# Meinhard Starostik

Rechtsanwalt

RA Starostik · Schillstraße 9 · 10785 Berlin


Landgericht Berlin
Littenstr. 12-12
10179 Berlin


Rechtsanwaltskanzlei:
Schillstraße 9 · 10785 Berlin
Tel.: 00 49 - 30 - 88 000 3 - 0
Fax: 00 49 - 30 - 88 000 346
Email: Kanzlei@Starostik.de
http://www.starostik.de
USt-ID-Nr. DE165877648

Zweigstelle und
Kanzlei vereidigter Buchprüfer:
Schwarzenberger Straße 7 · 08280 Aue
Tel.: 00 49 - 3771 - 564 700


Berlin, den 21.09.2017
Mein Zeichen: 45/08

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

In vorbezeichneter Angelegenheit wird zu dem Revisionsurteil des Bundesgerichtshofs wie folgt Stellung genommen:

**Das Revisionsurteil**

In erster Instanz hatte das Landgericht noch angenommen: „In rechtlicher Hinsicht ist der Begriff der Erforderlichkeit eng auszulegen (vgl. Spindler-Schuster, Recht der elektronischen Medien, 2. Auflage, § 15 Rn. 5). Nach Auffassung der Kammer umfasst er nicht den sicheren Betrieb der Seite, für den die Speicherung der IP-Adresse über das Ende des Nutzungsvorganges hinaus unter Umständen erforderlich ist."

Der zweite Leitsatz des Revisionsurteils lautet nunmehr: „§ 15 Abs. 1 TMG ist entsprechend Art. 7 Buchst. f der Richtlinie 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 (Fortführung von EuGH, 19. Oktober 2016, C-582/14, NJW 2016, 3579)." Die Einrichtungen des Bundes, die Online-Mediendienste anbieten, hätten „ein berechtigtes Interesse daran, die Aufrechterhaltung der Funktionsfähigkeit der von ihnen allgemein zugänglich gemachten Internetseiten über ihre konkrete Nutzung hinaus zu gewährleisten". Das Berufungsgericht habe aber noch „keine hinreichenden Feststellungen dazu getroffen, **ob die Speicherung der IP-Adressen des Klägers über das Ende eines Nutzungsvorgangs hinaus erforderlich ist, um im konkreten Fall die generelle Funktionsfähigkeit der jeweils in Anspruch genommenen Dienste zu gewährleisten**".

Der Begriff der „generellen Funktionsfähigkeit" eines Telemediums ist entsprechend § 15 Abs. 1 TMG dahin zu verstehen, dass die Inanspruchnahme des Telemediums möglich sein muss. Soweit der BGH den „Angriffsdruck", das „Gefahrenpotenzial" oder „Cyber-Angriffe wie ‚Denial-of-Service'-Attacken" anspricht, können nur Angriffsformen gemeint sein, wel-

che die generelle Funktionsfähigkeit und Nutzbarkeit des Telemediums beeinträchtigen. So können ‚Denial-of-Service'-Angriffe die Inanspruchnahme eines Telemediums extrem verlangsamen oder seine Verfügbarkeit insgesamt aufheben. Keine Auswirkung auf die generelle Funktionsfähigkeit haben dagegen beispielsweise Schwachstellenanalysen (Portscans) und erfolglose Einbruchsversuche. Eine weiter reichende Auslegung im Sinne der „IT-Sicherheit" allgemein hat der BGH nicht vorgenommen.

**Das weitere Verfahren**

Drei Fragen stellen sich dementsprechend für das weitere Verfahren:

1. Ist die Vorratsspeicherung der IP-Adresse des Klägers über das Ende eines Nutzungsvorgangs hinaus **geeignet**, um die generelle Funktionsfähigkeit der Telemedien der Beklagten zu gewährleisten?
2. Ist die Vorratsspeicherung der IP-Adresse des Klägers über das Ende eines Nutzungsvorgangs hinaus **erforderlich**, um die generelle Funktionsfähigkeit der Telemedien der Beklagten zu gewährleisten, oder gibt es dazu weniger eingreifende Mittel?
3. Ist es in Abwägung mit dem Interesse und den Grundrechten und -freiheiten der Nutzer **verhältnismäßig** deren IP-Adresse über das Ende eines Nutzungsvorgangs hinaus ohne Anlass auf Vorrat zu speichern, um die generelle Funktionsfähigkeit der Telemedien der Beklagten zu gewährleisten?

Es liegt nun zunächst an der Beklagten ihrer diesbezüglichen Darlegungs- und Beweislast zu genügen und substantiiert vorzutragen inwieweit eine Vorratsspeicherung von IP-Adressen geeignet und erforderlich sein soll um die generelle Funktionsfähigkeit der Telemedien der Beklagten zu gewährleisten. Die Beklagte mag auch dazu vortragen, wie hoch das „Gefahrenpotential" bei den einzelnen Telemedien des Bundes sein soll, sowie zu Art, Umfang und Wirkung von bereits erfolgten und etwa drohenden Angriffen sowie zu der Bedeutung der betroffenen Telemedien.

Einen Großteil des Vortrags dazu wird der Kläger der Beklagten zugestehen können – nicht jedoch dass ein Zusammenhang zwischen IP-Surfprotokollierung und Funktionsfähigkeit der Telemedien bestehen soll.

Was eine eventuelle Beweiserhebung angeht, kann das Landgericht das bereits eingeholte und bisher unverwertete Gerichtsgutachten nutzen und den Gerichtsgutachter mit weiteren Fragen beauftragen. In Betracht kommt auch eine mündliche Befragung des Sachverständigen. Zu einer komplett neuen Begutachtung oder gar einem Austausch des Gutachters besteht kein Anlass. Hier ist auch die ohnehin schon lange Verfahrensdauer zu berücksichtigen.

**Vortrag des Klägers**

In der Sache bleibt der Kläger bei seinem Vortrag:

1. Zur Eignung: Die Vorratsspeicherung der IP-Adresse des Klägers über das Ende eines Nutzungsvorgangs hinaus leistet keinen messbaren Beitrag zur Funktionsfähigkeit der Telemedien der Beklagten. Es gibt keinen Nachweis dafür, dass Webserver mit IP-Surfprotokollierung (und ggf. darauf aufbauender Maßnahmen) eine statistisch signifikant höhere Verfügbarkeit aufwiesen als fachgerecht eingerichtete Webserver ohne IP-Surfprotokollierung.
2. Zur Erforderlichkeit: Es gibt mildere Mittel als eine wahllose Vorratsspeicherung sämtlicher IP-Adressen um die Funktionsfähigkeit der Telemedien der Beklagten zu gewährleisten. Dazu gehören die fachgerechte Einrichtung und Instandhaltung von

Webservern, unter Umständen auch eine Speicherung der IP-Adresse nur von verdächtigen Zugriffen (und nicht auch von legitimen Benutzerzugriffen auf öffentlich verfügbare Informationen).

3. Zur Verhältnismäßigkeit: Selbst wenn eine wahllose Vorratsspeicherung sämtlicher IP-Adressen die Funktionsfähigkeit von Telemedien signifikant besser gewährleisten könnte (was bestritten wird), steht dieser hypothetische Nutzen vollkommen außer Verhältnis zu dem Schaden, den die Informations- und Meinungsfreiheit sowie das Recht auf informationelle Selbstbestimmung nehmen würden.

Zerstörte man das Recht sich als rechtschaffener Bürger im Netz ebenso unbeobachtet zu informieren und auszutauschen wie aus der Zeitung oder auf der Straße, würden Einzelpersonen, ganze Berufsgruppen und unsere Gesellschaft insgesamt unzumutbar belastet. Die große Vielzahl und Spezialisierung von Telemedien ermöglicht sogar noch weit tiefgründigere Einblicke in unsere Persönlichkeit, unser Privatleben, unsere Interessen und Vorlieben als die traditionellen, anonym nutzbaren Medien. Information und Beratung von Menschen in Not (z.B. Telefonseelsorge, Aidshilfe, Eheberatung), Recherche und Whistleblowing, politischer Aktivismus, Religion und Gesundheit – in all diesen Bereichen braucht unsere Gesellschaft Anonymität und ist ein wirklich freier, unbefangener Gebrauch von Grundrechten nur im Schutz der Anonymität möglich. Wer mit Nachteilen wegen des Inhalts seiner Internetnutzung rechnen muss, wird möglicherweise nicht mehr unbefangen von seiner Informations- und Meinungsäußerungsfreiheit im Internet Gebrauch machen. Eine Speicherung des Internet-Nutzungsverhaltens erlaubt die Rekonstruktion des Inhalts der gelesenen oder geschriebenen Informationen und hat damit eine noch weiter reichende Qualität als eine Speicherung von Verkehrs- oder Metadaten.

Der Bundesgerichtshof verkennt die Bedeutung der einschlägigen Grundrechte, wenn er einen „eher gering" wiegenden Grundrechtseingriff mit dem Argument annimmt, zur Zuordnung einer IP-Adresse durch die Beklagte komme es nur unter engen gesetzlich definierten Voraussetzungen: Der eigentliche Grundrechtseingriff liegt nicht erst in der Datenverwendung, sondern schon in der Datenerfassung. Schon die Vorratsdatenspeicherung wirkt abschreckend auf die freie Grundrechtsausübung, weil die Betroffenen eine spätere Verwendung der Daten befürchten müssen. Dazu gehören erfahrungsgemäß nicht nur legale Datenzugriffe, sondern auch das ständige Risiko von Datenverlust, Datenverkauf oder Datenmissbrauch durch Hacker oder Insider (einzelne Mitarbeiter), welches die Anlage einer Datenhalde schafft. Selbst zu den legalen Zugriffen gehören weitgehend voraussetzungslose Zugriffe durch Geheimdienste und außerdem Zugriffe durch Strafverfolger, die sich gegen zu Unrecht Verdächtigte richten können (falscher Verdacht). § 113 Abs. 3 TKG, der keinen Richtervorbehalt kennt, dürfte jährlich zu IP-Abfragen in fünf- bis sechsstelliger Zahl führen und kann mitnichten als enger Rahmen angesehen werden. Im Übrigen hatte das Landgericht bereits erkannt, dass die Beklagte die IP-Adresse des Klägers unter Umständen auch ohne IP-Abfrage zuordnen kann (z.B. aufgrund eines ausgefüllten Kontakt- oder Bestellformulars oder im Fall einer namentliche Registrierung).
Die Erwägung des Bundesgerichtshof zum Gewicht des Grundrechtseingriffs ist für das Landgericht nicht verbindlich, weil sie nicht kausal für die Aufhebung des Urteils ist (vgl. MüKoZPO/Krüger ZPO § 563 Rn. 9). Es handelt sich um ein obiter dictum.

Die Auffassung des Bundesgerichtshofs, bei der Abwägung sei der „Gesichtspunkt der Generalprävention gebührend zu berücksichtigen", ist mit dem Gesetz und höherrangigem Recht unvereinbar. § 15 TMG erlaubt eine Datenverarbeitung nur zur Gewährleistung der Funktionsfähigkeit der Telemedien des Anbieters, nicht aber zur generellen Abschreckung von Computerdelikten. Ein solcher Zweck wäre auch mit EU-Datenschutzrecht unvereinbar, denn dieses erlaubt eine Datenverarbeitung nur im berechtigten Interesse des Verarbeiters selbst und nicht in einem gesellschaftlichen oder staatlichen Generalinteresse. Im Übrigen bestreitet der Kläger, dass einer Surfprotokollierung eine abschreckende Wirkung zukommt,

da sich eine Rückführung der IP-Adresse über Zwischenserver leicht verhindern lässt. Wenn Zugriffe etwa über russische oder chinesische Server erfolgen, verliert sich jede Spur.
Die Erwägung des Bundesgerichtshof zur Generalprävention ist für das Landgericht nicht bindend, weil sie nicht kausal für die Aufhebung des Urteils ist (vgl. MüKoZPO/Krüger ZPO § 563 Rn. 9). Es handelt sich um ein obiter dictum.

Das Bundesverfassungsgericht hat bereits in seinem Urteil zur Vorratsdatenspeicherung betont, dass die Internetnutzung nicht inhaltlich festgehalten und damit rekonstruierbar bleiben darf (BVerfGE 125, 260, 348, Abs. 270). Die §§ 11 ff. TMG verpflichteten die Diensteanbieter grundsätzlich zur Löschung von nicht für die Abrechnung erforderlichen Daten und verhinderten so, dass die Internetnutzung inhaltlich in allgemeinen kommerziellen Datensammlungen festgehalten wird und damit rekonstruierbar bleibt (a.a.O.). Die Vorratsspeicherung von Verkehrsdaten nach § 113a TKG bleibe „eine begrenzte Ausnahme" (a.a.O.). § 15 TMG muss dementsprechend grundrechtskonform so ausgelegt und angewandt werden, dass die Löschung von nicht für die Abrechnung erforderlichen Daten der Grundsatz bleibt.

Zwischenzeitlich hat der EuGH auch im Telekommunikationsbereich eine anlasslose Vorratsdatenspeicherung als unverhältnismäßig und grundrechtswidrig verworfen, wenn sie Personen erfasst, die in keiner auch nur mittelbaren Beziehung zu irgend einer Gefahr oder Straftat stehen (EuGH NJW 2014, 2169, Abs. 58 f.; NJW 2017, 717, Abs. 105 ff.). Diese Abwägung für das Spannungsfeld Verbindungsdaten vs. Strafverfolgung getroffen wurde, muss erst recht für das Spannungsfeld Inhaltsdaten vs. technische Funktionsfähigkeit gelten. Die IP-Adresse, die auf die von einer Person in Anspruch genommenen Telemedien schließen lässt, gibt über den Inhalt der Internetnutzung, über private Vorlieben und Schwächen Aufschluss und ist ungleich sensibler als Telekommunikationsverbindungsdaten. Und das Interesse an einer besseren Funktionsfähigkeit eines Internetservers wiegt ungleich geringer als das öffentliche Interesse an der Verfolgung schwerer Straftaten. Der EuGH hat inzwischen auch für Fluggastdaten klargestellt, dass eine wahllose Vorratsspeicherung des Verhaltens beliebiger Personen unverhältnismäßig ist (EuGH vom 26.07.2017 - Gutachten 1/15, Abs. 205 ff.).

Vor diesem Hintergrund gilt für die Abwägung bei europarechtskonformer Auslegung im Einklang mit der EU-Grundrechtecharta: Es ist unverhältnismäßig, wegen der allgemeinen Möglichkeit von Störungen der Funktionsfähigkeit das Nutzungsverhalten auch aller rechtmäßig handelnder Nutzer personenbezogen aufzuzeichnen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit Störungen stehen könnte.

Sollte das Landgericht daran Zweifel haben, wird eine Vorlage an den EuGH zur Auslegung der EU-Grundrechtecharta beantragt.

In Anlehnung an Edward Snowden meint der Kläger: Niemand hat das Recht, alles, was wir im Netz sagen, und alles, was wir tun, aufzuzeichnen. Als Generation Internet haben wir das Recht, uns im Netz ebenso unbeobachtet und unbefangen informieren zu können, wie es unsere Eltern aus Zeitung, Radio oder Büchern konnten. Europa muss der NSA-Methode einer Totalerfassung des digitalen Lebens eine klare Absage erteilen und den Grundrechten auf Informations- und Meinungsfreiheit im Internet zur Geltung verhelfen.

Da das grundrechtlich gebotene Abwägungsergebnis bereits feststeht, kann aus Sicht des Klägers die tatsächliche Frage der Eignung und Erforderlichkeit einer IP-Surfprotokollierung offen bleiben und kann der Klage schon aus rechtlichen Gründen ohne Beweisaufnahme stattgegeben werden.

Beglaubigte und einfache Anschrift anbei.

Mit freundlichen Grüßen

Meinhard Starostik
- Rechtsanwalt -