BREYER LEGAL
RECHTSANWALTSKANZLEI

BREYER LEGAL • Klagenfurter Ring 2FA • 65187 Wiesbaden

Landgericht Berlin II
– 60 S 10/25 –
Littenstraße 12–17
10179 Berlin

Jonas Breyer
Rechtsanwalt
Zert. Datenschutz-beauftragter (FFD)

Felicia Früchtenicht
Rechtsanwältin
Freie Mitarbeiterin

14.04.2025

Klagenfurter Ring 2FA
65187 Wiesbaden
T +49 611 141 056 89
F +49 611 141 056 90

Mainzer Landstraße 69
60329 Frankfurt am Main
T +49 69 247 422 39
F +49 69 247 422 40

jbreyer@kanzlei-breyer.de
www.kanzlei-breyer.de

60 S 10/25

Az.: IP-Speicherung

Sehr geehrte Damen und Herren,

In dem Verfahren

Breyer ./. BRD

danken wir für die Fristverlängerung und nehmen zum Gutachten wie folgt Stellung.

I. Sachverhalt: aktuelle Speicherpraxis der Beklagten

Ausweislich der Datenschutzerklärungen werden aktuell mindestens folgende Telemedien der Beklagten **ohne Vorratsspeicherung/ Protokollierung der IP-Adressen** der Nutzer über die Dauer des Nutzungsvorgangs hinaus angeboten:

- Bundesrat (Bundesrat.de)
- Bundesdatenschutzbeauftragte (bfdi.bund.de)
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (bbk.bund.de), Aufsicht: Bundesinnenministerium
- Bundesjustizamt (bundesjustizamt.de)
- Paul-Ehrlich-Institut (pei.de)

Ausweislich der Datenschutzerklärungen werden aktuell mindestens folgende Telemedien der Beklagten **ohne Vorratsspeicherung/ Protokollierung der vollständigen IP-Adressen** der Nutzer über die Dauer des Nutzungsvorgangs hinaus angeboten, also mit nur anonymisierter, nicht personenbezogener Protokollierung des Nutzungsverhaltens:

- Wahlorgan: Bundeswahlleiterin (bundeswahlleiterin.de)
- Oberste Bundesbehörden:
  - Auswärtiges Amt (auswaertiges-amt.de)
  - Bundesministerium für Digitales und Verkehr (bmdv.bund.de)
  - Bundesrechnungshof (brh.de), wobei das Telemedium vom Informationstechnologiezentrum (ITZ) Bund bereitgestellt wird
  - Kulturstaatsministerin (kulturstaatsministerin.de)
  - Bundesbank (bundesbank.de)
  - Bundesgerichtshof (bundesgerichtshof.de)
  - Bundesfinanzhof (bundesfinanzhof.de)
  - Bundessozialgericht (bsg.bund.de)
- Nachgeordnete Bundesbehörden:
  - Bundesamt für Flugsicherung (baf.bund.de)
  - Bundesamt für Verbraucherschutz und Lebensmittelsicherheit (bvl.bund.de)
  - Bundesamt für zentrale Dienste und offene Vermögensfragen (badv.bund.de), Aufsicht: Bundesinnenministerium
  - Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (bdbos.bund.de), Aufsicht: Bundesinnenministerium
  - Bundesanstalt für Risikobewertung (bfr.bund.de)
  - Bundesinstitut für Arzneimittel und Medizinprodukte (bfarm.de)

- Bundesinstitut für Bevölkerungsforschung (bib.bund.de), Aufsicht: Bundesinnenministerium
- Bundesinstitut für öffentliche Gesundheit (bioeg.de)
- Bundesnetzagentur (bundesnetzagentur.de)
- Bundeszentrale für politische Bildung (bpb.de), Aufsicht: Bundesinnenministerium
- Luftfahrtbundesamt (lba.de)
- Technisches Hilfswerk (thw.de), Aufsicht: Bundesinnenministerium

Es sind nicht alle Telemedien ausgewertet worden, so dass es sich nur im Beispiele handelt.

Aus der aktuellen Liste ergibt sich, dass die Speicherpraxis nicht einmal im Geschäftsbereich des Bundesinnenministeriums einheitlich ist. Auch das zentrale Informationstechnologiezentrum (ITZ) des Bundes scheint in der Lage zu sein, Telemedien ohne Vorratsspeicherung des Nutzungsverhaltens anzubieten (siehe z. B. Bundesrechnungshof).

Außerdem zeigt sich, dass auch im Bereich kritischer Infrastruktur (z. B. Bundeswahlleiterin, Auswärtiges Amt, Bundesbank, Bundesgerichtshof, Bundesamt für Bevölkerungsschutz, Bundesamt für Flugsicherung, Bundesnetzagentur, Luftfahrbundesamt, Technisches Hilfswerk) vielfach eine Bereitstellung der Telemedien ohne personenbezogene Surfprotokollierung erfolgt. Das „Schadenspotenzial" ist also offensichtlich nicht maßgeblich für die willkürliche Speicherpraxis der Beklagten. Auch bei hohem Schadenspotenzial ist eine anlasslose Surfprotokollierung verzichtbar.

Das Internetportal speziell des Bundeswahlleiters war im Vorfeld der Bundestagswahl 2021 von einem Verfügbarkeitsangriff (DDoS-Angriff) betroffen und nur eingeschränkt erreichbar, der jedoch nach wenigen Minuten neutralisiert wurde. Der Bundeswahlleiter betonte, dass wahlbezogene IT-Systeme nicht betroffen waren und in separaten Netzen betrieben werden (Netzwerksegmentierung). IP-Adressen der Nutzer von *bundeswahlleiterin.de* werden ungeachtet des Angriffs nach wie vor nur anonymisiert gespeichert.

Eine dritte Gruppe von Telemedien der Beklagten speichert die **vollständige IP-Adresse des Nutzers über die Dauer des**

Nutzungsvorgangs hinaus nur aus besonderem Anlass. Beispielsweise führt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seiner Datenschutzerklärung aus:

> *„Die automatisierte Auswertung der Protokolldaten erfolgt unverzüglich, die Daten werden nach erfolgtem Abgleich sofort und spurenlos gelöscht. Soweit tatsächliche Anhaltspunkte bestehen, dass die Protokolldaten für den Fall der Bestätigung eines Verdachts nach § 5 Abs. 3 S. 2 BSIG zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich sein können, werden diese längstens für 18 Monate gespeichert, § 5 Abs. 2 S. 1 BSIG."*

Auch eine derartige Praxis steht der antragsgemäßen Verurteilung der Beklagten nicht entgegen: Der Kläger verlangt Unterlassung der personenbezogenen Protokollierung seiner eigenen Internetnutzung über die Dauer des Nutzungsvorgangs hinaus. Der Kläger nutzt die Telemedien der Beklagten ausschließlich rechtmäßig und regulär zur Recherche, mitunter zur Absendung von Formularen wie Broschürenbestellungen, ohne dass Schadprogramme aktiv wären oder der Kläger gar irgendwelche Angriffe vornehmen würde. Aus dem Nutzungsverhalten des Klägers ergeben sich insofern keinerlei Auffälligkeiten oder sonstige Anhaltspunkte für Verletzungen der IT-Sicherheit, die nach der beschriebenen Praxis des BSI zu einer Protokollierung führen würden.

Eine vierte Gruppe von Telemedien der Beklagten, beispielsweise das Internetportal des Bundesinnenministeriums, speichert die **vollständige IP-Adresse sämtlicher Nutzer über die Dauer des Nutzungsvorgangs hinaus auf Vorrat ohne jeden Anlass**, erfasst also das Nutzungsverhalten aller Bürger ins Blaue hinein. Dagegen richtet sich die Klage.

II. Aktuelle Rechtslage

Nach weiteren Gesetzesänderungen gibt es im deutschen Recht nunmehr keine spezielle Regelung zur Verarbeitung von Telemedien-Nutzungsdaten mehr. Die Beklagte darf die IP-Adresse des Klägers daher nur nach Maßgabe von Art. 6 Abs. 1 der Datenschutz-Grundverordnung (DSGVO) verarbeiten.

Art. 6 Abs. 1 S. 1 Buchst. f) DSGVO (berechtigtes Interesse) ist nach Art. 6 Abs. 1 S. 2 DSGVO nicht anwendbar. Die Bereitstellung ihrer Telemedien

gehört zu den öffentlichen Aufgaben der Behörden der Beklagten (Öffentlichkeitsarbeit), und die IP-Adressen der Nutzer der Telemedien werden von den Behörden in Erfüllung dieser öffentlichen Aufgabe verarbeitet. Sollte die Kammer Zweifel hieran haben, wird

Vorlage an den Europäischen Gerichtshof

beantragt.

In Betracht kommt folglich nur Art. 6 Abs. 1 S. 1 Buchst. e) DSGVO (Wahrnehmung öffentlicher Aufgaben). Es handelt sich dabei allerdings nur um eine Öffnungsklausel, nicht um eine Rechtsgrundlage. Art. 6 Abs. 3 S. 1 DSGVO fordert eine besondere unionsrechtliche oder nationale Rechtsgrundlage für die Datenverarbeitung durch öffentliche Stellen.

Erwägungsgrund 47 Satz 5 DSGVO; BVerwG, 7 C 5/17 vom 27.09.2018, Abs. 25; Simitis/Hornung/Spiecker, Datenschutzrecht, DSGVO Art. 6 Abs. 3 Rn. 14, beck-online unter Verweis auf EuGH, 30.03.2023 – C-43/21, Abs. 87; EuGH, 04.07.2023 – C-252/21, Abs. 128.

Eine Rechtsgrundlage für die Surfprotokollierung durch die Beklagte wie von Art. 6 Abs. 3 S. 1 DSGVO gefordert besteht nicht.

Dass das BSIG bereits nicht einschlägig ist, hat die Kammer selbst ausgesprochen.

Urteil vom 31.01.2013, S. 18-19.

Im Übrigen wird auf die umfassenden Ausführungen dazu mit Schriftsatz vom 17.08.2018, S. 9 ff., Bezug genommen. Oben zum Sachverhalt ist auch bereits ausgeführt worden, dass die im BSIG geregelte Datenverarbeitung die beklagtenseits teilweise praktizierte wahllose Surfprotokollierung auf Vorrat nicht abdeckt.

Vorschriften, die sich gar nicht auf öffentliche Stellen beziehen, kommen von vornherein nicht als Rechtsgrundlage für die Beklagte in Betracht. Art. 6 Abs. 1 S. 2 DSGVO zeigt, dass Regelungen zur Datenverarbeitung durch Private im öffentlichen Bereich nicht ausreichen sollten.

Es bleibt danach nur die Generalklausel des § 3 BDSG. Diese ist allerdings unionsrechtswidrig und nicht anwendbar, weil sie gegen Art. 6 Abs. 3 DSGVO verstößt

Paal/Pauly–Frenzel, § 3 BDSG, Rn. 1 f.; Sydow/Marsch–Reimer, § 3 BDSG, Rn. 18 f.; Reimer, Verwaltungsdatenschutzrecht, Rn. 165 – beck online). Während die DSGVO besondere Rechtsgrundlagen für die Datenverarbeitung durch öffentliche Stellen fordert (vgl. Erwägungsgrund 47 Satz 5 DSGVO

und insbesondere Art. 6 Abs. 1 S. 1 Buchst. e DSGVO eine Definition der öffentlichen Aufgaben fordert. Hingegen wiederholt § 3 BDSG im Grunde Art. 6 Abs. 1 S. 1 Buchst. e DSGVO, jedoch ohne besondere Rechtsgrundlagen zu fordern und ohne konkrete Aufgaben zu definieren. Das Bundesverwaltungsgericht hat entschieden, das DSGVO–Erfordernis einer gesonderten Ermächtigungsgrundlage „kann nicht durch einen umfassenden Auffangtatbestand überspielt werden"

BVerwG, 7 C 5/17 vom 27.09.2018, Abs. 26.

Sollte die Kammer Zweifel an der Unionsrechtswidrigkeit haben, wird

Vorlage an den Europäischen Gerichtshof

beantragt.

Selbst die Stimmen, die § 3 BDSG für unionsrechtskonform halten, wollen ihn wegen seiner Unbestimmtheit nur auf Eingriffe von geringer Intensität anwenden.

Bundesregierung in BT–Drs. 18/11325, 81, ebenso Gola/Heckmann–Starnecker, § 3 BDSG, Rn. 13; Simitis/Hornung/Spiecker–Roßnagel, § 3 BDSG, Rn. 2.

Aus den speziellen BDSG–Regelungen zu Videoüberwachung (§ 4 BDSG), zu Forschungs– und Statistikzwecken (§ 27 und 50 BDSG), zu staatlichen Auszeichnungen und Ehrungen (§ 86 BDSG) ergibt sich, dass der Gesetzgeber diesen Zwecken eine mehr als „geringe" Intensität zugemessen hat. Während die technisch notwendige Verarbeitung einer IP–Adresse zur Bereitstellung eines Telemediums noch als geringfügiger Eingriff gewertet werden kann, ist die personenbezogene Aufzeichnung des Internet–Nutzungsverhaltens offensichtlich ein schwerer Grundrechtseingriff – nicht zu vergleichen etwa mit der Verleihung staatlicher Auszeichnungen. § 3 BDSG kommt daher als Rechtsgrundlage dafür nicht in Betracht, auch wenn man ihn für unionsrechtskonform hielte.

In Ermangelung einer Rechtsgrundlage für die Vorratsspeicherung von Nutzungsdaten durch die Beklagte ist die Klage somit begründet und

hat sich die Beweisaufnahme, die auf die zwischenzeitlich außer Kraft getretene Erlaubnisnorm des § 15 Telemediengesetz gestützt war, erübrigt. Durch diese Rechtsänderung ist auch das Revisionsurteil des BGH zu § 15 TMG a.F. obsolet geworden.

Nur hilfsweise sei daher noch § 19 Abs. 2 S. 1 TDDDG angeführt, der keine Rechtsgrundlage darstellt, jedoch zusätzlich eine besondere Pflicht zur Ermöglichung der anonymen Dienstenutzung begründet, soweit dies technisch möglich und zumutbar ist. Die Vorschrift ist eine Konkretisierung des allgemeinen Verhältnismäßigkeitsgebots angesichts der besonderen Schutzwürdigkeit des Inhalts unserer Internetnutzung, die weit reichende Einblicke in unsere Persönlichkeit einschließlich unserer Gesundheit und unseres Sexuallebens, unserer Religion und unserer politischen Überzeugungen ermöglicht.

Dass es der Beklagten zumutbar ist, ihre Telemedien ohne personenbezogene Vorratsspeicherung der Internetnutzung anzubieten, folgt schon aus ihrer aktuellen vielfachen und langjährigen Praxis, einschließlich diverser Telemedien im Bereich kritischer Infrastruktur (siehe Darstellung der Speicherpraxis oben).

III. Auseinandersetzung mit dem Sachverständigengutachten, Einwendungen und Ergänzungsfragen

Sollte die Kammer die Beweisaufnahme trotz der nunmehr fehlenden Rechtsgrundlage für die Datenverarbeitung der Beklagten für erheblich halten, wird vorsorglich wie folgt zu dem schriftlichen Gutachten Stellung genommen:

Zu „Angriffsanalysen und die Rolle der IP-Adresse an zwei Beispielen"

Zu diesen Ausführungen im Gutachten sei angemerkt: In beiden geschilderten Beispielsfällen standen mildere Mittel zur Verfügung. Im ersten (fiktiven) Fall hatte die angegriffene Einrichtung ein unsicheres Plugin selbst programmiert. Die Beklagte kann zur Bereitstellung ihrer Telemedien darauf verzichten, eigenen Code zu programmieren. Im zweiten Beispielsfall berichtet der Sachverständige von „nicht aktualisierten Plugins". Man hätte die Installation also einfach auf dem aktuellen Stand halten müssen, um den Angriff zu verhindern, was auch automatisiert ohne menschliche Intervention möglich ist. Dazu brauchte es keine Protokollierung von IP-Adressen. Es fehlen auch Ausführungen dazu,

ob nicht auch eine anonymisiert gespeicherte IP-Adresse als Kompromittierungsindikator gereicht hätte. Auch fehlen Ausführungen, ob die Technik den Angriff anhand der Mustererkennung identifiziert hat und man auf dieser Grundlage eine gezielte anlassbezogene Speicherung hätte vornehmen können statt unterschiedslos alles auf Vorrat zu speichern.

Nachfrage an den Sachverständigen:

Wie häufig (in Prozent) genügt eine anonymisierte IP-Adresse als Kompromittierungsindikator? Wie häufig gelingt die Verkettung etwa anhand der restlichen IP-Adresse, der Browseridentifikation oder/oder anhand der URLs, auf die zugegriffen wurde?

Legitimer Zweck und Geeignetheit (zur Beweisfrage 1a)

Der Sachverständige hält in Beantwortung der Beweisfrage 1a eine Vorratsspeicherung von Nutzungsdaten für geeignet, um verschiedene Zwecke zu erreichen. Dabei orientiert er sich – ebenso wie der Beweisbeschluss – weder an gesetzlich festgelegten Zwecken noch an der vom Bundesgerichtshof nach früherem Recht für legitim gehaltenen Zweck der Gewährleistung der generellen Nutzbarkeit eines Telemediums.

Der erste im Gutachten angeführte Zweck (Ermittlung von Angriffsstrategien, Untersuchung von Angriffen) ist allerdings für sich genommen nicht als legitim anzuerkennen. Mit bloßen Ermittlungen und Untersuchungen ist für die Nutzbarkeit eines Telemediums noch nichts erreicht.

Die vom Sachverständigen unter Ziff. 2 und 3 genannten Zwecke (Schließung von Schwachstellen in der Backend-Infrastruktur und Blockierung von IP-Adressen) verfolgen die Zielrichtung der Gewährleistung der Nutzbarkeit von Telemedien. Jedoch wird noch auszuführen sein, dass es zur Schließung von Schwachstellen mildere Mittel gibt. Und die Blockierung von IP-Adressen ist in der Praxis unwirksam, weil ernsthafte Angreifer regelmäßig unschwer auf andere IP-Adresse oder IP-Adressblöcke ausweichen können.

Nachfragen an den Sachverständigen:

Wie effektiv ist die Blockierung von IP-Adressen oder IP-Adressblöcken angesichts der Tatsache, dass Angreifer die Blockade

feststellen und regelmäßig unschwer auf andere IP-Adressen ausweichen können?

Angesichts der Möglichkeiten zur Blockierung von IP-Adressen ohne selbst eine Protokollierung von IP-Adressen vorzunehmen (Verwendung automatisierter Schutzverfahren gegen Angriffe, Verwendung externer Blacklists): Hat die händische Blockierung von IP-Adressen anhand eigener Zugriffsprotokolle eine statistisch signifikante Verringerung der IT-Sicherheitsverletzungen bei öffentlich zugänglichen Telemedien zur Folge? Gibt es dazu wissenschaftliche oder sonst statistisch belastbare Erkenntnisse?

Ergänzend wird darauf hingewiesen: Wenn im Angriffsfall die Protokollierung und Sperrung von IP-Adressen erforderlich ist, um die Verfügbarkeit eines Telemediums sicherzustellen (z. B. DDoS-Überlastungsangriff), so lässt der Klageantrag dies ausdrücklich zu.

Der vierte angegebene Zweck (Unterstützung forensischer Analysen z.B. zur Unschädlichmachung von Botnetzen) ist wiederum nicht als legitim anzuerkennen. Mit bloßen Analysen ist für die Nutzbarkeit eines Telemediums noch nichts erreicht. Und die Unschädlichmachung von Botnetzen erfolgt in der Praxis auf andere, gezieltere Weise. Dazu schreibt das Bundesamt für Sicherheit in der Informationstechnik (https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Fragen-und-Antworten/fragen-und-antworten_node.html):

„Ein gängiges Verfahren zur Identifikation mit Schadprogrammen infizierter Systeme ist die Umleitung von Steuerungsdomänennamen auf sogenannte ‚Sinkholes'. Dabei werden die durch Analyse von Schadprogrammen ermittelten Domainnamen, mit denen die Schadprogramme kommunizieren, in Zusammenarbeit mit den zuständigen Domain-Registrierungsstellen auf Sinkhole-Server umgeleitet. Die Sinkholes protokollieren anschließend die Zugriffe auf die schädlichen Domainnamen mit Zeitstempel und der Quell-IP-Adresse sowie Quell-Port, von welcher der Zugriff erfolgte. Solche Sinkholes werden von zahlreichen Analysten und IT-Sicherheitsdienstleistern weltweit betrieben."

Nachfragen an den Sachverständigen:

Können Sie bestätigen, dass die Unschädlichmachung von Botnetzen in der Praxis im Wesentlichen durch Umleitung von Steuerungsdomänennamen auf sogenannte ‚Sinkholes' erfolgt und dazu eine Protokollierung von IP-Adressen der Nutzer von (legitimen) Telemedien nicht erforderlich ist?

Ist die Nutzung von Sinkholes effektiver, weil sie auch ohne Nutzung des Botnetzes für Angriffe (sozusagen im „Leerlauf") funktioniert?

Leistet eine unterschiedslose Protokollierung der IP-Adressen sämtlicher Nutzer von Telemedien einen statistisch signifikanten Beitrag zur Unschädlichmachung von Botnetzen? Gibt es dazu wissenschaftliche oder sonst statistisch belastbare Erkenntnisse?

Das BSI-Gesetz geht davon aus, dass sich Zugriffe von Schadprogrammen (einschließlich Botnetzen) bzw. tatsächliche Anhaltspunkte für solche Zugriffe automatisiert identifizieren lassen und in Abwesenheit solcher Anhaltspunkte – bei legitimen, unauffälligen Nutzungsvorgängen – eine sofortige Löschung der IP-Adresse erfolgen kann. Können Sie bestätigen, dass dies technisch möglich ist?

Der fünfte angeführte Zweck (Identifikation der Quelle einer Attacke) ist wiederum für sich genommen nicht als legitim anzuerkennen. Mit einer bloßen Identifikation der Region oder des Netzwerks, aus denen ein Angriff erfolgt, ist für die Nutzbarkeit eines Telemediums noch nichts erreicht. Für Angreifer ist die verwendete IP-Adresse ohnehin frei wechselbar.

Nötige Daten (Beweisfrage 1e)

Um die vom Sachverständigen aufgeführten Zwecke zu erreichen, müssten laut Gutachten zu jeder Anfrage neben der IP-Adresse eine Vielzahl weiterer Log-Daten gespeichert werden. Tatsächlich erfolgt dies seitens der Beklagten jedoch nicht. Schon alleine deshalb taugt die Protokollierungspraxis der Beklagten nicht zur Zweckerreichung (insbesondere Ermittlung von Angriffsstrategien und Aufdeckung von Schwachstellen), selbst wenn man das Gutachten zugrunde legt.

In der Datenschutzerklärung zum Internetportal der Bundesinnenministers heißt es beispielsweise, zu jeder Anfrage würden Zeitstempel und IP-

Adresse, Protokollversion, HTTP-Methode, Referrer- User-String, angefragte URL inkl. Query-String, Größe in Byte und HTTP Status Code gespeichert. Danach fehlt z. B. aus der Auflistung des vom Sachverständigen für erforderlich gehaltenen Speicherumfangs:

- Portnummer oder verwendete Netzwerkprotokolle
- Signatur oder Regel-ID
- Schweregrad
- Zieladresse und Zielport
- Exploit-Indikatoren
- Zielkomponente der Angriffe (z.B. Datenbankserver, Webserver, CMS-Plugins)
- Kompletter Netzwerkverkehr

Es wird bestritten, dass die Beklagte diese Datentypen zu Zugriffen auf ihre Telemedien – egal welche – speichert.

Erforderlichkeit, mildere Mittel (zu Beweisfragen 2a und b)

Der Sachverständige bestätigt auf Seite 19 seines Gutachtens zutreffend, dass eine Kombination technischer IT-Sicherheitsvorkehrungen auch ohne wahllose Surfprotokollierung die Sicherheit „auf ein hohes Niveau bringen" können. Zutreffend ist zwar sein weiterer Hinweis, dass ein vollständiger, 100-prozentiger Schutz nicht zu erreichen ist. Jedoch bietet selbstverständlich auch eine flächendeckende Protokollierung des Nutzungsverhaltens keinen vollständigen, 100-prozentigen Schutz vor Verletzungen der IT-Sicherheit. Mehr als ein hohes Schutzniveau ist technisch nicht zu erreichen. Da die Beklagte auch ohne wahllose Surfprotokollierung ein hohes Sicherheitsniveau erreichen kann, ist es ihr zumutbar, ihre Telemedien anonym nutzbar bereitzustellen und ohne flächendeckende Aufzeichnung des Nutzungsverhaltens anzubieten, § 19 Abs. 2 S. 1 TDDDG.

> <u>Nachfragen an den Sachverständigen:</u>
>
> Ist es richtig, dass auch eine flächendeckende Protokollierung des Nutzungsverhaltens keinen vollständigen, 100-prozentigen Schutz vor Verletzungen der IT-Sicherheit bietet?

Sie schreiben, dass eine Kombination technischer IT-Sicherheitsvorkehrungen auch ohne wahllose vollständige Protokollierung von IP-Adressen die Sicherheit „auf ein hohes Niveau bringen" kann. Können Sie bestätigen, dass Sie dabei keine Maßnahmen betrachtet haben, die mit unzumutbaren Kosten verbunden wären?

Im Vergleich zu einer Backend-Infrastruktur, die dementsprechend auf hohem Schutzniveau abgesichert ist (jedoch ohne IP-Protokollierung), hat die zusätzliche unverkürzte Speicherung sämtlicher IP-Adressen der Telemediennutzer eine statistisch signifikante Verringerung der Zahl der IT-Sicherheitsverletzungen zur Folge? Um wie viel Prozent? Gibt es dazu wissenschaftliche oder sonst statistisch belastbare Erkenntnisse?

Teilen Sie die Meinung des Sachverständigen Dr. Köpsell, die diversen alternativ möglichen IT-Sicherheitsvorkehrungen seien (für sich genommen oder in Kombination) „wesentlich effektiver" als eine Protokollierung von IP-Adressen?

Der Sachverständige betrachtet nicht alle in Betracht kommende mildere Mittel. So nimmt die Beklagte bei vielen Telemedien nur eine um ein oder zwei Byte verkürzte und dadurch anonymisierte Speicherung der IP-Adresse vor, was sich von einer Pseudonymisierung der gesamten IP-Adresse unterscheidet und Korrelationen erleichtert. Bei anderen Telemedien nimmt die Beklagte eine Speicherung der IP-Adresse nur anlassbezogen vor, wenn tatsächliche Anhaltspunkte für einen Angriff vorliegen, und vollzieht andernfalls eine sofortige Löschung.

Nachfragen an den Sachverständigen:

Im Vergleich zu einer nur eine um ein oder zwei Byte verkürzten Speicherung der IP-Adresse der Telemediennutzer, hat die unverkürzte Speicherung sämtlicher IP-Adressen der Telemediennutzer eine statistisch signifikante Verringerung der Zahl der IT-Sicherheitsverletzungen zur Folge? Um wie viel Prozent? Gibt es dazu wissenschaftliche oder sonst statistisch belastbare Erkenntnisse?

Im Vergleich zu einer Speicherung der IP-Adresse eines Telemediennutzers nur dann, wenn die automatisierte Analyse tatsächliche Anhaltspunkte ergibt, dass die IP-Adresse zum Schutz der IT-Sicherheit benötigt wird: Hat die unterschieds- und anlasslose

Speicherung sämtlicher IP-Adressen der Telemediennutzer eine statistisch signifikante Verringerung der Zahl der IT-Sicherheitsverletzungen zur Folge? Um wie viel Prozent? Gibt es dazu wissenschaftliche oder sonst statistisch belastbare Erkenntnisse?

Ferner erwähnt der Sachverständige an anderer Stelle seines Gutachtens als milderes Mittel, dass ein Telemedium auf schnelle Wiederherstellbarkeit ausgelegt werden und sich eine Angriffsanalyse dadurch erübrigen kann.

Nachfrage an den Sachverständigen:

Sind Ihnen Hindernisse bekannt, derentwegen die Beklagte nicht alle ihre öffentlich zugänglichen Telemedien auf schnelle Wiederherstellbarkeit auslegen könnte?

Der Sachverständige berichtet zum milderen Mittel regelmäßig aktualisierter Software, dass Schwachstellen etwa in Plugins häufig gleichwohl verblieben. Nun setzt die Beklagte standardmäßig aber kein Standard-Content-Management-System wie Wordpress ein, sondern regelmäßig ein eigenes mit Blick auf die Sicherheit entwickeltes Content-Management-System namens „Government Site Builder". Damit erübrigen sich die Probleme, die in der Praxis verbreitet im Zusammenhang mit Schwachstellen in Wordpress-Plugins auftreten. Wo die Beklagte den „Government Site Builder" noch nicht einsetzen mag, ist sein Einsatz jedenfalls ein zumutbares milderes Mittel im Vergleich zu einer Vorratsspeicherung des kompletten Nutzungsverhaltens.

Nachfrage an den Sachverständigen:

Sind Ihnen frühere oder aktuelle Schwachstellen im Content-Management-System „Government Site Builder" der Beklagten bekannt, die sich durch regelmäßige Aktualisierung nicht vermeiden ließen?

Telemedien der Beklagten, die ohne IP-Protokollierung bereit gestellt werden (Beweisfrage 3a)

Warum die Beklagte eine Vielzahl von Telemedien seit Jahren problemlos ohne Vorratsspeicherung des Nutzungsverhaltens bereit stellt, einschließlich Telemedien im Bereich kritischer Infrastruktur, vermag der Sachverständige nicht zu erklären. Er nennt zwar mögliche Gründe. Letztlich bleibt es aber schlicht bei der Erklärung der Beklagten, dass

intern unterschiedliche Stellen für die Bereitstellung der Telemedien zuständig sind und unterschiedlich entscheiden – und zwar ohne dass die unterschiedliche Praxis durch Unterschiede in der Sache begründet ist. Im Schriftsatz vom 10.08.2018 der Beklagten heißt es dementsprechend wörtlich zu der unterschiedlichen Praxis:

> „Nachvollziehbare Gründe hierfür sind nicht erkennbar."

Damit beweist die tatsächliche, bewährte Praxis der Beklagten, dass ihr die Bereitstellung von Telemedien auch ohne anlasslose Vorratsspeicherung der Nutzungsverhaltens möglich ist.

> Nachfrage an den Sachverständigen:
>
> Wenn Sie die Liste der öffentlich zugänglichen Telemedien eingangs dieses Schriftsatzes lesen, welche die Beklagte ohne IP-Protokollierung bereit stellt, erkennen Sie sachliche Unterschiede im Vergleich zu den übrigen öffentlich zugänglichen Telemedien der Beklagten, die im Fall der übrigen Telemedien eine IP-Protokollierung erfordern würden?

Werde der Schutzbedarf eines Telemediums (basierend auf möglichen Schäden) als normal eingestuft, könne die Speicherung vollständiger nicht-anonymisierter IP-Adressen dem Sachverständigen zufolge im Einzelfall überflüssig sein.

> Nachfrage an den Sachverständigen:
>
> Wenn Sie die Liste der öffentlich zugänglichen Telemedien eingangs dieses Schriftsatzes lesen, welche die Beklagte ohne IP-Protokollierung bereit stellt, erkennen Sie einen geringeren Schutzbedarf (basierend auf möglichen Schäden), einen geringeren Angriffsdruck oder ein geringeres Gefahrenpotenzial im Vergleich zu den übrigen öffentlich zugänglichen Telemedien der Beklagten, die eine IP-Protokollierung vornehmen?

Folgte man dem Sachverständigengutachten, läge es an der Beklagten nachzuweisen, dass der Schutzbedarf ihrer Telemedien höher als „normal" wäre und eine Vorratsspeicherung des Nutzungsverhaltens deshalb unentbehrlich sei. Dieser Beweis ist nicht geführt.

Häufigkeit von Angriffen (Beweisfrage 3b)

Der Sachverständige nimmt häufige Angriffe auf die Telemedien der Beklagten an. Insofern ist zu differenzieren:

Nachfragen an den Sachverständigen:

Im Vergleich zu „Angriffen" im Sinne von bloß vorbereiteten oder versuchten IT-Sicherheitsverletzungen (z.B. Portscans, Schwachstellensuche): Ist Ihnen bekannt, wie häufig öffentlich zugängliche Telemedien der Beklagten und die entsprechende Backend-Infrastruktur von tatsächlichen (erfolgreichen) IT-Sicherheitsverletzungen (also Verletzungen der Integrität, Vertraulichkeit oder Verfügbarkeit informationstechnischer Systeme) betroffen sind? Wenn nein, von welcher Häufigkeit gehen Sie aus?

Ist bekannt, wie häufig die generelle Nutzbarkeit von Telemedien der Beklagten durch Angriffe beeinträchtigt ist (z. B. Uptime)?

Sind die Telemedien der Beklagten, die eine IP-Speicherung praktizieren, signifikant häufiger von versuchten oder erfolgreichen IT-Sicherheitsverletzungen oder Einschränkungen der Nutzbarkeit betroffen als die übrigen Telemedien der Beklagten? Um wie viel Prozent? Gibt es dazu wissenschaftliche oder sonst statistisch belastbare Erkenntnisse?

Sind allgemein Telemedien, die eine Protokollierung von IP-Adressen praktizieren, signifikant häufiger von versuchten oder erfolgreichen IT-Sicherheitsverletzungen betroffen oder nicht nutzbar als andere Telemedien? Um wie viel Prozent? Gibt es dazu wissenschaftliche oder sonst statistisch belastbare Erkenntnisse?

Wie ändern sich Ihre Aussagen zu Art, Umfang und Wirkungen von Angriffen (z. B. in Bezug auf Bürgerdaten, Finanzdaten, Staatsgeheimnisse, regierungsinterne Kommunikationssysteme, Funktionsfähigkeit der Regierung), wenn die Beklagte (ohne anlasslose, vollständige IP-Protokollierung) andere Mittel und Maßnahmen zur Sicherheit ihrer Backend-Infrastrukturen auf hohem Niveau kombiniert (siehe Ihr Gutachten Seite 19 oben) und insbesondere eine Systemtrennung vornimmt, beispielsweise ihre Telemedien vom Rechenzentrum ITZ Bund oder extern (und damit getrennt von ihrer Verwaltungs-IT) bereitstellen lässt? Welche

Schäden durch Angriffe und Folgen in welchem Ausmaß drohen dann noch?

Trifft es zu, dass auch mit anlassloser, vollständiger IP-Protokollierung die drohenden Schäden von Angriffen, ihre Folgen und deren Ausmaß gleich bleiben, dass es sich also um allgemeine und nie ganz auszuschließende IT-Sicherheitsrisiken handelt?

Identifizierung von Angreifern (Beweisfrage 3c)

Der Sachverständige schätzt die Identifizierbarkeit von Angreifern zutreffend als gering (unter 10%) ein, weil nur wenige Angreifer Privatpersonen seien und überwiegend professionelle Angreifer und Organisationen mit gefälschten IP-Adressen agierten.

An anderer Stelle schreibt der Sachverständige zutreffend, dass die IT-Systeme des Bundes insbesondere von ausländischen Organisationen zum Zweck der Spionage angegriffen werden. Sowohl das Eindringen in Bundestagsserver im Jahr 2015 als auch das Eindringen in die IT von Bundesbehörden im Jahr 2018 („Bundeshack") wurde Russland zugeordnet. Aber auch auf China wird beispielsweise ein Angriff auf das Bundesamt für Kartografie Ende 2021 zurück geführt (dieses Bundesamt nahm übrigens eine Protokollierung von IP-Adressen der Nutzer seiner Website vor, was nicht vor dem Angriff schützte).

Es ist offensichtlich, dass Angriffe ausländischer Herkunft praktisch nie zur Identifizierung eines Täters anhand der IP-Adresse führen können, weil Russland oder China kaum bei der Identifizierung ihrer eigenen Hacker unterstützen werden.

Soweit der Sachverständige anmerkt, Angriffe unter Verwendung von Botnetzen könnten häufiger identifiziert werden, präzisiert er auf Seite 25, in einem „geringen Umfang" sei eine Austrocknung von Botnetzen anhand von Nutzungsprotokollen möglich. Weil Botnetz-Infektionen aber unbewusst und ungewollt erfolgen, kann auch eine selten erfolgreiche Identifizierung nicht zu strafrechtlichen Ermittlungen führen oder einen Abschreckungseffekt auf die Hacker entfalten, welche die Rechner steuern. Dementsprechend ergänzt der Sachverständige auf Seite 24 auch, dass auf die eigentlichen Täter keine Rückschlüsse gezogen werden können. Dass die „Austrocknung" von Botnetzen in der Praxis anders und wirksamer als durch Aufzeichnung des Nutzungsverhaltens erfolgt (mittels „Sinkhole-Servern"), ist oben bereits ausgeführt worden. Im Übrigen

können Brute-Force-Angriffe bereits aufgrund des Angriffsmusters automatisiert identifiziert und gezielt protokolliert werden.

Nachfrage an den Sachverständigen:

Trifft es zu, dass sich Brute-Force-Angriffe eindeutig von der normalen, rechtmäßigen Nutzung eines Telemediums unterscheiden?

Umfang der Datenspeicherung (Beweisfrage 3d)

Der Sachverständige betont zurecht, oftmals sei neben der IP-Adresse auch die Protokollierung der Portnummer nötig, um einen Nutzer identifizieren zu können. IP-Adressen werden von Internetzugangsanbietern nämlich oft mehrfach vergeben (sog. CGNAT-Verfahren). Die Standard-Backend-Infrastruktur zur Bereitstellung von Telemedien (am verbreitetsten sind Webserver von Nginx und Apache) protokolliert standardmäßig und üblicherweise („common log format" oder „combined log format") allenfalls die IP-Adresse von Nutzern, nicht aber ihre Portnummer. Das Internetportal des Bundesinnenministeriums (bmi.bund.de) wird etwa über einen Apache-Webserver bereit gestellt, und laut Datenschutzerklärung wird bei Zugriffen zwar die IP-Adresse protokolliert, nicht aber die Portnummer. Insofern geht der Kläger davon aus, dass die Beklagte generell keine Protokollierung der Portnummer von Telemediennutzern vornimmt.

Nachfrage an den Sachverständigen:

Wenn Sie ausführen, zur Identifizierung von Nutzern sei oftmals neben der IP-Adresse auch die Portnummer nötig, wie stark mindert es den Nutzen einer IP-Protokollierung, wenn nicht auch die Portnummer dazu gespeichert wird? Würden Sie den Restnutzen dann als wenig, stark oder größtenteils vermindert ansehen?

Verhältnismäßigkeit im engeren Sinn

Selbst wenn man entgegen der tatsächlichen Praxis der Beklagten als erwiesen erachten wollte, dass eine unterschiedslose Protokollierung des Nutzungsverhaltens anhand der unverkürzten IP-Adresse im Rechtssinne erforderlich sei, weil sie im Einzelfall nützlich sein könne, wo sämtliche mildere Mittel versagten: Die ungewisse, bestenfalls marginale Steigerung der allgemeinen Funktionsfähigkeit des Telemediums durch Einsatz dieses letzten Mittels steht außer jedem Verhältnis zum Gewicht des

Grundrechtseingriffs durch anlasslose Aufzeichnung des Inhalts der Telemediennutzung vollkommen rechtmäßig handelnder Bürger. Zu betonen ist die besondere Schutzwürdigkeit des Inhalts unserer Internetnutzung, die weit reichende Einblicke in unsere Persönlichkeit einschließlich unserer Gesundheit und unseres Sexuallebens, unserer Religion und unserer politischen Überzeugungen ermöglicht. Jede Vorratsspeicherung von Online-Aktivitäten begründet die Gefahr eines Diebstahls oder Missbrauchs hochsensibler Daten, eines falschem Verdachts oder sonstiger Nachteile. Unter ständiger Aufzeichnung der Online-Aktivitäten ist eine freie und unbefangene Grundrechtsausübung im Netz nicht möglich.

Letztlich sind die Telemedien von Bundesbehörden mit einer Art Lesesaal zu vergleichen, in dem der Öffentlichkeit Informationen bereit gestellt werden. In keinem Lesesaal wird personenbezogen festgehalten, wer wann was gelesen hat.

Über die Verhältnismäßigkeit im engeren Sinne als Rechtsfrage entscheidet die Kammer. Es ist keine sachverständig zu begutachtende Frage.

Soweit der Bundesgerichtshof in seinem Revisionsurteil keinen schweren Grundrechtseingriff gesehen hat, solange der Kläger nicht identifiziert werde, widerspricht das diametral der Rechtsprechung von Bundesverfassungsgericht und EuGH zur Vorratsdatenspeicherung. Diese sehen schon in der anlasslosen Vorratsdatenspeicherung – unabhängig von einer nachfolgenden Identifizierung – einen schwerwiegenden Grundrechtseingriff, weil schon die Sorge vor einer möglichen (gewollten oder unbeabsichtigten) Zuordnung ihres Kommunikationsverhaltens von einer freien Kommunikation abschrecken kann. Das Bundesverfassungsgericht schreibt, die Vorratsdatenspeicherung könne „ein diffus bedrohliches Gefühl des Beobachtetseins hervorrufen, das eine Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann".

BVerfG, 1 BvR 256/08 vom 02.03.2010, Abs. 212.

Es hat deshalb schon die Vorratsspeicherung von Telekommunikationsverkehrsdaten als „besonders schweren Eingriff" bewertet (a. a. O., Abs. 210), wobei im vorliegenden Fall die Beklagte sogar der Inhalt der abgerufenen Internetseiten (URL) speichert. Das Bundesverfassungsgericht hält Verbindungsdaten für weniger sensibel als eine Speicherung auch des Inhalts (a. a. O., Abs. 211), wie es teilweise die Beklagte praktiziert. Auch der EuGH hat entschieden, dass eine

Vorratsspeicherung von Telekommunikationsdaten einen Grundrechtseingriff „von großem Ausmaß“ darstellt.

EuGH, C–293/12 vom 08.04.2014, Abs. 37.

Auch der EuGH hat dabei berücksichtigt, dass – anders als vorliegend – noch keine Speicherung der „mit Hilfe eines elektronischen Kommunikationsnetzes abgerufenen Informationen“ erfolgte (a. a. O., Abs. 28).

Im Übrigen ist zu der vom Bundesgerichtshof erörterten Identifizierungsmöglichkeit darauf hinzuweisen, dass der Kläger durchaus im Rahmen von Broschürenbestellungen bei Bundesbehörden, beim Absenden ihrer Kontaktformulare oder auch beim Versand von E–Mails (welche notwendig auch die IP–Adresse enthalten) seine Personalien angibt und die Beklagte dann anhand der mitübermittelten IP–Adresse das gesamte Surfverhalten des Klägers rekonstruieren kann. Der Kläger muss zur Kommunikation mit Bundesbehörden in der Lage sein, ohne gleichzeitig sein Surfverhalten offenzulegen. Auch wenn die IP–Adresse des Klägers alle 24 Stunden wechseln mag, kann eine längere Identifizierung möglich sein. Jedes Endgerät verfügt über recht eindeutige Eigenschaften, die teilweise von der Beklagten mit gespeichert werden (sog. „Browser–Fingerprint“). Und wenn der Kläger eine IPv6–Adresse nutzt, kann diese eine permanente Identifikationskennung seiner Netzwerkkarte in Form der sog. MAC–Adresse enthalten. Die Beklagte kann dann aufgrund einer einzigen Angabe der Personalien des Klägers sein gesamtes Surfverhalten über lange Zeit hinweg dem Kläger zuordnen.

Nachfrage an den Sachverständigen:

Ist es richtig, dass bei Übermittlung der Personalien des Klägers etwa zum Zweck einer Broschürenbestellung eine Zuordnung seiner Telemediennutzung ungeachtet einer wechselnden IP–Adresse anhand seines Browser–Fingerprints oder anhand einer in der IPv6–Adresse permanent enthaltenen MAC–Adresse erfolgen kann?

Der Bundesgerichtshof hat im Revisionsurteil für maßgeblich erachtet, ob der „Angriffsdruck“ bzw. das Gefahrenpotenzial derjenigen Telemedien der Beklagten, bei denen IP–Adressen gespeichert werden, höher ist als bei den Telemedien, bei denen dies nicht erfolgt.

BGH, VI ZR 135/13 vom 16.05.2017, Abs. 41.

Der Beklagten ist dieser Nachweis nicht gelungen. Es ist nicht nachgewiesen, dass sich Art, Umfang und Wirkung von bereits erfolgten

und drohenden Angriffen bezüglich der Telemedien, die IP-Adressen speichern, von der Situation bei Telemedien ohne solche Vorratsspeicherung des Nutzungsverhaltens unterscheiden würden. Auch Unterschiede in der Bedeutung der Telemedien je nach Speicherpraxis sind nicht nachgewiesen, zumal zu der Gruppe der ohne Surfprotokollierung angebotenen Telemedien auch wichtige Informationsseiten von Behörden im Bereich kritischer Infrastruktur zählen (z. B. Bundeswahlleiterin, Auswärtiges Amt, Bundesbank, Bundesgerichtshof, Bundesamt für Bevölkerungsschutz, Bundesamt für Flugsicherung, Bundesnetzagentur, Luftfahrbundesamt, Technisches Hilfswerk).

Eine generalpräventive Wirkung gerade einer anlasslosen Surfprotokollierung – also dass Telemedien mit Protokollierung des Nutzungsverhaltens weniger vorbereiteten, versuchten oder erfolgreichen Beeinträchtigungen ihrer Funktionsfähigkeit ausgesetzt wären als Telemedien ohne solche Surfprotokollierung – ist ebenfalls nicht nachgewiesen. Wie der Sachverständige zutreffend ausführt (Seite 7), gibt es bewährte Technik, um eine Protokollierung nur im Fall bekannter Angriffsmuster oder sonst mutmaßlicher Angriffe vorzunehmen. Auch wenn diese Technik bei Angriffen nur in der Regel und nicht ausnahmslos greift, ergibt sich daraus jedenfalls ein Entdeckungsrisiko für Angreifer und eine generalpräventive Wirkung. Dass diese psychologische Abschreckungswirkung davon abhinge, wie hoch genau das Entdeckungsrisiko ist, wäre eine psychologisch realitätsfremde Annahme. Dass eine anlasslose Surfprotokollierung eine messbare, signifikante Steigerung des objektiven Entdeckungsrisikos erreichen würde, ist ohnehin nicht nachzuweisen.

IV. Anträge

Sollte die Kammer die Beweisaufnahme trotz der nunmehr fehlenden Rechtsgrundlage für die Datenverarbeitung der Beklagten für erheblich halten, wird beantragt,

> dem Sachverständigen Lehnigk-Emden die Nachfragen des Klägers entweder für eine kurze ergänzende schriftliche Stellungnahme vorzulegen oder den Sachverständigen zum Termin zu laden, damit die Fragen mündlich gestellt werden können. Weil die Fragen bereits vorliegen und angesichts ihres Umfangs könnte sich eine schriftliche Stellungnahme anbieten.

Es wird ferner beantragt,

> den Sachverständigen Dr. Köpsell zum Termin zu laden.

Es hat noch keine Gelegenheit bestanden, ihn mündlich zu seinem Gutachten zu befragen, obwohl Fragen dazu eingereicht waren (Schriftsatz vom 08.01.2013). Außerdem muss es auch möglich sein, den Sachverständigen zu dem nun vorliegenden Gutachten zu befragen, das zu einer entgegengesetzten Einschätzung gelangt, einschließlich der Ausführungen von Dr. Köpsell selbst (Seite 25). Bei sich widersprechenden Gutachten hat der Bundesgerichtshof betont, dass zunächst die Ursachen des Widerspruchs zu klären sind, etwa durch Ladung beider Gutachter zur mündlichen Erörterung

> BGH, VI ZR 6/79 vom 04.03.1980; BGH, VI ZR 261/85 vom 23.09.1986,

bevor eine Entscheidung darüber getroffen wird, welchem Gutachten gefolgt wird.

Die Auseinandersetzung mit den widersprüchlichen Gutachten erübrigt sich wiederum, wenn man entweder die Klage schon in Ermangelung einer Rechtsgrundlage für die Praktiken der Beklagten für begründet hält oder weil eine wahllose Vorratsspeicherung des Nutzungsverhaltens jedenfalls unverhältnismäßig im engeren Sinne ist. In diesem Fall erübrigen sich auch die Anträge des Klägers zu der weiteren Auseinandersetzung mit den Gutachten.

Mit freundlichem Gruß

Jonas Breyer
(Rechtsanwalt)