

/ BGH zur Speicherung von dynamischen IP-Adressen

17.05.2017

Telekommunikation | IT & Outsourcing

Der Bundesgerichtshof (BGH) hat mit Urteil vom 16. Mai 2017 (Az. VI ZR 135/13, [Pressemitteilung](#)) seine Entscheidung zur Rechtmäßigkeit der Speicherung von dynamischen IP-Adressen verkündet. Die Entscheidung markiert einen weiteren Meilenstein in der seit Jahren kontrovers geführten Diskussion um den Personenbezug von Daten, speziell auch bei (dynamischen) IP-Adressen.

Der Politiker der Piratenpartei, Patrick Breyer, sah sich durch die mehrwöchige Speicherung seiner IP-Adresse auf Webseiten verschiedener Bundesministerien in seinen Persönlichkeitsrechten verletzt. Bereits im Jahr 2008 hatte er deshalb von der Bundesrepublik im Klagewege die Unterlassung dieser Praxis verlangt.

Breyer berief sich auf §§ 12, 15 Telemediengesetz (TMG), wonach personenbezogene Daten – d.h. Daten, über eine bestimmte oder bestimmbare Person – lediglich während der laufenden Verbindung zur betreffenden Website (sog. Session) gespeichert werden dürfen. Eine Speicherung solcher Daten über die Dauer der Session hinaus sieht das Gesetz nur vor, wenn sie im Anschluss für die Abrechnung benötigt werden. Die Bundesregierung machte hingegen geltend, die Speicherung sei notwendig, um Hackerangriffe besser ahnden und sich vor weiteren Angriffen schützen zu können.

IP-Adressen als personenbezogene Daten

IP-Adressen sind Ziffernfolgen, die jedem mit dem Internet verbundenen Gerät zugeordnet sind. Bei Verbrauchern handelt es sich in der Regel um sogenannte dynamische IP-Adressen, das heißt vorübergehenden Adressen, die dem Nutzer von seinem Internetanbieter bei jeder Internetverbindung neu zugewiesen werden. Bei späteren Verbindungen wird dem Nutzer somit jeweils eine neue IP-Adresse zugeteilt.

Jeder Internetnutzer lässt damit beim Aufruf einer Website zwangsläufig einen „digitalen Fußabdruck“ zurück. Die Frage ist jedoch, ob der Websitebetreiber diesen Fußabdruck dem konkreten Nutzer zuordnen kann – denn nur dann ist die betreffende Person für ihn bestimmbar i.S.d. § 3 Abs. 1 BDSG. Zwar kann der Websitebetreiber anhand der IP-Adresse erkennen, dass jemand auf seine Seite zugreift. Ohne die Erhebung zusätzlicher Informationen, etwa durch Abfrage von Kontaktdaten in einer Registrierungsmaske, kann er jedoch nicht die dahinter stehende natürliche Person identifizieren. Lediglich der Internetanbieter kann die jeweilige IP-Adresse dem jeweiligen Anschlussinhaber zuordnen. Er ist aber nur ausnahmsweise unter bestimmten Voraussetzungen, etwa zur Aufklärung von Straftaten oder zur Durchsetzung von Urheberrechten, auf gerichtliche Anordnung zur Auskunft über diese Information verpflichtet. Im konkreten Fall des BGH gab es für derartige Auskunftsansprüche des Websitebetreibers jedoch keinerlei Anhaltspunkte. Im Übrigen ist anzumerken, dass die Internetanbieter die Information über die konkrete Zuteilung einer dynamischen IP-Adresse grundsätzlich (von engen Ausnahmen abgesehen) spätestens nach sieben Tagen löschen müssen. Spätestens ab diesem Zeitpunkt hat der Websitebetreiber somit eigentlich keine Möglichkeit mehr, rechtmäßig an diese Information zu gelangen.

Dennoch war für Herrn Breyer die – theoretisch – mögliche Identifikation der dahinter stehenden Person der Ausgangspunkt, IP-Adressen als personenbezogene Daten einzuordnen. Der BGH hatte im Jahr 2014 das Verfahren ausgesetzt und diese Frage dem Europäischen Gerichtshof (EuGH) vorlegt, da es um die Auslegung der sog. Datenschutzrichtlinie (95/46/EG – „EG-DSRL“) ging.

Mit Urteil vom 19. Oktober 2016 ([wir berichteten](#)) entschied der EuGH, dass es sich bei dynamischen IP-Adressen um personenbezogene Daten handelt, sofern der Betreiber der Website die rechtliche Möglichkeit hat, anhand von Zusatzinformationen die konkrete natürliche Person zu bestimmen. § 12 Abs. 1, Abs. 2 TMG i.V.m. § 3 Abs. 1 BDSG seien insofern richtlinienkonform auszulegen, dass unter das Tatbestandsmerkmal der „personenbezogenen Daten“ unter den oben genannten Voraussetzungen auch IP-Adressen zu subsumieren seien.

Speicherung kann zulässig sein

Als personenbezogenes Datum dürfte eine IP-Adresse nach deutschem Recht eigentlich nur unter den Voraussetzungen des § 15 Abs. 1 TMG gespeichert werden. Eine Abwägung der Interessen von Nutzer und Websitebetreiber sieht das TMG für Telemediendaten nicht vor. Hierin besteht ein Konflikt mit Art. 7 f) der EG-DSRL. Denn unter dieser Vorschrift kommt grundsätzlich bei jedweder Datenverarbeitung eine Rechtfertigung qua Interessenabwägung in Betracht (sofern die Interessen der verantwortlichen Stelle diejenigen der betroffenen natürlichen Person tatsächlich überwiegen). Laut EuGH muss die Vorschrift des § 15 TMG deshalb dahingehend richtlinienkonform ausgelegt werden, dass auch Daten aus Telemediendiensten (z.B. Website) auf Grundlage einer Interessenabwägung auch ohne Einwilligung des Nutzers über das Ende eines Nutzungsvorgangs hinaus erhoben und verwendet werden dürfen, soweit dies erforderlich ist, um die generelle Funktionsfähigkeit der Dienste zu gewährleisten.

Laut EuGH kann die Speicherung nach europäischem Datenschutzrecht zulässig sein, wenn der Betreiber ein „berechtigtes Interesse“ geltend machen könne, das die Grundrechte und Grundfreiheiten der Nutzer in einer Abwägung im Einzelfall überwiegt.

Das Interesse eines Websitebetreibers, sich vor Cyberangriffen zu schützen und so die generelle Funktionsfähigkeit seiner Dienste aufrecht zu erhalten, könne durchaus seine Berechtigung haben. Der konkrete Fall wurde vom EuGH an den BGH zurück verwiesen.

BGH: Persönlichkeitsrecht vs. Sicherheitsinteresse

Mit seinem Urteil hat der BGH entschieden, dass auch dynamische IP-Adressen grundsätzlich ein personenbezogenes Datum sind. Gleichzeitig hat er sich mit der Frage befasst, unter welchen Umständen IP-Adressen von Websitebetreibern gespeichert werden dürfen. Demnach ist eine Speicherung erlaubt, wenn die Gefahr besteht, dass die Internetseite von Hackern angegriffen wird. Soweit feststehe, dass die Speicherung für die Funktionsfähigkeit der Webseite erforderlich ist, müsse in einem zweiten Schritt geprüft werden, ob im konkreten Fall das Sicherheitsinteresse des Betreibers das Persönlichkeitsrecht des Nutzers überwiegt. Je größer die Gefahr eines Angriffs, desto eher sei die Speicherung zulässig.

In jedem Fall sei eine Einzelfallprüfung geboten. Der konkrete Fall wurde vom BGH an das Landgericht Berlin zurück verwiesen. Dort muss nun geprüft werden, wie stark gefährdet die Internetseiten des Bundes sind und ob dies eine Speicherung der IP-Adressen rechtfertigt.

Frage grundsätzlicher Bedeutung

Das Urteil betrifft bei weitem nicht nur Herrn Breyer und die Bundesregierung, sondern ist von grundsätzlicher Bedeutung. Ihre juristische Bewertung betrifft zum einen alle Websites die IP-Adressen über die konkrete Session hinaus speichern. Sie ist darüber auch grundsätzlich für die für den Begriff „personenbezogene Daten“ von hoher Relevanz. Denn es stellt sich automatisch die Folgefrage, ob man diese extrem weite Auffassung von EuGH und BGH auch auf ähnliche Datenkategorien, wie z.B. Gerätekennungen, MAC-Adressen, etc., entsprechend anwenden muss.

Daneben ist nun zu beleuchten, ob nicht auch andere restriktive Vorschriften des deutschen Datenschutzrechts wegen Art. 7 f) EG-DSRL richtlinienkonform auszulegen sind ([mehr dazu](#)).

Haben Sie Fragen? Kontaktieren Sie gerne: [Pascal Schumacher](#) , [Konrad Źdanowiecki](#)

Practice Groups: [IT, Outsourcing & Datenschutz](#) und [Telekommunikation](#)

Contact Person



Pascal Schumacher

Mitglied der Practice Group Telekommunikation

Mitglied der Practice Group Kartellrecht

Rechtsanwalt

T +49 30 20942030

www.noerr.com twitter.com/NoerrLLP xing.com/companies/NoerrLLP