Anmerkung zu LG Berlin, Urt. v. 31.1.12013 – 57 S 87/08: Personenbezug von IP-Adressen, ZD 2013, 618

- zuerst erschienen in ZD 2013, 625 -

Leitsätze:

1. Soweit der Betreiber einer Webseite nur (dynamische) IP-Adressen ohne den zugehörigen Zeitpunkt des Zugriffs speichert, stellt die IP-Adresse kein personenbezogenes Datum i.S.v. §§ 12 TMG, 3 BDSG dar.

2. Speichert der Betreiber einer Webseite die (dynamische) IP-Adresse mit dem zugehörigen Zeitpunkt des Zugriffs, ist diese nur dann personenbezogen, wenn dem Anbieter die Bestimmung der Person des Nutzers technisch und rechtlich möglich ist, z.B. weil der Nutzer in einem Formular auf der Webseite Klarnamen oder E-Mail-Adresse angegeben hat (relativer Personenbezug).

3. Die Herstellbarkeit eines Personenbezugs bezogen auf ein ansonsten nicht-personenbezogenes Datum in einem Ermittlungs- oder Strafverfahren oder einem Auskunftsverfahren nach § 101 UrhG führt grundsätzlich nicht dazu, dass das Datum für sich bereits als personenbezogen anzusehen ist.

4. Es schließt den Personenbezug der (dynamischen) IP-Adresse nicht aus, wenn die vom Nutzer in einem Formular angegebenen zu einem Personenbezug führenden Daten und die IP-Adresse getrennt gespeichert werden.

5. Der Erlaubnistatbestand des § 100 TKG ist nur auf Telekommunikationsdiensteanbieter und nicht auf Telemediendiensteanbieter anwendbar.

- 625 -

Anmerkung

Die Diskussion um die Frage, ob (dynamische) IP-Adressen auch für andere als den Access Provider personenbezogene Daten i.S.d. § 3 BDSG darstellen und damit unter das Regime des Datenschutzes fallen, ist bereits seit mehreren Jahren im Gange. Interessanterweise gibt es hierzu bisher trotzdem nur instanzgerichtliche Entscheidungen (für Personenbezug AG Berlin-Mitte K&R 2007, 600; LG Berlin MMR 2007, 799; LG Berlin CR 2006, 418; VG Wiesbaden MMR 2009, 428; gegen Personenbezug AG München MMR 2008, 860; LG Wuppertal, Beschl. v. 19.10.2010 – 26 Qs 10 Js 1977/08, BeckRS 2010, 25680; wohl auch OLG Hamburg MMR 2011, 281, 282). Das *LG Berlin* hat sich mit seiner Entscheidung umfassend mit der Thematik beschäftigt und sich nun im Ergebnis der Theorie des relativen Personenbezugs angeschlossen.

1. Im Kern geht es bei dem Streit um die Definition der Bestimmbarkeit des Personenbezugs von Daten speziell in Bezug auf (dynamische) IP-Adressen: Nach § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben über eine *bestimmte* oder *bestimmbare* natürliche Person. „Bestimmt“ in diesem Sinne ist die Person, wenn sich aus allen der verantwortlichen Stelle zur Verfügung stehenden Daten die Person unmittelbar ableiten lässt

(*Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 3 Rn. 10), beispielsweise, wenn die Stelle auch den Namen der Person erhoben und gespeichert hat. Bei der „Bestimmbarkeit" wiederum wird in der Regel darauf abgestellt, ob die konkrete Person mit Hilfe anderer Informationen und Zusatzwissen ermittelt werden kann (*Krüger/Maucher*, MMR 2011, 433). Dabei kann im Sinne einer Negativabgrenzung auf den in § 3 Abs. 6 BDSG definierten Begriff der Anonymität zurückgegriffen werden, da ein anonymes Datum nie, ein nicht-anonymes Datum stets als personenbezogen anzusehen ist (vgl. Simitis-*Dammann*, BDSG, 7. Aufl. 2011, § 3 Rn. 23). Nach § 3 Abs. 6 BDSG ist Anonymität anzunehmen, wenn die Einzelangaben nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Einen ähnlichen Ansatz wählt auch die Datenschutzrichtlinie 95/46/EG („RL") (Simitis-*Dammann*, a.a.O., § 3 Rn. 24), indem sie von „vernünftigerweise von der verantwortlichen Stelle eingesetzten Mitteln" spricht (Erwägungsgrund 26 der RL). Der Streit entbrennt nun hauptsächlich daran, ob das für die Bestimmbarkeit betrachtete Zusatzwissen generell irgend einer Person zur Verfügung stehen (absoluter Personenbezug) soll, oder ob nur das für die konkrete verantwortliche Stelle zugängliche Zusatzwissen Beachtung findet (relativer Personenbezug). Weiter dreht sich der Streit bei der Bestimmbarkeit um die Kriterien, die für die Verhältnismäßigkeits- bzw. Vernünftigkeitsprüfung gelten.

2. Das LG Berlin hat sich nun den Vertretern der Theorie des relativen Personenbezugs angeschlossen. Hier sollen die Argumente in diesem Streit nicht wiederholt werden (s. dazu *Karg*, MMR-Aktuell 2011, 315811; *Karg*, MMR 2011, 345; *Krüger/Maucher*, MMR 2011, 433; *Meyerdierks*, MMR 2009, 8; *Lundevall/Tranvik*, ZD-aktuell 2012, 03004; *Sachs*, CR 2010, 547; jew. m.w.N.), denn das *LG* hat auch darüber hinaus wichtige Feststellungen getroffen.

a. Das *LG* hat sich intensiv mit den für Telemediendiensteanbieter anwendbaren datenschutzrechtlichen Erlaubnistatbeständen befasst. Hervorzuheben ist hier insbesondere, dass die Verwendung eines Formulars auf einer Webseite, ggf. unter Angabe personenbezogener Daten wie des Klarnamens oder der E-Mail-Adresse, für sich keine Einwilligung in die Verwendung der IP-Adresse darstellt. Wer auf einer Webseite personenbezogene Daten erhebt, muss daher für die Speicherung der ansonsten anfallenden Daten stets eine ausdrückliche Einwilligung einholen, die den Voraussetzungen der §§ 13 TMG, 4a BDSG genügt.

b. Weiter hat das *LG* in begrüßenswerter Klarheit festgestellt, dass auch vor dem Hintergrund von § 15 Abs. 1 TMG die Speicherung von (z.B. durch Zusatzwissen personenbezogenen) IP-Adressen über den reinen Nutzungsvorgang hinaus nicht erforderlich und damit ohne andere Rechtfertigung unzulässig ist, und weiter § 100 TKG hier keine Anwendung findet. In diesem Zusammenhang ist darauf hinzuweisen, dass bei demjenigen, der IP-Adressen nicht zusätzlich (z.B. in einer Log-Datei) speichert oder zusätzlich verarbeitet, nach Auffassung des *OLG Düsseldorf* die IP-Adressen nur zur Abwicklung der Verbindung notwendigen Daten „anfallen" und damit bereits nicht nach § 3 Abs. 3 BDSG erhoben werden (OLG Düsseldorf K&R 2013, 344 m. Anm. *Mantz*).

c. Ebenfalls begrüßenswert ist die Feststellung des LG, dass eine organisatorische Trennung von Daten der Bestimmbarkeit einer Person nicht entgegensteht. Es reicht daher nicht aus, IP-Adressen separat von dem zur Bestimmbarkeit verwendbaren Zusatzwissen (hier der Daten aus dem Web-Formular) zu speichern, um den Personenbezug auszuschließen.

Maßstab ist daher – in Einbeziehung aller Datenquellen der verantwortlichen Stelle –, ob sich unter Zusammenführung der Quellen ein Personenbezug herstellen lässt.

Diese Feststellung ist einer der Kernpunkte des Urteils. Denn die Überlegungen des *LG* sind wohl auch übertragbar auf die Datenverarbeitung in Konzernen. Auch wenn einzelne Unternehmen eines Konzerns jeweils als eigene verantwortliche Stelle zu betrachten sind (*Gola/Schomerus*, a.a.O., § 27 Rn. 4), kann auch im Konzern eine rein organisatorische Trennung von Daten nicht ausreichen, wenn ein Datenaustausch unter den Konzernunternehmen (auch nur theoretisch) möglich ist. Selbst bei strikter (ggf. vertraglich vereinbarter) Trennung kann dies problematisch sein, wenn mehrere Konzernunternehmen – wie es häufig der Fall ist – ihre Daten im selben Rechenzentrum einer Konzerntochter speichern und verarbeiten, und im Rechenzentrum nicht ebenfalls eine absolute (rechtliche, idealerweise auch physische und personelle) Trennung der Daten sichergestellt wird.

d. Darüber hinaus hat das *LG* richtigerweise die von der Beklagten geäußerte Auffassung zurückgewiesen, dass es erforderlich sei, über die IP-Adresse den tatsächlichen Nutzer zu identifizieren. Eine IP-Adresse ist nämlich schon personenbezogen, wenn sie sich *einer* Person eindeutig zuordnen lässt, z.B. dem Anschlussinhaber. Dies gilt selbstverständlich auch für die hinter einer statischen IP-Adresse stehende Person, wobei statische IP-Adressen nach absolut h.M. personenbezogen sind, wenn sie auf eine natürliche Person registriert sind (Art. 29-Gruppe, WP 136, S. 20; *Hoeren*, ZD 2011, 3, 4; *Eckhardt*, CR 2011, 339, 340; Simitis-*Dammann*, a.a.O., § 3 Rn. 38; jew. m.w.N.; differenzierend *Gerlach*, CR 2013, 478, 480).

3. Bedenklich sind die Ausführungen des *LG* in Bezug auf den Hauptantrag des Klägers, wenn hieraus der Schluss gezogen wird, dass (dynamische) IP-Adressen außer beim Zugangsanbieter *generell* nicht personenbezogen sind. Im vorliegenden Fall und bei der Mehrzahl der im Internet betriebenen Webseiten wird zutreffen, dass beim Betreiber das erforderliche Zusatzwissen, um den Nutzer anhand der IP-Adresse zu identifizieren, nicht unmittelbar vorliegt. Andererseits hat das *LG* festgestellt, dass beim Anbieter alles Zusatzwissen zu berücksichtigen ist, z.B. könne über einen thematischen Bezug eines „anonymen“ Surfers ein Bezug zur vorher durchgeführten Nutzung unter Klarnahmen hergestellt werden.

Diese Sichtweise wird insbesondere im Hinblick auf Betreiber von großen Webdiensten relevant, kann aber auch auf Webseiten von Online-

Shops oder großen Unternehmen zutreffen. Im Zusammenhang mit dem Streit um IP-Adressen wird nämlich häufig übersehen, dass beim Surfen im Internet der Betreiber nicht nur die IP-Adresse erhält. Das Gerät des Nutzers verrät bei Aufruf einer Webseite viele weitere Informationen, z.B. Cookies, Browser-Version, Ausstattung des Geräts, Fonts etc. Zusätzlich haben viele Unternehmen heutzutage solche Mengen an Daten (und damit Zusatzwissen im Sinne von § 3 BDSG) zur Verfügung – oder können sie für vergleichsweise geringe Beträge bei entsprechenden Dienstleistern einkaufen –, dass die Unmöglichkeit der Bestimmbarkeit des Nutzers im Einzelfall immer unwahrscheinlicher wird. So sind

Unternehmen heute auf Basis ihrer Daten in der Lage, Nutzer wiederzuerkennen, selbst wenn sie unterschiedliche Geräte verwenden (vgl. *Miller/Sengupta*, New York Times v. 5.10.2013, http://www.nytimes.com/2013/10/06/technology/selling-secrets-of-phone-users-to-advertisers.html). Kann der Anbieter auf Standortdaten zugreifen, lässt sich zudem mit hoher Wahrscheinlichkeit der Wohnort und ggf. der Arbeitsplatz ermitteln. Teilweise kann über die Daten auch eine Verknüpfung mit im Internet verfügbaren Profilen (z.B. Twitter oder Facebook Open Graph) hergestellt werden, durch die dann eine Identifizierung möglich wird. In der Summe kann bei großen Datenmengen mit hoher Wahrscheinlichkeit auf die Identität wenigstens eines Teils der Nutzer geschlossen werden (vgl. *Rubinstein*, Big Data: The End of Privacy or a New Beginning?, N.Y.U. Public Law & Legal Theory Working Papers, Paper No. 357, (2012), http://lsr.nellco.org/nyu_plltwp/357; zur Deanonymisierung von Daten mit Fallbeispielen *Ohm*, Broken Promises of Privacy, UCLA Law Review, Vol. 57 (2010), 1701 ff., http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006). Die hierfür erforderlichen Rechenkapazitäten sind zudem auch für kleinere Unternehmen als Google & Co. über Cloud-Dienste leicht abrufbar. Außerdem entdecken Unternehmen zunehmend ihre „Datenschätze" und entwickeln Modelle, diese selbst auszunutzen oder zu kommerzialisieren (so bspw. bei TK-Anbietern, dazu *Mantz*, K&R 2013, 7). Vor diesem Hintergrund dürften für Anbieter wie Google, Facebook usw., ebenso wie für Betreiber großer Werbenetzwerke alle Daten inklusive der IP-Adresse personenbezogen sein, wenn sie nicht sicher (z.B. durch starke Aggregation) anonymisiert wurden. Auf dieser Sammlung von Daten und der Wiedererkennung von Nutzern beruht letztlich das Geschäftskonzept vieler großer Internetunternehmen, die dementsprechend kein Interesse an der Anonymisierung (und damit Entwertung) ihrer Daten haben. In diesem Zusammenhang stellt die IP-Adresse nur ein (weiteres) Mosaik-Stück zur Identifizierung des Nutzers dar.

4. Weiter kann die Auffassung des *LG*, dass die Durchführung eines Auskunftsverfahrens zur Ermittlung der Identität des Anschlussinhabers für den Anbieter einer Webseite eine so hohe Hürde darstelle, und daher i.S.v. § 3 BDSG als unverhältnismäßig anzusehen sei, durchaus mit einem Fragezeichen versehen werden. Das *LG* bezieht dabei insbesondere auf die gesetzlichen Anforderungen, die für solche Auskunftsverfahren bestehen. Der Zugangsanbieter sei nämlich datenschutzrechtlich daran gehindert, die relevanten Daten an Dritte zu übermitteln. Die entsprechenden Datenschutznormen sähen hierfür hohe Hürden vor. Insbesondere beim Auskunftsverfahren nach § 101 UrhG sei nach § 101 Abs. 9 UrhG ein Richtervorbehalt vorgesehen.

Die Zusammenführung des Wissens verschiedener verantwortlicher Stellen hindert die Bestimmbarkeit, wenn dem Zusammenbringen der Daten Hürden von einer solchen Qualität entgegenstehen, dass damit vernünftigerweise praktisch nicht zu rechnen ist (Simitis-*Dammann*, a.a.O, § 3 Rn. 26). Tatsächlich hat sich aber gerade das Auskunftsverfahren nach § 101 UrhG zu einem solchen Massenverfahren entwickelt (vgl. OLG Frankfurt GRUR-RR 2009, 407; OLG Köln GRUR-RR 2009, 9; *Sankol*, MMR 2008, 836, 838; *Hoffmann*, MMR 2009, 655, 656; *Malatidis*, MMR-aktuell 2012, 338259: Abfrage tausender IP-Adressen pro Antrag), dass die Gerichte hier allenfalls eine kursorische Prüfung durchzuführen vermögen. Die Effektivität des Richtervorbehalts wird auch vor diesem Hintergrund bereits in Zweifel gezogen (*Gusy*, ZRP 2003, 275: „Der Richtervorbehalt wird seinem rechtsstaatlichen Sinn nicht gerecht" m.N. zu rechtstatsächlichen Untersuchungen; ebenso *Stadler*, ZRP 2013, 179). Ferner ist im Hinblick auf die vom *LG* angesprochene Auskunft nach § 113 TKG zu berücksichtigen, dass der Zugangsanbieter eine Kontrollbefugnis nur für formale Anforderungen hat (BeckTKG- *Eckhardt*, 4. Auflage 2013, § 113 TKG, Rn. 48 m.w.N.). Auch ist zu beachten, dass neben den Daten der Zugangsanbieter auch andere Datenquellen

kommerzieller Unternehmen inklusive IP-Adressen mit Zugangszeitpunkt existieren, generiert z.B. durch die Verfolgung von Nutzern über mehrere Webseiten hinweg durch große Werbenetzwerke, Facebook etc., auf die Unternehmen gegen entsprechende Bezahlung zugreifen können. Es ist daher unklar, ob die Hürden hier tatsächlich derart hoch sind, dass *vernünftigerweise* nicht mit einem Zugriff zu rechnen ist. In der vom *LG* dargestellten Generalität lässt sich die Formel, dass nur legal verfügbares Wissens einzubeziehen sei, daher kaum halten (ebenso Simitis-*Dammann*, a.a.O., § 3 Rn. 28).

5. Das *LG Berlin* hat die Revision zugelassen. Möglicherweise wird der Streit daher endlich einer höchstgerichtlichen Klärung zugeführt. Unabhängig davon sollte – auch unter Zugrundelegung der relativen Theorie – trotzdem im konkreten Einzelfall überlegt werden, ob eine Speicherung von IP-Adressen nicht soweit wie möglich unterbleiben kann. Dabei sollte mit Blick auf das eigene Angebot insbesondere hinterfragt werden, warum eine Speicherung überhaupt erfolgt, und ob auf die Daten auch verzichtet werden kann. Wer unbedacht die IP-Adressen aller Nutzer speichert, speichert dabei nämlich mit hoher Wahrscheinlichkeit auch statische IP-Adressen (Art. 29-Gruppe, WP 136, S. 20, WP 159, S. 8). Von diesen ist jedenfalls ein Teil durch natürliche Personen registriert. In praktisch jeder IP-Adressensammlung dürften sich damit eindeutig personenbezogene Daten befinden. Nachdem die datenschutzrechtlichen Regelungen auch des TMG teilweise als Marktverhaltensregelungen i.S.d. UWG angesehen werden (OLG Hamburg ZD 2013, 511 m. Anm. *Schaub*; a.A. KG Berlin GRUR-RR 2013, 123; s. dazu auch *Spies*, MMR-aktuell 2011, 316402; *Rosenbaum/Tölle*, MMR 2013, 209, 211), werden mittlerweile vermehrt wettbewerbsrechtliche Abmahnungen wegen der Speicherung von IP-Adressen ausgesprochen. Zwar nimmt die Entscheidung des *LG* der Gefahr für Abmahnungen wegen der Speicherung dynamischer IP-Adressen die Spitze, jedenfalls im Hinblick auf die Speicherung statischer IP-Adressen besteht aber ein nicht von der Hand zu weisendes Risiko.

Mit Blick auf die anwaltliche Beratung ist daher zu überlegen, ob der auf die Empfehlung des sichersten Weges bedachte Anwalt nicht generell von der Erhebung und Speicherung von IP-Adressen abraten sollte, wenn hierfür im Einzelfall kein triftiger Grund besteht. Jedenfalls ist auf die entsprechenden Risiken hinzuweisen.

Dr. jur. Dipl.-Inf. Reto Mantz, Richter, Landgericht Frankfurt am Main