



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

60 S 10/25

Az.: IP-Speicherung

Sehr geehrte Damen und Herren,

In dem Verfahren

28.06.2025 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

Breyer ./ BRD

1. Entscheidungserheblichkeit der Beweisaufnahme

zahlt der Kläger vorsorglich den angeforderten Auslagenvorschuss für ein Ergänzungsgutachten ein, bittet die Kammer aber vorab zu prüfen, ob die Beweisaufnahme wirklich entscheidungserheblich ist. Die Kammer hatte mit Verfügung vom 16.04.2025 zurecht die vorrangig zu klärende Frage der Rechtsgrundlage für die Datenspeicherung hervorgehoben. Die von der Beklagten mit Schriftsatz vom 06.06.2025 angeführten Rechtsgrundlagen für die streitgegenständliche Vorratsspeicherung personenbezogener Nutzungsprotokolle kommen von vornherein nicht in Betracht – siehe dazu den Abschnitt „Aktuelle Rechtslage“ unten. Mangels Rechtsgrundlage zum gegenwärtigen Zeitpunkt kann die Frage der Erforderlichkeit dahin stehen und erübrigt sich die Beweisaufnahme.

Im Übrigen ist die beanstandete anlass- und wahllose Protokollierung der Internetnutzung jedenfalls grob unverhältnismäßig, so dass es auch aus diesem Grund auf die Beweiserhebung über ihre angebliche Erforderlichkeit nicht mehr ankommt.

Schließlich weist der Kläger darauf hin, dass ein etwaiges Ergänzungsgutachten des Sachverständigen Lehnigk-Emden seinen Antrag auf Ladung und Befragung des vormals tätigen Sachverständigen Dr. Köpsell unberührt lässt.

2. Aktuelle Rechtslage

a. § 9 TDDDG

Der von der Beklagten angeführte § 9 TDDDG bildet keine Rechtsgrundlage für die beklagtenseitige Vorratsspeicherung von Nutzungsdaten beim Abruf von Inhalten aus dem Internet. § 9 TDDDG ist auf die von der Beklagten protokollierten Nutzungsdaten (§ 2 Abs. 2 Nr. 3 TDDDG) nicht anwendbar. Die Vorschrift gilt ausweislich der Titelüberschrift („Datenschutz und Schutz der Privatsphäre in der Telekommunikation“), ihrer eigenen Überschrift und ihrem Wortlaut ausdrücklich nur für die „Verarbeitung von Verkehrsdaten“ und auch nur für „Nach § 3 Absatz 2 Satz 1 Verpflichtete“.

„Verkehrsdaten“ sind nach § 2 Abs. 1 TDDDG i.V.m. § 3 Nr. 70 TKG Daten, deren Verarbeitung bei der Erbringung eines Telekommunikationsdienstes erforderlich ist. Und nach § 3 Absatz 2 Satz 1 TDDDG zur Wahrung des Fernmeldegeheimnisses Verpflichtete sind nur Anbieter öffentlich zugänglicher Telekommunikationsdienste und daran Mitwirkende.

„Telekommunikationsdienste“ sind nach § 2 Abs. 1 TDDDG i.V.m. § 3 Nr. 61 TKG

„in der Regel gegen Entgelt über Telekommunikationsnetze erbrachte Dienste, die – mit der Ausnahme von Diensten, die Inhalte über Telekommunikationsnetze und – dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben – folgende Dienste umfassen:

- a) Internetzugangsdienste,
- b) interpersonelle Telekommunikationsdienste und
- c) Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden;“

Die öffentlichen Internetportale der Beklagten werden schon nicht „in der Regel gegen Entgelt“ bereit gestellt, sondern kostenfrei.

Zudem ist die Ausnahme des § 3 Nr. 61 TKG für Dienste einschlägig, „die Inhalte über Telekommunikationsnetze und -dienste anbieten“. Mit ihren Internetportalen bietet die Beklagte Inhalte über das Internet als Telekommunikationsnetz an. Die Bereitstellung von Webseiten ist digitaler Dienst (früher: Telemediendienst) und nicht Telekommunikationsdienst (Hornung/Schallbruch, IT-Sicherheitsrecht, § 21, Rn. 8 und 11; BeckOK IT-Recht/Herrmann, § 3 TKG, Rn. 55).

Die Definition der Telekommunikationsdienste in § 3 Nr. 61 TKG setzt wortgleich Art. 2 Nr. 4 der Richtlinie 2018/1972/EG um. In deren Erwägungsgründen 7 und 10 wird betont, dass die „Bereitstellung von internetgestützten Inhalten“ nicht unter diese Richtlinie fällt und keinen „elektronischen Kommunikationsdienst“ darstellt. Auch der EuGH hat klargestellt, dass die Bereitstellung von Inhalten mittels einer Website keinen (Tele-)Kommunikationsdienst darstellt (EuGH, NJW 2019, 983).

Dementsprechend handelt es sich bei den streitgegenständlichen Protokollen über die Nutzung der Internetinhalte der Beklagten nicht um Telekommunikations-Verkehrsdaten, sondern um Nutzungsdaten eines digitalen Dienstes. Diese sind im Teil 3 des TDDDGD geregelt, allerdings nur hinsichtlich des Auskunftsverfahrens (§ 24 TDDDGD). Im Übrigen hat der Bund nach Inkrafttreten der DS-GVO keine Gesetzgebungskompetenz für einen besonderen Telemediendatenschutz mehr.

Folglich ist auch dem auf § 15 TMG a. F. beruhenden Revisionsurteil des BGH im vorliegenden Verfahren durch Inkrafttreten der DSGVO der Boden entzogen worden.

b. Art. 6 Abs. 1 S. 1 lit. f) DS-GVO

Dass der beklagtenseits hilfsweise angeführte Art. 6 Abs. 1 S. 1 lit. f) DSGVO gemäß Satz 2 dieser Vorschrift nicht auf die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Datenverarbeitung anwendbar ist, wurde im letzten Schriftsatz umfassend ausgeführt. Deswegen ist auch der diesbezügliche Erwägungsgrund 49, der ausdrücklich nur den Begriff des berechtigten Interesses präzisiert, nicht einschlägig. Im Übrigen stellen die Erwägungsgründe von Unionsrechtsakten wie deutsche Gesetzgebungsmaterialien keine Rechtsnormen dar. Nach ständiger Rechtsprechung des EuGH gilt:

„Insoweit ist zunächst daran zu erinnern, dass die Erwägungsgründe eines Gemeinschaftsrechtsakts rechtlich nicht verbindlich sind und weder herangezogen

werden können, um von den Bestimmungen des betreffenden Rechtsakts abzuweichen, noch, um diese Bestimmungen in einem Sinn auszulegen, der ihrem Wortlaut offensichtlich widerspricht“ (EuGH, 02.04.2009 – C-134/08, Abs. 16; EuGH, 10.01.2006 – C-344/04, Abs. 76; EuGH, 19.12.2019 – C-418/18 P, Abs. 76).

Art. 6 Abs. 1 S. 1 lit. e) DS-GVO lässt ein berechtigtes Interesse nach seinem eindeutigen Wortlaut gerade nicht genügen, um die behördliche Verarbeitung persönlicher Daten zu rechtfertigen. Behörden brauchen dafür stets eine gesonderte Rechtsgrundlage, an der es hier fehlt.

Die einschlägige Kommentierung (Kühling/Buchner/Buchner/Petri, 4. Aufl. 2024, DS-GVO Art. 6 Rn. 129d, beck-online) betont wörtlich:

„Die behördliche eigeninitiative Öffentlichkeitsarbeit wird regelmäßig auf Art. 6 Abs. 1 lit. e, Abs. 3 S. 1 [DS-GVO] in Verbindung mit der Verarbeitungsgeneralklausel des jeweiligen allgemeinen Datenschutzgesetzes (z.B. § 3 BDSG) gestützt. Sie unterliegt strengeren Erforderlichkeitsmaßstäben als die entsprechende Öffentlichkeitsarbeit von nichtöffentlichen Stellen, die typischerweise auf Art. 6 Abs. 1 lit. f [DSGVO] beruht.“

Auch die Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) als Aufsichtsbehörde misst den Betrieb einer behördlichen Internetpräsenz auf Facebook (Fanpage) an Artikel 6 Absatz 1 lit. e DSGVO in Verbindung mit § 3 BDSG (siehe Bescheid vom 17.02.2023 zum Az. 23-507-3/005#0016,

[https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2023/Bescheid-Facebook-Fanpage.pdf?](https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2023/Bescheid-Facebook-Fanpage.pdf?__blob=publicationFile&v=1)

[__blob=publicationFile&v=1](https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2023/Bescheid-Facebook-Fanpage.pdf?__blob=publicationFile&v=1), S. 36). Nichts anderes kann für den Eigenbetrieb behördlicher Internetpräsenzen gelten.

Sogar in der eigenen Datenschutzerklärung des Bundesinnenministeriums, das die Beklagte in diesem Prozess vertritt, heißt es:

„Rechtsgrundlage der Verarbeitung ist hier Art. 6 Abs. 1 lit. e der Datenschutz-Grundverordnung der EU (DS-GVO) in Verbindung mit der entsprechenden innerstaatlichen oder europäischen Aufgabennorm bzw. in Verbindung mit § 3 BDSG.“

Die Beklagte weiß also ganz genau, dass nur Art. 6 Abs. 1 S. 1 lit. e) DS-GVO i.V.m. § 3 BDSG als Rechtsgrundlage für ihre Vorratsspeicherung des Nutzungsverhaltens in Betracht kommen. Wie im letzten Schriftsatz erläutert, vermögen diese Vorschriften ihre Praxis jedoch nicht zu rechtfertigen.

Die Auseinandersetzung mit den vorliegenden Sachverständigengutachten und die Beweisaufnahme erübrigt sich somit,

weil die Klage nach derzeitigem Recht schon in Ermangelung einer Rechtsgrundlage für die Praktiken der Beklagten begründet ist.

c. Verhältnismäßigkeit im engeren Sinn

Soweit die Beklagte nun das EuGH-Urteil La Quadrature du Net 2 anführt (Rechtssache C-470/21) und behauptet, die Totalerfassung des Inhalts der Internetnutzung wahlloser Bürger sei nur ein „geringfügiger“ Grundrechtseingriff, ist diese Rechtsprechung auf den vorliegenden Fall nicht ansatzweise übertragbar:

- **Andere Art der Datenverarbeitung:** Das EuGH-Urteil betrifft die Nutzbarkeit und Verwertbarkeit bereits gespeicherter Daten, im vorliegenden Fall geht es aber um die Zulässigkeit der Datensammlung selbst.
- **Anderer Speicherzweck:** Die EuGH-Entscheidung betrifft die Nutzung von Daten, die zur Verfolgung von Straftaten gespeichert worden waren. Im vorliegenden Fall wird die Datensammlung aber mit der bloßen besseren Verfügbarkeit von Internetportalen begründet.
- **Gesetzliche Grundlage:** Im EuGH-Fall war die Datensammlung aufgrund einer besonderen gesetzlichen Verpflichtung zur Vorratsdatenspeicherung erfolgt. Im vorliegenden Fall gibt es gerade kein Gesetz, welches die Beklagte zur Datensammlung verpflichten würde.
- **Andere speichernde Stelle:** Die EuGH-Entscheidung betrifft nur eine Vorratsdatenspeicherung durch Internetzugangsanbieter (siehe Urteilstenor: „Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste“); im vorliegenden Fall sammelt die Beklagte Daten als Anbieterin von Inhalten im Internet (Content-Anbieterin). Für solche Dienste hat der EuGH in ständiger Rechtsprechung keinen vergleichbaren Eingriff in Betracht gezogen.
- **Anderer Dateninhalt (Inhalteprotokollierung statt reiner Verkehrsdatenspeicherung):** Die EuGH-Rechtsprechung betrifft vor allem nur die Information, welchem Internetnutzer ein Internet-Zugangsanbieter wann welche IP-Adresse zugewiesen hat. Die Beklagte speichert dagegen die IP-Adresse zusammen mit den

abgerufenen Internetinhalten (URLs). Damit ist ein direkter Rückschluss auf das Internetnutzungsverhalten und Interessenprofil der Nutzer möglich. Die Kombination aus IP-Adresse und konkretem Nutzungsverhalten birgt ein hohes Missbrauchspotenzial und erlaubt tiefgehende Rückschlüsse auf persönliche Interessen, Neigungen und Lebensverhältnisse der betroffenen Nutzer. Die personenbezogene Erfassung der Nutzungsinhalte hat eine völlig andere Qualität als bloße Identifizierungsdaten. Der EuGH hat in seinen Urteilen zur Vorratsdatenspeicherung stets betont, dass damit – anders als vorliegend – keine Speicherung der „mit Hilfe eines elektronischen Kommunikationsnetzes abgerufenen Informationen“ erfolge (EuGH, C-293/12 vom 08.04.2014, Abs. 28). Die Beklagte tut jedoch genau dies und schafft damit eine Überwachungstiefe, die weit über das hinausgeht, was der EuGH selbst bei der Verfolgung schwerster Straftaten für zulässig erachtet.

Der Versuch der Beklagten, ihre umfassende Protokollierung von Nutzungsinhalten durch ein hochspezifisches Urteil zur staatlich angeordneten Vorratsdatenspeicherung durch Internet-Zugangs-anbietern zu legitimieren, ist zum Scheitern verurteilt. Jeder relevante Aspekt – der Handelnde, der Zweck, die Rechtsgrundlage und vor allem die Art der gespeicherten Daten – unterscheidet sich fundamental. Die hier praktizierte Datensammlung stellt nicht nur keinen „geringfügigen“, sondern einen besonders schweren Grundrechtseingriff dar.

Das alte Argument der Beklagten, ein schwerer Eingriff läge nur vor, wenn die Beklagte selbst die Person hinter der IP-Adresse identifizieren könnte, verkennt den Begriff der „personenbezogenen Daten“ nach Art. 4 Nr. 1 DS-GVO grundlegend. Eine Person gilt als „identifizierbar“, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einer IP-Adresse, identifiziert werden kann. Es ist dabei unerheblich, ob eine einzige Stelle über alle zur Identifizierung notwendigen Informationen verfügt. Entscheidend ist, ob die Identifizierung mit vernünftigen Aufwand möglich ist. Die Zuordnung einer IP-Adresse zu einem Anschlussinhaber durch dessen Access-Provider (zum Beispiel im Rahmen eines zivil- oder strafrechtlichen Auskunftsanspruchs) ist ein solcher vernünftiger und rechtlich vorgesehener Weg. Die Beklagte nimmt die Speicherung ausdrücklich vor, um gegebenenfalls eine solche Identifizierung vorzunehmen. So spricht die Datenschutzerklärung des

Bundesinnenministeriums von der möglichen „Einleitung einer Rechts- und Strafverfolgung“.

Dass die Beklagte ihre Praxis als einen „Sicherheitsbaustein“ ansieht, genügt der EuGH-Rechtsprechung zur strikten Erforderlichkeit und Verhältnismäßigkeit von Grundrechtseingriffen nicht und blendet die vielfältigen verfügbaren mildernden Mittel aus.

3. Sachverhalt: aktuelle Speicherpraxis der Beklagten

Soweit die Beklagte pauschal ins Blaue hinein und ohne jede Rücksprache bestreitet, dass die in ihren eigenen Datenschutzerklärungen öffentlich angegebene Speicherpraxis zutreffe, ist dieses Bestreiten unzulässig. Der Kläger hat die außerhalb seines Wahrnehmungsbereichs liegende Speicherpraxis von Behörden der Beklagten im Einzelnen und substantiiert dargelegt, so dass pauschales unsubstantiiertes Bestreiten durch die Beklagte, die alle Tatsachen kennt bzw. zumutbarerweise abfragen kann, nicht zulässig ist (BeckOK ZPO/v. Selle, § 138 ZPO, Rn. 18 m.w.N. auf die BGH-Rspr.).

Ein Bestreiten mit Wissen wäre unzulässig, weil das Bundesinnenministerium als Vertreter der Beklagten die tatsächliche Speicherpraxis der Bundesbehörden nicht in Erfahrung gebracht hat und folglich nicht kennt. Anerkanntermaßen darf ein nicht informierter Anwalt nicht ins Blaue hinein bestreiten (Musielak/Voit/Stadler § 138 ZPO, Rn. 13 m. w. N. auf die Rspr.).

Ein Bestreiten mit Nichtwissen ist wiederum nach § 138 Abs. 4 ZPO unzulässig, weil die beklagte BRD ihre eigene Speicherpraxis kennt. Anerkanntermaßen kann sich eine Partei nicht hinter ihrer arbeitsteiligen Binnenorganisation verschanzen: Sie trifft eine Erkundigungspflicht, sofern die maßgebenden Tatsachen Personen bekannt sind, die unter ihrer Anleitung, Aufsicht oder Verantwortung tätig sind (BeckOK ZPO/von Selle, § 138 ZPO, Rn. 26 m. w. N. auf die BGH-Rspr.). Dies ist bei Bundesbehörden der Fall. Die BRD trägt die rechtliche Verantwortung für das Handeln ihrer Behörden.

Im Übrigen muss sich die Beklagte nach Auffassung des Klägers an der öffentlich in Datenschutzerklärungen angegebenen Speicherpraxis festhalten lassen, egal ob sie zutrifft oder nicht. Datenschutzerklärungen

sind gesetzlich vorgeschrieben, gerade weil sich die Öffentlichkeit auf ihre Richtigkeit verlassen können muss.

Der Kläger suggeriert keineswegs, dass die Beklagte seine Internetnutzung „nur auf wenigen Webseiten speichern würde“. Es gibt zwar viele Internetportale von Bundesbehörden, auf denen das nicht erfolgt. Wohl die Mehrzahl speichert aber weiterhin wie das Bundesinnenministerium flächendeckend und ohne jeden Anlass, etwa die weitaus meisten Bundesministerien.

Entgegen der Darstellung der Beklagten bleibt richtig, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) selbst keine anlass- und wahllose personenbezogene Protokollierung, wie sie sich das Bundesinnenministerium anmaßt, bei Zugriffen auf die von ihm betriebenen Webseiten vornimmt. Richtig ist zwar, dass das BSI Protokolldaten der Website-Besucher für 30 Tage unter anderem zu dem Zweck speichert, die „Systemsicherheit der Website zu gewährleisten“ (Ziff. 1.1 der Datenschutzerklärung). Nach ausdrücklichen Angaben in der Datenschutzerklärung unter Ziff. 1.1 wird dazu aber nur gespeichert:

„Es werden folgende Daten gespeichert:

- Datum und Uhrzeit des Abrufs (Zeitstempel)
- Anfragedetails und Zieladresse (Protokollversion, HTTP-Methode, Referer, UserAgent-String)
- Name der abgerufenen Datei und übertragene Datenmenge (angefragte URL inkl. Query-String, Größe in Byte)
- Meldung, ob der Abruf erfolgreich war (HTTP Status Code)“

Die IP-Adresse wird vom BSI also gerade nicht anlasslos gespeichert.

Soweit die Beklagte auf Ziffer 2.2 der Datenschutzerklärung des BSI („Protokolldatenauswertung“) abhebt, heißt es dort zur Speicherdauer ausdrücklich:

„Die automatisierte Auswertung der Protokolldaten erfolgt unverzüglich, die Daten werden nach erfolgtem Abgleich sofort und spurlos gelöscht. Soweit tatsächliche Anhaltspunkte bestehen, dass die Protokolldaten für den Fall der Bestätigung eines Verdachts nach § 5 Abs. 3 S. 2 BStG 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 BStG.“

Die Protokolldatenauswertung erfolgt danach unverzüglich und noch während des Nutzungsvorgangs in Echtzeit. Eine Speicherung über die

Dauer des Nutzungsvorgangs hinaus erfolgt beim BSI nur anlassbezogen bei Vorliegen tatsächlicher Anhaltspunkten, wie sie beim Kläger nicht bestehen.

Es wird auch die Behauptung bestritten, dass das BSI anderen Behörden eine weiter gehende Protokollierung empfehle als es selbst praktiziert.

4. Fazit

Die Auseinandersetzung mit den widersprüchlichen Sachverständigen-gutachten erübrigt sich, 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)