatz aufgezeigt worden.

Der Beklagtenvertreter meint, eine Nutzerprotokollierung nur zur Wiederherstellung eines Telemediums sei, wie wenn man eine **Alarmanlage** erst nach dem Einbruch einschaltete. Dieser Vergleich ist falsch, denn die nachträgliche Aktivierung einer Alarmanlage ist nicht zur Wiederherstellung eines Gebäudes, in das eingebrochen wurde, erforderlich. Bei zutreffendem Vergleich entspräche es der beklagtenseits praktizierten Nutzererfassung, wenn jeder Besucher eines öffentlichen Gebäudes vor dem Eintreten seine Personalausweisnummer in eine Liste eintragen müsste und jeder Schritt, den er in dem Gebäude täte, aufgezeichnet würde. Solches ist in einer Demokratie schlechterdings undenkbar und darf auch im Internet nicht Wirklichkeit bleiben.

Der Beklagtenvertreter meint, eine Nutzerprotokollierung sei zur **Strafverfolgung** erforderlich, denn andernfalls komme das Internet einem Straßenverkehr mit Geschwindigkeitsbeschränkungen gleich, die „garantiert nicht überwacht“ würden. Der Beklagtenvertreter verkennt, dass die vorliegende Klage die gesetzlichen Befugnisse der Strafverfolgungsbehörden zum Einschreiten im Verdachtsfall unberührt lässt. Nach dem Gesetz sind nicht die Anbieter von Telemedien für die Strafverfolgung zuständig (vgl. § 15 Abs. 1 TMG), sondern die Staatsanwaltschaften und Gerichte. Da der Kläger

[17] Wikipedia, IPv6, http://de.wikipedia.org/wiki/Ipv6.

bei dem Besuch von Telemedien der Beklagten keine Straftaten begeht, ist die Speicherung seiner IP-Adresse zu diesem Zweck nicht erforderlich. Insbesondere ist keine verdachtsunabhängige Speicherung durch Stellen erforderlich, zu deren Aufgaben und Befugnissen die Strafverfolgung nicht gehört. Die Vorstellungen der Beklagten auf den Straßenverkehr übertragen würden bedeuten, dass jegliche Bewegungen von Pkw im Straßenverkehr verdachtsunabhängig und flächendeckend aufgezeichnet würden, um prophylaktisch eine etwaige Strafverfolgung zu erleichtern. Dieser Vergleich zeigt, dass das im vorliegenden Prozess vertretene maßlose Präventionsverständnis der Gegenseite einem diktatorischen Überwachungsapparat wie der DDR-Staatssicherheit würdig sein mag, nicht aber einem freiheitlichen Rechtsstaat.

Meinhard Starostik
Rechtsanwalt