ZEITSCHRIFT FÜR DATENSCHUTZ

ZD

EDITORIAL

3/2023

Sind IP-Adressen wirklich immer personenbezogene Daten? Ein Zwischenruf

Lesedauer: 9 Minuten

IP-Adressen spielen eine zunehmend wichtige Rolle in der datenschutzrechtlichen Praxis. Ein Beispiel war zuletzt die sog. „Abmahnwelle" gegen Webseiten, die Google Fonts dynamisch eingebunden haben. Auch wenn diese Welle gerade abebbt: Die Einbindung von Drittdiensten in Webseiten und die damit verbundene Übermittlung der IP-Adresse an die Server des Drittanbieters bei Seitenaufruf ist von zentraler Bedeutung. Längst haben auch die deutschen Datenschutzaufsichtsbehörden die Einbindung von Drittdiensten in ihren Prüfkatalog für Webseiten aufgenommen. Ein anderes aktuelles Beispiel betrifft die datenschutzrechtliche Diskussion rund um den Zensus 2022. Bereits mehrere deutsche Gerichte mussten sich mit der angeblich unzulässigen Verarbeitung von IP-Adressen durch den Dienstleister beschäftigen, den der Bund zur technischen Absicherung der Zensus2022.de-Webseite eingeschaltet hatte.

Diese Liste ließe sich fortsetzen. Allen Fällen ist eines gemeinsam: Es wird – ohne Prüfung und meist ohne Begründung – unterstellt, dass dynamische IP-Adressen personenbeziehbar nach Art. 4 Nr. 1 DS-GVO seien. Findet sich doch eine Begründung, wird auf das Urteil des EuGH in der Rs. Breyer (EuGH ZD 2017, 24 mAnm Kühling) verwiesen. Aber hat der EuGH dies wirklich so pauschal entschieden?

Diese Frage ist deshalb von praktischer Bedeutung, weil IP-Adressen bei jeder Kommunikation über das Internet zwingend erforderlich sind. Die IP-Adresse ist die Gerätekennung, die eine Kommunikation zwischen Geräten über das Internet erst ermöglicht. Ihre Übertragung lässt sich daher auch beim besten Willen nicht vermeiden. Mit dem Auslaufen des cookiebasierten Trackings wird die Bedeutung von IP-Adressen weiter steigen.

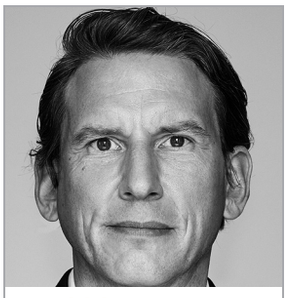
Umso wichtiger erscheint es, einen frischen Blick auf den angeblichen Personenbezug von dynamischen IP-Adressen zu werfen, anstatt einen solchen vorschnell zu bejahen.

Was sagt das Gesetz?

Als gute Juristen beginnen wir mit einem Blick in das Gesetz. Der Gesetzestext der DS-GVO schweigt zu IP-Adressen. Erwähnt werden sie jedoch in Erwägungsgrund 30 DS-GVO, wo es heißt: „Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen ... zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um [natürliche Personen] zu identifizieren."

Daraus wird bereits klar, dass IP-Adressen nicht isoliert, sondern nur in Kombination mit Zusatzinformationen einen Personenbezug ermöglichen können. Nach Erwägungsgrund 26 DS-GVO sollen jedoch nur solche Zusatzinformationen berücksichtigt werden, die „nach allgemeinem Ermessen wahrscheinlich genutzt werden", wobei objektive Faktoren wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand zu berücksichtigen sind.

Der europäische Verordnungsgeber blickt also durchaus differenziert auf einen möglichen Personenbezug von IP-Adressen.



Dr. Ulrich Baumgartner ist Rechtsanwalt und Partner bei BAUMGARTNER BAUMANN Rechtsanwälte in München.

Die jüngere Rechtsprechung und Aufsichtsbehördenpraxis erscheinen undifferenziert

Betrachtet man die anfangs genannten Fälle genauer, so fällt auf, dass sich die beteiligten Gerichte und Aufsichtsbehörden mit dem Personenbezug einer IP-Adresse nicht länger aufhalten, sondern diesen reflexartig unterstellen.

So belässt es das LG München I, das mit seinem Urteil (ZD 2022, 290 mAnm Fischer) die Google-Fonts-Abmahnwelle erst ins Rollen gebracht hat, bei der lapidaren Feststellung, dass die dynamische IP-Adresse für einen Webseitenbetreiber ein personenbezogenes Datum darstelle, wobei es nicht darauf ankomme, ob auch Google die konkrete Möglichkeit habe, die IP-Adresse mit dem Kläger zu verknüpfen. Ähnlich die Urteile, die im Zusammenhang mit dem Zensus 2022 ergangen sind (zB VG Neustadt/W. Beschl. v. 27.10.2022 – 3 L 763/22.NW).

Die deutschen Datenschutzaufsichtsbehörden, die seit vielen Jahren davon ausgehen, dass IP-Adressen stets personenbezogene Daten darstellen, verzichten ebenfalls meist auf eine Begründung – so wie jüngst in der finalen Fassung der DSK-Orientierungshilfe Telemedien (zB Rn. 136).

Back to the Roots: Das Breyer-Urteil des EuGH

Hintergrund dieser pauschalen Bejahung eines Personenbezugs von IP-Adressen ist, wie erwähnt, das Urteil des EuGH in der Rs. Breyer aus dem Jahre 2016. Dieses ist jedoch weniger klar und durchaus differenzierter, als es die geschilderte Praxis vermuten lässt.

Der EuGH hatte über Vorlagefragen des BGH zu entscheiden. Wie immer in Vorabentscheidungsverfahren war der EuGH also an die Formulierung der Vorlagefragen grundsätzlich gebunden. Die hier relevante Vorlagefrage des BGH lautete, ob Art. 2 lit. a DS-RL (RL 95/46/EG – also die Vorgängernorm von Art. 4 Nr. 1 DS-GVO) so auszulegen sei, dass eine IP-Adresse, die ein Webseitenbetreiber im Zusammenhang mit einem Zugriff auf seine Webseite speichert, für diesen ein personenbezogenes Datum darstelle, wenn der Internetzugangsanbieter über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt (BGH ZD 2015, 80 mAnm Bergt).

Diese Vorlagefrage ist also vergleichsweise eng: Sie betrifft zum einen nur die Verarbeitung einer IP-Adresse durch den Webseitenbetreiber, die er selbst bei Aufruf der eigenen Webseite erhoben hat. Die Vorlagefrage unterstellt außerdem, dass der Internetzugangsanbieter über das erforderliche Zusatzwissen verfügt, das es ihm ermöglicht, „die betroffene Person" zu identifizieren.

Insoweit ist die Vorlagefrage unklar: Meint der BGH mit der „betroffenen Person" den Inhaber des Internetanschlusses oder den konkreten Nutzer, der die betreffende Webseite aufgerufen hat? In der Praxis fallen diese Gruppen häufig auseinander, etwa bei offenen WLAN-Netzen oder wenn sich mehrere Familienmitglieder oder WG-Bewohner einen Internetanschluss teilen. Um wessen Identifizierbarkeit geht es also? Wäre der konkrete Nutzer gemeint, so wäre die Annahme des BGH, der Internetzugangsbetreiber verfüge über die zur Identifizierung erforderlichen Informationen, äußerst zweifelhaft, da sich über die IP-Adresse allenfalls der Anschlussinhaber bestimmen lässt. Der Vorlagebeschluss legt nahe, dass der BGH tatsächlich den Anschlussinhaber vor Augen hatte (BGH ZD 2015, 80 Rn. 30 mAnm Bergt), während er dann aber in seinem anschließenden Urteil von dem konkreten Nutzer ausging (BGH ZD 2017, 424 Rn. 26).

Der EuGH interpretierte die unklare Vorlagefrage offenbar dahingehend, dass die „betroffene Person" (der EuGH spricht von der „betreffenden Person") der Nutzer sei, der die Webseite abgerufen hat (EuGH ZD 2017, 24 Rn. 37). Es scheint also, als hätten der BGH in seinem Vorlagebeschluss und der EuGH in seinem Urteil in dieser entscheidenden Frage aneinander „vorbeigeredet".

Ebenfalls nicht auf einer Linie liegen BGH und EuGH in der nicht minder entscheidenden Frage der Zugänglichkeit der Zusatzinformationen: In seinem Vorlagebeschluss erwähnt der BGH zutreffend, dass dem Webseitenbetreiber kein direkter Auskunftsanspruch gegenüber dem Internetzugangsbetreiber zustehe. Auch den Umweg über ein staatsanwaltschaftliches Ermittlungsverfahren nach § 113 TKG aF lässt der BGH ausdrücklich nicht genügen und stellt fest, dass die Zusatzinformationen des Internetzugangsanbieters für den Webseitenbetreiber als nicht zugänglich anzusehen seien (BGH ZD 2015, 80 Rn. 32 mAnm Bergt).

Gleichwohl kommt der EuGH zu dem Schluss, dass „es offenbar … für den Anbieter von Online-Mediendiensten rechtliche Möglichkeiten [gebe], die es ihm erlauben, sich insbesondere im Fall von Cyberattacken an die zuständige Behörde zu wenden, um die fraglichen Informationen vom Internetzugangsanbieter zu erlangen und die Strafverfolgung einzuleiten" (EuGH ZD 2017, 24 Rn. 47). Das Urteil des EuGH enthält (wie auch die Schlussanträge des Generalanwalts) keine Anhaltspunkte dafür, dass der EuGH der absoluten Theorie des Personenbezugs zuneigt. Im Gegenteil: Das Gericht betont, dass die Identifizierung „praktisch durchführbar" sein müsse. Auch insoweit scheint also ein Missverständnis vorzuliegen, da der EuGH im Ergebnis feststellt, dass der Webseitenbetreiber „offenbar" über die Mittel verfüge, die „vernünftigerweise eingesetzt werden könnten, um mit Hilfe Dritter, und zwar der zuständigen Behörde und dem Internetzugangsanbieter, die betreffende Person anhand der gespeicherten IP-Adressen bestimmen zu lassen". Dies ist Grundlage für den EuGH, die Vorlagefrage positiv zu beantworten.

Es kommt auf den Kontext an

Diese – zugegeben kurze – Analyse des Breyer-Urteils des EuGH zeigt eines sehr deutlich: Das Judiz ist „mit Vorsicht zu genießen". Es erscheint im Kontext des Vorlagebeschlusses an entscheidender Stelle missverständlich und betrifft lediglich eines von vielen praktischen Szenarien, in denen IP-Adressen eine Rolle spielen.

Allenfalls in dem vom EuGH entschiedenen Kontext (Verarbeitung der IP-Adresse durch einen dem deutschen Recht unterfallenden Webseitenbetreiber) und ausschließlich bezogen auf den Anschlussinhaber erscheint das Urteil direkt anwendbar (wobei auch in diesem Fall angesichts der erwähnten Unklarheiten im EuGH-Urteil Zweifel angebracht sind). Schon eine Übertragung auf die Identifizierbarkeit des konkreten Nutzers erscheint dagegen zweifelhaft, wenn dieser nicht zugleich der Anschlussinhaber ist.

Nicht ohne Einzelfallprüfung übertragbar ist das Urteil auf Situationen, in denen IP-Adressen von anderen Verantwortlichen als dem Webseitenbetreiber verarbeitet werden (etwa von Google in den anfangs erwähnten Abmahnfällen). Ob auch Drittanbietern nach deutschem Recht die rechtlichen Auskunftsansprüche zustehen, haben weder BGH noch EuGH entschieden – ebenso wenig wie die Frage, ob derartige Ansprüche nach anderen anwendbaren Rechtsordnungen bestehen, wenn die Drittanbieter wie regelmäßig außerhalb Deutschlands sitzen. Dies erscheint fernliegend, wäre aber in jedem Einzelfall darzulegen. Auch die Möglichkeit für Drittanbieter, den Personenbezug auf Grundlage eigener Zusatzinformationen herzustellen, kann nicht einfach unterstellt, sondern muss im Einzelfall begründet werden (ein bloßes „Aussondern" macht keinen Nutzer indirekt identifizierbar). Erhebliche Zweifel am Personenbezug von IP-Adressen bestehen daher auch beim sog. „Server Side Tracking", bei dem u.a. aus IP-Adressen und „User Agent String" Werbe-Identifier gebildet werden.

In Konstellationen schließlich, in denen IP-Adressen in anderem Kontext als einem http-Request verarbeitet werden, liegt ein Personenbezug noch ferner. Verfügt die Stelle, die IP-Adressen verarbeitet, nicht über die bei einem http-Request übermittelten weiteren Informationen – etwas den Zeitstempel – ist eine Identifizierbarkeit kaum mehr denkbar. Dies betrifft etwa Sicherheitsdienstleister, die IP-Adressen nutzen, um Angreifer wie insbesondere Bot-Netze zu erkennen und abzuwehren.

Es zeigt sich also: Ob dynamische IP-Adressen personenbezogene Daten darstellen, bedarf stets einer fundierten Begründung; ohne eine solche erscheint die Wertung in vielen Fällen rechtlich angreifbar.