2017/11 Lifestyle

https://jungle.world/artikel/2017/11/ein-endloses-verfahren

Vor Gericht wird verhandelt, ob vom Staat betriebene Websites IP-Adressen speichern dürfen

Ein endloses Verfahren

Von **Enno Park**

2008 erhob Patrick Breyer von der Piratenpartei eine Unterlassungsklage gegen die Bundesrepublik Deutschland. Vom Staat betriebene Websites sollen IP-Adressen nicht länger speichern dürfen. Nun liegt der Fall wieder beim Bundesgerichtshof, der am 16. Mai ein Urteil fällen will.

Ohne IP-Adressen geht es nicht. Wann immer wir eine E-Mail verschicken, eine Website aufrufen oder einen anderen Internetdienst nutzen, erlauben diese kryptischen Zahlenreihen erst die Kommunikation im Netz. Wenn Websites und andere Anbieter automatisch Protokolle darüber führen, was auf ihren Servern so passiert, werden regelmäßig auch diese IP-Adressen gespeichert. Das stört Patrick Breyer. Der Politiker, der voraussichtlich noch bis Mai für die Piratenpartei im Landtag von Schleswig-Holstein sitzt, möchte Websites das Speichern der IP-Adresse grundsätzlich verbieten. Deshalb verklagte er die Bundesrepublik Deutschland, die auf ihren Websites die IP-Adressen der Nutzer speichert. Sollte er Erfolg haben, wäre es ein Präzedenzfall. Der Urteilsspruch würde auch für alle Website-Betreiber in Deutschland gelten. Breyer argumentiert, der Besuch von Websites im Internet zum Teil intimste Rückschlüsse auf das Privatleben der Nutzer zulasse. Schließlich enthalte das Internet neben Katzenbildern auch Informationen über Krankheiten, Stellenangebote oder Anleitungen zum Bombenbau. Wer solche Websites liest, mache sich verdächtig oder erpressbar, egal aus welchen Gründen er eine entsprechende Website besucht hat. Zwar weiß ein Anbieter nicht, welche Person sich hinter einer IP-Adresse verbirgt, aber das weiß der Internetprovider, der die Adressen regelmäßig neu zuteilt.

Die Provider wiederum müssen diese Daten ab dem 1. Juli 2017 zehn Wochen lang speichern und herausgeben, wenn ein Staatsanwalt wegen einer schweren Straftat ermittelt und ein Gericht das anordnet. Es gibt aber auch andere Wege, die Person hinter einer IP-Adresse ausfindig zu machen, beispielsweise mittels einer Klage wegen eines Urheberrechtsverstoßes. Die strafrechtlichen Verfahren werden zwar regelmäßig wieder eingestellt, allerdings wird zu Verfahrensbeginn grundsätzlich anhand der IP-Adresse ermittelt, wer überhaupt verklagt wird. Die klagenden Anwälte gelangen so an die zugehörigen Namen und Adressen, an die sie anschließend zivilrechtliche Abmahnungen und Klagedrohungen verschicken. Das ließe sich verhindern, wenn Websites und Internetdienste die IP-Adressen ihrer Nutzer gar nicht erst speichern dürften. Ein solches Verbot würde das Internet anonymer machen.

Es gibt aber durchaus viele Menschen, die das für keine gute Idee halten. Ein solches Verbot

würde es auch nahezu unmöglich machen, gegen Belästigungen und Morddrohungen per Internet vorzugehen. Breyers Forderung entspricht insofern vor allem dem Wunschdenken weißer, männlicher Nerds. Aber auch der Betreiber eines Onlineshops, der einem Kreditkartenbetrug zum Opfer fällt, oder der Systemadministrator eines Unternehmens, das Schäden wegen eines Hackerangriffs verzeichnet, haben ein berechtigtes Interesse, in den Protokolldateien nachsehen zu können, woher der Angriff stammt. Wenn sich kein Täter ermitteln lässt, weil die Attacke von einem Bot-Netz ausging, können die Daten wenigstens helfen, entsprechende Bot-Netze stillzulegen.

Das sah auch das Amtsgericht Berlin-Tiergarten so und wies Breyers Klage zunächst ab. Allerdings gab ihm in nächster Instanz das Landgericht Berlin 2013 teilweise recht. Gegen dieses Urteil legten beide Parteien Revision ein, so dass das Verfahren beim Bundesgerichtshof landete. Der wiederum fand die Angelegenheit zu wichtig, um sie nur auf nationaler Ebene zu klären, und gab die Sache an den Europäischen Gerichtshof weiter. Der urteilte 2016 deutlich: IP-Adressen sind tatsächlich personenbezogene Daten, die dem Datenschutz unterliegen. Allerdings ist ihre Speicherung sehr wohl gestattet, wenn ein berechtigtes Interesse daran vorliegt. Damit erklärte der EuGH Teile des deutschen Datenschutzrechts für ungültig. Nicht überraschend, stammt es doch aus einer Zeit, als es das Internet noch nicht gab und mit Magnetbändern und Lochkarten hantiert wurde. Mit den Anpassungen der vergangenen Jahre entstand eine juristische Chimäre, die einerseits Websites unter Bußgeldandrohung dazu verpflichtet, Warnungen zur Benutzung von Cookies einzublenden, während andererseits schwungvoller Handel mit personenbezogenen Adressdaten etwa durch Verlage oder die Deutsche Post völlig legal möglich ist.

Der Urteilsspruch des EuGH ist also ein Auftrag an die Parlamente, das Datenschutzrecht einmal mehr zu reformieren. Derlei ist tatsächlich in Arbeit. Auf europäischer Ebene wird über eine Reform der »E-Privacy-Richtlinie« beraten. In ihrer alten Form schützt sie das Grundrecht auf Kommunikation und Privatsphäre. Beispielsweise regelt sie, dass Telekommunikationsunternehmen die massenhaft anfallenden Kommunikations- und Standortdaten weder weitergeben noch zu Marketingzwecken nutzen dürfen. Ausnahmen gibt es für Strafverfolgung und zum Schutz der nationalen Sicherheit. Allerdings stammt die Richtlinie aus einer Zeit, in der es vor allem um Telefonate und SMS ging. Heute landen solche Daten nicht nur bei Providern und Mobilfunkanbietern, sondern auch bei zahlreichen anderen Unternehmen, allen voran etwa Amazon, Facebook und Google. Und was die dürfen, ist weniger streng reguliert.

Die Europäische Kommission möchte daran wenig ändern. Sie sorgt sich um die Wettbewerbschancen europäischer Internetfirmen gegenüber der Konkurrenz in den USA und Ostasien. Dafür setzt sich auch ein Zusammenschluss mehrerer Handelsverbände ein. Sie vertreten Technologiefirmen von Microsoft bis Google, von Samsung bis Huawei und von der Deutschen Telekom bis Airbus. Ihr Ziel ist, die E-Privacy-Richtlinie ersatzlos zu streichen, statt sie zu reformieren.

Auf der anderen Seite stehen NGOs wie Access Now, Privacy International und European Digital Rights (EDRi), die einen Forderungskatalog aufgestellt haben: Werbetracking, also das Verfolgen von Nutzern anhand von so genannten »Third-Party-Cookies« über viele Websites hinweg, möchten sie stark einschränken. Ganz verbieten wollen sie das »Browser Fingerprinting«. Diese Technik erkennt Nutzer einigermaßen sicher darüber, welche Browser- und Betriebssystemeinstellungen sie verwenden, und das ganz ohne Cookies. Außerdem kritisieren die NGOs, dass immer mehr Website-Betreiber diejenigen Anwender, die der Verwendung von Third-Party-Cookies nicht zustimmen, kurzerhand aussperren. Besonders vor Missbrauch und

Weitergabe schützen wollen die NGOs Daten, die im Rahmen von Quantifed-Self- und Gesundheitsanwendungen anfallen. Die von Patrick Breyer monierte Speicherung von IP-Adressen hingegen wird von den NGOs nur noch selten als Problem angesehen. Mit seiner Klage hinkt er also den tatsächlichen Datenschutzproblemen des Internets etwa zehn Jahre hinterher. Beim Rechtsstreit Breyer gegen Bundesrepublik Deutschland hilft die Reform der E-Privacy-Richtlinie erstmal nicht weiter. Bis die auf europäischer Ebene steht und danach auch von den Mitgliedsstaaten in nationales Recht übernommen wird, dürfte es noch mehrere Jahre dauern. Ohnehin ist nicht zu erwarten, dass der deutsche Gesetzgeber die Speicherung von IP-Adressen verbietet. Die große Koalition hat gerade erst gegen starke juristische Bedenken die Vorratsdatenspeicherung eingeführt, die Internetprovider verpflichtet, unter anderem die IP-Adressen ihrer Nutzer für zehn Wochen zu speichern. Ein Verbot für Website-Betreiber, dasselbe zu tun, ergäbe für die Anhänger der Vorratsdatenspeicherung überhaupt keinen Sinn. Die unendliche Geschichte wird also weiterhin die Gerichte beschäftigen. Eine Entscheidung soll der Bundesgerichtshof, auf dessen Schreibtischen die Klage erneut gelandet ist, am 16. Mai fällen.