

© Jan Sramek Verlag (<http://www.jan-sramek-verlag.at>). [Übersetzung wurde bereits in Newsletter Menschenrechte 2020/1 veröffentlicht] Die erneute Veröffentlichung wurde allein für die Aufnahme in die HUDOC-Datenbank des EGMR gestattet. Diese Übersetzung bindet den EGMR nicht.

© Jan Sramek Verlag (<http://www.jan-sramek-verlag.at>). [Translation already published in Newsletter Menschenrechte 2020/1] Permission to republish this translation has been granted for the sole purpose of its inclusion in the Court's database HUDOC. This translation does not bind the Court.

© Jan Sramek Verlag (<http://www.jan-sramek-verlag.at>). [Traduction déjà publiée dans Newsletter Menschenrechte 2020/1] L'autorisation de republier cette traduction a été accordée dans le seul but de son inclusion dans la base de données HUDOC de la Cour. La présente traduction ne lie pas la Cour.

Breyer gg. Deutschland – 50001/12

Urteil vom 30.1.2020, Sektion V

Sachverhalt

Die beiden Bf. waren in einer NGO aktiv, die sich gegen die generelle Speicherung von Telekommunikationsdaten einsetzte.

2004 wurde durch eine Änderung des Telekommunikationsgesetzes (TKG) eine Verpflichtung für Telekommunikationsanbieter eingeführt, persönliche Daten aller ihrer Kunden zu speichern. Dies betraf auch Nutzer vorausbezahlter (»prepaid«) SIM-Karten für Mobiltelefone, bei denen solche Details nicht zum Zweck der Abrechnung oder aus anderen vertraglichen Gründen erforderlich waren. Beide Bf. mussten gemäß § 111 TKG als Nutzer vorausbezahlter SIM-Karten bei deren Aktivierung gewisse persönliche Daten bei ihrem Anbieter registrieren. Diese Daten waren insbesondere gemäß § 112 und § 113 TKG unter bestimmten Voraussetzungen an die Behörden zu übermitteln.

§ 112 regelte ein automatisiertes Verfahren. Demnach mussten die Telekommunikationsanbieter die gemäß § 111 zu speichernden Daten so bereitstellen, dass sie von der Bundesnetzagentur ohne Kenntnis des Anbieters abgerufen werden konnten. Die Bundesnetzagentur hatte die Daten auf Ersuchen konkreter bezeichneter Behörden (insbesondere Strafverfolgungs- und Polizei-

behörden) abzurufen und an diese zu übermitteln. Auskünfte durften immer erteilt werden, wenn sie zur Erfüllung gesetzlicher Aufgaben erforderlich waren. Das in § 113 Abs. 1 1. Satz geregelte manuelle Verfahren verpflichtete die Telekommunikationsanbieter, selbst Auskünfte zu erteilen. Grundsätzlich waren alle Behörden berechtigt, eine Auskunft einzuholen. Voraussetzung für die Erteilung einer solchen war, dass sie im Einzelfall für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, die Gefahrenabwehr oder nachrichtendienstliche Aufgaben erforderlich war. Die Auskunft war schriftlich zu beantragen.

Im Juli 2005 erhoben die Bf. eine Verfassungsbeschwerde, die sich unter anderem gegen die §§ 111, 112 und 113 TKG richtete.¹ Die Bf. machten eine Verletzung ihres Rechts auf Vertraulichkeit der Korrespondenz und Telekommunikation sowie ihres Rechts auf informationelle Selbstbestimmung geltend. Das BVerfG erklärte mit Beschluss vom 24.1.2012 (1 BvR 1299/05) § 111 und

¹ Mit 21.12.2007 wurde § 111 TKG geändert. Das BVerfG prüfte nach einer Ergänzung der Beschwerde die am 1.1.2008 geltende Rechtslage.

§ 112 TKG für mit dem GG vereinbar. Die in § 111 vorgesehene Speicherung schaffe eine verlässliche Datenbasis für die Auskunftserteilung und sei angesichts der begrenzten Daten verhältnismäßig zum verfolgten legitimen Zweck der Verbesserung der Strafverfolgung und Gefahrenabwehr. Auch das automatisierte Auskunftsverfahren wurde für verfassungskonform erklärt, wobei das BVerfG darlegte, dass der Abruf der Daten durch die Behörden eine eigene Ermächtigungsgrundlage voraussetze. Das manuelle Verfahren verstoße ebenfalls nicht gegen das GG. Allerdings bedürfe § 113 Abs. 1 1. Satz insofern einer verfassungskonformen Auslegung, als die Bestimmung für sich allein noch keine Auskunftspflichten des Telekommunikationsanbieters begründe, sondern es für den Abruf von Daten seitens der auskunftsberechtigten Behörden einer rechtlichen Ermächtigungsgrundlage bedürfe, die eine solche Verpflichtung eigenständig und klar vorsehe.

Rechtsausführungen

Die Bf. behaupteten eine Verletzung von Art. 8 EMRK (hier: *Recht auf Achtung des Privatlebens und der Korrespondenz*) und von Art. 10 EMRK (*Meinungsäußerungsfreiheit*). Sie brachten vor, ihre jeweiligen Telekommunikationsdienstleister würden aufgrund der in § 111 TKG enthaltenen gesetzlichen Verpflichtung bestimmte persönliche Daten von ihnen als Nutzer vorausbezahlter SIM-Karten speichern.

I. Umfang der Rechtssache und der Beurteilung durch den GH

(60) [...] Die Bf. stellten vor dem GH lediglich die Vereinbarkeit von § 111 TKG mit der EMRK in Frage. Sie beschwerten sich nicht ausdrücklich über § 112 oder § 113 dieses Gesetzes [...] oder über irgendwelche weiteren Maßnahmen der Überwachung und des Abhörens von Telefongesprächen. Dies bedeutet allerdings nicht, dass sich diese weiteren Bestimmungen des TKG bei der Einschätzung seiner praktischen Anwendung und der Verhältnismäßigkeit des in Beschwerde gezogenen Eingriffs nicht als relevant erweisen können. [...]

(61) § 111 TKG betrifft nur die Speicherung von Teilnehmerdaten, nämlich Telefonnummer, Name und Anschrift, Geburtsdatum und Datum des Vertragsabschlusses. Die Bestimmung erstreckt sich nicht auf Verkehrsdaten, Standortdaten oder Daten, die den Inhalt von Kommunikation offenbaren. Zudem haben die Bf. nicht behauptet, dass ihre Kommunikation abgehört oder irgendeiner anderen Überwachungsmaßnahme unterworfen wurde. Der geltend gemachte Eingriff betrifft die Speicherung der soeben beschriebenen Datensätze und die Möglichkeit der nationalen Behör-

den, unter bestimmten näher definierten Umständen darauf zuzugreifen. Auch wenn sich der GH der Umstände der umstrittenen Datenspeicherung und ihrer Nähe zu telefonischer Kommunikation und dem Recht auf Korrespondenz bewusst ist, sieht er den Schlüsselaspekt der Beschwerde in der Speicherung der persönlichen Daten der Bf. und nicht in irgendeinem spezifischen Eingriff in ihre Korrespondenz oder ihre Meinungsäußerungsfreiheit.

(62) Der GH muss daher im vorliegenden Fall nicht entscheiden, ob und in welchem Ausmaß aus Art. 10 EMRK ein Recht der Nutzer von Telekommunikationsdiensten auf Anonymität abgeleitet werden kann und wie dieses Recht gegen andere Notwendigkeiten abzuwägen wäre.

(63) Der GH erachtet es daher als angemessen, das Vorbringen der Bf. nur anhand des [...] Rechts auf Achtung des Privatlebens zu prüfen.

(64) [...] Die Nutzerdaten der Bf. wurden von den Telekommunikationsdienstleistern seit der Registrierung ihrer SIM-Karten zeitweilig gespeichert. § 111 TKG wurde 2007 und 2012 geändert. Der GH stellt allerdings fest, dass das BVerfG in seinem Urteil vom 24.1.2012 das TKG in seiner am 1.1.2008 geltenden Fassung prüfte, und dass Verfahren betreffend die spätere Änderung des TKG von 2016 noch vor dem BVerfG anhängig sind. Der GH wird daher die einschlägigen Bestimmungen in der Fassung prüfen, die am 1.1.2008 in Kraft war.

II. Zulässigkeit

(65) [...] Die Beschwerde ist weder offensichtlich unbegründet [...] noch aus einem anderen Grund unzulässig. Sie muss daher für **zulässig** erklärt werden (einstimmig).

III. In der Sache

1. Allgemeine Grundsätze

(74) Im Zusammenhang mit persönlichen Daten [...] darf der Begriff »Privatleben« nicht restriktiv interpretiert werden. Die weite Auslegung entspricht jener der Datenschutzkonvention² [...], wonach unter »persönlichen Daten« »jede Information über eine bestimmte oder bestimmbare natürliche Person« zu verstehen ist.

(75) Aus der ständigen Rechtsprechung des GH ergibt sich weiters, dass sich in Fällen einer Sammlung von Daten über eine bestimmte Person Bedenken im Hinblick auf das Privatleben ergeben, wenn persönliche Daten in einer Weise oder einem Umfang verarbeitet, verwendet oder veröffentlicht werden, die über das nor-

² Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28.1.1981, BGBl. 317/1988.

malerweise vorhersehbare Maß hinausgehen. Art. 8 EMRK enthält somit ein Recht auf eine Form informationeller Selbstbestimmung, das es dem Einzelnen erlaubt, sich auf sein Recht auf Privatsphäre zu berufen, wenn es um Daten geht, die zwar neutral sind, aber kollektiv und in einer solchen Form gesammelt, verarbeitet und verbreitet werden, dass seine durch Art. 8 EMRK garantierten Rechte berührt sein könnten.

(76) Zwar hat der GH bereits ein weites Spektrum von Eingriffen in das Recht auf Privatleben [...] durch die Speicherung, Verarbeitung und Verwendung persönlicher Daten geprüft [...], doch betraf keiner dieser Fälle die Speicherung eines Datensatzes wie jenem, um den es im vorliegenden Fall geht.

(79) [...] Die nationalen Behörden genießen [...] bei der Wahl der Mittel, die sie einsetzen, um das legitime Ziel des Schutzes der nationalen Sicherheit zu erreichen, einen gewissen Ermessensspielraum. [...]

2. Anwendung auf den vorliegenden Fall

(81) Es steht außer Streit, dass die Verpflichtung von Telekommunikationsdienstleistern, gemäß § 111 TKG persönliche Daten zu speichern, in das Recht der Bf. auf Achtung ihres Privatlebens eingriff, da ihre persönlichen Daten gespeichert wurden. In diesem Zusammenhang erinnert der GH daran, dass die bloße Speicherung von Daten, die sich auf das Privatleben einer Person beziehen, einen Eingriff iSv. Art. 8 EMRK darstellt. [...]

(82) [...] Ein Eingriff in das Recht der Bf. auf Achtung ihres Privatlebens verletzt Art. 8 EMRK, wenn er nicht »gesetzlich vorgesehen« ist, eines der in Abs. 2 genannten legitimen Ziele verfolgt und zudem »in einer demokratischen Gesellschaft notwendig« ist, um dieses Ziel zu erreichen.

(83) [...] Im Kontext der Speicherung persönlicher Informationen ist es wesentlich, dass klare, detaillierte Regeln über Mindestgarantien bestehen, die unter anderem die Dauer, Speicherung, Verwendung und den Zugang Dritter sowie Verfahren zur Sicherstellung von Integrität und Vertraulichkeit der Daten und die Durchführung ihrer Vernichtung betreffen.

(84) [...] Die Speicherung der persönlichen Daten der Bf. erfolgte beim Kauf von SIM-Karten für Mobiltelefone auf der Grundlage von § 111 TKG, der hinsichtlich des Umfangs der gespeicherten Daten ausreichend klar und vorhersehbar war. Zudem war die Dauer der Speicherung klar geregelt und auch die technische Seite der Speicherung war, zumindest nach der Erlassung der einschlägigen Verordnung und technischen Leitlinie, klar umschrieben.

(85) Soweit es um Sicherheitsgarantien, den Zugang Dritter und die weitere Verwendung der gespeicherten Daten geht, muss § 111 TKG in Verbindung mit dessen

§§ 112 und 113 und – nach dem vom BVerfG erklärten »Doppeltürenmodell«³ in Verbindung mit der jeweiligen rechtlichen Grundlage der individuellen Auskunftersuchen – gelesen werden. Die Frage der Vorhersehbarkeit und ausreichenden Detailliertheit dieser Bestimmungen ist jedoch nach Ansicht des GH im vorliegenden Fall eng mit den umfassenderen Fragen verbunden, ob der Eingriff in einer demokratischen Gesellschaft notwendig und verhältnismäßig war. Er wird daher bei diesen Fragen darauf zurückkommen.

(86) Der GH akzeptiert [...] das Argument der Regierung, wonach der Eingriff die legitimen Ziele der öffentlichen Sicherheit, der Aufrechterhaltung der Ordnung, der Verhütung von Straftaten und des Schutzes der Rechte und Freiheiten anderer verfolgt.

(87) In diesem Zusammenhang nimmt der GH die Erklärung im Urteil des BVerfG zur Kenntnis, wonach der Zugang zu den gespeicherten Daten »zum Zweck der Gefahrenabwehr, zur Verfolgung von Straftaten oder Ordnungswidrigkeiten sowie zur Wahrnehmung nachrichtendienstlicher Aufgaben« erfolgt. Diese Zwecke werden im TKG betont, das ausführt, dass Auskunftersuchen insofern zulässig sind, als sie notwendig sind, um Straftaten und Ordnungswidrigkeiten zu verfolgen, Gefahren abzuwehren und nachrichtendienstliche Aufgaben zu erfüllen.

(88) Ein Eingriff kann als »in einer demokratischen Gesellschaft notwendig« zur Verwirklichung eines legitimen Ziels angesehen werden, wenn er ein »dringendes gesellschaftliches Bedürfnis« erfüllt. Der Kampf gegen Straftaten und insbesondere gegen das organisierte Verbrechen und den Terrorismus, [...] die Aufrechterhaltung der öffentlichen Sicherheit und der Schutz der Bürger stellen nach Ansicht des GH »dringende gesellschaftliche Bedürfnisse« dar. Er anerkennt auch, dass moderne Mittel der Telekommunikation und Änderungen im Kommunikationsverhalten eine Anpassung der Ermittlungswerkzeuge der Strafverfolgungsbehörden und Nachrichtendienste erfordern.

(89) [...] Die Regierung argumentierte, die Möglichkeit der Zuordnung von Mobiltelefonnummern vorausbezahlter SIM-Karten zu bestimmten Personen wäre für eine effektive Strafverfolgung und Gefahrenabwehr erforderlich. Die Bf. hingegen bestreiten die Effektivität von § 111 TKG, da es keinen empirischen Beleg für eine Verringerung der Kriminalität durch die Einführung der zwingenden Registrierung geben würde. [...]

(90) Wie der GH anerkennt, erleichtert und beschleunigt die Vorregistrierung von Mobiltelefon-Teilnehmern die Ermittlungen durch die Strafverfolgungsbehörden

3 Bildlich gesprochen muss der Gesetzgeber nicht nur die Tür zur Übermittlung von Daten öffnen, sondern auch die Tür zu deren Abfrage. Erst beide Rechtsgrundlagen gemeinsam berechnen zu einem Austausch personenbezogener Daten.

erheblich und kann dadurch zu einer effektiven Strafverfolgung und einer Verhütung von Straftaten beitragen. Das Bestehen von Möglichkeiten, rechtliche Verpflichtungen zu umgehen, kann kein Grund dafür sein, die Nützlichkeit und Effektivität einer rechtlichen Vorschrift insgesamt in Frage zu stellen. Schließlich erinnert der GH daran, dass die nationalen Behörden im Kontext der nationalen Sicherheit bei der Wahl der Mittel zum Erreichen eines legitimen Ziels einen gewissen Ermessensspielraum genießen, und er stellt fest, dass [...] zwischen den Mitgliedstaaten im Hinblick auf die Speicherung von Teilnehmerinformationen von Kunden vorausbezahlter SIM-Karten kein Konsens besteht. Angesichts dieses Ermessensspielraums akzeptiert der GH, dass die Verpflichtung zur Speicherung von Teilnehmerinformationen gemäß § 111 TKG generell eine passende Antwort auf Änderungen des Kommunikationsverhaltens und bei den Mitteln der Telekommunikation war.

(91) Es bleibt jedoch fraglich, ob der Eingriff verhältnismäßig war und einen fairen Ausgleich zwischen den widerstreitenden öffentlichen und privaten Interessen traf.

(92) Zunächst muss der GH den Grad des Eingriffs in das Recht der Bf. auf Achtung ihres Privatlebens feststellen. In dieser Hinsicht stimmt der GH mit der Ansicht des BVerfG überein, wonach nur begrenzte Daten gespeichert wurden. Diese Daten umfassten weder höchstpersönliche Informationen noch erlaubten sie die Erstellung von Persönlichkeitsprofilen oder die Ortung der Bewegungen von Mobiltelefon-Nutzern. Zudem wurden keine Daten über einzelne Kommunikationsvorgänge gespeichert. Der Grad des Eingriffs muss daher klar unterschieden werden von früheren Fällen des GH, die z.B. Überwachung (*Malone/GB, Copland/GB*), Lokalisierung (*Uzun/D*) oder die Speicherung von Gesundheits- und anderen sensiblen Daten (*S. und Marper/GB, M. M./GB*) betrafen. Außerdem muss der Fall von Fällen unterschieden werden, in denen die Registrierung in einer bestimmten Datenbank regelmäßige Kontrollen und eine weitere Sammlung privater Informationen nach sich zog.

(95) Insgesamt kommt der GH zu dem Schluss, dass der Eingriff, wenn auch nicht trivial, so doch von einer eher beschränkten Art war.

(96) Was Sicherheitsgarantien betrifft, bemerkt der GH, dass die Bf. keine technischen Unsicherheiten bei der fraglichen Datenspeicherung behauptet haben. Zudem ist die Dauer der Speicherung mit dem Ablauf des Kalenderjahres begrenzt, das auf das Jahr folgt, in dem das Vertragsverhältnis beendet wurde. Diese Speicherdauer erscheint nicht unangemessen, können doch strafrechtliche Ermittlungen einige Zeit in Anspruch nehmen und sich über den Zeitpunkt der Beendigung des Vertragsverhältnisses hinaus erstrecken. Außerdem

scheinen sich die gespeicherten Daten auf die Informationen zu beschränken, die eindeutig notwendig sind, um den betroffenen Teilnehmer zu identifizieren.

(97) [...] Obwohl sich die Bf. nur über die Speicherung ihrer persönlichen Daten gemäß § 111 TKG beschwert haben, wurde von beiden Parteien akzeptiert, dass die Datenspeicherung in Verbindung mit den §§ 112 und 113 dieses Gesetzes beurteilt werden muss. [...] Der GH stimmt den Parteien darin zu, dass er im vorliegenden Fall die Verhältnismäßigkeit des Eingriffs nicht beurteilen kann, ohne den möglichen künftigen Zugang zu den gespeicherten Daten und ihre Verwendung genau zu untersuchen. Daher hält er es für bedeutend, die Rechtsgrundlage für Auskunftersuchen und die verfügbaren Sicherheitsgarantien zu berücksichtigen.

(98) [...] § 112 TKG [...] hat Datenabfragen für die Behörden sehr vereinfacht. Das zentralisierte und automatisierte Verfahren erlaubt eine Form des Zugangs, der praktische Schwierigkeiten der Datensammlung weitgehend beseitigt und den Behörden Daten jederzeit ohne Verzögerung zugänglich macht. Allerdings stellt die Tatsache, dass die Behörden, die Zugang verlangen können, in § 112 TKG im Einzelnen aufgelistet sind, einen einschränkenden Faktor dar. Auch wenn die Liste weit erscheint, sind alle darin genannten Behörden mit der Strafverfolgung und dem Schutz der nationalen Sicherheit befasst.

(99) Was § 113 TKG betrifft, stellt der GH zunächst fest, dass die Datenabfrage nicht im selben Ausmaß vereinfacht ist wie nach § 112, da die Behörden die gewünschten Informationen schriftlich beantragen müssen. Ein weiterer Unterschied zwischen § 112 und § 113 TKG besteht darin, dass die Behörden, die befugt sind, Zugang nach § 113 zu beantragen, nicht ausdrücklich aufgezählt, sondern anhand der von ihnen ausgeübten Funktionen bestimmt werden. Auch wenn der GH diese Beschreibung der Aufgaben als weniger spezifisch und stärker einer Auslegung zugänglich ansieht, ist der Wortlaut der Bestimmung doch detailliert genug, um eindeutig vorherzusehen, welche Behörden befugt sind, um Informationen zu ersuchen. In diesem Kontext nimmt der GH auch die Feststellung des BVerfG zur Kenntnis, wonach die beschränkten Aufgaben der Nachrichtendienste deren weitreichende rechtliche Befugnisse rechtfertigen, im Vorfeld Informationen einzuholen.

(100) Im Hinblick auf beide Bestimmungen [...] werden die gespeicherten Daten durch die Tatsache weiter gegen exzessive oder missbräuchliche Auskunftersuchen geschützt, dass die ersuchende Behörde eine zusätzliche Rechtsgrundlage für das Abrufen der Daten benötigt. Wie das BVerfG mit seinem »Doppeltürenmodell« erklärt hat, gestatten die §§ 112 und 113 TKG nur die Weitergabe der Daten durch die Bundesnetzagentur oder den betroffenen Serviceanbieter. Es ist jedoch eine weitere Bestimmung erforderlich, die der spezifischen

Behörde gestattet, die Information einzuholen. Außerdem ist die Abfrage auf notwendige Daten beschränkt und diese Notwendigkeit wird durch eine generelle Verpflichtung der jeweiligen Behörden, von denen die Informationen abgefragt werden, abgesichert, unverzüglich alle Daten zu löschen, die sie nicht benötigen. Das BVerfG hat darauf hingewiesen, dass die Voraussetzung der Erforderlichkeit im Kontext der Verfolgung von Straftaten bedeutet, dass zumindest ein Anfangsverdacht vorliegen muss. Der GH akzeptiert, dass die Befugnis, Daten anzufordern, ausreichend beschränkt ist und dass die Voraussetzung der Erforderlichkeit nicht nur den spezifischen Vorschriften innewohnt, auf die sich diese Beschwerde bezieht, sondern auch dem deutschen und europäischen Datenschutzrecht.

(101) Angesichts dieser Elemente kann der GH die Schlussfolgerung des BVerfG akzeptieren, wonach die in § 113 TKG vorgesehenen Schwellen verfassungsrechtlich noch hinnehmbar waren, wobei auch berücksichtigt wurde, dass die Notwendigkeit eines schriftlichen Antrags die abfragende Behörde dazu bewegen würde, Informationen nur bei hinreichendem Bedarf einzuholen. Wie der GH dazu bemerkt, schienen manuelle Abfragen im Vergleich zu den automatischen Abfragen nach § 112 TKG nur in einer beschränkten Zahl von Fällen erfolgt zu sein.

(102) Zuletzt wird der GH die verfügbaren Möglichkeiten zur Kontrolle und Überprüfung von Informationssuchen nach § 112 und § 113 TKG betrachten. [...]

(103) Der GH hat sich im Hinblick auf verschiedene Eingriffe in das Recht auf Achtung des Privatlebens [...] auf [...] die Möglichkeit einer effektiven Kontrolle und Überprüfung bezogen [...]. Alle diese Fälle betrafen jedoch individualisierte Eingriffe in das Recht auf Achtung des Privatlebens, die schwerwiegender waren und stärker in dieses eindringen. Sie können daher nicht auf den Zugang zu Daten im vorliegenden Fall übertragen werden. Insgesamt ist das Ausmaß der Kontrolle und Überprüfung nach Ansicht des GH als ein wichtiges, aber nicht als entscheidendes Element der Prüfung der Verhältnismäßigkeit der Sammlung und Speicherung eines derart beschränkten Datensatzes zu betrachten.

(104) [...] § 113 Abs. 2 TKG stellt klar, dass die Verantwortung für die Rechtmäßigkeit des Auskunftersuchens grundsätzlich bei der anfragenden Behörde liegt und dass die Telekommunikationsanbieter nicht dafür zuständig sind, die Zulässigkeit einer Anfrage zu beurteilen, solange diese in Schriftform erfolgt und eine gesetzliche Grundlage genannt wird. Gemäß § 112 TKG ist die Bundesnetzagentur jedoch dafür zuständig, die Zulässigkeit der Übermittlung zu prüfen, wenn dafür ein besonderer Anlass besteht.

(105) Zudem werden jede Abfrage und die sich darauf beziehenden Informationen (Zeitpunkt, bei der Durchführung des Abrufs verwendete Daten, abgerufene

Daten, ein die abrufende Person eindeutig bezeichnendes Datum sowie die ersuchende Stelle, deren Aktenzeichen und ein die ersuchende Person eindeutig bezeichnendes Datum) zum Zweck der Datenschutzkontrolle protokolliert. Diese Kontrolle erfolgt durch die unabhängigen Datenschutzbehörden des Bundes und der Länder. Diese sind nicht nur dafür zuständig, die Einhaltung der Datenschutzregeln aller beteiligten Behörden zu überwachen, sondern sie können auch von jeder Person angerufen werden, die glaubt, dass ihre Rechte durch die Sammlung, Verarbeitung oder Verwendung ihrer persönlichen Daten durch öffentliche Stellen verletzt wurden.

(106) Wie der GH schließlich bemerkt, hat das BVerfG festgestellt, dass Rechtsschutz gegen Auskunftersuchen nach den allgemeinen Regeln gesucht werden kann, insbesondere im Zusammenhang mit Rechtsschutzverfahren gegen abschließende Entscheidungen der Behörden.

(107) Die Möglichkeit der Überwachung durch die zuständigen Datenschutzbehörden gewährleistet nach Ansicht des GH eine Überprüfung durch eine unabhängige Behörde. Zudem werfen das Fehlen einer Mitteilung und die Vertraulichkeit des Abfrageverfahrens kein Problem unter der Konvention auf, weil jeder, der glaubt, in seinen Rechten verletzt worden zu sein, eine Beschwerde erheben kann.

(108) Zuletzt anerkennt der GH, dass die Mitgliedstaaten angesichts des Fehlens eines Konsenses betreffend die Sammlung und Speicherung begrenzter Teilnehmerdaten einen gewissen Ermessensspielraum bei der Entscheidung hatten, zu welchen Mitteln sie greifen, um die legitimen Ziele des Schutzes der nationalen Sicherheit und der Bekämpfung des Verbrechens zu erreichen. Diesen Ermessensspielraum hat Deutschland im vorliegenden Fall nicht überschritten.

(109) Angesichts dieser Überlegungen kommt der GH zum Schluss, dass die Speicherung der persönlichen Daten der Bf. durch ihre jeweiligen Diensteanbieter gemäß § 111 TKG [in der am 8.1.2008 gültigen Fassung] verhältnismäßig und somit »in einer demokratischen Gesellschaft notwendig« war.

(110) Folglich hat **keine Verletzung** von **Art. 8 EMRK** stattgefunden (6:1 Stimmen; *abweichendes Sondervotum von Richter Ranzoni*).