**Anmerkung zu OLG Düsseldorf, Beschluss vom 07.03.2013 - I-20 W 121/12, I-20 W 5/13 - Keine Speicherung auf Zuruf**

**-- erschienen in Kommunikation & Recht (K&R) Heft 5/2013, S. 344 ff. --**

Dr. jur. Dipl.-Inf. Reto Mantz, Richter, LG Frankfurt a. M.*

Mit den vorliegenden Entscheidungen hat das OLG Düsseldorf (erneut) klargestellt, dass § 101 UrhG allein einen Auskunftsanspruch regelt, und dass hieraus keine Pflicht zur Erhebung und Speicherung von Daten erwächst. Die Entscheidungen des OLG Düsseldorf führen dabei die Linie des Gerichts fort und reihen sich in die absolut h. M. der Rechtsprechung ein.[1]

## I. Hintergrund

Jedes Gerät im Internet verfügt über eine eindeutige Adresse, die sog. IP-Adresse. Wer sich im Internet bewegt, ist daher im Grunde über seine IP-Adresse identifizierbar.[2] Die Identifizierung wird aber dadurch problematisch, dass Access-Provider ihren Kunden immer wieder wechselnde IP-Adressen zuweisen (sog. „dynamische IP-Adressen"). Die Zuweisung erfolgt in aller Regel nur für die Dauer einer Verbindung („Session"), wobei meist nach maximal 24 Stunden eine Zwangstrennung und ggf. Neuzuweisung durchgeführt wird. Aus diesem Grunde sind Rechteinhaber, wenn sie eine (potentielle) Rechtsverletzung über das Internet feststellen, darauf angewiesen, dass Access-Provider nachträglich einem Kunden die festgestellte IP-Adresse zu einem bestimmten Zeitpunkt zuordnen können. Dies ist aber nur möglich, wenn Access-Provider bewusst und zielgerichtet Informationen darüber erheben und speichern, welchem Nutzer sie zu welchem Zeitpunkt welche IP-Adresse zugewiesen hatten.

Der Großteil der deutschen Access-Provider erhebt und speichert diese Zuordnung der IP-Adressen für einen gewissen Zeitraum auch bei sog. Flatrates, also pauschal abgegoltenem Internetzugang. Der BGH hat diese in der Literatur kritisierte Praxis im Jahre 2011 für rechtmäßig gehalten und festgestellt, dass Access-Provider zum Zwecke der Störungs- und Missbrauchserkennung und -beseitigung nach § 100 Abs. 1 TKG die Zuordnung der IP-Adressen für einen Zeitraum von bis zu sieben Tagen speichern dürfen.[3] Einige Provider gehen über diese Vorgabe noch hinaus,[4] wobei es sich hierbei um freiwillige Speicherungen handelt, die – aber nur bis zu sieben Tagen – für zulässig gehalten werden. Eine Pflicht zur Speicherung hingegen sieht auch § 100 Abs. 1 TKG nicht vor.[5]

Auf der anderen Seite erheben und speichern einige Access-Provider die Zuordnung der dynamischen IP-Adressen nicht. Stellen Rechteinhaber (potentielle) Rechtsverletzungen von

---

* Mehr über den Autor erfahren Sie auf S. VIII.

1 Eine Übersicht zur Rechtsprechung zum § 101 UrhG findet sich unter http://www.retosphere.de/offenenetze/101urhg.

2 Zu den (möglichen) Änderungen, die sich durch den Wechsel des Format der IP-Adressen von Version 4 auf Version 6 (IPv6) *Wegener/Heidrich*, CR 2011, 479.

3 BGH, 13. 1. 2011 – III ZR 146/10, K&R 2011, 193 ff.; ebenso die vorgehenden Instanzen OLG Frankfurt a. M., 16. 6. 2010 – 13 U 105/07, MMR 2010, 645; LG Darmstadt, 6. 6. 2007 – 10 O 562/03; s. auch Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten v. 19. 12. 2012, http://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/LeitfadenZumSpeichernVonVerkehrsdaten.pdf?__blob=publicationFile; kritisch *Breyer*, MMR 2011, 573 m. w. N.

4 Übersicht der Speicherdauer verschiedener Access Provider unter http://wiki.vorratsdatenspeicherung.de/Speicherdauer.

5 LG München I, 12. 1. 2012 – 7 HK O 1398/11, CR 2012, 603 m. Anm. *Mantz*.

Kunden dieser Access-Provider fest, kann eine nachträgliche Zuordnung nicht mehr erfolgen. In solchen Fällen müssten daher die Rechteinhaber noch während der laufenden Session – also bereits Minuten bis maximal wenige Stunden nach der beobachteten potentiellen Rechtsverletzung – die Information von Access-Providern herausverlangen. Da § 101 Abs. 9 UrhG jedoch zur Kontrolle des erheblichen Eingriffs ins Fernmeldegeheimnis nach Art. 10 GG die Notwendigkeit eines richterlichen Beschlusses vorsieht, kommen Rechteinhaber in dieser Situation regelmäßig zu spät.

Auch im vorliegenden Fall hatte die Antragsgegnerin die Zuordnung der IP-Adressen nicht über das Ende der Verbindung hinaus gespeichert. Das Ziel der Verfahren war daher, die Antragsgegnerin per gerichtlicher Anordnung zur Erhebung und Speicherung der Daten zu zwingen. Dadurch sollte die Möglichkeit eröffnet werden, der Antragsgegnerin praktisch in Echtzeit IP-Adressen (der potentiellen Rechtsverletzer) zu übermitteln, für die sie bis zur Entscheidung des anschließend nach § 101 Abs. 9 UrhG anzurufenden Gerichts die Daten vorhalten sollte. Für dieses Vorgehen hat sich die Bezeichnung „Speicherung auf Zuruf" herausgebildet.

## II. Bisheriger Stand der Rechtsprechung

Eine solche Pflicht des Access-Providers zur „Speicherung auf Zuruf" hatten verschiedene Gerichte in den Jahren 2009 und 2010 noch angenommen.[6] Dabei hatte z. B. das LG Hamburg argumentiert, dass die Auskunftspflicht ein gesetzliches Schuldverhältnis begründe. Eine aus diesem Schuldverhältnis erwachsende Speicherpflicht sei erforderlich, um die Auskunft überhaupt erteilen zu können.[7] Dieser Ansatz ist jedoch verfehlt. Auskunftspflichten können sich aus einer Vielzahl von Normen ergeben, beispielsweise aus § 259 BGB. Aus einer Auskunftspflicht folgt aber gerade nicht auch eine Speicherpflicht.[8] Sie hätte im Ergebnis zur Folge, dass über einen (ggf. ungewissen) Auskunftsanspruch die datenschutzrechtlichen Grundsätze des Verbots mit Erlaubnisvorbehalt, der Datenvermeidung und der Datensparsamkeit vollständig ausgehebelt würden, da jede Erhebung und Speicherung auf eine drohende Pflicht zur Auskunft gestützt werden könnte.

Folgerichtig lehnte das OLG Frankfurt bereits im Jahr 2009 eine Speicherpflicht auf Zuruf ab.[9] Dieser Auffassung folgten u. a. OLG Hamm,[10] OLG Düsseldorf[11] und OLG München.[12] Im Jahr 2010 gab zudem auch das LG Hamburg seine zuvor vertretene Auffassung ausdrücklich auf.[13]

## III. Entscheidungen des OLG Düsseldorf

Die hiesigen Entscheidungen des OLG Düsseldorf führen die eben dargestellte Rechtsprechung fort. Dabei stellt das OLG Düsseldorf ebenfalls darauf ab, dass aus der Auskunftspflicht keine Speicherpflicht folge. Das OLG Düsseldorf unterscheidet dabei richtigerweise genau zwischen dem reinen „Anfallen", dem Erheben (§ 3 Abs. 3 BDSG) und dem Speichern

---

6 OLG Karlsruhe, 1. 9. 2009 – 6 W 47/09, K&R 2009, 731 ff.; OLG Hamburg, 17. 2. 2010 – 5 U 60/09, MMR 2010, 338; LG Hamburg, 11. 3. 2009 – 308 O 75/09, MMR 2009, 570 m. krit. Anm. *Schulz zur Wiesche*; LG Bielefeld, 19. 11. 2009 – 4 OH 740/09.

7 LG Hamburg, 11. 3. 2009 – 308 O 75/09, MMR 2009, 570.

8 LG München I, 12. 1. 2012 – 7 HK O 1398/11, CR 2012, 603.

9 OLG Frankfurt a. M., 17. 11. 2009 – 11 W 53/09, MMR 2010, 62 m. zust. Anm. *Maaßen*.

10 OLG Hamm, 2. 11. 2010 – 4 W 119/10, K&R 2011, 355 ff.

11 OLG Düsseldorf, 15. 3. 2011 – I-20 U 136/10, MMR 2011, 546.

12 OLG München, 21. 11. 2011 – 29 W 1939/11, K&R 2012, 223 ff.; ebenso LG München, 22. 8. 2011 – 21 O 13977/11.

13 LG Hamburg, 20. 10. 2010 – 308 O 320/10, MMR 2011, 475.

(§ 3 Abs. 4 Nr. 1 BDSG) von Daten. Das reine Anfallen von Daten durch einen technisch bedingten Vorgang, hier der IP-Adressen beim Access-Provider, sieht das Gericht noch nicht als Erheben der Daten an, weil die Daten nicht tatsächlich und zielgerichtet zur Kenntnis genommen werden. Da die Antragsgegnerin die Daten bisher noch nicht derart zielgerichtet erhoben, geschweige denn gespeichert hatte, verlangt das OLG Düsseldorf konsequent dem Grundsatz des Verbots mit Erlaubnisvorbehalt nach § 4 Abs. 1 BDSG folgend eine Rechtsgrundlage für die Erhebung zum einen und die Speicherung der Daten zum anderen. Weiter verlangt es unter Bezugnahme auf die Vorratsdatenspeicherungs-Entscheidung des BVerfG[14] zum Ausgleich der betroffenen Interessen zwingend eine gesetzliche Regelung. Eine solche sieht es weder in § 101 Abs. 2 UrhG, noch in § 96 TKG. Solange der Gesetzgeber eine solche explizite Regelung nicht schaffe, sei eine Speicherpflicht nicht gegeben.

## IV. Folgen für die Praxis

Die Entscheidungen des OLG Düsseldorf stellen, obwohl sie im Grunde nur die bereits vorherrschende Meinung bestätigen, auch im Jahr 2013 noch ein wichtiges Signal dar. Es besteht nämlich gerade bei kleinen Access-Providern häufig eine erhebliche Unsicherheit im Hinblick auf diejenigen Pflichten, die der Betrieb eines Telekommunikationsdienstes mit sich bringt. Diese Pflichten können durchaus vielfältig sein: Meldepflicht, Kundenschutz, Sicherheitsmaßnahmen etc. Bei einigen Providern besteht aber darüber hinaus der Eindruck, dass sie Daten über ihre Nutzer speichern müssten, um im Falle von Rechtsverletzungen durch ihre Kunden – im Wege der Auskunft an Rechteinhaber – reagieren zu können. Nur wer (potentielle) Rechtsverletzer identifiziere und ausliefere, könne sich vom Damoklesschwert der Störerhaftung[15] für die Rechtsverletzungen der Nutzer befreien. Dieser (falschen) Auffassung ist kürzlich das LG München I entschieden entgegengetreten und hat festgestellt, dass für den Access-Provider eine Pflicht zur Identifizierung der Nutzer nicht besteht.[16] Eine solche kann weder auf die Auskunftspflicht nach § 101 Abs. 2 UrhG, auf §§ 96, 109, 112 oder 113 TKG noch auf eine – aufgrund der Privilegierung des § 8 TMG im Übrigen ohnehin kaum vorliegende – eventuelle Störerhaftung gestützt werden. Dies gilt sogar dann, wenn die Rechtsverfolgung durch die Nichtidentifizierbarkeit erschwert oder verhindert wird.

In diesem Sinne sind auch die vorliegenden Entscheidungen zu verstehen: Wer keine Informationen über die Vergabe von dynamischen IP-Adressen an seine Nutzer erhebt und/oder speichert, verletzt nicht etwa Pflichten aus TKG, UrhG oder anderen Normen. Er verhält sich vielmehr gesetzestreu und kommt im Ergebnis seinen Pflichten zum Schutz des Fernmeldegeheimnisses und des Datenschutzes geradezu vorbildlich nach. Es bleibt zu hoffen, dass sich diese Erkenntnis unter den betroffenen Telekommunikationsdiensteanbietern verbreiten wird.

---

[14] BVerfG, 24. 01. 2012 – 1 BvR 1299/05, K&R 2012, 274 ff.

[15] S. dazu BGH, 12. 5. 2010 – I ZR 121/08, K&R 2010, 492 ff. = MMR 2010, 565 – Sommer unseres Lebens m. Anm. *Mantz*.

[16] LG München I, 12. 1. 2012 – 7 HK O 1398/11, CR 2012, 603 m. Anm. *Mantz*.