

Hintergrundpapier

zur Vorratsdatenspeicherung vor dem Bundesverwaltungsgericht

Berlin, 17.09.2019

I. Stand des Verfahrens

Am 25.09.2019 verhandelt das Bundesverwaltungsgericht, ob das Unternehmen SpaceNet AG nach den §§ 113a ff. TKG verpflichtet ist, Verkehrsdaten zu speichern. Das Unternehmen, das eco- Verband der Internetwirtschaft e.V. in dieser Angelegenheit von Anfang unterstützt, hatte am 25.04.2016 Klage gegen das Gesetz zur Höchstspeicherungsdauer von Verkehrsdaten erhoben und zugleich einen Eilantrag gestellt. Zuständig war das Verwaltungsgericht Köln. Im Januar 2017 wies das Gericht den Eilantrag als unbegründet zurück. Auf die Beschwerde gab das Oberverwaltungsgericht (OVG) Nordrhein-Westfalen der SpaceNet AG im Juni 2017 Recht. Die Speicherpflichten nach dem Telekommunikationsgesetz (TKG) seien nicht mit EU-Recht vereinbar. Der Europäische Gerichtshof (EuGH) hatte in einer wegweisenden Entscheidung (Tele 2/Watson) im Dezember 2016 zu Regelungen in Schweden und Großbritannien entschieden, dass eine generelle, anlasslose, und uneingeschränkte Vorratsdatenspeicherung nicht mit der e-Privacy-Richtlinie im Lichte der Art. 7, 8 und 52 der EU-Grundrechte-Charta im Einklang stünden. Das OVG sah die deutschen Regelungen wie die SpaceNet AG und eco im Wesentlichen vergleichbar und damit als unvereinbar mit EU-Recht an. Auf den Beschluss des OVG setzte die Bundesnetzagentur (BNetzA) wegen der über den Einzelfall hinausgehenden Bedeutung die Durchsetzung der Speicherpflichten gegenüber den betroffenen Unternehmen aus. Die Regulierungsbehörde hatte sich diesbezüglich mit den Bundeministerien für Wirtschaft und Energie und demjenigen für Justiz und Verbraucherschutz abgestimmt. Der Beschluss des OVG NRW gilt bis zu einer rechtskräftigen Entscheidung in der Hauptsache (Klageverfahren). Das Verwaltungsgericht (VG) Köln änderte daraufhin seine



Rechtsauffassung vollständig und gab der Klage der SpaceNet AG am 20.04.2018 statt. Von einer Vorlage an den EuGH sah das VG Köln wegen offensichtlicher Wesensgleichheit der deutschen Regelungen zu den schwedischen und großbritannischen ab. Auf Wunsch der Bundesrepublik Deutschland, vertreten durch die Bundesnetzagentur, stimmte die SpaceNet AG trotz des Sieges einer Sprungrevision zum Bundesverwaltungsgericht (Auslassung d. Berufungsinstanz) zu. Die SpaceNet AG teilt mit der Bundesregierung das Interesse an Rechtsicherheit durch eine höchstrichterliche Entscheidung.

II. Ziel der Klage

Die SpaceNet AG möchte festgestellt wissen, dass sie nicht verpflichtet ist, die Verkehrsdaten ihrer Kunden auf Vorrat zu speichern. Viele ihrer Kunden sind Berufsgeheimnisträger, z. B. Rechtsanwälte, Kliniken und Kirchen. Sie sieht sich dabei auch als Schutzherrin der Daten ihrer Kunden. Hinzu kommt, dass bei kleinen Unternehmen wie der SpaceNet AG eine sehr geringe Anzahl an Auskunftersuchen eingeht, meist einstellig im Jahr.

Demgegenüber stehen sehr hohe Investitionskosten für technische Vorrichtungen und Schnittstellen zur Beauskunftung von entsprechenden Behördenersuchen. Es entstehen einmalige und laufende Kosten, da der Stand der Technik und sich ändernde Vorgaben der Bundesnetzagentur zu beachten und umzusetzen sind. Daraus folgt, dass die Kosten für Sach- und Personalaufwand deutlich außer Verhältnis zu der Anzahl der Ersuchen der Behörden stehen.

Die SpaceNet AG und eco wollen gerichtlich prüfen lassen, ob die deutschen Vorschriften zur Vorratsdatenspeicherung der Achtung des Privat- und Familienlebens (Art. 7), dem Schutz der personenbezogenen Daten (Art. 8), die Berufsfreiheit (Art. 15), der unternehmerischen Freiheit (Art. 16) und dem Verhältnismäßigkeitsgrundsatz (Art. 52) nach der EU-Grundrechte-Charta ausreichend Rechnung tragen. Die SpaceNet AG und eco sehen den Schutz

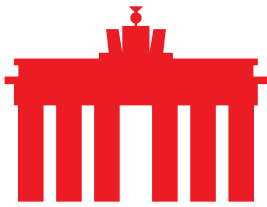


der Kundendaten als ein sehr großes Anliegen, da es um das Vertrauen der Kunden auf den Schutz ihrer Daten geht. Hier verletzen die deutschen Regelungen zur Speicherung und Herausgabe der Verkehrsdaten nach §§ 113a ff. die Grundrechte aus Art. 7 und 8 GrCh. Die Pflicht zur Speicherung gem. 113b Abs. 3 TKG sowie zum Vor- und Instandhalten der technischen Einrichtungen nach § 113f TKG verstoßen zudem gegen die Grundrechte der SpaceNet nach Art. 15 u. 16 GrCh. Angesichts des Umfangs der Kosten und des Aufwands gegenüber der sehr geringen Abfragezahl werden kleinere Unternehmen wie SpaceNet unverhältnismäßig belastet.

Da SpaceNet und eco der Auffassung waren, dass sich die Neuregelung der Vorratsdatenspeicherung sowohl am deutschen Grundgesetz als auch an den Unionsgrundrechten messen lassen muss, hat man den Weg zum Verwaltungsgericht gewählt und sich bewusst gegen eine Verfassungsbeschwerde beim Bundesverfassungsgericht entschieden. Dort sind derzeit immer noch mehrere Verfahren bzgl. der Vorratsdatenspeicherung anhängig. Eine Entscheidung noch dieses Jahr ist nicht wahrscheinlich.

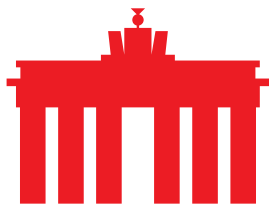
III. Hintergrund

Der EuGH hat in Tele2/Watson festgestellt, dass Regelungen wie in Schweden und Großbritannien, die eine generelle, anlasslose und uneingeschränkte Speicherung von Verkehrsdaten vorsehen, nicht mit Art. 15 Abs. 1 e-Privacy-Richtlinie (2002/58/EG) vereinbar sind. Diese Norm sieht die Speicherung von Verkehrsdaten, wenn sie nicht für betriebliche Zwecke (insb. Abrechnung) erfolgt, nur als Ausnahme vor. Somit verletzen die schwedischen und britischen Vorschriften das im EU-Recht postulierte Regel-Ausnahme-Verhältnis. Letzteres ist kein Selbstzweck, sondern gewährleistet die Achtung des Privat- und Familienlebens (Art. 7), den Schutz personenbezogener Daten (Art. 8) und die Wahrung des Verhältnismäßigkeitsgrundsatzes (Art. 52) nach der EU-Grundrechte-Charta. Viele Passagen im EuGH-Urteil erinnern an das Volkszählungsurteil des



Bundesverfassungsgerichts von 1983. So etwa, dass das Wissen um die Speicherung von Verkehrsdaten eine Änderung des Verhaltens der Bürger nach sich ziehen könnte, da die Verkehrsdaten in Gesamtheit sehr genaue Rückschlüsse auf das Privatleben zulassen (etwa: wer kommuniziert mit wem wie oft und wie lange, wer versucht, wie oft jemanden zu erreichen und wo halten sich Betroffene wie oft und wie lange auf). Der EuGH kommt zum Ergebnis, dass die Speicherung dieser Daten für sich gesehen einen Eingriff in die o. g. EU-Grundrechte darstellt. Der Abruf durch berechnigte Behörden stellt einen weiteren Eingriff dar. Staatliche Eingriffe in Grundrechte bedürfen der Rechtfertigung. Der EuGH schlussfolgert, dass die Eingriffe durch Speicherung und Abruf in Schweden und Großbritannien nicht auf das absolut notwendige Maß beschränkt seien. Dazu dürften solche Vorschriften die Speicherung nicht anlasslos erlauben. Es müssten Einschränkungen vorgenommen werden, die dafür sorgten, dass ein Zusammenhang der zu speichernden Daten mit schwerer Kriminalität besteht, etwa durch eine Beschränkung auf einen bestimmten Personenkreis oder lokale oder regionale Eingrenzungen im Zusammenhang mit schwerer Kriminalität. Weiter dürften sie allein zur Bekämpfung letzterer verwendet werden. In Deutschland ist indes die Verwendung bestimmter Vorratsdaten sogar zur Verfolgung von Ordnungswidrigkeiten zulässig.

Die Argumente der Bundesregierung, dass die deutsche Vorratsdatenspeicherung deswegen rechtmäßig sei, weil die Daten kürzer gespeichert würden als in Großbritannien oder Schweden, E-Mails ausgenommen seien, und die Vorgaben auf einem Gesetz beruhten, adressieren nicht die Kernfragen der materiellen Rechtmäßigkeit des Eingriffs. Denn die deutschen Regelungen erlauben die anlasslose Speicherung der Verkehrsdaten aller Nutzer von Telefonie (Mobil, Festnetz, VoIP) und Internetdiensten. Ein Zusammenhang der zu bevorratenden Daten mit schwerer Kriminalität ist nach dem deutschen Gesetz nicht verlangt. Die Speicherung und der Abruf der Verkehrsdaten sind nicht auf die Bekämpfung von schwerer Kriminalität begrenzt. All diese Vorgaben des EuGHs erfüllen die §§ 113ff. TKG nicht.



Politisch wurden weder hierzulande noch EU-weit Konsequenzen im Sinne der Aufhebung von Regelungen zur Vorratsdatenspeicherung gezogen. Im Juni 2019 beschlossen die Justizminister der EU-Mitgliedsstaaten, eine Studie von der EU-Kommission durchführen zu lassen. Im Studienauftrag drückt sich die Haltung der Minister aus, dass die Vorratsdatenspeicherung notwendig sei. Die Studie unterstellt die Notwendigkeit. Die langjährige Weigerung der Staaten, eine Evidenzbasis zu schaffen oder andere, mildere Mittel zu suchen, ist nicht nachvollziehbar.

IV. Mögliche Verfahrensausgänge

Sieg SpaceNet AG/eco

Das Bundesverwaltungsgericht weist die Sprungrevision der BRD, vertreten durch BNetzA zurück. In diesem Fall wäre das Gericht der Ansicht, dass die deutschen Regeln zur Vorratsdatenspeicherung gegen das EU-Recht verstoßen und nicht anwendbar sind. Unmittelbar würde sich diese Entscheidung zunächst nur auf das Verhältnis zwischen SpaceNet und BNetzA auswirken. Das BVerwG hat schon in einigen Fällen entschieden, dass deutsche Regelungen wegen Unvereinbarkeit mit dem EU-Recht nicht anwendbar seien.

Niederlage SpaceNet AG/eco

Das Bundesverwaltungsgericht gibt der Sprungrevision der BRD, vertreten durch BNetzA, statt. In diesem Fall wäre das Gericht der Ansicht, dass die deutschen VDS-Regeln mit dem EU-Recht vereinbar sind. Das Urteil des VG Köln vom 20.04.2018 würde, aufgehoben, der OVG-Beschluss (einstweiliges Verfahren) würde wirkungslos. Die Bundesnetzagentur dürfte die Speicherpflicht auf Grund des TKG gegenüber den Unternehmen, auch mit Zwangs- und Bußgeldern) durchsetzen. Die BNetzA hatte uns für diesen Fall zugesichert, den Unternehmen eine angemessene Umsetzungszeit zu geben. Eine solche Entscheidung ohne vorherige Befassung des EuGHs



würde allerdings nach unserer Überzeugung sowohl die unionsrechtliche Vorlagepflicht (Art. 267 AEUV) als auch das deutsche Recht auf den gesetzlichen Richter (Art. 101 GG) verletzen.

Vorabentscheidungsersuchen an EuGH

Das Bundesverwaltungsgericht setzt das Verfahren aus und formuliert Vorlagefrage(n) an den EuGH, konkret bezogen auf die deutschen Regeln und deren Vereinbarkeit mit der E-Privacy- Richtlinie im Lichte der EU- Grundrechte-Charta, konkret Art. 15 Abs. 1 E-Privacy-RL i. V. m. Art. 7, 8, 15, 16 und 52 Charta.

Über eco ist mit über 1.100 Mitgliedsunternehmen der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, formt Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Leitthemen sind Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie Ethik und Selbstregulierung. Deshalb setzt sich eco für ein freies, technikneutrales und leistungsstarkes Internet ein.

Über SpaceNet Die SpaceNet AG bietet seit 1993 als unabhängiger Fullservice-Internetprovider Unternehmen Lösungen rund um das Internet an. SpaceNet ist spezialisiert auf das Hosting von Anwendungen für Geschäftsmodelle wie etwa E-Commerce-Lösungen, die hochverfügbare IT-Umgebungen voraussetzen. Als Outsourcing-Partner betreibt SpaceNet für seine Kunden sowohl einzelne Anwendungen und Services in seinen Rechenzentren, übernimmt aber auch den kompletten Betrieb der Unternehmens-IT.

Als Anbieter von Cloud-Lösungen wie Mailarchiv, Mail-Dienste oder Hosting Continuity erdet SpaceNet die Cloud. Denn diese Lösungen brauchen als Basis Rechenzentren mit hochperformanter, stabiler und zuverlässiger Infrastruktur. SpaceNet hält die Daten in zwei lokal getrennten Hochsicherheitsrechenzentren in München redundant vor. Ein eigenes Backbone liefert eine unabhängige Infrastruktur mit Schnittstellen zu den weltweit wichtigsten Knotenpunkten und garantiert so hohe Übertragungsraten. Zur SpaceNet Familie zählen seit kurzem zwei weitere Unternehmen: Die SDC SpaceNet DataCenter GmbH & Co. KG, die derzeit ein Hochsicherheitsrechenzentrum in Kirchheim bei München baut und die brück IT GmbH, ein Systemhaus spezialisiert auf Rechtsanwälte.



Derzeit profitieren zirka 1.200 Geschäftskunden wie Antenne Bayern oder der Münchner Verkehrs- und Tarifverbund (MVV) von den Dienstleistungen der SpaceNet AG. Das Münchener Unternehmen beschäftigt rund 125 Mitarbeiter und ist zertifiziert nach dem Sicherheitsstandard ISO 27001.