



Bonn, den 21. April 2017

**Stellungnahme der Bundesbeauftragten für
den Datenschutz und die Informationsfreiheit**

ZUR

**Verfassungsbeschwerde des Herrn Patrick Löhr,
Posteo e.K.**

Aktenzeichen: 2 BvR 2377/16



Aus datenschutzrechtlicher Sicht geht es bei dem gegenständlichen Rechtsstreit um mehr, als um die Frage, ob ein unverhältnismäßiger Eingriff in die Grundrechte des Beschwerdeführers vorliegt. Vielmehr wirft das Verfahren inzident eine elementare telekommunikationsrechtliche Problematik auf, die erhebliche Auswirkungen auf den Datenschutz in diesem Sektor hat.

So stellt sich die Frage, ob ein Telekommunikationsanbieter seine Infrastruktur dahingehend ausgestalten muss, dass sämtliche Daten, die potenziell Gegenstand eines sicherheitsbehördlichen Auskunftsverlangens sein können, auch dann tatsächlich für einen solchen Fall zur Verfügung stehen, obwohl sie eigentlich nicht für die Erbringung des Dienstes benötigt werden.

1. Systematik des telekommunikationsrechtlichen Auskunftsanspruchs

Telekommunikationsanbieter sind verpflichtet, die bei ihnen bei der Dienstleistung anfallenden Daten anfragenden Sicherheitsbehörden im Rahmen eines Auskunftsersuchens zur Verfügung zu stellen. Entsprechende Rechtsgrundlagen finden sich in den §§ 110 ff. des Telekommunikationsgesetzes (TKG) und der Telekommunikationsüberwachungsverordnung (TKÜV).

Bislang war es jedoch unbestritten, dass sich diese Auskunftspflicht ausschließlich auf die Daten bezieht, die der Telekommunikationsanbieter nach § 96 TKG verarbeitet und die ihm in diesem Zusammenhang auch tatsächlich vorliegen (vgl. z.B. *MüKoStPO/Günther*, 1. Auflage, § 100g Rn. 8). Eine Ausnahme von diesem Grundsatz stellt lediglich die sogenannte Vorratsdatenspeicherung dar, die erst kürzlich durch das „Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten“ wieder eingeführt wurde.

Unabhängig davon, ob die Daten aus betrieblichen Zwecken oder für die Nutzung durch Sicherheitsbehörden im Rahmen der Vorratsdatenspeicherung bei den TK-Anbietern vorgehalten werden, sind die Rechtsgrundlagen für ihre Speicherung, schon aufgrund des mit ihrer Verarbeitung verbundenen Eingriffs in Artikel 10 GG – jedenfalls soweit es sich um Verkehrsdaten handelt –, explizit in entsprechenden gesetzlichen Normen aufgeführt.

a) Datenerhebung für betriebliche Zwecke

Die Rechtsgrundlagen, nach denen TK-Anbieter Bestands- und Verkehrsdaten für betriebliche Zwecke erheben dürfen, sind die §§ 95 und 96 TKG. Obwohl die



hier thematisierte Systematik des telekommunikationsrechtlichen Auskunftsanspruchs beide Datenarten betrifft, beziehe ich mich im Folgenden nur auf Verkehrsdaten, da es sich bei den im vorliegenden Verfahren streitgegenständlichen Daten um Verkehrsdaten in Form von IP-Adressen handelt.

Gemäß § 3 Nummer 30 TKG sind Verkehrsdaten solche Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. § 96 Abs. 1 Satz 1 TKG konkretisiert weitergehend, welche dieser Verkehrsdaten von TK-Anbietern für ihre betrieblichen Zwecke erhoben und verwendet werden dürfen. Dabei stellt die Norm lediglich die Berechtigung zur Erhebung der benannten Verkehrsdaten dar, nicht jedoch eine Erhebungspflicht (vgl. *LG München I, Urteil vom 12.01.2012 – 17 HK O 1398/11*).

Hierunter fallen zunächst einmal das eigentliche Erbringen des Telekommunikationsdienstes – also der Aufbau und das Halten einer Telekommunikationsverbindung zwischen zwei oder mehreren Parteien – sowie die damit verbundene Entgeltermittlung und Abrechnung im Sinne des § 97 TKG. Darüber hinaus sind das Erkennen und Beseitigen von Störungen nach § 100 Abs. 1 TKG oder eines Missbrauchs im Sinne des § 100 Abs. 3 TKG wesentliche Gründe für die Verarbeitung von Verkehrsdaten.

Alle dieser Erlaubnistatbestände stehen allerdings unter dem Vorbehalt der Erforderlichkeit. Hiermit wird unter anderem dem datenschutzrechtlichen Grundsatz der Datensparsamkeit Rechnung getragen. Dementsprechend sieht das TKG für die betriebliche Nutzung von Daten auch keine Mindestspeicherfrist, sondern lediglich Höchstspeicherfristen vor, die wiederum ebenfalls unter den Vorbehalt der Erforderlichkeit gestellt werden.

Ob das Erheben von Verkehrsdaten im jeweiligen Einzelfall erforderlich ist, hängt also von der konkreten Ausgestaltung des Telekommunikationsdienstes und des konkreten Verwendungszwecks ab (vgl. *Beck'scher TKG-Kommentar/Braun, 4. Auflage, § 96 Rn. 12*). Gerade aufgrund der hohen Sensibilität der unter das Fernmeldegeheimnis fallenden Verkehrsdaten versteht es sich von selbst, dass die Erforderlichkeit einer Datenverarbeitung vorliegend äußerst restriktiv auszulegen ist.

Eine darüber hinausgehende Erhebung oder Verwendung von Verkehrsdaten für betriebliche Zwecke ist nach § 96 Abs. 2 TKG explizit ausgeschlossen.



b) Datenerhebung für sicherheitsbehördliche Zwecke

Neben der Erhebungsbefugnis für betriebliche Zwecke sieht das TKG seit der Wiedereinführung der Vorratsdatenspeicherung durch das „Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten“ auch wieder die Verpflichtung vor, Verkehrsdaten unabhängig von der betrieblichen Erforderlichkeit eine gewisse Zeit zu speichern. Diese Daten dürfen jedoch ausschließlich genutzt werden, um sie berechtigten Sicherheitsbehörden im Bedarfsfall zur Verfügung zu stellen.

Die wesentlichen Vorgaben zu den zu speichernden Datenkategorien sowie den Speicher- und Löschrufen finden sich in § 113b TKG. Auch IP-Adressen fallen grundsätzlich unter diese Speicherpflicht und müssen von den verpflichteten TK-Anbietern für 10 Wochen vorgehalten werden. Dies gilt aber nur, soweit sie im Zusammenhang mit der Bereitstellung eines Internet- oder VoIP-Zugangs erzeugt werden. Eine Speicherung von Verkehrsdaten, die im Zusammenhang mit der Erbringung eines E-Mail-Dienstes stehen, hat der Gesetzgeber hingegen explizit von der Speicherpflicht aus §§ 113a TKG ff. ausgenommen (vgl. *BT-Drs. 18/5088, S. 23*).

Eine darüber hinausgehende weitere Verpflichtung zur Speicherung von Verkehrsdaten für sicherheitsbehördliche Zwecke existiert weder im TKG noch in anderen Gesetzen.

c) Zwischenergebnis

Erbringer eines TK-Dienstes haben das Recht, die IP-Adressen ihrer Kunden im Rahmen der Erforderlichkeit nach § 96 TKG zu erheben und verarbeiten. Eine darüber hinausgehende Verpflichtung zur Speicherung dieser Daten für eine Mindestfrist existiert hingegen nicht, wenn sie im Zusammenhang mit der Erbringung eines E-Mail-Dienstes erzeugt werden, da diese Daten explizit von der Speicherpflicht der §§ 113a TKG ff. ausgenommen sind.

2. Potentielle Erweiterung der Verkehrsdatenspeicherpflicht

Entsprechend den Vorgaben des Bundesverfassungsgerichts im Zusammenhang mit dem von diesem entwickelten sogenannten Doppeltürenmodell (vgl. *BVerfG, Beschluss vom 24.01.2012, 1 BvR 1299/05, Rn. 123*) existieren neben den oben beschriebenen Rechtsgrundlagen für die Datenerhebung bei TK-



Anbietern korrespondierende Rechtsgrundlagen, nach denen die auskunftser-suchenden Sicherheitsbehörden Verkehrsdaten bei den TK-Anbietern abfragen können. Entsprechende Vorschriften finden sich beispielsweise in § 100g StPO für retrograde Datenerhebungen oder in § 110 TKG i.V.m. § 7 TKÜV für Daten-übermittlungen in Echtzeit.

Aus Sicht der TK-Anbieter handelt es sich bei diesen Normen um „andere ge-setzliche Vorschriften“ i.S.d. § 96 Abs. 1 Satz 2 TKG. Sie sind damit Grundlage, um die Verwendung der Daten in Form einer Übermittlung an die abfragende Behörde im Rahmen eines Auskunftersuchens zu rechtfertigen. Da die Vor-schrift des § 96 TKG aber, wie bereits dargelegt, lediglich eine Berechtigung zur Datenerhebung und im Gegensatz zu den §§ 113a TKG ff. keine Erhebungs-pflicht darstellt, stellt auch § 96 Abs. 1 Satz 2 TKG i.V.m. einer sicherheitsbe-hördlichen Abfragenorm keine Datenerhebungsverpflichtung für TK-Anbieter dar.

In Anbetracht dessen könnte weitergehend argumentiert werden, dass eine konkludente Datenerhebungsverpflichtung für die TK-Anbieter unmittelbar aus einer entsprechenden sicherheitsbehördlichen Abfragegrundlage abgeleitet werden müsste. Gegen eine derartige Ausweitung des Regelungsgehalts dieser Normen sprechen allerdings gleich mehrere Aspekte.

Zum einen kann in vielen Fällen bereits dem Wortlaut der Vorschriften entnom-men werden, dass sie eben keine Datenerhebungsbegründung für TK-Anbieter darstellen sollen, sondern lediglich eine Legitimation zur Erhebung der Daten durch die jeweils ermächtigten Sicherheitsbehörden. Dass hierbei lediglich auf bei den TK-Anbietern bereits vorliegende Daten zugegriffen werden kann zeigt sich gerade im Fall des im vorliegenden Verfahren in Rede stehenden § 7 TKÜV unzweifelhaft. Hier heißt es in Bezug auf die bereitzustellenden Daten in Absatz 1:

*„Der Verpflichtete hat der berechtigten Stelle als Teil der Überwachungskopie auch die folgenden **bei ihm vorhandenen Daten** bereitzustellen, [...]“.*

Auch dem Wortlaut des § 100 g StPO kann man – wenn auch nicht gleicher-maßen offensichtlich – entnehmen, dass es sich bei den in Rede stehenden Daten um solche handelt, die bereits beim von der Norm selbst nicht adressier-ten TK-Anbieter vorliegen. So wird in Absatz 1 der Vorschrift explizit auf „Ver-kehrsdaten [nach] § 96 Absatz 1 des Telekommunikationsgesetzes“ Bezug ge-nommen. In Absatz 2 heißt es noch deutlicher „die nach § 113b des Telekom-munikationsgesetzes **gespeicherten Verkehrsdaten**“. Der Gesetzestext nimmt



SEITE 6 VON 9

damit eindeutig Bezug auf Daten, die nach oben unter 1. angeführten Rechtsgrundlagen erhoben worden sind.

Des Weiteren genügen die hier beispielhaft betrachteten Vorschriften nicht den verfassungsrechtlich gebotenen Voraussetzungen in Bezug auf die Normenklarheit, um in konkludenter Weise für TK-Anbieter eine Datenerhebungsverpflichtung begründen zu können. Zwar hat das Bundesverfassungsgericht im Zusammenhang mit dem bereits erwähnten Doppeltürenmodell, dessen Grundgedanken nach meinem Verständnis zumindest sinngemäß auf die hier diskutierte Rechtsfrage übertragen werden können, ausgeführt, dass erforderliche Rechtsgrundlagen für verschiedenartige Datenverarbeitungsvorgänge in einer Norm zusammengefasst werden können. Dabei hat es aber gleichzeitig darauf hingewiesen, dass die Maßgaben der Kompetenzordnung und die Anforderungen der Normenklarheit in einer solchen Norm zwingend berücksichtigt werden müssen (vgl. *BVerfG*, aaO). Mit Blick auf den bereits angesprochenen Wortlaut der Vorschriften und dem Fehlen anderweitiger Anhaltspunkte, aus denen darauf geschlossen werden könnte, dass die Normen eine Datenerhebungsverpflichtung für TK-Anbieter begründen sollen, wird deutlich, dass die vorab genannten Anforderungen hier nicht erfüllt werden.

Schließlich spricht auch eine systematische Überlegung gegen die konkludente Ausweitung von Normen zur Legitimation sicherheitsbehördlicher Abfragen. Hätte der Gesetzgeber ein derartiges Verständnis vom Regelungsgehalt der in Rede stehenden Vorschriften, wäre die Wiedereinführung der Vorratsdatenspeicherung durch das „Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten“ nicht erforderlich gewesen. Eine Verpflichtung zur Vorhaltung von Verkehrsdaten für sicherheitsbehördliche Auskunftersuchen wäre bereits als in der Abfragebefugnis inkludierte Vorgabe an die TK-Anbieter enthalten und eine gesonderte gesetzliche Speicherverpflichtung damit überflüssig.

Im Ergebnis gibt es somit auch keine weiteren Grundlagen, die eine Erweiterung der den TK-Anbietern obliegenden Pflichten zur Speicherung von Verkehrsdaten über die vom TKG vorgegebenen Regelungen hinaus legitimieren könnten.



3. Ergebnis

Die Funktionsfähigkeit einer effektiven Strafverfolgung und Gefahrenabwehr ist zum Schutz der Bevölkerung und für den Bestand des Rechtsstaats essentiell. Dementsprechend ist es richtig und notwendig, den mit diesen Aufgaben betrauten Behörden die erforderlichen Mittel an die Hand zu geben, um die ihnen zukommende Funktion bestmöglich erfüllen zu können. Dieser Grundsatz ist auch aus datenschutzrechtlicher Sicht nicht bestritten.

Ebenso unbestritten ist allerdings auch die Tatsache, dass ein Großteil der Maßnahmen, die Sicherheitsbehörden im Rahmen ihrer Aufgabenerfüllung ergreifen, mit teilweise erheblichen Grundrechtseingriffen einhergehen und daher verfassungsrechtlich nur dann legitimiert sein können, wenn sie verhältnismäßig ausgestaltet sind.

Bei dem hier gegenständlichen Rechtsstreit geht es aus datenschutzrechtlicher Sicht allerdings vorrangig weder darum, ob ein E-Mailanbieter unverhältnismäßig in seinen Grundrechten aus Art. 12 und 14 GG beschränkt wird, noch darum, ob die Ausleitung eines Verkehrsdatums in Form einer öffentlichen IP-Adresse im Rahmen einer Telekommunikationsüberwachung als ein im Einzelfall unverhältnismäßiger Grundrechtseingriff zu bewerten ist. Aus datenschutzrechtlicher Sicht ist das vorliegende Verfahren vielmehr gerade deshalb bedeutend, weil es einen Präzedenzfall für die zukünftige Systematik der sicherheitsbehördlichen Auskunftsverfahren im TK-Bereich darstellen kann.

Bislang gilt der Grundsatz: Bei Vorliegen einer entsprechenden Rechtsgrundlage müssen TK-Anbieter die bei ihnen vorliegenden Verkehrsdaten anfragenden Sicherheitsbehörden zur Verfügung stellen. Ob und welche Daten vorhanden sind, richtet sich nach den Vorgaben des TKG, das diesbezüglich in § 96 und §§ 113a ff. abschließend Regelungen trifft. Liegt ein von Sicherheitsbehörden abgefragtes Datum beim TK-Anbieter nicht vor, weil es aus betrieblichen Gründen für die Dienstleistung nicht oder nicht mehr erforderlich ist, oder weil eine anderweitige Verpflichtung zu dessen Speicherung nicht existiert, kann die begehrte Auskunft nicht erteilt werden. Insbesondere besteht aktuell keine weitergehende rechtliche Verpflichtung, die den TK-Anbieter nötigt, das begehrte Datum aufgrund der Anfrage überobligatorisch zu erheben.

Sollte nunmehr im Rahmen der zur Entscheidung vorliegenden Rechtsfrage festgestellt werden, dass ein TK-Anbieter in Abkehr von der bisherigen Regelungssystematik verpflichtet ist, seine Datenverarbeitungsprozesse aufgrund sicherheitsbehördlicher Auskunftersuchen über die nach dem TKG eigentlich



erforderlichen Maße hinaus umzugestalten, besteht die Gefahr, dass hierdurch das aktuell geltende Ursache-Folge-Verhältnis in diesem Bereich ins Gegenteil verkehrt wird.

Der Zugriff auf Verkehrsdaten durch Sicherheitsbehörden ist gegenwärtig erforderlich, um durch Schaffung eines hoheitlich behördlichen Handlungsspielraums auch im technischen Bereich der Telekommunikation hinreichende Sicherheit gewährleisten zu können. Ursache ist jedoch zunächst das Vorliegen von Telekommunikationsdaten, auf die als Folge der hoheitliche Zugriff ermöglicht werden muss.

Mit der Verpflichtung, nach den aktuellen Vorschriften des TKG eigentlich nicht erforderliche Daten überhaupt erst zu erheben, um ein Auskunftersuchen erfüllen zu können, würde das eigentliche Entstehen von Telekommunikationsdaten zu einem Mittel, das nicht der Telekommunikation selbst, sondern ausschließlich der Unterstützung und gegebenenfalls sogar Ermöglichung sicherheitsbehördlicher Maßnahmen dient. Letztere werden damit zur eigentlichen Ursache für die Datenverarbeitung.

Diese eher dogmatischen Überlegungen hätten auch einen unmittelbaren praktischen Effekt. Durch die vorab beschriebene Verschiebung würden sich auch die Befugnisse der Sicherheitsbehörden ändern. Diese könnten zukünftig selber bestimmen, welche Verkehrsdaten für sie erzeugt werden müssen und somit den TK-Anbieter eigenständig entsprechende Vorgaben machen. Ob, wo und wie hier sinnvolle Grenzen gezogen werden können, ist dabei gegenwärtig nicht absehbar.

Dies wiederum führt zwangsläufig erneut zu dem eingangs angeführten Erfordernis der Verhältnismäßigkeit sicherheitsbehördlichen Handelns. Das Bundesverfassungsgericht hat bereits in seiner Entscheidung zur Vorratsdatenspeicherung klargestellt, dass auch eine im Einzelfall verhältnismäßige hoheitliche Maßnahme verfassungsrechtlich kritisch zu sehen ist, wenn sie zusammen mit weiteren ähnlich gelagerten Grundrechtseingriffen dazu führt, dass diese in der Gesamtheit eine Gefahr für die Freiheitswahrnehmung der Bürgerinnen und Bürger in Deutschland darstellen kann (vgl. *BVerfG, Urteil vom 02.03.2010, 1 BvR 256/08, Rn. 218*).

Die oben dargelegte Abkehr von der aktuellen Systematik des telekommunikationsrechtlichen Auskunftsanspruchs und der damit einhergehenden Stärkung der sicherheitsbehördlichen Kompetenzen würde zwangsläufig auch die Gefahr einer Verschiebung der aktuellen Verhältnisse in dieser sogenannten „Überwachungs-Gesamtrechnung“ mit sich bringen. Gerade mit Blick auf die in den letz-

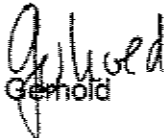


SEITE 9 VON 9

ten Jahren immer weiter ausgeweiteten Befugnisse der Sicherheitsbehörden – sei es durch die Wiedereinführung der Vorratsdatenspeicherung oder der Erweiterung der Befugnisse des Bundesnachrichtendienstes, des Bundesamtes für Verfassungsschutz oder des Bundeskriminalamts in ihren jeweiligen Gesetzen – sollte die Notwendigkeit jeder auch nur mittelbaren Kompetenzerweiterung in diesen Bereichen sorgfältig geprüft werden.

Bonn, den 21.04.2017

In Vertretung


Gerold