Meinhard Starostik ◆ Rechtsanwalt

RECHTSANWALTSKANZLEI
Wittestr. 30E ◆ D- 13509 Berlin
+49 30 8800030 ◆ Fax: +49 30 88000310
kanzlei@starostik.de
USt-ID-Nr.: DE165877648

KANZLEI VEREIDIGTER BUCHPRÜFER
Schwarzenberger Str. 7 ◆ D-08280 Aue
+49 3771 564700 ◆ Fax: +49 3771 5647025

Commerzbank AG
Konto: 3 855 855 00 ◆ BLZ: 430 400 36
IBAN: DE57 4304 0036 0385 5855 00
BIC: COBADEFFXXX

RA Starostik ◆ Wittestr. 30 E ◆ D-13509 Berlin

Landgericht
Littenstr. 12-17
10179 Berlin
Nur per EGVP

Mein Zeichen: 45/08

Berlin, den 8. Nov. 2017

Breyer ./. BRD
Aktenzeichen: 57 S 87/08

In vorbezeichneter Angelegenheit wird zu dem Schriftsatz des Beklagtenvertreters vom 28.09.2017 wie folgt Stellung genommen:

Personenbezug

Dass die Beklagte eingegebene Personendaten von Nutzern ohne Zeitstempel speichere, wird mit Nichtwissen bestritten, zumal das Bundesverwaltungsamt nur einen Teil der Internetangebote der Beklagten kontrolliert. Im Fall einer Bestellung ist davon auszugehen, dass diese per E-Mail an die zuständige Stelle versandt wird und insofern durchaus ein Zeitstempel gespeichert wird, welcher mit dem Logfile zusammengeführt werden kann. Hinzu kommt, dass die Beklagte auch laufend E-Mails von Bürgern (einschließlich des Klägers) empfängt, die zuvor ihre Telemedien genutzt haben. Auch aus diesen E-Mails ist der Beklagten die IP-Adresse des Absenders bekannt.

Rechtfertigung mit „Angriffsdruck" oder „Gefahrenpotenzial"

Bemerkenswerterweise verfehlen die von der Beklagten hierzu vorgetragenen Allgemeinplätze schon im Ansatz die vom Bundesgerichtshof für klärungsbedürftig gehaltene Frage, ob sich die von Telemedium zu Telemedium unterschiedliche Speicherpraxis der Beklagten durch einen jeweils unterschiedlichen „Angriffsdruck" bzw. „Gefahrenpotenzial" erklären lassen (Abs. 41 des Revisionsurteils). Wenn die Beklagte bei diversen Telemedien mangels „Angriffsdrucks" auf eine verdachtslose Vorratsspeicherung des Nutzungsverhaltens verzichtet, wäre vorzutragen, inwiefern die Funktionsfähigkeit der anderen Telemedien größeren Gefahren ausgesetzt ist – so der Gedanke des Bundesgerichtshofs.

Die Beklagte lässt jedoch weiterhin jeglichen Vortrag zu Unterschieden zwischen ihren Telemedien mit und ohne Vorratsspeicherung der Internetnutzung vermissen, so dass ihr Argument des „fehlenden Angriffsdrucks" unschlüssig bleibt. Voraussetzung der vom

Bundesgerichtshof vermissten Feststellungen (Abs. 41) wäre entsprechender Vortrag der darlegungs- und beweisbelasteten Beklagten, an dem es mangelt.

Tatsächlich ist es auch unzutreffend, dass die Telemedien der Beklagten, die ohne Vorratsdatenspeicherung angeboten werden, geringeren Gefahren ausgesetzt oder von geringerer Bedeutung wären als die Telemedien, für die eine Vorratsdatenspeicherung erfolgt. Die unterschiedliche Speicherpraxis ist schlicht nicht sachlich begründet und sachlich nicht zu begründen. Telemedien der Beklagten ohne Vorratsdatenspeicherung sind denselben Gefahren ausgesetzt und von ebenso großer Bedeutung wie die Telemedien mit Vorratsdatenspeicherung. Ihre generelle Funktionsfähigkeit ist ebenso gut gewährleistet wie die der Telemedien mit Vorratsdatenspeicherung. Die Verfügbarkeit und Funktionsfähigkeit der Telemedien der Beklagten hängt nicht davon ab, ob der jeweilige Webserver das Nutzungsverhalten auf Vorrat speichert oder nicht. Etwas anderes trägt die Beklagte schon nicht vor, so dass sich eine Beweiserhebung darüber erübrigt.

Allerdings ergibt sich aus dem Vortrag der Beklagten, dass die „generelle Funktionsfähigkeit" ihrer Telemedien gewährleistet und das Risiko von Ausfällen denkbar gering ist. Die Beklagte nennt nämlich nur einen einzigen Ausfall zweier Telemedien (Familien- und Wirtschaftsministerium) in der 34. Kalenderwoche, der offenbar schnell behoben war – offensichtlich auch ohne Rückgriff auf anlasslos gespeicherte Nutzungsdaten.

Dies bedeutet im Umkehrschluss, dass die Telemedien der Beklagten generell funktionsfähig sind, ob eine Vorratsspeicherung von Nutzungsdaten erfolgt oder nicht. Das Risiko von Ausfällen ist extrem gering. Vermutlich hätte eine fachgerechte technische Gestaltung auch die Ausfälle in der 34. Kalenderwoche verhindert. Zum Umgang mit Überlastungsangriffen (DoS-Angriffen) ist bereits vorgetragen worden. Im Übrigen ist dieser Fall vom Klageantrag ausgenommen, wenn es darin heißt:

> *„...soweit die Speicherung nicht im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich ist*"

Gewährleistung der generellen Funktionsfähigkeit der Telemedien der Beklagten

Von den vielfältigen vorgetragenen Zielen, welche die Beklagte mit ihrer anlasslosen Surfprotokollierung verfolgt, kann nach § 15 Abs. 1 TMG und EU-Datenschutzrecht einzig die Ermöglichung der Inanspruchnahme, also die Gewährleistung der Funktionsfähigkeit des Telemediums, die Speicherung von Nutzungsdaten rechtfertigen.

Um die Funktionsfähigkeit von Telemedien zu überprüfen und Funktionsstörungen zu erkennen, ist die Speicherung von Nutzungsdaten unstreitig nicht erforderlich. Es genügt eine Beobachtung der Verfügbarkeit durch regelmäßige automatisierte Testzugriffe („Monitoring"). Diese kann sehr engmaschig, etwa im Sekundentakt, erfolgen. Auch ist eine Beobachtung der Auslastung des Webservers anhand anonymisierter Daten möglich. Verfügbarkeitsangriffe sind nicht mehrstufig. Zur Erkennung von Verfügbarkeitsstörungen ist es nicht erforderlich, mehrere Schritte „zusammenzuführen".

Ob die Speicherung von Nutzungsdaten erforderlich ist, um Störungen der Verfügbarkeit zu beseitigen, kann offen bleiben. Denn der Klageantrag gesteht dies der Beklagten bereits zu, „...soweit die Speicherung ... im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich ist".

Neben der Verfügbarkeit setzt die Inanspruchnahme von Telemedien auch deren Integrität voraus, also die Korrektheit (Unversehrtheit) der bereit gestellten Daten und ihre korrekte Funktionsweise. Die Vorratsspeicherung von Nutzungsdaten ist aber weder geeignet noch erforderlich, um eine unautorisierte Modifikation von Informationen zu verhindern oder zu beseitigen. Die Nutzungsdaten erlauben keinen Rückschluss darauf, ob eine Modifikation stattgefunden hat und welche. Vielmehr ist eine ständige Beobachtung der Integrität des Telemediums erforderlich. Anhand technischer Verfahren wie Quersummen oder Hashwerten können Manipulationen an Dateien oder Datenbanken erkannt und ihre Berechtigung überprüft werden. Die Beklagte darf interne Manipulationen aus ihrem internen Netz heraus nach Art und Quelle protokollieren, weil dies nicht die Nutzer des Telemediums betrifft (keine Nutzungsdaten). Sie kann so erkennen, welche Veränderungen berechtigt sind und welche nicht. Funktionsstörungen durch Integritätsveränderungen an Telemedien scheinen bei der Beklagten allerdings ohnehin kein praktisch relevantes Problem zu sein. Die Beklagte trägt keinen solchen Fall vor.

Schadsoftware kann in der Tat zum Ausfall eines Telemediums führen. Die Vorratsspeicherung von Nutzungsdaten ist aber weder geeignet noch erforderlich, um Schadsoftware fernzuhalten oder zu beseitigen. Die IP-Adresse der Telemediennutzer erlaubt keinen Rückschluss darauf, ob eine Infektion stattgefunden hat und welche. Es ist dazu auch nicht erforderlich, „Zugriffsmuster" zu erkennen. Vielmehr ist neben einem vorbeugenden Schutz („Härtung") eine ständige Beobachtung der Integrität des Telemediums erforderlich. Anhand technischer Verfahren wie Virenscanner und Integritätsprüfung kann Schadsoftware erkannt werden.

Verwaltungsdienste können tatsächlich sicherheitskritisch und von hoher Bedeutung sein. Wegen der allgemeinen und nicht zu vermeidenden Unsicherheit der Internet-Infrastruktur sollten sicherheitskritische und wichtige Verwaltungsdienste aber niemals vom Internet, seiner Funktionsfähigkeit und Verfügbarkeit abhängig sein. Es darf keine Telemedien geben, deren 100-prozentige Funktionsfähigkeit unabweisbar ist, weil es unmöglich ist, die Funktionsfähigkeit eines Telemediums zu 100% zu garantieren. Als milderes Mittel gegenüber einer totalen Protokollierung der Internetnutzung hat die Beklagte ihre Verwaltungsdienste folglich so zu organisieren, dass sie im Notfall auch ohne Internet funktionieren. Im Übrigen ist eine totale Protokollierung der Internetnutzung ohnehin nicht geeignet, die Verfügbarkeit und Integrität der Telemedien der Beklagten messbar besser zu gewährleisten (vgl. das gerichtliche Sachverständigengutachten).

Richtig ist, dass die fachgerechte Einrichtung eines Telemediums keinen 100-prozentigen Schutz vor Störungen der Funktionsfähigkeit bietet. Falsch ist aber, dass eine Vorratsspeicherung der Internetnutzung die Funktionsfähigkeit von Telemedien messbar besser gewährleisten würde (siehe das gerichtliche Sachverständigengutachten). Eine permanente, wahllose Aufzeichnung der gesamten Telemediennutzung erhöht die Funktionsfähigkeit nicht und ist vor allem ein völlig unverhältnismäßiger Eingriff in die Grundrechte der Nutzer auf Datenschutz und informationelle Selbstbestimmung.

Sonstige Ziele der Beklagten

Weitere von der Beklagten verfolgte Ziele rechtfertigen eine anlasslose Surfprotokollierung nach § 15 Abs. 1 TMG schon deshalb nicht, weil die Vorschrift als legitimes Ziel einer Speicherung der höchst vertraulichen Nutzungsdaten einzig die Ermöglichung der Inanspruchnahme, also die Gewährleistung der Funktionsfähigkeit, des Telemediums anerkennt:

Zur Ermittlung der Identität von Angreifern erlaubt § 15 Abs. 1 TMG die Speicherung höchst vertraulicher Nutzungsdaten nicht, weil die Identität eines Angreifers für die Funktionsfähigkeit eines Telemediums ohne Bedeutung ist.

Zur Sanktionierung von Rechtsverstößen erlaubt § 15 Abs. 1 TMG die Speicherung höchst vertraulicher Nutzungsdaten nicht, weil dieser Zweck von der Gewährleistung der Funktionsfähigkeit zu unterscheiden ist. Dass Strafverfolgung auch generalpräventiv wirken soll, ändert daran nichts. Die Rechtsordnung hat die Verfolgung von Straftaten den dafür zuständigen Stellen übertragen und ihre Befugnisse geregelt. Eine vorsorgliche Vorratsspeicherung der Internetnutzung durch die Anbieter von Telemedien gehört nicht dazu. Ihr würde im Übrigen auch keine generalpräventive Wirkung zukommen, weil Angreifer eine Strafverfolgung anhand der IP-Adresse leicht verhindern können (z.B. über russische oder chinesische oder sonst gekaperte IP-Adressen).

Allgemein zur Gewährleistung eines „sicheren Betriebs" von Telemedien („IT-Sicherheit") erlaubt § 15 Abs. 1 TMG die Speicherung höchst vertraulicher Internet-Nutzungsdaten nicht, weil der Gesetzgeber diese wegen der hohen Grundrechtsrelevanz auf die Gewährleistung der Funktionsfähigkeit des Telemediums beschränkt hat. Der Betreiber eines Telemediums kann und muss dessen Sicherheit ohne Totalprotokollierung des Nutzungsverhaltens gewährleisten.

Zum Schutz anderer IT-Systeme erlaubt § 15 Abs. 1 TMG die Speicherung höchst vertraulicher Internet-Nutzungsdaten wegen deren hoher Schutzwürdigkeit nicht, sondern nur zur Gewährleistung der Funktionsfähigkeit des Telemediums selbst. Die Betreiber anderer IT-Systeme können und müssen sich selbst schützen.

Zur Warnung Dritter vor Schadsoftware oder zur „Bekämpfung von Botnetzen" erlaubt § 15 Abs. 1 TMG die Speicherung hochsensibler Nutzungsdaten wegen deren hoher Schutzwürdigkeit nicht, sondern nur zur Gewährleistung der Funktionsfähigkeit des Telemediums selbst. Dritte können und müssen ihre Systeme selbst vor Schadsoftware schützen. Stellt die Beklagte eine gefährliche Infektion ihrer Telemedien fest, kann und muss sie allgemein warnen und nicht versuchen nur einzelne Nutzer davon zu benachrichtigen (was ohnehin anhand der IP-Adresse nicht möglich ist). Zur Erkennung von Botnetzen ist die Protokollierung von Zugriffen auf Telemedien von vornherein ungeeignet, weil Botnetze nicht auf Telemedien der Beklagten zugreifen.

Zur Erkennung der Vorbereitung oder des Versuchs von Angriffen (z.B. ungewöhnliche oder unzulässige Zugriffe, Schwachstellenprüfung, versuchte DoS-Angriffe) erlaubt § 15 Abs. 1 TMG die Speicherung hochsensibler Nutzungsdaten nicht, weil bloß versuchte und erfolglose Angriffe die Funktionsfähigkeit des Telemediums nicht beeinträchtigen. Im Übrigen ist die unverkürzte IP-Adresse nicht zur Erkennung der Vorbereitung oder des Versuchs von Angriffen erforderlich. Angriffsversuche wie Schwachstellenprüfungen finden im Internet ständig statt. Sie sind vergleichbar mit einem Fußgänger, der Wohnhäuser in Augenschein nimmt oder die Pforte zu öffnen versucht. Selbst wenn ungewöhnliches Verhalten festgestellt wird, resultiert daraus nichts. Man kann lediglich Vorkehrungen treffen, um zu verhindern, dass Angriffe Erfolg haben. Dazu benötigt man keine Nutzungsdaten (vgl. das gerichtliche Sachverständigengutachten).

Zur Rekonstruktion/Analyse zusammengesetzter Angriffe und Verhinderung einer Wiederholung erlaubt § 15 Abs. 1 TMG die Speicherung hochsensibler Nutzungsdaten nicht, weil eine Rekonstruktion auch anhand anonymisierter Protokolle möglich ist. Wird die IP-Adresse durch Verkürzung anonymisiert, lässt der restliche Teil und gegebenenfalls weitere Protokollinhalte (z.B. zum System des Angreifers) eine Verfolgung der einzelnen Schritte

eines Angreifers zu. Die IP-Adresse gewährleistet eine Rekonstruktion im Übrigen schon deshalb nicht zuverlässig, weil der Angreifer wechselnde IP-Adressen einsetzen kann.

Zur Erkennung von Spionage-Schadsoftware wie der von der Beklagten angeführten Uroburos-Schadsoftware erlaubt § 15 Abs. 1 TMG die Speicherung hochsensibler Nutzungsdaten schon deshalb nicht, weil Spionagesoftware die Funktionsfähigkeit des Telemediums unberührt lässt. Die Uroburos-Schadsoftware wird mutmaßlich von russischen Diensten für Spionagezwecke eingesetzt, was Unauffälligkeit voraussetzt und jede Funktionsstörung vermeidet. Die Beklagte macht selbst nicht geltend, dass die Funktionsfähigkeit ihres Telemediums beeinträchtigt gewesen wäre. Es wird im Übrigen mit Nichtwissen betritten, dass der betroffene Webserver nach dem Stand der Technik geschützt war. Für Webserver ist das Betriebssystem Windows, auf dem die Schadsoftware Uroburos vorwiegend läuft, nicht als Stand der Technik anzusehen. Andernfalls war es jedenfalls vermeidbares menschliches Versagen, welches die Ausführung der Schadsoftware ermöglicht hat (z.B. Öffnen unsicherer E-Mail-Anhänge, Software-Download von unsicheren Seiten). Die Beklagte bleibt jeglichen Vortrag zum Infektionsweg schuldig, obwohl sich aus dem Infektionsweg ergibt, welche weniger eingreifende Mittel die Infektion hätten vermeiden können. Auch die Erkennung der Uroburos-Schadsoftware ist ohne Speicherung von Nutzungsdaten möglich, z.B. indem Zugriffe des Systems auf bekannte Steuerserver erkannt werden und Anti-Virussoftware eingesetzt wird. Zur Beseitigung der Infektion ist die (nichtssagende) IP-Adresse des Angreifers ebenso wenig erforderlich wie zur Erkennung und Beseitigung der genutzten Schwachstelle. Welche IP-Adresse vom Angreifer genutzt wurde, ist schlichtweg bedeutungslos. Die Verantwortlichen können für ihre Zwecke eine beliebige IP-Adresse nutzen. Es wird auch bestritten, dass die IP-Adresse des Angreifers erforderlich gewesen sei, um die Ursache zu beseitigen und weitere Angriffe zu verhindern. Eine Rekonstruktion ist schon anhand anonymisierter Protokolle möglich. Wird die IP-Adresse durch Verkürzung anonymisiert, lässt der restliche Teil und gegebenenfalls weitere Protokollinhalte (z.B. zum System des Angreifers) eine Rekonstruktion der einzelnen Schritte eines Angreifers zu. Die IP-Adresse gewährleistet eine Rekonstruktion im Übrigen schon deshalb nicht zuverlässig, weil der Angreifer wechselnde IP-Adressen einsetzen kann.

Bei alledem ist darauf hinzuweisen, dass § 15 TMG nur die Nutzer des Telemediums schützt. Diverse Angriffe (z.B. Schwachstellenprüfung) sind von der Telemediennutzung technisch klar zu unterscheiden und dürfen dann auch nach Maßgabe des allgemeinen Datenschutzrechts protokolliert werden.

Zu dem pauschalen Verweis der Beklagten auf ihr Parteigutachten verweist der Kläger ebenso pauschal auf seinen dazu eingereichten Schriftsatz vom 08.01.2013 (S. 3 ff.).

Letztlich hat die Beklagte mit Schriftsatz vom 22. März 2010 ihre wahllose Datenhordung schon einmal umfassend zu rechtfertigen versucht („Angriffsszenarien und Sicherheitsmaßnahmen") – jedoch schon damals ohne Erfolg. Der gerichtlich bestellte Sachverständige ist in seinem Gutachten vom 29.07.2011 nach eingehender Prüfung zu den folgenden Feststellungen gekommen:

> „Aus meiner Sicht dient die Speicherung von IP-Adressen nicht dem nationalen oder internationalen Stand der Technik. (S. 3) [...] Eine Speicherung von IP-Adressen ist weder zur Angriffserkennung noch zur Angriffsabwehr zwingend erforderlich. (S. 3) [...] Es treten jedoch im Wesentlichen keine zusätzlichen Kosten durch den Verzicht auf die IP-Adressen-Speicherung auf, da wie unter 2. erwähnt diese anderen Sicherheitsmaßnahmen in jedem Fall zwingend erforderlich für den sicheren Betrieb des IT-Systems sind. (S. 3) [...] Insbesondere ist in beiden Fällen die Absenderangabe frei festlegbar. (S. 5) [...] eine Speicherung von IP-Adressen kann bestenfalls einen

> marginalen Sicherheitsgewinn bringen (S. 9) [...] Zum anderen existiert für die Absicherung von IT-Systemen eine Vielzahl von anderen, wesentlich effektiveren Mitteln und Methoden. (S. 10)".

Das Landgericht hatte diese Feststellungen damals nicht in sein Urteil aufgenommen, weil es nach der zuletzt von der Kammer vertretenen Auffassung aus Rechtsgründen nicht darauf ankam.

Nach dem jetzt vorliegenden Urteil des Bundesgerichtshofs ist allerdings über die Eignung, Erforderlichkeit und Verhältnismäßigkeit einer verdachtslosen Vorratsspeicherung von Nutzungsdaten zu entscheiden. Die Entscheidung kann nunmehr auf das eingeholte Gerichtsgutachten gestützt werden. Allerdings ist darauf Rücksicht zu nehmen, dass die damaligen Beweisfragen (Beweisbeschluss vom 20.05.2010) teils zu unbestimmt und zu weit gefasst waren („IT-Sicherheit"). Sie beinhalten jedoch auch die rechtlich maßgebliche Frage, ob zur Gewährleistung der Funktionsfähigkeit der von der Beklagten angebotenen Telemedien eine anlasslose Vorratsspeicherung der IP-Adressen sämtlicher Nutzer erforderlich ist. Insofern ist das Gutachten verwertbar.

(Meinhard Starostik – Rechtsanwalt)