



RECHTSANWÄLTE

TCI Partnerschaft von Rechtsanwälten Müller Schmidt mbB
Fasanenstr. 61 · D - 10719 Berlin

Nur per beA

Landgericht Berlin II
ZK 60
Littenstraße 12 - 17
10179 Berlin

Berlin, den 6. Juni 2025

Ansprechpartner: [REDACTED]

E-Mail-Adresse: [REDACTED]

Aktenzeichen: 172/000123-08/ms

In dem Rechtsstreit

Patrick Breyer ./. Bundesrepublik Deutschland,
vertr. d. d. Bundesministerium des Innern und für Heimat
- 60 S 10/25 -

**TCI Partnerschaft von
Rechtsanwälten
Müller Schmidt mbB**

Fasanenstr. 61
D - 10719 Berlin
Tel: +49 - (0)30 - 20 05 42-0
Fax: +49 - (0)30 - 20 05 42-11
www.tcilaw.de

Norman Müller
Markus Schmidt
Carsten Gerlach ¹
Katharina Anders*
Hanno Dormagen*
Jakob Hiller*

In Kooperation mit

TCI Rechtsanwälte München

Ruth Dünisch
Dr. Truiken J. Heydn
Dr. Michael Karger ^{1,2}
Harald Krüger ³
Dr. Andreas Stadler
Dr. Thomas Stögmüller ¹
LL.M. (Berkeley)

TCI Rechtsanwälte Mainz

Stephan Breckheimer ^{3,5}
LL.M. (Medienrecht)
Sabine Brumme
Helena Golla*⁴
LL.M. (gewerblicher Rechtsschutz)
Dr. Olaf Griebenow
Stephan Schmidt ¹
Christian Welkenbach ^{1,4}

Fachanwalt für

¹ Informationstechnologierecht

² Verwaltungsrecht

³ Arbeitsrecht

⁴ Gewerblichen Rechtsschutz

⁵ Urheber- und Medienrecht

*angestellte(r) Rechtsanwältin/-anwalt

⁴ Gewerblichen Rechtsschutz

⁵ Urheber- und Medienrecht

*angestellte(r) Rechtsanwältin/-anwalt

nehmen wir zum Schriftsatz des Klägers vom 14. April 2025 wie folgt Stellung:

1. Rechtsgrundlage der Speicherung

Entgegen der Behauptung des Klägers erfolgt die Speicherung der IP-Adressen durch die Beklagte sehr wohl auf einer gültigen Rechtsgrundlage. Die Entscheidung des Bundesgerichtshofes vom 16. Mai 2017, VI ZR 135/13 hat weiterhin uneingeschränkte Gültigkeit, auch wenn sie sich formal mit dem zwischenzeitlich durch § 9 TDDDG abgelösten § 15 TMG beschäftigte.

§ 15 Abs. 1 TMG hatte folgenden Wortlaut:

„§ 15 Nutzungsdaten

(1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind insbesondere

- 1. Merkmale zur Identifikation des Nutzers,*
- 2. Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und*
- 3. Angaben über die vom Nutzer in Anspruch genommenen Telemedien.“*

Der BGH hat hierzu in seiner Entscheidung unter Berufung auf die entsprechende Vorlageentscheidung des EuGH vom 19. Oktober 2016, C-582/14 wie folgt tenoriert:

„§ TMG § 15 Abs. 1 ist entsprechend Art. 7 lit. f RL 95/46/EG dahin auszulegen, dass ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung auch über das Ende eines Nutzungsvorgangs hinaus dann erheben und verwenden darf, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die generelle Funktionsfähigkeit der Dienste zu gewährleisten, wobei es allerdings einer Abwägung mit dem Interesse und den Grundrechten und -freiheiten der Nutzer bedarf.“

Der nunmehr einschlägige § 9 TDDDG hat folgenden Wortlaut:

„§ 9 Verarbeitung von Verkehrsdaten

(1) Nach § 3 Absatz 2 Satz 1 Verpflichtete dürfen folgende Verkehrsdaten nur verarbeiten, soweit dies zum Aufbau und zur Aufrechterhaltung der Telekommunikation, zur Entgeltabrechnung oder zum Aufbau weiterer Verbindungen erforderlich ist:

- 1. die Nummer oder Kennung der beteiligten Anschlüsse oder der Endrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten,*
- 2. den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,*
- 3. den vom Nutzer in Anspruch genommenen Telekommunikationsdienst,*

4. *die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen und*
5. *sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.*

Im Übrigen sind Verkehrsdaten von den nach § 3 Absatz 2 Satz 1 Verpflichteten nach Beendigung der Verbindung unverzüglich zu löschen. Eine über Satz 1 hinausgehende Verarbeitung der Verkehrsdaten ist unzulässig. Die Pflicht zur Verarbeitung von Verkehrsdaten aufgrund von anderen Rechtsvorschriften bleibt unberührt.“

Wie dem Wortlaut des § 9 Abs. 1 TDDDG zu entnehmen ist, handelt es sich dabei um die in den entscheidenden Punkten inhaltsgleiche Nachfolgeregelung zu § 15 Abs. 3 TMG. Die durch den BGH im Einklang mit dem EuGH im Urteil vom 16. Mai 2017 aufgestellte Auslegungsregel ist daher uneingeschränkt auch auf § 9 Abs. 1 TDDDG anzuwenden. Da es sich bei dem TDDDG für die hier in Rede stehenden Telemedien weiterhin um die Umsetzung der Richtlinie 2002/58/EG handelt, liegt nach wie vor eine *lex specialis* i. S. d. Art. 95 DSGVO für den Bereich der Telemedien vor.

Im Übrigen entspricht Art. 6 Abs. 1 lit. f) DSGVO im Wortlaut dem Art. 7 lit. f) der Richtlinie 95/46/EG, der Grundlage der Entscheidung des EuGH war. Auch europarechtlich sind daher die Grundlagen für die Entscheidung des BGH inhaltlich unverändert. Im Ergebnis hat sich die Rechtslage daher entgegen der Behauptung des Klägers seit den grundlegenden Entscheidungen des EuGH und des BGH nicht geändert.

Selbst wenn man § 9 TDDDG nicht für einschlägig hält, ergäbe sich entgegen der Auffassung des Klägers die Befugnis zur Speicherung für die Beklagte aus Art. 6 DS-GVO. Die Befugnis zur Verarbeitung der IP-Adresse als personenbeziehbares Datum ergibt sich für die Beklagte demnach zunächst aus Art. 6 Abs. 1 S. 1 lit. f) DS-GVO, soweit die Beklagte Telemedien außerhalb der Erfüllung

ihrer originären Aufgaben betreibt. Im Rahmen ihrer originären Aufgabenerfüllung ergibt sich die Befugnis aus Art. 6 Abs. 1 S. 1 lit. e) DS-GVO i. V. m. Art. 6 Abs. 3 DS-GVO und § 3 BDSG.

Im Erwägungsgrund 49 zur DS-GVO wird dazu herausgestellt, dass für die Verarbeitung personenbezogener Daten, also auch der IP-Adresse, bei Behörden ein berechtigtes Interesse besteht, soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen.

2. unterschiedliches Speicherverhalten bei unterschiedlichen Telemedien

Es ist zutreffend, dass verschiedene Behörden und Institutionen der Beklagten beim Betrieb ihrer Telemedien (digitalen Dienste) eine unterschiedliche Speicherpraxis bezüglich der IP-Adresse des zugreifenden Systems an den Tag legen. Diese Erkenntnis ist allerdings keinesfalls neu (vgl. hiesiger Schriftsatz vom 10. August 2018, an dem inhaltlich insoweit ausdrücklich festgehalten wird). Die Gründe hierfür sind, wie bereits zum damaligen Zeitpunkt erläutert, vielfältig und können von der Beklagten aus den genannten Gründen keinesfalls abschließend beurteilt werden. Ob eine Speicherung der IP-Adresse bei allen vom Kläger aufgeführten Webseiten tatsächlich nicht erfolgt, muss daher bestritten werden. Der Kläger beruft sich insoweit ausschließlich auf die Datenschutzerklärungen der jeweiligen Webseiten. Ein Beweis dafür, dass eine Speicherung dort tatsächlich nicht erfolgt, ist dies nicht.

Definitiv unzutreffend ist der Vortrag des Klägers, das Bundesamt für Sicherheit in der Informationstechnik (BSI) würde eine derartige Speicherung bei Zugriffen

auf die von ihm betriebenen Webseiten nicht vornehmen. Das angeführte Zitat ist irreführend.

Richtig ist vielmehr, dass das BSI sehr wohl die Protokolldaten der Website-Besucher und damit auch die IP-Adresse des zugreifenden Systems für 30 Tage zum Schutz vor Angriffen und damit der Sicherstellung des ordnungsgemäßen Betriebs speichert. Dazu wird in den Datenschutzhinweise ausgeführt:

Name der Verarbeitung	Kategorie pb Daten	Betroffene	Verarbeitungszweck	Speicher-dauer
Protokolldateien	Allg. technische Daten	Website-Besucher	Ordnungsgemäßer Betrieb der Website, Schutz vor Angriffen	30 Tage

Die vom Kläger zitierte Textpassage bezieht sich dagegen ausschließlich auf das eingesetzte Schadsoftwareerkennungssystem (siehe Ziffer 2.1 der Datenschutzerklärung) und nicht auf die Protokolldaten der Website-Zugriffe (siehe Ziffer 2.2 der Datenschutzerklärung).

Seitens des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wird deshalb auch allen Behörden empfohlen, die IP-Adresse der auf ihre Telemedien zugreifenden Systems jedenfalls vorübergehend zu speichern. Allerdings hat insoweit weder das BSI, noch das Bundesministerium des Innern eine Weisungsbefugnis für alle anderen Behörden und Institutionen der Beklagten. Dies gilt insbesondere, soweit es sich um eigenständige Verfassungsorgane (wie z. B. den Bundesrat) oder im Zuge der Gewaltenteilung unabhängige Einrichtungen (z. B. oberste Bundesgerichte) handelt.

Letztendlich spielt die Frage, welche Behörden und Institutionen der Empfehlung des BSI folgen, für die Entscheidung dieses Rechtsstreits keine Rolle. Maßgeblich ist alleine, dass ein sicherer Betrieb der Telemedien ohne Speicherung

der IP-Adressen nicht möglich ist. Im Übrigen verweisen wir zur Vermeidung von Wiederholungen auf unseren Schriftsatz vom 13. März 2025.

3. **Stellungnahme des Klägers zum Sachverständigengutachten und Fragen des Klägers an den Sachverständigen**

Die Ausführungen des Klägers zum Sachverständigengutachten sowie die geltend gemachten Fragen an den Sachverständigen sind ohne jegliche Entscheidungsrelevanz. Dies wird insbesondere an den eigenen Ausführungen des Klägers auf den Seiten 17 ff. („Verhältnismäßigkeit im engeren Sinn“) seines Schriftsatzes vom 14. April 2025 deutlich.

Der Kläger macht hier deutlich, dass seine gesamte Argumentation auf eine vermeintlich abweichende Speicherpraxis der Beklagten ausgerichtet ist. Selbst wenn es diese abweichende Speicherpraxis bei der Beklagten tatsächlich einheitlich gäbe, was gerade nicht zutreffend ist (vgl. oben Ziffer 2), könnte der Beklagten nicht untersagt werden, zukünftig die für einen sicheren Betrieb notwendigen Speicherungen vorzunehmen. Der Kläger kann seinen geltend gemachten umfassenden Unterlassungsanspruch nicht damit begründen, die Beklagte hätte bislang eine solche Speicherung nicht in allen ihr zuzurechnenden Telemedien vorgenommen. Der Kläger kann seinen Unterlassungsanspruch auch nicht damit begründen, die Speicherung der IP-Adresse sei keine (alleine) ausreichende Maßnahme für einen sicheren Telemedien-Betrieb. Der Kläger versucht hier die durch den Sachverständigen zu beantwortenden Beweisfragen, ob die Speicherung für einen sicheren Betrieb erforderlich sei, dahin zu verkehren, ob die Speicherung für einen sicheren Betrieb hinreichend sei. Letzteres spielt jedoch für die Entscheidung des Rechtsstreits keinerlei Rolle.

Der Vortrag des Klägers als richtig unterstellt, stellt vielmehr das Rechtsschutzinteresse des Klägers massiv in Frage. Der Kläger behauptet fortgesetzt, die Beklagte könnte über die Speicherung seiner IP-Adresse umfassende Profile seines

Online-Nutzungsverhaltens erstellen, was einen schweren Eingriff in seine Persönlichkeitsrechte darstellen würde. Wenn aber tatsächlich die Beklagte, wie vom Kläger suggeriert, seine IP-Adresse nur auf wenigen Webseiten speichern würde, wäre eine solche Profilerstellung schon theoretisch ausgeschlossen.

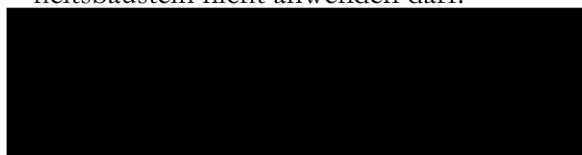
Hinzukommt, dass auch der EuGH zwischenzeitlich seine Rechtsprechung zur Vorratsdatenspeicherung modifiziert hat. In der Entscheidung vom 30. April 2024 – C-470/21 (La Quadrature du Net ua/ Premier ministre ua) hat der EuGH nunmehr ausdrücklich festgestellt, dass nicht jede allgemeine und unterschiedslose Vorratsspeicherung der von einer Person innerhalb eines bestimmten Zeitraums genutzten statischen und dynamischen IP-Adressen zwangsläufig einen schweren Eingriff in seine garantierten Grundrechte darstellt. Insbesondere kann die allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen nach Ansicht des EuGH gegebenenfalls durch das Ziel der Bekämpfung von Straftaten im Allgemeinen gerechtfertigt sein. Dies gilt insbesondere dann, wenn tatsächlich ausgeschlossen ist, dass diese Speicherung schwere Eingriffe in das Privatleben des Betroffenen zur Folge haben kann, die darauf beruhen, dass insbesondere durch eine Verknüpfung dieser IP-Adressen mit einem von den Betreibern ebenfalls gespeicherten Satz von Verkehrs- oder Standortdaten die Möglichkeit besteht, genaue Schlüsse in Bezug auf ihn zu ziehen.

Der EuGH nennt damit als Voraussetzung für einen schweren Eingriff in die Persönlichkeitsrechte die Möglichkeit, die hinter der IP-Adresse stehende Person und weitere Verkehrsdaten deshalb zusammenführen zu können, weil sie vom bzw. beim gleichen Betreiber gespeichert werden.

Übertragen auf den hiesigen Sachverhalt läge damit nach der neuen Rechtsprechung des EuGH ein schwerer Eingriff in die Persönlichkeitsrechte des Klägers nur dann vor, wenn die Beklagte die konkreten Nutzungsdaten des Klägers wie z. B. aufgerufenen Webseiten, Zeitpunkt des Zugriffs usw. selbst mit der hinter der von ihr gespeicherten IP-Adresse stehenden Person zusammenführen

könnte. Dies ist der Beklagten unzweifelhaft nicht möglich, da die Zuordnung seiner jeweiligen IP-Adresse zur Identität des Klägers allenfalls dem Access-Provider des Klägers möglich ist und die dafür notwendigen Informationen auch nur bei dem Access-Provider und gerade nicht bei der Beklagten gespeichert werden.

Im Ergebnis unterstreicht daher der EuGH mit seiner aktuellen Rechtsprechung die bereits vom BGH in seiner Entscheidung vom 16. Mai 2017 vertretene Auffassung, dass es sich bei dem Eingriff in die Persönlichkeitsrechte des Klägers durch die streitgegenständliche Speicherung der IP-Adresse um einen allenfalls geringfügigen Eingriff handelt. Demgegenüber steht die Notwendigkeit für die Beklagte die ihr obliegenden staatlichen Aufgaben, insbesondere auch vor dem Hintergrund der erforderlichen zunehmenden Digitalisierung dieser Aufgaben, durch einen sicheren Betrieb ihrer Telemedien gewährleisten zu können. Selbst wenn die Speicherung der IP-Adresse der zugreifenden Systeme hierfür nur einen Baustein darstellt, muss in der Abwägung der Interessen die Entscheidung zugunsten der Beklagten ausfallen, da die Beklagte nicht verpflichtet werden kann, die Erfüllung ihrer Aufgaben dadurch zu riskieren, dass sie einen Sicherheitsbaustein nicht anwenden darf.



Rechtsanwalt