JONAS BREYER
RECHTSANWALT

Rechtsanwaltskanzlei Breyer
Schiersteiner Straße 37a
65187 Wiesbaden

Jonas Breyer
Rechtsanwalt

T [redacted]
F
M

www.ra-breyer.de

17.08.2018

Kanzlei Breyer ▪ Schiersteiner Straße 37a ▪ 65187 Wiesbaden
Landgericht Berlin
– 57 S 87/08 –
Tegeler Weg 17-21
10589 Berlin

57 S 87/08

In der Zivilsache

Breyer ./. Bundesrepublik Deutschland

wird auf den Schriftsatz der Beklagten vom 10.08.2018 wie folgt erwidert:

Vorab ist darauf hinzuweisen, dass auf Beweisantritte verzichtet wird, weil die Beklagte beweisbelastet wird. Sollte die Kammer anderer Auffassung sein, wird um einen Hinweis gebeten.

Zu 1. Gerichtliche Auflagen vom 02.07.2018

Zu 1.1. (Telemedien ohne Vorratsspeicherung personenbezogener Nutzungsdaten):

Die Anlage BB8 belegt, dass die Beklagte selbst im Bereich sicherheitskritischer Infrastrukturen Telemedien ohne personenbezogene Vorratsspeicherung der Internetnutzung anbietet, darunter die Internetplattform zum Schutz Kritischer Infrastrukturen selbst (KRITIS), Internetportale des Auswärtigen Amts (samt Reisewarnungen), des Bundesnachrichtendienstes, der Bundesanstalt für Finanzdienstleistungsaufsicht, der Deutschen Bundesbank, des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (Katastrophenschutz samt Warnhinweisen), des Deutschen Wetterdienstes (samt Unwetterwarnungen) und Internetportalen zu Behördenfunk, Atomaufsicht und Strahlenschutz. Eine eigene Recherche ergibt, dass auch das Internetangebot der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITIS) ohne Surfprotokollierung angeboten wird. Dies belegt, dass die Beklagte eine personenbezogene Vorratsspeicherung der Internetnutzung vielfach sogar zum Schutz kritischer Infrastrukturen nicht für erforderlich hält – und zwar nach Einschätzung der dafür zuständigen Stellen.

Unter den Telemedien ohne Surfprotokollierung befinden sich auch sensible Inhalte, deren Nutzer ein erkennbares Interesse an Anonymität haben, um Informationen über ihr Privatleben zu schützen (z. B. im Bereich Antidiskriminierung, Demenz, Migration, Arzneimittel, Psychologie, Pflegebedürftigkeit).

Die nun offengelegte Liste von Telemedien ohne Surfprotokollierung widerlegt auch die Behauptung der Beklagten, im Zuständigkeitsbereich des Bundesverwaltungsamts erfolge durchgängig eine Surfprotokollierung (Gegenbeispiel: *www.bund.de* bzw. *www.service.bund.de*).

Eine personenbezogene Vorratsspeicherung der Nutzung dieser Portale erfolgt auch nicht an anderer Stelle, etwa durch private Betreiber (Hoster):

- Eine Vielzahl der Telemedien ohne Surfprotokollierung wird nach dem eigenen Vortrag der Beklagten „von ihr selbst im Informationstechnikzentrum Bund (ITZ Bund) betrieben“ (laut Anlage BB7 z.B. Bundesamt für kerntechnische Entsorgungssicherheit, Bundesamt für Strahlenschutz, Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, Bundesanstalt für Finanzdienstleistungsaufsicht, Bundesnachrichtendienst, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe). Bei selbst betriebenen Telemedien ist eine Surfprotokollierung durch Private technisch ausgeschlossen. Dass das ITZ Bund die IP-Adresse der Telemediennutzer entgegen der dies verneinenden Datenschutzerklärung der Telemedien über das Ende des Nutzungsvorgangs hinaus speichere, trägt die darlegungs- und beweisbelastete Beklagte selbst nicht vor und wird mit Nichtwissen bestritten. Eine Verarbeitung der IP-Adresse durch das ITZ Bund findet in diesen Fällen nur technisch notwendig im Rahmen der Bereitstellung des Telemediums, also für die Dauer der Nutzung zu deren Ermöglichung (vgl. § 15 Abs. 1 TMG), statt.

- Soweit die Beklagte private Betreiber (Hoster) einschaltet, um ihre Telemedien anzubieten, wird mit Nichtwissen bestritten, dass die IP-Adresse der Telemediennutzer entgegen der dies verneinenden Datenschutzerklärung gespeichert werden könnte. Die Beklagte wäre dafür darlegungs- und beweisbelastet, sie benennt aber kein einziges Telemedium als Fallbeispiel dafür. Der Anbieter eines Telemediums ist auch für die Verarbeitung personenbezogener Daten seitens der genutzten technischen Plattform verantwortlich (vgl. EuGH, Urteil vom 05.06.2018, Az. C-210/16). Die Datenschutzerklärung eines Telemedienanbieters muss deshalb vollständig über die Verarbeitung der Daten seiner Nutzer aufklären, egal durch wen diese Verarbeitung erfolgt. Erfolgt laut (Datenschutz-)Erklärung einer Bundesbehörde keine Surfprotokollierung, muss sich die Beklagte daran festhalten lassen. Viele private Hoster bieten im Übrigen an, die IP-Adresse nicht oder nur verkürzt zu protokollieren, wovon die betroffenen Bundesbehörden ausweislich ihrer Datenschutzerklärungen offenbar Gebrauch machen. Dieses Angebot privater Betreiber (Hoster) belegt, dass auch diese eine personenbezogene Vorratsspeicherung der Internetnutzung für verzichtbar halten.

Zu 1.2 (Zusammenhang zwischen Einschränkungen der Nutzbarkeit und Speicherpraxis):

I. Zugriff auf weitere Infrastrukturen

Die von der Beklagten hervorgehobene mögliche Schadenshöhe ist ohne Bedeutung, weil die Vorratsspeicherung der Internetnutzung zum Schutz vor Schäden von vornherein nicht geeignet und nicht erforderlich ist.

Wenn sich der Schaden eines Angriffs auf ein Telemedium nicht auf dieses beschränkt, sondern der Angreifer Zugriff auf weitere Infrastrukturen erlangt, so ist das Telemedium nicht nach dem Stand der Technik eingerichtet. Die Beklagte selbst definiert die nach dem Stand der Technik notwendige Härtung nämlich wie folgt: „Grundsätzliches Leitbild aller Maßnahmen ist, dass die potentielle Kompromittierung eines einzelnen Clients nicht zur Kompromittierung des gesamten Netzwerkes oder der gesamten Organisation führen darf. Geeignete Maßnahmen werden deutschen Behörden und der deutschen Wirtschaft regelmäßig durch das BSI empfohlen.“ (BT-Drucksache 19/2587). Die Beklagte kann und muss also ihre Webserver technisch so abschotten, dass darüber kein Zugriff auf weitere Infrastrukturen erfolgen kann. Dass es geeignete Maßnahmen gibt, ergibt sich aus der vorbenannten Aussage der Beklagten selbst. Auch in der Anlage BB9 heißt es: „Die Netze der einzelnen, über den IVBB verbundenen Behörden sind segmentiert. Der Angreifer hatte daher keine Möglichkeit, sich frei im IVBB zu bewegen.“

II. Angriff auf das Auswärtige Amt

Im Fall des Angriffs auf das Auswärtige Amt, der mutmaßlich von ausländischen Nachrichtendiensten veranlasst wurde („Bundeshack“), macht die Beklagte selbst nicht geltend, dass eine Vorratsspeicherung der Internetnutzung den Angriff hätte verhindern können. Die Schadsoftware ist über die Lernplattform „Ilias“ der Hochschule des Bundes für öffentliche Verwaltung eingeschleust worden. Die Hochschule des Bundes praktiziert eine Vorratsspeicherung der Internetnutzung (samt IP-Adressen), welche den Angriff jedoch nachweislich nicht verhindert hat.

Die Surfprotokollierung war nicht nur ungeeignet zur Abwehr dieses Angriffs. Es standen auch andere und grundrechtsschonendere Mittel zur Abwehr zur Verfügung, die nicht genutzt wurden. Der infizierte Webserver war nicht nach dem Stand der Technik eingerichtet und geschützt. Insbesondere waren völlig veraltete Versionen der Lernsoftware „Ilias“ installiert. Erst am 20. Dezember 2016 wurde die Softwareversion 5.1.16 mitsamt enthaltenen Sicherheitsupdates installiert, die jedoch bereits seit März 2016 verfügbar gewesen war. Im Dezember 2016 wäre bereits die mehrfach weiterentwickelte Softwareversion 5.1.22 aktuell gewesen, die jedoch nicht installiert wurde. Bevor die Beklagte einen Grundrechtseingriff mit einer so massiven Streubreite wie eine Vorratsspeicherung der kompletten Nutzung ihrer Telemedien auch nur in Betracht zieht, hat sie die milderen Mittel zum Schutz ihrer Webserver wie insbesondere die unverzügliche Installation verfügbarer Updates auszuschöpfen.

Die Vorratsspeicherung der Internetnutzung war auch nicht geeignet und erforderlich, um den Angriff zu beenden. Durch einen Angreifer manipulierte bzw. eingebrachte Dateien können bereits durch eine regelmäßige Integritätsprüfung des Systems erkannt werden, ohne dass dazu eine Vorratsspeicherung der Internetnutzung erforderlich ist. Eine Rückverfolgung von IP-Adressen ist auch nicht ausreichend zur Feststellung manipulierter Dateien, weil die Manipulation auch ohne Zugriff von außen durch die Schadsoftware selbst erfolgen kann. Im Übrigen ist eine Rückverfolgung auch bei Anonymisierung der IP-Adressen anhand des verbleibenden Teils der

IP-Adresse und der sonstigen Protokolleinträge (z. B. hinsichtlich des zugreifenden Systems) hinreichend möglich.

Soweit das BSI laut Anlage BB9 nach Feststellung des Angriffs anlassbezogen eine Protokollierung von Zugriffen auf das Netz des Auswärtigen Amts vornahm, um das Vorgehen des ausländischen Dienstes zu beobachten, betraf dies nicht die Nutzer der Telemedien des Bundes (die Steuerung von Schadsoftware ist keine Telemediennutzung) und ist für den vorliegenden Rechtsstreit daher von vornherein unerheblich. Solange nicht Nutzer ihrer Telemedien betroffen sind, darf die Beklagte externe Zugriffe auf ihre internen Netze nach Maßgabe des allgemeinen Datenschutzrechts verarbeiten. Zur Beobachtung ausländischer nachrichtendienstlicher Aktivitäten erlaubt § 15 Abs. 1 TMG allerdings nicht die Verarbeitung von Telemedien-Nutzungsdaten, zumal es bei der bloßen Beobachtung nicht um die Beseitigung der Schadsoftware ging. Die Schadsoftware auf den Rechnern des Auswärtigen Amts konnte ohne Vorratsspeicherung der Telemediennutzung beseitigt werden. Dies ergibt sich schon daraus, dass nach der eigenen Aufstellung der Beklagten das Auswärtige Amt die Nutzung seines Internetportals nicht personenbezogen protokolliert.

III. Verfügbarkeitsangriffe

Soweit die Beklagte gebetsmühlenartig wieder einmal DDoS-Angriffe (im Mai 2018) zur Rechtfertigung ihrer anlass- und wahllosen Surfprotokollierung anführt, ist sie schon unzählige Male darauf hingewiesen worden, dass die Verarbeitung von IP-Adressen zur Beseitigung laufender Verfügbarkeitsangriffe vom Klageantrag ausdrücklich ausgenommen ist. Auch wurde bereits eingehend erläutert, welche milderen Mittel zur Abwehr von Verfügbarkeitsangriffen zur Verfügung stehen. Sollte ein DDoS-Angriff auf ein Telemedium der Beklagten nachteilige Auswirkungen auf andere Telemedien haben, so sind die Systeme der Beklagten (oder der eingesetzten Anbieter) nicht fachgerecht voneinander separiert, was ebenfalls bereits erläutert wurde. Durch Abschottung der einzelnen Angebote können nachteilige Wirkungen des Ausfalls eines Telemediums auf andere Systeme verhindert werden, ohne dass dazu IP-Adressen verarbeitet werden müssten.

Gerade Wordpress Pingpack-Angriffe lassen sich durch einfache Abschaltung der Pingpack-Funktionalität in der Software „Wordpress“ und durch Blockieren von „Pingpack“-Zugriffen im Webserver verhindern, ohne dass dazu Nutzungsdaten gespeichert werden müssten. Entsprechende Anleitungen sind im Internet frei verfügbar. Zur Abwehr von Pingpack-Angriffen ist die Sperrung von IP-Adressen demgegenüber ungeeignet, weil sich Pingpack-Angriffe gerade dadurch auszeichnen, dass sie von einer wechselnden Vielzahl von legitimen Systemen und IP-Adressen aus erfolgen.

Mit Wordpress-Pingpack-Angriffen kann keineswegs „jede beliebige Webseite angegriffen werden“, sondern nur Telemedien, auf denen die Software „Wordpress“ mit eingeschalteter Pingpack-Funktionalität und ohne Blockieren von „Pingpack“-Zugriffen im Webserver läuft. Die wenigsten Telemedien der Beklagten nutzen die Software „Wordpress“. Insbesondere wird bestritten, dass die Software auf den Webseiten *www.bundesregierung.de*, *www.bundeskanzlerin.de* oder *www.bundestag.de* zum Einsatz komme.

Die Vorratsspeicherung von Nutzungsdaten taugt auch nicht zur Rückverfolgung von Angreifern, weil die Quelladressen von DDoS-Angriffen einem Angreifer nicht zuzuordnen sind. Gerade Wordpress Pingpack-Angriffe erfolgen von einer wechselnden Vielzahl von legitimen Systemen und IP-Adressen aus.

Die aktuelle BSI-Empfehlung zur „Prävention von DDoS-Angriffen“ vom 11.07.2018 empfiehlt an technischen Schutzmaßnahmen u. a.:

- Netzwerksegmentierung
- Absicherung der Netzwerkinfrastruktur
- Leistungsgrenzen identifizieren und gezielt Abhilfe schaffen
- Härtung und Konfiguration der Systeme
- Einsatz gezielter DDoS-Abwehrsysteme
- Verlagerung besonders bedrohter Systeme zu Drittanbietern

Es wird bestritten, dass eine anlasslose Vorratsspeicherung von Nutzungsdaten darüber hinaus einen messbar besseren Schutz vor Verfügbarkeitsangriffen biete als die Anwendung der vorbezeichneten Mittel.

Soweit die Beklagte zum Beweis der Erforderlichkeit einer Vorratsspeicherung sämtlicher Nutzungsdaten die Einholung eines Sachverständigengutachtens anbietet, ist dies bereits erfolgt und hat die Beweisfrage verneint. Bei Bedarf mag der Sachverständige zur mündlichen Erläuterung seiner Ausführungen geladen werden.

Zu 1.3 (Gründe für Telemedienangebote ohne Vorratsspeicherung von Nutzungsdaten):

Soweit das Bundesjustizministerium eine Vorratsspeicherung von Nutzungsdaten unterlässt, liegt zwar eine gerichtliche Verurteilung vor. Jedoch hat das Ministerium im Vorprozess selbst eingeräumt, dass es andere Mittel zum Schutz seiner Systeme gibt. Wenn das Bundesjustizministerium nun seit Jahren beanstandungslos und ohne erkennbare Beeinträchtigung seine Telemedien anbietet, widerlegt dies sehr wohl die Behauptung der Beklagten, zum Angebot ihrer Telemedien sei eine Vorratsspeicherung der Internet-Nutzungsdaten des Klägers erforderlich.

Wenn die Beklagte keinen sachlichen Grund dafür nennen kann, warum sie bei einer Vielzahl der von ihr betriebenen Portale auf eine Vorratsspeicherung von Nutzungsdaten verzichtet, ist damit der Annahme des Revisionsgerichts die Grundlage entzogen, dieser Verzicht erfolge „mangels eines ‚Angriffsdrucks‘“ (Abs. 41). Stellt sich der Sachverhalt demzufolge anders dar als vom Bundesgerichtshof zugrunde gelegt, entfällt die Bindungswirkung des Revisionsurteils (BGH NJW-RR 1992, 611; NJW-RR 2017, 1020 Rn. 11). Die noch vom BGH geforderten Feststellungen zum „Gefahrenpotenzial bei den übrigen Online-Mediendiensten des Bundes“ (Abs. 41) erübrigen sich, da die Beklagte nun selbst nicht (mehr) behauptet, dass die speichernden Telemedien ein höheres „Gefahrenpotenzial“ aufwiesen als die nicht speichernden Telemedien. Der Rechtsstreit ist damit entscheidungsreif.

Auf die weiteren Ausführungen der Beklagten zu diesem Punkt braucht deswegen nur in aller Kürze eingegangen zu werden:

- Die Beklagte irrt, wenn sie meint, aus verfassungsrechtlichen Gründen könne keine einheitliche Praxis sämtlicher Behörden vorgeschrieben werden. Vielmehr hat der Bundesgesetzgeber im Wege des Telemediengesetzes einheitlich festgelegt, dass Nutzungsdaten nicht auf Vorrat gespeichert werden dürfen.

- Sollten Telemedienangebote der Beklagten als Einstieg für Angriffe auf weitere IT-Infrastrukturen der Beklagten genutzt werden, so hat die Beklagte versäumt, ihre Telemedien fachgerecht von ihren weiteren Systemen abzuschotten (siehe oben).

- Entschieden bestritten wird, dass Straftäter bei ihren Angriffen Systeme gezielt danach auswählen, ob Nutzungsdaten gespeichert werden und eine Rückverfolgung möglich sei. Straftäter – und erst recht ausländische Dienste – verschleiern ihre IP-Adresse, so dass ihnen eine Protokollierung von Nutzungsdaten gleich ist. Der „Bundeshack“ betraf gerade ein System mit Vorratsspeicherung von Nutzungsdaten.

- Bestritten wird die Behauptung der Beklagten, „gerade wegen“ des Verzichts auf eine Vorratsspeicherung von Nutzungsdaten würden bei diesen Systemen weniger Angriffe beobachtet. Fakt ist, dass Angriffe nicht anhand von IP-Adressen aufgedeckt werden. So ist der „Bundeshack“ durch den Hinweis eines ausländischen Dienstes bekannt geworden.

- Im Fall des „Bundeshacks“ hat nicht ein Hochschulserver die Ausspähung von Daten des Auswärtigen Amts ermöglicht; ermöglicht hat dies die Ausführung von Software von diesem Server durch Mitarbeiter des Auswärtigen Amts.

- Dass die Vorratsspeicherung von Nutzungsdaten zur „Untersuchung und Aufarbeitung“ von „IT-Sicherheitsvorfällen“ geeignet und erforderlich sei, wird bestritten. Der Infektionsweg kann auch anhand anonymisierter Protokolle hinreichend nachvollzogen werden. Manipulierte Daten können durch Integritätsprüfungen ohne Kenntnis von Nutzungsdaten festgestellt werden. Im Übrigen rechtfertigt § 15 Abs. 1 TMG die Verarbeitung personenbezogener Daten für bloße Untersuchungszwecke nicht.

Zu 1.4 (Häufigkeit der Identifizierung und Verfolgung von Straftätern aufgrund von Nutzungsdaten):

Bezüglich dieser Frage wird vorab wiederholt, dass Betreiber von Telemedien Nutzungsdaten legitimerweise einzig zur Bereitstellung ihrer Telemedien verarbeiten dürfen (§ 15 Abs. 1 TMG) und die Identifizierung und strafrechtliche Verfolgung von Straftätern davon nicht abgedeckt ist. Eine unterstellte Nützlichkeit von Nutzungsdaten zur Strafverfolgung (die bestritten wird) rechtfertigte eine Vorratsspeicherung von Telemedien-Nutzungsdaten also nicht. Vielmehr bedürfte zur Rechtfertigung einer Datenspeicherung für den öffentlichen Zweck der Strafverfolgungsvorsorge einer besonderen Rechtsgrundlage (vgl. Art. 6 Abs. 1 S. 1 lit. e) DSGVO), gegen die sich der Bundesgesetzgeber mehrfach ausdrücklich entschieden hat. Zu den

abgelehnten Änderungsentwürfen des Bundesregierung am Telemediengesetz ist bereits vorgetragen worden.

Im Übrigen vermag die Beklagte selbst nicht dartun, dass in einer nennenswerten Zahl von Fällen anhand von Nutzungsdaten tatsächlich Angreifer auf ihre Webserver identifiziert und strafrechtlich verfolgt worden seien. Ihr Vortrag beschränkt sich auf eine bloß hypothetische Nützlichkeit, was einen so massiven Grundrechtseingriff wie eine anlasslose und personenbezogene Vorratsspeicherung des Inhalts der Internetnutzung von vornherein nicht rechtfertigen kann.

Dass die IP-Adresse ein tauglicher Ansatzpunkt zur Identifizierung und Verfolgung von IT-Straftätern sei, wird von der Beklagten nicht dargetan und wird klägerseits bestritten. Wie bereits vorgetragen ist es für jeden ernsthaften Angreifer ein Leichtes, seine Rückverfolgung anhand der angreifenden IP-Adresse zu verhindern, und zwar durch Zwischenschaltung anderer, insbesondere ausländischer Server.

Soweit die Beklagte zum Beweis der Eignung die Einholung eines Sachverständigengutachtens anbietet, ist dies bereits erfolgt und hat die Beweisfrage verneint. Bei Bedarf mag der Sachverständige zur mündlichen Erläuterung seiner Ausführungen geladen werden.

Soweit die Beklagte personenbezogene Nutzungsdaten zur „politischen Bewertung und Zurechnung von Cyber-Angriffen“ protokollieren will, ist dies bereits kein legitimer Zweck für die personenbezogene Aufzeichnung der Telemediennutzung durch den Anbieter (vgl. § 15 Abs. 1 TMG). Dies ergibt sich auch aus dem Revisionsurteil im vorliegenden Fall. Die IP-Adresse eines Angreifers ist zur Zuordnung von Angriffen ohnehin ungeeignet, weil Angreifer IP-Adressen aus beliebigen Ländern nutzen (und vorschieben) können. Die beklagtenseits behaupteten Rekonstruktions- und Zurechnungsmöglichkeiten hinsichtlich IT-Angriffen anhand der eingesetzten IP-Adresse werden bestritten. Im Übrigen ist die Speicherung der vollständigen IP-Adresse zur geografischen Zuordnung auch nicht erforderlich, weil bereits einer anonymisierten IP-Adresse Informationen über das Herkunftsland entnommen werden können. Die Zuordnung der Schadsoftware im Fall des „Bundeshacks“ ist mitnichten anhand einer IP-Adresse erfolgt, sondern unter anderem anhand des Codes der Schadsoftware selbst, der Übereinstimmungen mit anderer Schadsoftware der russischen Hackergruppe aufwies. Die Beklagte nennt als Zurechnungsmittel selbst den „modus operandi, technische Merkmale sowie deren Opferflächen“, wozu IP-Adressen nicht zählen.

Zu 1.5 (Erforderlichkeit weiterer Nutzungsdaten):

Die potenzielle Nützlichkeit anonymisierter Nutzungsdaten wird klägerseits nicht bestritten. In Verbindung mit technischen Schutzmaßnahmen sind anonymisierte Nutzungsdaten auch ausreichend zum Betrieb von Telemedien.

Was den Personenbezug von IP-Adressen anbelangt, verkennt die Beklagte die Bedeutung der Vorabentscheidung des EuGH in ihrer berichtigten Fassung. Dem EuGH zufolge besteht ein Personenbezug bereits deshalb, weil die Beklagte als Telemedienanbieterin die rechtliche Möglichkeit hat, den Kläger als Nutzer des Internetportals im Bedarfsfall an Strafverfolgungsbehörden, Gefahrenabwehrbehörden oder Nachrichtendienste zu melden und

den Kläger von diesen Behörden anhand von IP-Adresse und Zeitstempel identifizieren zu lassen. Die Beklagte verfügt über Strafverfolgungsbehörden, Gefahrenabwehrbehörden und Nachrichtendienste, welche diese Identifikation im Wege der Bestandsdatenauskunft vornehmen können. Insbesondere im Fall (versuchter) Computersabotage etwa durch absichtlich herbeigeführte Serverüberlastungen (Verfügbarkeitsangriffe) kann die Beklagte Polizeibehörden wie das BKA einschalten, damit diese die fraglichen Informationen vom Internetzugangsanbieter anfordern (§ 113 TKG) und die Strafverfolgung einleiten. Die Beklagte begründet ihre Speicherpraxis öffentlich damit, sich diese Möglichkeit offen halten zu wollen (z. B. Datenschutzerklärung des Bundesinnenministeriums). Nach dem Urteil des EuGH ist keine Voraussetzung des Personenbezugs, dass der Telemedienanbieter selbst die Identität seiner Nutzer bestimmen kann.

Zu 1.6 (Erforderliche Speicherdauer):

Da eine personenbezogene Vorratsspeicherung der Internetnutzung schon dem Grunde nach unzulässig ist, geht der Kläger auf die Frage der Speicherdauer nicht ein.

Zu 2.1 (Anwendbarkeit des Telemediengesetzes):

Die pauschale Annahme der Beklagten, die Datenschutz-Grundverordnung entfalte Anwendungsvorrang vor dem Telemediengesetz, geht fehl. Dies hat der Kläger in dem bereits vorgelegten Aufsatz, der zwischenzeitlich in der ZD 2018, 302 veröffentlicht worden ist, im Einzelnen ausgeführt. Die Beklagte verkennt bereits, dass die Datenschutz-Grundverordnung für nationale Vorschriften zur Datenverarbeitung durch öffentliche Stellen eine Öffnungsklausel enthält (Art. 6 Abs. 2 DSGVO, vgl. Breyer, ZD 2018, 302). Die Voraussetzungen eines Anwendungsvorrangs liegen aber auch im privaten Bereich nicht vor, weil die in der Datenschutz-Grundverordnung enthaltenen Begriffe des berechtigten Interesses und des überwiegenden Betroffeneninteresses (Art. 6 Abs. 1 S. 1 lit. f) DSGVO) bezogen auf Telemedien-Nutzungsdaten zu demselben Ergebnis führen wie § 15 TMG. Es fehlt hinsichtlich der Rechtsfolgen an einer Kollision zwischen Telemediengesetz und Europarecht, wenn man § 15 TMG so auslegt wie vom Revisionsgericht entschieden. Die Vereinbarkeit ist im vorliegenden Prozess bereits geklärt worden, zumal Art. 6 DSGVO inhaltlich nicht von der früheren Datenschutzrichtlinie abweicht. Nach Art. 20 Abs. 3 GG ist sowohl die Beklagte als auch die Kammer an Gesetz und Recht gebunden, was den weiterhin in Kraft befindlichen § 15 TMG umfasst.

Sollte die Kammer trotz der bereits vorliegenden EuGH-Entscheidung zur inhaltsgleichen Datenschutzrichtlinie Zweifel an der Vereinbarkeit des § 15 TMG in der Auslegung durch den Bundesgerichtshof mit der Datenschutz-Grundverordnung haben,

wird eine erneute Vorlage an den EuGH beantragt.

Zu 2.2 (Datenschutz-Grundverordnung als Rechtsgrundlage?):

Dass die Anwendung des Art. 6 Abs. 1 S. 1 lit. f) DSGVO zu keinem anderen Ergebnis führen kann als § 15 Abs. 1 TMG, ist bereits ausgeführt worden (vgl. Breyer, ZD 2018, 302). Die Vorschrift ist auf die von Behörden in Erfüllung ihrer Aufgaben angebotenen Telemedien von vornherein nicht anwendbar, wie Art. 6 Abs. 1 S. 2 DSGVO klarstellt. Sämtliche von der Beklagten angebotenen Telemedien werden in Erfüllung ihrer Aufgaben angeboten.

In keinem Fall ist über Art. 6 Abs. 1 S. 1 lit. e) i. V. m. Art. 6 Abs. 3 DSGVO § 3 BDSG anwendbar; vielmehr ist § 15 TMG als lex specialis anzuwenden. Die Datenschutzvorschriften des Telemediengesetzes regeln eindeutig, dass die Verarbeitung von Nutzungsdaten nicht auf Vorschriften außerhalb des Gesetzes gestützt werden kann. Dies folgt aus § 12 Abs. 1 TMG (§ 3 BDSG bezieht sich nicht ausdrücklich auf Telemedien) und aus § 15 Abs. 1 S. 1 TMG („nur“).

Der Erwägungsgrund zu einer Verordnung ist keine taugliche Rechtsgrundlage für Grundrechtseingriffe. Im Übrigen wiederholt Erwägungsgrund 49 DSGVO nur § 15 Abs. 1 TMG und stellt keine Abweichung davon dar. Er spricht insbesondere nicht von einer anlasslosen Vorratsspeicherung der Internetnutzung über die Dauer der Nutzung hinaus, sondern setzt die Prüfung der Eignung, Erforderlichkeit und Verhältnismäßigkeit jeder Verarbeitung personenbezogener Daten voraus.

Zu DDoS-Angriffen ist bereits ausgeführt worden.

Zu 2.3 (BSI-Gesetz als Rechtsgrundlage?):

Soweit die Beklagte nun wieder das BSI-Gesetz als vermeintliche Rechtsgrundlage für ihre Surfprotokollierung aus der Mottenkiste holt, hat die Kammer dieses Argument bereits mit Urteil vom 31.01.2013 verworfen (S. 18 UA) und ist auch das Revisionsgericht zurecht mit keinem Wort darauf eingegangen.

I. Kein Kommunikationsdienst

Die Kammer hat die Bereitstellung von Telemedien mit Urteil vom 31.01.2013 schon nicht als Kommunikationsdienst im Sinne des BSIG eingeordnet.

II. Unanwendbarkeit auf andere Bundesbehörden als das BSI

Ohnehin ermächtigt § 5 BSIG einzig das Bundesamt für Sicherheit in der Informationstechnik zur Verarbeitung von Protokolldaten. Die Beklagte trägt selbst nicht vor, dass das Bundesamt für Sicherheit in der Informationstechnik die beanstandete personenbezogene Vorratsspeicherung der Nutzung der Telemedien der Beklagten vornehme; dies wird vorsorglich mit Nichtwissen bestritten. § 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.

III. Begründetheit der Klage auch bezüglich des BSI

§ 5 BSIG ermächtigt auch 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 (BT-Drs. 16/11967, 12). Dementsprechend bleibt die Klage mit dem Hilfsantrag (vgl. S. 5 des Urteils vom 31.01.2013) selbst auf der Grundlage des Vortrags der Beklagten begründet.

§ 5 Abs. 1 BSIG ermächtigt das BSIG außerdem nur zu einer „unverzüglichen“ Verarbeitung und anschließenden Löschung von Protokolldaten, etwa um laufende Angriffe festzustellen. Die mag anhand einer „ungewöhnlichen Zugriffsmethode“ möglich sein, wie die Beklagte geltend macht. Die vorliegende Klage richtet sich indes 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. § 5 Abs. 2 BSIG erfasst nur den Fall, dass eine automatisierte Echtzeitauswertung von Protokolldaten tatsächliche Anhaltspunkte für Schadprogramme ergibt. Die Telemediennutzung des Klägers ergibt selbstverständlich keine Anhaltspunkte für das Vorliegen eines Schadprogramms.

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, hat das Sachverständigengutachten ergeben. 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.

IV. Mögliche Verfassungswidrigkeit des § 5 BSIG

Sollte § 5 BSIG hingegen nach Auffassung der Kammer 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 (Breyer, RDV 2004, 147; vgl. auch Bundesrat, BR-Drs. 62/09, 10) und von den Gerichten notdürftig einschränkend ausgelegt und angewandt wird (LG Darmstadt, MMR 2006, 330), 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 (Bundesrat, BR-Drs. 62/09 (Beschluss), 6). Nach der Rechtsprechung des Bundesverfassungsgerichts darf eine automatisierte Datenerfassung „nicht anlasslos erfolgen oder flächendeckend durchgeführt werden“ (BVerfG, MMR 2008, 308, 308; BVerfG, NVwZ 2007, 688, 691). Begriffe wie „erforderlich“ oder „sachdienlich“ stellen keine hinreichende Eingrenzung dar (BVerfG, MMR 2007, 93, 94; BVerfG, NVwZ 2007, 688, 691). Das „strikte Verbot der Sammlung personenbezogener Daten auf Vorrat“ ist zu gewährleisten (BVerfG, MMR 2006, 531).

In seiner Stellungnahme vom 06.03.2009 äußerte der Bundesrat dementsprechend „erhebliche Bedenken“, ob der mit § 5 BSIG verbundene Grundrechtseingriff „verfassungsrechtlich zu rechtfertigen ist“ (BR-Drs. 62/09 (Beschluss), 5). 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 (BR-Drs. 62/09 (Beschluss), 5).

Im April 2009 kritisierte auch der Deutsche Anwaltverein, § 5 BSIG fehle es an der verfassungsrechtlich gebotenen Anlassbezogenheit der Überwachung (DAV, Stellungnahme 2009-31 vom April 2009, 3). 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“ (DAV, Stellungnahme 2009-31 vom April 2009, 3).

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 (BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 218). 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 (BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 218). Diese Rechtfertigungsvoraussetzungen erfüllt § 5 BSIG in einer Auslegung als Ermächtigung zur Vorratsdatenspeicherung nicht: Die dort vorgesehene Speicherung erfolgt direkt durch eine staatliche Stelle und umfasst gerade auch die Speicherung jeder aufgerufenen Internetseite. In seiner Entscheidung vom 02.03.2010 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 (BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 270). 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 die Kammer § 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.

V. Mögliche Europarechtswidrigkeit des § 5 BSIG

Sollte die Kammer § 5 BSIG – selbst in möglichst grundrechtskonformer Auslegung – eine Ermächtigung zu einer personenbezogenen Vorratsspeicherung des Internet-Nutzungsverhaltens des Klägers entnehmen, liegt auch ein Verstoß gegen Europarecht vor, nämlich gegen das Grundrecht auf Achtung des Privatlebens (Art. 7 GRCh). Der Anwendungsvorrang des Europarechts führt zur Unanwendbarkeit des § 5 BSIG.

Nach ständiger Rechtsprechung des EuGH verstößt eine anlass- und wahllose Vorratsspeicherung von Telekommunikationsdaten gegen Art. 7 der Grundrechtecharta (EuGH,

Urteil vom 08.04.2014 – C-293/12 und C-594/12; EuGH, Urteil vom 21.12.2016 – C-203/15, C-698/15; vgl. auch OVG Nordrhein-Westfalen, Beschluss vom 22.06.2017 – 13 B 238/17). Erst recht muss die Rechtsprechung des EuGH gelten, wenn eine Speicherung nicht zur Aufdeckung, Aufklärung und Verfolgung schwerer Straftaten erfolgt, sondern zur bloßen Aufdeckung und Aufklärung leichter Straftaten, nämlich des Einbringens von Schadsoftware. Das Einbringen von Schadsoftware kann zwar nach den §§ 202a, 303a StGB strafbar sein, es handelt sich dabei aber nicht um schwere Straftaten, wie sie Gegenstand der Regelungen zur Vorratsspeicherung von Telekommunikationsdaten waren (siehe § 100a und 100g Abs. 2 StPO). Und erst recht muss die Rechtsprechung des EuGH gelten, wenn nicht nur die näheren Umstände einzelner Kommunikationsverbindungen gespeichert werden sollen, sondern sogar die aufgerufenen Internetseiten und damit der Inhalt der Kommunikation.

§ 5 BSIG muss sich an der Grundrechtecharta messen lassen, weil die Vorschrift im Anwendungsbereich des Unionsrechts liegt. Sie hat nämlich die Verarbeitung personenbezogener Daten in Ausübung öffentlicher Gewalt zum Gegenstand (Art. 6 Abs. 1 S. 1 lit. e) DSGVO). Die Rechtsgrundlage für eine solche Datenverarbeitung kann die Beklagte beibehalten (Art. 6 Abs. 2 DSGVO) oder schaffen (Art. 6 Abs. 3 DSGVO), jedoch handelt sie dabei in Durchführung des Unionsrechts und muss dessen Grenzen, insbesondere die Unionsgrundrechte, wahren.

Sollte die Kammer § 5 BSIG eine Ermächtigung zu einer personenbezogenen Vorratsspeicherung des Internet-Nutzungsverhaltens des Klägers entnehmen und an der Unvereinbarkeit des § 5 BSIG mit Art. 7 GRCh zweifeln, wird beantragt,

die Frage dem EuGH zur Vorabentscheidung vorzulegen.

Dieser Antrag gilt auch für den Fall, dass die Kammer dem Telemediengesetz oder der Datenschutz-Grundverordnung eine Ermächtigung zur Vorratsspeicherung von Internetnutzungsdaten entnehmen will; auch dies wäre mit Art. 7 GRCh und der EuGH-Rechtsprechung dazu unvereinbar.

VI. Zur Gesetzesbegründung

Soweit die Beklagte die Gesetzesbegründung zu Art. 5 Abs. 1 BSIG zitiert, richtet sich die vorliegende Klage nicht gegen die Erhebung und Echtzeitauswertung von Kommunikationsdaten durch die Beklagte, sondern nur gegen die nicht-anonymisierte Aufbewahrung von Nutzungsdaten über die Dauer des Nutzungsvorgangs hinaus. Soweit die Gesetzesbegründung auf die Auswertung des Datenvolumens abstellt, genügen dazu anonymisierte Nutzungsprotokolle, ohne dass die vollständige IP-Adresse dazu erforderlich wäre. Soweit ein automatisiertes Absurfen von aus dem Bundesnetz abgerufenen URLs festgestellt werden soll, betrifft dies ohnehin nicht die öffentliche Nutzung von Telemedien.

VII. Zur Anlage BB11

Die Anlage BB11 beweist keineswegs die Eignung und Erforderlichkeit einer Vorratsspeicherung von Nutzungsdaten zur „Angriffsaufklärung“:

- „Angriffsaufklärung“ ist bereits kein legitimer Zweck einer Speicherung von Nutzungsdaten, weil sie nicht die Inanspruchnahme von Telemedien ermöglichen soll (§ 15 Abs. 1 TMG). Legitim ist nur die Abwehr von Störungen, wozu die Vorratsspeicherung von Nutzungsdaten auch in diesem Fall erkennbar nicht geeignet war.
- Das vorgelegte Protokoll beschreibt keinen Angriff, sondern eine Suche nach Schwachstellen. Diese kann der Vorbereitung eines Angriffs gedient haben, aber auch dem legitimen Zweck, Sicherheitslücken aufzudecken (sog. Penetrationstest). Bei fachgerechter Einrichtung des Webservers kann keine der Sicherheitslücken, nach denen gesucht worden ist, bestehen. Eine Protokollierung dieser Suche war also von vornherein nicht nötig.
- Im Übrigen hätte diese Suche selbstverständlich auch ohne vollständige Speicherung der IP-Adresse nachvollzogen werden können, beispielsweise anhand der zeitlichen Abfolge, einer verkürzt (anonymisiert) gespeicherten IP-Adresse oder der ungewöhnlichen URLs. Die IP-Adresse ist zudem untauglich zur Rekonstruktion eines Angriffs, weil ein Angreifer beliebig wechselnde IP-Adressen einsetzen kann.
- Wären Schwachstellen vorhanden gewesen und genutzt worden, wäre die vollständige IP-Adresse (auch pseudonymisiert) nicht erforderlich gewesen, um den Angriff aufzudecken und zu beenden. Dies ist bereits in den früheren Schriftsätzen umfangreich erläutert und vom Sachverständigen auch bestätigt worden, so dass hier keine Wiederholung erfolgen soll.

Zu 3. (Personenbezug):

Das Urteil des EuGH beantwortet – wie auch der Generalanwalt hervorgehoben hat – keineswegs abschließend die Frage des Personenbezugs, sondern nur im Hinblick auf die spezifische Vorlagefrage (genügt es, dass der Zugangsanbieter über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt?). Die Beklagte hat neben Bestandsdatenauskünften des Internet-Zugangsanbieters auch andere realistische Möglichkeiten der Identifizierung eines Nutzers anhand von IP-Adresse und Zeitstempel, darunter vom Nutzer selbst angegebene Daten (z. B. per Formular oder E-Mail) oder die bei anderen Telemedienanbietern (z. B. Google, Facebook, Wikipedia-Bearbeitungshistorie) vorhandenen Daten (vgl. § 15 Abs. 5 S. 3 TMG, § 8a BVerfSchG).

4. Zusammenfassung

Zusammenfassend ist festzuhalten:

1. Die Beklagte vermag die Eignung und Erforderlichkeit einer personenbezogenen Vorratsspeicherung von Telemedien-Nutzungsdaten zur Bereitstellung funktionsfähiger Telemedien schon deswegen nicht zu beweisen, weil sie selbst eine Vielzahl von Telemedien ohne eine solche Vorratsdatenspeicherung funktionsfähig bereitstellt.

2. Die Beklagte macht selbst nicht (mehr) geltend, diese Telemedien seien einem geringeren „Angriffsdruck“ oder „Gefahrenpotenzial“ ausgesetzt als die Telemedien mit Vorratsspeicherung von Telemedien-Nutzungsdaten.

3. Vor diesem Hintergrund erübrigt es sich, diesen Fragen weiter nachzugehen und Feststellungen zum „Gefahrenpotenzial“ zu treffen. Das Revisionsurteil entfaltet insoweit keine Bindungswirkung mehr.

4. Eine weitere Beweiserhebung zu der beklagtenseits behaupteten Eignung und Erforderlichkeit ihrer Datenverarbeitung erübrigt sich, weil bereits ein Sachverständigengutachten dazu eingeholt worden ist und die Beklagte beweisfällig geblieben ist. Die Beklagte beantragt auch nicht die Ladung des gerichtlich bestellten Sachverständigen zur Erläuterung seines Gutachtens.

5. Eine Beweiserhebung zu der beklagtenseits behaupteten Eignung und Erforderlichkeit ihrer Datenverarbeitung erübrigt sich vor allem aus rechtlichen Gründen, weil eine Vorratsspeicherung von Telemedien-Nutzungsdaten unabhängig von ihrer behaupteten Nützlichkeit mit den Grundrechten der betroffenen Internetnutzer unvereinbar wäre, deren Grundrechte also etwaige Speicherinteressen überwiegen.

6. Eine Eignung der Protokollierung zur Strafverfolgung vermag die Beklagte nicht darzutun. Es fehlt aber ohnehin an einer Rechtsgrundlage zur Vorratsspeicherung von Telemedien-Nutzungsdaten zur Strafverfolgungsvorsorge.

Mit freundlichem Gruß

Jonas Breyer
(Rechtsanwalt)