1 BvR 1873/13 und 1 BvR 2618/13 - Schrankenlose Auskunft zu Bestandsdaten verfassungswidrig

?? 113 TKG teilweise verfassungswidrig, Gefahrenabwehr und Geheimdienste (pr??ventiv) erhalten Bestandsdaten nur bei im Einzelfall vorliegender konkreter Gefahr, bei Strafverfolgung ist ein Anfangsverdacht notwendig

Mit Beschluss vom 27.05.2020 hat der Erste Senat des Bundesverfassungsgerichts § 113 TKG (des Telekommunikationsgesetzes) und mehrere Fachgesetze des Bundes, die die manuelle Bestandsdatenauskunft regeln, für verfassungswidrig erklärt. Sie verletzen die beschwerdeführenden Inhaber von Telefon- und Internetanschlüssen in ihren Grundrechten auf informationelle Selbstbestimmung sowie auf Wahrung des Telekommunikationsgeheimnisses (Art. 10 Abs. 1 GG).

Die manuelle Bestandsdatenauskunft ermöglicht es Sicherheitsbehörden, von Telekommunikationsunternehmen Auskunft insbesondere über den Anschlussinhaber eines Telefonanschlusses oder einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse zu erlangen. Mitgeteilt werden personenbezogene Daten der Kunden, die im Zusammenhang mit dem Abschluss oder der Durchführung von Verträgen stehen (sogenannte Bestandsdaten). Nicht mitgeteilt werden dagegen Daten, die sich auf die Nutzung von Telekommunikationsdiensten (sogenannte Verkehrsdaten) oder den Inhalt von Kommunikationsvorgängen beziehen.

Die Erteilung einer Auskunft über Bestandsdaten ist grundsätzlich verfassungsrechtlich zulässig. Der Gesetzgeber muss aber nach dem Bild einer Doppeltür sowohl für die Übermittlung der Bestandsdaten durch die Telekommunikationsanbieter als auch für den Abruf dieser Daten durch die Behörden jeweils verhältnismäßige Rechtsgrundlagen schaffen. Übermittlungs- und Abrufregelungen müssen die Verwendungszwecke der Daten hinreichend begrenzen, indem sie insbesondere tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz vorsehen.

Der Senat hat klargestellt, 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. Findet eine Zuordnung dynamischer IP-Adressen statt, muss diese im Hinblick auf ihr erhöhtes Eingriffsgewicht darüber hinaus auch dem Schutz oder der Bewehrung von Rechtsgütern von zumindest hervorgehobenem Gewicht dienen. Bleiben die Eingriffsschwellen im Bereich der Gefahrenabwehr oder der nachrichtendienstlichen Tätigkeit hinter dem Erfordernis einer konkreten Gefahr zurück, müssen im Gegenzug erhöhte Anforderungen an das Gewicht der zu schützenden Rechtsgüter vorgesehen werden. Die genannten Voraussetzungen wurden von den angegriffenen Vorschriften weitgehend nicht erfüllt. Im Übrigen hat der Senat wiederholend festgestellt, dass eine Auskunft über Zugangsdaten nur dann erteilt werden darf, wenn die gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind.

Sachverhalt:

§ 113 TKG berechtigt Anbieter von Telekommunikationsdiensten zur Übermittlung von Bestandsdaten im sogenannten manuellen Auskunftsverfahren. Die weiteren angegriffenen Normen regeln den Abruf dieser Daten durch verschiedene Sicherheitsbehörden des Bundes, wie etwa das Bundeskriminalamt, die Bundespolizei und das Bundesamt für Verfassungsschutz. Alle angegriffenen Regelungen sollten der Umsetzung der Entscheidung des Bundesverfassungsgerichts vom 24. Januar 2012 (Bestandsdatenauskunft I) dienen, mit der § 113 TKG in seiner damaligen Fassung teilweise für verfassungswidrig erklärt und das Fehlen fachrechtlicher Abrufregelungen beanstandet wurde.

Die Auskunft nach § 113 TKG erfolgt auf Verlangen einer der dort genannten Sicherheitsbehörden an die Anbieter von Telekommunikationsdiensten. Nach § 113 Abs. 1 Satz 1 TKG umfasst die zu erteilende

Auskunft neben den gemäß § 111 TKG verpflichtend zu speichernden Bestandsdaten wie etwa Name, Geburtsdatum und Rufnummer eines Anschlussinhabers auch die von den Dienste-anbietern nach § 95 TKG freiwillig zu betrieblichen Zwecken gespeicherten Kundendaten. Dazu gehören üblicherweise die Anschrift der Vertragspartner, die Art des kontrahierten Dienstes und weitere Daten wie zum Beispiel die Bankverbindung.

Nach § 113 Abs. 1 Satz 2 TKG ist eine Auskunft auch über vom Diensteanbieter vergebene Zugangsdaten wie zum Beispiel die Persönliche Identifikationsnummer (PIN) zu erteilen. Von Nutzerinnen und Nutzern selbst vergebene Passwörter werden dagegen von den Diensteanbietern üblicherweise nur verschlüsselt gespeichert. Eine Auskunft kann insoweit nicht erteilt werden.

Bestandsdaten dürfen gemäß § 113 Abs. 1 Satz 3 TKG auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokolladresse (dynamische IP-Adresse) bestimmt werden. Gegenstand der Auskunft ist die Zuordnung der IP-Adresse zu einem bestimmten Anschlussinhaber und damit selbst ein Bestandsdatum. Dies ist nur möglich, wenn Anbieter zuvor bei ihnen gespeicherte Verkehrsdaten auswerten, um festzustellen, welchem Anschlussinhaber die verwendete IP-Adresse zu dem angefragten Zeitpunkt zugeordnet war.

Gemäß § 113 Abs. 2 Satz 1 TKG darf eine Auskunft nur erteilt werden, soweit eine in § 113 Abs. 3 TKG genannte Stelle dies zum Zweck der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste unter Angabe einer Abrufregelung verlangt.

Die mit den Verfassungsbeschwerden angegriffenen Abrufregelungen des Bundes bestimmen, dass die Sicherheitsbehörden von den Diensteanbietern Auskunft über Bestandsdaten verlangen dürfen. Im Wesentlichen verlangen sie nur, dass die Auskunft zur Erfüllung ihrer jeweils genannten Aufgaben erforderlich sein muss. Für die Auskunft über Zugangsdaten wird vorausgesetzt, dass die gesetzlichen Voraussetzungen für deren Nutzung vorliegen. Weiter sehen die Vorschriften jeweils vor, dass auch die Auskunft von Bestandsdaten, die anhand einer dynamischen IP-Adresse bestimmt werden, verlangt werden darf. Ermächtigt werden das Bundeskriminalamt, die Bundespolizei, das Zollkriminalamt sowie die Nachrichtendienste des Bundes.

Wesentliche Erwägungen des Senats:

I. Die angegriffenen Übermittlungsbefugnisse in § 113 TKG genügen in materieller Hinsicht nicht den verfassungsrechtlichen Anforderungen des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG sowie des durch Art. 10 Abs. 1 GG gewährleisteten Telekommunikationsgeheimnisses. Zwar dienen sie legitimen Zwecken – der Effektivierung der Strafverfolgung und der Gefahrenabwehr sowie der Erfüllung der Aufgaben der Nachrichtendienste. Mit den Anforderungen der Verhältnismäßigkeit im engeren Sinne sind die Übermittlungsregelungen aber nur vereinbar, wenn sie die Verwendungszwecke der einzelnen Befugnisse selbst hinreichend normenklar begrenzen.

1. Diesen Anforderungen genügt die in § 113 Abs. 1 Satz 1 TKG geregelte Befugnis zur allgemeinen Bestandsdatenauskunft nicht.

a) Die in § 113 Abs. 1 Satz 1 TKG eröffnete allgemeine Bestandsdatenauskunft begründet einen Eingriff in das Recht auf informationelle Selbstbestimmung. Dieser ist zwar nicht von sehr großem Gewicht. Trotzdem erweist sich die angegriffene Übermittlungsbefugnis aufgrund ihrer Reichweite als unverhältnismäßig. Auch Auskünfte über Daten, deren Aussagekraft und Verwendungsmöglichkeiten eng begrenzt sind, dürfen nicht ins Blaue hinein zugelassen werden. Dazu bedarf es begrenzender Eingriffsschwellen, die sicherstellen, dass Auskünfte nur bei einem auf tatsächliche Anhaltspunkte gestützten Eingriffsanlass eingeholt werden können. Anlasslose Auskünfte, die allein der allgemeinen Wahrnehmung behördlicher Aufgaben dienen, sind nicht zulässig. Eingriffsschwellen müssen schon in der Übermittlungsregelung selbst – als der im Bild der Doppeltür ersten Tür – geregelt werden.

Erforderlich ist bezogen auf die Gefahrenabwehr und die Tätigkeit der Nachrichtendienste grundsätzlich eine im Einzelfall vorliegende konkrete Gefahr. Bezogen auf die Strafverfolgung genügt das Vorliegen eines Anfangsverdachts.

Der Gesetzgeber ist von Verfassungs wegen aber nicht von vornherein auf die Schaffung von Eingriffstatbeständen beschränkt, die dem tradierten sicherheitsrechtlichen Modell der Abwehr konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren entsprechen. Vielmehr kann er die Grenzen unter besonderen Voraussetzungen auch weiter ziehen, indem er die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs reduziert. Eingriffsgrundlagen müssen regelmäßig zumindest eine hinreichend konkretisierte Gefahr verlangen. Eine solche Absenkung der Eingriffsschwellen ist aus Gründen der Verhältnismäßigkeit untrennbar verbunden mit erhöhten Anforderungen an die konkret geschützten Rechtsgüter, wobei stets auch das Eingriffsgewicht der jeweiligen Maßnahme zu berücksichtigen ist. Weniger gewichtige Eingriffe wie die allgemeine Bestandsdatenauskunft können daher beim Vorliegen einer konkretisierten Gefahr bereits dann zu rechtfertigen sein, wenn sie dem Schutz von Rechtsgütern von zumindest erheblichem Gewicht dienen.

Diese verfassungsrechtlichen Anforderungen gelten grundsätzlich für alle Eingriffsermächtigungen mit präventiver Zielrichtung und damit auch für die Verwendung der Daten durch Nachrichtendienste. Dort kann es bereits genügen, dass eine Auskunft zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten ist, denn damit wird ein wenigstens der Art nach konkretisiertes und absehbares Geschehen vorausgesetzt.

Demgegenüber kann im Bereich der Strafverfolgung eine in tatsächlicher Hinsicht unterhalb des Anfangsverdachts liegende Eingriffsschwelle zur Vornahme von grundrechtsrelevanten Eingriffen nicht genügen.

b) Diesen verfassungsrechtlichen Anforderungen genügt § 113 Abs. 1 Satz 1 TKG nicht. Die Übermittlungsregelung öffnet das manuelle Auskunftsverfahren sehr weit, indem sie Auskünfte allgemein zum Zweck der Gefahrenabwehr, zur Verfolgung von Straftaten oder Ordnungswidrigkeiten sowie zur Erfüllung nachrichtendienstlicher Aufgaben erlaubt und dabei keine ihre Reichweite näher begrenzenden Eingriffsschwellen enthält. Die Regelung ermöglicht die Erteilung einer Auskunft im Einzelfall vielmehr bereits dann, wenn dies allgemein zur Wahrnehmung der genannten Aufgaben erfolgt.

3. Auch die in § 113 Abs. 1 Satz 3 TKG neu geschaffene Befugnis, anhand einer dynamischen IP-Adresse bestimmte Bestandsdaten zu übermitteln, genügt nicht den Anforderungen der Verhältnis-mäßigkeit und verstößt damit gegen Art. 10 Abs. 1 GG.

a) Die Vorschrift hat ein gegenüber der allgemeinen Bestandsdatenauskunft erhöhtes Eingriffsgewicht. Ihr kommt aufgrund der Aussagekraft der Zuordnung einer dynamischen IP-Adresse, die eine Rekonstruktion der individuellen Internetnutzung zu einem bestimmten Zeitpunkt ermöglicht, sowie der Verwendung von Verkehrsdaten durch die Anbieter eine erheblich größere Persönlichkeitsrelevanz zu. Zudem begründet sie einen Eingriff in das Fernmeldegeheimnis des Art. 10 Abs. 1 GG. Dem erhöhten Eingriffsgewicht muss durch eine Beschränkung auf den Schutz oder die Bewehrung von Rechtsgütern von zumindest hervorgehobenem Gewicht Rechnung getragen werden. Dies schließt die Zuordnung dynamischer IP-Adressen etwa zur Verfolgung nur geringfügiger Ordnungswidrigkeiten aus. Soll schon eine konkretisierte Gefahr als Eingriffsschwelle genügen, bedarf es einer darüber hinausgehenden Beschränkung der Auskunft auf den Schutz von besonders gewichtigen Rechtsgütern. Dazu zählt die Verhütung zumindest schwerer Straftaten.

b) Diesen Anforderungen genügt § 113 Abs. 1 Satz 3 TKG nicht. Die Vorschrift lässt eine Zuordnung dynamischer IP-Adressen unter denselben Voraussetzungen wie die allgemeine Bestandsdatenauskunft zu. Sie ist damit weder an ihre Reichweite näher begrenzende Eingriffsschwellen gebunden noch enthält sie Anforderungen an das Gewicht der zu schützenden Rechtsgüter. Die Vorschrift ist daher unverhältnismäßig.

II. Die mit § 113 TKG korrespondierenden Abrufregelungen des Bundeskriminalamtgesetzes, des Bundespolizeigesetzes, des Zollfahndungsdienstgesetzes, des Bundesverfassungsschutzgesetzes, des

BND-Gesetzes und des MAD-Gesetzes, die – als zweite Tür – den Abruf der von den Telekommunikationsunternehmen erhobenen Daten durch die Sicherheitsbehörden regeln, genügen weitgehend ebenfalls nicht den verfassungsrechtlichen Anforderungen.

1. Da Übermittlung und Abruf personenbezogener Daten je eigenständige Grundrechtseingriffe begründen, müssen auch die einzelnen Abrufregelungen auf einer eigenen gesetzlichen Grundlage beruhen und den Anforderungen der Verhältnismäßigkeit sowie der Normenklarheit und Bestimmtheit genügen.

2. a) Die Abrufregelungen schaffen zwar jeweils hinreichend bestimmt und normenklar spezifische Ermächtigungsgrundlagen. Sie sind jedoch mit Blick auf ihr Eingriffsgewicht überwiegend nicht verhältnismäßig ausgestaltet. Fast alle Regelungen, die zur allgemeinen Bestandsdatenauskunft ermächtigen, setzen keine den Datenabruf begrenzenden Eingriffsschwellen voraus und enthalten solche auch nicht durch normenklare Verweisungen, sondern erlauben – wie schon die Übermittlungsregelung – den Abruf von Bestandsdaten generell zur Wahrnehmung der behördlichen Aufgaben. Ausnahmen stellen insoweit nur Teilregelungen des Bundespolizeigesetzes und des Bundeskriminalamtgesetzes dar.

b) Die angegriffenen Befugnisse zum Abruf von Zugangsdaten sind dagegen für sich genommen hinreichend begrenzt und verhältnismäßig. Die Regelungen stellen sicher, dass Zugangsdaten nicht unabhängig von den Anforderungen an deren Nutzung und damit gegebenenfalls unter leichteren Voraussetzungen abgefragt werden können.

c) Abrufregelungen, die zum Abruf von Bestandsdaten anhand dynamischer IP-Adressen ermächtigen, müssen neben einer hinreichenden Begrenzung der Verwendungszwecke auch eine nachvollziehbare und überprüfbare Dokumentation der Entscheidungsgrundlagen des Abrufs vorsehen. Diesen Anforderungen genügen die angegriffenen Regelungen nicht. Sie sind ganz überwiegend schon deshalb unverhältnismäßig, weil sie keine begrenzenden Eingriffsschwellen voraussetzen. Zudem enthält keine der angegriffenen Regelungen eine Pflicht zur Dokumentation der Entscheidungsgrundlagen.