Bestandsdatenerfassung verfassungswidrig, Privacy Shield unwirksam

Bestandsdatenerfassung verfassungswidrig, Privacy Shield unwirksam

Sowohl der Europäische Gerichtshof (EuGH) als auch das Bundesverfassungsgericht (BVerfG) haben die privaten Rechte auf Schutz von Daten gestärkt: Das oberste Gericht der Europäischen Union erklärte das „Privacy Shield“ Abkommen mit den USA für unwirksam. Das Karlsruher Gericht erklärte die bestehenden Regelungen zur Bestandsdatenauskunft für verfassungswidrig.

Mit Beschluss vom 27. Mai 2020 (veröffentlicht erst Ende Juli) hat der Erste Senat des Bundesverfassungsgerichts **§ 113 des Telekommunikationsgesetzes (TKG)** und mehrere Fachgesetze des Bundes, die die manuelle Bestandsdatenauskunft regeln, für **verfassungswidrig** erklärt. Die Richter erklärten hierbei, die Regelungen verletzten sowohl das Grundrecht auf **informationelle Selbstbestimmung (RiS, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG)** als auch auf Wahrung des **Telekommunikationsgeheimnisses (Art. 10 Abs. 1 GG).** Zwar dienten die Ermächtigungsgrundlagen legitimen Zwecken. Sie seien aber nur verhältnismäßig, insbesondere angemessen, wenn sie die **Verwendungszwecke der einzelnen Befugnisse selbst hinreichend normenklar begrenzten**.

Die manuelle Bestandsdatenauskunft ermöglicht es Sicherheitsbehörden bislang, von Telekommunikationsunternehmen Auskunft zu erlangen, etwa über zu einem bestimmten Zeitpunkt zugewiesene IP-Adressen oder den Anschlussinhaber eines Telefonanschlusses. Mitgeteilt werden müssen hierbei personenbezogene Daten der Kunden, die im Zusammenhang mit dem Abschluss oder der Durchführung von Verträgen stehen (sogenannte Bestandsdaten). Nicht mitgeteilt werden hingegen Daten, die sich auf die Nutzung von Telekommunikationsdiensten (sogenannte Verkehrsdaten) oder den Inhalt von Kommunikationsvorgängen beziehen. Alle angegriffenen Regelungen wurden zur Umsetzung des Beschlusses des Ersten Senats vom 24. Januar 2012 - 1 BvR 1299/05 -, BVerfGE 130, 151 - 212 (**Bestandsdatenauskunft I**) geschaffen bzw. geändert, mit der § 113 TKG in seiner damaligen Fassung für teils verfassungswidrig erklärt und das Fehlen fachrechtlicher Ergänzungen beanstandet wurde.

Diese Regelungen verstoßen nach Ansicht des 1. Senats gegen Grundrechte. So stellte es das BVerfG in den Verfahren 1 BvR 1873/13 und 2618/13 (**Bestandsdatenauskunft II**) fest. Die Erteilung einer Auskunft über Bestandsdaten sei zwar grundsätzlich verfassungsrechtlich zulässig. Aber: der Gesetzgeber müsse sowohl für a) die Übermittlung der Bestandsdaten durch die Telekommunikationsanbieter als auch für b) den Abruf dieser Daten durch die Behörden jeweils eigene, verhältnismäßige Rechtsgrundlagen schaffen. Übermittlungs- und Abrufregelungen müssten die **Verwendungszwecke der Daten hinreichend begrenzen**, indem sie insbesondere einen **hinreichend gewichtigen Rechtsgüterschutz** und zudem **tatbestandliche Eingriffsschwellen** vorsähen. In diesem Hinblick stellt der Senat klar, dass die allgemeinen Befugnisse zur Übermittlung und zum Abruf von Bestandsdaten trotz ihres gemäßigten Eingriffsgewichts für die Gefahrenabwehr und die Tätigkeit der Nachrichtendienste grundsätzlich einer im Einzelfall vorliegenden **konkreten Gefahr** und für die Strafverfolgung eines **Anfangsverdachts** bedürfen. Fände darüber hinaus eine Zuordnung dynamischer IP-Adressen statt, müsse diese im Hinblick auf ihr **erhöhtes Eingriffsge**wicht zudem auch dem **Schutz oder der Bewehrung von Rechtsgütern von zumindest hervorgehobenem Gewicht** dienen. Blieben die **Eingriffsschwellen** im Bereich der Gefahrenabwehr oder der nachrichtendienstlichen Tätigkeit hinter diesem Erfordernis einer konkreten Gefahr zurück, müssten zum Ausgleich **erhöhte Anforderungen an das Gewicht der zu schützenden Rechtsgüter** vorgesehen werden. Diese Voraussetzungen wurden von den Vorschriften nach Ansicht des BVerfG weitgehend nicht erfüllt, daher seien diese verfassungswidrig.

Um eine verfassungsgemäße Datenauskunftsregelung schaffen zu können setzt das BVerfG Hürden: a) Der Gesetzgeber muss bei der Einrichtung eines Auskunftsverfahrens auf Grundlage **jeweils**

eigener Kompetenzen für sich genommen verhältnismäßige Rechtsgrundlagen schaffen. Dies gilt sowohl für die Übermittlung als auch für den Abruf der Daten. Es bedarf also zweier unabhängiger, jeweils verhältnismäßiger Ermächtigungsgrundlagen. b) Diese Übermittlungs- und Abrufregelungen für Bestandsdaten müssen die **Verwendungszwecke** der Daten **hinreichend begrenzen.** D.h. die Datenverwendung muss an **bestimmte Zwecke, tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz** gebunden sein. c) Schon die Übermittlungsregelung bedarf einer in sich geschlossenen **Begrenzung der Zwecke der möglichen späteren Datenverwendung in der Übermittlungsregelung**. d) Die Befugnis zum **Datenabruf** muss nicht nur für sich genommen **verhältnismäßig** sein, sondern ist überdies an die in der Übermittlungsregelung **begrenzten Verwendungszwecke** gebunden. Die beiden Regelungen müssen also ein in sich geschlossenes Konstrukt darstellen und begrenzen sich gegenseitig.

Auch die Eingriffsschwellen sind eng und klar begrenzt: a) Trotz des geringeren Eingriffsgewichts bedürfen die allgemeinen Befugnisse zur Übermittlung und zum Abruf von Bestandsdaten für die Gefahrenabwehr und die Tätigkeit der Nachrichtendienste **grundsätzlich einer im Einzelfall vorliegenden konkreten Gefahr** und für die Strafverfolgung eines **Anfangsverdachts**. b) Die deutlich schwerwiegendere Zuordnung dynamischer IP-Adressen muss auch dem **Schutz oder der Bewehrung von Rechtsgütern von hervorgehobenem Gewicht** dienen; zudem ist eine ordnungsgemäße **Dokumentation** der Entscheidungsgrundlagen notwendig. c) Das Vorliegen einer **konkretisierten Gefahr** kann ausnahmsweise genügen, soweit es um den Schutz von Rechtsgütern oder die Verhütung von Straftaten von zumindest **erheblichem Gewicht** (allgemeine Bestandsdatenauskunft) oder **besonderem Gewicht** (Zuordnung dynamischer IP-Adressen) geht. Darüber hinaus stellt das BVerfG klar, dass es dem Gesetzgeber freistünde, den Abruf der Daten an noch weitergehende Anforderungen zu binden.

Die angegriffenen Regelungen genügten diesen Anforderungen nicht. Die in § 113 Abs. 1 Satz 1 TKG geregelte allgemeine Bestandsdatenauskunft stelle einen Eingriff in das Recht auf informationelle Selbstbestimmung dar, der zwar nicht von sehr großem Gewicht, aber dennoch unverhältnismäßig sei. **Anlasslose Auskünfte seien nicht zulässig**. Eingriffsgrundlagen müssten regelmäßig zumindest eine hinreichend konkretisierte Gefahr verlangen. Eine Absenkung der Eingriffsschwellen sei aus Gründen der Verhältnismäßigkeit untrennbar verbunden mit erhöhten Anforderungen an die konkret zu schützenden Rechtsgüter. Das BVerfG schafft also eine klare Notwendigkeit der Verhältnismäßigkeit im engeren Sinne, eine Abwägung muss dabei zwischen Mittel und Zweck erfolgen. Diesen verfassungsrechtlichen Anforderungen genüge § 113 Abs. 1 Satz 1 TKG nicht, denn die Übermittlungsregelung öffneten das manuelle Auskunftsverfahren viel zu weit.

Zudem dürften die beiden Schritte weder voneinander losgelöst betrachtet werden noch zur Begründung aufeinander verweisen. Denn die Übermittlung und der Abruf personenbezogener Daten stellten je einen eigenständigen Grundrechtseingriff dar. Daher müssten sie auch auf einer **eigenen gesetzlichen Grundlage** beruhen und den **Anforderungen der Verhältnismäßigkeit sowie der Normenklarheit und Bestimmtheit** genügen.
Der 1. Senat bedient sich hier des Bildes einer **Doppeltür**: Eingriffsschwellen müssten schon in der Übermittlungsregelung selbst – als der im Bild der Doppeltür ersten Tür – geregelt werden. Die korrespondierenden Abrufregelungen des Bundeskriminalamtgesetzes, des Bundespolizeigesetzes, des Zollfahndungsdienstgesetzes, des Bundesverfassungsschutzgesetzes, des BND-Gesetzes und des MAD-Gesetzes, seien hier als zweite Tür zu sehen. Sie erlauben den Abruf der erhobenen Daten durch die Sicherheitsbehörden. Nach Ansicht des 1. Senats genügen auch sie weitgehend nicht den verfassungsrechtlichen Anforderungen.

Auch auf **europarechtlicher und internationaler Ebene** wurde der Datenschutz gestärkt: Im **„Schrems II"-Verfahren** erklärte der **EuGH** ein Abkommen zur **Übermittlung von personenbezogenen Daten in die Vereinigten Staaten** für unwirksam (Urt. v. 16. Juli 2020, Az. C-311/18). Informationen über europäische Verbraucher seien auf US-Servern nicht genügend vor dem Zugriff dortiger Behörden und Geheimdienste geschützt, entschieden die Richter.

Unter dem Datenschutzabkommen **„Privacy Shield"** hatten sich über 4.000 US-amerikanische

Unternehmen zertifizieren lassen. Das Abkommen erlaubte es ihren Geschäftspartnern in der EU, personenbezogene Daten zertifizierten Unternehmen in den USA zu übermitteln. Der „Privacy Shield“ fußt auf einem Durchführungsbeschluss der EU-Kommission. Dieses wurde notwendig, nachdem der EuGH 2015 das sog. **„Safe Harbor“** Abkommen für ungültig erklärt hatte **(Urt. v. 6. Oktober 2015, Az. C-362/14, „Schrems I“)**. Doch auch das nachgebesserte Abkommen genüge nicht den Anforderungen des EU-Datenschutzes: Auch wenn die US-Nachrichtendienste beim Zugriff auf personenbezogene Daten bestimmte Anforderungen zu beachten hätten, seien deren Überwachungsprogramme weiterhin nicht auf das zwingend erforderliche Maß beschränkt, die Daten europäischer Nutzer in den USA damit **nicht angemessen geschützt**. Auch der **Ombudsmechanismus** böte Betroffenen in der EU **keinen genügenden Rechtsbehelf**. Damit verstoße der „Privacy Shield“ auch gegen Art. 47 der Europäischen Grundrechte-Charta, wonach jeder Person ein wirksamer Rechtsbehelf gegen Grundrechtseingriffe zustehen muss. Die sogenannten **Standardvertragsklauseln**, die ebenfalls Gegenstand des Verfahrens waren, hält der EuGH aber weiterhin für **gültig**. Bedenken wie beim „Privacy Shield“ hatten die Richter hier nicht.

https://www.juracademy.de

Stand: 31.07.2020