Meinhard Starostik

Rechtsanwalt/vereidigter Buchprüfer

Schlüterstr. 38 ◆ 10629 Berlin
Tel.: 030 - 88 000 345
Fax:030 - 88 000 346
email: Kanzlei@Starostik.de
internet: www.Starostik.de

RA/vBP Starostik, Schlüterstr. 38, 10629 Berlin

An das
Bundesverfassungsgericht
Schloßbezirk 3

76131 Karlsruhe

Berlin, den 13. Juli 2005

AZ: 42/05
(bitte stets angeben)

Verfassungsbeschwerde

1. des Herrn Patrick Breyer, [redacted] und

2. des Herrn Jonas Breyer, [redacted]

jeweils gegen die:

§§ 88 Abs. 3 S. 1, 92, 95 Abs. 3, 97 Abs. 3 S. 3 und Abs. 4, 100, 111, 112, 113 des Telekommunikationsgesetzes (TKG) vom 22. Juni 2004 (BGBl I S. 1190),

sowie der

3. der mediaBEAM GmbH,
vertreten durch den Geschäftsführer [redacted]
Parallelstr. 38, 48683 Ahaus,

4. der Speedbone Internet & Connectivity GmbH,
vertreten durch die Geschäftsführerin [redacted]
Alboinstr. 36-42, 12103 Berlin,

5. des Herrn Fabian Urhausen, [redacted]

jeweils gegen die §§ 95 Abs. 3, 110
des Telekommunikationsgesetzes (TKG) vom 22. Juni 2004 (BGBl I S. 1190).

Verfahrensbevollmächtigter der Beschwerdeführer zu 1-5:

Rechtsanwalt Starostik, Schlüterstr. 38, 10629 Berlin -

Die Beschwerdeführer zu 1 und 2 beantragen,

1. **die §§ 88 Abs. 3 S. 1 und 92 des Telekommunikationsgesetzes (TKG) vom 22. Juni 2004 (BGBl. I S. 1190) für unvereinbar mit Artikel 10 Absatz 1 des Grundgesetzes,**
2. **die §§ 95 Abs. 3 und Abs. 4, 100, 111, 112, 113 des Telekommunikationsgesetzes (TKG) vom 22. Juni 2004 (BGBl. I S. 1190) für unvereinbar mit Artikel 10 Absatz 1, hilfsweise mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1, sowie für unvereinbar mit Artikel 3 Absatz 1 des Grundgesetzes,**
3. **§ 97 Abs. 3 S. 3 und Abs. 4 des Telekommunikationsgesetzes (TKG) vom 22. Juni 2004 (BGBl. I S. 1190) für unvereinbar mit Artikel 10 Absatz 1 sowie für unvereinbar mit Artikel 3 Absatz 1 des Grundgesetzes zu erklären.**

Die Beschwerdeführer/innen zu 3 bis 5 beantragen,

die §§ 95 Abs. 3, 110 des Telekommunikationsgesetzes (TKG) vom 22. Juni 2004 (BGBl. I S. 1190) für unvereinbar mit Artikel 3 Absatz 1 in Verbindung mit Artikel 12 Absatz 1 des Grundgesetzes zu erklären.

Gründe

1. Tatbestand

1.1 Beschwerdeführer zu 1

Der Beschwerdeführer zu 1 besitzt und benutzt eine vorausbezahlte Mobiltelefonkarte der Firma Vodafone D2 GmbH, die er nach Inkrafttreten des Telekommunikationsgesetzes 2004 erworben hat. Zum Erwerb der Karte musste er in Übereinstimmung mit § 111 TKG seine persönlichen Daten angeben, die dann der Firma Vodafone D2 GmbH übermittelt wurden.

Weiterhin benutzt er den Dienst Alice, um Informationen aus dem Internet abzurufen (Internet-Zugang). Die Firma Hanse-Net Telekommunikation GmbH, Hamburg speichert Identifikationskennungen, die sie ihren Kunden für die Dauer der Nutzung zuweist (IP-Adressen), in Übereinstimmung mit § 100 TKG zu Zwecken der Störungsbeseitigung und Missbrauchsbekämpfung 60 Tage lang.

1.2 Beschwerdeführer zu 2

Der Beschwerdeführer zu 2 besitzt und benutzt eine Mobiltelefonkarte der Firma T-Mobile Deutschland GmbH. Zum Erwerb vorausbezahlter Karten müsste er in Übereinstimmung mit § 111 TKG seine persönlichen Daten angeben, die dann der Firma T-Mobile Deutschland GmbH übermittelt würden.

Weiterhin benutzt er den Dienst T-Online, um Informationen aus dem Internet abzurufen (Internet-Zugang). Die Firma T-Online International AG speichert sämtliche Identifikationskennungen, die sie ihren Kunden für die Dauer der Nutzung zuweist (IP-Adressen), in Übereinstimmung mit § 100 TKG zu Zwecken der Störungsbeseitigung und Missbrauchsbekämpfung mindestens 80 Tage lang.

1.3 Beschwerdeführerin zu 3

Die Beschwerdeführerin zu 3 stellt der Öffentlichkeit dauerhaft Email- und weitere Kommunikationsdienste zur Verfügung (siehe ihre Webseite www.mediabeam.com). Ihr Angebot ist auf Gewinnerzielung gerichtet. Einnahmen erzielt sie durch Werbeeinblendungen und durch Entgelte der Nutzer von kostenpflichtigen Diensten. Die Anzahl der Nutzer ihrer Telekommunikationsdienste ist sechsstellig.

1.4. Beschwerdeführerin zu 4

Die Beschwerdeführerin zu 4 stellt der Öffentlichkeit dauerhaft unter anderem Emaildienste zur Verfügung (siehe ihre Webseite www.prosite.de). Ihr Angebot ist auf Gewinnerzielung gerichtet. Einnahmen erzielt sie insbesondere durch Entgelte der Nutzer ihrer Dienste. Die Anzahl der Nutzer ihrer Telekommunikationsdienste ist fünfstellig.

1.5 Beschwerdeführer zu 5

Der Beschwerdeführer zu 5 stellt der Öffentlichkeit dauerhaft unter anderem Emaildienste zur Verfügung (siehe seine Webseite www.urifabi.net). Sein Angebot ist auf Gewinnerzie-

lung gerichtet. Einnahmen erzielt er insbesondere durch Entgelte der Nutzer seiner Dienste. Die Anzahl der Nutzer seiner Telekommunikationsdienste ist vierstellig.

2. Zulässigkeit der Verfassungsbeschwerde

2.1 Beschwerdeführer zu 1

Der Beschwerdeführer zu 1 ist von den §§ 92, 95 Abs. 3, 97 Abs. 3 S. 3 und Abs. 4, 100, 111, 112, 113 TKG selbst, gegenwärtig und unmittelbar in Grundrechten betroffen:

Nach § 88 Abs. 3 S. 1 TKG dürfen die Diensteanbieter, deren Kunde der Beschwerdeführer zu 1 ist, Inhalt und nähere Umstände seiner Telekommunikation zu Zwecken "des Schutzes ihrer technischen Systeme" zu Kenntnis nehmen. Ob die Diensteanbieter von dieser Möglichkeit Gebrauch machen, ist ihm zwar nicht bekannt. Von etwa erfolgenden Kenntnisnahmen erlangt der Beschwerdeführer jedoch auch keine Kenntnis (vgl. BVerfG, 1 BvR 2378/98 vom 3.3.2004, Absatz-Nrn. 96 f.). Unter diesen Umständen muss es genügen, dass eine Kenntnisnahme von Daten des Beschwerdeführers durch Diensteanbieter zu Zwecken des Systemschutzes "möglich" oder "nicht auszuschließen" ist, wenn also eine "mögliche Grundrechtsbetroffenheit" vorliegt (BVerfGE 100, 313 [356 f.]). Dies ist bei dem Beschwerdeführer aus den genannten Gründen der Fall. Unschädlich ist, wenn die Möglichkeit der Betroffenheit "praktisch für jedermann" besteht (BVerfG, 1 BvR 2378/98 vom 3.3.2004, Absatz-Nr. 101). Der effektive Grundrechtsschutz verlangt die Zulassung von Beschwerden selbst dann, wenn sich nachträglich herausstellt, dass der Beschwerdeführer tatsächlich zu keiner Zeit von der angegriffenen Bestimmung betroffen war (Europäischer Gerichtshof für Menschenrechte, Klass u.a.-D (1978), EuGRZ 1979, 278 ff., Abs. 34 und 37). Es muss insoweit genügen, dass die Grundrechte des Beschwerdeführers jederzeit betroffen werden können.

Nach § 92 TKG dürfen die Diensteanbieter, deren Kunde der Beschwerdeführer zu 1 ist, auf seine Person bezogene Daten "für die Missbrauchsbekämpfung" an ausländische nicht öffentliche Stellen übermitteln. Ob die Diensteanbieter von dieser Möglichkeit Gebrauch machen, ist ihm zwar nicht bekannt. Von etwa erfolgenden Übermittlungen erlangt der Beschwerdeführer jedoch auch keine Kenntnis. Insoweit muss, wie zuvor dargelegt, die mögliche Grundrechtsbetroffenheit des Beschwerdeführers zu 1 genügen.

Nach § 95 Abs. 3 TKG müssen die Diensteanbieter, deren Kunde der Beschwerdeführer zu 1 ist, auf seine Person bezogene Bestandsdaten nach Vertragsende noch bis zum Ende des auf das Vertragsende folgende Jahr speichern. Hiervon ist der Beschwerdeführer zu 1 sowohl im Fall der Firma Vodafone D2 GmbH wie auch der Firma T-Online International AG betroffen.

Nach § 97 Abs. 3 S. 3 und Abs. 4 TKG dürfen die Diensteanbieter, deren Kunde der Beschwerdeführer zu 1 ist, seine Verkehrsdaten unabhängig von seinem Willen bis zu sechs Monate über die Abrechnung der Verbindungen hinaus speichern. Die Firma Vodafone D2 GmbH, deren Kunde der Beschwerdeführer zu 1 ist, macht von diesem Recht insoweit Gebrauch als sie Verbindungsdaten ihrer Kunden "bis zu 6 Monate" lang speichert (vgl. Ziff. 10 der AGB). Der Beschwerdeführer zu 1 ist damit sicher von § 97 Abs. 3 S. 3 und Abs. 4 TKG betroffen.

Nach § 100 TKG dürfen die Diensteanbieter, deren Kunde der Beschwerdeführer zu 1 ist, auf seine Person bezogene Bestands- und Verkehrsdaten zur Störungs- und Missbrauchsbekämpfung erheben und beliebig lang speichern. Die Firma T-Online International AG, deren Kunde der Beschwerdeführer zu 1 ist, macht von diesem Recht insoweit Gebrauch als sie ihren Kunden zugewiesene IP-Adressen mindestens 80 Tage lang zu den genannten Zwecken speichert. Der Beschwerdeführer zu 1 ist damit sicher von § 100 TKG betroffen. Inwieweit die Firma T-Online International AG im Übrigen – und auch die Firma Vodafone D2 GmbH – von § 100 TKG Gebrauch machen, ist dem Beschwerdeführer zu 1 nicht bekannt, und er würde von einer solchen Datenspeicherung auch nicht benachrichtigt. Insoweit muss, wie oben (Seite 6) dargelegt, seine mögliche Grundrechtsbetroffenheit genügen.

Nach § 111 TKG müssen die Diensteanbieter, deren Kunde der Beschwerdeführer zu 1 ist, diverse auf seine Person bezogene Bestandsdaten erheben und speichern. Die Firma Vodafone D2 GmbH, deren Kunde der Beschwerdeführer zu 1 ist, hat entsprechend § 111 TKG die dort bezeichneten Daten von dem Beschwerdeführer zu 1 erhoben und speichert sie. Der Beschwerdeführer zu 1 ist damit sicher von § 111 TKG betroffen.

Nach § 112 Abs. 1 TKG muss die Vodafone D2 GmbH, deren Kunde der Beschwerdeführer zu 1 ist, die in § 111 TKG bezeichneten Daten in eine Datenbank einstellen und diese zum Abruf bereit halten. Nach § 112 Abs. 2 TKG ist diversen Behörden auf Anfrage Auskunft über gespeicherte Daten zu erteilen. Ob Daten des Beschwerdeführers zu 1 entsprechend dieser Vorschrift an Behörden übermittelt worden sind, ist diesem zwar nicht bekannt. Von etwa erfolgenden Übermittlungen erlangt der Beschwerdeführer jedoch auch keine Kenntnis. Die Vodafone D2 GmbH darf Zugriffe dem Gesetz zufolge nicht aufzeichnen (§ 112 Abs. 1 S. 5 TKG), und die Protokolldaten der Regulierungsbehörde dürfen nur zu Zwecken der Datenschutzkontrolle durch die zuständige Stelle verwendet werden (§ 112 Abs. 4 S. 5 TKG). Insoweit muss, wie oben Seite(6) dargelegt, die mögliche Grundrechtsbetroffenheit des Beschwerdeführers zu 1 genügen.

Nach § 113 TKG haben die Diensteanbieter, deren Kunde der Beschwerdeführer zu 1 ist, diversen Behörden auf Anfrage Auskunft über Bestandsdaten zu erteilen. Ob Daten des Beschwerdeführers zu 1 entsprechend dieser Vorschrift übermittelt worden sind, ist diesem zwar nicht bekannt. Von etwa erfolgenden Übermittlungen erlangt der Beschwerdeführer jedoch auch keine Kenntnis. § 113 Abs. 1 S. 4 TKG verbietet es Diensteanbietern vielmehr ausdrücklich, ihre Kunden von Auskünften zu benachrichtigen. Insoweit muss wiederum, wie oben Seite(6) dargelegt, die mögliche Grundrechtsbetroffenheit des Beschwerdeführers zu 1 genügen.

Gegen die unmittelbar durch Gesetz erfolgte Grundrechtsverletzung ist der Rechtsweg nicht zulässig. Der Beschwerdeführer zu 1 hat auch sonst keine andere Möglichkeit, um gegen die Grundrechtsverletzung vorzugehen.

Das TKG trat am 26.06.2004 in Kraft, so dass die bis zum 25.06.2005 laufende Beschwerdefrist des § 93 Abs. 3 BVerfGG gewahrt ist.

2.2 Beschwerdeführer zu 2

Dass auch der Beschwerdeführer zu 2 von den §§ 92, 95 Abs. 3, 97 Abs. 3 S. 3 und Abs. 4, 100, 111, 112, 113 TKG selbst, gegenwärtig und unmittelbar in Grundrechten betroffen ist, ergibt sich aus den Ausführungen bezüglich des Beschwerdeführers zu 1, die für den Beschwerdeführer zu 2 entsprechend gelten. Die Praxis der Erhebung und Verwendung von personenbezogenen Daten der Firma T-Mobile Deutschland GmbH entspricht im Wesentlichen der der Firma Vodafone D2 GmbH. Bezüglich § 111 TKG muss es genügen, dass der Beschwerdeführer von der zwangsweisen Erhebung von vorausbezahlten Mobiltelefonkarten bei jedem künftigen Erwerb betroffen sein wird.

2.3 Beschwerdeführer zu 3 bis 5

Die Beschwerdeführer/innen zu 3 bis 6 sind von den §§ 95 Abs. 3, 110 TKG selbst, gegenwärtig und unmittelbar in Grundrechten betroffen. Sie sind Unternehmen, die geschäftsmäßig Telekommunikationsdienste für die Öffentlichkeit erbringen. Gemäß § 110 TKG sind sie verpflichtet, ohne staatliche Kostenerstattung die zur Überwachung der Telekommunikation erforderlichen Vorrichtungen vorzuhalten. Aufgrund der Teilnehmerzahl gilt die Ausnahmevorschrift des § 3 TKÜV für sie nicht. Nach § 95 Abs. 3 TKG dürfen sie Bestandsdaten erst mit Ablauf des auf die Vertragsbeendigung folgenden Jahres löschen.

Gegen die unmittelbar durch Gesetz erfolgte Grundrechtsverletzung ist der Rechtsweg nicht zulässig. Die Beschwerdeführer/innen zu 3 bis 6 haben auch sonst keine andere Möglichkeit, um gegen die Grundrechtsverletzung vorzugehen.

Das TKG trat am 26.06.2004 in Kraft, so dass die bis zum 25.06.2005 laufende Beschwerdefrist des § 93 Abs. 3 BVerfGG gewahrt ist.

3. Begründetheit der Verfassungsbeschwerde

3.1. § 100 TKG

§ 100 TKG lautet:
§ 100 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten
(1) Soweit erforderlich, darf der Diensteanbieter zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden.
(2) Zur Durchführung von Umschaltungen sowie zum Erkennen und Eingrenzen von Störungen im Netz ist dem Betreiber der Telekommunikationsanlage oder seinem Beauftragten das Aufschalten auf bestehende Verbindungen erlaubt, soweit dies betrieblich erforderlich ist. Das Aufschalten muss den betroffenen Gesprächsteilnehmern durch ein akustisches Signal angezeigt und ausdrücklich mitgeteilt werden.
(3) Soweit erforderlich, darf der Diensteanbieter bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte die Bestandsdaten und Verkehrsdaten erheben und verwenden, die zum Aufdecken sowie Unterbinden von Leistungserschleichungen und sonstigen rechtswidrigen Inanspruchnahmen der Telekommunikationsnetze und -dienste erforder-

lich sind. Zu dem in Satz 1 genannten Zweck darf der Diensteanbieter die erhobenen Verkehrsdaten in der Weise verwenden, dass aus dem Gesamtbestand aller Verkehrsdaten, die nicht älter als sechs Monate sind, die Daten derjenigen Verbindungen des Netzes ermittelt werden, für die tatsächliche Anhaltspunkte den Verdacht der rechtswidrigen Inanspruchnahme von Telekommunikationsnetzen und -diensten begründen. Insbesondere darf der Diensteanbieter aus den nach Satz 1 erhobenen Verkehrsdaten und den Bestandsdaten einen pseudonymisierten Gesamtdatenbestand bilden, der Aufschluss über die von den einzelnen Teilnehmern erzielten Umsätze gibt und unter Zugrundelegung geeigneter Missbrauchskriterien das Auffinden solcher Verbindungen des Netzes ermöglicht, bei denen der Verdacht einer Leistungserschleichung besteht. Die Daten der anderen Verbindungen sind unverzüglich zu löschen. Die Regulierungsbehörde und der oder die Bundesbeauftragte für den Datenschutz sind über Einführung und Änderung eines Verfahrens nach Satz 1 unverzüglich in Kenntnis zu setzen.
(4) Unter den Voraussetzungen des Absatzes 3 Satz 1 darf der Diensteanbieter im Einzelfall Steuersignale erheben und verwenden, soweit dies zum Aufklären und Unterbinden der dort genannten Handlungen unerlässlich ist. Die Erhebung und Verwendung von anderen Nachrichteninhalten ist unzulässig. Über Einzelmaßnahmen nach Satz 1 ist die Regulierungsbehörde in Kenntnis zu setzen. Die Betroffenen sind zu benachrichtigen, sobald dies ohne Gefährdung des Zwecks der Maßnahmen möglich ist.

3.1.1 Art. 10 GG

3.1.1.1 Schutzbereich

Das Fernmeldegeheimnis schützt die vertrauliche Inanspruchnahme der Telekommunikation frei von staatlicher Kenntnisnahme. Unstreitig geschützt sind Kommunikationsinhalte wie auch die näheren Umstände der Telekommunikation. Die in § 100 TKG angesprochenen Verkehrsdaten sind definiert als "Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden" (§ 3 Nr. 30 TKG). Nach § 96 Abs. 1 TKG handelt es sich dabei insbesondere um folgende Daten: *die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten, den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen, den vom Nutzer in Anspruch genommenen Telekommunikationsdienst, die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen, sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.* All diese Daten geben Auskunft über die näheren Umstände der Telekommunikation einzelner Teilnehmer. Damit fallen Verkehrsdaten in den Schutzbereich des Fernmeldegeheimnisses (vgl. BVerfG, 1 BvR 330/96 vom 12.3.2003, Absatz-Nrn. 46 und 47, http://www.bverfg.de/entscheidungen).

Vom Schutzbereich des Fernmeldegeheimnisses erfasst sind aber auch Angaben über das Telekommunikationsunternehmen, das ein Kunde in Anspruch nimmt, sowie Angaben über die Ausgestaltung des Vertragsverhältnisses (sogenannte Bestandsdaten, z.B. zugewiesene Rufnummer, zugewiesene PIN zur Ermöglichung der Nutzung des Dienstes, Datum des Vertragsschlusses und -endes, Anschrift und Geburtsdatum des Kunden). Nur, wenn auch Angaben über das Vertragsverhältnis mit Telekommunikationsunternehmen

vor staatlichen Zugriffen geschützt sind, ist eine vertrauliche Inanspruchnahme der Telekommunikation frei von staatlicher Kenntnisnahme gewährleistet. Zur weiteren Begründung wird auf die Ausführungen bei Breyer, RDV 2003, 218 (218 f.) verwiesen, wobei die zentralen Argumente die folgenden sind:

- Bestandsdaten beschreiben die einzelnen Kommunikationsvorgänge näher (z.B. nach dem eingesetzten Unternehmen und den an der Kommunikation Beteiligten) und ermöglichen den staatlichen Zugriff auf Inhalts- und Verkehrsdaten (z.B. durch Überwachungsanordnungen oder durch den unmittelbaren Zugriff auf Mailboxen mittels Zugangscodes).
- Schutzzweck des Fernmeldegeheimnisses ist es, die an der Telekommunikation Beteiligten so zu stellen, wie sie bei unmittelbarer Kommunikation miteinander stünden. Im Fall unmittelbarer Kommunikation aber würden keine Bestandsdaten anfallen und gespeichert werden.

Die relevanten Ausführungen bei Breyer, RDV 2003, 218 (218 f.) lauten im Einzelnen wie folgt:

> **Verfassungsrechtliche Einordnung**
>
> Bestandsdaten sind personenbezogene Daten, die als solche jedenfalls durch das Recht auf informationelle Selbstbestimmung geschützt sind[1]. Dies entspricht dem Schutzzweck dieses Rechts, Grundrechtsträger vor der Gefahr zu schützen, dass der Staat über sie unbegrenzt Kenntnisse sammelt und infolgedessen nachteilige Maßnahmen ihnen gegenüber ergreifen kann. Nicht nur die staatliche Kenntnis von Kommunikationsinhalten oder Verbindungsdaten begründet diese Gefahr. Auch die Kenntnis der Tatsache, dass ein Bürger überhaupt ein vertragliches Verhältnis mit einem bestimmten Diensteanbieter begründet hat und wie dieses ausgestaltet ist, kann zu unerwünschten Kommunikationsanpassungen seitens des Einzelnen führen. Wer beispielsweise an der Teilnahme an einem Internet-Chat für Muslime in Deutschland interessiert ist, wird es in Erinnerung an Maßnahmen der "Anti-Terror-Rasterfahndung" mit anschließender Befragung der "Ausgefilterten" möglicherweise vorziehen, auf die Ausübung seiner Grundrechte (hier unter anderem der Religionsfreiheit) zu verzichten. Dasselbe kann etwa für die Anmeldung zur Teilnahme an einem Meinungsforum gelten, in dem Protestaktivitäten gegen die Atomkraft diskutiert werden (Meinungsfreiheit, Versammlungsfreiheit). Auch die Mitgliedschaft in sonstigen geschlossenen Netzen, bereitgestellt etwa von einer Aids-Selbsthilfegruppe, kann Rückschlüsse auf bestimmte Problemlagen erlauben[2]. Dasselbe gilt bereits für

[1] OVG Münster, MMR 2002, 563 (564).

[2] DSB-Konferenz vom 14./15.03.2000, www.bfd.bund.de/information/info5/anl/an06.html.

Standard-Telekommunikationsdienste[3]. Wer beispielsweise einen Internetzugang zum Pauschaltarif nutzt, wird von den Behörden als intensiver Internetnutzer angesehen werden. Wer bei der deutschen Telefongesellschaft "Alo Vatan" angemeldet ist, wird im Zweifel einen Bezug zu der Türkei aufweisen. Wer einen bestimmten Optionstarif im Mobilfunknetz nutzt, bei dem man fünf Festnetzanschlüsse vom Handy aus besonders preisgünstig erreichen kann (wird etwa von der Firma Eplus angeboten), gibt schon mit diesen Bestandsdaten preis, mit wem er oft telefoniert. Die genannten Beispiele zeigen, dass Bestandsdaten nicht nur besonders sensibel sein können, sondern auch weit gehende Rückschlüsse auf Inhalt und Umstände einzelner Kommunikationsvorgänge erlauben können.

Fraglich ist, ob Telekommunikations-Bestandsdaten auch durch das Fernmeldegeheimnis (Art. 10 GG) geschützt sind[4]. Einer Einbeziehung von Bestandsdaten in den Schutzbereich des Art. 10 GG steht der Wortlaut "Fernmeldegeheimnis" zunächst nicht entgegen. Er erlaubt die Auslegung, dass das "Geheimnis" auch das Vertragsverhältnis umfassen soll, welches den einzelnen Fernmeldevorgängen zugrunde liegt.

Für eine Einbeziehung von Bestandsdaten in den Schutzbereich des Art. 10 GG spricht, dass die Information, welcher Anbieter für die Telekommunikation genutzt wird und wie das Vertragsverhältnis zu diesem Anbieter ausgestaltet ist, die im Rahmen dieses Vertragsverhältnisses abgewickelten Kommunikationsvorgänge inhaltlich näher beschreibt und damit einen näheren Umstand der einzelnen Kommunikationsvorgänge darstellt[5]. Dass das Fernmeldegeheimnis für die näheren Umstände einzelner Kommunikationsvorgänge gilt, ist anerkannt. Bestandsdaten unterscheiden sich von Verbindungsdaten nur dadurch, dass sie die Umstände von Kommunikationsvorgängen stets in gleicher Weise wiedergeben, während sich Verbindungsdaten typischerweise von Verbindung zu Verbindung ändern. Dass darin kein relevanter Unterschied liegt, zeigt aber das Beispiel der Internetnutzung. Während manche Internet-Access-Provider dem Nutzer eine IP-Adresse fest zuweisen (dann Bestandsdatum), teilen andere Dienste dem Nutzer für jede Verbindung eine andere IP-Adresse zu (dann Verbindungsdatum). Solche Zufälligkeiten können für die Bestimmung des Schutzbereichs des Fernmeldegeheimnisses richtigerweise keine Rolle spielen.

---

[3] Vgl. ULD-SH, Sichere Informationsgesellschaft, www.datenschutzzentrum.de/material/themen

[4] Dafür, soweit Bestandsdaten eine staatliche Überwachung ermöglichen AK-GG-Bizer, Art. 10 Rn. 71; dagegen OVG Münster, MMR 2002, 563 (564); Schaar, Sicherheit und Freiheitsrechte, www.peter-schaar.de/schutzkonzepte.pdf, 21; Kooperationskreis "IuK-Datenschutz", in: Garstka, Jahresbericht 1998, www.datenschutz-berlin.de/jahresbe/98/teil5.htm, unter 5.3 sowie die h.M.

[5] A.A. ohne Begründung Wuermeling/Felixberger, CR 97, 230 (234).

Darüber hinaus lässt sich aus der Information, dass eine Person Kunde eines Kommunikationsmittlers ist, regelmäßig schließen, dass der jeweilige Dienst auch in Anspruch genommen wird. Bereits die Tatsache, dass sich jemand des Mediums der Telekommunikation bedient, fällt als "Ob" der Telekommunikation nach der Definition des Bundesverfassungsgerichts in den Schutzbereich des Art. 10 GG, wenn das Gericht feststellt, zu den Kommunikationsumständen gehöre "insbesondere, ob, wann und wie oft zwischen welchen Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat"[6]. Diese Definition ist bereits ihrem Wortlaut nach nicht auf einzelne Telekommunikationsvorgänge beschränkt.

Hinzu kommt, dass die Kenntnis von Bestandsdaten oftmals Vorbedingung für den staatlichen Zugriff auf einzelne Kommunikationsvorgänge ist. Anbieter von Telekommunikationsdiensten müssen beispielsweise immer auf Bestandsdaten zurück greifen, um dem Staat Auskunft darüber erteilen zu können, welche Personen an einem Kommunikationsvorgang beteiligt waren. In den Aufzeichnungen der Anbieter über einzelne Kommunikationsvorgänge ist nämlich regelmäßig nur ein technisches Merkmal zur Identifizierung der Kunden gespeichert (beispielsweise deren Rufnummer), nicht aber auch deren Name und Anschrift. Auch dieser Zusammenhang spricht dafür, Bestandsdaten in den Schutz des Fernmeldegeheimnisses einzubeziehen.

Schließlich ist der Schutzzweck des Fernmeldegeheimnisses zu beachten, nämlich die an der Telekommunikation Beteiligten so zu stellen, wie sie bei unmittelbarer Kommunikation miteinander stünden[7]. Im Falle der unmittelbaren Kommunikation gäbe es keine Vertragsverhältnisse zu einem Kommunikationsmittler, in deren Rahmen personenbezogene Daten über die an der Kommunikation Beteiligten gespeichert würden. Insoweit realisiert sich das spezifische Risiko für die Vertraulichkeit der Telekommunikation, das mit der Inanspruchnahme von Telekommunikationsdiensten verbunden ist, in der Speicherung von Bestandsdaten bei Kommunikationsmittlern. Bestandsdaten über das Vertragsverhältnis mit Kommunikationsmittlern sind daher nicht nur durch das Recht auf informationelle Selbstbestimmung sondern auch durch das Fernmeldegeheimnis geschützt.

---

[6] BVerfGE 100, 313 (358).

[7] BVerfGE 85, 386 (396); BVerfGE 100, 313 (363); Gusy, JuS 86, 89 (90 f.); vgl. auch Dreier-Hermes, Art. 10 Rn. 47.

3.1.1.2 Eingriff

§ 100 TKG greift in das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG ein. Die Vorschrift räumt Telekommunikationsunternehmen nämlich das Recht ein, Bestands- und Verkehrsdaten länger als für ihre Zwecke erforderlich speichern zu dürfen.

Es stellt einen staatlichen Eingriff in Art. 10 GG dar, wenn Telekommunikationsunternehmen das Recht eingeräumt wird, Bestands- und Verkehrsdaten länger als für ihre Zwecke erforderlich speichern zu dürfen, und wenn gleichzeitig staatlichen Behörden Zugriffsrechte auf diese Daten eingeräumt werden. Zur Begründung wird auf die Ausführungen bei Breyer, Vorratsspeicherung (2005)[8], Seiten 90-101 verwiesen, wobei die zentralen Argumente die folgenden sind:

- Nach dem modernen Eingriffsbegriff ist ein Grundrechtseingriff schon dann anzunehmen, wenn der Staat eine besondere Beeinträchtigungsgefahr für ein Grundrecht schafft, die sich jederzeit verwirklichen kann (vgl. BVerfGE 100, 313 [366]).
- Die Speicherung von Telekommunikations-Verkehrsdaten durch Telekommunikationsunternehmen macht diese Daten für eine spätere staatliche Kenntnisnahme verfügbar, birgt also in Verbindung mit staatlichen Zugriffsrechten wie den §§ 100g, 100h StPO die latente Gefahr späterer, weiterer Eingriffe in Art. 10 GG.
- Dass § 100 TKG Telekommunikationsunternehmen zur Datenspeicherung nicht verpflichtet sondern "nur" berechtigt, ist unerheblich, weil nur die Kunden in eine Verarbeitung ihrer Daten einwilligen können. Die bloße Nutzung eines Telekommunikationsdienstes stellt keine Einwilligung dar (BVerwG, 6 C 23.02 vom 22.10.2003, Absatz-Nr. 20, http://www.bundesverwaltungsgericht.de).
- Die Datenspeicherung durch Telekommunikationsunternehmen ist dem Staat nur insoweit nicht zuzurechnen, wie sie für betriebliche Zwecke erforderlich ist. Nur insoweit schafft der Staat, der eine solche Datenspeicherung gestattet, keine besondere, über das Notwendige hinaus gehende Beeinträchtigungsgefahr für Grundrechte.

Die relevanten Ausführungen bei Breyer, Vorratsspeicherung (2005)[9], Seiten 90-101 lauten hierzu im Einzelnen wie folgt:

> **Verpflichtung Privater zur Vorratsdatenspeicherung als Eingriff**
>
> Entsprechend den genannten Kriterien des Bundesverfassungsgerichts stellt die staatliche Kenntnisnahme von Telekommunikationsdaten ebenso einen Eingriff in Art. 10 GG dar wie eine Rechtsnorm, die den Staat zu einer solchen Kenntnisnahme ermächtigt. Fraglich ist aber, ob der Gesetzgeber in Art. 10 GG bereits

[8] Breyer, Patrick Breyer: Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staaatliche Zwecke in Deutschland (Vorratsspeicherung, traffic data retention), ISBN 3-937231-46-3, www.vorratspeicherung.de.vu

[9] Breyer, (Fn. 8).

dadurch eingreift, dass er Telekommunikationsunternehmen die Pflicht auferlegt, personenbezogene Daten über die näheren Umstände der Telekommunikation auf Vorrat zu speichern und für den Abruf durch staatliche Behörden verfügbar zu halten.

Für den Fall einer Auskunftsanordnung nach § 12 FAG (jetzt § 100g StPO) hat das Bundesverfassungsgericht entschieden, dass bereits die gerichtliche Anordnung gegenüber einem Kommunikationsmittler, Telekommunikationsdaten an staatliche Stellen zu übermitteln, einen Eingriff in den Schutzbereich des Fernmeldegeheimnisses darstelle[10]. Bereits die gerichtliche Anordnung ermögliche nämlich die spätere Kenntnisnahme der Telekommunikationsdaten durch staatliche Stellen[11]. Auch eine generelle Vorratsspeicherungspflicht ermöglicht eine spätere staatliche Kenntnisnahme der Daten. Im Unterschied zur gerichtlichen Anordnung steht im Fall einer Vorratsspeicherung allerdings noch nicht fest, dass eine staatliche Kenntnisnahme erfolgen wird. Das Kommunikationsunternehmen wird zunächst nur zur Vorhaltung der Daten verpflichtet.

Nach dem modernen Eingriffsbegriff schützen die speziellen Grundrechte auch vor mittelbaren Eingriffen durch staatliche Maßnahmen, welche die Beeinträchtigung eines grundrechtlich geschützten Verhaltens typischerweise und vorhersehbar zur Folge haben oder die eine besondere Beeinträchtigungsgefahr in sich bergen, die sich jederzeit verwirklichen kann[12]. Auf dieser Linie liegt das Bundesverfassungsgericht, wenn es bereits die einer Kenntnisnahme von Telekommunikation "vorangehenden Arbeitsschritte" als Eingriff ansieht, soweit es sich nicht um eine rein sachbedingte Speicherung handelt: "Für die Kenntnisnahme von erfassten Fernmeldevorgängen durch Mitarbeiter des Bundesnachrichtendienstes steht folglich die Eingriffsqualität außer Frage. Aber auch die vorangehenden Arbeitsschritte müssen in ihrem durch den Überwachungs- und Verwendungszweck bestimmten Zusammenhang betrachtet werden. Eingriff ist daher schon die Erfassung selbst, insofern sie die Kommunikation für den Bundesnachrichtendienst verfügbar macht und die Basis des nachfolgenden Abgleichs mit den Suchbegriffen bildet. An einem Eingriff fehlt es nur, soweit Fernmeldevorgänge zwischen deutschen Anschlüssen ungezielt und allein technikbedingt zunächst miterfasst, aber unmittelbar nach der Signalaufbereitung technisch wieder spurenlos ausgesondert werden."[13]

---

[10] BVerfG, NJW 2003, 1787 (1789).

[11] BVerfG, NJW 2003, 1787 (1789).

[12] Windthorst, § 8, Rn. 50 und 52 m.w.N.

[13] BVerfGE 100, 313 (366).

Die Beurteilung einer Vorratsspeicherung von Telekommunikationsdaten kann nicht anders ausfallen[14], denn auch die Speicherung von Telekommunikations-Verkehrsdaten macht diese für eine spätere staatliche Kenntnisnahme verfügbar und birgt damit die latente Gefahr späterer, weiterer Eingriffe. Deswegen stellt eine Vorratsspeicherung auch nicht nur eine "allein technikbedingt[e]" Miterfassung dar, die keine Spuren hinterlässt und damit jede staatliche Kenntnisnahme ausschließt. Hiervon kann allenfalls die Rede sein, soweit bestimmte auf einen Kommunikationsvorgang bezogene Daten für die Dauer des Vorgangs technikbedingt gespeichert sein müssen. Eine Verpflichtung zur Vorratsspeicherung von Verkehrsdaten über diese Dauer hinaus begründet dagegen die besondere Gefahr, dass der Staat die gespeicherten Daten aufgrund von staatlichen Zugriffsbefugnissen wie den §§ 100g, 100h StPO anfordert. Beeinträchtigungen der von Art. 10 GG geschützten Vertraulichkeit der Telekommunikation vor dem Staat sind daher die typische und vorhersehbare Folge einer generellen Verkehrsdatenspeicherungspflicht. Damit stellt bereits die Anordnung einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten durch den Normgeber einen staatlichen Eingriff in Art. 10 GG dar.

Dass sich der Staat zur Speicherung privater Unternehmen bedient, kann keinen Unterschied machen, wenn er sich gleichzeitig den Zugriff auf die gespeicherten Daten eröffnet[15]. Andernfalls könnte der Staat seine Grundrechtsbindung durch ein bloßes "Outsourcing" umgehen. Die Inanspruchnahme Privater erhöht das Gewicht des Eingriffs sogar noch, weil sich der Kreis von – weitgehend ohne Schuld – beeinträchtigten Personen durch den zusätzlichen Eingriff in Art. 12 GG noch vergrößert. Zudem ist das Risiko, dass gespeicherte Daten missbraucht werden, bei einer Verkehrsdatenspeicherung durch eine Vielzahl von Privatunternehmen erheblich höher einzuschätzen als bei einer staatlichen Speicherung, so dass die Privilegierung einer privaten Vorratsspeicherung auch sachlich nicht gerechtfertigt wäre.

Bereits entschieden hat das Bundesverfassungsgericht, dass die Übermittlung von Telekommunikation an staatliche Stellen durch einen privaten Kommunikationsmittler, der die Telekommunikation auf gerichtliche Anordnung gemäß § 100a StPO hin aufzeichnet und den staatlichen Stellen verfügbar macht, ei-

[14] Ebenso für eine Pflicht zur generellen Speicherung von Telekommunikations-Bestandsdaten unter dem Aspekt des Grundrechts auf informationelle Selbstbestimmung BVerwG, 6 C 23.02 vom 22.10.2003, Absatz-Nr. 19, www.bundesverwaltungsgericht.de/enid

[15] Vgl. Bizer, Forschungsfreiheit, 159 für das "Auf-Abruf-Bereithalten" von Daten.

nen Eingriff in das Fernmeldegeheimnis der an dem Kommunikationsvorgang Beteiligten darstellt[16]. Die Tatsache, dass sich der Staat dabei eines Privaten bediene, sei unerheblich, da der Eingriff hoheitlich angeordnet werde und dem Privaten kein Handlungsspielraum zur Verfügung stehe[17]. Ebenso verhält es sich bei einer Vorratsspeicherungspflicht.

Auch die Bundesregierung sieht das Fernmeldegeheimnis für eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten als einschlägig an[18]. Dass auch der Gesetzgeber von einem Eingriff insoweit ausgehen würde, zeigt sich daran, dass er in § 16b WpHG Art. 10 GG zitiert hat. § 16b WpHG sieht vor, dass unter bestimmten Umständen angeordnet werden kann, dass ein Unternehmen bereits gespeicherte Telekommunikations-Verbindungsdaten aufzubewahren hat. Ob die Behörde die aufbewahrten Verbindungsdaten später tatsächlich anfordert und zur Kenntnis nimmt, steht in diesem Zeitpunkt noch nicht fest. Wie das Zitat des Art. 10 GG zeigt, sieht der Gesetzgeber bereits in dieser vorsorglichen Aufbewahrung von Verkehrsdaten zu staatlichen Zwecken einen Eingriff in die Rechte der an dem Kommunikationsvorgang Beteiligten aus Art. 10 GG.

Unerheblich für die Einordnung als Eingriff ist auch, ob die betroffenen Unternehmen Verkehrsdaten allein zu staatlichen Zwecken speichern müssen oder ob ihnen zugleich die Nutzung der gespeicherten Daten zu eigenen Zwecken erlaubt ist, etwa zu Abrechnungs- oder Marketingzwecken. In jedem Fall begründet das Bestehen staatlicher Zugriffsrechte die latente Gefahr staatlicher Eingriffe. An dieser Gefahr ändern zusätzliche Nutzungsrechte nichts.

Zu einer abweichenden Beurteilung einer Vorratsspeicherungspflicht gibt auch die Ansicht des Bundesverfassungsgerichts keinen Anlass, dass die so genannte Zielwahlsuche nur einen Eingriff in die Grundrechte derjenigen Personen darstelle, deren Anschlussnummern schließlich an den Staat übermittelt werden[19]. Eine Zielwahlsuche nach § 100g Abs. 2 StPO kann angeordnet werden, wenn ermittelt werden soll, von welchen Anschlüssen aus in einem bestimmten Zeitraum Verbindungen zu einem bestimmten, der Eingriffsbehörde bekannten, anderen Telefonanschluss hergestellt worden sind. Im Fall eines Mordes kann beispielsweise von Interesse sein, welche Personen das Opfer in der letzten Zeit vor sei-

[16] BVerfG, NJW 2003, 1787 (1789).
[17] BVerfG, NJW 2003, 1787 (1789).
[18] BT-Drs. 14/9801, 14 (15).
[19] BVerfG, NJW 2003, 1787 (1792 f.).

nem Tod angerufen haben. Da Verbindungsdaten bei den Telefongesellschaften geordnet nach der Rufnummer des Anrufers gespeichert werden, ist zur Durchführung einer Suche nach bestimmten Zielrufnummern die Durchsuchung des gesamten Datenbestands der Telefongesellschaft erforderlich. Die letztendlich erteilte Auskunft enthält dann nur die Rufnummern, von denen aus der vorgegebene Anschluss angerufen wurde. Aus ihr lässt sich aber auch entnehmen, dass die Nummer von anderen Telefonanschlüssen aus nicht angerufen wurde. Das Bundesverfassungsgericht sieht einen Grundrechtseingriff in diesem Fall gleichwohl nur bezüglich derjenigen Personen, deren Anschlussnummern schließlich an die Behörden übermittelt werden. Hinsichtlich der übrigen Personen erfolge der Zugriff lediglich maschinell und bleibe anonym, spurenlos und ohne Erkenntnisinteresse für die Strafverfolgungsbehörden, so dass es insoweit an einem Eingriff fehle[20]. Auf den Fall der Vorratsspeicherung übertragen könnte diese Ansicht bedeuten, dass ein Eingriff nur in Bezug auf diejenigen Personen vorläge, deren Daten schließlich an die Behörden übermittelt würden.

Subsumiert man den Vorgang der Zielwahlsuche jedoch unter die anerkannte Definition, der zufolge jede dem Staat zuzurechnende Verarbeitung von Daten, die durch das Fernmeldegeheimnis geschützt sind, einen Eingriff in Art. 10 GG darstellt, so ergibt sich klar, dass ein Eingriff auch in das Fernmeldegeheimnis der unmittelbar nicht von der Auskunft betroffenen Personen vorliegt[21]. Auch ihre Daten werden im Rahmen der Zielwahlsuche nämlich verarbeitet. In einer früheren Entscheidung stellte das Bundesverfassungsgericht ausdrücklich fest, dass die "Prüfung, ob die mittels der Fernmeldeüberwachung erlangten personenbezogenen Daten für die Zwecke, die diese Maßnahmen legitimieren, erforderlich sind, [...] Eingriffsqualität [hat], weil es sich um einen Selektionsakt handelt"[22]. Dass die Verarbeitung im Rahmen der Zielwahlsuche dem Staat zuzurechnen ist, ergibt sich daraus, dass die staatliche Kenntnisnahme der Zweck der Zielwahlsuche ist. Die Eingriffsqualität kann auch nicht davon abhängen, an welchen der übermittelten Daten die Behörde im Zeitpunkt der Übermittlung gerade interessiert sein mag. Woran die Behörde interessiert ist, lässt sich nicht feststellen und kann sich jederzeit ändern. Weiterhin ist auch die Information, wer nicht mit dem Zielanschluss telefoniert hat, nicht unbedingt ohne Erkenntnisinteresse für die Strafverfolgungsbehörden. Denkbar ist beispielsweise der Fall, dass ein Beschuldigter angibt, zum Tatzeitpunkt in einer Kneipe mit einem Freund telefoniert zu haben. Stellt sich durch eine Zielwahlsuche heraus, dass in

[20] BVerfG, NJW 2003, 1787 (1792 f.).

[21] So offenbar auch BVerwG, 6 C 23.02 vom 22.10.2003, Absatz-Nr. 19, www.bundesverwaltungsgericht.de/enid für Bestandsdaten.

[22] BVerfGE 100, 313 (367).

der fraglichen Zeit zu dem Telefonanschluss des Freundes keine Verbindungen hergestellt wurden, dann ist diese Negativauskunft für die Strafverfolgungsbehörde durchaus von Interesse und wirkt für den Betroffenen auch belastend. Solange einer Behörde das Ergebnis der Zielwahlsuche bekannt ist, kann auch keine Rede davon sein, dass die Daten der nicht unmittelbar Betroffenen "spurlos" ausgesondert würden; der Auskunft lässt sich im Umkehrschluss schließlich jederzeit entnehmen, von welchen Anschlüssen aus keine Verbindungen hergestellt wurden. Auch die Information, dass keine Anrufe erfolgt sind, kann jederzeit in den Mittelpunkt des staatlichen Ermittlungsinteresses geraten. Die Zielwahlsuche stellt somit einen Eingriff in die Grundrechte sämtlicher Anschlussinhaber dar. Der gegenteiligen Ansicht des Bundesverfassungsgerichts kann nicht gefolgt werden, so dass es auf die Bedeutung dieser Ansicht für eine Vorratsspeicherungspflicht nicht ankommt.

Berechtigung Privater zur Vorratsdatenspeicherung als Eingriff

Fraglich ist schließlich, ob der Gesetzgeber in Art. 10 GG bereits dann eingreift, wenn er Telekommunikationsunternehmen lediglich fakultativ das Recht einräumt, Verkehrsdaten länger als für ihre Zwecke erforderlich speichern zu dürfen, und den staatlichen Behörden gleichzeitig den Zugriff auf diese Daten ermöglicht. Diese Frage ist zu bejahen. Dass eine Speicherung freiwillig erfolgt, ist im Hinblick auf die oben dargestellte Eingriffsdefinition irrelevant, denn auch eine freiwillige Datenspeicherung birgt die latente Gefahr staatlicher Kenntnisnahme, wenn der Staat entsprechende Zugriffsrechte vorsieht. Nur ein Einverständnis der betroffenen Grundrechtsträger würde der Annahme eines staatlichen Eingriffes entgegen stehen, nicht aber das Einverständnis des speichernden Unternehmens. Für das Vorliegen eines Eingriffs in Art. 10 GG kommt es somit nicht darauf an, ob Kommunikationsmittler zur Datenspeicherung verpflichtet oder nur berechtigt werden.

In Deutschland ermächtigt § 97 Abs. 3 S. 3 TKG Telekommunikationsunternehmen zur Speicherung von Verbindungsdaten für bis zu sechs Monate nach Rechnungsversand. Auf diese Daten können die gesetzlich ermächtigten Behörden zu staatlichen Zwecken zugreifen (etwa nach den §§ 100a, 100g StPO), so dass § 97 Abs. 3 S. 3 TKG einen staatlichen Grundrechtseingriff darstellt, wenn er die Speicherung von Verkehrsdaten über die sachlich gebotene Dauer hinaus erlaubt.

Für die Berechnung des Nutzungsentgelts ist eine Speicherung von Verkehrsdaten zunächst nur für kurze Zeit erforderlich. Nach Beendigung eines Nutzungsvorgangs kann unter Einsatz der heute verwendeten Computertechnik das angefallene Entgelt sofort ermittelt und sämtliche Verkehrsdaten sodann gelöscht werden. Dementsprechend sieht § 96 Abs. 2 S. 2 TKG vor, dass nicht benötigte Daten "unverzüglich", also ohne schuldhaftes Zögern, zu löschen sind.

Eine Speicherung von Verkehrsdaten über den Zeitpunkt der Berechnung des Entgelts hinaus könnte zunächst damit gerechtfertigt werden, dass es Telekommunikationsunternehmen möglich sein müsse, diejenigen Benutzer zu identifizieren, die ihre Leistungen in der Absicht in Anspruch nehmen, ihnen das geschuldete Entgelt vorzuenthalten. Es ist allerdings kein Grund ersichtlich, weshalb gerade Telekommunikationsunternehmen Selbsthilferechte eingeräumt werden sollten. Telekommunikationsunternehmen können im Falle des Verdachts einer Straftat (hier § 265a StGB) wie jedes andere Opfer einer Straftat Strafanzeige erstatten und die Ermittlungen den zuständigen Behörden überlassen. Liegen tatsächliche Anhaltspunkte für Leistungserschleichung durch bestimmte Nutzer vor, so kann die Speicherung derer Daten im Einzelfall als erforderlich angesehen werden (vgl. §§ 6 Abs. 8 TDDSG, 19 Abs. 9 MDStV). Eine generelle Speicherung von Verkehrsdaten zur Aufdeckung von Leistungserschleichungen ist jedoch nicht gerechtfertigt.

Teilweise wird unter den Tatbestand der Leistungserschleichung auch illegales Nutzerverhalten subsumiert, das sich nicht gegen den genutzten Dienst, sondern gegen Dritte richtet, etwa die Begehung von Betrug gegenüber einem anderen Internetnutzer unter Inanspruchnahme der Leistungen eines Internet-Providers. Zur Begründung wird darauf verwiesen, dass die meisten Dienste in ihren AGB die Inanspruchnahme des Dienstes zu illegalen Zwecken untersagten[23]. Die Inanspruchnahme eines Dienstes zu illegalen Zwecken führt aber auch aufgrund solcher AGB nicht dazu, dass der Nutzungsvorgang selbst illegal wird, solange das Entgelt dafür entrichtet wird. Wenn es schon in Fällen von Leistungserschleichungen keinen Grund gibt, Telekommunikationsunternehmen Selbsthilferechte einzuräumen, so gilt dies erst recht, wenn die Unternehmen von illegalem Verhalten nicht selbst betroffen sind. Telekommunikationsunternehmen müssen sich also auch hier darauf verweisen lassen, sich wie jeder Andere an die zuständigen Behörden zu wenden. Dies gilt auch für das Argument, Ver-

[23] LINX, Traceability (I), Punkt 11.2.

kehrsdaten müssten aufbewahrt werden, um gestohlene Mobiltelefone mit Hilfe ihrer IMEI-Codes identifizieren zu können[24].

Fraglich ist, ob die Möglichkeit einer Verfolgung vorsätzlicher Angriffe auf die Einrichtungen eines Anbieters, z.B. durch "Hacking", eine generelle Speicherung der Verkehrsdaten aller Kunden rechtfertigt. Zwar müssen dem Anbieter angemessene Maßnahmen zur Gewährleistung des ordnungsgemäßen Betriebs seiner Anlagen zugestanden werden. Insoweit kommen aber zuallererst technische Abwehrmaßnahmen in Betracht. Nur diese sind in der Lage, eine bestimmte Angriffsart dauerhaft und auch gegenüber anderen Nutzern zu unterbinden. Die Identifizierung eines einzelnen Störers wird dagegen regelmäßig nicht erforderlich sein. Jedenfalls genügt es hierzu, im Fall eines Angriffs eine Aufzeichnung von Verkehrsdaten vorzunehmen. Eine generelle Aufzeichnung und Aufbewahrung von Verkehrsdaten ist nicht erforderlich.

Soweit kein vorsätzliches Handeln einzelner Personen im Spiel ist, etwa bei technischen Problemen, kann ebenfalls nicht davon ausgegangen werden, dass zur Gewährleistung der Netzsicherheit, also zur Bereitstellung des Angebots frei von technischen Störungen, die Nutzung personenbezogener Daten erforderlich ist. Insoweit kann allenfalls eine Speicherung technischer Daten in anonymisierter Form gerechtfertigt sein[25]. Das Gleiche gilt für ähnliche Zwecke wie die Beobachtung der Netzauslastung[26], die Erstellung von Fehlerstatistiken, die Überprüfung der Zuverlässigkeit des Dienstes, die Überprüfung der Funktionstüchtigkeit einzelner technischer Elemente eines Dienstes, die Erstellung von Statistiken über die Entwicklung der Leistungsfähigkeit des Dienstes und die Vorhersage von Auslastungsgraden. Es gibt zumutbare technische Mittel zur unwiederbringlichen Anonymisierung von Datenbeständen, deren Einsatz gleichwohl die Nutzbarkeit der Daten zu den genannten Zwecken gewährleistet[27]. Es ist unbefriedigend, dass solche Verfahren nicht in gängige Softwarepakete zur Verwaltung von Verkehrsdaten integriert sind. Ebenso wie die Regierungen eine Erleichterung der Telekommunikationsüberwachung durch die technische Gestaltung von Produkten auf Herstellerebene forcieren[28], müsste auch auf die standardmäßige Berücksichtigung datenschutzfreundlicher Techniken hingewirkt werden.

---

[24] Dazu BfD, Jahresbericht 1999/2000, Kapitel 10.

[25] LINX, User Privacy (I), Punkt 7.2.4.

[26] LINX, User Privacy (I), Punkt 7.2.5.

[27] Nähere Beschreibung bei LINX, User Privacy (I), Punkt 7.4.

[28] DG Research, Economic risks arising from the potential vulnerability of electronic commercial media to interception; Weichert, Bekämpfung von Internet-Kriminalität (I).

Eine Speicherung von Verkehrsdaten über den Zeitpunkt der Berechnung des Entgelts hinaus kann somit nur "zu Beweiszwecken für die Richtigkeit der berechneten Entgelte" erforderlich sein. Fraglich ist, ob § 97 Abs. 3 S. 3 TKG die Aufbewahrung von Verkehrsdaten auf das zu Beweiszwecken erforderliche Maß beschränkt. Zunächst ist zu berücksichtigen, dass es im Vergleich zu den insgesamt anfallenden Entgelten nur in wenigen Fällen zu Entgeltstreitigkeiten kommt[29]. Zudem ist die Aufstellung eines Einzelverbindungsnachweises erst seit Einführung der Digitaltechnik Anfang der 90er Jahre möglich. Vor dieser Zeit konnte man Entgeltstreitigkeiten also offenbar auch ohne Einzelverbindungsnachweis hinreichend klären.

Nach gegenwärtiger Rechtslage trifft den Telekommunikationsanbieter keine Beweislast für die Richtigkeit seiner Abrechnung, soweit er Verkehrsdaten gelöscht hat, weil er zur Löschung verpflichtet war (§ 16 Abs. 2 S. 1 TKV)[30]. Mithin kann für die Bemessung der Aufbewahrungsfrist nur das Interesse der Telekommunikationsnutzer maßgeblich sein. Dieses Interesse rechtfertigt es grundsätzlich nicht, Verkehrsdaten allein deswegen zu speichern, weil sie den Nutzungsvorgang im Falle eines Rechtsstreits über angefallene Nutzungsentgelte plausibel machen können[31]. Mit diesem Argument ließe sich sogar eine Inhaltsspeicherung rechtfertigen, weil auch Telekommunikationsinhalte Indizien für die Berechtigung einer Entgeltforderung darstellen können. Für einen Nachweis der Richtigkeit einer Entgeltforderung wird vielmehr oft die Angabe von Uhrzeit und Dauer eines Gesprächs sowie weniger Ziffern der Anschlussnummer genügen[32].

Dass der Kunde schriftlich eine unverzügliche Löschung der Zielrufnummern nach Rechnungsversand verlangen kann (§ 97 Abs. 4 S. 1 Nr. 2 TKG), steht einem Eingriff durch § 97 Abs. 3 S. 3 TKG nicht entgegen, weil anzunehmen ist, dass viele Kunden aus Unkenntnis oder Unverständnis über die Konsequenzen eines solchen Verlangens von diesem Recht keinen Gebrauch machen. Außerdem ist ein Löschungsverlangen nach der gesetzlichen Ausgestaltung mit dem Risiko verbunden, dass der abgesandte Einzelverbindungsnachweis auf dem Postweg verloren gehen kann und der Kunde daher eventuell eine überhöhte

[29] OVG Bremen, NJW 1995, 1769 (1773): "Es ist mit dem verfassungsrechtlichen Maßstab des Übermaßverbotes unvereinbar, Datenspeicherungen in großem Umfang vorzunehmen, nur um Beweiserleichterungen in den am Gesamtvolumen der Entgeltfälle gemessen wenigen Entgeltstreitigkeiten zu erreichen, wenn es technische Möglichkeiten gibt, die den berechtigten Beweisinteressen der Telekom und den berechtigten Verbraucherschutzinteressen ihrer Kunden in angemessener Weise genügen, dabei aber in geringerer Weise in die grundrechtsgeschützte Sphäre des Fernmeldegeheimnisses eingreifen."

[30] Vgl. auch Bizer, Telekommunikation und Innere Sicherheit 2000, 505: "Zwar handelt es sich [bei der Sechsmonatsfrist] nur um eine 'kann'-Regelung, jedoch ist unter den TK-Dienstanbietern entgegen § 16 TKV die Meinung verbreitet, eine frühzeitige Löschung führe zu Beweisnachteilen, wenn Kunden die Höhe eines Entgeltes bestreiten."

[31] LINX, User Privacy (I), Punkt 7.3.

Rechnung begleichen muss (vgl. § 16 Abs. 2 S. 1 TKV). Schließlich gilt § 97 Abs. 4 S. 1 Nr. 2 TKG nicht für andere Verkehrsdaten als Zielrufnummern.

In Anlehnung an Fristen, die im Geschäftsverkehr beispielsweise zur Prüfung von Kontoauszügen der Banken üblich sind, erscheint grundsätzlich eine vierwöchige Aufbewahrung der für die Berechnung der Entgeltforderung maßgeblichen Daten ausreichend, um den Kunden nach Übersendung einer Rechnung hinreichende Zeit zur Erhebung von Einwendungen zu geben. Wird die Rechnung innerhalb dieses Zeitraums vorbehaltlos beglichen, ist eine Aufbewahrung von Verkehrsdaten nicht mehr erforderlich[33].

Eine Aufbewahrung von Verkehrsdaten ist auch dann nicht erforderlich, wenn der Kunde im Voraus auf Einwendungen gegen Rechnungsforderungen verzichtet. Diesen Gedanken setzt § 97 Abs. 4 S. 1 Nr. 2 TKG, wonach der Kunde eines Telekommunikationsanbieters die Löschung der gewählten Zielrufnummern mit Versand einer Rechnung verlangen kann, nur unzureichend um. Verzichtet der Kunde im Voraus auf Einwendungen gegen Rechnungsforderungen, dann ist die Aufbewahrung seiner Verbindungsdaten auch bis zum Versand einer Rechnung nicht erforderlich. Es genügt vielmehr, das angefallene Entgelt sofort nach Beendigung eines Nutzungsvorgangs zu ermitteln und die Verbindungsdaten sodann zu löschen.

Sinnvoll erscheint auch eine Erweiterung der Wahlmöglichkeiten von Kunden. Eine datenschutzfreundliche Regelung bestünde etwa darin, den Kunden die Dauer der Speicherung wählen zu lassen (z.B. zehn Tage nach Rechnungsversand, einen Monat nach Rechnungsversand, drei Monate nach Rechnungsversand oder genereller Verzicht auf Speicherung). Eine weitere Möglichkeit, das Spannungsverhältnis zwischen dem zivilrechtlichen Nachweisinteresse und dem Grundsatz der Datensparsamkeit zu lockern, besteht darin, den Kunden eine Schwelle vorzusehen zu lassen, bei deren Überschreitung eine grundsätzlich nicht gewünschte Speicherung von Verkehrsdaten einsetzt, z.B. ab einem Entgeltvolumen von mehr als 100 Euro oder ab einem doppelt so hohen Entgeltvolumen wie im Vormonat. Auch die Speicherung der kompletten Zielrufnummer ist zur Berechnung des Entgelts nicht erforderlich, so dass man es dem Kunden überlassen sollte, ob er diese Speicherung wünscht oder nicht. Soweit der Kun-

[32] LINX, User Privacy (I), Punkt 7.3 für Internet-Access-Provider.

[33] Vgl. DSB-Konferenz, Vorratsspeicherung (I).

de nicht aus freiem Willen eine Speicherung seiner Daten zu Nachweiszwecken verlangt, ist diese nicht als erforderlich anzusehen.

Entsprechend dem Rechtsgedanken der strafprozessualen Belehrungspflichten (etwa §§ 52 Abs. 3, 55 Abs. 2, 57 S. 2, 63, 115 Abs. 4, 115a Abs. 3 S. 2, 117 Abs. 4 S. 2, 136 Abs. 1, 171 S. 2, 172 Abs. 2 S. 2 StPO) sollte der Kunde bei seiner Wahl der Speicherdauer nicht nur darüber aufzuklären sein, dass er die Beweislast trägt, wenn er auf die Aufbewahrung seiner Verbindungsdaten verzichtet[34]. Er sollte auch darüber aufzuklären sein, dass er seine Daten dem Zugriff der gesetzlich ermächtigten Behörden aussetzt, wenn er eine Aufbewahrung wünscht.

Schließlich darf nicht vergessen werden, dass der Kunde mit seiner Wahl zugleich über die Daten seiner Kommunikationspartner verfügt. An einem Kommunikationsvorgang sind notwendig immer mindestens zwei Stellen beteiligt, so dass die Abrechnungsdaten einer Person Rückschlüsse auch auf ihre Kommunikationspartner zulassen[35]. Auch dies spricht für eine restriktive Speicherpraxis. Am effektivsten wäre es insoweit, es dem Kommunikationspartner zu ermöglichen, die Speicherung seiner Kennung zu unterbinden[36]. Ebenso wie bei Beratungseinrichtungen (vgl. § 99 Abs. 2 TKG) muss in solchen Fällen das Interesse des Kunden an der Überprüfung von Entgeltforderungen zurücktreten. Dies ist jedenfalls dann gerechtfertigt, wenn die gewählte Rufnummer nicht mit besonderen Entgelten verbunden ist.

§ 97 Abs. 3 S. 3 TKG ist somit als Eingriff in Art. 10 GG anzusehen, weil er Telekommunikationsunternehmen das Recht einräumt, Verkehrsdaten länger als für ihre Zwecke erforderlich speichern zu dürfen, und den staatlichen Behörden damit auch den Zugriff auf diese Daten ermöglicht. Das Gleiche gilt für § 97 Abs. 4 S. 1 Nr. 2 TKG.

Eine quasi unbegrenzte Ermächtigung zur Vorratsspeicherung von Verkehrsdaten sieht § 100 Abs. 1 und 3 TKG vor. Die Norm erlaubt die Erhebung und Verwendung von Verkehrsdaten zur Beseitigung technischer Störungen sowie zur Bekämpfung des Missbrauchs von Telekommunikationsnetzen. Im Unterschied zur Vorgängervorschrift des § 9 TDSV wird eine Datenspeicherung zu diesen Zwecken nicht mehr nur "im Einzelfall" für zulässig erklärt. Aus dieser Änderung

[34] Vgl. LG Memmingen, MMR 2002, 403 (403) m.w.N.
[35] Rieß, DuD 1996, 328 (329).
[36] Rieß, DuD 1996, 328 (330).

ist zu schließen, dass eine Vorhaltung von Verkehrsdaten generell und ohne zeitliche Begrenzung zulässig sein soll, um eine eventuell erforderliche Störungsbeseitigung oder Missbrauchsbekämpfung zu ermöglichen. Dass eine Datenspeicherung nach § 100 TKG nur im Rahmen des Erforderlichen zulässig sein soll, bedeutet keine Einschränkung, da sich nie ausschließen lässt, dass ein Datum einmal zu den dort genannten Zwecken gebraucht werden könnte. Das Gleiche gilt für die Bestimmung, wonach eine Datenspeicherung zur Missbrauchsbekämpfung nur "bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte" zulässig sein soll. Dass Telekommunikationsnetze missbraucht werden, liegt auf der Hand. Hierfür werden sich stets auch tatsächliche Anhaltspunkte finden und dokumentieren lassen. § 100 Abs. 1 und 3 TKG stellt daher letztlich ein umfassendes Vorratsspeicherungsrecht für Telekommunikationsunternehmen dar, das aus den genannten Gründen einen Eingriff in Art. 10 GG darstellt.

Während das Fernmeldegeheimnis insoweit nicht einschlägig ist, könnte man unter dem Aspekt der Art. 2 Abs. 1, 1 Abs. 1 GG daran denken, die für Tele- und Mediendienst-Nutzungsdaten geltende sechsmonatige Aufbewahrungsfrist (§§ 6 Abs. 7 S. 1 TDDSG, 19 Abs. 8 S. 1 MDStV) ebenfalls als Grundrechtseingriff anzusehen. Diese sechsmonatige Aufbewahrungsfrist gilt nur für Abrechnungsdaten und nur, wenn der Nutzer eines entgeltpflichtigen Tele- oder Mediendienstes einen Nachweis über die einzelnen Nutzungsvorgänge besonders verlangt (§§ 6 Abs. 7 S. 1 TDDSG, 19 Abs. 8 S. 1 MDStV). Auch hier rechtfertigt die Klärung von Entgeltstreitigkeiten eine Speicherung von Abrechnungsdaten nur, bis der Kunde den Einzelnachweis erhalten hat oder, falls kein Einzelnachweis verlangt wird, wenn der Dienst ungewöhnlich intensiv in Anspruch genommen wird. Bei der Frage, ob die Sechsmonatsfrist daher einen Grundrechtseingriff darstellt, ist allerdings zu beachten, dass der Auskunftsanspruch staatlicher Behörden nach der gegenwärtigen Rechtslage auf Telekommunikations-Verbindungsdaten beschränkt ist. Anbieter von Tele- und Mediendiensten sind zur Auskunfterteilung über von ihnen gespeicherte Tele- und Mediendienst-Nutzungsdaten demgegenüber nicht verpflichtet, sondern nur berechtigt (§§ 28 Abs. 3 Nr. 2 BDSG, 6 Abs. 5 S. 5 TDDSG, 19 Abs. 6 S. 5 MDStV für Zwecke der Strafverfolgung und §§ 8 Abs. 8 BVerfSchG, 10 Abs. 3 MAD-G, 8 Abs. 3a BND-G für nachrichtendienstliche Zwecke). Dass im Fall einer Anfrage durch eine Eingriffsbehörde von diesem Auskunftsrecht vielfach Gebrauch gemacht wird, ist indes anzunehmen, so dass auch in Bezug auf gespeicherte Nutzungsdaten stets die latente Gefahr einer staatlichen Kenntnisnahme ohne Einverständnis der Betroffenen besteht. Aus diesem Grund ist ein Eingriff in das Recht auf informationelle Selbstbestimmung bereits darin zu sehen, dass der Staat An-

> bieter von Tele- und Mediendiensten zu einer Aufbewahrung personenbezogener Daten über die erforderliche Dauer hinaus ermächtigt.

Die von § 100 TKG gestattete Datenspeicherung und -verarbeitung geht weit über das sachlich erforderliche Maß hinaus. Im Vergleich zu § 9 TDSV 2000 und auch im Vergleich zu § 100 Abs. 4 TKG verzichtet § 100 Abs. 1 und 3 TKG auf das Merkmal "im Einzelfall" und erlaubt damit letztlich die vorsorgliche und zeitlich unbegrenzte Speicherung sämtlicher Bestands- und Verkehrsdaten unter Berufung auf die Störungs- oder Missbrauchsbekämpfung (siehe im Einzelnen Breyer, RDV 2004, 147 [147 f.]). Es lässt sich nämlich nie ganz ausschließen, dass ein Verkehrsdatum einmal erforderlich sein könnte, um die rechtswidrige Inanspruchnahme von Telekommunikationsdiensten zu unterbinden oder Störungen zu beseitigen.

Die relevanten Ausführungen bei Breyer, RDV 2004, 147 [147 f.] lauten im Einzelnen wie folgt:

> Der neue § 100 TKG bringt eine problematische Ausweitung der Datenspeicherungsrechte von TK-Unternehmen mit sich und stellt aus Sicht der Bürgerrechte wohl die wichtigste Änderung des Telekommunikationsdatenschutzrechts im Zuge der TKG-Novelle dar. Bisher durften Verkehrsdaten im Grundsatz nur insoweit gespeichert werden, wie es zur Abrechnung der genutzten Dienste erforderlich war (§ 89 Abs. 2 Nr. 1 Buchst. c TKG a.F., § 7 TDSV). Die Speicherung personenbezogener Daten für Zwecke der Störungs- oder Missbrauchsbekämpfung war nur "im Einzelfall" zulässig (§ 9 TDSV). Die Regelungen der TDSV wurden nunmehr weitgehend in das neue TKG übernommen. Im Vergleich zu § 9 TDSV verzichtet § 100 TKG jedoch auf das Merkmal "im Einzelfall" und erlaubt damit letztlich die vorsorgliche und zeitlich unbegrenzte Speicherung sämtlicher Telekommunikations-Verkehrsdaten unter Berufung auf die Störungs- oder Missbrauchsbekämpfung. Es lässt sich nämlich nie ganz ausschließen, dass ein Verkehrsdatum einmal erforderlich sein könnte, um die rechtswidrige Inanspruchnahme von Telekommunikationsdiensten zu unterbinden oder Störungen zu beseitigen. Jedes Datum ist hierzu potenziell geeignet. Deswegen wird sich auch das in § 100 TKG vorausgesetzte Merkmal der Erforderlichkeit der Datenverarbeitung zu den genannten Zwecken stets begründen lassen. Keine nennenswerte Einschränkung liegt auch in der Bestimmung, wonach eine Datenspeicherung zur Missbrauchsbekämpfung nur "bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte" zulässig sein soll (§ 100 Abs. 3 TKG). Dass Telekommunikationsnetze teilweise missbraucht werden, liegt auf der Hand. Hierfür werden sich stets auch tatsächliche Anhaltspunkte finden und dokumentieren lassen. Entscheidend ist, dass das Gesetz keine einzelfallbezogenen Anhaltspunkte verlangt und nicht voraussetzt,

dass der Diensteanbieter von der "rechtswidrigen Inanspruchnahme" der Telekommunikationsnetze selbst betroffen ist.

In der Praxis berufen sich TK-Unternehmen tatsächlich auf Erfordernisse der Störungs- und Missbrauchsbekämpfung, um die Speicherung höchst sensibler personenbezogener Daten auf Vorrat zu rechtfertigen, obwohl diese für Abrechnungszwecke nicht erforderlich sind und auch zu sonstigen Zwecken nur in den seltensten Ausnahmefällen benötigt werden. Dies hat sich im Fall des Internet-Access-Providers T-Online gezeigt[37]. Dieses Unternehmen speichert die IP-Adressen, die seinen Kunden für die Internetnutzung zugewiesen werden, sechs Monate lang auf Vorrat und ermöglicht es damit ohne jeden Verdacht, das Nutzungsverhalten sämtlicher Kunden im Nachhinein nachzuvollziehen. Ausweislich der Begründung des Regierungsentwurfs[38] soll § 100 TKG genau diese Praxis legalisieren und ausweiten: "Zur Verhinderung von Missbrauch und zur Datensicherheit können hiervon auch IP-Adressen erfasst sein [...]". Dabei haben gerade Berechnungen von T-Online ergeben, dass nur 0,0004% der insgesamt dort anfallenden Verkehrsdaten später von Strafverfolgungsbehörden angefordert werden[39]. Die Chance, dass ein Verkehrsdatum zur Missbrauchsbekämpfung benötigt wird, beträgt danach lediglich 1:250.000.

Ebenso wie IP-Adressen könnten TK-Unternehmen nach dem neuen TKG auch sämtliche von ihren Kunden gewählten Telefonnummern auf beliebige Zeit hinaus speichern. Auch diese Daten können zur Aufdeckung der rechtswidrigen Inanspruchnahme von Telekommunikationsdiensten oder zur Störungsbeseitigung einmal von Nutzen sein. Wozu Gesetze wie § 100 TKG führen, zeigt das Beispiel der USA, wo einige TK-Unternehmen seit ihrer Gründung noch keine Verkehrsdaten gelöscht haben, diese also auf unbegrenzte Zeit speichern. Eine solche Vorratsdatenspeicherung birgt höchste Datensicherheits- und Missbrauchsrisiken.

Die Beseitigung von Störungen ist zwar zur ordnungsgemäßen Bereitstellung von Telekommunikationsdiensten erforderlich, wobei Störungen auch durch vorsätzliches Verhalten Dritter herbei geführt werden können. Zur Beseitigung von Störungen ist die Speicherung personenbezogener Daten aber – wenn überhaupt – allenfalls im Einzelfall erforderlich, wenn nämlich eine konkrete Störung vorliegt, und nicht generell.

Die "Bekämpfung" von "Missbrauch" ist zur Bereitstellung von Telekommunikationsdiensten nicht erforderlich, soweit der "Missbrauch" nicht gerade die Bereitstellung von Tele-

---

[37] Hierzu ausführlich Jonas Breyer, DuD 2003, 491 (491 ff.).

[38] BT-Drs. 15/2316, 122, im Internet abrufbar unter www.bmwa.bund.de/Redaktion/Inhalte/Downloads/...

[39] Uhe/Herrmann, Überwachung im Internet, http://ig.cs.tu-berlin.de/

kommunikationsdiensten behindert (z.B. "Hackerangriffe"; siehe im Einzelnen Breyer, RDV 2004, 147 [148]).

Die relevanten Ausführungen bei Breyer, RDV 2004, 147 [148] lauten im Einzelnen hierzu wie folgt:

> Umgekehrt hätte der Gesetzgeber – auch gegenüber der bisherigen Rechtslage – Anlass gehabt, in § 100 Abs. 3 TKG einschränkend klarzustellen, dass Telekommunikationsunternehmen keine Strafverfolgungsbehörden sind. Ohne richterliche Anordnung dürfen sie auch bei Vorliegen tatsächlicher Anhaltspunkte im Einzelfall nicht auf eigene Faust in das Fernmeldegeheimnis eingreifen, um vermeintliche "rechtswidrige Inanspruchnahmen der Telekommunikationsnetze und -dienste" aufzudecken, zumal sie für derartiges Verhalten ihrer Kunden nicht haften. Eine Ausnahme ist allenfalls für Leistungserschleichungen und Hackerangriffen gerechtfertigt, von denen das jeweilige TK-Unternehmen selbst betroffen ist. In anderen Fällen haben TK-Unternehmen – wie jeder andere Bürger auch – die Strafverfolgungsbehörden einzuschalten. Das Fernmeldegeheimnis muss Vorrang vor rechtsstaatlich bedenklichen Überwachungsambitionen von TK-Unternehmen haben.

Eine Auslegung des § 100 Abs. 1 und 3 TKG dahin gehend, dass die Speicherung von Daten nur im Einzelfall gestattet sei, würde dem Willen des Gesetzgebers widersprechen, der das Merkmal "im Einzelfall" im Vergleich zu § 9 TDSV 2000 und zu § 100 Abs. 4 TKG ausdrücklich aufgegeben hat. Eine derartige Auslegung stünde auch mit dem Gebot der Normenklarheit nicht in Einklang.

3.1.1.3 Rechtfertigung

Art. 10 Abs. 2 S. 1 GG bestimmt: "Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden." Bereits aus dieser Bestimmung ergibt sich, dass das Fernmeldegeheimnis nicht generell "durch Gesetz" eingeschränkt werden darf, sondern dass Beschränkungen des Fernmeldegeheimnisses nur "auf Grund eines Gesetzes" im Einzelfall "angeordnet" werden dürfen. § 100 TKG ist von dem Gesetzesvorbehalt des Art. 10 Abs. 2 S. 1 GG nicht gedeckt, weil § 100 TKG das Fernmeldegeheimnis generell einschränkt und nicht nur Beschränkungen im Einzelfall zulässt.

Daneben ist § 100 TKG auch deswegen verfassungswidrig, weil § 100 TKG das eingeschränkte Grundrecht (das Fernmeldegeheimnis) nicht unter Angabe des Artikels (Art. 10 Abs. 1 GG) nennt, wie es Art. 19 Abs. 1 S. 2 GG vorschreibt.

Darüber hinaus ist § 100 TKG auch wegen Verstoßes gegen das Verhältnismäßigkeitsgebot verfassungswidrig. Die von § 100 TKG legalisierte generelle und systematische Speicherung von Bestands- und Verkehrsdaten ist nicht durch überwiegende Allgemeininteressen gerechtfertigt (vgl. zu diesem Kriterium BVerfGE 65, 1 [44, 46]). Stattdessen steht ihr möglicher Nutzen klar außer Verhältnis zu ihren negativen Auswirkungen auf die Grund-

rechtsträger. Zur Begründung wird auf die Ausführungen bei Breyer, Vorratsspeicherung (2005)[40], Seiten 133-261 verwiesen, wobei die zentralen Argumente die folgenden sind:

- Eine systematische Speicherung von Bestands- und Verkehrsdaten ist kaum geeignet, Allgemeininteressen zu fördern. Die Bekämpfung ernsthaften Missbrauchs und ernsthafter Straftaten wird nicht erleichtert, weil ernsthafte Kriminelle Telekommunikationsdienste anonym oder unter falschem Namen nutzen. Letzteres wird dadurch begünstigt, dass das TKG keinerlei Überprüfung der Angaben von Neukunden hinsichtlich ihrer persönlichen Daten vorschreibt.
- Überdies lässt eine intensivierte Strafverfolgung ohnehin keinen verbesserten Rechtsgüterschutz erwarten.
- Demgegenüber ist eine systematische Speicherung von Bestands- und Verkehrsdaten äußerst eingriffsintensiv, weil sie es ermöglicht, das Telekommunikationsverhalten (bei Mobiltelefonen auch die Bewegungen) von Bürgern jederzeit nachzuvollziehen.
- Hiervon geht eine äußerst abschreckende Wirkung auf die freie Kommunikation, Bewegung und sonstige Handlungsfreiheit der Bürger aus, welche die unbefangene Mitwirkung der Bürger an der demokratischen Willensbildung beeinträchtigt (z.B. durch staatskritische Personen).
- Dieser "Chilling Effect" beruht auf der u.a. durch § 100 TKG geschaffenen Möglichkeit der befugten oder unbefugten Kenntnisnahme von Bestands- und Verkehrsdaten durch staatliche Stellen (vgl. z.B. § 113 TKG und § 100g StPO) und der Gefahr der unbefugten Kenntnisnahme dieser Daten durch Dritte.

Die relevanten Ausführungen bei Breyer, Vorratsspeicherung (2005)[41], Seiten 133-261 sind im Anhang wiedergegeben.

3.1.2. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Soweit der Schutzbereich des Fernmeldegeheimnisses in Bezug auf Bestandsdaten nicht für einschlägig gehalten wird, ist jedenfalls das Grundrecht auf informationelle Selbstbestimmung einschlägig, weil Bestandsdaten personenbezogene Daten darstellen. In diesem Fall gelten die obigen Ausführungen zu Art. 10 GG , Seiten 13 bis 26, mit Ausnahme der Ausführungen zum Gesetzesvorbehalt und zum Zitiergebot – entsprechend unter dem Aspekt des Rechts auf informationelle Selbstbestimmung.

[40] Breyer, (Fn. 8).
[41] Breyer, (Fn. 8).

3.1.3 Art. 3 Abs. 1 GG

3.1.3.1 Ungleichbehandlung von wesentlich Gleichem

Die Kunden von Telekommunikationsunternehmen, deren Daten nach § 100 TKG systematisch gespeichert werden dürfen, werden benachteiligt gegenüber Kunden von anderen Kommunikationsmittlern (z.B. Briefbeförderungsunternehmen) und überhaupt anderen Unternehmen, die Daten speichern, die für die Strafverfolgung und Gefahrenabwehr nützlich sein können (z.B. Verkehrsunternehmen, Versorgungsunternehmen). Hierin liegt eine Ungleichbehandlung von wesentlich Gleichem, weil sich beide Fallgruppen einem gemeinsamen Oberbegriff zuordnen lassen.

Weiterhin liegt eine Benachteiligung vor gegenüber Personen, die unmittelbar, also ohne Einschaltung eines Kommunikationsmittlers, miteinander kommunizieren. Auch dieser Sachverhalt ist mit der Telekommunikationsnutzung vergleichbar, weil in beiden Fällen kommuniziert wird.

3.1.3.2 Rechtfertigung

Wegen der hohen Eingriffsintensität des § 100 TKG (siehe Seiten 13 bis 27) und weil viele Personen zur Nutzung von Telekommunikationsnetzen gezwungen sind, kann nicht jeder sachliche Grund zur Rechtfertigung der genannten Ungleichbehandlungen genügen. Erforderlich ist vielmehr ein sachlicher Grund von solcher Art und solchem Gewicht, dass er die Intensität der Ungleichbehandlung aufwiegt (vgl. im Einzelnen Breyer, Vorratsspeicherung (2005)[42], Seiten 315-331). Ein sachlicher Grund von solcher Art und solchem Gewicht, dass er die Benachteiligung von Telekommunikationsnutzern rechtfertigt, ist nicht ersichtlich (vgl. im Einzelnen Breyer, Vorratsspeicherung (2005)[43], Seiten 315-331):

Dass der Gesetzgeber gerade Telekommunikationsunternehmen die einzelfallunabhängige Speicherung personenbezogener Daten zur Störungs- und Missbrauchsbekämpfung gestattet, ist darauf zurückzuführen, dass staatliche Stellen auf diese Weise den vielfach geforderten (vgl. etwa BR-Drs. 275/02 vom 31.05.2002 und BR-Drs. 755/03 vom 19.12.2003) generellen Zugriff auf das Kommunikationsverhalten der Bevölkerung erhalten. Vorschriften wie die §§ 100g, 100h StPO erlauben staatlichen Stellen nämlich den Zugriff auf Datendepots, die in Übereinstimmung mit § 100 TKG geschaffen werden.

Dass der Gesetzgeber gerade Telekommunikationsunternehmen die einzelfallunabhängige Speicherung personenbezogener Daten zur Störungs- und Missbrauchsbekämpfung gestattet, lässt sich nur damit erklären, dass in anderen Bereichen die systematische Speicherung von Daten über das Verhalten der Bürger entweder nicht (z.B. bei unmittelbarer Kommunikation) oder nur mit weit höherem Aufwand (z.B. bei Briefbeförderungsunternehmen) durchführbar wäre. Alleine die Tatsache, dass sich das Verhalten der Bürger auf dem Gebiet der Telekommunikation leicht und mit begrenztem Aufwand aufzeichnen und überwachen lässt, kann zur Benachteiligung der Telekommunikationsnutzung jedoch nicht genügen, zumindest nicht in Anbetracht der Eingriffsintensität des § 100 TKG (vgl. im Einzelnen Breyer, Vorratsspeicherung (2005)[44], Seiten 315-331).

---

[42] Breyer, (Fn. 8).

[43] Breyer, (Fn. 8).

[44] Breyer, (Fn. 8).

Einen sachlichen Grund für die Ungleichbehandlung würde es etwa darstellen, wenn Telekommunikations-Bestands- und Verkehrsdaten für den Schutz von Rechtsgütern nützlicher wären als die bei den Vergleichsgruppen anfallenden Daten. Hiervon ist aber weder der Gesetzgeber ausgegangen noch ist dies ersichtlich; dahin gehende Erkenntnisse liegen nicht vor. Dass Telekommunikationsnetze missbraucht werden, liegt zwar auf der Hand. Dies rechtfertigt aber keine Benachteiligung der Telekommunikation, denn auch die Leistungen von Briefbeförderungsunternehmen, Verkehrsunternehmen und anderen Unternehmen sowie die Möglichkeiten unmittelbarer Kommunikation werden missbraucht.

Die relevanten Ausführungen bei Breyer, Vorratsspeicherung (2005)[45], Seiten 315-331 lauten im Einzelnen hierzu wie folgt:

Der allgemeine Gleichheitssatz (Artikel 3 Abs. 1 GG)

a) Ungleichbehandlung des Informationsaustausches über Telekommunikationsnetze gegenüber dem räumlich-unmittelbaren Informationsaustausch

Nicht selten wird gegen eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten eingewandt, dass eine solche Maßnahme Telekommunikation einem ungleich höheren Überwachungsdruck aussetze als er bei vergleichbarem Verhalten in der realen Welt existiere[46]. Wenn außerhalb des Telekommunikationsbereiches unbeobachtet gehandelt werden könne, so dürften im Bereich der Telekommunikationsnetze keine größeren Überwachungsmöglichkeiten vorgesehen werden[47]. In eine juristische Argumentation gekleidet handelt es sich bei dieser Überlegung um ein Gleichbehandlungsproblem, das im Rahmen des Art. 3 Abs. 1 GG verfassungsrechtlich relevant ist. Zu diskutieren ist zunächst die zwischenmenschliche Individualkommunikation.

aa) Individualkommunikation

(1) Eingriff in den Schutzbereich des Art. 3 Abs. 1 GG

---

[45] Breyer, (Fn. 8).

[46] DSB-Konferenz, Datenschutzbeauftragte des Bundes und der Länder: Entschließung zur systematischen verdachtslosen Datenspeicherung in der Telekommunikation und im Internet der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25.10.2002, BT-Drs. 15/888, 199; ULD-SH, Sichere Informationsgesellschaft (I), Punkt 6.

[47] Artikel-29-Gruppe der EU, Anonymität, 7; The President's Working Group on Unlawful Conduct on the Internet (USA), The Electronic Frontier (I).

Art. 3 Abs. 1 GG gewährleistet, dass der Staat Sachverhalte, die im Wesentlichen gleich sind, auch gleich behandelt[48]. Diese Pflicht trifft nach Art. 1 Abs. 3 GG auch den Gesetzgeber[49]. Im Wesentlichen gleich sind zwei Sachverhalte dann, wenn sie sich einem gemeinsamen Oberbegriff zuordnen lassen[50]. Der Oberbegriff muss die Sachverhalte vollständig erfassen[51]. Nicht erforderlich ist dagegen, dass der Oberbegriff ausschließlich die beiden zu vergleichenden Sachverhalte umfasst. Die Vergleichbarkeit zweier Sachverhalte, die sich einem gemeinsamen Oberbegriff zuordnen lassen, kann allenfalls dann verneint werden, wenn die Sachverhalte unterschiedlichen rechtlichen Ordnungsbereichen angehören und in anderen systematischen und sozialgeschichtlichen Zusammenhängen stehen[52].

Eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten führt zur unterschiedlichen Behandlung von Telekommunikation einerseits und räumlich-unmittelbarer Kommunikation andererseits, weil Kommunikationsvorgänge nur im ersten Fall ihren Umständen nach festgehalten würden. Beide Sachverhalte unterscheiden sich dadurch, dass ein Kommunikationsvorgang im einen Fall über eine räumliche Distanz hinweg und unter Nutzung von Telekommunikationstechnik stattfindet, im anderen Fall in räumlicher Gegenwart der Beteiligten. Dieser Unterschied ändert jedoch nichts daran, dass es sich in beiden Fällen um menschliche Kommunikation handelt. Gemeinsamer Oberbegriff ist daher die menschliche Kommunikation. Die Telekommunikation und die räumlich-unmittelbare Kommunikation gehören auch nicht unterschiedlichen rechtlichen Ordnungsbereichen an, so dass sie vergleichbar sind. Der Schutzbereich des Art. 3 Abs. 1 GG ist durch eine generelle Vorratsspeicherung allein von Telekommunikations-Verkehrsdaten demnach betroffen.

Ein Eingriff in Art. 3 Abs. 1 GG liegt vor, wenn eine Person durch eine Ungleichbehandlung von wesentlich Gleichem nachteilig betroffen ist[53]. Dies ist bei einer Vorratsspeicherung von Telekommunikations-Verkehrsdaten bei denjenigen Menschen der Fall, die sich des Mittels der Telekommunikation bedienen und deren Kommuni-

48 St. Rspr. seit BVerfGE 1, 14 (52).
49 BVerfGE 1, 14 (52).
50 P/S, Rn. 431 ff.
51 P/S, Rn. 435.
52 J/P6-Jarass, Art. 3, Rn. 4 m.w.N.
53 Vgl. BVerfGE 67, 239 (244).

kation dabei durchgängig registriert wird, während dies im Bereich der räumlich-unmittelbaren Kommunikation nicht geschieht. Damit stellt eine Vorratsspeicherung von Telekommunikationsdaten einen rechtfertigungsbedürftigen Eingriff in das Grundrecht der Telekommunikationsnutzer aus Art. 3 Abs. 1 GG dar.

(2) Rechtfertigungsmaßstab

Unter welchen Umständen eine Ungleichbehandlung verfassungsrechtlich gerechtfertigt ist, hängt nach der Rechtsprechung des Bundesverfassungsgerichts von dem jeweiligen Regelungsgegenstand und Differenzierungsmerkmal ab[54]. In manchen Fällen lässt das Bundesverfassungsgericht jeden sachlichen Grund als Rechtfertigung genügen[55]. Für eine bloße Willkürprüfung spricht es etwa, wenn eine Ungleichbehandlung von Sachverhalten ohne engen menschlichen Bezug vorliegt[56], wenn der Bereich der gewährenden Staatstätigkeit betroffen ist[57], es sich um wirtschaftsordnende Maßnahmen handelt[58] oder wenn eine Differenzierung bereits im Grundgesetz angelegt ist[59].

Dasselbe soll im Bereich vielgestaltiger Sachverhalte gelten, die im Einzelnen noch nicht bekannt sind[60]. Richtigerweise handelt es sich hierbei allerdings um eine Erscheinungsform des allgemeinen Problems der Behandlung unbekannter Tatsachen im Rahmen der verfassungsrechtlichen Prüfung, das differenziert zu lösen ist. Tatsächliche Unsicherheiten rechtfertigen einen Einschätzungsspielraum des Gesetzgebers nur hinsichtlich der Einschätzung der unbekannten Tatsachen. Auswirkungen auf den generellen Kontrollmaßstab können sie dagegen nicht haben[61].

In anderen Fallgruppen wendet das Bundesverfassungsgericht einen strengeren Prüfungsmaßstab an, dem zufolge zu untersuchen ist, ob ein sachlicher Grund von solcher Art und solchem Gewicht vorliegt, dass er die Ungleichbehandlung recht-

54 BVerfGE 88, 87 (96); BVerfGE 95, 267 (316).
55 BVerfGE 88, 87 (96); BVerfGE 95, 267 (316).
56 Etwa BVerfGE 38, 225 (229).
57 Etwa BVerfGE 49, 280 (282).
58 Etwa BVerfGE 18, 315 (331).
59 J/P[6]-Jarass, Art. 3, Rn. 23; vgl. etwa BVerfGE 52, 303 (346) für Beamte.
60 BVerfGE 33, 171 (189 f.); BVerfGE 78, 249 (288).
61 Chryssogonos, Verfassungsgerichtsbarkeit und Gesetzgebung, 189.

fertigt[62]. Im Kern handelt es sich um eine Prüfung der Verhältnismäßigkeit[63]. Für die Vornahme einer Verhältnismäßigkeitsprüfung spricht es etwa, wenn die diskriminierende Maßnahme in ein Freiheitsgrundrecht eingreift[64] oder wenn die Diskriminierten keinen Einfluss auf ihre Behandlung nehmen können[65]. Insgesamt wird die Verhältnismäßigkeit insbesondere in denjenigen Fällen zu prüfen sein, in denen von einer Ungleichbehandlung erhebliche Belastungen für die Betroffenen ausgehen.

Misst man eine generelle Verkehrsdatenspeicherung an den genannten Kriterien, so fragt sich zunächst, ob diese lediglich eine Ungleichbehandlung von Sachverhalten ohne engen menschlichen Bezug darstellt, was für eine bloße Willkürprüfung sprechen würde. Für diese Annahme könnte man anführen, dass die meisten Menschen sowohl Telekommunikation einsetzen wie auch räumlich-unmittelbar kommunizieren. Ein strikter Personenbezug in dem Sinn, dass ein Sachverhalt ausschließlich eine bestimmte Gruppe von Menschen und der andere Sachverhalt ausschließlich eine andere Menschengruppe betrifft, liegt nicht vor. Fraglich ist aber, ob dies Voraussetzung für die Annahme eines „engen menschlichen Bezugs" ist oder ob es nicht auch genügt, dass bestimmte Personengruppen von der Ungleichbehandlung typischerweise stärker betroffen sind als andere. Von einer Vorratsspeicherung von Telekommunikationsdaten sind etwa Berufstätige und Personen, die weit von ihrer Familie entfernt leben, stärker betroffen als andere Personengruppen, die nicht im gleichen Maße auf Telekommunikation angewiesen sind. Überhaupt haben die von einer Vorratsspeicherung Betroffenen in vielen Fällen keine Ausweichmöglichkeit. Dass in der heutigen Informationsgesellschaft ein Leben ohne Telekommunikationsnetze kaum noch denkbar ist, beruht keineswegs nur auf Bequemlichkeit und Komfort. Die moderne Arbeitsgesellschaft beispielsweise zwingt zu immer mehr räumlicher Mobilität und bringt vielfach unfreiwillige und kaum überwindbare Trennungen selbst von sich nahe stehenden Personen mit sich. Auch bestimmte Berufsgruppen, etwa Journalisten, sind in hohem Maße auf die Nutzung von Telekommunikationsnetzen angewiesen. Unternehmen, die ein auf den Fernabsatz ausgerichtetes Vertriebs- oder Dienstleistungssystem anbieten, werden oftmals zur Nutzung der Telekommunikationsnetze gezwungen sein, weil nur diese Ni-

62 Vgl. allgemein BVerfGE 87, 234 (255); BVerfGE 91, 389 (401); BVerfGE 95, 267 (317).

63 Vgl. nur BVerfGE 82, 126 (146) und J/P[7]-Jarass, Art. 3, Rn. 27.

64 Für das allgemeine Persönlichkeitsrecht BVerfGE 60, 123 (134); BVerfGE 88, 87 (97).

65 Vgl. BVerfGE 88, 87 (96); BVerfGE 97, 169 (181).

sche ihr ökonomisches Überleben sichert. Auch Kunden können auf die Leistungen solcher Unternehmen angewiesen sein, etwa wenn jemand spezielle Waren oder Dienstleistungen benötigt, die in seinem räumlichen Umkreis nicht angeboten werden.

Festzuhalten ist somit, dass vielen Menschen in weiten Bereichen keine zumutbare Alternative zur Telekommunikation zur Verfügung steht und dass dies zumeist nicht auf einer freien Willensentscheidung beruht. Dies spricht nach den Kriterien des Bundesverfassungsgerichts für die Vornahme einer Verhältnismäßigkeitsprüfung. Zudem stellt eine Vorratsspeicherung von Telekommunikationsdaten einen schwerwiegenden Eingriff in verschiedene Freiheitsgrundrechte dar (Fernmeldegeheimnis oder Recht auf informationelle Selbstbestimmung, Berufsfreiheit, Meinungsfreiheit, Informationsfreiheit und Rundfunkfreiheit)[66]. Unabhängig davon, ob man einen engen menschlichen Bezug der Ungleichbehandlung annimmt oder nicht, überwiegen damit jedenfalls die Gesichtspunkte, die für eine Verhältnismäßigkeitsprüfung sprechen. Prüfungsmaßstab ist daher, ob ein sachlicher Grund von solcher Art und solchem Gewicht existiert, dass er es rechtfertigt, die näheren Umstände der Kommunikation über Telekommunikationsnetze generell zu erfassen, die näheren Umstände der räumlich-unmittelbaren Kommunikation dagegen nicht.

(3) Machbarkeit und Finanzierbarkeit als Rechtfertigungsgrund

Zunächst kann die höhere Praktikabilität einer Regelung einen sachlichen Grund für eine damit verbundene Ungleichbehandlung darstellen[67]. Im vorliegenden Zusammenhang liegt es auf der Hand, dass eine Erfassung der Umstände der räumlich-unmittelbaren Kommunikation nicht nur weniger praktikabel wäre als eine Vorratsspeicherung von Telekommunikationsdaten. Eine ähnlich umfassende Erfassung des Kommunikationsverhaltens der Bevölkerung wie im Telekommunikations- und Onlinebereich wäre im Bereich der unmittelbaren Kommunikation schlichtweg nicht machbar. Selbst Überwachungsapparate wie das mit unvorstellbaren personellen und finanziellen Ressourcen ausgestattete Ministerium für Staatssicherheit der

66 **Fehler! Textmarke nicht definiert.** ff.

67 BVerfGE 17, 337 (354); BVerfGE 41, 126 (288); im Einzelfall ablehnend BVerfGE 55, 159 (169); BVerfGE 60, 68 (78).

DDR konnten die unmittelbare Kommunikation in der Bevölkerung immer nur bruchstückhaft erfassen.

Auch finanzielle Vorteile einer Regelung können einen sachlichen Grund für eine damit verbundene Ungleichbehandlung bilden[68]. Eine Erfassung des räumlich-unmittelbaren Kommunikationsverhaltens der Bevölkerung würde jedenfalls an finanziellen Gesichtspunkten scheitern. Zwar sind bei der Bemessung der finanziellen Folgen einer Vorratsspeicherung von Verkehrsdaten richtigerweise auch die mittelbar damit verbundenen Kosten zu berücksichtigen, die bei den Telekommunikationsunternehmen und den Endverbrauchern anfallen[69]. Dennoch sind diese Kosten immer noch ungleich geringer als die Kosten des Aufbaus und der Unterhaltung einer Überwachungsstruktur im Bereich der unmittelbaren Kommunikation, soweit dies überhaupt möglich wäre. Somit hat das Finanzierungsargument ebenfalls eine gewisse Berechtigung.

Es fragt sich allerdings, ob Gesichtspunkte der Machbarkeit und Finanzierbarkeit in der Abwägung die schwerwiegende Ungleichbehandlung überwiegen können, die eine Vorratsspeicherung ausschließlich von Telekommunikations-Verkehrsdaten mit sich bringt. Angesichts der tief greifenden, nicht zu kompensierenden Freiheitseinbußen durch eine solche Maßnahme sowie der Tatsache, dass die Betroffenen heutzutage oftmals zu einer Nutzung von Telekommunikationsnetzen gezwungen sind, ist dies zu verneinen. Allein die Tatsache, dass sich das Verhalten der Menschen in Telekommunikationsnetzen umfassend überwachen lässt und sich die dazu erforderlichen materiellen Ressourcen in Grenzen halten, kann zur Rechtfertigung dieser massiven Ungleichbehandlung gegenüber der unmittelbaren Kommunikation nicht genügen[70].

(4) Erschwerung der staatlichen Aufgabenwahrnehmung als Rechtfertigungsgrund

---

68 BVerfGE 3, 4 (11); BVerfGE 75, 40 (72); BVerfGE 87, 1 (45); im Einzelfall ablehnend BVerfGE 61, 43 (63); BVerfGE 87, 1 (46); BVerfGE 92, 53 (69).

69 Allgemein zur Berücksichtigung von mittelbaren Kosten eines Gesetzes Scholz, ZRP 2002, 361 (361).

70 Bäumler, DuD 2001, 348 (349).

Zur Rechtfertigung einer generellen Verkehrsdatenspeicherung wird ferner angeführt, dass die besonderen Eigenschaften der Telekommunikationsnetze die Tätigkeit der Gefahrenabwehr- und Strafverfolgungsbehörden erschwerten[71]. In der Tat führt elektronische Kommunikation nicht selten dazu, dass Spuren entweder von Anfang an nicht entstehen – beispielsweise bei anonymer Telekommunikation – oder nachträglich beseitigt werden – beispielsweise durch Datenlöschung nach Begleichung der Rechnung[72]. Von staatlicher Seite wird teilweise vorgebracht, dass sich in der wirklichen Welt oftmals Zeugen oder andere Beweismittel für begangene Straftaten finden ließen. Diese Möglichkeit scheide im Bereich der Telekommunikationsnetze von vornherein und generell aus, wenn keine Telekommunikationsdaten gespeichert würden, wie es gegenwärtig bei vorausbezahlten oder pauschal berechneten Abrechnungsmodellen oder bei kostenlosen Diensten der Fall sei[73].

Dieser Argumentation ist entgegenzusetzen, dass sich auch im Bereich der räumlich-unmittelbaren Kommunikation Zeugen oder andere Beweismittel typischerweise nur für auffälliges Verhalten außerhalb der Privatsphäre der Straftäter finden lassen. Geht es um die Vorbereitung einer Straftat oder um Verhalten im Anschluss an die Tatbegehung, dann kann die Nutzung von Telekommunikationsnetzen für Straftäter zwar auch nützlich sein. Auch ohne sie lassen sich diese Aktivitäten aber konspirativ und geheim durchführen. Das Auge des Gesetzes ist offline nicht überall, so dass es keinen Grund gibt, warum dies online anders sein müsste[74].

Schon die Annahme, dass die Wahrnehmung staatlicher Aufgaben unter den besonderen Umständen der Telekommunikationsnetze leide, ist kritisch zu hinterfragen. In Fällen, in denen Telekommunikationsnetze eine ordnungsgemäße Aufgabenwahrnehmung nur erschweren (etwa durch die Erforderlichkeit qualifizierten Personals oder sonstiger Mittel wie Zeit und Geld), in denen aber auch ohne einen Zugriff auf vorratsgespeicherte Verkehrsdaten erfolgreich eingeschritten werden kann, rechtfertigt die bloße Erleichterung der Aufgabenwahrnehmung in Anbetracht der

71 Sieber, COMCRIME-Studie (I), 60.

72 NCIS Submission (I), Summary Punkt 2.1.3.

73 Tony Hutchings, UK National Hi-Tech Crime Project Team, zitiert in Kommission, Cybercrime-Anhörung (I); Kronqvist, Leiter der IT-Kriminalitätsgruppe der nationalen schwedischen Strafverfolgungsbehörde, Cybercrime-Anhörung; Graf, Jürgen (Generalbundesanwalt), zitiert bei Neumann, Andreas: Internet Service Provider im Spannungsfeld zwischen Strafverfolgung und Datenschutz, Bericht von der Veranstaltung in Bonn am 26./27.02.2002, www.artikel5.de/artikel/ecoveranstaltung2002.html; NCIS Submission (I), Summary Punkt 2.1.3.; a.A. Schmitz, MMR 2003, 214 (216): keine generell schlechtere Beweislage.

74 Artikel-29-Gruppe der EU, Anonymität, 7.

hohen Eingriffsintensität keine generelle Vorratsspeicherung[75]. In Fällen, in denen die Aufgabenwahrnehmung mangels Verkehrsdaten vereitelt wird, ist es nicht sicher, ob eine Vorratsspeicherung tatsächlich weiter geholfen hätte. Auch im Rahmen des Art. 3 Abs. 1 GG ist zu berücksichtigen, dass eine Vorratsspeicherung von Telekommunikationsdaten nur in begrenztem Maße von Nutzen ist.

Im Übrigen darf nicht außer Acht gelassen werden, dass Telekommunikationsnetze den Behörden die Wahrnehmung ihrer Aufgaben ungemein erleichtern[76]. Vor 100 Jahren hatten die Eingriffsbehörden keine Chance, verdächtige Personen so unbemerkt, kostengünstig und personalsparend zu überwachen wie heute. Im Vergleich zu den Möglichkeiten der Telekommunikationsüberwachung ist eine Überwachung von unmittelbarer Kommunikation erheblich schwerer. Was die Beweislage angeht, so werden Telekommunikations-Verkehrsdaten, wenn sie vorliegen und soweit ihr Informationsgehalt reicht, meist aussagekräftiger und zuverlässiger sein als Zeugenaussagen oder andere Beweismittel für räumlich-unmittelbare Kommunikation. Der Nutzen des staatlichen Zugriffs auf Verkehrsdaten wird zudem durch eine generelle Vorratsspeicherung unterminiert, weil dieses Verfahren Straftätern eindringlich ins Bewusstsein ruft, die Benutzung von Telekommunikationsnetzen zu meiden. Letztlich gefährdet eine Vorratsspeicherung von Telekommunikationsdaten dadurch den Erfolg der bisher bestehenden Überwachungsbefugnisse im Einzelfall.

Insgesamt ist unklar, ob die staatliche Aufgabenwahrnehmung durch die Möglichkeit der Kommunikation über Telekommunikationsnetze tatsächlich erschwert wird. Ohnehin kann richtigerweise nicht schon die abstrakte Erschwerung der staatlichen Aufgabenwahrnehmung eine Ungleichbehandlung der Telekommunikationsnutzung rechtfertigen, sondern erst erhöhte, dadurch verursachte Gefahren für konkrete Rechtsgüter. Auf dem Gebiet der Strafverfolgung stellt sich damit immer noch das Problem, dass eine gewisse Steigerung der Aufklärungsrate infolge einer generellen Verkehrsdatenspeicherung keine merkliche Senkung des Kriminalitätsniveaus und damit keinen nennenswert verbesserten Rechtsgüterschutz erwarten lässt.

---

75 Vgl. allgemein J/P[7]-Jarass, Art. 3, Rn. 16 a.E.; für die geheime Erhebung von Daten L/D[3]-Bäumler, J 37.

76 vgl. auch MDG, Entwurf für Schlussfolgerungen des Rates zur Informationstechnologie (I), 3: „Der Rat der Europäischen Union [...] stellt fest, dass die beträchtliche Zunahme der Möglichkeiten elektronischer Kommunikation dazu geführt hat, dass Daten über die Verwendung elektronischer Kommunikation heutzutage ein besonders wichtiges und hilfreiches Mittel bei der Aufklärung und Verfolgung von Straftaten, insbesondere von organisierter Kriminalität, darstellen".

(5) Erhöhtes Gefahrenpotenzial durch besondere Eigenschaften der Telekommunikation als Rechtfertigungsgrund

Zur Rechtfertigung einer Ungleichbehandlung der Telekommunikation könnte weiter vorgebracht werden, dass die Kommunikation über Telekommunikationsnetze größere Gefahren für Rechtsgüter mit sich bringe als die räumlich-unmittelbare Kommunikation. Ob dies der Fall ist, ist umstritten[77] und empirisch noch nicht untersucht worden. Für eine höhere Gefährlichkeit der Telekommunikation sprechen ihre besonderen Eigenschaften, die in bestimmten Fällen die Begehung von Straftaten begünstigen können[78]. Telekommunikationsnetze erleichtern den Austausch von Informationen und ermöglichen diesen kostengünstig, einfach, schnell, vertraulich und über weite Entfernungen – auch Ländergrenzen – hinweg.

Dass die besonderen Eigenschaften der Telekommunikation die Gefährdung von Rechtsgütern in einzelnen Fällen begünstigen, bedeutet indes nicht zwangsläufig, dass sie dies auch in höherem Maße tun als die Kommunikation in räumlicher Gegenwart der Beteiligten[79]. Bei der Untersuchung dieser Frage ist richtigerweise zu berücksichtigen, wie viele Kommunikationsvorgänge insgesamt über Telekommunikationsnetze oder räumlich-unmittelbar abgewickelt werden. Nur auf diese Weise ist feststellbar, inwieweit höhere Gefahren infolge einer Kommunikationsweise (Telekommunikation oder räumlich-unmittelbare Kommunikation) auf die Eigenart der jeweiligen Kommunikationsweise und nicht bloß auf das Maß an Nutzung der jeweiligen Kommunikationsform zurückzuführen sind. Zu vergleichen ist also das relative Maß an Rechtsgutsgefährdung. Es ist darauf abzustellen, in welchem Maß der durchschnittliche Kommunikationsvorgang Rechtsgüter gefährdet.

Dies hat unter anderem zur Folge, dass die absolut steigende Zahl der Fälle von Netzkriminalität im weiteren Sinn in Verhältnis zu setzen ist zu dem Maß, in dem Telekommunikationsnetze insgesamt genutzt werden. Die bisher vorliegenden Zahlen

---

77 Vgl. etwa Weßlau, ZStW 113 (2001), 681 (703), wonach weder Internet-Provider noch Internet-Nutzer gefahrenträchtig handelten; ebenso Bäumler, DuD 2001, 348 (349) und Werner, Befugnisse der Sicherheitsbehörden, 51 für das Telekommunikationsnetz; meist unausgesprochen a.A. sind die Vertreter der Eingriffsbehörden.

78 Sieber, COMCRIME-Studie (I), 60.

79 In diese Richtung allerdings Sieber, COMCRIME-Studie (I), 61: „computer crime and the Internet have become especially attractive for organised crime groups".

zur Computerkriminalität im engeren Sinne etwa sind in den vergangenen Jahren weit weniger stark gestiegen als die Internetnutzung insgesamt. Zu berücksichtigen ist auch, in welchem Maße es jeweils zur Gefährdung von Rechtsgütern kommt. Bisher existieren keine Statistiken oder Untersuchungen über das Ausmaß der Schäden, die durch die Inanspruchnahme von Telekommunikationsnetzen durch Straftäter entstehen. Nach Ermittlung des relativen Gefahrenpotenzials der Telekommunikationsnetze ist dieses mit der Situation im Bereich der räumlich-unmittelbaren Kommunikation zu vergleichen. Zahlen insoweit liegen bisher nicht vor. Die Behauptung, dass Telekommunikation Rechtsgüter in höherem Maße gefährdete als räumlich-unmittelbare Kommunikation, stellt aus diesem Grund lediglich eine Hypothese dar, deren Richtigkeit bisher noch nicht untersucht worden ist.

Die von der Polizeistatistik ausgewiesenen Fallzahlen der allgemeinen Kriminalität sind in den letzten Jahren ungefähr stabil geblieben, so dass sich nicht feststellen lässt, dass der Einzug der Telekommunikationsnetze in das tägliche Leben insgesamt zu mehr Straftaten geführt hat. Unter der Voraussetzung, dass die Entwicklung der Polizeistatistik der tatsächlichen Kriminalitätsentwicklung entspricht, ist dies ein Indiz für die These, dass mittels Telekommunikation begangene Straftaten ohne die Möglichkeiten der Telekommunikation mittels unmittelbarer Kommunikation begangen würden, dass die Telekommunikationsnetze also nur zu einer Kriminalitätsverlagerung geführt haben[80].

Zwar können Telekommunikationsnetze durchaus als „gefährliche Werkzeuge" oder Hilfsmittel bei der Gefährdung von Rechtsgütern eingesetzt werden. Allerdings kann prima facie und ohne nähere Untersuchungen nicht davon ausgegangen werden, dass die Telekommunikation zu größeren Schäden führt oder mit weitergehenden Gefahren verbunden ist als die unmittelbare Kommunikation. In Anbetracht der Tatsache, dass sich Telekommunikation leichter überwachen lässt, ist auch das Gegenteil denkbar. In diesem Fall aber sind weitergehende Überwachungsmaßnahmen als im Bereich der unmittelbaren Kommunikation nicht gerechtfertigt.

80 In diesem Sinne Pfitzmann, Andreas in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 52.

(6) Höherer Nutzen der Telekommunikationsüberwachung als Rechtfertigungsgrund

Weiterhin könnte eine Vorratsspeicherung allein von Telekommunikationsdaten dadurch gerechtfertigt sein, dass die Kenntnis der näheren Umstände von Telekommunikationsvorgängen typischerweise von größerem Nutzen für den Rechtsgüterschutz sein könnte als die Kenntnis der näheren Umstände von unmittelbaren Kommunikationsvorgängen. Beispielsweise lässt sich denken, dass Straftäter sensible Informationen über geplante oder abgeschlossene Straftaten öfter telefonisch austauschen könnten als im unmittelbaren Gespräch. Diese Annahme erscheint allerdings unzutreffend. Straftäter werden sich heutzutage regelmäßig des Instruments der Telekommunikationsüberwachung bewusst sein und die unmittelbare Kommunikation einem Einsatz von Telekommunikation daher wann immer möglich vorziehen. Auch sonst ist nicht ersichtlich, dass die Kenntnis der näheren Umstände von Telekommunikationsvorgängen typischerweise einen größeren Nutzen für den Rechtsgüterschutz aufweist als die Kenntnis der Umstände von unmittelbaren Kommunikationsvorgängen. Ein Rechtfertigungsgrund kann hierin daher nicht erblickt werden.

(7) Unterschiedliche Schutzwürdigkeit als Rechtfertigungsgrund

Als Rechtfertigungsgrund kommt schließlich in Betracht, dass die Umstände unmittelbarer Kommunikation schutzwürdiger sein könnten als die Umstände von Telekommunikation. Für diese These könnte angeführt werden, dass sich Menschen bei Einsatz von Telekommunikationsnetzen ihrer Kommunikation willentlich entäußern und dass sie dementsprechend mit einem höheren Maß an Überwachung rechnen müssten als im Fall unmittelbarer Kommunikation. Wie bereits gezeigt, kann die bloße Tatsache, dass sich Telekommunikation einfacher überwachen lässt, zur Rechtfertigung einer generellen Verkehrsdatenspeicherung aber nicht genügen. Ebenso wenig kann daraus eine verminderte Schutzwürdigkeit von Telekommunikation hergeleitet werden. Wenn Menschen miteinander telekommunizieren, vertrauen sie typischerweise darauf, ebenso ungestört zu sein wie im Fall unmittelbarer Kommunikation. Hinzu kommt, dass heutzutage in vielen Situationen keine Möglichkeit unmit-

telbarer Kommunikation mehr besteht. Dieser Umstand darf nicht zulasten der Betroffenen gehen.

Für eine verminderte Schutzwürdigkeit von Telekommunikation könnte weiterhin angeführt werden, dass vertrauliche Gespräche zumeist in Wohnungen geführt würden, dass Telekommunikation den Bereich einer Wohnung dagegen stets verlässt. Auch diese Tatsache scheint indes nicht geeignet, die Schutzwürdigkeit von Telekommunikation zu reduzieren. Die Funktion eines Gespräches innerhalb einer Wohnung unterscheidet sich nicht von der Funktion eines Telefongesprächs zwischen zwei Wohnungen.

Die hohe Sensibilität und Aussagekraft von Telekommunikations-Verkehrsdaten wurde bereits ausführlich dargestellt. Es sind keine Anhaltspunkte dafür ersichtlich, dass Telekommunikation typischerweise weniger sensibel ist als räumlich-unmittelbare Kommunikation. Dementsprechend kann von einer verminderten Schutzwürdigkeit von Telekommunikation nicht ausgegangen werden.

(8) Abwägung und Ergebnis

Festzuhalten ist, dass sich eine generelle Vorratsspeicherung allein von Telekommunikations-Verkehrsdaten nur dann rechtfertigen lässt, wenn der durchschnittliche Telekommunikationsvorgang Rechtsgüter in erheblich höherem Maß gefährdet als der typische räumlich-unmittelbare Kommunikationsvorgang. Als Unterfall der Gefährdung von Rechtsgütern ist es dabei anzusehen, wenn der Schutz von Rechtsgütern durch die Eingriffsbehörden vereitelt wird, weil diese keine Kenntnis von den Umständen eines Kommunikationsvorgangs haben.

Ob die Kommunikation über Telekommunikationsnetze Rechtsgüter tatsächlich in überdurchschnittlichem Maße gefährdet, ist unbekannt. Bei der Einschätzung dieser Tatsache kommt dem Gesetzgeber ein gewisser Spielraum zu, dessen Ausmaß sich nach den oben diskutierten Kriterien bestimmt. Wegen der hohen Eingriffsintensität einer generellen Verkehrsdatenspeicherung ist zu verlangen, dass der Gesetzgeber eine vertretbare Entscheidung trifft und die ihm zugänglichen Erkenntnisquellen vor der Einführung einer solchen Maßnahme ausschöpft, etwa durch Einholung einer

wissenschaftlichen Vergleichsstudie. Es liegt keine besondere Dringlichkeitssituation vor, in der von der vorherigen Analyse der maßgeblichen Tatsachen abgesehen werden könnte. Ebenso wenig verspricht die Einführung einer Vorratsspeicherung von Telekommunikationsdaten einen Erkenntnisgewinn bezüglich des Maßes an Rechtsgutsgefährdung durch Telekommunikation oder räumlich-unmittelbare Kommunikation, so dass sich eine solche Maßnahme auch nicht als notwendiges Experiment rechtfertigen lässt.

Auf der Basis des gegenwärtigen Erkenntnisstandes ist nicht ersichtlich, dass der durchschnittliche, über Telekommunikationsnetze abgewickelte Kommunikationsvorgang Rechtsgüter in höherem Maße gefährdet als der typische räumlich-unmittelbare Kommunikationsvorgang. Wie oben gezeigt, legt die leichtere Überwachbarkeit der Telekommunikation eher den umgekehrten Schluss nahe. Ohne entsprechende empirische Befunde ist die Unterstellung einer besonderen Rechtsgutsgefährdung durch menschliche Kommunikation über Telekommunikationsnetze angesichts dessen unvertretbar. Ausgehend von den derzeit vorliegenden Erkenntnissen ist die Einführung einer Vorratsspeicherung von Telekommunikationsdaten daher mit Art. 3 Abs. 1 GG unvereinbar.

bb) Massenkommunikation

Telekommunikationsnetze stellen nicht nur ein Medium für Individual- sondern auch für Massenkommunikation dar. Für das Angebot und die Nutzung von Informationen, die an eine unbestimmte Vielzahl von Personen gerichtet sind, eignet sich insbesondere das Internet. Eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten führt dazu – eine entsprechende Ausgestaltung vorausgesetzt –, dass die Nutzung telekommunikativer Informationsangebote ihren Umständen nach festgehalten wird, während die räumlich-unmittelbare Nutzung traditioneller Massenmedien (z.B. Zeitschriften, Bücher, Fernsehen) überwachungsfrei bleibt. Wegen der Frage, ob diese Ungleichbehandlung gerechtfertigt ist, kann weitgehend auf die obigen Ausführungen zur Individualkommunikation verwiesen werden.

Eine stärkere Überwachung der Massenkommunikation über Telekommunikationsnetze ist nur dann gerechtfertigt, wenn aus dieser – gemessen an der Gesamtzahl von Nutzungsvorgängen – überproportional hohe Gefahren erwachsen. Ver-

gleichsmaßstab ist das Gefahrenpotenzial von räumlich-unmittelbarer Massenkommunikation. Für ein höheres Gefahrenpotenzial der Telekommunikationsnetze könnte sprechen, dass Telekommunikationsnetze und insbesondere das Internet nicht selten zum Angebot und zur Nutzung illegaler Informationen eingesetzt werden und dass sich insbesondere das Internet hierzu besser eignet als Printmedien und andere traditionelle Massenmedien. Telekommunikationsnetze erleichtern aber andererseits auch das Angebot und die Nutzung legaler Informationen. Speziell das Internet wird in hohem Maße zur Verbreitung legaler und sogar nützlicher und politisch wichtiger Informationen genutzt. Aus diesem Grund können steigende Zahlen hinsichtlich der Verbreitung illegaler Informationen über das Internet dessen stärkere Überwachung für sich genommen nicht rechtfertigen. Zu berücksichtigen ist stets die Entwicklung des gesamten Telekommunikationsaufkommens und die Situation im Bereich der traditionellen Massenmedien.

Ob über Telekommunikationsnetze abgewickelte Massenkommunikation prozentual öfter illegalen Zwecken dient als traditionelle Massenkommunikation, ist bisher noch nicht empirisch untersucht worden, obwohl dies in gewissem Maße möglich wäre. Beispielsweise könnten die Erkenntnisse des Bundesamts für Verfassungsschutz über die Verbreitung verfassungsfeindlicher Druckschriften mit den Angaben von Internet-Suchmaschinen über die Verbreitung solcher Angebote im Internet verglichen werden. Angesichts der unüberschaubaren Vielzahl legaler Angebote im Internet ist es nicht vertretbar, über Telekommunikationsnetze verbreitete Massenkommunikation ohne stichhaltige, dahin gehende Anhaltspunkte als schadensträchtiger anzusehen als die traditionelle Massenkommunikation. Aus diesem Grund ist die Einführung einer Vorratsspeicherung von Telekommunikationsdaten auf der Grundlage des gegenwärtigen Kenntnisstandes mit Art. 3 Abs. 1 GG unvereinbar.

cc) Computerdaten

Außer als Medium für die zwischenmenschliche Kommunikation können Telekommunikationsnetze auch zur Übertragung von Computerdaten (z.B. Musik, Software) eingesetzt werden. Technisch geschieht dies, indem fremde Computer (so genannte Server) zur Übermittlung von Daten angewiesen werden oder indem Daten an diese Computer übermittelt werden. Auch im Bereich der Netzkriminalität im enge-

ren Sinne werden Telekommunikationsnetze als Mittel zur Steuerung anderer Computersysteme eingesetzt.

Eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten zeichnet nur die telekommunikative Computerbenutzung ihren Umständen nach auf, nicht dagegen die unmittelbare Benutzung eines Computers. Als unmittelbare Computerbenutzung ist dabei auch der Zugriff mittels selbst betriebener Netzwerke (z.B. Unternehmensnetzwerke) anzusehen, der keine Telekommunikation im Sinne des TKG darstellt. Der gemeinsame Oberbegriff liegt in der Benutzung von Computern, so dass die Vergleichbarkeit der Sachverhalte gegeben ist. Da im Fall einer Vorratsspeicherung von Telekommunikationsdaten nur die telekommunikative Computerbenutzung ihren Umständen nach aufgezeichnet wird, werden diejenigen Personen benachteiligt, die Computer mittels Telekommunikation und nicht unmittelbar benutzen. Ein Eingriff in das Grundrecht dieser Personen aus Art. 3 Abs. 1 GG liegt damit vor.

Fraglich ist, welcher Maßstab bei der Rechtfertigungsprüfung anzuwenden ist. Wie im Bereich der zwischenmenschlichen Kommunikation gibt es viele Menschen und Berufsgruppen, die auf die telekommunikative Computerbenutzung angewiesen sind, ohne zumutbarerweise auf die unmittelbare Computerbenutzung ausweichen zu können. Gerade das Internet ermöglicht die Nutzung von Computern in der ganzen Welt, zu denen kein unmittelbarer Zugang besteht. Im Berufsleben sind auch Direktverbindungen von Berufstätigen mit dem Computer ihres Arbeitgebers üblich, um Daten auszutauschen. Da viele Berufe die räumliche Trennung von dem jeweiligen Arbeitgeber mit sich bringen, ist Telekommunikation in diesen Bereichen unersetzlich. Eine generelle Verkehrsdatenspeicherung stellt darüber hinaus einen schweren Eingriff in verschiedene Freiheitsgrundrechte dar, was ebenfalls für eine strikte Prüfung spricht. Insgesamt ergibt sich wiederum, dass eine Verhältnismäßigkeitsprüfung durchzuführen ist.

Auf dem Gebiet der Computerbenutzung kann nicht geltend gemacht werden, dass eine Aufzeichnung und Vorhaltung von Daten über die näheren Umstände der unmittelbaren Computerbenutzung nicht realisierbar sei. In vielen Unternehmen gibt es bereits Mechanismen, um die Computernutzung durch Mitarbeiter zu protokollieren. Diese Verfahren könnten auf sämtliche Computer ausgedehnt werden.

Dass eine Vorratsspeicherung im Bereich der Benutzung einzelner Computer mit höherem Aufwand verbunden wäre als im Bereich der Telekommunikation, kann entsprechend den obigen Ausführungen auch hier nicht die gravierende Ungleichbehandlung rechtfertigen, die mit einer generellen Vorratsspeicherung allein von Telekommunikations-Verkehrsdaten verbunden ist.

Als Rechtfertigungsgrund kommt weiterhin in Betracht, dass von der telekommunikativen Computerbenutzung ein höheres Gefährdungspotenzial ausgehen könnte als von der unmittelbaren Computerbenutzung. Ob dies der Fall ist, ist bisher nicht bekannt. Einerseits lassen sich beispielsweise Computerangriffe über das Internet über weitere Entfernungen hinweg vornehmen als wenn unmittelbar auf einen Computer des Opfers zugegriffen werden müsste. Zudem sind Computer nur für einen eingeschränkten Personenkreis unmittelbar zugänglich. Andererseits wurde bereits ausgeführt, dass ein großer Teil der durch Netzkriminalität im engeren Sinne verursachten Schäden auf Mitarbeiter der betroffenen Unternehmen zurückzuführen ist und dass Telekommunikationsnetze insoweit nur selten zum Einsatz kommen. Wo die Möglichkeit eines unmittelbaren Computerzugriffs besteht, werden Straftäter die Benutzung von Telekommunikationsnetzen schon deshalb meiden, weil ihnen regelmäßig bekannt sein wird, dass dabei Verkehrsdaten anfallen können. Ohne entsprechende empirische Erkenntnisse kann mithin nicht unterstellt werden, dass der typische Telekommunikationsvorgang öfter dem Angriff auf Computersysteme dient als die durchschnittliche unmittelbare Computernutzung. Es spricht vielmehr einiges für die Annahme, dass die unmittelbare wie die telekommunikative Benutzung von Computern gleichermaßen ganz überwiegend zu legitimen Zwecken und nur äußerst selten zum Zweck von Computerangriffen erfolgt.

Die Ausnahme der unmittelbaren Computerbenutzung von einer Vorratsspeicherungspflicht könnte ferner damit gerechtfertigt werden, dass es jeder Betreiber eines Computersystems in der Hand habe, den unmittelbaren Zugriff auf sein System zu unterbinden oder zu kontrollieren, dass er den Zugriff mittels Telekommunikationsnetzen dagegen nicht in gleichem Maße kontrollieren könne. Gegen diese Argumentation ist einzuwenden, dass sich der Personenkreis, der unmittelbaren Zugriff auf Computersysteme hat, zwar einschränken lässt (z.B. durch Eingangskontrollen), dass es aber auch im Bereich der Telekommunikationsnetze Mechanismen gibt, welche das sichere Authentifizieren von Benutzern ermöglichen. Computerkriminali-

tät im engeren Sinne wird zudem oft von Mitarbeitern des Geschädigten begangen, die legalen räumlichen Zugang zu den angegriffenen Systemen haben. Nicht selten sind diese Personen technisch äußerst versiert und können dadurch Schutzmechanismen umgehen. Oft wird Computerkriminalität im engeren Sinne auch gerade von denjenigen Personen begangen, die für die Sicherheit der angegriffenen Systeme sorgen sollen (Administratoren). Im Gegensatz dazu gestaltet sich der Angriff auf Computersysteme mittels Telekommunikationsnetzen regelmäßig schwieriger. Der Betreiber hat es insoweit in hohem Maße in der Hand, Computerangriffen durch technische Maßnahmen vorzubeugen. Wenn die eingesetzte Software regelmäßig aktualisiert wird, lassen sich Schäden infolge von „Hacking" weitgehend ausschließen. Jedenfalls lässt sich nicht ohne genauere Untersuchungen behaupten, dass der Schutz vor unmittelbaren Zugriffen einfacher möglich sei als der Schutz vor Angriffen mittels Telekommunikationsnetzen.

In Anbetracht der insoweit bestehenden Unsicherheitsfaktoren bemisst sich der Einschätzungsspielraum des Gesetzgebers nach den oben diskutierten Kriterien. Wegen der Eingriffsintensität einer Vorratsspeicherung von Verkehrsdaten ist zu verlangen, dass der Gesetzgeber eine vertretbare Entscheidung trifft und die für die Beurteilung der Verfassungsmäßigkeit relevanten Tatsachen zuvor möglichst vollständig ermittelt. Die Einführung einer auf den Telekommunikationsbereich beschränkten Vorratsspeicherung ist nur dann eine vertretbare Entscheidung des Gesetzgebers, wenn er sich zuvor durch Aufklärung der Sachlage versichert, dass von der telekommunikativen Computerbenutzung überproportional größere Gefahren ausgehen. Größere Gefahren können sich dabei auch aus verminderten Schutzmöglichkeiten gegenüber Angriffen über Telekommunikationsnetze ergeben.

Auf der Grundlage der bisherigen Kenntnisse kann von größeren Gefahren infolge von telekommunikativer Computerbenutzung – wie gezeigt – nicht ausgegangen werden, so dass derzeit keine Gründe von solcher Art und solchem Gewicht ersichtlich sind, dass sie eine Ungleichbehandlung der telekommunikativen gegenüber der unmittelbaren Computerbenutzung rechtfertigen könnten. Aus diesem Grund ist die Einführung einer Vorratsspeicherung von Telekommunikationsdaten gegenwärtig mit Art. 3 Abs. 1 GG unvereinbar.

3.2 § 97 Abs. 3 S. 3 und Abs. 4 TKG

§ 97 TKG lautet wie folgt:

§ 97 Entgeltermittlung und Entgeltabrechnung
(1) Diensteanbieter dürfen die in § 96 Abs. 1 aufgeführten Verkehrsdaten verwenden, soweit die Daten zur Ermittlung des Entgelts und zur Abrechnung mit ihren Teilnehmern benötigt werden. Erbringt ein Diensteanbieter seine Dienste über ein öffentliches Telefonnetz eines fremden Betreibers, darf der Betreiber des öffentlichen Telefonnetzes dem Diensteanbieter die für die Erbringung von dessen Diensten erhobenen Verkehrsdaten übermitteln. Hat der Diensteanbieter mit einem Dritten einen Vertrag über den Einzug des Entgelts geschlossen, so darf er dem Dritten die in Absatz 2 genannten Daten übermitteln, soweit es zum Einzug des Entgelts und der Erstellung einer detaillierten Rechnung erforderlich ist. Der Dritte ist vertraglich zur Wahrung des Fernmeldegeheimnisses nach § 88 und des Datenschutzes nach den §§ 93 und 95 bis 97, 99 und 100 zu verpflichten. § 11 des Bundesdatenschutzgesetzes bleibt unberührt.
(2) Der Diensteanbieter darf zur ordnungsgemäßen Ermittlung und Abrechnung der Entgelte für Telekommunikationsdienste und zum Nachweis der Richtigkeit derselben folgende personenbezogene Daten nach Maßgabe der Absätze 3 bis 6 erheben und verwenden:
1. die Verkehrsdaten nach § 96 Abs. 1,
2. die Anschrift des Teilnehmers oder Rechnungsempfängers, die Art des Anschlusses, die Zahl der im Abrechnungszeitraum einer planmäßigen Entgeltabrechnung insgesamt aufgekommenen Entgelteinheiten, die übermittelten Datenmengen, das insgesamt zu entrichtende Entgelt,
3. sonstige für die Entgeltabrechnung erhebliche Umstände wie Vorschusszahlungen, Zahlungen mit Buchungsdatum, Zahlungsrückstände, Mahnungen, durchgeführte und aufgehobene Anschlusssperren, eingereichte und bearbeitete Reklamationen, beantragte und genehmigte Stundungen, Ratenzahlungen und Sicherheitsleistungen.

(3) Der Diensteanbieter hat nach Beendigung der Verbindung aus den Verkehrsdaten nach § 96 Abs. 1 Nr. 1 bis 3 und 5 unverzüglich die für die Berechnung des Entgelts erforderlichen Daten zu ermitteln. Nicht erforderliche Daten sind unverzüglich zu löschen. Die Verkehrsdaten dürfen - vorbehaltlich des Absatzes 4 Satz 1 Nr. 2 - höchstens sechs Monate nach Versendung der Rechnung gespeichert werden. Hat der Teilnehmer gegen die Höhe der in Rechnung gestellten Verbindungsentgelte vor Ablauf der Frist nach Satz 3 Einwendungen erhoben, dürfen die Verkehrsdaten gespeichert werden, bis die Einwendungen abschließend geklärt sind.

(4) Nach Wahl des Teilnehmers hat der rechnungsstellende Diensteanbieter die Zielnummer
1. vollständig oder unter Kürzung um die letzten drei Ziffern zu speichern oder
2. mit Versendung der Rechnung an den Teilnehmer vollständig zu löschen.
Der Teilnehmer ist auf sein Wahlrecht hinzuweisen; macht er von seinem Wahlrecht keinen Gebrauch, ist die Zielnummer ungekürzt zu speichern. Soweit ein Teilnehmer zur vollständigen oder teilweisen Übernahme der Entgelte für bei seinem Anschluss ankommende Verbindungen verpflichtet ist, dürfen ihm die Rufnummern der Anschlüsse, von denen die Anrufe ausgegangen sind, nur gekürzt übermittelt werden. Die Sätze 1 und 2 gelten nicht für Diensteanbieter, die ihre Dienste nur den Teilnehmern geschlossener Benutzergruppen anbieten.

(5) Soweit es für die Abrechnung des Diensteanbieters mit anderen Diensteanbietern oder mit deren Teilnehmern sowie anderer Diensteanbieter mit ihren Teilnehmern erforderlich ist, darf der Diensteanbieter Verkehrsdaten verwenden.

(6) Zieht der Diensteanbieter mit der Rechnung Entgelte für Leistungen eines Dritten ein, die dieser im Zusammenhang mit der Erbringung von Telekommunikationsdiensten erbracht hat, so darf er dem Dritten Bestands- und Verkehrsdaten übermitteln, soweit diese im Einzelfall für die Durchsetzung der Forderungen des Dritten gegenüber seinem Teilnehmer erforderlich sind.

3.2.1 Art. 10 GG

3.2.1.1 Schutzbereich

Dass der Schutzbereich des Fernmeldegeheimnisses Verkehrsdaten als Angaben über die näheren Umstände der Telekommunikation erfasst, ist unstreitig.

3.2.1.2 Eingriff

Es stellt einen staatlichen Eingriff in Art. 10 GG dar, wenn Telekommunikationsunternehmen das Recht eingeräumt wird, Verkehrsdaten länger als für ihre Zwecke erforderlich speichern zu dürfen, und wenn gleichzeitig staatlichen Behörden Zugriffsrechte auf diese Daten eingeräumt werden. Dies ergibt sich aus den Ausführungen zum Eingriffscharakter des § 100 TKG auf den Seiten 13 bis 27, auf die Bezug genommen wird.

Dass § 97 Abs. 3 S. 3 TKG Telekommunikationsunternehmen das Recht einräumt, Verkehrsdaten länger als für ihre Zwecke erforderlich speichern zu dürfen, ergibt sich aus den Ausführungen bei Breyer, Vorratsspeicherung (2005)[81], Seiten 95-101 und bei Breyer, RDV 2004, 147 (149 f.), auf die Bezug genommen wird, wobei die zentralen Argumente die folgenden sind:

- Zur Abrechnung ist die Speicherung von Verkehrsdaten nicht erforderlich. Es genügt, wenn – wie bis 1990 – unverzüglich nach Verbindungsende das angefallene Entgelt ermittelt und zum insgesamt fälligen Rechnungsbetrag hinzuaddiert wird.
- Zu Nachweiszwecken ist die Speicherung von Verkehrsdaten nur dann erforderlich, wenn der Kunde im voraus einen Einzelverbindungsnachweis (§ 99 TKG) verlangt hat (so auch § 6 Abs. 7 TDDSG). Unterlässt der Kunde dies, so ist er beweispflichtig für eine angeblich falsche Abrechnung.
- Selbst wenn der Gesetzgeber aus Gründen des Verbraucherschutzes die Möglichkeit der nachträglichen Anforderung eines Einzelnachweises gewährleisten möchte (vgl. § 16 TKV 1997), so ist eine Speicherung von Verbindungsdaten jedenfalls dann nicht erforderlich, wenn der Kunde die sofortige Löschung seiner Verkehrsdaten ausdrücklich wünscht. Eine ähnliche Regelung sahen die §§ 16 Abs. 2 TKV 1997, 7 Abs. 4 TDSV

[81] Breyer, (Fn. 8).

2000 noch ausdrücklich vor. § 97 Abs. 4 TKG erlaubt es dagegen nur noch, die Löschung der Zielrufnummern (nicht auch der übrigen Verkehrsdaten) mit Versand der Rechnung (nicht schon mit Verbindungsende) zu verlangen.

Dass staatliche Stellen Zugriff auf die nach § 97 Abs. 3 S. 3 TKG gespeicherten Verkehrsdaten haben, folgt etwa aus den §§ 100g, 100h StPO.

Es wird insofern auf die Seiten 18 – 22 oben verwiesen, auf denen auch die Ausführungen in Breyer, Vorratsspeicherung (2005), S. 95 – 101 abgedruckt sind.

Ergänzend wird auf Breyer, RDV 2004, 147 (149f.) Bezug genommen:

„Insgesamt wird bei der Diskussion um die Aufbewahrungsdauer von Verkehrsdaten verkannt, dass die Speicherung solcher Daten über das Ende einer Verbindung hinaus an sich nicht erforderlich ist. Bis zur Einführung des digitalen Telefonnetzes Anfang der 90er Jahre sind die damalige Bundespost und die Bürger ohne eine Speicherung von Verkehrsdaten ausgekommen. Es genügte damals und es würde auch heute noch genügen, nach dem Ende einer jeden Verbindung die angefallenen Kosten zu ermitteln und diese dem Kundenkonto zu belasten. Technisch ist dies allen Anbietern möglich und wird verbreitet bereits heute praktiziert. Ein solches Verfahren geht nicht zulasten der Anbieter, weil der Kunde die Beweislast hinsichtlich der Richtigkeit der Abrechnung trägt, wenn er die sofortige Löschung seiner Daten wählt (§ 16 Abs. 2 TKV). Zwar kann der Kunde bei sofortiger Löschung der Verkehrsdaten die Richtigkeit der Abrechnung des Anbieters im Nachhinein nicht mehr nachprüfen. Es sollte aber jedem Bürger überlassen bleiben, ob ihm diese Überprüfungsmöglichkeit wichtiger ist als seine Privatsphäre. Immerhin ist es sehr unwahrscheinlich, dass Abrechnungssysteme falsch arbeiten, und bis Anfang der 90er Jahre ist man, wie bereits erwähnt, problemlos auch ohne die Speicherung von Verkehrsdaten ausgekommen. Zudem verhindert auch die Aufbewahrung von Verkehrsdaten nicht, dass das Abrechnungssystem bereits bei der Erfassung der einzelnen Verbindungen fehlerhaft arbeitet. Angesichts dessen gibt es keine Notwendigkeit, die Löschung von Verkehrsdaten frühestens mit Versand der Rechnung vorzusehen. Die TKG-Novelle hätte Kunden vielmehr das Recht einräumen sollen, die sofortige Löschung sämtlicher Verkehrsdaten nach dem Ende jeder Verbindung verlangen zu können. Wenn das Gesetz dies anders handhabt, so lässt sich das nur mit dem Interesse der Sicherheitsbehörden an einer möglichst lückenlosen Aufzeichnung des Kommunikationsverhaltens der Bevölkerung erklären. Dieses Interesse rechtfertigt jedoch keine Vorratsspeicherung ansonsten nicht benötigter Daten, zumal ernsthaften Kriminellen ohnehin Mittel und Wege zur Verfügung stehen,

um sich der Überwachung ihrer Telekommunikation zu entziehen (z.B. durch Nutzung von Prepaid-Mobiltelefonkarten, die auf den Namen einer anderen Person angemeldet sind).

Zu kritisieren ist auch die Bemessung der maximal zulässigen Aufbewahrungsdauer. Dass zur Abrechnung benötigte Verkehrsdaten bis zu sechs Monate lang gespeichert werden dürfen (§ 97 Abs. 3 S. 3 TKG, ebenso § 7 Abs. 3 S. 3 TDSV), dient offenbar dem Zweck, die Überwachung der Telekommunikation durch die Sicherheitsbehörden zu erleichtern. Eine angemessene Frist stellen sechs Wochen nach Rechnungsversand dar, wie es noch die TKV 1995 vorsah. Innerhalb von sechs Wochen hat jedermann die Möglichkeit, Einwendungen zu erheben.

3.2.1.3 Rechtfertigung

Art. 10 Abs. 2 S. 1 GG bestimmt: "Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden." Bereits aus dieser Bestimmung ergibt sich, dass das Fernmeldegeheimnis nicht generell "durch Gesetz" eingeschränkt werden darf, sondern dass Beschränkungen des Fernmeldegeheimnisses nur "auf Grund eines Gesetzes" im Einzelfall "angeordnet" werden dürfen. § 97 Abs. 3 S. 3 TKG ist von dem Gesetzesvorbehalt des Art. 10 Abs. 2 S. 1 GG nicht gedeckt, weil § 97 Abs. 3 S. 3 TKG das Fernmeldegeheimnis generell einschränkt und nicht nur Beschränkungen im Einzelfall zulässt.

Daneben ist § 97 Abs. 3 S. 3 TKG auch deswegen verfassungswidrig, weil die Vorschrift das eingeschränkte Grundrecht (das Fernmeldegeheimnis) nicht unter Angabe des Artikels (Art. 10 Abs. 1 GG) nennt, wie es Art. 19 Abs. 1 S. 2 GG vorschreibt.

Dass die Einräumung von Vorratsspeicherungsrechten auf dem Gebiet der Telekommunikation darüber hinaus unverhältnismäßig ist, ergibt sich aus den Ausführungen zu Art. 3 GG auf Seite 28, die für § 97 Abs. 3 S. 3, Abs. 4 TKG entsprechend gelten und auf die deswegen Bezug genommen wird.

3.2.2 Art. 3 Abs. 1 GG

Dass die Einräumung von Vorratsspeicherungsrechten auf dem Gebiet der Telekommunikation gegen Art. 3 Abs. 1 GG verstößt, ergibt sich aus den Ausführungen auf Seite 28, die im Hinblick auf § 97 Abs. 3 S. 3, Abs. 4 TKG entsprechend gelten und auf die deswegen Bezug genommen wird. Auch § 97 Abs. 3 S. 3, Abs. 4 TKG stellt eine ungerechtfertigte Ungleichbehandlung dar:

- der Telekommunikationsnutzung gegenüber der Nutzung anderer Formen der Fernkommunikation,
- der Telekommunikationsnutzung gegenüber der Inanspruchnahme anderer Unternehmen, die für den Staat nützliche Daten erheben und bereitstellen könnten, und

- der Telekommunikationsnutzung gegenüber der räumlich-unmittelbaren Kommunikation.

3.3 § 111 TKG

§ 111 TKG lautet:
§ 111 Daten für Auskunftsersuchen der Sicherheitsbehörden
(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113 die Rufnummern, den Namen und die Anschrift des Rufnummerninhabers, das Datum des Vertragsbeginns, bei natürlichen Personen deren Geburtsdatum, sowie bei Festnetzanschlüssen auch die Anschrift des Anschlusses vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind; das Datum des Vertragsendes ist bei Bekanntwerden ebenfalls zu speichern. Satz 1 gilt auch, soweit die Daten nicht in Teilnehmerverzeichnisse (§ 104) eingetragen werden. Wird dem Verpflichteten nach Satz 1 eine Änderung bekannt, hat er die Daten unverzüglich zu berichtigen; in diesem Zusammenhang hat er bisher noch nicht erfasste Daten nach Satz 1 nachträglich zu erheben und zu speichern, sofern ihm eine Erhebung der Daten ohne besonderen Aufwand möglich ist. Nach Ende des Vertragsverhältnisses sind die Daten mit Ablauf des auf die Beendigung folgenden Kalenderjahres zu löschen. Eine Entschädigung für die Datenerhebung und -speicherung wird nicht gewährt. Für das Auskunftsverfahren nach § 113 ist die Form der Datenspeicherung freigestellt.
(2) Bedient sich der Diensteanbieter nach Absatz 1 Satz 1 eines Vertriebspartners, hat der Vertriebspartner die Daten nach Absatz 1 Satz 1 zu erheben und diese sowie die nach § 95 erhobenen Daten unverzüglich dem Diensteanbieter zu übermitteln; Absatz 1 Satz 2 gilt entsprechend. Satz 1 gilt auch für Daten über Änderungen, soweit sie dem Vertriebspartner im Rahmen der üblichen Geschäftsabwicklung zur Kenntnis gelangen.
(3) Für Vertragsverhältnisse, die am Tage des Inkrafttretens dieser Vorschrift bereits bestehen, müssen Daten im Sinne von Absatz 1 Satz 1 außer in den Fällen des Absatzes 1 Satz 3 nicht nachträglich erhoben werden.

3.3.1 Art. 10 GG

3.3.1.1 Schutzbereich

Dass der Schutzbereich des Fernmeldegeheimnisses Bestandsdaten erfasst, ergibt sich aus den Ausführungen auf den Seiten 9 bis 12 zu Bestandsdaten, auf die Bezug genommen wird.

3.3.1.2 Eingriff

Es stellt einen staatlichen Eingriff in Art. 10 GG dar, wenn Telekommunikationsunternehmen verpflichtet werden, für ihre Zwecke nicht erforderliche Bestandsdaten zu erheben und zu speichern, und wenn gleichzeitig staatlichen Behörden Zugriffsrechte auf diese Daten eingeräumt werden. Dies ergibt sich aus den Ausführungen auf den Seiten 13 bis 27, die im Hinblick auf § 111 TKG entsprechend gelten und auf die daher Bezug genommen wird.

§ 111 TKG verpflichtet bestimmte Telekommunikationsunternehmen zur Erhebung von Bestandsdaten, selbst wenn dieses nicht zur Bereitstellung der Telekommunikationsdienste

erforderlich ist (so ausdrücklich § 111 Abs. 1 S. 1 Hs. 1 a.E. TKG). Es liegt ein Eingriff vor, weil § 111 TKG in Verbindung mit den staatlichen Zugriffsrechten auf diese Daten (§§ 112, 113 TKG) eine besondere Gefahr staatlicher Kenntnisnahme schafft.

3.3.1.3. Rechtfertigung

Art. 10 Abs. 2 S. 1 GG bestimmt: "Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden." Bereits aus dieser Bestimmung ergibt sich, dass das Fernmeldegeheimnis nicht generell "durch Gesetz" eingeschränkt werden darf, sondern dass Beschränkungen des Fernmeldegeheimnisses nur "auf Grund eines Gesetzes" im Einzelfall "angeordnet" werden dürfen. § 111 TKG ist von dem Gesetzesvorbehalt des Art. 10 Abs. 2 S. 1 GG nicht gedeckt, weil § 111 TKG das Fernmeldegeheimnis generell einschränkt und nicht nur Beschränkungen im Einzelfall zulässt.

Daneben ist § 111 TKG auch deswegen verfassungswidrig, weil die Vorschrift das eingeschränkte Grundrecht (das Fernmeldegeheimnis) nicht unter Angabe des Artikels (Art. 10 Abs. 1 GG) nennt, wie es Art. 19 Abs. 1 S. 2 GG vorschreibt.

Darüber hinaus ist § 111 TKG auch wegen Verstoßes gegen das Verhältnismäßigkeitsgebot verfassungswidrig. Die von § 111 TKG angeordnete generelle, systematische Erhebung von Bestandsdaten ist nicht durch überwiegende Allgemeininteressen gerechtfertigt (vgl. zu diesem Kriterium BVerfGE 65, 1 [44, 46]), sondern ihr möglicher Nutzen steht klar außer Verhältnis zu ihren negativen Auswirkungen auf die Grundrechtsträger. Zur Begründung wird auf die Ausführungen bei Breyer, RDV 2003, 218 (220 ff.) verwiesen, wobei die zentralen Argumente auf Seite 28 aufgeführt sind.

Die relevanten Ausführungen bei Breyer, RDV 2003, 218 (220 ff.) lauten im Einzelnen wie folgt:

> **Vorratsspeicherung von Bestandsdaten**
>
> § 106 TKG-RefE soll nunmehr eindeutig die Frage regeln, ob sich Telekommunikationsnutzer gegenüber dem Telekommunikationsunternehmen auch dann identifizieren müssen, wenn dies für die Erbringung des Telekommunikationsdienstes nicht erforderlich ist (z.B. bei vorausbezahlten Mobiltelefonkarten). Die gesetzliche Klarstellung gegenüber § 90 TKG ist zu begrüßen und verfassungsrechtlich geboten. Seiner inhaltlichen Ausgestaltung nach ist § 106 TKG-RefE jedoch höchst problematisch, weil er eine allgemeine Identifizierungspflicht mit anschließender Vorratsdatenspeicherung vorsieht. Anbieter von Telekommunikationsdiensten für die Öffentlichkeit, die Rufnummern vergeben, sollen § 106 TKG-RefE zufolge nämlich vor Freischaltung des Dienstes die Rufnummer, den Namen, die Anschrift und das Geburtsdatum des Rufnummerninhabers erheben und speichern. Diese Daten sollen bis ein Jahr nach Vertragsende für staatliche Abrufe bereit gehalten werden. § 90 Abs. 3 TKG-RefE verpflichtet auch andere Anbieter von Telekommunikationsdiensten, etwa erfasste Bestandsdaten bis ein Jahr nach Vertragsende aufzubewahren.

Abgesehen von Sondergebieten wie dem Bereich finanzieller Transaktionen (Geldwäschegesetz) ist eine staatlich angeordnete Identifizierungspflicht im deutschen Recht bisher einmalig. In Verbindung mit den oben beschriebenen, breiten staatlichen Zugriffsrechten auf die erfassten Kundendaten stellt § 106 TKG-RefE einen einzigartigen Präzedenzfall vorsorglicher staatlicher Überwachung der Bürger dar. Verfassungsrechtlich ist die in § 106 TKG-RefE vorgesehene Datenerfassung und -speicherung durch Telekommunikationsunternehmen als staatlicher Grundrechtseingriff anzusehen, weil sie hoheitlich angeordnet ist und den Unternehmen dabei kein Handlungsspielraum zur Verfügung steht[82]. § 106 TKG-RefE muss sich daher an dem Verhältnismäßigkeitsprinzip messen lassen.

Bisher liegen keinerlei empirische Erkenntnisse bezüglich der Frage vor, in welchem Maße eine Identifizierungspflicht zur Erreichung der damit verfolgten Ziele geeignet ist[83]. Zwar ist bekannt, dass Straftäter heutzutage verbreitet anonym gekaufte, vorausbezahlte Mobiltelefonkarten einsetzen, um einer Überwachung ihrer Telekommunikation zu entgehen[84]. Gerade bei ernsthaften und daher wirklich gefährlichen Kriminellen erscheint es aber naiv, anzunehmen, dass diese durch eine Identifizierungspflicht dazu bewegt werden könnten, bei dem Kauf von Karten für ihr "Arbeitshandy" brav ihre persönlichen Daten anzugeben.

Guthabenkarten lassen sich vielmehr ohne Weiteres privat handeln und weitergeben[85]. Anbieter von Mobiltelefonie schätzen, dass schon heute etwa 50% aller Prepaid-Karten innerhalb eines Jahres weitergegeben werden[86]. § 106 TKG-RefE sieht eine Identifizierungspflicht nur für Telekommunikationsanbieter und ihre Vertriebspartner vor, nicht aber für private Gelegenheitsverkäufer von Guthabenkarten. Dies trägt der Tatsache Rechnung, dass eine Identifizierungspflicht bei oder gar ein Verbot von Privatverkäufen nicht durchsetzbar wäre. Die Folge davon ist aber, dass Kriminelle auch nach Einführung des § 106 TKG-RefE Guthabenkarten ohne Weiteres privat erwerben könnten, ohne sich identifizieren zu müssen. Die Identifizierungspflicht liefe damit leer.

In Frankreich, wo eine Identifizierungspflicht für den Kauf von Guthabenkarten bereits besteht, hat man die Erfahrung gemacht, dass erfasste Daten nicht selten unzutreffend sind[87]. In der Tat haben Kriminelle ohne Weiteres die Möglichkeit, sich Händler auszusuchen, die es mit der Identifizierung nicht allzu genau

---

[82] Vgl. BVerfG, 1 BvR 330/96 vom 12.3.2003, Absatz-Nr. 50, www.bverfg.de/entscheidungen

[83] Entschließung zwischen der 63. und 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24.05.2002, www.datenschutz-berlin.de

[84] Heise Newsticker, IMSI-Catcher zur Mobilfunküberwachung bald legal, www.heise.de/newsticker/data.

[85] Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 24.05.2002 (Fn. 83).

[86] BMWi-Ressortarbeitsgruppe, Eckpunkte zur Anpassung der Regelungen des § 90 TKG, 28.03.2002, 7, www.almeprom.de/-fiff/material/Eckpunkte_90_TKG_Prepaid.pdf.

[87] BMWi-Ressortarbeitsgruppe, Eckpunkte (Fn. 86), 4 f.

nehmen. Es gibt keine praktikable Möglichkeit, dies zu verhindern. Das Gleiche gilt für die fortbestehende Möglichkeit der Nutzung anonym im Ausland gekaufter Guthabenkarten in Deutschland ("Roaming"). Jedenfalls in Anbetracht der gegenwärtigen Erkenntnisse lässt sich daher nicht vertretbarerweise behaupten, dass eine Identifizierungspflicht einen nennenswerten Beitrag zur Bekämpfung ernsthafter Kriminalität leisten könnte. Ein Nutzen der Maßnahme ist allenfalls in Bezug auf Unbedarfte zu erwarten, also im Bereich von Kleinkriminalität und Ordnungswidrigkeiten.

Demgegenüber belastet eine Identifizierungspflicht unbescholtene Bürger in ganz erheblichem Maße, weil diesen eine anonyme Telekommunikationsnutzung in weiten Bereichen unmöglich gemacht würde. Bisher konnten Personen wie Journalisten, die staatliche Missstände recherchierten, Organisatoren staatskritischer Demonstrationen oder Vertreter von Wirtschaftsunternehmen, die Wirtschaftsspionage befürchteten, durch die Benutzung vorausbezahlter Mobiltelefonkarten anonym telefonieren. Ein Identifizierungszwang könnte dagegen zur Folge haben, dass auf den Austausch sensibler Informationen mittels Telekommunikation zunehmend verzichtet würde. Damit drohen Beeinträchtigungen der gesamtgesellschaftlichen Kommunikation und, wo es sich um politische Kommunikation handelt, auch eine Beeinträchtigung der Funktionsfähigkeit unseres demokratischen Systems. Auf dem Gebiet der Verschlüsselung hat die Politik erkannt, dass die Gewährleistung der Vertraulichkeit der Telekommunikation wichtiger ist als die marginalen Sicherheitsgewinne, die eine Kryptoregulierung bestenfalls bewirken könnte. Nicht anders verhält es sich in Bezug auf die Möglichkeiten anonymer Telekommunikation.

Angesichts dessen liegt es auf der Hand, dass der mögliche Nutzen einer Identifizierungspflicht von Telekommunikationsnutzern außer Verhältnis zu den damit verbundenen Nachteilen steht. Eine Vorratsspeicherung von Telekommunikations-Bestandsdaten wäre also unverhältnismäßig[88]; eine derart weitgehende Registrierung der Bürger aus dem Bestreben nach möglichst großer Effektivität der Polizeigewalt und Erleichterung der polizeilichen Überwachung der Bevölkerung widerspräche den Prinzipien des freiheitlichen Rechtsstaates[89]. § 106 TKG-RefE ist daher mit den Art. 2 Abs. 1, Art. 1 Abs. 2 GG und mit Art. 10 GG unvereinbar. Die außerdem drohenden Belastungen für die Wirtschaft – beispielsweise müssten ganze Vertriebskanäle wie der Kartenvertrieb mittels Automaten eingestellt werden – seien nur kurz erwähnt. Es ist nicht einmal klar, ob § 106 TKG-RefE noch den Betrieb öffentlicher Telefonzellen, die über eine Rufnummer erreichbar sind, zuließe.

---

[88] Ebenso Schaar, Forderungen an Politik und Gesetzgebung, www.peter-schaar.de/FES-statement.pdf; GDD, Stellungnahme zum Entwurf für Änderungen der §§ 89, 90 und 96 TKG, www.gdd.de/pdf/ak-stellTKG.pdf.

Die konkrete Ausformung der Identifizierungspflicht in § 106 TKG-RefE verstärkt die allgemeine Unangemessenheit einer solchen Regelung. § 106 TKG-RefE schreibt nämlich nicht vor, dass die Angaben von Kunden bezüglich ihrer persönlichen Daten überprüft werden müssen. Eine Nachprüfung der Angaben anhand eines Ausweisdokuments, wie es eine Entscheidung des OVG Münster[90] und ein Kabinettsbeschluss aus dem Jahr 2002[91] noch vorsahen, schreibt § 106 TKG-RefE nicht mehr vor. Vielmehr soll es nach § 90 Abs. 4 TKG-RefE den Anbietern überlassen bleiben, ob sie sich einen Ausweis vorzeigen lassen oder nicht. Müssen die von Kunden angegebenen persönlichen Daten demnach in keiner Weise überprüft werden, dann ist die "Identifizierungspflicht" des § 106 TKG-RefE ohnehin Makulatur. Daneben ermöglicht es § 106 Abs. 3 TKG-RefE, Altverträge auf unbegrenzte Zeit identifizierungsfrei fortzuführen. Auf diese Weise wird eine weitere Umgehungsmöglichkeit eröffnet.

Unter dem Aspekt des Art. 3 Abs. 1 GG ist schließlich zu beachten, dass sich mangels empirischer Anhaltspunkte derzeit nicht vertretbarerweise behaupten lässt, dass die Benutzung von Telekommunikationsnetzen gefahrenträchtiger als sonstige Alltagshandlungen sei, oder dass Telekommunikations-Bestandsdaten für die Gefahrenabwehr oder Strafverfolgung nützlicher seien als Daten über beliebige andere Vertragsverhältnisse. Dass sich eine Vorratsspeicherung von Bestandsdaten nur auf dem Gebiet der Telekommunikation finanziell günstig realisieren lassen mag, kann die gravierende Ungleichbehandlung der Telekommunikationsbenutzung gegenüber der Inanspruchnahme sonstiger Leistungen nicht rechtfertigen, so dass § 106 TKG-RefE auch mit Art. 3 Abs. 1 GG unvereinbar ist.

3.3.2 Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Soweit der Schutzbereich des Fernmeldegeheimnisses in Bezug auf Bestandsdaten nicht für einschlägig gehalten wird, ist jedenfalls das Grundrecht auf informationelle Selbstbestimmung einschlägig, weil Bestandsdaten personenbezogene Daten darstellen. In diesem Fall gelten die obigen Ausführungen zu Art. 10 GG ab Seite 51 – mit Ausnahme der Ausführungen zum Gesetzesvorbehalt und zum Zitiergebot – entsprechend unter dem Aspekt des Rechts auf informationelle Selbstbestimmung.

---

[89] Vgl. BVerwGE 26, 169 (170).

[90] OVG Münster, MMR 2002, 563 (563).

[91] Kabinettbeschluss des Bundesregierung vom 17.04.2002, www.dud.de/dud/documents/tkg-aend-e-020417.pdf.

3.3.3 Art. 3 Abs. 1 GG

3.3.3.1 Ungleichbehandlung der Telekommunikationsnutzung gegenüber anderen Tätigkeiten, bei denen für den Staat nützliche Daten erhoben und bereitgestellt werden könnten

Die Ausführungen auf den Seiten 28 bis 29 gelten für § 111 TKG entsprechend. Auch § 111 TKG stellt eine ungerechtfertigte Ungleichbehandlung dar:

- der Telekommunikationsnutzung gegenüber der Nutzung anderer Formen der Fernkommunikation,
- der Telekommunikationsnutzung gegenüber der Inanspruchnahme anderer Unternehmen, die für den Staat nützliche Daten erheben und bereitstellen könnten, und
- der Telekommunikationsnutzung gegenüber der räumlich-unmittelbaren Kommunikation.

3.3.3.2 Ungleichbehandlung des Angebots von Telekommunikationsdienstleistungen gegenüber dem Angebot anderer Unternehmen, die für den Staat nützliche Daten erheben und bereitstellen könnten

Darüber hinaus stellt § 111 TKG auch eine ungerechtfertigte Benachteiligung der Telekommunikationsunternehmen gegenüber anderen Kommunikationsunternehmen (z.B. Anbieter von Postfächern) und anderen Unternehmen, die für den Staat nützliche Daten erheben und bereitstellen könnten, dar (siehe im Einzelnen Breyer, Vorratsspeicherung (2005)[92], Seiten 331-338). Von der Ungleichbehandlung der Telekommunikation betroffen sind also nicht nur die Telekommunikationsnutzer, sondern auch die in § 111 TKG genannten Telekommunikationsanbieter.

Die relevanten Ausführungen bei Breyer, Vorratsspeicherung (2005)[93], Seiten 331-338 lauten im Einzelnen wie folgt:

Ungleichbehandlung der Telekommunikation gegenüber dem Postwesen

Ungleichbehandlung des distanzierten Informationsaustausches per Telekommunikation gegenüber dem distanzierten Austausch verkörperter Informationen

Des Weiteren ist fraglich, ob es gerechtfertigt ist, eine Pflicht zur Vorratsspeicherung von Verkehrsdaten nur im Telekommunikationsbereich vorzusehen, nicht aber im Postbereich. Zu vergleichen ist also die Übermittlung von Informationen mittels Tele-

[92] Breyer, (Fn. 8).
[93] Breyer, (Fn. 8).

kommunikation mit der postalischen Übermittlung von Informationen. Gemeinsamer Oberbegriff ist die räumlich distanzierte Übermittlung von Informationen, so dass die Vergleichbarkeit der Sachverhalte gegeben ist. Dies gilt auch im Hinblick auf computerlesbare Daten, weil auch diese auf Datenträgern postalisch versandt werden können. Durch den intensiven Eingriff in verschiedene Freiheitsgrundrechte werden die Telekommunikationsnutzer gegenüber den Nutzern von Postdienstleistungen benachteiligt, weil die näheren Umstände der Informationsübermittlung nur im ersten Fall festgehalten werden. Darin liegt ein Eingriff in das Grundrecht der Telekommunikationsnutzer aus Art. 3 Abs. 1 GG.

Was den Rechtfertigungsmaßstab anbelangt, so gibt es viele Menschen und Berufsgruppen, die typischerweise auf die Möglichkeit des telekommunikativen Informationsaustausches angewiesen sind, ohne zumutbarerweise auf die Post ausweichen zu können. Dies gilt besonders für Arbeitnehmer und Selbstständige, die sich bei ihrer Tätigkeit nach äußeren Zwängen richten müssen. Zu dieser Gruppe gehören auch Journalisten, deren zum Teil vertrauliche Arbeit in unserer freiheitlichen Demokratie besonders wichtig ist. Dasselbe gilt etwa für Menschenrechtsorganisationen. Auch außerhalb des beruflichen Bereichs wird im Zeitalter der Informationsgesellschaft der körperliche Informationsaustausch immer mehr verdrängt. Während es beispielsweise Bürger- und Sorgentelefone gibt, die Bürgern eine fachkundige Beratung in Notlagen bieten, ist die Nutzung solcher Angebote per Post meist nicht möglich. Ähnlich verhält es sich mit dem Internet, dessen reichhaltiges Informationsangebot sich durch keine Bibliothek mit Fernleihemöglichkeit ersetzen lässt. Nimmt man die hohe Eingriffsintensität einer Vorratsspeicherung von Telekommunikationsdaten hinzu, dann wiegt die Ungleichbehandlung gegenüber der Postbenutzung so schwer, dass wiederum eine Verhältnismäßigkeitsprüfung erforderlich ist.

Im Unterschied zum unmittelbaren Informationsaustausch kann auf dem Gebiet der Postdienstleistungen nicht geltend gemacht werden, dass eine Aufzeichnung und Vorhaltung von Verkehrsdaten nicht realisierbar sei. Auch dass der Absender auf postalischen Sendungen bisher nicht angegeben werden muss, hindert die Aufzeichnung von Verkehrsdaten nicht, weil eine Identifizierungspflicht eingeführt werden könnte. Im Übrigen ist auch im Telekommunikationsbereich stets nur der Anschlussinhaber, nicht aber der jeweilige Benutzer des Anschlusses identifizierbar. Dass eine Vorratsspeicherung im Postbereich mit höherem Aufwand verbunden

sein könnte als im Bereich der Telekommunikation, genügt nach dem oben Gesagten nicht, um die gravierende Ungleichbehandlung zu rechtfertigen, zumal der Aufwand einer Vorratsspeicherung im Postbereich ungleich geringer wäre als im Bereich unmittelbarer Kommunikation.

Als Rechtfertigungsgrund kommt weiterhin in Betracht, dass von dem telekommunikativen Informationsaustausch ein höheres Gefahrenpotenzial ausgehen könnte als von dem Informationsaustausch per Post. Ob dies der Fall ist, ist unbekannt und lässt sich empirisch wohl nur im Wege von repräsentativen Untersuchungen feststellen. Fest steht zwar, dass Telekommunikationsnetze im Vergleich zur Nutzung der Post den Austausch von Informationen allgemein erleichtern und diesen kostengünstig, einfach, schnell, vertraulich und über weite Entfernungen – auch Ländergrenzen – hinweg ermöglichen. Allerdings ist auch dem Postverkehr ein spezifisches Gefährdungspotenzial zueigen. Weil bei dem postalischen Verkehr kein Absender angegeben werden muss oder die Absenderangabe nicht überprüft wird, eröffnet die Post zusätzliche Möglichkeiten des konspirativen Informationsaustausches zwischen Straftätern. Ebenso wie im Telekommunikationsbereich lässt sich auch beim postalischen Informationsaustausch jegliche Kontrolle unterbinden, indem man verschlüsselte Informationen versendet. Zudem kann der Inhalt von Postsendungen schon des hohen Aufwandes wegen nicht in nennenswertem Maße auf einschlägige Hinweise kontrolliert werden. Damit kann sich die Post als Ausweichmöglichkeit für Straftäter anbieten, die ihre Kommunikation nicht mehr konspirativ über Telekommunikationsnetze abwickeln können, weil in diesem Bereich eine generelle Verkehrsdatenspeicherung eingeführt wurde.

Summa summarum lassen die generellen Merkmale von Telekommunikationsnetzen nicht mit hinreichender Sicherheit auf ein höheres Gefahrenpotenzial der Telekommunikation schließen als es der Austausch von Informationen per Post aufweist. Entsprechend der obigen Feststellungen ist der Gesetzgeber auch in Bezug auf die Frage, ob von dem telekommunikativen Informationsaustausch größere Gefahren ausgehen als von dem Informationsaustausch per Post, gemäß Art. 3 Abs. 1 GG zur Aufklärung verpflichtet, bevor er eine Vorratsspeicherung allein von Telekommunikationsdaten beschließen darf. Nach bisherigen Erkenntnissen existieren keine Gründe von solcher Art und solchem Gewicht, dass sie eine Diskriminierung der Telekommunikationsbenutzung gegenüber der Postbenutzung im Wege einer gene-

rellen Vorratsspeicherung nur von Telekommunikations-Verkehrsdaten rechtfertigen könnten.

Ungleichbehandlung von Telekommunikationsunternehmen gegenüber Postunternehmen

Statt aus der Nutzerperspektive lässt sich der Vergleich von Telekommunikation und Post auch aus Sicht der befördernden Unternehmen anstellen. Eine Pflicht zur generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten trifft nur Telekommunikations-, nicht aber Postunternehmen, so dass eine Ungleichbehandlung erfolgt. Beide Arten von Unternehmen unterfallen dem Oberbegriff der beruflichen Übermittler von Informationen, so dass sie vergleichbar sind. Von der Ungleichbehandlung nachteilig betroffen sind die Telekommunikationsunternehmen, so dass eine Speicherungspflicht nur für Telekommunikations-Verkehrsdaten einen Eingriff in das Grundrecht der Telekommunikationsunternehmen aus Art. 3 Abs. 1 GG darstellt. Was den Rechtfertigungsmaßstab angeht, so knüpft eine generelle Verkehrsdatenspeicherung eindeutig an Personengruppen – nämlich an den Beruf des Telekommunikationsdienstleisters – und nicht nur an Sachverhalte an. Wie gezeigt, greift die Verkehrsdatenspeicherungspflicht auch intensiv in das Grundrecht der betroffenen Unternehmen aus Art. 12 Abs. 1 GG ein, wenn keine umfassende Kostenerstattung vorgesehen wird. Es ist daher eine Verhältnismäßigkeitsprüfung vorzunehmen.

Wie gezeigt, gibt es nach derzeitigen Erkenntnissen keine hinreichenden Gründe für die Annahme, dass mit der postalischen Vermittlung von Informationen typischerweise geringere Gefahren verbunden seien als mit der telekommunikativen Informationsübermittlung. Weil damit gegenwärtig nicht ersichtlich ist, dass die mit einer Verkehrsdatenspeicherungspflicht verbundene Benachteiligung von Telekommunikationsunternehmen gerechtfertigt ist, ist eine solche Maßnahme mit Art. 3 Abs. 1 GG unvereinbar.

Ungleichbehandlung der Telekommunikation gegenüber sonstigen Leistungen
Ungleichbehandlung der Inanspruchnahme von Telekommunikation gegenüber der Inanspruchnahme sonstiger Leistungen

Teilweise wird argumentiert, es sei nicht ersichtlich, dass Telekommunikations-Verkehrsdaten für die Eingriffsbehörden nützlicher sein könnten als jegliche andere personenbezogenen Daten, wie sie etwa bei Banken oder Fluggesellschaften gespeichert werden. Im Hinblick darauf sei es nicht gerechtfertigt, nur im Telekommunikationsbereich eine Vorratsspeicherung zu staatlichen Zwecken vorzusehen. Aus verfassungsrechtlicher Sicht ist diese Frage wiederum unter dem Aspekt des Art. 3 Abs. 1 GG zu prüfen.

Eine generelle Verkehrsdatenspeicherung führt dazu, dass die Inanspruchnahme von Telekommunikation anders behandelt wird als die Inanspruchnahme sonstiger Leistungen, bei deren Erbringung Daten anfallen oder gespeichert werden können, die für die Gefahrenabwehr oder Strafverfolgung nützlich sein können. Allgemein existiert nämlich keine Pflicht zur Vorhaltung gefahrenabwehr- und strafverfolgungsrelevanter Daten zu staatlichen Zwecken. Gemeinsamer Oberbegriff der genannten Sachverhalte ist die Inanspruchnahme von Leistungen, bei deren Erbringung Daten anfallen oder gespeichert werden können, die für die Gefahrenabwehr oder Strafverfolgung nützlich sein können. Eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten benachteiligt Telekommunikationsbenutzer unter anderem gegenüber Kunden von Banken und Fluggesellschaften, so dass ein Eingriff in das Recht der Telekommunikationsnutzer aus Art. 3 Abs. 1 GG vorliegt.

Bezüglich der Anforderungen an eine verfassungsmäßige Rechtfertigung dieser Ungleichbehandlung ist zunächst festzuhalten, dass sich eine Ungleichbehandlung von Sachverhalten ohne unmittelbaren Personenbezug annehmen ließe. Allerdings gilt auch hier wieder, dass man die Benutzung von Telekommunikationsnetzen heutzutage kaum vermeiden kann und dass bestimmte Personengruppen typischerweise besonders darauf angewiesen sind, insbesondere bestimmte Berufsgruppen. Außerdem ist eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten mit einem schwerwiegenden Eingriff in verschiedene Freiheitsgrundrechte verbunden, so dass eine Verhältnismäßigkeitsprüfung vorzunehmen ist. Prüfungsmaßstab ist daher, ob ein sachlicher Grund von solcher Art und solchem Gewicht existiert, dass er die Ungleichbehandlung rechtfertigt.

Dass eine Vorratsspeicherung der Kundendaten von Banken, Fluggesellschaften und anderen Unternehmen nicht machbar oder finanzierbar sei, lässt sich nicht be-

haupten. Im Unterschied zu Telekommunikations-Verkehrsdaten wäre in diesen Bereichen vielfach sogar keine zusätzliche Erfassung, sondern nur eine verlängerte Speicherung ohnehin erfasster Daten erforderlich, so dass der Aufwand eher geringer wäre.

Weiterhin ist zu überlegen, ob die Kundendaten von Banken und Fluggesellschaften für die Gefahrenabwehr oder Strafverfolgung typischerweise weniger nützlich sind als Telekommunikations-Verkehrsdaten. Gegen diese Überlegung spricht, dass gerade bei der organisierten Kriminalität vermehrt finanzielle Transaktionen und räumliche Mobilität anzunehmen sind. Angesichts der äußerst geringen Wahrscheinlichkeit, dass ein Telekommunikations-Verkehrsdatum bei der Abwehr einer Gefahr von Nutzen ist, liegt es nahe, dass diese Wahrscheinlichkeit bei Daten etwa über finanzielle Transaktionen und Flüge mindestens ebenso hoch liegt[94]. Es ist sogar wahrscheinlich, dass in diesen Bereichen zahlenmäßig erheblich weniger Daten anfallen als Telekommunikations-Verkehrsdaten, was für den höheren Nutzen eines typischen, bei Banken oder Fluggesellschaften anfallenden Datums spricht. Dass Telekommunikations-Verkehrsdaten einen höheren Nutzen für die Gefahrenabwehr- oder die Strafverfolgungsbehörden aufweisen, kann daher nicht ohne Weiteres, das heißt nicht ohne entsprechende empirische Erkenntnisse, unterstellt werden, so dass ein unterschiedlicher Nutzen gegenwärtig als Rechtfertigungsgrund ausscheidet.

Ferner ist daran zu denken, dass Daten über finanzielle Transaktionen und über Flüge von Personen schutzwürdiger sein könnten als Telekommunikations-Verkehrsdaten. Dagegen ist die hohe Sensibilität und Aussagekraft von Telekommunikations-Verkehrsdaten anzuführen. Zwar kann man anhand von Flugdaten grobe Bewegungsprofile erstellen. Eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten und damit auch der Mobiltelefon-Positionsdaten ermöglicht die Erstellung von Bewegungsprofilen aber in viel genauerem Maße. Ebenso mögen, was bei Banken gespeicherte Daten angeht, Daten über das Vermögen von Personen besonders sensibel sein. Daten über die Nutzung von Telefon und Internet sind aber nicht weniger sensibel. Dass Telekommunikations-

94 Ebenso Schmitz, MMR 2003, 214 (216) für die Benutzung von Flohmärkten, Supermärkten und Autobahnen.

Verkehrsdaten typischerweise weniger schutzwürdig seien als die anderen genannten Daten, lässt sich daher nicht sagen.

Mithin ist kein sachlicher Grund von solcher Art und solchem Gewicht ersichtlich, dass er die generelle Vorratsspeicherung nur von Telekommunikations-Verkehrsdaten rechtfertigen kann. Die Einführung einer solchen Maßnahme ist daher nach gegenwärtigem Erkenntnisstand mit Art. 3 Abs. 1 GG unvereinbar.

Banken und Fluggesellschaften wurden hier im Übrigen nur beispielhaft heraus gegriffen. Sammlungen personenbezogener Daten existieren auch bei einer Vielzahl anderer Stellen wie etwa Kreditauskunfteien, Direktmarketingfirmen, Anwälten, Steuerberatern, Wirtschaftsprüfern, Krankenhäusern, Hotels, Ärzten, Apotheken und Behörden, ohne dass zugunsten der Eingriffsbehörden Mindestspeicherfristen oder auch nur Zugriffsrechte im Einzelfall vorgesehen sind. Weitergehende Möglichkeiten zur Speicherung potenziell nützlicher Daten sind nahezu unbegrenzt denkbar. So könnte man sämtliche Läden und Geschäfte dazu verpflichten, die Identität ihrer Besucher festzuhalten oder die Videobänder von Überwachungskameras aufzubewahren[95]. Man könnte Bewegungen des Straßenverkehrs registrieren, die Benutzung des öffentlichen Personenverkehrs und die Anwesenheit auf öffentlichen Veranstaltungen. Derartige Pflichten wären jedenfalls für diejenigen Stellen, die Kundendaten ohnehin erfassen und im Fall einer Vorratsspeicherungspflicht nur länger aufbewahren müssten, nicht belastender als es eine Verkehrsdatenspeicherungspflicht für Telekommunikationsunternehmen ist. Zudem scheinen solche Maßnahmen zur Strafverfolgung und Gefahrenabwehr mindestens ebenso geeignet zu sein wie eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten. Überhaupt ist zweifelhaft, ob Telekommunikations-Verkehrsdaten nützlicher sind als jegliche sonstige Daten oder Kenntnisse über das Verhalten der Bevölkerung.

3.3.3.3 Ungleichbehandlung von Telekommunikationsunternehmen gegenüber anderen Unternehmen, z.B. Banken und Fluggesellschaften

Die zuvor diskutierte Ungleichbehandlung lässt sich auch unter dem Blickwinkel derjenigen betrachten, die zur Durchführung einer Vorratsspeicherung von Telekom-

95 APIG, Communications Data, 29.

munikations-Verkehrsdaten verpflichtet wären. Zu vergleichen sind dann Telekommunikationsunternehmen einerseits mit Unternehmen wie Banken und Fluggesellschaften andererseits. Als gemeinsamer Oberbegriff ist die Gruppe der Unternehmen anzusehen, die Leistungen anbieten, bei deren Erbringung Daten anfallen oder gespeichert werden können, welche für die Gefahrenabwehr oder Strafverfolgung nützlich sein können. Die benachteiligende Pflicht zur Vorratsspeicherung knüpft an eine bestimmte Personengruppe an, nämlich an den Beruf des Telekommunikationsdienstleisters, so dass alle der oben genannten Kriterien für eine Verhältnismäßigkeitsprüfung sprechen. Nach dem zuvor Gesagten ist kein sachlicher Grund von solcher Art und solchem Gewicht ersichtlich, dass er die Einführung einer Mindestspeicherungspflicht nur für Telekommunikations-Verkehrsdaten rechtfertigen kann. Die Einführung einer Vorratsspeicherungspflicht ist daher auch wegen ungerechtfertigter Benachteiligung der Telekommunikationsunternehmen gegenüber sonstigen Unternehmen der genannten Art mit Art. 3 Abs. 1 GG unvereinbar.

Schließlich sind die in § 111 TKG genannten Unternehmen auch dadurch in ihrem Grundrecht aus Art. 3 Abs. 1 i.V.m. Art. 12 Abs. 1 GG verletzt, dass sie die Kosten der Datenerhebung entschädigungslos (§ 111 Abs. 1 S. 5 TKG) selbst tragen müssen (vgl. im Einzelnen Breyer, Vorratsspeicherung (2005)[96], Seiten 357-368). Hierin liegt eine Benachteiligung dieser Unternehmen gegenüber den übrigen Steuerzahlern. Die Vergleichbarkeit der Personengruppen ergibt sich daraus, dass beide Gruppen dem Oberbegriff der Gesamtheit steuerpflichtiger Rechtssubjekte zuzuordnen sind.

Es ist kein sachlicher Grund dafür ersichtlich, dass Telekommunikationsunternehmen die Kosten der Erhebung von Kundendaten zu staatlichen Zwecken tragen sollen. Zwar mag es sein, dass nur die in § 111 TKG genannten Unternehmen die Datenerhebung durchführen können. Die Frage der Kostentragungspflicht ist aber hiervon zu trennen, wie auch in der Rechtsprechung anerkannt ist (vgl. im Einzelnen Breyer, Vorratsspeicherung (2005)[97], Seiten 357-368).

§ 111 TKG stellt eine Inpflichtnahme Privater zu öffentlichen Zwecken dar, denn die dort angeordnete Datenerhebung soll "für die Auskunftverfahren nach den §§ 112, 113" TKG erfolgen (§ 111 Abs. 1 S. 1 TKG). Weil diese Auskunftverfahren dem Allgemeininteresse dienen, muss auch die Allgemeinheit für die insoweit entstehenden Kosten aufkommen. Die alleinige Abwälzung der Kosten auf die verpflichteten Unternehmen ist sachlich nicht gerechtfertigt. Weder begründen die Unternehmen durch ihr Angebot eine Quelle besonderer, sozialinadäquater Gefahren, noch entfalten die §§ 111 ff. TKG einen besonderen Nutzen für sie (vgl. im Einzelnen Breyer, Vorratsspeicherung (2005)[98], Seiten 357-368).

[96] Breyer, (Fn. 8).
[97] Breyer, (Fn. 8).
[98] Breyer, (Fn. 8).

Weiterhin trägt das Argument nicht, die Unternehmen könnten ihre Kosten auf den Kunden abwälzen. Selbst wenn man hiervon ausgeht, so wären hierdurch die Kunden gegenüber sonstigen Steuerzahlern benachteiligt. Auch dies ist unter dem Aspekt des Art. 3 Abs. 1 GG nicht gerechtfertigt, denn auch Telekommunikationsnutzer schaffen keine besondere Gefahr und haben keinen besonderen Nutzen von den §§ 111 ff. TKG.

Die relevanten Ausführungen bei Breyer, Vorratsspeicherung (2005)[99], Seiten 357-368 lauten im Einzelnen wie folgt:

Rechtfertigung

Was die Frage der Rechtfertigung anbelangt, so wird teilweise die Auffassung vertreten, eine Inpflichtnahme Privater zu öffentlichen Zwecken, die ohne Kostenerstattung erfolge, sei einer Sonderabgabe vergleichbar und daher nur zulässig, wenn die insoweit vom Bundesverfassungsgericht entwickelten Kriterien vorlägen[100]. Zur Begründung wird vorgetragen, es mache keinen Unterschied, ob der Gesetzgeber Personen entschädigungslos in Anspruch nehme oder ob er eine Kostenerstattung vorsehe und die erstatteten Kosten im Wege einer Sonderabgabe wiederum von den Verpflichteten erhebe[101].

Verkehrsdatenspeicherungspflicht als entschädigungslose Inpflichtnahme Privater zu öffentlichen Zwecken

Die Verpflichtung privater Unternehmen zur Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Behörden stellt eine Inpflichtnahme Privater zu öffentlichen Zwecken dar. Dies gilt unabhängig davon, ob den Unternehmen auch der eigene Zugriff auf die Datenbestände erlaubt ist.

Fraglich ist, ob eine Kostenerstattung oder wenigstens eine Entschädigung der betroffenen Unternehmen für die Vorratsspeicherung vorgesehen ist. Bisher kennt das deutsche Recht eine Entschädigungspflicht bei Auskunftanordnungen von Strafverfolgungsbehörden (§ 23 Abs. 1 S. 1 Nr. 2 JVEG) und von Nachrichtendiensten (§ 20 G10). Nach dem JVEG ist zu entschädigen, wer einem Beweiszwecken

---

[99] Breyer, (Fn. 8).

[100] BeckTKG-Ehmer, § 88, Rn. 51 m.w.N.; Welp, Überwachung und Kontrolle, 136 m.w.N.; „prima facie" auch Schenke, AöR 125 (2000), 1 (39) m.w.N.; a.A. Germann, 576.

[101] BeckTKG-Ehmer, § 88, Rn. 51 m.w.N.; Waechter, VerwArch 87 (1996), 68 (96).

dienenden Ersuchen einer Strafverfolgungsbehörde um Auskunfterteilung nachkommt (§ 23 Abs. 1 S. 1 Nr. 2 JVEG). Nach den §§ 23 Abs. 2, 22 S. 1 JVEG kann für einen dazu eingesetzten Mitarbeiter Aufwendungsersatz in Höhe des gezahlten Gehalts verlangt werden, maximal aber 17 Euro pro Stunde und Mitarbeiter. Auch sonst erforderliche Aufwendungen werden ersetzt (§ 7 Abs. 1 S. 1 JVEG), allerdings nur, wenn sie ohne das Auskunftsersuchen nicht angefallen wären[102]. Die Entschädigung umfasst daher nicht die vorbeugende Vorhaltung von Personal und Einrichtungen[103] und bleibt infolgedessen regelmäßig erheblich hinter den tatsächlichen Kosten zurück[104]. So wird unter anderem für die Nutzung zusätzlicher Rechnerkapazitäten, etwa zur Durchführung einer Zielwahlsuche, keine Entschädigung gewährt[105].

§ 23 Abs. 1 S. 1 Nr. 4 Buchst. b JVEG sieht zwar eine Entschädigungspflicht für den Fall vor, dass Dritte „auf Grund eines Beweiszwecken dienenden Ersuchens der Strafverfolgungsbehörde [...] durch telekommunikationstechnische Maßnahmen die Ermittlung [...] der von einem Telekommunikationsanschluß hergestellten Verbindungen ermöglichen (Zählvergleichseinrichtung)". Man wird dieser Regelung aber keinen Kostenerstattungsanspruch für den Fall einer generellen Verkehrsdatenspeicherungspflicht entnehmen können. Dies würde nicht nur dem historischen Willen des Gesetzgebers, sondern auch dem Wortlaut widersprechen, der darauf abstellt, dass die Ermittlung der Daten erst auf Ersuchen der Strafverfolgungsbehörde, also im Einzelfall, erfolgt und nicht im Wege einer generellen Verkehrsdatenspeicherung. Im Zeitalter digitaler Kommunikation kann man zudem von einer „Zählvergleichseinrichtung" schon begrifflich nicht mehr sprechen.

Auch die Vorschläge des Bundesrats und der RSV-Entwurf sehen keinen Anspruch auf Kostenerstattung vor. Dem ErmittlungsG-Entwurf zufolge sollten umgekehrt Auskünfte nach § 100g StPO – anders als bisher (vgl. § 23 Abs. 1 S. 1 Nr. 2 JVEG) –

---

102 Höver, Rn. 9.2.1.

103 Höver, Rn. 9.2.1; Pernice, DuD 2002, 207 (210); Germann, 575 f.; Koenig/Koch/Braun, K&R 2002, 289 (294).

104 Graf, Jürgen (Generalbundesanwalt), zitiert bei Neumann, Andreas: Internet Service Provider im Spannungsfeld zwischen Strafverfolgung und Datenschutz, Bericht von der Veranstaltung in Bonn am 26./27.02.2002, www.artikel5.de/artikel/-ecoveranstaltung
2002.html; BITKOM: Stellungnahme zur Gesetzesinitiative des Bundesrates vom 31.05.2002 (BR-Drs. 275/02), 12.08.2002, www.bitkom.org/files/documents
www.bundestag.de/gremien15/a09/004Anhoerungen/TKG/materialeingeladene.pdf, 20 (33): die gesetzliche Entschädigung decke durchschnittlich nur 2% der Kosten; ebenso die Deutsche Telekom AG (Fn. 8)., 150 (164); vgl. auch Bundesrat, BR-Drs. 755/03, 35: es sei kein Kostenersatz „in nennenswertem Umfang" vorgesehen.

nicht mehr entschädigungspflichtig sein (Art. 1 Nr. 3 Punkt a.aa.bbb ErmittlungsG-E). In seiner Stellungnahme zur Novelle des Telekommunikationsgesetzes meldet der Bundesrat immerhin Zweifel an, ob die entschädigungslose Inanspruchnahme der Telekommunikationsunternehmen zu Überwachungszwecken verfassungsgemäß ist, und fordert eine Überprüfung der bisherigen Kostentragungsvorschriften[106], ohne aber in seinem zugleich unterbreiteten Vorschlag für eine generelle Verkehrsdatenspeicherungspflicht[107] eine Kostenerstattung vorzusehen.

Rechtfertigung als Sonderabgabe nach der Rechtsprechung des Bundesverfassungsgerichts

Geht man von dem Fehlen eines Kostenerstattungsanspruchs aus, dann richtet sich die Verfassungsmäßigkeit einer generellen Verkehrsdatenspeicherungspflicht der oben dargestellten Meinung zufolge nach den Kriterien für die Zulässigkeit einer Sonderabgabe. Sonderabgaben bedürfen in einem Steuerstaat besonderer sachlicher Rechtfertigung[108]. Als Rechtfertigungsgründe kommen beispielsweise Ausgleichs- oder Lenkungszwecke in Betracht[109]. Wenn allerdings die Inpflichtnahme Privater zur Durchführung einer Verkehrsdatenspeicherung ohne Kostenerstattung erfolgt, so soll dies weder Vorteile ausgleichen, die der Staat oder die Allgemeinheit Telekommunikationsunternehmen gewähren (Ausgleichsfunktion) noch soll es die betroffenen Unternehmen zu einem bestimmten Verhalten anhalten (Lenkungsfunktion). Eine Kostenerstattung unterbleibt vielmehr allein, um dem Staatshaushalt Ausgaben zu ersparen und die Finanzierbarkeit einer generellen Verkehrsdatenspeicherung zu gewährleisten. Damit sind nach der aufgezeigten Meinung die Kriterien für die Zulässigkeit von Sonderabgaben mit Finanzierungsfunktion anzuwenden.

Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Auferlegung von Sonderabgaben mit Finanzierungsfunktion nur dann zulässig, wenn die belastete Gruppe „durch eine gemeinsame, in der Rechtsordnung oder in der gesellschaftlichen Wirklichkeit vorgegebene Interessenlage oder durch besondere gemein-

105 OLG Stuttgart, NStZ 2001, 158; OLG Köln, NStZ-RR 2001, 31.

106 BR-Drs. 755/03, 35 f.

107 BR-Drs. 755/03, 33 f.

108 BVerfG, NVwZ 1996, 469 (471).

109 Zusammenfassend BVerfG, NVwZ 1996, 469 (471).

same Gegebenheiten von der Allgemeinheit und anderen Gruppen abgrenzbar ist"[110], wenn sie dem mit der Abgabenerhebung verfolgten Zweck evident näher steht als jede andere Gruppe oder die Allgemeinheit der Steuerzahler[111], wenn die Aufgabe, die mit Hilfe des Abgabenaufkommens erfüllt werden soll, ganz überwiegend in die Sachverantwortung der belasteten Gruppe fällt und nicht der staatlichen Gesamtverantwortung zuzuordnen ist[112] und wenn die erzielten Mittel entweder gruppennützig verwendet werden oder „die Natur der Sache eine finanzielle Inanspruchnahme der Abgabenpflichtigen zugunsten fremder Begünstigter aus triftigen Gründen eindeutig rechtfertigt"[113].

Die Abgrenzbarkeit der Gruppe der Anbieter von Telekommunikationsdiensten ist zunächst gegeben. Das Kriterium der besonderen Sachnähe dieser Gruppe kann man hingegen nur dann als erfüllt ansehen, wenn die Anbieter von Telekommunikation durch ihr Angebot eine Quelle besonderer Gefahren für bestimmte Rechtsgüter schaffen. Um dies zu begründen, könnte man auf die besonderen Eigenschaften der Telekommunikation verweisen, die sich Kriminelle in vielen Fällen zunutze machen[114]. Daraus ließe sich eine mittelbare Rechtsgutsgefährdung durch das Angebot von Telekommunikation herleiten.

Gegen eine solche Argumentation ist jedoch anzuführen, dass § 9 Abs. 1 TDG deutlich der Gedanke einer prinzipiellen Nichtverantwortlichkeit der Anbieter von Telediensten zugrunde liegt, wenn er bestimmt: „Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie 1. die Übermittlung nicht veranlasst, 2. den Adressaten der übermittelten Informationen nicht ausgewählt und 3. die übermittelten Informationen nicht ausgewählt oder verändert haben. Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem der Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen." Die Begründung zur ursprünglichen Gesetzesfassung führte dazu aus[115]: „Dem Diensteanbieter, der fremde Inhalte lediglich, ohne auf sie Ein-

110 BVerfGE 55, 274 (305 f.).
111 BVerfGE 55, 274 (306).
112 BVerfGE 55, 274 (306).
113 BVerfGE 55, 274 (306).
114 Welp, Überwachung und Kontrolle, 137.
115 BT-Drs. 13/7385, 1 (20).

fluss nehmen zu können, zu dem abrufenden Nutzer durchleitet, obliegt es nicht, für diese Inhalte einzutreten. Er soll nicht anders behandelt werden als ein Anbieter von Telekommunikationsdienstleistungen. Denn der bloße Zugangsvermittler leistet ebenfalls keinen eigenen Tatbeitrag." Die Begründung zur Neufassung stellt fest[116]: „Diese Tätigkeit ist automatischer Art, bei der der Diensteanbieter in der Regel keine Kenntnis über die weitergeleitete oder kurzzeitig zwischengespeicherte Information hat und diese auch nicht kontrolliert. Bei dem automatisiert ablaufenden Prozess trifft der Diensteanbieter im Hinblick auf die Informationen keine eigene Entscheidung. [...] [I]n den Fällen, in denen der Diensteanbieter keine Kontrolle ausübt und keine Kenntnis von der Information haben kann, kann sie ihm auch nicht im Sinne eigener Verantwortlichkeit zugerechnet werden." Diese Ausführungen betreffen zwar unmittelbar nur Teledienste. Die Lage stellt sich bei Telekommunikationsdiensten aber ganz genauso dar[117]. Der Auffassung des Gesetzgebers zufolge sind Betreiber von Telekommunikationsdiensten daher grundsätzlich nicht für die Nutzung ihrer Dienste zu rechtswidrigen Zwecken verantwortlich zu machen.

Die Annahme, dass Telekommunikationsnetze eine besondere Rechtsgutsgefahr darstellten oder erhöhten, ist folglich abzulehnen[118]. Die aus Telekommunikationsnetzen resultierenden Gefahren erscheinen nicht höher als die aus anderen neutralen Tätigkeiten wie Alltagsverrichtungen einer Bank, eines Verkehrs- oder eines Versorgungsunternehmen resultierenden Gefahren. Auch die Tätigkeit eines Automobilherstellers ist beispielsweise kausal dafür, dass Autos als Fluchtfahrzeuge missbraucht werden können, ohne dass man Automobilhersteller deswegen besonders in die Pflicht nehmen dürfte[119]. Ebenso wenig ist es gerechtfertigt, Automobilhändlern die Kosten aufzuerlegen, welche dem Staat durch die Verfolgung von Geschwindigkeitsüberschreitungen entstehen[120]. Nicht anders verhält es sich bei dem Missbrauch von Telekommunikationsnetzen. Solche mit Alltagstätigkeiten

116 BT-Drs. 14/6098, 1 (24).

117 Vgl. BT-Drs. 13/7385, 1 (20).

118 Germann, 576; Werner, Befugnisse der Sicherheitsbehörden, 51; ähnlich Schenke, AöR 125 (2000), 1 (39); für Betreiber von Telekommunikationsanlagen auch Kube/Schütze, CR 2003, 663 (669).

119 So Mobilkom Austria und Telekom Austria in Österr. Verfassungsgerichtshof, G 37/02-16 u.a. vom 27.02.2003, S. 18 f., www.vfgh.gv.at/presse/G37-16-02.pdf.

120 Mobilkom Austria und Telekom Austria in Österr. Verfassungsgerichtshof, G 37/02-16 u.a. vom 27.02.2003, S. 19, www.vfgh.gv.at/presse/G37-16-02.pdf.

verbundene Gefahren sind in den Bereich des allgemeinen Lebensrisikos zu verweisen, der keine besondere Verantwortlichkeit begründen kann[121].

Es kann somit keine Rede davon sein, dass die von einer Vorratsspeicherungspflicht belasteten Unternehmen dem mit der Vorratsspeicherung verfolgten Zweck evident näher stünden als die Allgemeinheit der Steuerzahler. Ebenso wenig fällt die Aufgabe der Strafverfolgung und der Gefahrenabwehr ganz überwiegend in die Sachverantwortung der belasteten Unternehmen[122].

Was das Kriterium der Gruppennützigkeit angeht, so kommt ein Sondernutzen durch eine generelle Verkehrsdatenspeicherung insoweit in Betracht, als sie das Vertrauen der Nutzer stärken und dadurch die Nutzung der Telekommunikationsnetze insgesamt fördern könnte. Dieser Zusammenhang kann allerdings bestenfalls indirekter Art sein, weil er nicht Ziel der Verkehrsdatenspeicherung ist, sondern allenfalls ein möglicher Nebeneffekt. Es ist nicht nur in hohem Maße unsicher, ob eine generelle Verkehrsdatenspeicherung tatsächlich zu einem niedrigeren Kriminalitätsniveau führt. Noch unsicherer ist es, ob sich ein objektiv niedrigeres Kriminalitätsniveau auch auf das subjektive Nutzervertrauen und letztlich auf das Maß an Inanspruchnahme der Telekommunikationsnetze durchschlägt. Umgekehrt gibt es Untersuchungen, die auf die Abwesenheit eines solchen Zusammenhangs hindeuten. Die genannte These ist daher mit so vielen Unsicherheitsfaktoren behaftet, dass sie – vorbehaltlich neuer Forschungserkenntnisse – abzulehnen ist[123].

Zu überlegen ist außerdem, ob eine generelle Verkehrsdatenspeicherung in besonderem Maße Betreiber von an Telekommunikationsnetze angeschlossenen Computersystemen, insbesondere Betreiber von Internet-Servern, schützt. Allein diese Personengruppe ist nämlich von Netzkriminalität im engeren Sinne betroffen. Dieser Zusammenhang rechtfertigt eine Sonderbelastung der Betreiber solcher Systeme allerdings nur dann, wenn diese Systeme störanfälliger und kriminalitätsgefährdeter sind als andere Anlagen. Nur in diesem Fall dürfen die Kosten von Maßnahmen, die über den Schutz der Allgemeinheit hinaus gehen, anteilig auf

---

121 Weichert, Terrorismusbekämpfungsgesetze (I), Punkt I.

122 Im Ergebnis auch BITKOM: Stellungnahme zur Gesetzesinitiative des Bundesrates vom 31.05.2002 (BR-Drs. 275/02), 12.08.2002, www.bitkom.org/files/documents/Position_BITKOM_Vorratsdatenspeicherung_u.a._12.08.2002.pdf, 9.

123 Im Ergebnis auch Schenke, AöR 125 (2000), 1 (39).

die Serverbetreiber abgewälzt werden. Soweit Serverbetreiber von Maßnahmen nicht in besonderer Weise profitieren, sind die Kosten dagegen von der Allgemeinheit zu tragen[124]. Letztlich kann die Frage im vorliegenden Zusammenhang offen bleiben, weil von einer generellen Verkehrsdatenspeicherung keine merkliche Schutzwirkung zugunsten der Betreiber von Servern zu erwarten ist. Einen wirksamen Schutz auf diesem Gebiet erlauben nur technisch-organisatorische Maßnahmen der Betreiber selbst.

Für andere Personen oder Unternehmen, die zu einer Vorratsspeicherung verpflichtet wären, ist ein möglicher Sondernutzen von vornherein nicht zu erkennen. Telefongesellschaften und Internet-Provider etwa sind Netzkriminalität im engeren Sinne grundsätzlich nicht ausgesetzt, weil ihre Einrichtungen für Computerangriffe regelmäßig unzugänglich sind. Auch sonst ist ein Sondernutzen für diese Gruppe nicht zu erkennen, so dass eine entschädigungslose Inanspruchnahme der betroffenen Unternehmen zugunsten der Allgemeinheit durchweg ungerechtfertigt ist.

Soweit das Bundesverfassungsgericht Unternehmen auf die Möglichkeit einer Abwälzung von Kosten auf ihre Kunden verweist, ist es denkbar, die Kriterien der besonderen Sachnähe und der Gruppennützigkeit auf die Telekommunikationsnutzer anzuwenden, welche die Kosten einer generellen Verkehrsdatenspeicherung letztlich zu tragen haben[125]. Tut man dies, so gelangt man zu dem Ergebnis, dass auch auf Seiten der Telekommunikationsnutzer keine spezifische Nähe zu dem Missbrauch von Telekommunikationseinrichtungen durch einzelne unter ihnen vorliegt[126]. Von einer besonderen Gruppennützigkeit lässt sich ebenso wenig sprechen[127].

Überhaupt sind kaum Menschen denkbar, die sich jeglicher Telekommunikation enthalten, so dass schon fraglich ist, ob man hier von einer bestimmten Gruppe sprechen kann. In seiner Kohlepfennig-Entscheidung hat das Bundesverfassungsgericht argumentiert, das Interesse an einer funktionsfähigen Energieversorgung sei ein Allgemeininteresse, das nicht im Wege einer Sonderabgabe, sondern nur

---

124 Vgl. BVerwGE 112, 194 (205).

125 BeckTKG-Ehmer, § 88, Rn. 54 m.w.N.; der Sache nach wohl auch Pernice, Ina (Deutscher Industrie- und Handelskammertag) in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 14.

126 BeckTKG-Ehmer, § 88, Rn. 54; Welp, Überwachung und Kontrolle, 137.

127 Welp, Überwachung und Kontrolle, 137.

durch Steuermittel befriedigt werden dürfe[128]. Auch in der Feuerwehrabgabenentscheidung heißt es: „Das Feuerwehrwesen ist eine öffentliche Angelegenheit, deren Lasten nur die Allgemeinheit treffen dürfen und die deshalb [...] nur mit von der Allgemeinheit zu erbringenden Mitteln, im Wesentlichen also durch die Gemeinlast Steuer, finanziert werden darf (vgl. BVerfGE 55, 274 [306]; 82, 159 [180]). Wird in einem solchen Fall nur ein abgegrenzter Personenkreis mit der Abgabe belastet, so verstößt dies auch gegen den allgemeinen Gleichheitssatz nach Art. 3 Abs. 1 GG (vgl. auch BVerfGE 9, 291 [301])."[129] Diese Ausführungen gelten grundsätzlich auch für die Inpflichtnahme Privater im Bereich der Telekommunikation[130]. Sinngemäß haben dies der französische Verfassungsgerichtshof im Dezember 2000[131] und der österreichische Verfassungsgerichtshof im Februar 2003[132] bereits entschieden. Auch in Italien und den USA trägt der Staat die Kosten für die Vorhaltung von Überwachungseinrichtungen durch Privatunternehmen[133]. Kommt eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten danach hauptsächlich der Allgemeinheit zugute, dann dürfen ihre Kosten auch nicht allein den betroffenen Unternehmen oder ihren Kunden auferlegt werden.

Gemessen an den Kriterien für die Zulässigkeit einer Sonderabgabe ist es demnach unzulässig, die Telekommunikationsanbieter zur Finanzierung einer generellen Verkehrsdatenspeicherung heranzuziehen.

Anwendung auf tatsächliche Inpflichtnahmen

Fraglich ist, ob hieraus zwangsläufig auch die Unzulässigkeit ihrer entschädigungslosen Heranziehung zur Mitwirkung bei einer generellen Verkehrsdatenspeicherung folgt. Das Bundesverfassungsgericht wendet die Kriterien für die Zulässigkeit einer Sonderabgabe nicht auf tatsächliche Inpflichtnahmen Privater zu öffentlichen Zwecken an. In solchen Fällen prüft es nur die Verhältnismäßigkeit der

128 BVerfGE 91, 186 (206); vgl. schon BVerfGE 23, 12 (23); ähnlich für Betreiber elektrischer und elektronischer Geräte BVerwGE 112, 194 (205).

129 BVerfGE 92, 91 (121).

130 BeckTKG-Ehmer, § 88, Rn. 55.

131 Conseil constitutionnel, 2000-441 DC vom 28.12.2000, www.conseil-constitutionnel.fr/decision/2000/2000441/2000441dc.htm.

132 Österr. Verfassungsgerichtshof, G 37/02-16 u.a. vom 27.02.2003, www.vfgh.gv.at/presse/G37-16-02.pdf.

133 wik-Consult, Studie (I), 41, 50 und 89.

Inpflichtnahme[134]. Für eine enge Auslegung der Rechtsprechung zu Sonderabgaben spricht, dass sich diese auf das Argument stützt, dass das Grundgesetz grundsätzlich abschließend regele, auf welche Weise der Staat Einnahmen erzielen dürfe[135]. Dieser Gesichtspunkt trifft auf die tatsächliche Inpflichtnahme Privater nicht zu, weil der Staat auf diese Weise keine Einnahmen erzielt.

Ein weiteres Argument, welches das Bundesverfassungsgericht in Bezug auf Sonderabgaben heran zieht, ist demgegenüber ohne weiteres auf Inpflichtnahmen Privater übertragbar. Der Grundsatz der Vollständigkeit des Haushaltsplans[136], welcher die Transparenz der Kosten staatlicher Aktivitäten und die Überschaubarkeit und Kontrolle der dem Bürger auferlegten Lasten gewährleisten soll, ist nämlich in beiden Fällen beeinträchtigt[137].

Ein Grund für die Zurückhaltung des Bundesverfassungsgerichts bei der Ausweitung seiner Rechtsprechung zu Sonderabgaben mag darin liegen, dass die staatliche Inpflichtnahme Privater zu öffentlichen Zwecken weit verbreitet ist und eine restriktive verfassungsrechtliche Beurteilung daher weitreichende Konsequenzen hätte[138]. Beispiele solcher Pflichten sind die Inanspruchnahme der Banken zum Abzug der Kapitalertragssteuer, die Heranziehung der Arbeitgeber zum Lohnsteuerabzug und zur Abführung von Sozialversicherungsbeiträgen, die Verpflichtung von Versicherungsunternehmen zur Einbehaltung der Versicherungssteuer und die Auferlegung von Bevorratungspflichten für Ölimporteure[139]. Eine besondere Verantwortlichkeit wegen Schaffung einer Gefahrenquelle ließe sich wohl in keinem dieser Fälle begründen.

Für eine Gleichbehandlung beider Fälle kann man geltend machen, dass eine Inanspruchnahme Privater ohne Kostenerstattung einer Inanspruchnahme mit Kostenerstattung, bei der die erstatteten Kosten im Wege einer Sonderabgabe von den Verpflichteten wieder erhoben werden, gleich kommt[140]. Weiter kann man anführen, dass die Inpflichtnahme Privater in Verbindung mit der aus einer

134 Etwa BVerfGE 30, 292 (315).

135 BVerfGE 55, 274 (299 f.) spricht von einer Gefahr der Aushöhlung der Finanzverfassung durch Sonderabgaben.

136 BVerfG, NVwZ 1996, 469 (471).

137 Elicker, NVwZ 2003, 304 (306).

138 Vgl. VG Köln, CR 2000, 747 (750).

139 Beispiele nach BVerfGE 73, 102 (119 f.).

Sonderabgabe finanzierten Kostenerstattung den betroffenen Unternehmen eher zumutbar sein kann als eine entschädigungslose Inpflichtnahme ohne Sonderabgabe. Das gilt insbesondere deswegen, weil eine Sonderabgabe Ausnahmen für besonders hart betroffene Unternehmen zulassen kann, ohne zu Effektivitätseinbußen zu führen. So kann man beispielsweise kleine Internet-Access-Provider von einer Sonderabgabe zur Finanzierung einer generellen Verkehrsdatenspeicherung ausnehmen, während ihre Befreiung von der Speicherungspflicht selbst nicht ohne Effektivitätseinbußen möglich ist. Kann damit aber die Auferlegung einer Sonderabgabe für die Gruppe der Betroffenen insgesamt weniger belastend sein, dann können für die Zulässigkeit einer Sonderabgabe auch keine strengeren Kriterien gelten als für die Zulässigkeit einer entschädigungslosen Inpflichtnahme.

Es ist demnach überzeugender, beide Fälle gleich zu behandeln[141]. Ein durchgreifender sachlicher Grund für eine Unterscheidung ist nicht ersichtlich. Dies gilt gerade für eine Vorratsspeicherungspflicht, deren Schwerpunkt nicht in der Auferlegung von Hilfsdiensten liegt – die Speicherung von Telekommunikations-Verkehrsdaten könnte der Staat auch selbst vornehmen – sondern in der Abwälzung der hohen, damit verbundenen Kosten.

Gemeinsame Rechtfertigungskriterien

Sind Sonderabgaben und entschädigungslose Inpflichtnahmen somit gleich zu behandeln, so bedeutet dies noch nicht, dass die engen Kriterien des Bundesverfassungsgerichts zur Zulässigkeit von Sonderabgaben zu akzeptieren sind. Vielmehr kann die verbreitete Inpflichtnahme Privater umgekehrt Anlass sein, auch die finanzielle Heranziehung Privater im Wege von Sonderabgaben in höherem Maße zuzulassen als es das Bundesverfassungsgericht bisher tut.

Schon die Abgrenzung der „Sonderabgaben" von den Steuern ist nicht unproblematisch[142]. Wann das Bundesverfassungsgericht eine Geldleistungspflicht als Sonderabgabe ansieht und dementsprechend strenge Kriterien anwendet, lässt sich nicht eindeutig vorhersehen. Nach § 3 AO sind Steuern „Geldleistungen, die nicht eine Gegenleistung für eine besondere Leistung darstellen und von einem

---

140 Vgl. Nachweise auf Seite 64, Fn. 100.

141 So auch Friedrich, Verpflichtung, 184 m.w.N.; Friauf, FS Jahrreiß, 45 (56 f.); Waechter, VerwArch 87 (1996), 68 (76); Elicker, NVwZ 2003, 304 (306); a.A. VG Köln, CR 2000, 747 (750).

öffentlich-rechtlichen Gemeinwesen zur Erzielung von Einnahmen allen auferlegt werden, bei denen der Tatbestand zutrifft, an den das Gesetz die Leistungspflicht knüpft; die Erzielung von Einnahmen kann Nebenzweck sein." Worin sich hiervon eine Sonderabgabe unterscheiden soll, ist nicht ersichtlich.

Zwar mag der Kreis der von einer Sonderabgabe Betroffenen klein sein. Das kann aber auch bei besonderen Steuern der Fall sein (z.B. Spielbankenabgabe). Es kann legitime Gründe dafür geben, einem kleinen Personenkreis eine besondere Abgabenlast aufzuerlegen. Im heutigen Zeitalter der Globalisierung kann etwa der Gesichtspunkt maßgeblich sein, dass Rechtssubjekte einer bestimmten Besteuerung nicht durch Ausweichen in das Ausland entgehen können. Ein weiterer Gesichtspunkt kann die besondere Leistungsfähigkeit einzelner Steuersubjekte sein, etwa wenn deren Tätigkeit besonders profitabel ist. Weiterhin kann vorrangig eine Lenkungswirkung angestrebt sein, die es erforderlich macht, gerade bestimmte Personen in Anspruch zu nehmen.

Festzuhalten bleibt, dass es nicht gerechtfertigt ist, die Zulässigkeit der Inanspruchnahme einzelner Personen davon abhängig zu machen, ob diesen Personen aufgrund ihrer spezifischen Sachnähe eine Kostenverantwortung zugeteilt werden kann und ob die Einnahmen gruppennützig verwendet werden. Stattdessen sind die allgemeinen Kriterien über die Zulässigkeit von Steuern anzuwenden, die vornehmlich auf die Verhältnismäßigkeit der Belastung[143] und auf die Gleichmäßigkeit der Besteuerung[144] abstellen. Diese Kriterien sind sowohl in Fällen von Sonderabgaben wie auch in Fällen der tatsächlichen Inpflichtnahme Privater zu öffentlichen Zwecken anzuwenden, da sich diese beiden Fallgruppen – wie oben dargelegt – nicht maßgeblich unterscheiden.

Rechtfertigung im Fall einer Vorratsspeicherung

Im vorliegenden Zusammenhang ist daher eine Prüfung des allgemeinen Gleichheitssatzes vorzunehmen[145]. In Bezug auf den Rechtfertigungsmaßstab liegt eine

142 BVerfGE 50, 274 (300): „Abgrenzungsprobleme"; BVerfG, NVwZ 1996, 469 (471): „große Ähnlichkeit".

143 BVerfGE 91, 207 (221).

144 BVerfGE 66, 214 (223): „Gebot der Steuergerechtigkeit".

145 Vgl. auch Friedrich, Verpflichtung, 174 für die Vorhaltung von Überwachungseinrichtungen.

eindeutige Anknüpfung an Personengruppen – nämlich an die Gruppe der Telekommunikationsunternehmen – und nicht nur an Sachverhalte vor. Wie gezeigt, greift eine Pflicht zur Vorratsspeicherung von Telekommunikations-Verkehrsdaten ohne Kostenerstattung auch intensiv in das Grundrecht der Telekommunikationsunternehmen aus Art. 12 Abs. 1 GG ein. Es ist daher eine Verhältnismäßigkeitsprüfung vorzunehmen. Das Gleiche gilt, wenn man auf die Kunden der Telekommunikationsunternehmen abstellt.

Die tatsächliche Inpflichtnahme Privater hat das Bundesverfassungsgericht mitunter damit gerechtfertigt, dass die normativ vorgeschriebene Tätigkeit an diejenige Tätigkeit angelehnt sei, die eine Person ohnehin verrichte[146]. In der Tat mag es volkswirtschaftlich gesehen Sinn machen, Telekommunikationsunternehmen zur Durchführung der Telekommunikationsüberwachung zu verpflichten anstatt ein kompliziertes staatliches Einsatzsystem aufzubauen. Dieser Einsparungseffekt ist allerdings auch dann zu erzielen, wenn den betroffenen Unternehmen ihre Kosten erstattet werden, so dass die bloße Tatsache der Berufsnähe keine entschädigungslose Inpflichtnahme rechtfertigt.

Nach dem oben Gesagten ist auch sonst kein Grund ersichtlich, der nach Art und Gewicht die Belastung der beteiligten Unternehmen oder mittelbar ihrer Kunden mit den Kosten einer Verkehrsdatenspeicherung zu staatlichen Zwecken rechtfertigen kann. Die Abwehr von Gefahren und die Ahndung von Straftaten ist eine Aufgabe der Allgemeinheit, deren Lasten nur die Allgemeinheit treffen dürfen und die deshalb im Wesentlichen nur mit Steuermitteln finanziert werden darf[147]. Eine abweichende Regelung im Zusammenhang mit einer Vorratsspeicherungspflicht für Telekommunikations-Verkehrsdaten ist mit Art. 3 Abs. 1 GG unvereinbar. [148]

3.4 §§ 112, 113 TKG

Die §§ 112, 113 TKG lauten wie folgt:

§ 112 Automatisiertes Auskunftsverfahren

---

146 BVerfGE 30, 292 (324 f.).

147 Friedrich, Verpflichtung, 183 m.w.N.; allgemein für Staatsaufgaben BVerfGE 23, 12 (23).

148 So auch Schmidt-Preuß in Gutachten zur TKUe-Entschädigung, www.bitkom.org/files/documents/050506 Gutachten TKUe -Entschädigung.pdf

(1) Wer Telekommunikationsdienste für die Öffentlichkeit erbringt, hat die nach § 111 Abs. 1 Satz 1 und 3 und Abs. 2 erhobenen Daten unverzüglich in Kundendateien zu speichern, in die auch Rufnummern und Rufnummernkontingente, die zur weiteren Vermarktung oder sonstigen Nutzung an andere Anbieter von Telekommunikationsdiensten vergeben werden, sowie bei portierten Rufnummern die aktuelle Portierungskennung aufzunehmen sind. Für die Berichtigung der Kundendateien gilt § 111 Abs. 1 Satz 3 und 4 entsprechend. In Fällen portierter Rufnummern sind die Rufnummer und die zugehörige Portierungskennung erst nach Ablauf des Jahres zu löschen, das dem Zeitpunkt folgt, zu dem die Rufnummer wieder an den Netzbetreiber zurückgegeben wurde, dem sie ursprünglich zugeteilt worden war. Der Verpflichtete hat zu gewährleisten, dass

1. *die Regulierungsbehörde für Auskunftsersuchen der in Absatz 2 genannten Stellen jederzeit Daten aus den Kundendateien automatisiert im Inland abrufen kann,*
2. *der Abruf von Daten unter Verwendung unvollständiger Abfragedaten oder die Suche mittels einer Ähnlichenfunktion erfolgen kann.*

Die ersuchende Stelle hat unverzüglich zu prüfen, inwieweit sie die Daten, die als Antwort geliefert werden, benötigt und nicht benötigte Daten unverzüglich zu löschen. Der Verpflichtete hat durch technische und organisatorische Maßnahmen sicherzustellen, dass ihm Abrufe nicht zur Kenntnis gelangen können.
(2) Auskünfte aus den Kundendateien nach Absatz 1 werden

1. *den Gerichten und Strafverfolgungsbehörden,*
2. *den Polizeivollzugsbehörden des Bundes und der Länder für Zwecke der Gefahrenabwehr,*
3. *dem Zollkriminalamt und den Zollfahndungsämtern für Zwecke eines Strafverfahrens sowie dem Zollkriminalamt zur Vorbereitung und Durchführung von Maßnahmen nach § 39 des Außenwirtschaftsgesetzes,*
4. *den Verfassungsschutzbehörden des Bundes und der Länder, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst,*
5. *den Notrufabfragestellen nach § 108 sowie der Abfragestelle für die Seenotrufnummer 124 124,*
6. *der Bundesanstalt für Finanzdienstleistungsaufsicht sowie*
7. *den nach Landesrecht für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 4 Abs. 3 des Gesetzes zur Bekämpfung der Schwarzarbeit zuständigen Behörden über zentrale Abfragestellen*

nach Absatz 4 jederzeit erteilt, soweit die Auskünfte zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind und die Ersuchen an die Regulierungsbehörde im automatisierten Verfahren vorgelegt werden.
(3) Das Bundesministerium für Wirtschaft und Arbeit wird ermächtigt, im Einvernehmen mit dem Bundeskanzleramt, dem Bundesministerium des Innern, dem Bundesministerium der Justiz, dem Bundesministerium der Finanzen sowie dem Bundesministerium der Verteidigung eine Rechtsverordnung mit Zustimmung des Bundesrates zu erlassen, in der geregelt werden

1. *die wesentlichen Anforderungen an die technischen Verfahren*
   a) zur Übermittlung der Ersuchen an die Regulierungsbehörde,
   b) zum Abruf der Daten durch die Regulierungsbehörde von den Verpflichteten einschließlich der für die Abfrage zu verwendenden Datenarten und

c) zur Übermittlung der Ergebnisse des Abrufs von der Regulierungsbehörde an die ersuchenden Stellen,

2. *die zu beachtenden Sicherheitsanforderungen sowie*
3. *für Abrufe mit unvollständigen Abfragedaten und für die Suche mittels einer Ähnlichenfunktion, für die die Vorgaben für die in die Suche einzubeziehenden Zeichenfolgen von den an der Rechtsverordnung zu beteiligenden Ministerien bereitgestellt werden,*

   a) die Mindestanforderungen an den Umfang der einzugebenden Daten zur möglichst genauen Bestimmung der gesuchten Person,

   b) der zulässige Umfang der an die ersuchende Stelle zu übermittelnden Treffer und

   c) die Anforderungen an die Löschung der nicht benötigten Daten.

Im Übrigen können in der Verordnung auch Einschränkungen der Abfragemöglichkeit für die in Absatz 2 Nr. 5 bis 7 genannten Stellen auf den für diese Stellen erforderlichen Umfang geregelt werden. Die technischen Einzelheiten des automatisierten Abrufverfahrens gibt die Regulierungsbehörde in einer unter Beteiligung der betroffenen Verbände und der berechtigten Stellen zu erarbeitenden Technischen Richtlinie vor, die bei Bedarf an den Stand der Technik anzupassen und von der Regulierungsbehörde in ihrem Amtsblatt bekannt zu machen ist. Der Verpflichtete nach Absatz 1 und die berechtigten Stellen haben die Anforderungen der Technischen Richtlinie spätestens ein Jahr nach deren Bekanntmachung zu erfüllen. Nach dieser Richtlinie gestaltete mängelfreie technische Einrichtungen müssen im Falle einer Änderung der Richtlinie spätestens drei Jahre nach deren Inkrafttreten die geänderten Anforderungen erfüllen.
(4) Auf Ersuchen der in Absatz 2 genannten Stellen hat die Regulierungsbehörde die entsprechenden Datensätze aus den Kundendateien nach Absatz 1 abzurufen und an die ersuchende Stelle zu übermitteln. Sie prüft die Zulässigkeit der Übermittlung nur, soweit hierzu ein besonderer Anlass besteht. Die Verantwortung für die Zulässigkeit der Übermittlung tragen die in Absatz 2 genannten Stellen. Die Regulierungsbehörde protokolliert für Zwecke der Datenschutzkontrolle durch die jeweils zuständige Stelle bei jedem Abruf den Zeitpunkt, die bei der Durchführung des Abrufs verwendeten Daten, die abgerufenen Daten, die die Daten abrufende Person sowie die ersuchende Stelle und deren Aktenzeichen. Eine Verwendung der Protokolldaten für andere Zwecke ist unzulässig. Die Protokolldaten sind nach einem Jahr zu löschen.
(5) Der Verpflichtete nach Absatz 1 hat alle technischen Vorkehrungen in seinem Verantwortungsbereich auf seine Kosten zu treffen, die für die Erteilung der Auskünfte nach dieser Vorschrift erforderlich sind. Dazu gehören auch die Anschaffung der zur Sicherstellung der Vertraulichkeit und des Schutzes vor unberechtigten Zugriffen erforderlichen Geräte, die Einrichtung eines geeigneten Telekommunikationsanschlusses und die Teilnahme an dem geschlossenen Benutzersystem sowie die laufende Bereitstellung dieser Vorkehrungen nach Maßgaben der Rechtsverordnung und der Technischen Richtlinie nach Absatz 3. Eine Entschädigung für im automatisierten Verfahren erteilte Auskünfte wird den Verpflichteten nicht gewährt.

§ 113 Manuelles Auskunftsverfahren
(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, hat im Einzelfall den zuständigen Stellen auf deren Verlangen unverzüglich Auskünfte über die nach den §§ 95 und 111 erhobenen Daten zu erteilen, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Si-

cherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes erforderlich ist. Auskünfte über Daten, mittels derer der Zugriff auf Endgeräte oder in diesen oder im Netz eingesetzte Speichereinrichtungen geschützt wird, insbesondere PIN oder PUK, hat der nach Satz 1 Verpflichtete auf Grund eines Auskunftsersuchens nach § 161 Abs. 1 Satz 1, § 163 Abs. 1 der Strafprozessordnung, der Datenerhebungsvorschriften der Polizeigesetze des Bundes oder der Länder zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung, § 8 Abs. 1 des Bundesverfassungsschutzgesetzes, der entsprechenden Bestimmungen der Landesverfassungsschutzgesetze, § 2 Abs. 1 des BND-Gesetzes oder § 4 Abs. 1 des MAD-Gesetzes zu erteilen; an andere öffentliche oder nicht öffentliche Stellen dürfen diese Daten nicht übermittelt werden. Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen, ist nur unter den Voraussetzungen der hierfür einschlägigen gesetzlichen Vorschriften zulässig. Über die Auskunftserteilung hat der Verpflichtete gegenüber seinen Kundinnen und Kunden sowie Dritten gegenüber Stillschweigen zu wahren.
(2) Der Verpflichtete nach Absatz 1 hat die in seinem Verantwortungsbereich für die Auskunftserteilung erforderlichen Vorkehrungen auf seine Kosten zu treffen. Im Falle einer Auskunftserteilung wird dem Verpflichteten durch die ersuchende Stelle eine Entschädigung gewährt, deren Umfang sich abweichend von § 17a Abs. 1 Nr. 2 des Gesetzes über die Entschädigung von Zeugen und Sachverständigen nach der Rechtsverordnung nach § 110 Abs. 9 bemisst. Satz 2 gilt auch in den Fällen, in denen im manuellen Auskunftsverfahren lediglich Daten erfragt werden, die der Verpflichtete auch für den Abruf im automatisierten Auskunftsverfahren nach § 112 bereithält. Satz 2 gilt nicht in den Fällen, in denen die Auskunft im automatisierten Auskunftsverfahren nach § 112 nicht vollständig oder nicht richtig erteilt wurde.

3.4.1 Art. 10 GG

3.4.1.1 Schutzbereich

Dass der Schutzbereich des Fernmeldegeheimnisses Bestandsdaten erfasst, ergibt sich aus den Ausführungen zum Schutz von Bestandsdaten auf den Seiten 10 bis 13, auf die Bezug genommen wird.

3.4.1.2 Eingriff

Für § 12 FAG hat das Bundesverfassungsgericht bereits festgestellt, dass Normen, welche Telekommunikationsunternehmen zur Auskunfterteilung über nach Art. 10 GG geschützte Daten an staatliche Stellen verpflichten, einen Eingriff in dieses Grundrecht darstellen (vgl. BVerfG, 1 BvR 330/96 vom 12.3.2003, Absatz-Nr. 55, http://www.bverfg.de/entscheidungen/rs20030312_1bvr033096.html). Nicht anders verhält es sich bei den §§ 112, 113 TKG.

3.4.1.3 Rechtfertigung

Dieser Eingriff in Art. 10 GG ist schon deswegen verfassungswidrig, weil die §§ 112, 113 TKG nicht das eingeschränkte Grundrecht unter Angabe des Artikels nennen, wie es Art. 19 Abs. 1 S. 2 GG vorschreibt.

Darüber hinaus sind die §§ 112, 113 TKG auch wegen Verstoßes gegen das Verhältnismäßigkeitsgebot verfassungswidrig. Die von den §§ 112, 113 TKG geschaffenen Zugriffsrechte einer Vielzahl staatlicher Stellen "zur Erfüllung ihrer gesetzlichen Aufgaben" sind nicht durch überwiegende Allgemeininteressen gerechtfertigt (vgl. zu diesem Kriterium BVerfGE 65, 1 [44, 46]), sondern ihr möglicher Nutzen steht klar außer Verhältnis zu ihren negativen Auswirkungen auf die Grundrechtsträger. Zur Begründung wird auf die Ausführungen bei Breyer, RDV 2003, 218 (219 f.) und RDV 2004, 147 (151) verwiesen, wobei die zentralen Argumente die folgenden sind:

- Ernsthafte Kriminelle werden regelmäßig ausländische Telekommunikationsdienste oder Verträge, die auf andere Personen registriert sind, nutzen. Gegen sie sind die §§ 112, 113 TKG daher nicht wirksam.
- Der Gesetzgeber hat keine Vorkehrungen getroffen, um eine Evaluierung der §§ 112, 113 TKG zu ermöglichen. Dass sie in nennenswertem Maß dem Schutz von Rechtsgütern dienen, ist daher nicht erkennbar.
- Die §§ 112, 113 TKG sehen keine Eingriffsschwelle vor. Insbesondere ist der Zugriff nicht nur zur Vorbereitung der Telekommunikationsüberwachung zulässig. Vielmehr ist keinerlei Zusammenhang mit der Telekommunikation vorausgesetzt.
- Die §§ 112, 113 TKG enthalten keine Subsidiaritätsklausel, so dass die Bestandsdatendateien von den zugriffsberechtigten Behörden als Adresskartei und Telefonauskunft missbraucht werden können.
- Die Reihenabfrage einer Vielzahl von Datensätzen mittels "Jokerzeichen" ist nach § 112 Abs. 1 S. 4 Nr. 2 TKG zulässig.

- Im Jahr 2002 sind etwa 2 Mio. Zugriffe im Wege des automatischen Abrufverfahrens erfolgt. Seit dem Jahr 2000 hat sich die Anzahl der Zugriffe jedes Jahr um 50% Jahr erhöht.
- § 113 TKG verpflichtet auch zur Auskunft über Daten, mittels derer auf Telekommunikationsinhalte und -umstände zugegriffen werden kann. Er nimmt selbst solche Daten nicht aus, die ausschließlich dazu dienen, auf Telekommunikationsinhalte und -umstände zuzugreifen (z.B. PIN für einen elektronischen Anrufbeantworter).

Daneben liegt auch ein Verstoß gegen die grundrechtliche Pflicht zur Benachrichtigung der Betroffenen vor (siehe näher Breyer, RDV 2003, 218 [220]). Der Gesetzgeber unterlässt es nicht nur, eine Benachrichtigung Betroffener von staatlichen Zugriffen zu gewährleisten, selbst wenn die Benachrichtigung keine Rechtsgüter gefährden würde. Er verhindert mit § 112 Abs. 1 S. 6, Abs. 4 S. 5 und 6 und § 113 Abs. 1 S. 4 TKG selbst eine Auskunfterteilung auf Anfrage der Betroffenen. Hält man Art. 10 GG insoweit nicht für einschlägig, so ist jedenfalls Art. 19 Abs. 4 GG verletzt.

Sodann fehlt in den §§ 112, 113 TKG die verfassungsrechtlich gebotene (BVerfGE 65, 1 [46]) Anordnung, dass die Verwendung erlangter Daten nur zur Verfolgung derjenigen Zwecke zulässig ist, zu deren Erreichung die Daten nach dem Gesetz erhoben werden durften (Zweckbindungsgebot).

Außerdem fehlt es, von § 112 Abs. 4 TKG abgesehen, an der verfassungsrechtlich gebotenen (BVerfGE 100, 313 [395 f.]) Anordnung der Protokollierung jeder Erhebung, Verwendung, Übermittlung und Vernichtung von Telekommunikations-Bestandsdaten.

Weiterhin liegt ein Verstoß gegen den Parlamentsvorbehalt und das Gebot der Normenklarheit vor, weil die §§ 112, 113 TKG das Ausmaß der Eingriffsermächtigung nicht gemessen an der Eingriffsintensität hinreichend detailliert regeln. So ist nicht festgelegt, welche Angaben Suchanfragen enthalten müssen und über wie viele Personen Auskunft verlangt werden darf. Wegen der Grundrechtswesentlichkeit dieser Frage ist ihre Regelung in einer Rechtsverordnung (§ 112 Abs. 3 TKG) nicht ausreichend. Für § 113 TKG ist nicht einmal eine Regelung durch Rechtsverordnung vorgesehen. Zudem benennt § 113 TKG nicht die Stellen, an die Auskunft zu erteilen ist.

Schließlich liegt ein schwerwiegender Verstoß gegen das Gebot der Normenklarheit darin, dass § 112 TKG die Weitergabe personenbezogener Daten an bestimmte Behörden pauschal "zur Erfüllung ihrer gesetzlichen Aufgaben" erlaubt (vgl. BVerfGE 65, 1 [66 f.] zu einer vergleichbaren Formulierung), anstatt klar festzulegen, "um welche konkreten, klar definierten Zwecke es sich dabei handelt" (BVerfG ebenda).

Die relevanten Ausführungen bei Breyer, RDV 2003, 218 (219 ff.) lauten im Einzelnen wie folgt:

> **Der staatliche Zugriff auf Bestandsdaten**
>
> Konsequenz daraus ist zunächst, dass in den Normen, die den staatlichen Zugriff auf Bestandsdaten regeln (§§ 89 Abs. 6, 90 TKG und §§ 107-108 TKG-RefE), Art. 10 GG zu zitieren ist. Darüber hinaus sollte die grundsätzliche Gleichstellung

der Bestandsdaten mit Verbindungsdaten Anlass geben, die Verhältnismäßigkeit des bisher ohne Eingriffsschwelle zulässigen Zugriffs auf Bestandsdaten zu überprüfen. Die genannten Vorschriften verpflichten Telekommunikationsanbieter nämlich bisher zur Auskunfterteilung über Bestandsdaten zur Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung und zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes. Daneben dürfen folgende Stellen kostenfrei im Wege eines weltweit einzigartigen[149] automatischen Online-Abrufverfahrens auf Bestandsdaten zugreifen: Gerichte, Staatsanwaltschaften, andere Justizbehörden, sonstige Strafverfolgungsbehörden, Polizeien des Bundes und der Länder für Zwecke der Gefahrenabwehr, Zollfahndungsämter für Zwecke von Strafverfahren, das Zollkriminalamt zur Vorbereitung und Durchführung von Abhörmaßnahmen, die Verfassungsschutzbehörden des Bundes und der Länder, der Militärischen Abschirmdienst sowie der Bundesnachrichtendienst zur Wahrnehmung sämtlicher ihrer Aufgaben. § 108 TKG-RefE will dieser Liste Einrichtungen, die Notrufe bearbeiten, die Bundesanstalt für Finanzdienstleistungsaufsicht und die für die Verfolgung und Ahndung von Schwarzarbeit zuständigen Behörden hinzufügen.

Die praktische Relevanz des staatlichen Zugriffs auf Bestandsdaten wird nicht nur an der Aufzählung der berechtigten Stellen sondern zahlenmäßig auch daran deutlich, dass im Jahr 2002 etwa 2 Mio. Zugriffe im Wege des automatischen Abrufverfahrens erfolgten[150]. Seit dem Jahr 2000 hat sich die Anzahl der Zugriffe jedes Jahr um 50% Jahr erhöht[151]. Da jede Abfrage eine Vielzahl von Datensätzen umfassen kann, ist die Wahrscheinlichkeit, dass an einem beliebigen Tag auf die Bestandsdaten eines beliebigen Bürgers zugegriffen wird, hoch. Diese Wahrscheinlichkeit wird weiter erhöht durch § 108 Abs. 1 S. 4 TKG-RefE, der die Verwendung von Jokerzeichen bei Online-Abfragen erlauben soll. Die Sicherheitsbehörden dürften danach also beispielsweise den Namen, die Adresse und das Geburtsdatum aller Anschlussinhaber, die in einer bestimmten Straße wohnen, abrufen.

Der staatliche Zugriff auf Telekommunikations-Bestandsdaten kann allenfalls insoweit relativ unproblematisch sein, wie er erforderlich ist, um zur Durchführung von Maßnahmen der Telekommunikationsüberwachung nach den §§ 100a, 100g StPO, nach dem G10 oder dem AWG das Unternehmen ausfindig zu ma-

[149] Berliner Kommentar-Groß, Art. 10 Rn. 36.

[150] BfD, 19. Tätigkeitsbericht (2001-2002), 79, www.bfd.bund.de/information/19tb0102.pdf.

[151] BfD, 19. Tätigkeitsbericht (2001-2002), 79, www.bfd.bund.de/information/19tb0102.pdf.

chen, über welches die Zielperson ihre Telekommunikation abwickelt[152]. Wenn der staatliche Zugriff auf Kommunikationsinhalte und Verbindungsdaten zulässig ist, dann ist es auch der vorbereitende Zugriff auf Bestandsdaten.

Die §§ 89 Abs. 6, 90 TKG bzw. §§ 107-108 TKG-RefE beschränken den Zugriff jedoch keineswegs auf Fälle der Telekommunikationsüberwachung. Sie erlauben die Anforderung von Bestandsdaten vielmehr sogar zur Verfolgung von Ordnungswidrigkeiten, zu deren Ahndung eine Telekommunikationsüberwachung in keinem Fall zulässig ist. Die Bestandsdaten von Telekommunikationsunternehmen dürfen demnach von den oben aufgeführten Behörden ohne jeden Telekommunikationsbezug als eine Art bundesweites Adressregister missbraucht werden, was für die berechtigten Behörden einen Zugriff auf Einwohnermeldedaten entbehrlich macht. Insoweit existiert nicht einmal eine Subsidiaritätsklausel. Mit dem Argument, durch die Auskunftspflicht solle nur der bis 1996 durch die Bundespost im Wege der Amtshilfe gewährte Zugriff auf Bestandsdaten fortgeschrieben werden[153], übersah der Gesetzgeber des TKG, dass Art. 10 GG und das Recht auf informationelle Selbstbestimmung schon immer amtshilfefest waren[154], so dass die damalige Amtshilfe durch die Bundespost mangels gesetzlicher Grundlage verfassungswidrig war.

Die obige Darstellung zeigt, dass Bestandsdaten nicht generell mehr oder weniger schutzwürdig als Kommunikationsinhalte oder sonstige Kommunikationsumstände sind, dass die Unterscheidung von Bestandsdaten also nur technische Bedeutung haben kann. Entsprechend ihrer hohen Schutzwürdigkeit stellt beispielsweise das englische Recht Bestandsdaten den Telekommunikations-Verkehrsdaten gleich und unterwirft sämtliche dieser "Kommunikationsdaten" ("communications data") den gleichen Schutzmechanismen[155]. Dasselbe gilt für Österreich und Finnland[156]. Gemäß den Art. 2 Abs. 1, Art. 1 Abs. 2 GG und Art. 10 GG ist auch in Deutschland eine Gleichstellung geboten, so dass zumindest die §§ 100g, 100h StPO als Vergleichsmaßstab heranzuziehen sind. Der lange Katalog berechtigter Stellen in den §§ 89 Abs. 6, 90 TKG bzw. §§ 107-108 TKG-RefE sowie die gänzlich fehlende Eingriffsschwelle wird der besonderen Sensibilität von Telekommunikations-Bestandsdaten nicht gerecht und ist daher mit den genannten Grundrechten in Verbindung mit dem Verhältnismäßigkeitsprinzip unvereinbar. Der Zugriff auf Bestandsdaten darf nur zur Abwehr

---

[152] Ähnlich BfD, Info 5, www.bfd.bund.de/information/info5/kap04/04_06_01.html: "Daten, die keinen spezifischen Telekommunikationsbezug haben, dürfen nach Auffassung des Bundesbeauftragten für den Datenschutz nicht abgefragt werden"; Kooperationskreis "IuK-Datenschutz", in: Garstka, Jahresbericht 1998, unter 5.2.

[153] Bundesregierung, BT-Drs. 13/3609, 55.

[154] Enderle, MMR 2002, 565 (565); vgl. BVerfGE 65, 1 (46).

[155] Queen Mary (University of London), Studie über Netzkriminalität, http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/-Study2000/Report.html, wo ein vergleichbares Schutzniveau für Bestandsdaten, Verkehrsdaten und Inhalten gefordert wird.

[156] EU-Questionnaire, www.statewatch.org/news/2002/nov/euintercept-2002-11-20.html.

dringender Gefahren für wichtige Rechtsgüter sowie zur Verfolgung schwerer Straftaten zugelassen werden.

Im Hinblick auf Art. 3 Abs. 1 GG stellt sich außerdem die Frage, ob es zu rechtfertigen ist, dass eine Auskunftspflicht über Bestandsdaten alleine für Telekommunikationsunternehmen, nicht aber beispielsweise für Banken oder Stromversorgungsunternehmen vorgesehen ist. Weder sind Telekommunikations-Bestandsdaten weniger sensibel als sonstige Bestandsdaten, noch sind sie für die staatliche Aufgabenwahrnehmung nützlicher. Letzteres gilt jedenfalls außerhalb der Bereichs der Vorbereitung von Maßnahmen der Telekommunikationsüberwachung. Während im Bereich der Telekommunikationsüberwachung mit besonderen Gefahren des freien Informationsaustauschs mittels Telekommunikation argumentiert werden könnte, ist diese Argumentation ausgeschlossen, wo jeder Zusammenhang mit Telekommunikation fehlt und Bestandsdaten als allgemeines Adressregister missbraucht werden. Jedenfalls außerhalb des Bereichs der Telekommunikationsüberwachung existieren daher keine Gründe von solcher Art und solchem Gewicht, dass sie eine Diskriminierung der Telekommunikationsbenutzung gegenüber sonstigen Vertragsverhältnissen rechtfertigen könnten, so dass eine auf Telekommunikationsunternehmen beschränkte Auskunftspflicht über Bestandsdaten mit Art. 3 Abs. 1 GG unvereinbar ist.

In den §§ 89 Abs. 6, 90 TKG bzw. §§ 107-108 TKG-RefE fehlt im Übrigen die verfassungsrechtlich gebotene Anordnung, dass die Verwendung erlangter Daten nur zur Verfolgung derjenigen Zwecke zulässig ist, zu deren Erreichung die Daten nach dem Gesetz erhoben werden durften (Zweckbindungsgebot)[157]. Eine darüber hinaus gehende Verwendung ist nur aufgrund einer normenklaren gesetzlichen Ermächtigung zulässig[158]. Außerdem fehlt es an der verfassungsrechtlich gebotenen Anordnung der Protokollierung jeder Erhebung, Verwendung, Übermittlung und Vernichtung von Telekommunikations-Bestandsdaten[159].

Verfassungsrechtlich geboten ist es auch, eine Benachrichtigung der Betroffenen von Eingriffen sicherzustellen[160]. Von dem Grundsatz der Benachrichtigungspflicht abweichende Regelungen sind zwar im Rahmen der Verhältnismäßigkeit zulässig[161]. Unverhältnismäßig ist ein Ausschluss der Benachrichtigung aber jedenfalls dann, wenn die Benachrichtigung den Zweck der Maßnahme nicht mehr gefährden kann[162]. Dass eine unüberschaubare Vielzahl von Personen betroffen ist und eine Benachrichtigung daher unpraktikabel wäre, kann den Aus-

[157] BVerfGE 65, 1 (46).
[158] Dazu BVerfGE 65, 1 (62 f.).
[159] Vgl. BVerfGE 100, 313 (395 f.).
[160] BVerfGE 30, 1 (31); BVerfGE 100, 313 (361).
[161] BVerfGE 100, 313 (361).
[162] BVerfGE 100, 313 (361).

schluss einer Benachrichtigung allenfalls dann rechtfertigen, wenn die Daten sofort nach ihrer Erhebung als irrelevant vernichtet werden, ohne verwendet worden zu sein[163]. Ansonsten müssen Wege gefunden werden, um Massenbenachrichtigungen praktikabel und kostengünstig zu machen. Beispielsweise ist an eine Benachrichtigung auf der Telefonrechnung des Betroffenen oder per Email an eine von diesem angegebene Emailadresse zu denken.

Darüber hinaus sehen die §§ 89 Abs. 6, 90 TKG bzw. §§ 107-108 TKG-RefE keinerlei Evaluierungsregelungen vor. Während Erkenntnisse über die Effektivität der Befugnisse möglicherweise noch im Wege repräsentativer Teiluntersuchungen gewonnen werden können, lässt sich die Belastungswirkung der Befugnisse nur einschätzen, wenn eine Statistik über die Anzahl von Anfragen sowie über die Anzahl der jeweils betroffenen Bestandsdatensätze geführt wird. Da die Kenntnis dieser Daten für die Beurteilung der Verhältnismäßigkeit der §§ 89 Abs. 6, 90 TKG bzw. §§ 107-108 TKG-RefE erforderlich ist, ist die Erstellung einer solchen Statistik verfassungsmäßig geboten.

Die relevanten Ausführungen bei Breyer, RDV 2004, 147 (151) lauten im Einzelnen wie folgt:

Ausweitung des Zugriffs auf Bestandsdaten, §§ 112, 113 TKG

§ 112 TKG zufolge haben Anbieter von Telekommunikationsdiensten für die Öffentlichkeit Bestandsdaten in eine besondere Datenbank einzustellen. Auf diese Datenbank darf eine Vielzahl öffentlicher Stellen im Wege eines Online-Abrufverfahrens zugreifen, und zwar jeweils "zur Erfüllung ihrer gesetzlichen Aufgaben"[164]. Die TKG-Novelle hat die Liste der zugriffsberechtigten Behörden erweitert um Einrichtungen, die Notrufe bearbeiten, die Bundesanstalt für Finanzdienstleistungsaufsicht und die für die Verfolgung und Ahndung von Schwarzarbeit zuständigen Behörden (§ 112 TKG).

Im Jahr 2002 sind etwa 2 Mio. Zugriffe auf Bestandsdaten im Wege des automatischen Abrufverfahrens erfolgt[165]; seit dem Jahr 2000 hat sich die Anzahl der Zugriffe jedes Jahr um 50% erhöht[166]. Da jede Abfrage eine Vielzahl von Datensätzen umfassen kann, ist die Wahrscheinlichkeit, dass an einem beliebigen Tag auf die Bestandsdaten eines beliebigen Bürgers zugegriffen wird, hoch. Diese Wahrscheinlichkeit wird weiter erhöht durch § 112 Abs. 1 S.

---

[163] BVerfGE 100, 313 (397 ff.).

[164] Zur verfassungsrechtlichen Problematik der §§ 112, 113 TKG vgl. Breyer, RDV 2003, 218 (220 ff.); Simitis, Spiros: Schriftliche Stellungnahme zur öffentlichen Anhörung des Ausschusses für Wirtschaft und Arbeit am 09.02.2004 in Berlin zum Entwurf eines Telekommunikationsgesetzes (TKG), in: Ausschussdrucksache 15(9)961, www.bundestag.de/gremien15/a09/-004Anhoerungen/TKG/materialeingeladene.pdf, 222 (224 ff.).

[165] BfD, 19. Tätigkeitsbericht (2001-2002), 79, www.bfd.bund.de/information/19tb0102.pdf.

[166] BfD, 19. Tätigkeitsbericht (2001-2002), 79, www.bfd.bund.de/information/19tb0102.pdf.

4 Nr. 2 TKG, der die Verwendung von Jokerzeichen bei Online-Abfragen erlaubt. Die ursprünglich vom Bundestag beschlossene Begrenzung der Abfragemöglichkeit auf jeweils 20 Datensätze wurde im Vermittlungsverfahren wieder fallen gelassen. Die Behörden dürfen daher nach § 112 Abs. 1 S. 4 Nr. 2 TKG beispielsweise den Namen, die Adresse und das Geburtsdatum aller Anschlussinhaber, die in einer bestimmten Straße wohnen, abrufen, also praktisch eine Rasterung von Haushalten vornehmen. Diese Befugnis greift in besonderem Maße in die Rechte der Betroffenen ein. Mit dem Parlamentsvorbehalt für derart grundrechtswesentliche Fragen ist es unvereinbar, dass die Grenzen dieser Befugnis erst in einer Rechtsverordnung geregelt werden sollen (§ 112 Abs. 3 S. 1 Nr. 3 TKG). Die Verordnung bedarf der Zustimmung des Bundesrats (§ 112 Abs. 3 S. 1 TKG).

Auf Passwörter und andere Codes, mittels derer auf Mobiltelefone, Mailboxen, Anrufbeantworter u.ä. zugegriffen werden kann, haben Staatsanwaltschaft, Polizei, Verfassungsschutzämter und Nachrichtendienste nun weitgehend uneingeschränkten Zugriff (§ 113 Abs. 1 S. 2 TKG). Diensteanbieter müssen derartige Codes auf Anfrage herausgeben, wenn sie über diese verfügen. § 113 Abs. 1 S. 2 TKG bildet allerdings keine gesetzliche Grundlage für Eingriffe in Art. 10 GG, wie sie mit der Kenntnisnahme von Telekommunikationsinhalten und -umständen verbunden sind (vgl. § 113 Abs. 1 S. 3 TKG). Es obliegt daher den zugriffsberechtigten Behörden, Zugriffscodes nur insoweit einzusetzen, wie kein Eingriff in das Fernmeldegeheimnis erfolgt.

3.4.2 Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Soweit der Schutzbereich des Fernmeldegeheimnisses in Bezug auf Bestandsdaten nicht für einschlägig gehalten wird, ist jedenfalls das Grundrecht auf informationelle Selbstbestimmung einschlägig, weil Bestandsdaten personenbezogene Daten darstellen. In diesem Fall gelten die obigen Ausführungen zu Art. 10 GG auf Seite 79 – mit Ausnahme der Ausführungen zum Zitiergebot – entsprechend unter dem Aspekt des Rechts auf informationelle Selbstbestimmung.

3.4.3 Art. 3 Abs. 1 GG

3.4.3.1 Ungleichbehandlung der Telekommunikationsnutzung gegenüber anderen Tätigkeiten, bei denen für den Staat nützliche Daten erhoben und bereitgestellt werden könnten

Die Ausführungen auf den Seiten 28 bis 29 sowie 55 bis 75 zu Art. 3 GG gelten für die §§ 112, 113 TKG entsprechend. Auch die §§ 112, 113 TKG stellen eine ungerechtfertigte Ungleichbehandlung dar:

- der Telekommunikationsnutzung gegenüber der Nutzung anderer Formen der Fernkommunikation,

- der Telekommunikationsnutzung gegenüber der Inanspruchnahme anderer Unternehmen, die für den Staat nützliche Daten erheben und bereitstellen könnten,
- der Telekommunikationsnutzung gegenüber der räumlich-unmittelbaren Kommunikation,
- des Angebots von Telekommunikationsdienstleistungen gegenüber dem Angebot anderer Kommunikationsdienstleistungen,
- des Angebots von Telekommunikationsdienstleistungen gegenüber dem Angebot anderer Unternehmen, die für den Staat nützliche Daten erheben und bereitstellen könnten, und
- der von den §§ 112, 113 TKG betroffenen Telekommunikationsunternehmen gegenüber den übrigen Steuerzahlern.

3.5 § 92 TKG

§ 92 TKG lautet:
§ 92 Datenübermittlung an ausländische nicht öffentliche Stellen
An ausländische nicht öffentliche Stellen dürfen Diensteanbieter personenbezogene Daten nach Maßgabe des Bundesdatenschutzgesetzes nur übermitteln, soweit es für die Erbringung von Telekommunikationsdiensten, für die Erstellung oder Versendung von Rechnungen oder für die Missbrauchsbekämpfung erforderlich ist.

3.5.1 Art. 10 GG

Nach der Rechtsprechung des Bundesverfassungsgerichts kann aus Grundrechten eine Schutzpflicht folgen. Dies ist insbesondere dann der Fall, wenn einem Grundrecht Gefahr droht, die vom Grundrechtsträger selbst nicht oder nicht mit legalen Mitteln beseitigt werden kann. Ein Ermessensspielraum des Staates kommt nicht in Betracht, wenn eine Gefahr für ein wichtiges Grundrecht vorliegt und wenn dieses Vorrang vor entgegenstehenden Interessen hat. Ein Anspruch auf Tätigwerden gegen die Legislative wegen Ermessensreduktion besteht allerdings nur unter den weiteren Voraussetzungen, dass die getroffenen Maßnahmen evident unzureichend sind und auch nicht angesichts der vielschichtigen Interessen vertretbar erscheinen.

Mit dem Erlass des § 92 TKG hat der Gesetzgeber seine aus Art. 10 GG folgende Schutzpflicht verletzt:

- Dass der Schutzbereich des Fernmeldegeheimnisses Verkehrsdaten als Angaben über die näheren Umstände der Telekommunikation erfasst, ist anerkannt.
- § 92 TKG setzt die von Art. 10 GG geschützte Vertraulichkeit der Telekommunikation einer besonderen Gefahr aus, wenn er die Übermittlung von Daten in das Ausland pauschal "für die Missbrauchsbekämpfung" erlaubt. Dadurch, dass eine solche Übermittlung nicht nur im Einzelfall gestattet wird (so noch §§ 3 Abs. 6, 9 Abs. 1 Nr. 2 TDSV 2000), wird die Anlage systematischer Datendepots im Ausland ermöglicht, wo

die Daten dem staatlichen Zugriff nach Maßgabe des ausländischen Rechts ausgesetzt sind.

- Die betroffenen Grundrechtsträger können diese Gefahr nicht selbst beseitigen.
- Art. 10 GG ist ein wichtiges Grundrecht. Das Fernmeldegeheimnis schützt die freie Kommunikation und ermöglicht damit unter anderem die demokratische Willensbildung in der Gesellschaft.
- Das Interesse des Bürgers an vertraulicher Kommunikation hat Vorrang vor dem Interesse von Telekommunikationsunternehmen, zum Zweck der Missbrauchsbekämpfung im Ausland systematische Depots mit Telekommunikationsdaten anlegen zu dürfen. Zur Bekämpfung ernsthaften Missbrauchs ist die Anlage solcher Depots nämlich nicht geeignet, wohingegen von ihnen schwerwiegende Gefahren für die Grundrechtsträger ausgehen (siehe Seiten 13 bis 27).
- Die vom Gesetzgeber zum Schutz des Fernmeldegeheimnisses getroffenen Vorkehrungen sind evident unzureichend. § 92 TKG überlässt die Frage der Erforderlichkeit der Datenübermittlung vollkommen den Telekommunikationsunternehmen. Er gewährleistet insbesondere nicht, dass eine Datenverarbeitung zur Missbrauchsbekämpfung nur im Einzelfall erfolgt.

3.6 § 88 Abs. 3 S. 1 TKG

§ 88 TKG lautet:
§ 88 Fernmeldegeheimnis
(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.
(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.
(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.
(4) Befindet sich die Telekommunikationsanlage an Bord eines Fahrzeugs für Seefahrt oder Luftfahrt, so besteht die Pflicht zur Wahrung des Geheimnisses nicht gegenüber der Person, die das Fahrzeug führt oder gegenüber ihrer Stellvertretung.

3.6.1 Art. 10 GG

3.6.1.1 Eingriff in den Schutzbereich

Es stellt einen staatlichen Eingriff in Art. 10 GG dar, wenn Telekommunikationsunternehmen das Recht eingeräumt wird, Inhalt und nähere Umstände der Telekommunikation länger als für ihre Zwecke erforderlich speichern zu dürfen, und wenn gleichzeitig staatlichen Behörden Zugriffsrechte auf diese Daten eingeräumt werden. Dies ergibt sich aus den Ausführungen auf Seite 9 bis 27, auf die Bezug genommen wird.

Dass § 88 Abs. 3 S. 1 TKG Telekommunikationsunternehmen das Recht einräumt, dem Fernmeldegeheimnis unterliegende Daten länger als für ihre Zwecke erforderlich speichern zu dürfen, ergibt sich aus den folgenden Erwägungen: § 88 Abs. 3 S. 1 TKG erlaubt Diensteanbietern – anders als noch § 85 Abs. 3 S. 1 TKG a.F. – die Speicherung von Inhalt und den näheren Umständen der Telekommunikation "für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme". Die Einfügung der Worte "einschließlich des Schutzes ihrer technischen Systeme" erlaubt dem Wortlaut nach beliebige Eingriffe in das Fernmeldegeheimnis, wenn sie nur dem (angeblichen) Zweck des Schutzes der technischen Systeme eines Betreibers dienen sollen. Da § 88 Abs. 3 S. 1 TKG, soweit er den "Schutz technischer Systeme betrifft", insbesondere nicht nur eine Kenntnisnahme im Einzelfall erlaubt, geht er weit über das Maß des Erforderlichen hinaus (vgl. Seite 28 sowie die Ausführungen im Anhang).

Dass staatliche Stellen Zugriff auf nach § 88 Abs. 3 S. 1 TKG gespeicherte Verkehrsdaten haben, folgt etwa aus den §§ 100g, 100h StPO.

3.6.1.2 Rechtfertigung

Art. 10 Abs. 2 S. 1 GG bestimmt: "Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden." Bereits aus dieser Bestimmung ergibt sich, dass das Fernmeldegeheimnis nicht generell "durch Gesetz" eingeschränkt werden darf, sondern dass Beschränkungen des Fernmeldegeheimnisses nur "auf Grund eines Gesetzes" im Einzelfall "angeordnet" werden dürfen. § 88 Abs. 3 S. 1 TKG ist von dem Gesetzesvorbehalt des Art. 10 Abs. 2 S. 1 GG nicht gedeckt, weil § 88 Abs. 3 S. 1 TKG das Fernmeldegeheimnis generell einschränkt und nicht nur Beschränkungen im Einzelfall zulässt.

Daneben ist § 88 Abs. 3 S. 1 TKG auch deswegen verfassungswidrig, weil die Vorschrift das eingeschränkte Grundrecht (das Fernmeldegeheimnis) nicht unter Angabe des Artikels (Art. 10 Abs. 1 GG) nennt, wie es Art. 19 Abs. 1 S. 2 GG vorschreibt.

Darüber hinaus ist § 88 Abs. 3 S. 1 TKG auch wegen Verstoßes gegen das Verhältnismäßigkeitsgebot verfassungswidrig. Eine Ermächtigung zur einzelfallunabhängigen Speicherung von Daten, die dem Fernmeldegeheimnis unterliegen, ist auch zum "Schutz technischer Systeme" unverhältnismäßig (vgl. Seite 28 und Anhang).

3.7 § 110 TKG

§ 110 TKG lautet:

§ 110 Technische Umsetzung von Überwachungsmaßnahmen
(1) Wer eine Telekommunikationsanlage betreibt, mit der Telekommunikationsdienste für die Öffentlichkeit erbracht werden, hat

1. *ab dem Zeitpunkt der Betriebsaufnahme auf eigene Kosten technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation vorzuhalten und organisatorische Vorkehrungen für deren unverzügliche Umsetzung zu treffen,*
2. *der Regulierungsbehörde unverzüglich nach der Betriebsaufnahme*
   a) zu erklären, dass er die Vorkehrungen nach Nummer 1 getroffen hat sowie
   b) eine im Inland gelegene Stelle zu benennen, die für ihn bestimmte Anordnungen zur Überwachung der Telekommunikation entgegennimmt,
3. *der Regulierungsbehörde den unentgeltlichen Nachweis zu erbringen, dass seine technischen Einrichtungen und organisatorischen Vorkehrungen nach Nummer 1 mit den Vorschriften der Rechtsverordnung nach Absatz 2 und der Technischen Richtlinie nach Absatz 3 übereinstimmen; dazu hat er unverzüglich, spätestens nach einem Monat nach Betriebsaufnahme,*
   a) der Regulierungsbehörde die Unterlagen zu übersenden, die dort für die Vorbereitung der im Rahmen des Nachweises von der Regulierungsbehörde durchzuführenden Prüfungen erforderlich sind, und
   b) mit der Regulierungsbehörde einen Prüftermin für die Erbringung dieses Nachweises zu vereinbaren; bei den für den Nachweis erforderlichen Prüfungen hat er die Regulierungsbehörde zu unterstützen,
4. *der Regulierungsbehörde auf deren besondere Aufforderung im begründeten Einzelfall eine erneute unentgeltliche Prüfung seiner technischen und organisatorischen Vorkehrungen zu gestatten sowie*
5. *die Aufstellung und den Betrieb von Geräten für die Durchführung von Maßnahmen nach den §§ 5 und 8 des Artikel 10-Gesetzes in seinen Räumen zu dulden und Bediensteten der für diese Maßnahmen zuständigen Stelle sowie den Mitgliedern und Mitarbeitern der G 10-Kommission (§ 1 Abs. 2 des Artikel 10-Gesetzes) Zugang zu diesen Geräten zur Erfüllung ihrer gesetzlichen Aufgaben zu gewähren.*

Wer Telekommunikationsdienste für die Öffentlichkeit erbringt, ohne hierfür eine Telekommunikationsanlage zu betreiben, hat sich bei der Auswahl des Betreibers der dafür genutzten Telekommunikationsanlage zu vergewissern, dass dieser Anordnungen zur Überwachung der Telekommunikation unverzüglich nach Maßgabe der Rechtsverordnung nach Absatz 2 und der Technischen Richtlinie nach Absatz 3 umsetzen kann und der Regulierungsbehörde unverzüglich nach Aufnahme seines Dienstes mitzuteilen, welche Telekommunikationsdienste er erbringt, durch wen Überwachungsanordnungen, die seine Teilnehmer betreffen, umgesetzt werden und an welche im Inland gelegene Stelle Anordnungen zur Überwachung der Telekommunikation zu richten sind. Änderungen der den Mitteilungen nach Satz 1 Nr. 2 Buchstabe b und Satz 2 zugrunde liegenden Daten sind der Regulierungsbehörde unverzüglich mitzuteilen. In Fällen, in denen noch keine Vorschriften nach Absatz 3 vorhanden sind, hat der Verpflichtete die technischen Einrichtungen nach Satz 1 Nr. 1 in Absprache mit der Regulierungsbehörde zu gestalten. Die

Sätze 1 bis 4 gelten nicht, soweit die Rechtsverordnung nach Absatz 2 Ausnahmen für die Telekommunikationsanlage vorsieht. § 100b Abs. 3 Satz 1 der Strafprozessordnung, § 2 Abs. 1 Satz 3 des Artikel 10-Gesetzes sowie entsprechende landesgesetzliche Regelungen zur polizeilich-präventiven Telekommunikationsüberwachung bleiben unberührt.

(2) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates

1. *Regelungen zu treffen*
   a) über die grundlegenden technischen Anforderungen und die organisatorischen Eckpunkte für die Umsetzung von Überwachungsmaßnahmen einschließlich der Umsetzung von Überwachungsmaßnahmen durch einen von dem Verpflichteten beauftragten Erfüllungsgehilfen,
   b) über den Regelungsrahmen für die Technische Richtlinie nach Absatz 3,
   c) für den Nachweis nach Absatz 1 Satz 1 Nr. 3 und 4 und
   d) für die nähere Ausgestaltung der Duldungsverpflichtung nach Absatz 1 Satz 1 Nr. 5 sowie
2. *zu bestimmen,*
   a) in welchen Fällen und unter welchen Bedingungen vorübergehend auf die Einhaltung bestimmter technischer Vorgaben verzichtet werden kann,
   b) dass die Regulierungsbehörde aus technischen Gründen Ausnahmen von der Erfüllung einzelner technischer Anforderungen zulassen kann und
   c) bei welchen Telekommunikationsanlagen und damit erbrachten Diensteangeboten aus grundlegenden technischen Erwägungen oder aus Gründen der Verhältnismäßigkeit abweichend von Absatz 1 Satz 1 Nr. 1 keine technischen Einrichtungen vorgehalten und keine organisatorischen Vorkehrungen getroffen werden müssen.

(3) Die Regulierungsbehörde legt technische Einzelheiten, die zur Sicherstellung einer vollständigen Erfassung der zu überwachenden Telekommunikation und zur Gestaltung des Übergabepunktes zu den berechtigten Stellen erforderlich sind, in einer im Benehmen mit den berechtigten Stellen und unter Beteiligung der Verbände und der Hersteller zu erstellenden Technischen Richtlinie fest. Dabei sind internationale technische Standards zu berücksichtigen; Abweichungen von den Standards sind zu begründen. Die Technische Richtlinie ist von der Regulierungsbehörde in ihrem Amtsblatt bekannt zu machen.
(4) Wer technische Einrichtungen zur Umsetzung von Überwachungsmaßnahmen herstellt oder vertreibt, kann von der Regulierungsbehörde verlangen, dass sie diese Einrichtungen im Rahmen einer Typmusterprüfung im Zusammenwirken mit bestimmten Telekommunikationsanlagen daraufhin prüft, ob die rechtlichen und technischen Vorschriften der Rechtsverordnung nach Absatz 2 und der Technischen Richtlinie nach Absatz 3 erfüllt werden. Die Regulierungsbehörde kann nach pflichtgemäßem Ermessen vorübergehend Abweichungen von den technischen Vorgaben zulassen, sofern die Umsetzung von Überwachungsmaßnahmen grundsätzlich sichergestellt ist und sich ein nur unwesentlicher Anpassungsbedarf bei den Einrichtungen der berechtigten Stellen ergibt. Die Regulierungsbehörde hat dem Hersteller oder Vertreiber das Prüfergebnis schriftlich mitzuteilen. Die Prüfergebnisse werden von der Regulierungsbehörde bei dem Nachweis der Übereinstimmung der technischen Einrichtungen mit den anzuwendenden technischen

Vorschriften beachtet, den der Verpflichtete nach Absatz 1 Satz 1 Nr. 3 oder 4 zu erbringen hat. Die vom Bundesministerium für Wirtschaft und Arbeit vor Inkrafttreten dieser Vorschrift ausgesprochenen Zustimmungen zu den von Herstellern vorgestellten Rahmenkonzepten gelten als Mitteilungen im Sinne des Satzes 3.

(5) Wer nach Absatz 1 in Verbindung mit der Rechtsverordnung nach Absatz 2 verpflichtet ist, Vorkehrungen zu treffen, hat die Anforderungen der Rechtsverordnung und der Technischen Richtlinie nach Absatz 3 spätestens ein Jahr nach deren Bekanntmachung zu erfüllen, sofern dort für bestimmte Verpflichtungen kein längerer Zeitraum festgelegt ist. Nach dieser Richtlinie gestaltete mängelfreie technische Einrichtungen für bereits vom Verpflichteten angebotene Telekommunikationsdienste müssen im Falle einer Änderung der Richtlinie spätestens drei Jahre nach deren Inkrafttreten die geänderten Anforderungen erfüllen. Stellt sich bei dem Nachweis nach Absatz 1 Satz 1 Nr. 3 oder einer erneuten Prüfung nach Absatz 1 Satz 1 Nr. 4 ein Mangel bei den von dem Verpflichteten getroffenen technischen oder organisatorischen Vorkehrungen heraus, hat er diesen Mangel nach Vorgaben der Regulierungsbehörde in angemessener Frist zu beseitigen; stellt sich im Betrieb, insbesondere anlässlich durchzuführender Überwachungsmaßnahmen, ein Mangel heraus, hat er diesen unverzüglich zu beseitigen. Sofern für die technische Einrichtung eine Typmusterprüfung nach Absatz 4 durchgeführt worden ist und dabei Fristen für die Beseitigung von Mängeln festgelegt worden sind, hat die Regulierungsbehörde diese Fristen bei ihren Vorgaben zur Mängelbeseitigung nach Satz 3 zu berücksichtigen.
(6) Jeder Betreiber einer Telekommunikationsanlage, der anderen im Rahmen seines Angebotes für die Öffentlichkeit Netzabschlusspunkte seiner Telekommunikationsanlage überlässt, ist verpflichtet, den gesetzlich zur Überwachung der Telekommunikation berechtigten Stellen auf deren Anforderung Netzabschlusspunkte für die Übertragung der im Rahmen einer Überwachungsmaßnahme anfallenden Informationen unverzüglich und vorrangig bereitzustellen. Die technische Ausgestaltung derartiger Netzabschlusspunkte kann in einer Rechtsverordnung nach Absatz 2 geregelt werden. Für die Bereitstellung und Nutzung gelten mit Ausnahme besonderer Tarife oder Zuschläge für vorrangige oder vorzeitige Bereitstellung oder Entstörung die jeweils für die Allgemeinheit anzuwendenden Tarife. Besondere vertraglich vereinbarte Rabatte bleiben von Satz 3 unberührt.

(7) Telekommunikationsanlagen, die von den gesetzlich berechtigten Stellen betrieben werden und mittels derer in das Fernmeldegeheimnis oder in den Netzbetrieb eingegriffen werden soll, sind im Einvernehmen mit der Regulierungsbehörde technisch zu gestalten. Die Regulierungsbehörde hat sich zu der technischen Gestaltung innerhalb angemessener Frist zu äußern.

(8) Die nach den §§ 100a und 100b der Strafprozessordnung verpflichteten Betreiber von Telekommunikationsanlagen haben eine Jahresstatistik über nach diesen Vorschriften durchgeführte Überwachungsmaßnahmen zu erstellen und der Regulierungsbehörde unentgeltlich zur Verfügung zu stellen. Die Ausgestaltung der Statistik im Einzelnen kann in der Rechtsverordnung nach Absatz 2 geregelt werden. Die Betreiber dürfen die Statistik Dritten nicht zur Kenntnis geben. Die Regulierungsbehörde fasst die von den Unternehmen gelieferten Angaben zusammen und veröffentlicht das Ergebnis jährlich in ihrem Amtsblatt.

(9) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Deutschen Bundestages und des Bundesrates Regelungen über die den Diensteanbietern zu gewährenden angemessenen Entschädigungen für Leistungen zu treffen, die von diesen

1. *bei der Ermöglichung der Überwachung nach den §§ 100a und 100b der Strafprozessordnung, nach § 2 Abs. 1, § 5 oder § 8 des Artikel 10-Gesetzes, nach § 39 des Außenwirtschaftsgesetzes oder nach entsprechenden landesgesetzlichen Vorschriften und*
2. *bei der Erteilung von Auskünften nach § 113 erbracht werden. Die Kosten der Vorhaltung der technischen Einrichtungen, die für die Erbringung der Leistungen nach Satz 1 erforderlich sind, sind nicht Gegenstand dieser Entschädigungsregelungen.*

3.7.1 Art. 3 Abs. 1 GG

§ 110 TKG verpflichtet Telekommunikationsunternehmen zur entschädigungslosen Vorhaltung von Einrichtungen und Personal zur Durchführung von Telekommunikationsüberwachungsmaßnahmen.

3.7.1.1 Ungleichbehandlung des Angebots von Telekommunikationsdienstleistungen gegenüber dem Angebot anderer Unternehmen, die für den Staat nützliche Daten erheben und bereitstellen könnten

§ 110 TKG stellt eine ungerechtfertigte Benachteiligung der Telekommunikationsunternehmen gegenüber anderen Kommunikationsunternehmen (z.B. Anbieter von Postfächern) und anderen Unternehmen, die für den Staat nützliche Daten erheben und bereitstellen könnten, dar (siehe im Einzelnen Breyer, Vorratsspeicherung (2005)[167], Seiten 331-338).

Die relevanten Ausführungen bei Breyer, Vorratsspeicherung (2005)[168], Seiten 331-338 sind bereits auf Seiten 55 bis 75 wiedergegeben.

3.7.1.2 Ungleichbehandlung der von § 110 TKG betroffenen Telekommunikationsunternehmen gegenüber den übrigen Steuerzahlern

Außerdem sind die in § 110 TKG genannten Unternehmen auch dadurch in ihrem Grundrecht aus Art. 3 Abs. 1 i.V.m. Art. 12 Abs. 1 GG bzw. Art. 3 Abs. 1 i.V.m. Art. 2 Abs. 1 GG verletzt, dass sie die Kosten der Vorhaltung technischer Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation sowie organisatorischer Vorkehrungen für deren unverzügliche Umsetzung entschädigungslos (§ 110 Abs. 1 S. 1 Nr. 1 TKG) selbst tragen müssen (vgl. im Einzelnen Breyer, Vorratsspeicherung (2005)[169], Seiten 357-368). Hierin liegt eine Benachteiligung dieser Unternehmen gegenüber den übrigen Steuerzahlern. Die Vergleichbarkeit der Personengruppen ergibt sich daraus, dass beide Gruppen dem Oberbegriff der Gesamtheit steuerpflichtiger Rechtssubjekte zuzuordnen sind.

Es ist kein sachlicher Grund dafür ersichtlich, dass Telekommunikationsunternehmen die Kosten der Überwachung der Telekommunikation zu staatlichen Zwecken tragen sollen.

---

[167] Breyer, (Fn. 8).

[168] Breyer, (Fn. 8).

[169] Breyer, (Fn. 8).

Zwar mag es sein, dass nur die in § 110 TKG genannten Unternehmen Überwachungsmaßnahmen technisch umsetzen können. Die Frage der Kostentragungspflicht ist aber hiervon zu trennen, wie auch in der Rechtsprechung anerkannt ist (vgl. im Einzelnen Breyer, Vorratsspeicherung (2005)[170], Seiten 357-368).

§ 110 TKG stellt eine Inpflichtnahme Privater zu öffentlichen Zwecken dar, denn die dort angeordneten Tätigkeiten sollen "zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation" erfolgen (§ 110 Abs. 1 S. 1 Nr. 1 TKG). Weil die Überwachung der Telekommunikation dem Allgemeininteresse dienen, muss auch die Allgemeinheit für die insoweit entstehenden Kosten aufkommen. Die alleinige Abwälzung der Kosten auf die verpflichteten Unternehmen ist sachlich nicht gerechtfertigt. Weder begründen die Unternehmen durch ihr Angebot eine Quelle besonderer, sozialinadäquater Gefahren, noch entfaltet § 110 TKG einen besonderen Nutzen für sie (vgl. im Einzelnen Breyer, Vorratsspeicherung (2005)[171], Seiten 357-368).

Weiterhin trägt das Argument nicht, die Unternehmen könnten ihre Kosten auf den Kunden abwälzen. Selbst wenn man hiervon ausgeht, so wären hierdurch die Kunden gegenüber sonstigen Steuerzahlern benachteiligt. Auch dies ist unter dem Aspekt des Art. 3 Abs. 1 GG nicht gerechtfertigt, denn auch Telekommunikationsnutzer schaffen keine besondere Gefahr und haben keinen besonderen Nutzen von § 110 TKG.

Die relevanten Ausführungen bei Breyer, Vorratsspeicherung (2005)[172], Seiten 357-368 sind bereits auf Seite 64 wiedergegeben.

3.7.1.3 Gleichbehandlung der von § 110 TKG betroffenen Kleinunternehmen gegenüber den übrigen Betroffenen

Eine unterschiedslose Verpflichtung aller Telekommunikationsunternehmen zu Überwachungsvorkehrungen verstößt auch deswegen gegen den Gleichheitssatz, weil damit "innerhalb der betroffenen Berufsgruppe nicht nur einzelne, aus dem Rahmen fallende Sonderfälle, sondern bestimmte, wenn auch zahlenmäßig begrenzte, Gruppen typischer Fälle ohne zureichende sachliche Gründe wesentlich stärker belastet" werden[173]. In solchen Fällen liegt eine unzulässige Gleichbehandlung ungleicher Sachverhalte vor[174]. Es handelt sich um eine Ausnahme von dem Grundsatz, dass der Gesetzgeber ungleiche Sachverhalte aus Gründen der Praktikabilität grundsätzlich typisieren und die Mitglieder typischer Gruppen gleich behandeln darf.

Im vorliegenden Zusammenhang belastet § 110 TKG insbesondere die Gruppe der Email-Anbieter wesentlich stärker als die sonst betroffenen Unternehmen. Unter diesen Anbietern gibt es eine Vielzahl kleiner, unabhängiger Unternehmen, die keine Finanzpolster aufweisen und von einer staatlichen Inpflichtnahme folglich empfindlich getroffen werden. Daran ändert die grundsätzliche Möglichkeit der Kostenabwälzung – soweit sie in der Praxis überhaupt besteht – jedenfalls insoweit nichts, als sich etwa erforderliche Anlaufinvestitionen nur allmählich wieder amortisieren können, wenigstens für eine Über-

---

[170] Breyer, (Fn. 8).
[171] Breyer, (Fn. 8).
[172] Breyer, (Fn. 8).
[173] Vgl. BVerfGE 30, 292 (327).
[174] BVerfGE 30, 292 (333).

gangszeit aber aus eigenen Mitteln vorfinanziert werden müssen. In den Niederlanden sollen einige kleine Unternehmen an dieser Hürde gescheitert sein, als der Staat Auflagen zur Sicherstellung der Überwachbarkeit von Internetkommunikation machte. Dementsprechend ist auch in Deutschland davon auszugehen, dass eine bedeutende Zahl von kleinen Unternehmen nicht in der Lage ist, die Mittel aufzubringen, die erforderlich sind, um § 110 TKG nachzukommen.

Auf die Wettbewerbssituation von Kleinunternehmen wirken sich Kosten steigernde Belastungen von vornherein stärker aus als auf größere Unternehmen, die über eine gewisse Kapitaldecke verfügen und – im Fall von Konzernen – teilweise auch auf die Ressourcen verbundener Unternehmen zurückgreifen können[175]. Weil die großen Unternehmen am Markt das Preisniveau vorgeben, ist kleinen Unternehmen die Abwälzung von Überwachungskosten nur in geringerem Maße möglich als Großunternehmen. Ein Großteil dieser Kosten stellt Fixkosten dar, deren Höhe von der Unternehmensgröße unabhängig ist. Solche Kosten treffen Kleinunternehmen daher – gemessen an ihrem Kundenkreis, ihrer Größe und Kapitalausstattung – ungleich härter. Hinzu kommt, dass größere Unternehmen erforderliche Einrichtungen oder Leistungen in größeren Mengen einkaufen und dadurch niedrigere Preise aushandeln können. Der Größenvorteil von Großunternehmen wirkt sich auch bei den variablen Kosten und bei den Möglichkeiten, staatliche Anforderungen kostensparend umzusetzen, aus[176]. Größere Unternehmen werden den Kunden folglich günstigere Konditionen bieten können, was zu einem weiteren Nachteil der Kleinunternehmen führt, die oft gerade auf günstige Preise angewiesen sind, um im Wettbewerb bestehen zu können.

Im Internetbereich stellt Werbung zudem oft die einzige Einnahmequelle von Kleinunternehmen dar. Diese Unternehmen können selbst eine geringe Kostenerhöhung an ihre Nutzer nicht weiter geben, weil die Anziehungskraft ihres Angebots gerade in dessen Unentgeltlichkeit liegt. Dienste im Internet, die sich bisher werbefinanzieren und ihre Leistungen daher unentgeltlich anbieten konnten (z.B. E-Mail-Dienste), müssen teilweise eingestellt werden. Dies hat letztlich zur Folge, dass weniger finanzkräftige Bürger, Unternehmen und Organisationen zu einer Einschränkung ihrer Telekommunikation gezwungen werden können. Unentgeltliche Kommunikationsdienste im Internet sind für die freie Kommunikation in unserer Gesellschaft heute von höchster Bedeutung. Im Regelfall können zudem nur unentgeltliche Angebote anonym in Anspruch genommen werden, was etwa für Menschen in besonderen Konfliktsituationen oder auch für politisch kritische Aktivisten von großer Wichtigkeit ist.

Nach aktuellen Untersuchungen ist im Übrigen nur eine Minderheit von Internetnutzern zur Zahlung eines Entgelts für Internetdienste bereit. Dies gilt besonders für Dienste, die an anderer Stelle (z.B. im Ausland) kostenfrei angeboten werden, etwa E-Mail- oder Chatdienste.

Aus diesen Gründen sind aufgrund von § 110 TKG seitens der Kleinunternehmen Geschäftsaufgaben und ähnliche schwerste Belastungen ernsthaft zu befürchten. Ist der Eintritt einer unzumutbaren – insbesondere existenzgefährdenden – Belastung typischer Gruppen von Betroffenen nicht auszuschließen, so ist den Betroffenen ein Abwarten bis zu dem möglichen Eintritt irreparabler Schäden unzumutbar; eine Verletzung des Gleich-

[175] So schon BVerfGE 30, 292 (330 f.).

[176] Vgl. schon BVerfGE 30, 292 (330 f.).

heitssatzes liegt schon dann vor, wenn ein Gesetz für den Fall des Eintritts unzumutbarer Belastungen keine Abhilfemöglichkeit vorsieht[177].

So verhält es sich bei § 110 TKG. Zwar hat der Gesetzgeber in § 110 Abs. 2 Nr. 2c TKG vorgesehen, dass der Verordnungsgeber "aus Gründen der Verhältnismäßigkeit" Ausnahmen vorsehen kann. Eine derart unbestimmte Regelung genügt zum Schutz von Kleinunternehmen jedoch nicht, weil die verfassungsrechtlich gebotenen Einschränkungen in keiner Weise vorgegeben werden. Dies wurde im Gesetzgebungsverfahren ursprünglich auch erkannt, denn der Bundestag beschloss, Telekommunikationsanlagen mit weniger als 1000 Teilnehmern von der gesetzlichen Verpflichtung auszunehmen[178]. Diese Einschränkung wurde im weiteren Gesetzgebungsverfahren jedoch wieder fallengelassen. Ohnehin ist im Hinblick auf derartige zahlenmäßige Beschränkungen zu kritisieren, dass die Schwellen für Email-Anbieter einerseits und für sonstige Anbieter andererseits gleich hoch angesetzt werden. Email-Anbieter erreichen derartige Schwellen sehr viel schneller, weil ihr Angebot kaum Investitionen erfordert und zudem für die Teilnehmer meist unentgeltlich ist. Ein Schwellenwert, der im Bereich der Sprachtelefonie geeignet ist, Kleinunternehmen auszuschließen, erfasst die meisten Kleinunternehmen im Bereich von Email-Diensten nicht. Diesen fundamentalen Unterschied muss der Gesetzgeber nachvollziehen.

In Verbindung mit dem Parlamentsvorbehalt ist aus Art. 3 Abs. 1 GG abzuleiten, dass der Gesetzgeber jedenfalls zahlenmäßig erhebliche Fallgruppen, in denen durchweg die Gefahr unzumutbarer Belastungen besteht, von einer Regelung ausnehmen muss. Derartige Ausnahmen oder Differenzierungen sieht § 110 TKG nicht vor. Die Bestimmung gewährleistet auch nicht, dass der Verordnungsgeber hinreichende Ausnahmen vorsieht.

Das Risiko des Eintritts unzumutbarer Belastungen für Unternehmen der genannten Art lässt sich nur dann weitgehend ausschließen, wenn der Gesetzgeber die Kosten vorgeschriebener Überwachungsvorkehrungen für diese Unternehmen gering hält oder eine Kostenbelastung ausschließt. Dies lässt sich einerseits durch staatliche Sach- oder Geldmittel erreichen oder andererseits durch Ausnahme der Unternehmen von der Vorhaltepflicht. Wird keiner der vorgenannten Wege eingeschlagen, dann kann es zu unzumutbaren Belastungen betroffener Unternehmen kommen. Im Vergleich zum Ausmaß dieser Schwierigkeiten müssen Effektivitätserwägungen des Staates zurücktreten, zumal Maßnahmen der Telekommunikationsüberwachung in Deutschland nur in jeweils etwa 0,5-1% der Fälle Betreiber privater Telekommunikationsnetze oder Unternehmen im Internet-Bereich betreffen[179]. In diesen wenigen Fällen muss es ausreichen, wenn die Unternehmen bei Bedarf unverzüglich ihren gesetzlichen Pflichten nachkommen, ohne vorher besondere Vorkehrungen getroffen zu haben.

3.8 § 95 Abs. 3 und § 111 Abs. 1 S. 4 TKG

§ 95 Abs. 3 und § 111 Abs. 1 S. 4 TKG lauten:
§ 95 Vertragsverhältnisse
[...]

---

[177] BVerfGE 30, 292 (333).

[178] § 108 TKG i.d.F. der Beschlussempfehlung des Ausschusses für Wirtschaft und Arbeit vom 10.03.2004, BT-Drs. 15/2674, 83.

[179] Schulzki-Haddouti, Lauscher unter Beschuss, c't 09/2001, 24 ff.

(3) Endet das Vertragsverhältnis, sind die Bestandsdaten vom Diensteanbieter mit Ablauf des auf die Beendigung folgenden Kalenderjahres zu löschen. § 35 Abs. 3 des Bundesdatenschutzgesetzes gilt entsprechend. [...]

§ 111 Daten für Auskunftsersuchen der Sicherheitsbehörden
(1) [...] Nach Ende des Vertragsverhältnisses sind die Daten mit Ablauf des auf die Beendigung folgenden Kalenderjahres zu löschen. [...]

3.8.1 Art. 10 GG

3.8.1.1 Schutzbereich

Dass der Schutzbereich des Fernmeldegeheimnisses Bestandsdaten erfasst, ergibt sich aus den Ausführungen zu Punkt (0 oben), auf die Bezug genommen wird.

3.8.1.2 Eingriff

Es stellt einen staatlichen Eingriff in Art. 10 GG dar, wenn Telekommunikationsunternehmen verpflichtet werden, Bestandsdaten länger als für ihre Zwecke erforderlich zu speichern, und wenn staatlichen Behörden gleichzeitig Zugriffsrechte auf diese Daten zustehen. Dies ergibt sich aus den Ausführungen zu Punkt 3.1.1, auf die Bezug genommen wird.
Dass die §§ 95 Abs. 3, 111 Abs. 1 S. 3 TKG Telekommunikationsunternehmen verpflichten, Bestandsdaten länger als für ihre Zwecke erforderlich zu speichern, ergibt sich daraus, dass eine Speicherung von Bestandsdaten über das Vertragsende hinaus allenfalls noch bis zur Begleichung offener Forderungen erforderlich ist. Nicht erforderlich ist dagegen die Aufbewahrung sämtlicher (also auch abrechnungsirrelevanter) Bestandsdaten bis zum Ende des folgenden Jahres. Diese Aufbewahrung ordnet der Gesetzgeber ausschließlich deswegen an, damit die Daten für staatliche Auskunftersuchen zur Verfügung stehen.

Dass staatliche Stellen Zugriff auf die gespeicherten Verkehrsdaten haben, folgt aus den §§ 112, 113 TKG.

3.8.1.3 Rechtfertigung

Art. 10 Abs. 2 S. 1 GG bestimmt: "Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden." Bereits aus dieser Bestimmung ergibt sich, dass das Fernmeldegeheimnis nicht generell "durch Gesetz" eingeschränkt werden darf, sondern dass Beschränkungen des Fernmeldegeheimnisses nur "auf Grund eines Gesetzes" im Einzelfall "angeordnet" werden dürfen. Die §§ 95 Abs. 3, 111 Abs. 1 S. 3 TKG sind von dem Gesetzesvorbehalt des Art. 10 Abs. 2 S. 1 GG nicht gedeckt, weil sie das Fernmeldegeheimnis generell einschränken und nicht nur Beschränkungen im Einzelfall zulassen.

Daneben sind die §§ 95 Abs. 3, 111 Abs. 1 S. 3 TKG auch deswegen verfassungswidrig, weil die Vorschriften das eingeschränkte Grundrecht (das Fernmeldegeheimnis) nicht unter Angabe des Artikels (Art. 10 Abs. 1 GG) nennen, wie es Art. 19 Abs. 1 S. 2 GG vorschreibt.

Dass die Einführung von Vorratsspeicherungspflichten auf dem Gebiet der Telekommunikation darüber hinaus unverhältnismäßig ist, ergibt sich aus den Ausführungen zu Punkt 3.1.1 und 3.1.2 oben, die für § 95 Abs. 3 und § 111 Abs. 1 S. 4 TKG entsprechend gelten und auf die deswegen Bezug genommen wird.

3.8.2 Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Soweit der Schutzbereich des Fernmeldegeheimnisses in Bezug auf Bestandsdaten nicht für einschlägig gehalten wird, ist jedenfalls das Grundrecht auf informationelle Selbstbestimmung einschlägig, weil Bestandsdaten personenbezogene Daten darstellen. In diesem Fall gelten die obigen Ausführungen zu Art. 10 GG (Punkt 0 oben, – mit Ausnahme der Ausführungen zum Gesetzesvorbehalt und zum Zitiergebot – entsprechend unter dem Aspekt des Rechts auf informationelle Selbstbestimmung.

3.8.3 Art. 3 Abs. 1 GG

Dass die Einführung von Vorratsspeicherungspflichten auf dem Gebiet der Telekommunikation gegen Art. 3 Abs. 1 GG verstößt, ergibt sich aus den Ausführungen zu Punkt 0 oben und zu Punkt 3.2.1 oben, auf die Bezug genommen wird. Auch die §§ 95 Abs. 3, 111 Abs. 1 S. 4 TKG stellen eine ungerechtfertigte Ungleichbehandlung dar:

- der Telekommunikationsnutzung gegenüber der Nutzung anderer Formen der Fernkommunikation,
- der Telekommunikationsnutzung gegenüber der Inanspruchnahme anderer Unternehmen, die für den Staat nützliche Daten erheben und bereitstellen könnten,
- der Telekommunikationsnutzung gegenüber der räumlich-unmittelbaren Kommunikation,
- des Angebots von Telekommunikationsdienstleistungen gegenüber dem Angebot anderer Kommunikationsdienstleistungen,
- des Angebots von Telekommunikationsdienstleistungen gegenüber dem Angebot anderer Unternehmen, die für den Staat nützliche Daten erheben und bereitstellen könnten, und
- der von den §§ 95 Abs. 3, 111 Abs. 1 S. 4 TKG betroffenen Telekommunikationsunternehmen gegenüber den übrigen Steuerzahlern.

4. Annahmevoraussetzungen

Der Verfassungsbeschwerde kommt grundsätzliche Bedeutung zu, weil sie verfassungsrechtliche Fragen aufwirft, die sich nicht ohne weiteres aus dem Grundgesetz beantworten lassen und noch nicht durch die verfassungsgerichtliche Rechtsprechung gelöst sind. Insoweit wird auf die obigen Ausführungen verwiesen. Die zugrunde liegenden Erwägungen sind in der Literatur keinesfalls unumstritten, woran die Relevanz ihrer Klärung deutlich wird. Dass die aufgeworfenen Fragen über den Einzelfall hinaus für alle Telekommunikationskunden und -anbieter dauerhaft von Bedeutung sind, liegt auf der Hand.

Die Annahme der Verfassungsbeschwerde ist auch zur Durchsetzung der verletzten Grundrechte angezeigt. Die Grundrechtsverletzung hat besonderes Gewicht, weil in ihr eine generelle Vernachlässigung der gerügten Grundrechte durch den Gesetzgeber

beim Beschluss des TKG zum Ausdruck kommt. Er hat warnende Hinweise, die Sachverständige anlässlich von Anhörungen gaben, letztlich nicht beachtet.

Sollte das Gericht wegen fehlender Ausführungen oder wegen mangelnder Substantiierung des Vortrags der Beschwerdeführer eine rechtlich nachteilhafte Entscheidung beabsichtigen, so wird um vorherige Gewährung rechtlichen Gehörs gebeten, also um einen Hinweis und um Einräumung einer Gelegenheit zur Ergänzung der Ausführungen.

Die Beschwerdeführer sind mit einer Entscheidung ohne mündliche Verhandlung einverstanden, wenn das Gericht eine solche nicht für erforderlich erachtet.

5. Anhang (Verhältnismäßigkeit einer Vorratsspeicherung von Verkehrsdaten)

Die relevanten Ausführungen bei Breyer, Vorratsspeicherung (2005)[180], Seiten 133-261 zur Verhältnismäßigkeit einer Vorratsspeicherung von Verkehrsdaten lauten im Einzelnen wie folgt:

Verhältnismäßigkeitsprinzip

Aus dem Rechtsstaatsprinzip folgt das Gebot der Verhältnismäßigkeit[181]. Eine Beschränkung von Grundrechten ist danach nur insoweit zulässig, wie sie zur Erreichung des angestrebten Zweckes geeignet und erforderlich ist und der mit ihr verbundene Eingriff seiner Intensität nach nicht außer Verhältnis zur Bedeutung der Sache und den von den Betroffenen hinzunehmenden Einbußen steht[182].

Eignung

Was das erste Erfordernis der grundsätzlichen Eignung einer Maßnahme angeht, so hat das Bundesverfassungsgericht eine Regelung des Volkszählungsgesetzes 1983 für ungeeignet erklärt, wonach zu statistischen Zwecken erhobene Daten an die Meldebehörden weitergegeben werden durften[183]. Für den Bürger sei nicht vorhersehbar, zu welchen konkreten Zwecken die Daten von den Meldebehörden verwendet und an andere Stellen weitergegeben würden[184]. Dies habe zur Folge, dass die „Bereitschaft, wahrheitsgemäße Angaben zu machen, nicht herzustellen" sei[185], was wiederum die „Funktionsfähigkeit der amtlichen Statistik" zumindest „auf Dau-

[180] Breyer, (Fn. 8).
[181] BVerfGE 43, 127 (133); BVerfGE 61, 126 (134); BVerfGE 80, 109 (120).
[182] BVerfGE 65, 1 (54).
[183] BVerfGE 65, 1 (64).
[184] BVerfGE 65, 1 (64).
[185] BVerfGE 65, 1 (50).

er" gefährde[186]. „Läßt sich die hochindustrialisierte Gesellschaften kennzeichnende ständige Zunahme an Komplexität der Umwelt [aber] nur mit Hilfe einer zuverlässigen Statistik aufschlüsseln und für gezielte staatliche Maßnahmen aufbereiten, so läuft die Gefährdung der amtlichen Statistik darauf hinaus, eine wichtige Voraussetzung sozialstaatlicher Politik in Frage zu stellen."[187] Das Bundesverfassungsgericht verneint die Eignung der Regelung zur Datenweitergabe also bereits wegen einer graduellen Gefährdung des Zwecks der Volkszählung.

Systematisch ist diese Überlegung allerdings richtigerweise erst bei der Beurteilung der Verhältnismäßigkeit im engeren Sinne anzustellen: Im Beispiel der Volkszählung überwiegt das Gewicht der beeinträchtigten Bürgerrechte und das Bedürfnis nach einer zutreffenden Statistik den Nutzen einer Regelung, die eine uferlose Weitergabe von Daten erlaubt. Bei der Beurteilung der Frage, ob das Maß an Eignung einer Regelung ihren Schaden überwiegt, ist eine Abwägung widerstreitender Interessen erforderlich, weswegen diese Prüfung systematisch im Rahmen der Verhältnismäßigkeit im engeren Sinne zu erfolgen hat.

Für die isolierte Eignungsprüfung muss es demgegenüber genügen, wenn die abstrakte Möglichkeit der Zweckerreichung besteht, die zugelassenen Maßnahmen also nicht von vornherein untauglich sind, sondern dem gewünschten Erfolg förderlich sein können[188]. Dabei muss der Erfolg nicht in jedem Einzelfall tatsächlich erreichbar sein[189]; die Formulierung abstrakter Rechtssätze kann es vielmehr mit sich bringen, dass von dem Wortlaut einer Regelung auch Fälle erfasst werden, in denen der Zweck der Norm nicht erreicht werden kann. Dies bedarf allerdings zweierlei Ergänzungen: Erstens muss der Normgeber, gerade bei erheblichen Belastungen der Grundrechtsträger, die Norm so genau wie möglich formulieren. Gibt es daher abstrakt bestimmbare Fallgruppen, in denen Eingriffe stets zu Erreichung des Zwecks ungeeignet sind, dann muss eine Norm diese Fallgruppen ausdrücklich von ihrem Anwendungsbereich ausnehmen[190]. Zweitens begegnen der Exekutive bei der Vornahme von Eingriffen in Einzelfällen die bei der Formulierung abstrakter Rechtssätze bestehenden Schwierigkeiten nicht.

186 BVerfGE 65, 1 (64).
187 BVerfGE 65, 1 (50 f.).
188 BVerfGE 30, 292 (316); BVerfGE 67, 157 (175); BVerfGE 100, 313 (373).
189 BVerfGE 67, 157 (175).
190 Vgl. BVerfGE 100, 313 (384 f.); ähnlich L/D³-Bäumler, J 34 zu Generalklauseln.

Dementsprechend sind eingreifende Gesetze der so genannten Wechselwirkungslehre zufolge strikt im Lichte des jeweiligen Grundrechts auszulegen. Auf der Verwaltungsvollzugsebene bedeutet dies, dass in jedem Einzelfall geprüft werden muss, ob eine Maßnahme zur Erreichung ihres Zwecks geeignet ist[191]. Steht schon von vornherein fest, dass eine Einzelmaßnahme den gewünschten Erfolg nicht fördern kann, dann ist ihr Vollzug unzulässig.

In Bezug auf die Pläne zur Einführung einer Vorratsspeicherung von Verkehrsdaten lässt sich eine abstrakte Eignung zur Förderung des angestrebten Zwecks nicht bestreiten: Es ist nicht von vornherein ausgeschlossen, dass eine Vorratsspeicherung in einzelnen Fällen der Erreichung des jeweils angestrebten Zwecks – nämlich der Förderung der Strafverfolgung oder der Gefahrenabwehr – förderlich sein kann.

Erforderlichkeit

Verhältnismäßig ist eine Grundrechtseingriff weiterhin nur, wenn er sich auf das zur Zweckerreichung unerlässliche Minimum beschränkt[192]. Die Verfügbarkeit eines milderen Mittels gegenüber dem gewählten führt aber nur dann zur zwangsläufigen Verfassungswidrigkeit eines Eingriffs, wenn der Einsatz des milderen Mittels die Erreichung des angestrebten Zwecks in gleichem Maße und mit der gleichen Sicherheit ermöglicht wie das gewählte Mittel[193]. Ist dies nicht der Fall, dann kann die Verfügbarkeit milderer Mittel nur im Rahmen einer Prüfung des allgemeinen Gleichheitssatzes eine Rolle spielen.

- Bisheriger Rechtszustand

Was die Ausgestaltung des staatlichen Zugriffs auf Telekommunikationsdaten durch den Gesetzgeber angeht, so lässt sich eine Reihe von verschieden stark belastenden Mitteln denken, welche die Verfolgung von Straftaten und die Abwehr von Gefahren fördern können. Gegenüber einer Verpflichtung zur generellen Aufbewahrung und Speicherung von Telekommunikationsdaten (Vorratsspeicherung) ist zunächst einmal der bestehende Rechtszustand ein milderes Mittel. Schon bisher unterliegen Telekommunikationsverbindungsdaten in gewissem Maße dem staatli-

191 BVerfGE 69, 161 (169).

192 BVerfGE 65, 1 (44); BVerfGE 67, 157 (177); BVerfGE 77, 1 (47).

193 BVerfGE 30, 292 (316 und 322); BVerfGE 67, 157 (176 f.); BVerfGE 100, 313 (375).

chen Zugriff. Den Strafverfolgungsbehörden sind Verbindungsdaten einerseits gemäß den §§ 100a, 100b StPO zu übermitteln, wenn die inhaltliche Überwachung der Telekommunikation angeordnet worden ist. Darüber hinaus ist ein isolierter Zugriff auf Verbindungsdaten nach den §§ 100g, 100h StPO zulässig.

Den allgemeinen Gefahrenabwehrbehörden sind demgegenüber bisher nur in Rheinland-Pfalz[194], Niedersachsen[195], Hessen[196] und Thüringen[197] Eingriffe in das Fernmeldegeheimnis gestattet. Dies verwundert, weil die Abwehr von Gefahren ein gewichtigeres Allgemeininteresse darstellt als die Strafverfolgung und somit an sich weitergehende Eingriffe rechtfertigt[198]. Diese unterschiedliche Gewichtung ist darauf zurückzuführen, dass nicht ohne Weiteres davon ausgegangen werden kann, dass mit einer verstärkten Strafverfolgung auch ein signifikant höheres Maß an Sicherheit einhergeht. Auch kann die Strafverfolgung, anders als die Gefahrenabwehr, dem Rechtsgüterschutz allenfalls mittelbar dienen. Die Landespolizeigesetze könnten den Zugriff auf Telekommunikationsverbindungsdaten daher eröffnen. Dabei ist einerseits Art. 10 GG zu zitieren und andererseits eine spezifische Ermächtigungsgrundlage für den Zugriff auf Verkehrsdaten zu schaffen. Letzteres Erfordernis folgt jedenfalls aus § 88 Abs. 3 S. 3 TKG.

Speziellen Gefahrenabwehrbehörden steht der Zugriff auf Verkehrsdaten schon heute offen. Das G10 ermächtigt die Verfassungsschutzbehörden des Bundes und der Länder, den Militärischen Abschirmdienst und den Bundesnachrichtendienst zum Zugriff auf Telekommunikationsinhalte und -umstände. Zudem dürfen diese Behörden bei Telekommunikations- und Teledienstanbietern Auskünfte über Telekommunikations-Verbindungsdaten einschließlich der Standortdaten empfangsbereiter Mobiltelefone[199] sowie über Teledienstnutzungsdaten „einholen" (§§ 8 Abs. 8 BVerfSchG, 10 Abs. 3 MAD-G, 8 Abs. 3a BND-G). Dieses Recht auf Auskunfterteilung ist allerdings nicht mit Zwang durchsetzbar[200]. Das Bundesamt für Verfassungsschutz

194 § 31 POG RLP.

195 §§ 33 ff. Nds. SOG.

196 § 10 HSOG; vgl. Schenke, JZ 2001, 997 (997).

197 § 34a Thür. PAG; Nowak, Peter: Lauschen zur Gefahrenabwehr, Telepolis, Heise-Verlag, 18.06.2002, www.heise.de/tp/deutsch/inhalt/te/12739/1.html.

198 BVerfGE 100, 313 (383 und 394 f.); Schenke, JZ 2001, 997 (997); vgl. auch Art. 13 Abs. 3 GG im Vergleich zu Art. 13 Abs. 4 GG sowie Art. 13 Abs. 7 GG.

199 BT-Drs. 14/7386, 40.

200 Vgl. § 8 Abs. 3 BVerfSchG und BT-Drs. 14/7386, 39; der Berliner Datenschutzbeauftragte, Bericht zum 31. Dezember 2001, LT-Drs. 15/591, 9 sieht schon keine Übermittlungspflicht.

darf zum Zweck der Terrorismusbekämpfung darüber hinaus technische Mittel zur Ermittlung der Kartennummer von Mobiltelefonen einsetzen (§ 9 Abs. 4 BVerfSchG). Der BND darf nach § 5 G10 außerdem internationale Telekommunikation nach Inhalt und Umständen verdachtslos überwachen, wobei Internet-Kommunikation nicht erfasst ist („soweit eine gebündelte Übertragung erfolgt"). Nach § 39 AWG darf das Zollkriminalamt zur Verhütung bestimmter Straftaten nach dem Außenwirtschafts- und dem Kriegswaffenkontrollgesetz auf Telekommunikationsinhalte und -umstände zugreifen.

Bei den genannten Regelungen geht es jeweils um Eingriffe, die im Einzelfall angeordnet werden müssen. Es liegt daher auf der Hand, dass die Erreichung des angestrebten Zwecks nicht immer in gleichem Maße und mit der gleichen Sicherheit ermöglicht wird wie es eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten ermöglichen würde. Dies gilt namentlich dann, wenn der Zugriff auf Daten aus der Vergangenheit erforderlich wird, diese aber bereits gelöscht worden sind. Der bestehende Rechtszustand kann daher nicht als gleichwertiges Mittel gegenüber einer generellen Verkehrsdatenspeicherung angesehen werden.

- Datenspeicherungspflicht im Einzelfall

Weiterhin ist eine Verpflichtung Privater zur unverzüglichen Aufbewahrung, Speicherung und Übermittlung von Telekommunikations-Verkehrsdaten im Einzelfall weniger belastend als eine Pflicht zur generellen Aufbewahrung und Speicherung der Daten (Vorratsspeicherung). Insoweit kommen die in der von Deutschland unterzeichneten[201] Cybercrime-Konvention des Europarates vorgesehenen Befugnisse in Betracht.

Zu beachten ist, dass sich der Anwendungsbereich dieser Konvention auf computergestützte Kommunikation beschränkt (Art. 1 CCC) und somit die Kommunikation beispielsweise per Telefon und Fax nicht erfasst. Weiterhin regelt die Konvention nur den Zugriff auf Verkehrsdaten im Rahmen von Strafverfahren. Deutschland ist allerdings durch die Konvention nicht gehindert, weiter gehende Regelungen vorzusehen.

---

201 EPIC/PI, Privacy and Human Rights 2002 (I), Teil II, 94.

Die Konvention sieht zunächst vor, dass die Vertragsstaaten ihre zuständigen Stellen ermächtigen, zu Zwecken der Strafverfolgung die unverzügliche Sicherung gespeicherter Verkehrsdaten anordnen zu dürfen (Art. 16 CCC). Soweit Verkehrsdaten also bereits bei einem Telekommunikations-, Tele- oder Mediendiensteunternehmen gespeichert sind, wird durch eine solche Anordnung sicher gestellt, dass die Daten nicht durch Löschung verloren gehen. Dies ist insbesondere in Bezug auf Abrechnungsdaten relevant, die in Deutschland bis zu sechs Monate lang aufbewahrt werden dürfen (§§ 97 Abs. 3 S. 3 TKG, 6 Abs. 7 S. 1 TDDSG, 19 Abs. 8 S. 1 MDStV).

Weiterhin sind die zuständigen Stellen befugt, zu Zwecken der Strafverfolgung die Erhebung und Aufzeichnung bestimmter, neu anfallender Verkehrsdaten durch den Anbieter eines Kommunikationsdienstes anzuordnen (Art. 20 CCC). Soweit also der Zugriff auf zukünftige Telekommunikations-Verkehrsdaten im Einzelfall erforderlich wird, stellt eine solche Anordnung eine Alternative zu der Einführung einer Vorratsspeicherung dar. Sie ist in den Fällen nützlich, in denen Verkehrsdaten ansonsten nicht aufgezeichnet würden oder wenn ein zeitgleicher Zugriff darauf erforderlich ist.

Trotz dieser weitgehenden Befugnisse nach der Cybercrime-Konvention handelt es sich wiederum um Einzelfallbefugnisse. Die Erreichung des angestrebten Zwecks wird daher nicht immer in gleichem Maße und mit gleicher Sicherheit ermöglicht wie durch eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten[202]. Dies gilt namentlich dann, wenn der Zugriff auf Daten aus der Vergangenheit erforderlich wird, die in der Zwischenzeit bereits gelöscht worden sind. Die Befugnisse nach der Cybercrime-Konvention, von deren beschränktem Anwendungsbereich abgesehen, können daher nicht als gleichwertiges Mittel im Vergleich zur Einführung einer Vorratsspeicherung angesehen werden.

- Ergebnis

Somit ist kein Mittel ersichtlich, dessen Einsatz die Erreichung des angestrebten Zwecks in gleichem Maße und mit gleicher Sicherheit fördert wie die Einführung ei-

202 A.A. Uhe/Herrmann, Überwachung im Internet (I), 164.

ner Vorratsspeicherung von Telekommunikations-Verkehrsdaten. Eine solche Maßnahme ist daher im abstrakten Sinne auch erforderlich.

Angemessenheit

Der Verhältnismäßigkeitsgrundsatz verlangt weiterhin, dass der Verlust an grundrechtlich geschützter Freiheit nicht in einem unangemessenen Verhältnis zu den Gemeinwohlzwecken stehen darf, denen die Grundrechtsbeschränkung dient[203]. Bei einer Gesamtabwägung zwischen der Schwere des Eingriffs und dem Gewicht der ihn rechtfertigenden Gründe muss die Grenze des Zumutbaren noch gewahrt sein[204]. Der Gesetzgeber muss zwischen den Allgemein- und Individualinteressen einen angemessenen Ausgleich herbeiführen[205]. Dabei sind der Grundsatz der grundrechtsfreundlichen Auslegung und die grundsätzliche Freiheitsvermutung zu beachten[206]. Jede Grundrechtsbeschränkung muss durch überwiegende Allgemeininteressen gerechtfertigt sein[207], so dass nicht jedes staatliche Interesse zur Rechtfertigung einer Grundrechtsbeschränkung genügt[208].

Fraglich ist, ob die Abwägung abstrakt anhand des Gewichts der betroffenen Rechtsgüter erfolgen kann. Gegen eine solche Abwägungsmethode sprechen die Schwierigkeiten bei der Bestimmung des Gewichts von Rechtsgütern im Vergleich zueinander. So hat das Bundesverfassungsgericht einerseits festgestellt, dass das Grundgesetz dem Fernmeldegeheimnis hohen Rang zuweise, weil es die freie Entfaltung der Persönlichkeit durch einen privaten, vor den Augen der Öffentlichkeit verborgenen Austausch von Nachrichten, Gedanken und Meinungen (Informationen) gewährleiste und damit die Würde des denkenden und freiheitlich handelnden Menschen wahre[209]. Andererseits hat das Gericht wiederholt[210] die unabweis-

---

203 BVerfGE 100, 313 (375 f.).

204 St. Rspr. des BVerfG seit E 4, 7 (15 f.); in neuerer Zeit BVerfGE 78, 77 (85 und 87).

205 BVerfGE 100, 313 (375 f.).

206 BVerfGE 6, 55 (72); BVerfGE 32, 54 (72); BVerfGE 55, 159 (165); BVerfGE 103, 142 (153): „Derjenigen Auslegung einer Grundrechtsnorm ist der Vorrang zu geben, die ihre Wirksamkeit am stärksten entfaltet."

207 St. Rspr. seit BVerfGE 65, 1 (44, 46); in neuerer Zeit etwa BVerfGE 100, 313 (375 f.); BVerfGE 109, 279 (376).

208 EGMR, Klass u.a.-D (1978), EuGRZ 1979, 278 (285), Abs. 49; SächsVerfGH, JZ 1996, 957 (965); IWGDPT, Terrorismus (I); L/D³-Bäumler, J 680: vermutete Nützlichkeit ist ungenügend; Lisken, ZRP 1990, 15 (16): „Es genügt nicht, dass die vom Gesetzgeber auszuwählenden Methoden im Sinne größtmöglicher Verwaltungseffektivität ‚erforderlich' erscheinen."; Minderheitenvotum in BVerfGE 30, 1 (46): „Die ‚Staatsraison' ist kein unbedingt vorrangiger Wert.".

209 BVerfGE 67, 157 (171).

210 Etwa BVerfGE 44, 353 (374) m.w.N.; BVerfGE 46, 214 (222); BVerfGE 77, 65 (76); BVerfGE 80, 367 (375); BVerfGE 103, 21 (33).

baren Bedürfnisse einer wirksamen Strafverfolgung und Verbrechensbekämpfung sowie das öffentliche Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafprozess betont, die wirksame Aufklärung gerade schwerer Straftaten als einen wesentlichen Auftrag eines rechtsstaatlichen Gemeinwesens bezeichnet und die Notwendigkeit der Aufrechterhaltung einer funktionstüchtigen Rechtspflege, ohne die der Gerechtigkeit nicht zum Durchbruch verholfen werden könne, hervorgehoben[211]. In einer Entscheidung des Gerichts heißt es dazu: „Die Sicherheit des Staates als verfaßter Friedens- und Ordnungsmacht und die von ihm zu gewährende Sicherheit seiner Bevölkerung sind Verfassungswerte, die mit anderen im gleichen Rang stehen und unverzichtbar sind, weil die Institution Staat von ihnen die eigentliche und letzte Rechtfertigung herleitet."[212] Gegenüber diesen Interessen der Allgemeinheit komme dem Persönlichkeitsrecht allerdings keine geringere Bedeutung zu[213]. Vielmehr betont das Bundesverfassungsgericht, dass die Überwachung des Fernmeldeverkehrs nicht nur zu Verhaltensanpassungen bei einer Vielzahl einzelner Grundrechtsträger führen könne, sondern auch die freie Kommunikation der Gesellschaft insgesamt gefährde[214]. Eine freie Kommunikation sei „elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens"[215]. Im Ergebnis zeigen diese Ausführungen, dass sich eine Abwägung nicht schon abstrakt auf Rechtsgüterebene vornehmen lässt. Nutzen und Schaden einer Regelung müssen vielmehr im Einzelnen festgestellt und abgewogen werden.

Die aufgezeigten Umschreibungen des Gebots der Verhältnismäßigkeit im engeren Sinne machen deutlich, dass bei der Abwägung der gesamte Verlust an grundrechtlich geschützter Freiheit zu berücksichtigen ist („Gesamtabwägung"). Greift eine Maßnahme also in mehrere Grundrechte ein, so müssen sich die damit verfolgten Gemeinwohlzwecke an dem gesamten Gewicht des Eingriffs messen lassen. Es kann nicht richtig sein, die Verhältnismäßigkeit nur für jedes Grundrecht gesondert zu prüfen und dadurch die verfolgten Gemeinwohlzwecke mehrfach in die Waagschale zu werfen. Daraus folgt, dass sich die Unverhältnismäßigkeit einer Regelung

211 Nachweise bei BVerfGE 34, 238 (248 f.).
212 BVerfGE 49, 24 (56 f.).
213 BVerfGE 85, 367 (375); BVerfGE 106, 28 (49).
214 BVerfGE 100, 313 (381).
215 BVerfGE 65, 1 (43).

auch erst aus der Summe ihrer nachteiligen Wirkungen auf verschiedene Grundrechte ergeben kann.

Gewichtung der geförderten Interessen

Auf Seiten der Gemeinwohlinteressen ist für die Abwägung das Gewicht der Ziele und Belange maßgeblich, denen die Grundrechtsbeschränkung dient. Bei deren Gewichtung kommt es unter anderem darauf an, wie groß die Gefahren sind, denen mit Hilfe der Eingriffe begegnet werden soll, und wie wahrscheinlich deren Eintritt ist[216]. Die Gewährleistung der physischen Integrität von Personen rechtfertigt weiter gehende Freiheitseingriffe als die Verfolgung nur sozialer oder ökonomischer Ziele[217]. Wenn der Allgemeinheit eine Gefahr droht, sind weitergehende Eingriffe zulässig, als wenn es nur um die Rechtsgüter Einzelner geht[218]. Neben dem Gewicht der Belange, denen eine Grundrechtsbeschränkung dient, kann auch das Maß an Eignung der Grundrechtsbeschränkung zur Förderung dieser Belange für die Frage ihrer Angemessenheit nicht ohne Bedeutung sein. Mit dem Schutzzweck der Grundrechte ließe es sich nämlich nicht vereinbaren, wenn eine kaum effektive, aber mit schwerwiegenden Grundrechtsbeschränkungen verbundene Norm alleine deshalb als verhältnismäßig anzusehen wäre, weil sie in seltenen Fällen dem Schutz höchster Gemeinschaftsgüter dienen kann.

Gewichtung der beeinträchtigten Interessen

Das Gewicht eines Eingriffs bemisst sich der Rechtsprechung des Bundesverfassungsgerichts zufolge danach, unter welchen Voraussetzungen Eingriffe zulässig sind, welche und wie viele Grundrechtsträger von ihnen betroffen sind und wie intensiv die Grundrechtsträger beeinträchtigt werden[219]. Zu berücksichtigen ist auch, ob und in welcher Zahl Personen mitbetroffen werden, die für den Eingriff keinen Anlass gegeben haben[220]. Die Eingriffsintensität hängt bei Informationseingriffen unter anderem von Art, Umfang und denkbaren Verwendungen der erhobenen Da-

216 BVerfGE 100, 313 (376).
217 Callies, ZRP 2002, 1 (7).
218 Ossenbühl, Tatsachenfeststellungen und Prognoseentscheidungen, 509.
219 BVerfGE 109, 279 (353).

ten sowie von der Gefahr ihres Missbrauchs ab[221]. Bei der Feststellung der Möglichkeiten zur Verwendung erlangter Daten ist zu berücksichtigen, ob die Betroffenen anonym bleiben und welche Nachteile ihnen aufgrund der Maßnahmen drohen oder von ihnen nicht ohne Grund befürchtet werden[222]. Bei der Gewichtung möglicher Nachteile ist die Nutzbarkeit und Verwendungsmöglichkeit der Daten maßgeblich, und zwar unter besonderer Berücksichtigung der Möglichkeit, dass die Daten mit anderen Daten kombiniert und dadurch weitergehende Kenntnisse gewonnen werden können[223].

Für die Beurteilung der Verhältnismäßigkeit sind primär die rechtlich zulässigen Verwendungsmöglichkeiten maßgeblich. Einzubeziehen sind aber auch die sonstigen, tatsächlich und technisch vorhandenen Verwendungsmöglichkeiten. Dies ist einerseits vor dem Hintergrund erforderlich, dass sich die rechtlichen Grenzen des staatlichen Zugriffs vergleichsweise leicht erweitern lassen, nachdem die grundsätzliche Zugriffsmöglichkeit erst einmal eingeführt und die erforderliche Überwachungsstruktur aufgebaut worden ist[224]. Die unzählige Male vorgenommene Ausweitung des Straftatenkatalogs in § 100a StPO zeigt, wie wahrscheinlich eine solche Entwicklung auch in anderen Bereichen ist. Zum anderen ist auch an die Gefahr eines illegalen Missbrauchs zu denken, gerade dort, wo dieser nur schwer zu bemerken ist. Zwar ist, was den Staat selbst angeht, die bloß abstrakte Möglichkeit eines Missbrauches, das heißt unbegründete Befürchtungen dahin gehend, nicht zu berücksichtigen, weil grundsätzlich davon auszugehen ist, dass eine Norm „in einer freiheitlich-rechtsstaatlichen Demokratie korrekt und fair angewendet wird"[225]. Eine reale Missbrauchsgefahr ist im Rahmen der Abwägung demgegenüber durchaus zu berücksichtigen[226]. Die Grundrechte schützen den Einzelnen nämlich auch „vor fehlerhafter, mißbräuchlicher oder exzessiver Verwertung von Kommunikationsdaten durch

---

220 BVerfGE 109, 279 (353).

221 BVerfGE 65, 1 (46).

222 BVerfGE 100, 313 (376).

223 BVerfGE 65, 1 (45).

224 Vgl. Dembart, Lee: The End User Privacy undone, International Herald Tribune, 10.06.2002, coranet.radicalparty.org/-pressreview/print_250.php?func=detail&par=2477 über die Vorratsspeicherung von Verkehrsdaten, die ursprünglich als Maßnahme gegen den Terrorismus dargestellt wurde: „As surely as night follows day, law enforcement will use that database to investigate things other than terrorism." Vgl. auch Kaleck, Wolfgang u.a.: Stellungnahme von Bürgerrechtsorganisationen zur Anhörung des Innenausschusses des Deutschen Bundestages am 30.11.2001 zum Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz), www.cilip.de/terror/atg-stell-281101.pdf, 5; Ruhmann/Schulzki-Haddouti, Abhör-Dschungel (I).

225 BVerfGE 30, 1 (27).

226 BVerfGE 65, 1 (45 f.).

[...] staatliche Stellen"[227]. Die „in der Gesprächsbeobachtung liegende Gefahr einer Grundrechtsverletzung der [...] Gesprächsteilnehmer wie auch die Gefahr der Sammlung, Verwertung und Weitergabe der Informationen zu anderen Zwecken" als den gesetzlich vorgesehenen darf daher nicht aus den Augen verloren werden[228]. Wenn das Fernmeldegeheimnis das unbefangene Gebrauchmachen von Grundrechten in einer Demokratie schützen soll, dann darf außerdem nicht unberücksichtigt bleiben, dass sich der einzelne Bürger bei seinen Entscheidungen weniger durch die Feinheiten der Gesetzesformulierung beeindrucken lassen wird als vielmehr durch seine Eindrücke, Emotionen und Befürchtungen. Dementsprechend kommt es im Rahmen der Abwägung auch nicht nur darauf an, welche Nachteile den Grundrechtsträgern konkret aufgrund der Überwachungsmaßnahmen drohen. Ebenso zu berücksichtigen sind entferntere Risiken, deren Eintritt von den Bürgern nicht ohne Grund befürchtet wird[229]. Das Gewicht drohender oder befürchteter Nachteile in der Abwägung hängt dabei unter anderem von der Wahrscheinlichkeit des Eintritts eines Schadens und von dessen potenziellem Ausmaß ab.

Auf die Frage, inwieweit von einer gesetzlichen Eingriffsermächtigung tatsächlich Gebrauch gemacht wird, kann es bei der Beurteilung der Eingriffsintensität richtigerweise nicht ankommen[230], weil eine Vollzugspraxis jederzeit geändert werden kann[231] und weil der Gesetzgeber verpflichtet ist, die wesentlichen Eingriffsgrenzen selbst zu regeln. Eine Verwaltungspraxis ist für die Betroffenen regelmäßig nicht vorhersehbar und daher bei der Verhältnismäßigkeitsprüfung ohne Bedeutung[232]. Zwar entspricht es der Eigenart von Rechtsnormen, dass diese bis zu einem gewissen Grad allgemein gehalten sind. Nichtsdestotrotz muss der Gesetzgeber eine Norm jedenfalls dann eingrenzen, wenn sie ansonsten in abstrakt umschreibbaren Fallgruppen zu Eingriffen ermächtigen würde, in denen der Verhältnismäßigkeitsgrundsatz durchweg verletzt würde[233]. Dem Bundesverfassungsgericht ist daher entgegenzutreten, wenn es bei der Bestimmung des Gewichts eines Eingriffs damit argumentiert, dass dieser „sowohl rechtlich als auch tatsächlich begrenzt"[234] sei.

---

227 BVerfGE 85, 386 (397).

228 BVerfGE 85, 386 (400).

229 BVerfGE 100, 313 (376).

230 MVVerfG, LKV 2000, 149 (154); AK-GG-Bizer, Art. 10, Rn. 86; a.A. wohl BVerfGE 100, 313 (376 ff.).

231 Vgl. BVerfGE 100, 313 (380).

232 EGMR, Khan-GB (2000), Decisions and Reports 2000-V, Abs. 27.

233 Vgl. BVerfGE 100, 313 (384 f.).

234 BVerfGE 100, 313 (376).

Daneben ist zu beachten, dass rechtliche oder tatsächliche Begrenzungen gesetzlicher Eingriffsermächtigungen die Eignung der Maßnahme für den angestrebten Zweck beeinträchtigen können, etwa wenn eine Überwachungsmaßnahme nur einen Teil aller Kommunikationsvorgänge erfasst. Gerade wo vorhersehbar ist, welche Kommunikationsvorgänge nicht erfasst werden, bieten sich Schlupflöcher, die insbesondere von denjenigen genutzt werden, die ein Maximum an krimineller Energie aufwenden und denen die Regelung daher zuvörderst gilt[235]. Eine solchermaßen reduzierte Eignung geht zu Lasten der Verhältnismäßigkeit einer Maßnahme und kann schwerer wiegen als der Nutzen einer Begrenzung. Insgesamt sind Begrenzungen daher differenziert zu beurteilen.

Berücksichtigung von Sekundärzwecken

Fraglich ist, welchen Einfluss es auf die Abwägung hat, wenn der Gesetzgeber die Verwendung der aus einem Informationseingriff erlangten Daten nicht nur zu den Zwecken erlaubt, derentwegen er zu dem Informationseingriff ermächtigt hat (Primärzwecke), sondern wenn er zusätzlich zur Zweitverwendung erlangter Daten zu anderen Zwecken (Sekundärzwecke) ermächtigt. So könnte der Gesetzgeber beispielsweise bestimmen, dass Telekommunikations-Verbindungsdaten, die nach § 100g StPO zur Verfolgung einer Straftat erheblicher Bedeutung erhoben wurden, auch zur Verfolgung von Bagatellstraftaten verwendet werden dürfen. Fest steht, dass die erstmalige Kenntnisnahme von Informationen zu einem Zweck, dessen Verfolgung der Gesetzgeber nur für bereits erlangte Daten erlaubt, rechts- und verfassungswidrig wäre[236]. Darf ein Sekundärzweck bei der Entscheidung über eine Maßnahme aber keine Rolle spielen, dann darf sein möglicher Nutzen bei der Beurteilung der Verfassungsmäßigkeit der Maßnahme auch nicht berücksichtigt werden. Ob der Sekundärzweck durch eine im Hinblick auf einen ganz anderen Zweck vorgenommene Maßnahme gefördert werden kann, ist insoweit nämlich rein zufällig. Will der Gesetzgeber schon den ursprünglichen Eingriff mit einer möglichen Förderung von Sekundärzwecken legitimieren, dann muss er dazu ermächtigen, den Eingriff von vornherein zur Verfolgung dieser Zwecke vorzunehmen. Tut er dies nicht, so

235 Germann, 325.

236 Vgl. BVerfGE 67, 157 (180 f.).

müssen Regelungen über eine mögliche Weitergabe von Daten an andere Stellen bei der Frage der Zumutbarkeit des ursprünglichen Eingriffs außer Betracht bleiben. Sie stellen einen eigenständigen Eingriff dar, dessen Zulässigkeit gesondert zu prüfen ist. Spiegelbildlich bleiben bei der Prüfung der mit dem Eingriff verbundenen Gefahren diejenigen Gefahren außer Betracht, die erst aus der weiteren staatlichen Verwendung erlangter Daten zu Sekundärzwecken resultieren.

Unsicherheitssituationen

Die Prüfung der Verhältnismäßigkeit einer Maßnahme wird nicht selten durch Unsicherheiten tatsächlicher Art erschwert. Wenn entweder schon die gegenwärtige Sachlage unbekannt ist oder aber sich zukünftige Entwicklungen nicht sicher abschätzen lassen, ist die Anwendung des Verhältnismäßigkeitsprinzips nicht ohne weiteres möglich. Bei der Überprüfung der Verfassungsmäßigkeit von Gesetzen gebietet es das Demokratieprinzip (Art. 20 Abs. 1 GG), dass der demokratisch gewählte und verantwortliche Gesetzgeber das letzte Wort haben muss und nicht das Bundesverfassungsgericht. Dem Gesetzgeber kommt in Unsicherheitssituationen also ein Einschätzungsspielraum zu[237]. Innerhalb gewisser Grenzen obliegt ihm die Entscheidung, in welchem Umfang er Anstrengungen zur Aufklärung der maßgeblichen Tatsachen unternimmt und, soweit er von einer Aufklärung absieht oder eine Klärung nicht möglich ist, von welchen Tatsachen und zukünftigen Entwicklungen er für seine Entscheidung ausgeht.

Der Einschätzungsspielraum des Gesetzgebers bezieht sich wohlgemerkt nur auf Tatsachen und nicht auf Rechtsfragen[238]; die letztverbindliche Auslegung und Anwendung des Rechts obliegt nach der Kompetenzordnung des Grundgesetzes den Gerichten und nicht dem Gesetzgeber. Daraus folgt, dass der Gesetzgeber das Vorliegen rechtlicher Merkmale, etwa der Eignung einer Norm, nicht einfach annehmen darf. Sein Einschätzungsspielraum ist erst dann einschlägig, wenn er konkrete Annahmen über Tatsachen macht. Erst diese Tatsachen können dann den Rechtsbegriff ausfüllen, also beispielsweise die Eignung der Norm begründen.

---

237 St. Rspr. des BVerfG seit E 50, 290 (332 f.); in neuerer Zeit etwa BVerfGE 90, 145 (173); ebenso für den Verordnungsgeber BVerfGE 53, 135 (145) und BVerfG, NJW 2002, 1638 (1639).

238 Baumeister, Das Rechtswidrigwerden von Normen, 235 ff.

Wie weit der Einschätzungsspielraum des Gesetzgebers reicht, hängt einerseits von den verfügbaren Möglichkeiten der Bildung eines sicheren Urteils ab[239]. Diese sind reduziert, wenn ein Sachgebiet raschen Veränderungen unterliegt oder der Regelungsgegenstand komplex und schwer überschaubar ist[240]. Daneben sind für die Bemessung des Einschätzungsspielraums auch das Gewicht der auf dem Spiel stehenden Rechtsgüter[241] und, bei Grundrechtseingriffen, die Eingriffsintensität maßgeblich[242]. Während zumutbare, schon vor Normerlass bestehende Aufklärungsmöglichkeiten sowie hohe aufgrund einer Norm drohende Belastungen den Handlungsspielraum des Gesetzgebers reduzieren, eröffnen ihm wahrscheinliche Gefahren für wichtige Rechtsgüter einen erweiterten Handlungsspielraum. Äußere oder vom Gesetzgeber zu vertretende Umstände wie Zeitnot oder unzureichende Beratung begründen keine Einschätzungsspielräume des Gesetzgebers[243].

Mit dem variablen Einschätzungsspielraum des Gesetzgebers korrespondiert ein variabler Maßstab bei der verfassungsrechtlichen Prüfung. Teilweise hat es das Bundesverfassungsgericht genügen lassen, wenn die Einschätzung des Gesetzgebers nicht evident unzutreffend war[244], etwa wo es um den Grundlagenvertrag mit der DDR[245] oder um das Weinwirtschaftsgesetz[246] ging. Bei Eingriffen niedriger Intensität ist der Gesetzgeber auch nicht zu tatsächlichen Feststellungen verpflichtet[247]. In Fällen von größerem Gewicht hat das Bundesverfassungsgericht verlangt, dass die Einschätzung des Gesetzgebers vertretbar sein müsse[248]. Insoweit sei erforderlich, dass der Gesetzgeber durch Ausschöpfung der ihm zugänglichen Erkenntnisquellen[249] die maßgeblichen gegenwärtigen und vergangenen Tatsachen möglichst vollständig ermittele[250], um eine möglichst zuverlässige Einschätzung treffen zu können[251]. Auf welche Weise der Gesetzgeber die maßgeblichen Tatsachen feststellt,

239 BVerfGE 50, 290 (332 f.); BVerfGE 57, 139 (159); BVerfGE 62, 1 (50); BVerfGE 106, 62 (152).
240 BVerfGE 50, 290 (333); BVerfGE 106, 62 (152).
241 BVerfGE 50, 290 (333); BVerfGE 106, 62 (152).
242 BVerfGE 90, 145 (173).
243 BVerfGE 106, 62 (152).
244 BVerfGE 36, 1 (17); BVerfGE 40, 196 (223).
245 BVerfGE 36, 1 (17 f.).
246 BVerfGE 37, 1 (20 f.).
247 BVerfGE 88, 203 (310).
248 BVerfGE 25, 1 (12 f. und 17); BVerfGE 39, 210 (225 f.).
249 BVerfGE 50, 290 (333 f.).
250 BVerfGE 106, 62 (151).
251 BVerfGE 50, 290 (334).

ist grundsätzlich ihm überlassen[252]. Von dem Vertretbarkeitsmaßstab ist das Bundesverfassungsgericht etwa im Volkszählungsurteil ausgegangen[253]. Wo es um zentrale Rechtsgüter wie die Gesundheit oder Freiheit einer Person ging, hat das Gericht schließlich eine eigene und intensive inhaltliche Kontrolle vorgenommen[254]. Dieser Maßstab wurde auch bei Gesetzen angewandt, welche die freie Berufswahl einschränkten[255].

Zu beachten ist, dass die unterschiedliche Kontrollintensität auf den beiden letztgenannten Stufen nur quantitativer Art ist[256], weswegen die Bedeutung der Unterscheidung zwischen diesen beiden Stufen nicht überbewertet werden darf. Der Prüfungsmaßstab unterscheidet sich lediglich in den unterschiedlichen Anforderungen, die an die Eindeutigkeit des Prüfungsergebnisses gestellt werden[257]. Auch die Dogmatik zu Art. 3 Abs. 1 GG unterscheidet nur zwischen einer Willkürprüfung einerseits und einer Verhältnismäßigkeitsprüfung andererseits, was dafür spricht, dies im Bereich anderer Grundrechte ebenso zu handhaben.

In dem aufgezeigten Rahmen ist der Gesetzgeber zur Feststellung aller gegenwärtigen und vergangenen Tatsachen verpflichtet, von denen die Verfassungsmäßigkeit eines Gesetzes abhängt[258]. Diese Pflicht des Gesetzgebers ist aus dem Rechtsstaatsprinzip herzuleiten[259], aus dem sich auch weitere Eingriffsgrenzen ergeben: Schon das allgemeine Verwaltungsrecht folgert aus dem Rechtsstaatsprinzip, dass Eingriffe der Verwaltung vor der vollständigen Ermittlung des Sachverhalts nur ausnahmsweise gerechtfertigt sind[260]. Auch auf dem Gebiet des Polizeirechts entnimmt man dem Rechtsstaatsprinzip, dass in Fällen von Gefahrenverdacht grundsätzlich nur vorläufige Eingriffe zulässig sind, die keinen irreparablen Schaden anrichten und die allein der Gefahrenerforschung dienen dürfen[261]. Diese Grundgedanken müssen auch für Maßnahmen des Gesetzgebers gelten, für den das Rechtsstaatsprinzip

252 BVerfGE 106, 62 (151).
253 BVerfGE 65, 1 (55 f.).
254 BVerfGE 7, 377 (415); BVerfGE 45, 187 (238).
255 Etwa BVerfGE 7, 377.
256 Chryssogonos, Verfassungsgerichtsbarkeit und Gesetzgebung, 187.
257 Chryssogonos, Verfassungsgerichtsbarkeit und Gesetzgebung, 187.
258 BVerfGE 106, 62 (150).
259 Zur Ableitung von Verhaltenspflichten des Gesetzgebers aus dem Rechtsstaatsprinzip Köck, VerwArch 93 (2002), 1 (15 und 18) m.w.N.
260 Stelkens/Bonk/Sachs-Stelkens/Stelkens, § 35, Rn. 175.
261 L/D^3-Denninger, E 38; Schenke, Polizei- und Ordnungsrecht, Rn. 86 f.

ebenso verbindlich ist[262]. In Unsicherheitssituationen sind irreparable Grundrechtseingriffe durch den Gesetzgeber daher grundsätzlich erst dann zulässig, wenn der Gesetzgeber die ihm zugänglichen Erkenntnisquellen ausgeschöpft und die maßgeblichen gegenwärtigen und vergangenen Tatsachen möglichst vollständig ermittelt hat. Insofern tritt von Verfassungs wegen eine „Beweislastumkehr" ein, der zufolge der Gesetzgeber die Verfassungsmäßigkeit einer geplanten Norm nachweisen muss, bevor er sie erlassen darf[263]. Nur unter außergewöhnlichen Umständen können Sofortmaßnahmen ohne die an sich erforderliche Aufklärung des Sachverhalts zulässig sein, nämlich wenn die Maßnahme zum Schutz wichtiger Rechtsgüter vor dringenden und hinreichend wahrscheinlichen Gefahren, hinter welche die beeinträchtigten Rechtspositionen zurücktreten müssen, erforderlich ist.

Ein Hauptanwendungsfall eines gesetzgeberischen Einschätzungsspielraums stellt die Eignung einer Norm zur Erreichung ihres Zwecks beziehungsweise das Maß an Eignung der Norm dar. Ist die Effektivität einer Regelung im Zeitpunkt ihres Erlasses noch nicht absehbar, dann ist dem Normgeber grundsätzlich die experimentelle Einführung der Regelung gestattet, wenn dies zur Gewinnung gesicherter Erkenntnisse über ihre Effektivität erforderlich ist[264]. Allerdings muss die begründete Erwartung der Effektivität der Regelung bestehen[265]. Auch ist das allgemeine Verhältnismäßigkeitsprinzip zu beachten, das der experimentellen Einführung einer Norm entgegen stehen kann. Überdies bleibt es dabei, dass die bereits vor Einführung der Norm zugänglichen Erkenntnisquellen vorab ausgeschöpft werden müssen, um die Eignung der Norm möglichst zuverlässig prognostizieren zu können.

Allgemein gilt für Prognosen über zukünftige Tatsachen folgendes: Die oben genannten Grundsätze bezüglich der Feststellung gegenwärtiger und vergangener Tatsachen gelten uneingeschränkt auch für die Feststellung derjenigen gegenwär-

---

262 Vgl. auch Ossenbühl, Tatsachenfeststellungen und Prognoseentscheidungen, 486: Bei zweifelhafter tatsächlicher Basis müsse der Gesetzgeber von Eingriffen absehen, „in dubio pro libertate"; ders., 487: Verfassungsrechtlich sei „eine verlässliche empirischen Basis" für einen Eingriff erforderlich, weil die Dispositionsfreiheit des Gesetzgebers lediglich im Bereich der Wertung, nicht aber im Bereich der Tatsachenfeststellung liege.

263 Lisken, ZRP 1990, 15 (16): Vorfeldbefugnisse müssten „unabweisbar, also nachweislich, für den Grundrechtsschutz notwendig" sein; Bürgerrechtsorganisationen: Die falsche Antwort auf den 11. September: Der Überwachungsstaat, Presseerklärung vom 24.10.2001, www.cilip.de/terror/pe241001.htm; Kaleck, Wolfgang u.a.: Stellungnahme von Bürgerrechtsorganisationen zur Anhörung des Innenausschusses des Deutschen Bundestages am 30.11.2001 zum Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz), www.cilip.de/terror/atg-stell-281101.pdf, 6; Ossenbühl, Tatsachenfeststellungen und Prognoseentscheidungen, 486.

264 SächsVerfGH, DuD 1996, 429 (435) für die Erhebung personenbezogener Daten zur Gefahrenabwehr unter verdeckter Anwendung technischer Mittel.

265 SächsVerfGH, DuD 1996, 429 (435) für die Erhebung personenbezogener Daten zur Gefahrenabwehr unter verdeckter Anwendung technischer Mittel.

tigen und vergangenen Tatsachen, die einer Prognose über zukünftige Tatsachen zugrunde liegen[266]. Hinsichtlich des angewandten Prognoseverfahrens hat das Bundesverfassungsgericht entschieden, dass es sich um ein angemessenes Verfahren handeln muss, dass das gewählte Verfahren konsequent verfolgt werden muss, dass in die Prognose keine sachfremden Erwägungen einfließen dürfen und dass das Prognoseergebnis ein vertretbares Resultat des Prozesses darstellen muss[267]. Was die Richtigkeit des Prognoseergebnisses anbelangt, so liegt es in der Natur der Sache, dass sich selbst die beste Prognose im zeitlichen Verlauf als falsch erweisen kann. Dieses Risiko kann einem Handeln des Gesetzgebers nicht von vornherein entgegen stehen, weil ein Nichthandeln des Gesetzgebers noch größere Risiken bergen kann. Soweit also das Prognoseergebnis nicht bereits durch gesicherte empirische Daten oder verlässliche Erfahrungssätze vorgeben ist[268], greift in Bezug auf das Prognoseergebnis wieder der oben aufgezeigte, variable Einschätzungsspielraum des Gesetzgebers ein[269].

Fraglich sind die Auswirkungen von Verstößen des Gesetzgebers gegen seine prozeduralen Pflichten. Verfassungswidrig ist eine Norm nach dem Gesagten jedenfalls dann, wenn sie aufgrund der bekannten tatsächlichen Umstände als unverhältnismäßig anzusehen ist. Gegebenenfalls kann das Bundesverfassungsgericht während eines laufenden Verfahrens eigene Maßnahmen zur Aufklärung des Sachverhalts treffen. Dies wird insbesondere bei belastungsintensiven Normen in Betracht kommen. Mangels Ursächlichkeit für den Verfassungsverstoß sind Verfahrensfehler unbeachtlich, wenn sich die Norm auf andere, zutreffende Tatsachen stützen lässt, deren Vorliegen sich im Rahmen der gerichtlichen Prüfung ergibt[270].
Problematisch sind Fälle, in denen sich die Verfassungsmäßigkeit einer Norm nicht beurteilen lässt, weil der Gesetzgeber seiner Aufklärungspflicht nicht nachgekommen ist. Erstens ist denkbar, Verletzungen der Pflicht an keine Konsequenzen zu knüpfen außer an die Feststellung des Bestehens der Aufklärungspflicht durch das Bundesverfassungsgericht. Im Bereich der Grundrechte scheint diese Lösung den Grundrechtsschutz indes unangemessen zu verkürzen, weil sie es dem Gesetzgeber

266 BVerfGE 106, 62 (150 f.).
267 BVerfGE 106, 62 (152 f.).
268 BVerfGE 106, 62 (151).
269 BVerfGE 106, 62 (152).
270 BVerfGE 106, 62 (150 und 152).

erlaubt, durch Unterlassen einer Sachverhaltsaufklärung jedes Vorgehen gegen eine Norm zu blockieren. Dieser Ansatz ist daher abzulehnen.

Zweitens wird in Anlehnung an das Verwaltungsrecht[271] vertreten, ein Verstoß gegen prozedurale Pflichten des Gesetzgebers führe dann zur Verfassungswidrigkeit eines Gesetzes, wenn konkrete Anhaltspunkte im Einzelfall vorlägen, die es als möglich erscheinen lassen, dass die Einhaltung der prozeduralen Pflichten zu einer anderen Gesetzesfassung geführt hätte[272]. Gegen die Anwendung dieses verwaltungsrechtlichen Grundsatzes im vorliegenden Zusammenhang spricht, dass eine Prüfung der hypothetischen Kausalität bei Verletzungen der Aufklärungspflicht des Gesetzgebers regelmäßig ausgeschlossen ist. Der Grund für das Bestehen einer Aufklärungspflicht liegt gerade darin, dass bestimmte Tatsachen unbekannt sind und sich nicht ohne Weiteres einschätzen lassen. Lassen sich die maßgeblichen Tatsachen aber nicht einschätzen, dann kann auch nicht beurteilt werden, welche Entscheidung der Gesetzgeber bei Kenntnis dieser Tatsachen getroffen haben könnte. Auf die konkrete Möglichkeit einer anderen Gesetzesfassung kann es daher ebenfalls nicht ankommen.

Drittens kommt in Betracht, auf unzureichender Tatsachenbasis beschlossene Normen für verfassungswidrig zu erklären. Diesem Ansatz ist grundsätzlich zuzustimmen. Bei Grundrechtseingriffen ergibt sich aus dem Verhältnismäßigkeitsgebot regelmäßig, dass den Betroffenen eine möglicherweise verfassungswidrige Grundrechtsbeschränkung unzumutbar ist, wenn der Gesetzgeber die verfügbaren Erkenntnisquellen nicht ausgeschöpft hat. Nur in Ausnahmefällen ist es denkbar, dass eine Norm zum Schutz wichtiger Rechtsgüter vor wahrscheinlichen Gefahren unabdingbar sein kann, so dass von ihrer Verwerfung abgesehen werden muss.

Angemessenheit einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten

Im Folgenden wird die Angemessenheit einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten geprüft. Im Rahmen dieser Prüfung kommt es

271 Etwa BVerwGE 64, 33 (35 ff.).

272 Köck, VerwArch 93 (2002), 1 (19 f.).

auf eine Reihe von Tatsachen an, bezüglich derer erhebliche tatsächliche Unsicherheiten bestehen, etwa im Hinblick auf die Auswirkungen einer solchen Regelung. Aus diesem Grund fragt sich, welcher Einschätzungsspielraum dem Gesetzgeber insoweit zusteht.

Es ist zunächst nicht ersichtlich, dass der maßgebliche Sachverhalt raschen Veränderungen unterliegen könnte oder besonders komplex oder schwer überschaubar wäre. Eine Aufklärung der maßgeblichen Tatsachen ist bereits vor Einführung einer Vorratsspeicherung in vielerlei Hinsicht möglich und zumutbar, vor allem was das Maß an Eignung einer Vorratsspeicherung anbelangt. Eine Vorratsspeicherung von Verkehrsdaten würde im Wesentlichen nur eine quantitative Ausweitung der bestehenden Zugriffsbefugnisse auf Telekommunikations-Verkehrsdaten bewirken (z.B. § 100g StPO), weil eine größere Menge an Verkehrsdaten als bisher gespeichert würde. Dies macht es möglich, auch ohne die experimentelle Einführung einer Vorratsspeicherung deren mögliche Wirksamkeit zu überprüfen, indem man die zuständigen Behörden festhalten lässt, in wie vielen und in welchen Fällen ein Auskunftsersuchen daran scheitert, dass die gewünschten Daten nicht oder nicht mehr verfügbar sind. Anhand dieser Statistik ließe sich überprüfen, in wie vielen Fällen eine Vorratsspeicherung Abhilfe hätte schaffen können[273]. Die Aussagekraft der Statistik wäre weiter zu verbessern, indem auch der Anlass des Auskunftsersuchens registriert wird. Damit ließe sich überprüfen, ob es in einer erheblichen Anzahl von Fällen schwerer Kriminalität an Verkehrsdaten fehlt.

Auch mit Blick auf die Frage, inwieweit eine Vorratsspeicherung tatsächlich zur Abwehr von Gefahren oder zu strafgerichtlichen Verurteilungen führen könnte, ließen sich bereits durch die Evaluierung der bestehenden Befugnisse wichtige Anhaltspunkte gewinnen. Da die Einführung einer Vorratsspeicherung im Wesentlichen eine quantitative Ausweitung dieser Befugnisse zur Folge hätte, kann man davon ausgehen, dass der Anteil erfolgreicher Auskunftsersuchen im Falle einer generellen Vorratsspeicherung jedenfalls nicht niedriger liegen würde als bisher.

---

[273] Entsprechende Untersuchungen fordert auch ISPA, Internet Service Providers' Association (UK): Memorandum by the Internet Services Providers' Association (ISPA), 19 November 2001, www.parliament.the-stationery-office.co.uk/pa/-cm200102/cmselect/
cmhaff/351/351ap10.htm.

Die Evaluierung der bisher bestehenden Befugnisse für den Zugriff auf Telekommunikations-Verkehrsdaten müsste dazu freilich in Angriff genommen werden, was bisher – wie bei fast allen informationell eingreifenden Ermittlungsmaßnahmen – versäumt worden ist[274]. Während bereits im Bereich der Telekommunikationsüberwachung nach § 100a StPO vielfach beklagt wird, dass empirische kriminalistische Daten weitgehend unbekannt sind[275], existieren im Bereich des isolierten Zugriffs auf Verkehrsdaten bisher augenscheinlich keinerlei Statistiken[276].

Von der nationalen Ebene abgesehen existieren auf internationaler Ebene geradezu ideale Bedingungen für eine Evaluierung dadurch, dass einige EU-Staaten eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten bereits eingeführt haben und andere dies in Kürze zu tun beabsichtigen[277]. Dies macht es möglich, sowohl im zeitlichen Vergleich innerhalb dieser Staaten wie auch im Vergleich mit Staaten ohne Vorratsspeicherung zu überprüfen, inwieweit die Vorratsspeicherung den Gefahrenabwehr- und Strafverfolgungsbehörden tatsächlich hilft, in wie vielen und welchen Fällen die Vorratsspeicherung für die Gefahrenabwehr oder Strafverfolgung letztlich wesentlich war, ob es den Strafverfolgungsorganen gelungen ist, in die Reihe der Hintermänner organisierter Kriminalität einzudringen, und ob die Einführung der Vorratsspeicherung insgesamt eine spürbare Senkung des Kriminalitätsniveaus herbei geführt hat. Im Bereich der Netzkriminalität im engeren Sinne ließe sich als Indikator etwa die Aufklärungsquote in Bezug auf diese Delikte heranziehen. Diese Quote wird in den meisten Staaten ohnehin ermittelt und müsste einige Zeit nach der Einführung einer Vorratsspeicherung von Telekommunikations-Verkehrsdaten merklich ansteigen, wenn dieser Mechanismus tatsächlich effektiv sein sollte. In die Evaluierung ließen sich auch die negativen Effekte einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten einbeziehen, soweit sie offen zutage treten, etwa Standortverlagerungen von Firmen oder Preiserhöhungen.

Eine Vorratsspeicherung von Telekommunikationsdaten stellt einen empfindlichen Eingriff in die Privatsphäre der Betroffenen dar, weil die Kenntnis von Verkehrsdaten

---

274 Weichert, Bekämpfung von Internet-Kriminalität (I), Punkt 7.

275 Welp, TKÜV, 3 (7).

276 Fox, DuD 2002, 194 (194).

277 Übersicht bei MDG, EU-Questionnaire (I).

große Verknüpfungs- und Verwendungsmöglichkeiten eröffnet und dementsprechend einschneidende Folgen für die Betroffenen haben kann. Eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten würde dazu führen, dass es unbeobachtete Telekommunikation grundsätzlich nicht mehr gäbe. Sie rückt damit in die Nähe einer Antastung des Wesensgehaltes des Fernmeldegeheimnisses nach Art. 10 Abs. 1 Var. 3 GG und ist äußerst belastungsintensiv. Anders als im Bereich der Außenpolitik oder der Wirtschaftslenkung kann man daher nicht von einem Eingriff eher geringer Intensität ausgehen, der die Beschränkung auf eine Willkürprüfung erlauben würde.

Mit dem Volkszählungsurteil des Bundesverfassungsgerichts wird man vielmehr zumindest eine vertretbare Entscheidung des Gesetzgebers verlangen müssen, zumal das Volkszählungsgesetz 1983 nur eine inhaltlich begrenzte, einmalige und offene Datenerhebung zu primär statistischen Zwecken und damit eine erheblich weniger eingreifende Maßnahme vorsah. Die Anwendung des Vertretbarkeitsmaßstabs macht eine eigene inhaltliche Prüfung der Verhältnismäßigkeit im engeren Sinne erforderlich, anhand deren Ergebnis dann zu entscheiden ist, ob der Gesetzgeber vertretbar die Verhältnismäßigkeit einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten annehmen darf.

(aa) Durch Telekommunikation gefährdete Gemeinschaftsgüter, ihr Gewicht und die Wahrscheinlichkeit ihrer Beeinträchtigung

(i) Einschlägige Gemeinschaftsgüter

Im Rahmen der Abwägung ist auf Seiten der Gemeinwohlinteressen zunächst fraglich, welche Rechtsgüter die einschlägigen Regelungsvorschläge hinsichtlich der Einführung einer Vorratsspeicherung schützen sollen. Eine Verkehrsdatenspeicherung wird vor allem zur Effektivierung der Strafverfolgung angestrebt. Bei der Bemessung des Gewichts der Gewährleistung einer effektiven Strafverfolgung ist die Rechtsprechung des Bundesverfassungsgerichts zu beachten, der zufolge die Gewährleistung einer effektiven Strafverfolgung eine wesentliche Staatsaufgabe sein soll. Im Rahmen der Verhältnismäßigkeitsprüfung sieht das Gericht in der effektiven Strafverfolgung – teilweise spricht es auch von der „Rechtspflege" – ein eigenstän-

diges Verfassungsgut, das aus dem Rechtsstaatsprinzip herzuleiten sei und zu dessen Gewährleistung der Gesetzgeber verpflichtet sei[278]. Den Inhalt dieses Verfassungsgutes sieht das Gericht abstrakt in der „Durchsetzung von Gerechtigkeit", der Gewährleistung einer „wirksamen Strafverfolgung", einer „umfassenden Wahrheitsermittlung im Strafverfahren", der „Aufklärung schwerer Straftaten" und der „umfassenden Aufklärung der materiellen Wahrheit"[279], ohne dass es darauf ankomme, ob der konkrete Eingriff dem Schutz von Rechtsgütern dienen könne[280].

Diese Ansicht des Bundesverfassungsgerichts ist abzulehnen. Strafverfolgung ist kein Selbstzweck[281] und eine „geordnete Strafrechtspflege" als solche ist daher auch kein Verfassungswert[282]. Andernfalls könnte der Staat, der die Definitionsmacht über das Strafrecht hat, alle Grundrechte im Staatsinteresse relativieren[283]. Der Gedanke einer „Durchsetzung von Gerechtigkeit" im Strafverfahren zielt bei genauer Betrachtung auf nichts anderes als Vergeltung. Strafe als bloße Vergeltung für in der Vergangenheit begangenes Unrecht kann aber keine Eingriffe in Grundrechte legitimieren[284], jedenfalls keine Eingriffe in die Grundrechte Unbeteiligter, wie sie mit den meisten strafrechtlichen Ermittlungsverfahren verbunden sind.

Auch aus dogmatischer Sicht ist ein Verfassungsgut „Strafrechtspflege" abzulehnen. In der Abwägung mit Grundrechten und anderen Verfassungsgütern lässt sich das Gewicht eines derart abstrakten Verfassungsgutes nicht bestimmen. Daran ändert es nichts, wenn das Bundesverfassungsgericht allgemein feststellt, dass bei der Strafverfolgung höhere Eingriffsschwellen hingenommen werden müssen als bei der präventiven Gefahrenabwehr[285], dass Strafverfolgungsinteressen also von geringerem Gewicht sind als der unmittelbare Rechtsgüterschutz.

---

278 Etwa BVerfGE 77, 65 (76).

279 Etwa BVerfGE 77, 65 (76).

280 BVerfGE 107, 299 (324): „eigenständige verfassungsrechtliche Bedeutung".

281 BVerfGE 39, 1 (46); BGHSt 24, 40 (42): kein Schuldausgleich um seiner selbst willen.

282 L/D²-Lisken/Denninger, D 25.

283 L/D²-Lisken/Denninger, D 25, Fn. 81.

284 Vgl. schon Platon, in deutscher Übersetzung bei Niggli, Kriminologische Überlegungen zur Strafzumessung (I), 3: „Niemand bestraft einen Rechtsbrecher aufgrund abstrakter Überlegungen oder einfach deshalb, weil der Täter das Recht gebrochen hat, es sei denn einer nehme unbedacht Rache wie ein wildes Tier. Jener der mit Vernunft straft, rächt sich nicht für das geschehene Unrecht, denn er kann es nicht ungeschehen machen. Vielmehr schaut er in die Zukunft und versucht, den Täter und andere mit der Strafe davon abzuhalten, das Recht wieder zu brechen."

285 BVerfGE 100, 313 (394 ff.); ebenso Schenke, AöR 125 (2000), 1 (29); dagegen AK-GG-Bizer, Art. 10, Rn. 95.

Eingriffe können auch nicht allein mit dem Argument der Sicherung der Gleichmäßigkeit der Strafverfolgung legitimiert werden, also durch den bloßen Verweis darauf, dass Straftäter gegenwärtig in vielen Kriminalitätsbereichen nicht systematisch aufgespürt, sondern nur in vergleichsweise wenigen und vorwiegend leichten Fällen durch Zufall entdeckt werden können. Wenn die staatlichen Mittel zur Sicherung einer gleichmäßigen Strafverfolgung nicht ausreichen, dann spricht dies allein gegen die Verhältnismäßigkeit der jeweiligen Strafnorm selbst und wirft die Frage auf, ob das Strafrecht insoweit ein probates Mittel zur Erreichung des gesetzgeberischen Ziels ist. Zur Rechtfertigung weiter gehender Eingriffsbefugnisse können Vollzugsdefizite nicht heran gezogen werden, weil die Strafverfolgung kein Selbstzweck ist.

Fraglich ist, ob erweiterte Ermittlungsbefugnisse mit dem Verweis auf die Interessen des in einem Strafverfahren Beschuldigten gerechtfertigt werden können. Das Bundesverfassungsgericht argumentiert insoweit, dass Ermittlungsbefugnisse auch der Entlastung unschuldiger Beschuldigter dienen könnten, die ansonsten zu Unrecht einem Ermittlungsverfahren ausgesetzt oder gar verurteilt werden könnten. Ohne hinreichende Kenntnisse bestünde die Gefahr, dass Gerichte ihre Entscheidungen auf mangelhafter Tatsachengrundlage träfen[286].
Bei dieser Argumentation wird indes unbesehen davon ausgegangen, dass erweiterte Ermittlungsbefugnisse mehr Unschuldige ent- als belasten. Hiervon kann aber jedenfalls auf dem Gebiet des staatlichen Zugriffs auf Verkehrsdaten keine Rede sein. Verkehrsdaten dienen im Wesentlichen dazu, Ermittlungsansätze oder Indizien zu bilden[287]. Sie sind demgegenüber nicht hinreichend aussagekräftig, um eine Person unmittelbar zu be- oder entlasten, weil sie sich nur auf einen Telekommunikationsanschluss beziehen und nicht erkennen lassen, wer diesen Anschluss bedient hat[288]. Aus diesem Grund stellen Verkehrsdaten nicht nur als Ermittlungsansätze ein unsicheres Mittel dar. Sie bergen auch die besondere Gefahr in sich, dass unschuldige Personen einem falschen Verdacht ausgesetzt werden[289]. Dies hat sich in den USA gezeigt, wo die Industrie gerichtlich gegen vermeintliche Nutzer illegaler

286 BVerfGE 77, 65 (76).

287 Clayton, Richard: The Limits of Traceability, 28.08.2001, www.cl.cam.ac.uk/~rnc1/The_Limits_of_Traceability.html.

288 Clayton, Richard: (Fn. 8).

289 Clayton, Richard: (Fn. 8).

Tauschbörsen für urheberrechtlich geschützte Inhalte vorgegangen ist. In mehreren Fällen sind dort im Laufe des Verfahrens Zweifel aufgetreten, ob die Beklagten zu den von den Rechteverwertern angegebenen Zeitpunkten ihren Computer überhaupt benutzt haben[290].

Eine erhöhte Gefahr falscher Verdächtigungen entsteht, wenn die Sicherheitsbehörden durch Abarbeiten einer lange Liste von „Verdächtigen" nach dem Eliminierungsprinzip vorgehen, wie es Auskünfte über Telekommunikations-Verkehrsdaten oft erforderlich machen (etwa bei einer Auskunft über alle Personen, die innerhalb eines bestimmten Zeitraums einen bestimmten Telefonanschluss angerufen haben, oder über alle Personen, die sich zu einer bestimmten Zeit im Bereich einer bestimmten Mobilfunkzelle aufgehalten haben). Es spricht daher viel dafür, dass der staatliche Zugriff auf Verkehrsdaten mehr Unschuldige be- als entlastet. Daneben ist zu beachten, dass Maßstab einer gerichtlichen Verurteilung die richterliche Überzeugung ist. Im Zweifel ist von einer Verurteilung abzusehen (Art. 6 Abs. 2 EMRK). Aus diesem Grund ist die Gefahr, dass Gerichte aufgrund mangelhafter Tatsachengrundlage verurteilen, klar begrenzt. Schließlich ist darauf hinzuweisen, dass der Staat entsprechend dem Verhältnismäßigkeitsprinzip erheblich weiter gehende Eingriffe vorsehen darf, wenn er die Verwendung der Kenntnisse effektiv auf die mögliche Entlastung von Beschuldigten beschränkt. Die Erforderlichkeit einer Maßnahme zur Entlastung von Beschuldigten zwingt daher keineswegs dazu, die Maßnahme auch zur Belastung von Personen vorzusehen. In letztgenannten Fall gebietet es das Verhältnismäßigkeitsprinzip vielmehr, die Eingriffsschwelle erheblich höher anzusiedeln. Festzuhalten bleibt damit, dass sich ein erweiterter staatlicher Zugriff auf Telekommunikations-Verkehrsdaten nicht mit dem Verweis auf eine mögliche Entlastung Unschuldiger begründen lässt.

Durch die genannten Argumente lassen sich Eingriffe zum Zwecke der Strafverfolgung mithin nicht rechtfertigen. Das Strafrecht ist vielmehr nur als Mittel des Rechtsgüterschutzes legitim[291], als Instrument zur Verhütung des Eintritts konkreter Schäden. Die Gewährleistung einer geordneten Strafrechtspflege als solche ist demgegen-

290 Krempl, Stefan: Schwere Bedenken gegen Ausschnüffelung der Nutzer bei Copyright-Verstößen, Heise-Verlag, Meldung vom 12.12.2003, www.heise.de/newsticker/data/jk-12.12.03-005/.

über nicht als Gemeinschaftsgut im Rahmen der Verhältnismäßigkeitsprüfung anzusehen und bleibt daher im Folgenden außer Betracht.

Angesichts dessen muss man dem Bundesverfassungsgericht vorwerfen, falsche Prioritäten zu setzen[292]. Das Gericht achtet sehr darauf, den Entscheidungsspielraum des Gesetzgebers zu wahren und seine eigene Abwägung nicht an die Stelle der des Gesetzgebers zu setzen. Dies entspricht zwar dem Demokratieprinzip (Art. 20 Abs. 1 GG) und dem Grundsatz der Gewaltenteilung (Art. 20 Abs. 2 S. 2 GG). In einem Spannungsverhältnis dazu stehen aber die Grundrechte, deren Schutz es verlangt, dem Abwägungsspielraum des Gesetzgebers dort Grenzen zu setzen, wo das Ergebnis seiner Abwägung zu unangemessenen und daher unvertretbaren Ergebnissen führt. Staats- und Sicherheitsinteressen haben keinen uneingeschränkten Vorrang vor den Individualgrundrechten[293], sondern sind von Verfassungs wegen in ein ausgewogenes Verhältnis zu bringen.

Dies scheint dem Bundesverfassungsgericht oftmals nicht zu gelingen. Wo sich das Gericht einer substanziellen Abwägung nicht ganz enthält[294], konzentriert sich seine Argumentation nicht selten auf die formelle Gewährleistung von Transparenz in Bezug auf Eingriffe oder auf sonstige verfahrensrechtliche Anforderungen zum Grundrechtsschutz[295]. Klare Normen allein können aber schon deshalb nicht genügen, weil der Bürger mit einem Gesetzestext – nach der Rechtsprechung des Bundesverfassungsgerichts muss er sogar noch die Gesetzgebungsmaterialien und die einschlägigen Gerichtsentscheidungen hinzuziehen sowie juristische Auslegungskünste beherrschen – in aller Regel nichts anfangen kann. Die aufgrund der gesetzlichen Ermächtigung vorgenommenen Eingriffsmaßnahmen bleiben in den meisten Fällen ohnehin geheim, so dass die Kenntnis der einschlägigen Regelungen durch die Bürger nur begrenzt wirken kann. Selbst wenn die Betroffenen das Ausmaß von Eingriffen genau kennen würden, können exzessive Ermächtigungen sie von einem unbefangenen Gebrauchmachen ihrer Grundrechte abhalten. Bereits dadurch ist

---

291 BVerfGE 38, 312 (321); BVerfGE 39, 1 (46); BVerfGE 88, 203 (257 f.); vgl. auch BVerfGE 45, 187 (228): „der Mensch muss immer Zweck an sich selbst bleiben"; a.A. BVerfGE 107, 299 (324): „Das Interesse an der Aufklärung und Verfolgung von Straftaten hat neben dem Interesse an der Verhinderung weiterer Straftaten eine eigenständige verfassungsrechtliche Bedeutung."

292 Weßlau, ZStW 113 (2001), 681 (707).

293 Vgl. Minderheitenvotum in BVerfGE 30, 1 (46).

294 Z.B. durch nicht näher begründeten Verweis auf die „Funktionstüchtigkeit der Strafrechtspflege" in BVerfGE 44, 353 (373); BVerfGE 46, 214 (222 f.); BVerfGE 80, 367 (375); BVerfGE 100, 313 (388).

die Funktionsfähigkeit der Demokratie gefährdet. Der Zweck der Grundrechte verlangt daher, der Informationsmacht des Staates materielle Grenzen zu setzen[296]. Dem widerspricht es, wenn das Bundesverfassungsgericht Grundrechtsbeschränkungen zu Strafverfolgungszwecken hinnimmt, ohne die tatsächliche Wirksamkeit der Strafverfolgung zu untersuchen.

(ii) Einschlägige Gemeinschaftsgüter im Bereich der Netzkriminalität

Fraglich ist, welche konkreten Rechtsgüter mit Hilfe einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten geschützt werden können, welches Gewicht diese Rechtsgüter aufweisen und in welchem Maße sie bedroht sind.

Besonders nützlich ist eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten im Bereich von Straftaten, die unter Verwendung von Telekommunikationsnetzen begangen werden, weil sich oftmals nur anhand von Verkehrsdaten ermitteln lässt, wer an dem entsprechenden Telekommunikationsvorgang beteiligt war. Zum Ersten ist das Feld der Netzkriminalität im engeren Sinne[297] zu betrachten. Computer und Telekommunikationsnetze bilden heute eine wichtige Stütze unserer Volkswirtschaften[298]. Insofern ist es wichtig, die Verfügbarkeit der Systeme und Netze zu gewährleisten und die gespeicherten und übertragenen Daten vor unberechtigtem Zugang und Manipulationen zu schützen[299]. Das unberechtigte Auslesen, Schreiben, Verändern oder Löschen von automatisch verarbeiteten Daten ist in weiten Bereichen ohne Telekommunikationsnetze undenkbar. Dies gilt beispielsweise für die rasche Verbreitung von Computerviren per E-Mail oder für die Sabotage von Internetangeboten durch „DDoS-Attacks". Es liegt daher auf der Hand, dass viele Fälle von Hacking die Benutzung der Telekommunikationsnetze voraussetzen. Insoweit kann man von Telekommunikationsnetzen als „gefährlichen Werkzeugen" sprechen.

Denkbar ist, dass von Telekommunikationsnetzen ein eigenständiges Gefahrenpotenzial ausgehen könnte. Für diese Annahme könnte sprechen, dass es in der Vergangenheit vorgekommen ist, dass sich ansonsten unbescholtene Jugendliche („Script-Kiddies") „zum Spaß" öffentlich zugänglicher Software bedient haben, um

295 Etwa BVerfGE 65, 1 (66 ff.).

296 Ähnlich Simitis, NJW 1998, 2473 (2478 f.) mit der Forderung nach „Informationsverzicht".

297 Definition auf **Fehler! Textmarke nicht definiert.**.

298 Kommission, Sichere Informationsgesellschaft (I), 7.

bekannte kommerzielle Internetangebote „lahm zu legen". Erst das Internet hat es möglich gemacht, Schäden diesen Ausmaßes derart leicht und grenzüberschreitend zu verursachen. Andererseits waren Jugendliche schon immer anfällig für die Begehung milieutypischer Straftaten, die der Profilierung in ihrem Umfeld dienen.

Allgemein ist denkbar, dass sich die Netzkriminalität im engeren Sinne im Wesentlichen durch eine Verlagerung von Kriminalität aus anderen Feldern erklären lässt. Für diese These spricht, dass der Siegeszug der Informationsgesellschaft nicht zu einem höheren Gesamtkriminalitätsniveau geführt hat, wie die Entwicklung der polizeilichen Kriminalitätsstatistik über die letzten Jahre hinweg zeigt. Aus der Tatsache, dass Telekommunikationsnetze zur Begehung von Straftaten eingesetzt werden, lässt sich mithin nicht eindeutig schließen, ob und inwieweit das Kriminalitätsniveau ohne Telekommunikationsnetze niedriger wäre. Vielmehr spricht die allgemeine Erkenntnis, dass Kriminalität ein normales gesellschaftliches Phänomen darstellt, für die Annahme, dass mit der zunehmenden Verlagerung des sozialen Lebens in den Bereich der Telekommunikationsnetze die Kriminalität in diesem Bereich in gleichem Maße zunimmt.

Hinzu kommt das vergleichsweise geringe Gewicht der durch Netzkriminalität im engeren Sinne bedrohten Rechtsgüter. In ihren praktischen Auswirkungen führt diese Art von Kriminalität vor allem zu Vermögensschäden, sei es durch die Störung von Computersystemen, sei es durch die Weitergabe von Geschäftsgeheimnissen. Die Wahrscheinlichkeit, dass Leib und Leben von Menschen gefährdet werden könnten, wird zwar allenthalben heraufbeschworen. Die „lebenswichtigen Infrastrukturen" wie Stromnetze, deren Störung zu solchen Gefahren führen könnte, sind aber in aller Regel nicht an das Internet angeschlossen und für telekommunikative Angriffe daher nicht zugänglich. Dass solche Infrastrukturen mit Hilfe von Telekommunikationsnetzen angegriffen werden könnten oder gar ein organisierter Angriff auf einen Staat unter Einsatz von Telekommunikationsnetzen („Information Warfare", „Cyberwar", „Infowar") stattfinden könnte, muss man daher auf absehbare Zeit in den Bereich der Science-Fiction verweisen[300]. Ein Anschluss national wichtiger Systeme an öffentlich zugängliche Telekommunikationsnetze ist nicht erforderlich und

[299] Kommission, Sichere Informationsgesellschaft (I), 7.

wäre auch äußerst leichtsinnig. Hier ist zuallererst an technische Maßnahmen zur Abwendung von Schäden zu denken. Eine US-amerikanische Umfrage hat keinerlei terroristisch motivierte Netzkriminalität feststellen können[301].

Mithin beschränken sich die Auswirkungen von Netzkriminalität im engeren Sinne fast durchweg auf Vermögensschäden. Dies macht es möglich, derart entstandene Schäden gegen die finanziellen Kosten abzuwägen, die der Gesellschaft durch eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten entstehen würden. Zu diesen Kosten zählen etwa die Aufwendungen der Telekommunikationsunternehmen bei der Mitwirkung an der staatlichen Telekommunikationsüberwachung. Diese Kosten werden von den Unternehmen über ihre Preise auf die Nutzer abgewälzt. Eine umfassende Abwägung der Kosten wäre angesichts der Belastung durch eingreifende Maßnahmen angebracht, findet bisher aber nicht statt.
Zweitens ist der Bereich der Netzkriminalität im weiteren Sinne zu betrachten. Einen Teil der Netzkriminalität im weiteren Sinne stellen Inhaltsdelikte dar, also das rechtswidrige Übermitteln von Inhalten über Telekommunikationsnetze. Zu nennen ist etwa der illegale Austausch von urheberrechtlich geschütztem Material, von Kinderpornografie oder von rassistischer Propaganda. Die neuen Netze ermöglichen solche Delikte nicht erst; sie können ihre Begehung aber erleichtern. Dies gilt wohlgemerkt nur bei abstrakter Betrachtung. In einzelnen Fällen mögen auch Inhaltsdelikte erst wegen den Möglichkeiten der Telekommunikationsnetze begangen werden. Diese Frage ist bisher allerdings noch nicht untersucht worden.

Eine Gefährdung von Leib, Leben oder Freiheit erscheint auch im Bereich der Netzkriminalität im weiteren Sinne in aller Regel ausgeschlossen. Gerade im Bereich des illegalen Austauschs von Inhalten liegt es zwar auf der Hand, dass es das Internet so leicht wie nie zuvor macht, an illegale Inhalte zu gelangen. Dies bedeutet allerdings noch nicht, dass die leichtere Erreichbarkeit auch zu mehr Anhängern von Kinderpornografie, Rassismus usw. geführt hat. Diesen Schluss zu ziehen, wäre ohne eine eingehende Untersuchung verfehlt. Das Internet beruht gerade auf dem Konzept eines freien Informationsaustausches und auf der Idee des mündigen Bürgers. Be-

---

300 Olaf Lindner (Direktor Security Services bei Symatec), zitiert bei Schürmann, Hans: Angriff aus dem Web abgewehrt, Handelsblatt vom 10.02.2003, S. 19; BMI/BMJ, Sicherheitsbericht 2001, 205: „Konkrete Hinweise hinsichtlich [...] eines ‚Information Warfare' existieren [...] derzeit nicht."

301 Symantec, Symantec Internet Security Threat Report (I), 5.

nutzer des Internet stoßen nicht unfreiwillig auf illegales Material, sondern sie müssen aktiv nach solchen Inhalten suchen, um mit ihnen konfrontiert zu werden.

Selbst wenn sie das tun, ist noch nicht gesagt, dass der Konsum solcher Materialien schädliche Auswirkungen hat. Gerade bei Jugendlichen ist es natürlich, dass sie die Grenzen des sozial Erlaubten ausloten, um ganz regelmäßig schließlich doch wieder in die Mitte der Gesellschaft zurückzukehren. In anderen Fällen legen die Umstände zwar nahe, dass bestimmte Inhalte mitursächlich für Straftaten waren, etwa im Falle des Schulmassakers von Erfurt. Inwieweit eine Ursächlichkeit tatsächlich gegeben ist, ist allerdings ungeklärt. In dem zuletzt genannten Fall ging es übrigens um eine Beeinflussung des Täters durch bestimmte Videofilme, Bücher, CDs und Computerspiele, so dass eine Verbindung zu Telekommunikationsnetzen nicht bestand.

Welche Auswirkungen eine Prohibition von Inhalten und deren Aufhebung haben kann, verdeutlicht folgendes Beispiel[302]: In Dänemark gab es bis 1967 steigende Zahlen für die Herstellung und den Absatz verbotener pornographischer Literatur. Schon zwei Jahre nach der Aufhebung diesbezüglicher Verbotsbestimmungen gingen diese Zahlen rapide zurück. Es liegt nahe, dass dies auf einen Sättigungsprozess durch Befriedigung der diesbezüglichen Neugierde der Bevölkerung zurückzuführen ist. Dementsprechend lässt sich auch in anderen Bereichen nicht von vornherein behaupten, dass die Zugänglichkeit illegaler Inhalte über das Internet sozial schädlich sei, zumal der Konsum solcher Inhalte nicht in jedem Fall und allenfalls mittelbar Gefahren für konkrete Rechtsgüter mit sich bringt.

Auch im Bereich von Verstößen gegen das Urheberrecht ist nicht geklärt, ob die immer weitere Stärkung der IP-Rechte dem Zweck des Rechtsinstituts des geistigen Eigentums entspricht. Ein Copyrightschutz aus rein wirtschaftlichen Gründen steht nämlich tendenziell im Widerspruch zum ursprünglichen Sinn des Urheberschutzes, den Fortschritt auf diesem Gebiet zu fördern, indem ein Anreiz für Erfindungen und Weiterentwicklungen geschaffen wird[303]. Heutzutage dient der Schutz geistigen Eigentums nur selten dem kleinen Tüftler, sondern zumeist den Interessen weltweit tätiger Unternehmen. Deren Interessen scheinen dem Allgemeinwohl nicht selten zu widersprechen. Besonders deutlich zeigt sich dies an der Diskussion über Patente an

302 Eisenberg, Kriminologie, § 23, Rn. 50.

Aids-Medikamenten: Die Inhaber dieser Patente verlangen ein Vielfaches der Produktionskosten für die lebensrettenden Stoffe und nehmen so den Tod unzähliger Aidskranker vor allem in Entwicklungsländern in Kauf.

Zwar hat der ursprüngliche Gedanke des Schutzes geistigen Eigentums, dass sich die Entwicklung von Innovationen nur bei einem angemessenem Schutz der Rechte an dem Produkt lohnt, auch weiterhin seine Berechtigung. Angesichts der langen Schutzfristen stellt sich aber die Frage, ob dies den Fortschritt nicht eher behindert als fördert. Beispielsweise ist fraglich, ob das gegenwärtige Recht einen ausreichenden Anreiz für den Softwaremonopolisten Microsoft bietet, seine profitablen Produkte zu verbessern. Zweifel hieran wecken die zahlreichen Qualitätsmängel (etwa „Abstürze" und Sicherheitsmängel) der Produkte dieses Unternehmens. Teilweise wird sogar vertreten, Copyrightverstöße könnte die Verbreitung eines Produkts fördern und dessen Marktmacht unter Umständen noch stärken. Jedenfalls sind Einschränkungen der freien Internetnutzung insoweit kontraproduktiv, wie sie das Vertrauen der Bürger in dieses Medium schwächen und daher auch den Absatz von Produkten in diesem Bereich erschweren. Außerdem können sie zu einem Ausweichen auf kostenfrei verfügbare „Open Source"-Software führen, was nicht im Sinne der Anbieter kommerzieller Produkte liegen kann. In anderen Fällen würde die Unterbindung illegaler Kopien dazu führen, dass auf die Benutzung der Software gänzlich verzichtet würde. Nur in einem geringen Teil der Fälle würde anstelle der Anfertigung illegaler Kopien die Originalsoftware gekauft, was die astronomischen Schadensschätzungen der Industrie nicht berücksichtigen.

Weiterhin sind „Raubkopien" auch außerhalb der Telekommunikationsnetze verbreitet, gerade durch die Technologie der CD-Brenner. Man denke nur an den Tausch von Software oder Musik-CDs auf dem Schulhof. Auch kommt in Betracht, dass Straftäter ohne die Möglichkeiten der Telekommunikationsnetze teilweise andere Straftaten im Bereich traditioneller Kriminalität begehen könnten. Wenn das Motiv eines potenziellen Täters beispielsweise darin besteht, unbedingt an ein teures Computerspiel zu bekommen, könnte er statt einer „Raubkopie" aus dem Internet auch einen Diebstahl in Betracht ziehen. Er könnte auch jemanden betrügen, um an Geld zu kommen, mit dem er das Spiel erwerben könnte.

---

303 Tallo, Bericht zum Entwurf des Cybercrime-Abkommens (I), Unterpunkt F.36.

Somit ist auch im Bereich des geistigen Eigentums das letzte Wort in Bezug auf den tatsächlich durch „Raubkopien" entstehenden Schaden noch nicht gesprochen. Zudem ist in der Abwägung wiederum zu berücksichtigen, dass auch hier nur Vermögensschäden entstehen können, was es fraglich erscheinen lässt, ob derart weit reichende Überwachungsmaßnahmen, wie sie die Industrie zu ihrem Vorteil fordert, gerechtfertigt sind.

Überhaupt ist es im Bereich der Netzkriminalität im weiteren Sinne fragwürdig, ob die Telekommunikationsnetze zu einem insgesamt höheren Kriminalitätsniveau führen. In diesem Feld, in dem Telekommunikationsnetze lediglich als Medium für zwischenmenschliche Kommunikation eingesetzt werden, besteht ein besonders hohes Maß an Substituierbarkeit. Dies legt die Annahme nahe, dass die Telekommunikation in diesem Bereich größtenteils die unmittelbare Kommunikation in der „Offline-Welt" nachvollzieht und im Wesentlichen nur eine Verlagerung von ehemaligem „Offline-Verhalten" in die Telekommunikationsnetze stattfindet. Die neuen Medien scheinen in diesem Bereich also den Platz traditioneller Kommunikationsmittel einzunehmen, ohne – der Kriminalitätsstatistik nach zu urteilen – eine spürbare Kriminalitätssteigerung nach sich zu ziehen. Eine erhöhte Gefahr durch Telekommunikationsnetze kann daher auf der Basis bisheriger Erkenntnisse nicht angenommen werden.

(iii) Ausmaß der Gefährdung durch Netzkriminalität

Bisher liegen keine zuverlässigen Statistiken über das Ausmaß an Netzkriminalität oder die dadurch verursachten oder verursachbaren Schäden vor[304]. Erst recht sind keine Erkenntnisse über die insgesamt durch Telekommunikation verursachten Schäden vorhanden. Wenn überhaupt, dann wurde meist das zahlenmäßige Ausmaß von Computerkriminalität untersucht. Aber auch auf diesem Gebiet fehlt es weitgehend an verlässlichen Statistiken[305]. Jenseits statistischer Angaben ist immerhin anerkannt, dass sich die Nutzer der neuen Medien in den allermeisten Fällen le-

[304] BMI/BMJ, Sicherheitsbericht 2001, 201; Holznagel, Bernd: Stellungnahme für die öffentliche Anhörung „Von der Industrie- zur Wissensgesellschaft: Wirtschaft, Arbeitswelt und Recht, Privatisierung und Patentierung von Wissen", 08.10.2001, www.bundestag.de/gremien/welt/weltto/weltto126_stell004.pdf, 22.

gal verhalten und dass der Missbrauch der Datennetze im Vergleich zu ihrer legaler Nutzung einen verschwindend geringen Anteil bildet[306].

Für den Bereich der Netzkriminalität im engeren Sinne lässt sich diese Annahme durch die deutsche polizeiliche Kriminalitätsstatistik bestätigen. Allerdings ist vorweg darauf hinzuweisen, dass die Aussagekraft der Kriminalitätsstatistik nicht überschätzt werden darf. Dies gilt insbesondere im Hinblick auf die erhebliche Anzahl von Straftaten, die den Strafverfolgungsorganen nicht bekannt werden (Dunkelfeld). Das Ausmaß des Dunkelfeldes schwankt sowohl im zeitlichen Vergleich wie auch im Vergleich der einzelnen Deliktsgruppen zueinander in kaum vorhersehbarer Weise. Tatsächlich gibt es so viele Ursachen für Veränderungen der erfassten Fallzahlen, dass Schlüsse auf die Entwicklung des tatsächlichen Kriminalitätsniveaus verfehlt wären[307].

Lässt man diese Bedenken außer Acht, weil die polizeiliche Kriminalitätsstatistik einen der wenigen tatsächlichen Anhaltspunkte zur Einschätzung des Ausmaßes an Netzkriminalität im engeren Sinne darstellt, dann ergibt sich folgendes Bild: Auf je 1000 Einwohner kam 2001 ein Fall von Computerkriminalität im engeren Sinne[308], wobei mehr als die Hälfte der Fälle auf Betrug mittels rechtswidrig erlangter Karten für Geld- oder Kassenautomaten entfiel. Nach Abzug dieser Delikte, bei denen von vornherein kein Zusammenhang mit Telekommunikationsnetzen bestehen kann, verbleiben höchstens 30.000 Fälle von Netzkriminalität im engeren Sinne im Jahre 2001. In dieser Größenordnung liegen ansonsten bereits einzelne Deliktsgruppen wie „Diebstähle aus Neubauten" oder der Handel mit Cannabis. Zum Vergleich: Es gab 100-mal mehr Diebstähle, 20-mal mehr Sachbeschädigungen und fünfmal mehr Beleidigungen als alle potenziellen Fälle von Netzkriminalität zusammen genommen. Gemessen an der Gesamtzahl der erfassten Delikte handelt es sich um 0,5% der Delikte. Das Kriminalitätsfeld der Netzkriminalität im engeren Sinne ist der polizei-

---

305 BMI/BMJ, Sicherheitsbericht 2001, 201; Kommission, Sichere Informationsgesellschaft (I), 13: „Mangels aussagekräftiger Statistiken ist es erforderlich, stichhaltige Belege für das Ausmaß der Computerkriminalität zusammenzutragen."

306 Holznagel, Bernd: Stellungnahme für die öffentliche Anhörung „Von der Industrie- zur Wissensgesellschaft: Wirtschaft, Arbeitswelt und Recht, Privatisierung und Patentierung von Wissen", 08.10.2001, www.bundestag.de/gremien/welt/weltto/-weltto126_stell004.
pdf, 22; Norbert Geis (MdB) u.a., BT-Drs. 14/4173, 1; ULD-SH, Sichere Informationsgesellschaft (I), Punkt 6.

307 BMI/BMJ, Sicherheitsbericht 2001, 1; str., vgl. Kury, Kriminalistik 2001, 74 (77) m.w.N.

308 BMI/BMJ, Sicherheitsbericht 2001, 201; Holznagel, Bernd: Stellungnahme für die öffentliche Anhörung „Von der Industrie- zur Wissensgesellschaft: Wirtschaft, Arbeitswelt und Recht, Privatisierung und Patentierung von Wissen", 08.10.2001, www.bundestag.de/gremien/welt/weltto/weltto126_stell004.pdf, 20.

lichen Kriminalitätsstatistik zufolge also eher zu vernachlässigen. Gegen ein großes Ausmaß von Netzkriminalität im engeren Sinne im Vergleich zu dem allgemeinen Kriminalitätsniveau sprechen auch Zahlen aus Großbritannien, denen zufolge der Zugriff auf Verkehrsdaten regelmäßig im Zusammenhang mit Ermittlungen wegen allgemeiner Kriminalität erfolgt, dagegen nur in einem Bruchteil der Fälle im Zusammenhang mit Computerkriminalität[309].

Es ist plausibel, im Bereich der Netzkriminalität von steigenden Fallzahlen auszugehen[310], weil die Nutzung der Telekommunikationsnetze allgemein zunimmt. Die durchschnittliche jährliche Steigerungsrate der Computerkriminalität in den letzten Jahren (1997-2001: 21%)[311] liegt allerdings weit[312] unter der durchschnittlichen jährlichen Wachstumsrate der Anzahl von Internetnutzern in Deutschland (1997-2002: 49%)[313]. Für die statistisch ausgewiesenen Fallzahlen im Bereich der Netzkriminalität ist zudem in großem Maße der Umfang polizeilicher Aufklärungsaktivitäten maßgebend[314], weswegen tatsächlich eine erheblich geringere Steigerungsrate des Ausmaßes an Netzkriminalität vorliegen kann als sie sich aus der Kriminalitätsstatistik ergibt.

Fest steht, dass die polizeiliche Kriminalitätsstatistik nur einen Teil aller Fälle von Computerkriminalität widerspiegelt und die tatsächlichen Zahlen erheblich höher sind[315]. Auf dem Gebiet der Netzkriminalität ist dies beispielsweise darin begründet, dass viele Straftaten nicht bemerkt werden (z.B. Hacking) oder von betroffenen Unter-

309 NCIS Submission (I), Punkt 6.1.1.

310 BMI/BMJ, Sicherheitsbericht 2001, 197; Holznagel, Bernd: Stellungnahme für die öffentliche Anhörung „Von der Industrie- zur Wissensgesellschaft: Wirtschaft, Arbeitswelt und Recht, Privatisierung und Patentierung von Wissen", 08.10.2001, www.bundestag.de/gremien/welt/weltto/weltto126_stell004.pdf, 21 f.

311 Nach BMI, PKS 2001 (I) und ohne Abzug von Betrug mit Zahlungskarten.

312 Holznagel, Bernd: Stellungnahme für die öffentliche Anhörung „Von der Industrie- zur Wissensgesellschaft: Wirtschaft, Arbeitswelt und Recht, Privatisierung und Patentierung von Wissen", 08.10.2001, www.bundestag.de/gremien/welt/weltto/-weltto126_stell004.
pdf, 22: „deutlich".

313 Heise Verlag: 44 Prozent der Deutschen gehen ins Netz, Meldung vom 05.09.2002, www.heise.de/newsticker/data/anw-05.09.02-005/.

314 BMI/BMJ, Sicherheitsbericht 2001, 197.

315 Sieber, COMCRIME-Studie (I), 22 f.; Kommission, Sichere Informationsgesellschaft (I), 13; Holznagel, Bernd: Stellungnahme für die öffentliche Anhörung „Von der Industrie- zur Wissensgesellschaft: Wirtschaft, Arbeitswelt und Recht, Privatisierung und Patentierung von Wissen", 08.10.2001, www.bundestag.de/gremien/welt/weltto/ weltto126_stell004.pdf, 21; für Internetkriminalität auch BMI/BMJ, Sicherheitsbericht 2001, 197 und 198; French Delegation of Police Cooperation Working Party, Enfopol 38 (I), 10.

nehmen nicht gemeldet werden, um kein schlechtes Bild in der Öffentlichkeit abzugeben[316].

Fraglich ist aber, ob das Dunkelfeld auf dem Gebiet der Netzkriminalität im Vergleich zu anderen Deliktsgruppen besonders hoch ist[317]. Nur in diesem Fall würde es sich um eine besorgniserregende Besonderheit auf diesem Gebiet handeln. Grundsätzlich existiert die Dunkelfeldproblematik bei allen Delikten. Ob ein besonders hohes Dunkelfeld auf dem Gebiet der Netzkriminalität existiert, ist soweit ersichtlich noch nicht empirisch untersucht worden[318]. Eine Umfrage unter 3.623 Unternehmen weltweit – darunter 1.476 europäischen Unternehmen – ergab, dass über die Hälfte der Unternehmen jeden Fall von Wirtschaftskriminalität anzeigen[319]. Ein weiteres Drittel der Unternehmen reagiert ab einer bestimmten Erheblichkeitsschwelle mit einer Anzeige[320], so dass insgesamt nahezu 90% der befragten Unternehmen gravierende Fälle von Wirtschaftskriminalität – darunter auch Netzkriminalität – anzeigen. Einer Meinungsumfrage unter US-amerikanischen Unternehmen und Organisationen zufolge haben immerhin 34% der Befragten auf Fälle von Computerkriminalität meistens mit einer Strafanzeige reagiert[321], was eine Dunkelziffer von 66% der Gesamtkriminalität bedeuten würde.

In anderen Kriminalitätsbereichen wird die Dunkelziffer weit höher geschätzt[322]. Beispielsweise ist anzunehmen, dass nur ein kleiner Bruchteil aller Beleidigungen angezeigt wird, weil in der Gesellschaft andere Regelungsmechanismen für diese Fälle existieren. Auch in vielen Fällen von versuchtem Betrug wird oft von einer Anzeige abgesehen werden, weil die betroffene Person die versuchte Täuschung bemerkt und daher keinen Schaden erleidet. Bei vollendetem Betrug werden sich viele Opfer schämen, dass sie auf den Täter hereingefallen sind. Dabei kann es sich auch

316 Kommission, Sichere Informationsgesellschaft (I), 13; Weichert, Bekämpfung von Internet-Kriminalität (I), Punkt 2; Sieber, COMCRIME-Studie (I), 22 f.; French Delegation of Police Cooperation Working Party, Enfopol 38 (I), 10; BSI, zitiert bei Lücke, Hayo: Studie: 60 Prozent der Firmen Opfer von Computer-Sabotage, Meldung des Internet-Portals teltarif.de vom 06.03.2003, www.teltarif.de/arch/2003/kw10/s10049.html.

317 In diese Richtung für Internetkriminalität BMI/BMJ, Sicherheitsbericht 2001, 197, wonach „von einem extrem großen Dunkelfeld ausgegangen werden" müsse.

318 Etwa BMI/BMJ, Sicherheitsbericht 2001, 198 für Internetkriminalität: „Bei Kriminalität im Internet kann von einem großen Dunkelfeld ausgegangen werden; entsprechende Dunkelfeldforschungen existieren bisher jedoch nicht. Insofern ist eine aussagekräftige Beschreibung des Phänomens anhand statistischer Zahlenwerte kaum möglich."

319 PricewaterhouseCoopers, Wirtschaftskriminalität 2003 (I), 11.

320 PricewaterhouseCoopers, Wirtschaftskriminalität 2003 (I), 11.

321 CSI/FBI, 2002 Survey (I), 20.

322 Zahlen bei Eisenberg, Kriminologie, § 44, Rn. 16 ff.: Das Dunkelfeld bei einfachen Diebstahlsdelikten betrage einer deutschen Untersuchung zufolge 89%, einer amerikanischen Studie zufolge 75% bei Gewaltkriminalität, einer britischen Studie zufolge 80% insgesamt, 83% bei Körperverletzung, 92% bei Sachbeschädigung; vgl. auch Kury, Kriminalistik 2001, 74 (78).

um Anlagebetrug in Millionenhöhe von prominenten Mitgliedern der Gesellschaft handeln, so dass sich das Dunkelfeld nicht auf Bagatellfälle beschränkt. Auch bei Delikten, bei denen in der Bevölkerung kein Unrechtsbewusstsein existiert und die dementsprechend weit verbreitet sind, geht man von einem großen Dunkelfeld aus[323]. Diese beispielhaft aufgezählten Bereiche außerhalb der Netzkriminalität sprechen gegen die Annahme, dass gerade im Bereich der Netzkriminalität ein außergewöhnlich hohes Dunkelfeld bestehen könnte.

Für ein besonders großes Dunkelfeld spricht auch nicht, dass Computerviren äußerst verbreitet sind und dennoch kaum einmal Anzeigen diesbezüglich erstattet werden[324]. Die insoweit einschlägigen Straftatbestände setzen sämtlich Vorsatz voraus, wohingegen sich Computerviren ganz regelmäßig unbemerkt verbreiten. Zwar wird der Programmierer eines Computervirus regelmäßig vorsätzlich handeln. Dieses Delikt würde aber nur als ein Fall in die Kriminalitätsstatistik eingehen und fiele daher kaum ins Gewicht. Computerviren stammen außerdem vergleichsweise selten aus Deutschland, so dass Ermittlungen deutscher Behörden regelmäßig keinen Erfolg versprechen.

Für ein erhöhtes Dunkelfeld könnte sprechen, dass ein Teil der Netzkriminalität in den Bereich der Wirtschaftskriminalität fällt und die Kriminologie der Wirtschaftskriminalität insgesamt ein vergleichsweise großes Dunkelfeld zuschreibt[325]. Bei Straftaten, die persönliche oder staatliche Schutzgüter erheblich verletzen, schätzt die Wissenschaft das Dunkelfeld allerdings als vergleichsweise klein ein[326], weil – selbst innerhalb geschlossener Zirkel – Schäden für Leib, Leben oder Freiheit einer Person oder Vermögensschäden Dritter der Außenwelt kaum verborgen bleiben werden. Ein hohes Dunkelfeld auf dem Gebiet der Netzkriminalität kann man damit allenfalls dort sehen, wo ausschließlich das Vermögen oder Geschäftsgeheimnisse des Opfers von Netzkriminalität beschädigt wurden. Dabei handelt es sich nicht um höchstwertige Rechtsgüter, was im Rahmen der Abwägung von Bedeutung ist.
Es erscheint auch wahrscheinlich, dass Firmen ihre Geheimhaltungsinteressen zurückstellen, wenn es um wirklich hohe Summen geht oder wenn sie sich einer dau-

323 Kury, Kriminalistik 2001, 74 (78).
324 In diese Richtung aber BMI/BMJ, Sicherheitsbericht 2001, 201.
325 Kury, Kriminalistik 2001, 74 (78); BMI/BMJ, Sicherheitsbericht 2001, 160.
326 Kury, Kriminalistik 2001, 74 (78).

erhaften Gefahr ausgesetzt sehen. Für diese Annahme spricht, dass schwere Delikte generell eher angezeigt werden als leichte[327] und dass der Hauptgrund für das Absehen von einer Strafanzeige darin liegt, dass die betroffenen Personen den entstandenen Schaden als zu gering einschätzen als dass eine Anzeige lohnen würde[328]. Außerdem muss man anerkennen, dass geschädigte Firmen, die aus Gründen ihres guten Rufes von einer Anzeige absehen, insoweit regelmäßig rational und wohlbegründet handeln. Ein Ermittlungs- und Strafverfahren, von dem die Öffentlichkeit erfahren würde, könnte sie in der Tat mehr schädigen als ihnen die präventiven Wirkungen eines Strafverfahrens selbst im besten Fall nutzen könnten. Sind staatliche Ermittlungsverfahren in bestimmten Fällen aber nicht sinnvoll, dann kann ein insoweit bestehendes Dunkelfeld auch nicht angeführt werden, um weiter gehende staatliche Eingriffe im Ermittlungsverfahren zu legitimieren.

Dass die Anzahl von Fällen, in denen Straftaten durch das Opfer nicht erkannt werden, im Bereich der Netzkriminalität besonders hoch sein soll, ist nicht ersichtlich. Das Bundesamt für Sicherheit in der Informationstechnik schätzt, dass nur zehn Prozent aller Angriffe auf Unternehmen von diesen nicht erkannt werden[329]. Der Hauptgrund für das Dunkelfeld auf dem Gebiet der Netzkriminalität wird vielmehr in der mangelnden Anzeigebereitschaft liegen.

Zusammenfassend lässt sich sagen, dass ohne spezifische empirische Nachweise nicht davon ausgegangen werden kann, dass das Dunkelfeld im Bereich der Netzkriminalität größer ist als im Bereich anderer Kriminalität.

In Bezug auf die Höhe der Vermögensschäden durch Netzkriminalität liegen keine aussagekräftigen Daten vor[330]. Das Bundesamt für Sicherheit in der Informationstechnik gibt als jährlichen Gesamtschaden durch Computerkriminalität in Deutsch-

---

327 Eisenberg, Kriminologie, § 44, Rn. 16.

328 Kury, Kriminalistik 2001, 74 (80).

329 BSI, zitiert bei Lücke, Hayo: Studie: 60 Prozent der Firmen Opfer von Computer-Sabotage, Meldung des Internet-Portals teltarif.de vom 06.03.2003, www.teltarif.de/arch/2003/kw10/s10049.html.

330 Holznagel, Bernd: Stellungnahme für die öffentliche Anhörung „Von der Industrie- zur Wissensgesellschaft: Wirtschaft, Arbeitswelt und Recht, Privatisierung und Patentierung von Wissen", 08.10.2001, www.bundestag.de/gremien/welt/weltto/weltto126_stell004.
pdf, 22.

land „einen hohen dreistelligen Millionenbetrag" an[331]. Auf welche Quellen sich diese Schätzung stützt und inwieweit die angegebenen Schäden unter Verwendung von Telekommunikationsnetzen verursacht wurden, bleibt offen. Eine im Jahr 2003 durchgeführte Unternehmensbefragung ergab, dass 6% der beklagten Schäden durch Wirtschaftskriminalität auf Computerkriminalität zurückgeführt wurden[332]. Demgegenüber machte etwa Industriespionage 30% der angegebenen Schäden aus[333].

Absolute Zahlen benennt eine in den USA jährlich stattfindende, nicht repräsentative Umfrage über Computerkriminalität und -sicherheit[334]. Lässt man diejenigen der untersuchten Deliktsgruppen außer Acht, bei deren Begehung Telekommunikationsnetze von vornherein nicht (z.B. Laptopdiebstahl) oder kaum (z.B. Missbrauch von Internetzugängen durch Mitarbeiter) als Tatwerkzeug in Betracht kommen, dann wurden von den befragten Organisationen Schäden in Höhe von 389 Millionen US-$ im Jahre 2001 beklagt. Die Angabe von 389 Millionen US-$ kann einerseits zu niedrig sein, weil nur vergleichsweise wenige Organisationen befragt wurden. Sie kann aber auch zu hoch sein, weil sie lediglich auf freien Schätzungen der Organisationen beruht. Jedenfalls müsste jede Bezifferung in Relation zu anderen Zahlen gesetzt werden, etwa zu den gesamten Ausgaben oder Umsätzen der befragten Organisationen in dem betreffenden Jahr. So ist bekannt, dass der Kreditkartengesellschaft Mastercard 1999 durch Kreditkartenmissbrauch ein Verlust in Höhe von ca. 700 Millionen US-$ weltweit entstanden ist, dass dieser Schaden aber nur 0,1% der Kreditkartenumsätze ausmachte[335]. Im Jahr 2001 entstand übrigens allein in Deutschland und allein durch Diebstahl ein Schaden in Höhe von 2,2 Milliarden Euro[336].

Auch aus weiteren Gründen ist bei der Übertragung von Zahlen aus dem Gebiet der Computerkriminalität auf den Bereich der Netzkriminalität Vorsicht angebracht. Zwar wurde das Internet von 74% der befragten Firmen als häufiger Angriffspunkt

---

331 BSI, zitiert bei Lücke, Hayo: Studie: 60 Prozent der Firmen Opfer von Computer-Sabotage, Meldung des Internet-Portals teltarif.de vom 06.03.2003, www.teltarif.de/arch/2003/kw10/s10049.html.

332 PricewaterhouseCoopers, Wirtschaftskriminalität 2003 (I), 12.

333 PricewaterhouseCoopers, Wirtschaftskriminalität 2003 (I), 12.

334 CSI/FBI, 2002 Survey (I).

335 Kubica, Die Kriminalpolizei 9/2001.

336 BMI, PKS 2001 (I), 11.

genannt, interne Computer dagegen nur von 33%[337]. Dies bedeutet aber nicht, dass die zahlenmäßig selteneren Fälle internen Missbrauchs nicht für den Großteil der Schäden verantwortlich sein könnten. Zu vermuten ist, dass ein großer Teil der schadensträchtigen Computerkriminalität von Mitarbeitern oder ehemaligen Mitarbeitern eines Unternehmens begangen wird und dass der Zugriff mittels Telekommunikationsnetzen insoweit keine Rolle spielt, weil Mitarbeiter direkten Zugriff auf die Computeranlagen ihres Unternehmens haben und durch deren Nutzung vermeiden können, dass aufgrund der Zwischenschaltung von Telekommunikationsnetzen Datenspuren entstehen, die sie verraten könnten. Einer deutschen Untersuchung zufolge gehen zwei Drittel der Fälle von Computerkriminalität im engeren Sinne von Mitarbeitern oder ehemaligen Mitarbeitern des angegriffenen Unternehmens aus[338]. Eine US-amerikanische Umfrage kommt zu dem Ergebnis, dass mehr als 50% aller Fälle von Netzkriminalität auf internen Missbrauch zurückzuführen seien; außerdem seien die aufgetretenen Schäden in diesem Bereich besonders hoch[339]. Die oben zitierte, jährliche Umfrage unter US-amerikanischen Unternehmen und Organisationen ergab, dass sich 76% der befragten Unternehmen und Organisationen von ihren eigenen Mitarbeitern angegriffen fühlten[340] und dass immerhin 44% aller Schäden mit Telekommunikationsnetzrelevanz auf unbefugte Informationsabrufe zurückzuführen seien. Gerade unbefugte Informationsabrufe dürften besonders oft und besonders erfolgreich von den Mitarbeitern des betroffenen Unternehmens vorgenommen werden, weil diese entsprechendes Insiderwissen besitzen.
Die Höhe der Vermögensschäden, die gerade durch den Missbrauch von Telekommunikationsnetzen entstehen, darf daher nicht überschätzt werden, gerade im Verhältnis zu dem Aufwand, der mit der Einführung einer Vorratsspeicherung von Verkehrsdaten verbunden wäre. Allgemein ist zu beobachten, dass sich die politische Diskussion auf Felder wie Wirtschaftskriminalität, Rauschgiftkriminalität, organisierte Kriminalität und jetzt auch Netzkriminalität konzentriert, obwohl diese Kriminalitätsfelder nur einen Bruchteil der Gesamtkriminalität ausmachen[341] und die Bürger im Vergleich zur Massenkriminalität nicht merklich beeinträchtigen.

---

337 CSI/FBI, 2002 Survey (I), 8.

338 Thomas Eßer (Mummert Consulting), zitiert bei Lücke, Hayo: Studie: 60 Prozent der Firmen Opfer von Computer-Sabotage, Meldung des Internet-Portals teltarif.de vom 06.03.2003, www.teltarif.de/arch/2003/kw10/s10049.html.

339 Symantec, Symantec Internet Security Threat Report (I), 5.

340 CSI/FBI, 2002 Survey (I), 9.

341 Dietel, Innere Sicherheit, 63.

(iv) Einschlägige Gemeinschaftsgüter im Bereich sonstiger Kriminalität

Weiterhin ist zu untersuchen, ob von den Telekommunikationsnetzen Gefahren ausgehen, wenn sie nicht unmittelbar als Werkzeug zur Begehung von Straftaten eingesetzt werden. In Betracht kommt zunächst die Nutzung durch Straftäter im Zusammenhang mit der Begehung traditioneller Straftaten, etwa als Hilfsmittel bei der Vorbereitung oder Begehung einer Straftat oder bei der Flucht, dem Absatz der Beute usw. Das klassische Beispiel in diesem Bereich ist das Mobiltelefon, dass sich bei Kriminellen offenbar größter Beliebtheit erfreut, weil es eine ständige Kommunikation mit Komplizen ermöglicht. Durch allgemeine Kriminalität können potenziell Rechtsgüter jeder Art gefährdet werden. Fraglich ist allerdings, ob es für die Begehung einer Straftat wirklich eine Rolle spielt, ob Telekommunikationsmöglichkeiten zur Verfügung stehen. Auch in diesem Bereich ist es problematisch, von der Nutzung des Mediums durch Straftäter darauf zu schließen, dass ohne die Telekommunikationsnetze weniger Straftaten begangen würden.

Der Zugriff auf Verkehrsdaten ist schließlich nicht nur dann von Bedeutung, wenn Telekommunikationsnetze im Zusammenhang mit einer Straftat genutzt wurden. Es geht vielmehr oft um das Überführen oder Auffinden Beschuldigter anhand von deren allgemeiner Telekommunikationsnutzung, die sich von der jedes anderen Bürgers nicht unterscheidet. In dieser Fallkonstellation, die sogar die Mehrzahl der Zugriffe auf Telekommunikations-Verkehrsdaten ausmachen könnte, lässt sich nicht sagen, dass von der Telekommunikationsnutzung Gefahren ausgehen. Zwar mag von der Person, gegen die ermittelt wird, eine Gefahr ausgehen, zu deren Beseitigung das Auffinden und Überführen der Person erforderlich sein mag. Diese Gefahr würde aber auch dann bestehen, wenn der Beschuldigte auf die Telekommunikationsnutzung verzichten würde, so dass den Telekommunikationsnetzen in diesen – zahlenmäßig bedeutenden – Fällen kein eigenständiges Gefährdungspotenzial zugeschrieben werden kann. Nichtsdestotrotz ist der Zugriff auf Telekommunikations-Verkehrsdaten in diesem Bereich geeignet, Rechtsgüter aller Art vor strafbaren Angriffen zu schützen.

(v) Zwischenergebnis

Als Zwischenergebnis bleibt festzuhalten, dass eine Gefährdung der Allgemeinheit oder der physischen Sicherheit einzelner Bürger durch die Nutzung von Telekommunikationsnetzen kaum denkbar ist. Gefährdet ist vielmehr vorwiegend das Vermögen Einzelner, also ein Rechtsgut von vergleichsweise geringerem Gewicht. In wie vielen Fällen und in welchem Ausmaß durch die Nutzung von Telekommunikationsnetzen tatsächlich Rechtsgüter geschädigt werden, ist noch nicht empirisch untersucht worden. Wo Rechtsgüter anders als durch Nutzung von Telekommunikationsnetzen gefährdet werden, kann der Zugriff auf Telekommunikations-Verkehrsdaten in einzelnen Fällen der Abwendung von Gefahren für Rechtsgüter jeder Art dienen.

(bb) Maß an Eignung zur Begegnung der Gefahren

Nachdem festgestellt wurde, welche Rechtsgüter durch die Einführung einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten geschützt werden könnten, stellt sich die Frage nach dem praktischen Nutzen einer solchen Maßnahme. Bei der Untersuchung dieser Frage ist zweckmäßigerweise danach zu unterscheiden, zu welchem Zweck ein Zugriff auf Verkehrsdaten erfolgt. Umfassender als der EU-Vorschlag zielen die Bundesrats-Vorschläge darauf ab, die auf Vorrat gespeicherten Daten allen wichtigen Strafverfolgungs- und Gefahrenabwehrbehörden einschließlich der Nachrichtendienste zugänglich zu machen. Fraglich ist, in welchem Maße der Zugriff auf Verkehrsdaten für die einzelnen Behördenzweige von Bedeutung ist.

Den Schwerpunkt wird man eindeutig im Bereich der Strafverfolgung sehen müssen[342]. Nicht umsonst hat schon § 142 der Paulskirchenversammlung von 1848 Ausnahmen von dem Briefgeheimnis nur und gerade für „strafgerichtliche Untersuchungen und in Kriegsfällen" zugelassen. Auch auf der nationalen und internationalen Bühne – dort insbesondere im Rahmen des Europarats, der EU und der G8 – konzentrieren sich die Diskussionen und Anstrengungen auf das Gebiet der Strafver-

folgung. Schließlich hat es der Polizeigesetzgeber – von Ausnahmen abgesehen – bisher nicht für erforderlich gehalten, die Gefahrenabwehrbehörden zu ermächtigen, auf Verkehrsdaten zuzugreifen.

Zu beachten ist allerdings, dass sich die Bereiche der Gefahrenabwehr und der Strafverfolgung oft überschneiden, weil die Gefährdung von Rechtsgütern oft strafbar ist. Jedenfalls die vorsätzliche Gefährdung von Rechtsgütern wird durch das Strafrecht weitgehend abgedeckt, so dass eine „reine" Gefahrenabwehr im Wesentlichen nur im Bereich fahrlässiges Verhaltens oder unverschuldeter Gefahren denkbar ist. Dass in diesen, schon für sich genommen wenig relevanten Bereichen ein Zugriff auf Verkehrsdaten erforderlich werden könnte, ist kaum denkbar.

Im Bereich strafbarer Handlungen sind die praktischen Möglichkeiten der Gefahrenabwehrbehörden, die zukünftige Begehung einer Straftat zu verhindern, gering[343]. Eine Gefahrenabwehr wird daher in der Praxis ganz regelmäßig in der Form erfolgen, dass die weitere Begehung einer strafbaren Handlung unterbunden und in dieser Weise zugleich die dadurch verursachte Gefahr beseitigt wird. Beispielsweise könnte im Fall einer Entführung der Zugriff auf die Mobiltelefon-Positionsdaten des Opfers erforderlich werden, um das Opfer zu befreien und zugleich den Täter festzunehmen.

Der Zugriff auf Telekommunikations-Verkehrsdaten ist somit vor allem im Bereich strafbarer Handlungen erforderlich, so dass sich die folgenden Ausführungen auf dieses Feld konzentrieren.

Bei der Diskussion um erweiterte informationelle Eingriffsbefugnisse wird regelmäßig – meist unausgesprochen[344], manchmal ausdrücklich[345] – vorausgesetzt, dass eine verstärkte Strafverfolgung dem Rechtsgüterschutz dient. Nur selten wird problematisiert, ob dies überhaupt der Fall ist, in welchem Maße präventive Wirkungen infolge einer Eingriffsbefugnis zu erwarten sind und wie sich dieser Nutzen zu dem Ausmaß

342 L/D³-Bäumler, J 536 und 679.

343 L/D³-Bäumler, J 535; Kube, Edwin (BKA-Abteilungspräsident), zitiert bei Feltes, Fehlerquellen im Ermittlungsverfahren (I): Die Polizei sei nicht in der Lage, „einen nennenswerten Anteil der Gesamtkriminalität zu verhüten".

344 Etwa Bayern und Thüringen in ihrem Gesetzesantrag, BR-Drs. 1014/01 (Entwurf eines Gesetzes zur Verbesserung des strafrechtlichen Instrumentariums für die Bekämpfung des Terrorismus und der Organisierten Kriminalität), 1.

345 Etwa LINX, Traceability (I), Punkt 1: „Of course, the ability to trace actions back to their source will, in itself, discourage unreasonable behaviour."

an unerwünschten Folgen der Befugnis verhält. Um diese Problematik näher zu beleuchten, soll an dieser Stelle zunächst näher auf kriminologische Erkenntnisse über die Wirksamkeit der Strafverfolgung eingegangen werden.

(i) Empirische Erkenntnisse über den Nutzen von Strafverfolgung

Präventive Wirkungen kann die Strafverfolgung einerseits dadurch entfalten, dass Straftäter an der Begehung weiterer Straftaten gehindert werden oder freiwillig davon absehen (Spezialprävention). Daneben könnten Strafverfahren auch Personen, die von Strafverfahren gegen andere Kenntnis erlangen, von der Begehung von Straftaten abhalten (Generalprävention).

Im Bereich der Spezialprävention kann das Strafverfahren zunächst im Wege unmittelbaren Zwangs präventiv wirken. So kann eine freiheitsentziehende Untersuchungsmaßnahme, Strafe oder Maßnahme der Besserung und Sicherung (§§ 61 ff. StGB) dem Täter bereits die Möglichkeit nehmen, in dieser Zeit fremde Rechtsgüter zu gefährden. Neben der Verhinderung zukünftiger Straftaten kann das Strafverfahren auch die weitere Begehung einer noch nicht vollendeten Straftat unterbinden (vgl. etwa §§ 23, 24, 30 Abs. 2, 127 ff. StGB) oder wenigstens den Eintritt weiterer Schäden und Gefahren infolge einer bereits vollendeten Straftat verhindern. Dies kann beispielsweise im Wege der Festnahme des Täters erfolgen. Auch eine Restitution des Geschädigten kann erfolgen, etwa durch die Rückgabe betrügerisch erlangter Gegenstände.

Während diese Aspekte des Rechtsgüterschutzes durch Strafverfolgung theoretisch auf der Hand liegen, ist für die verfassungsrechtliche Abwägung ihr tatsächliches Gewicht maßgeblich. Dieses bestimmt sich danach, ob und in welchem Maße die erwünschten präventiven Effekte tatsächlich eintreten. Was eine mögliche Restitution des Geschädigten anbelangt, so ist nicht bekannt, in wie vielen Fällen und in welchem Maße eine Restitution infolge eines strafrechtlichen Ermittlungsverfahrens gegenwärtig stattfindet. An den Geschädigten zurückgegeben werden kann jedenfalls nur Vermögen. Da strafbare Zugriffe auf fremdes Vermögen regelmäßig erfolgen werden, um das erlangte Vermögen zu eigenen Zwecken einzusetzen, wird dieses oft nicht mehr vorhanden sein. Da außerdem zu vermuten ist, dass Straftäter

nur selten über nennenswertes eigenes Vermögen verfügen, wird auch eine Restitution im Wege des Schadensersatzes zumeist ausscheiden.

Weiterhin ist der Nutzen einer Inhaftierung von Straftätern zu betrachten. Dass eine eingesperrte Person während der Haftzeit regelmäßig keine Straftaten begehen kann, steht fest[346]. Dennoch sind Auswirkungen des amerikanischen Konzepts der „Incapacitation" auf das allgemeine Kriminalitätsniveau nicht nachgewiesen[347]. Wegen der großen Zahl von Kleinkriminellen und der beschränkten Anzahl an Gefängnisplätzen ist der Nutzen einer „Verwahrung" jedenfalls bei weniger schwer wiegenden Delikten gering[348]. Auch eine Beschränkung des Freiheitsentzugs auf besonders gefährliche Straftäter ist praktisch nicht durchführbar, weil sich die zukünftige Straffälligkeit von Straftätern nicht prognostizieren lässt[349]. Gegen jeden potenziell gefährlichen Straftäter eine Gefängnisstrafe zu verhängen, ist schon wegen der hohen Kosten der Vollstreckung von Freiheitsstrafen unmöglich.

Gerade auf dem Gebiet der organisierten Kriminalität ist außerdem die Annahme plausibel, dass es einen lukrativen Markt für bestimmte kriminelle Aktivitäten gibt und dass „unschädlich gemachte" Straftäter alsbald durch andere Personen ersetzt werden. Hinzu kommen die kontraproduktiven Effekte des Freiheitsentzugs auf Insassen[350]: Die Vertrautheit mit dem Übel der Freiheitsstrafe kann deren abschreckende Wirkung für die Zukunft vermindern[351]. Gerade ein Aufenthalt in einer Justizvollzugsanstalt kann dazu führen, dass jemand zum Wiederholungstäter wird[352]. Überreaktionen von staatlichem Personal können auf Täter stigmatisierend wirken[353]. Die Erfahrung von Demütigung ist ein wichtiges Motiv gerade von Terroristen[354]. Im Übrigen spricht das Beispiel der USA gegen die Annahme, ein verstärkter Freiheitsentzug könne das Kriminalitätsniveau senken. Obwohl sich in den USA ein weltweit

346 BMI/BMJ, Sicherheitsbericht 2001, 381.

347 Sherman u.a.-Sherman, Preventing Crime, 44: „Recent reviews conclude there is very little evidence that increased incarceration has reduced crime".

348 Diekmann, Die Befolgung von Gesetzen, 149.

349 Sherman u.a.-MacKenzie, Preventing Crime, 431.

350 BMI/BMJ, Sicherheitsbericht 2001, 381.

351 Kunz, Kriminologie, § 31, Rn. 17.

352 Kunz, Kriminologie, § 31, Rn. 17.

353 Schneider, Kriminologie, 324.

354 Limbach, Jutta: Ist die kollektive Sicherheit Feind der individuellen Freiheit? 10.05.2002, www.zeit.de/reden/-Deutsche%20Innenpolitik/200221_limbach_sicherheit.
html; Rötzer, Florian: Armut ist keine Ursache für den Terrorismus, Telepolis, Heise-Verlag, 01.08.2002, www.heise.de/tp/-deutsch/inhalt/co/13015/1.html.

nahezu einmaliger Anteil der Bevölkerung im Freiheitsentzug befindet, ist die Kriminalität laut Statistik erheblich höher als in Deutschland[355].

Was die möglichen Auswirkungen des Strafverfahrens auf den freien Entschluss von Straftätern in Bezug auf die zukünftige Begehung weiterer Straftaten angeht, so gibt es trotz intensiver Forschung weltweit keinen empirischen Beleg für die Annahme, dass eine Verurteilung in spezialpräventiver Hinsicht einer Verfahrenseinstellung überlegen sein könnte[356]. Ebenso wenig erwiesen ist, dass die Bekanntgabe eines Ermittlungsverfahrens an eine Person spezialpräventiv wirken könnte.

Letztlich lässt sich also nicht feststellen, dass das Betreiben eines Ermittlungs-, Gerichts- oder Strafvollstreckungsverfahrens irgendeine spezialpräventive Wirkung auf den jeweiligen Beschuldigten, Angeklagten oder Verurteilten hat. Dass sich spezialpräventive Wirkungen der Strafverfolgung nicht empirisch belegen lassen, bedeutet zwar nicht zwangsläufig, dass sie nicht existieren[357]. Wenn sich für eine Theorie aber trotz beträchtlichen Aufwands über Jahrzehnte keine Belege haben finden lassen, dann muss diese Theorie als gescheitert bezeichnet werden[358].

Was eine mögliche generalpräventive Wirkung der Strafverfolgung anbelangt, so kommen einige der vielen empirischen Untersuchungen auf diesem Gebiet zu dem Ergebnis, dass ein gewisser Einfluss des subjektiv angenommenen Entdeckungsrisikos auf die Delinquenz nachweisbar sei[359]. Anerkannt ist dies jedoch nur bei einigen minder schweren Delikten[360]. Anderen einschlägigen Forschungsergebnissen zufolge sollen keinerlei generalpräventive Wirkungen der Erwartung, bei Begehung einer Straftat bestraft zu werden, feststellbar sein[361]. Die geringe oder fehlende Bedeutung des subjektiv angenommenen Entdeckungsrisikos lässt sich mit der empirisch gewonnenen Erkenntnis erklären, dass Straftäter das Entdeckungsrisiko bei ihrer Entschlussfassung nur selten berücksichtigen[362].

---

355 Bottger/Pfeiffer, ZRP 1994, 7 (14).

356 BMI/BMJ, Sicherheitsbericht 2001, 382.

357 Göppinger, Kriminologie, 179.

358 Niggli, Kriminologische Überlegungen zur Strafzumessung (I), 8 für die negative Spezial- und Generalprävention.

359 Diekmann, Die Befolgung von Gesetzen, 129 und 133.

360 BMI/BMJ, Sicherheitsbericht 2001, 382.

361 Kunz, Kriminologie, § 30, Rn. 15; Eisenberg, Kriminologie, § 41, Rn. 6; Diekmann, Die Befolgung von Gesetzen, 131; Bönitz, Strafgesetze und Verhaltenssteuerung, 329.

Den genannten Untersuchungen ist gemeinsam, dass eine generalpräventive Wirkung der wahrgenommenen Sanktionswahrscheinlichkeit, sofern sie überhaupt existiert, gering und im Vergleich zu anderen Faktoren minimal ist[363]. So spielt der Grad der Abweichung eines strafbaren Verhaltens von sozialen Normen sowie die soziale Integration einer Person eine erheblich größere Rolle für den Entschluss, eine Straftat zu begehen oder nicht, als die wahrgenommene Sanktionswahrscheinlichkeit[364]. Daneben gibt es eine Vielzahl weiterer Faktoren, die jeweils für sich genommen erheblich bedeutsamer für die Delinquenz sind als die Sanktionswahrscheinlichkeit, etwa der von dem Delikt erhoffte Nutzen, die soziale Bezugsgruppe einer Person, ihr Einkommen, ihre etwaige Arbeitslosigkeit[365], ihre Freizeittätigkeiten, ihre individuellen Moralvorstellungen[366], vermutete negative Reaktionen des Umfelds auf eine Straftat, die Delinquenz in der Vergangenheit, gerichtliche Vorverurteilungen und das Ausmaß der im Bekanntenkreis beobachteten Kriminalität[367]. Im Vergleich zur Bedeutung dieser Faktoren ist der Einfluss der empfundenen Sanktionswahrscheinlichkeit nicht nennenswert[368]. Dass ein potenzieller Straftäter von seinem Vorhaben absieht, weil er damit rechnet, dass ihn die Polizei überführen kann, ist mithin selten[369].

Überdies würde der Versuch, das subjektiv angenommene Entdeckungsrisiko durch eine verstärkte Strafverfolgung zu erhöhen, schon daran scheitern, dass potenzielle Straftäter das objektive Entdeckungsrisiko beziehungsweise die tatsächliche Aufklärungsrate nicht kennen[370] und ihr Verhalten folglich nicht daran ausrichten können. In den USA hat man etwa versucht, das subjektiv wahrgenommene Entdeckungsrisiko durch eine stete Ausweitung der Ermittlungsbefugnisse zu steigern[371]. Ein kriminalitätssenkender Einfluss dieser Strategie ist jedoch nicht zu erkennen. In der Bevölkerung wird das Entdeckungsrisiko ohnehin durchgehend weit überschätzt[372], so

362 Kunz, Kriminologie, § 30, Rn. 19; Niggli, Kriminologische Überlegungen zur Strafzumessung (I), 9.

363 Feltes, MschrKrim 1993, 341 (344 f.); Bönitz, Strafgesetze und Verhaltenssteuerung, 329.

364 Diekmann, Die Befolgung von Gesetzen, 133; Feltes, MschrKrim 1993, 341 (344 f.).

365 Diekmann, Die Befolgung von Gesetzen, 133.

366 Feltes, MschrKrim 1993, 341 (344 f.).

367 Bönitz, Strafgesetze und Verhaltenssteuerung, 329.

368 Bönitz, Strafgesetze und Verhaltenssteuerung, 329.

369 L/D^{3}-Bäumler, J 535.

370 Kunz, Kriminologie, § 30, Rn. 20; Eisenberg, Kriminologie, § 41, Rn. 9; Niggli, Kriminologische Überlegungen zur Strafzumessung (I), 9.

371 Rohe, Verdeckte Informationsgewinnung mit technischen Hilfsmitteln zur Bekämpfung der Organisierten Kriminalität, 47.

372 Kunz, Kriminologie, § 30, Rn. 20; Bönitz, Strafgesetze und Verhaltenssteuerung, 329.

dass selbst ein objektiv gesteigertes Entdeckungsrisiko noch hinter dem subjektiv wahrgenommenen zurückbleiben würde[373].

Man muss danach annehmen, dass die generalpräventive Abschreckungswirkung der Strafverfolgung im Wesentlichen dadurch ausgeschöpft wird, dass sich potenzielle Straftäter einem gewissen Entdeckungsrisiko ausgesetzt sehen. Solange die Bevölkerung nicht den Eindruck hat, eine Strafverfolgung sei in bestimmten Bereichen generell ausgeschlossen, kommt es auf das tatsächliche Ausmaß an Strafverfolgung für das allgemeine Kriminalitätsniveau also nicht an. Dass die Entscheidung einer Person für oder gegen eine Straftat von einer um einige Prozentpunkte höheren oder niedrigeren Entdeckungswahrscheinlichkeit abhängen könnte, ist nicht plausibel. Ob die Aufklärungsrate 10 oder 20% beträgt, wird für den Entschluss einer Person, eine Straftat zu begehen, keine Rolle spielen. In höherem Maße als um einige Prozentpunkte ließe sich die Ermittlungserfolgsrate realistischerweise nicht steigern. In Übrigen werden die Kosten einer Steigerung der Aufklärungsrate um nur 1% auf eine halbe Milliarde Euro geschätzt[374].

Gemessen an dem genannten Maßstab ist es auf dem Gebiet des Zugriffs auf Telekommunikations-Verkehrsdaten vollkommen ausreichend, wenn in einzelnen Fällen die Aufbewahrung von Telekommunikations-Verkehrsdaten zur Strafverfolgung angeordnet werden kann, wie es in der Cybercrime-Konvention des Europarates für Verbindungen zum Datenaustausch vorgesehen ist und in den USA allgemein praktiziert wird. Bereits dadurch können sich potenzielle Straftäter vor einer Entdeckung nicht sicher fühlen. Darüber hinaus gehende generalpräventive Wirkungen durch eine generelle Vorratsspeicherung aller Verkehrsdaten sind nach dem Gesagten nicht ernsthaft zu erwarten, zumal jeder rational planende Kriminelle eine solche Maßnahme leicht umgehen könnte[375].

Fasst man die Forschungsergebnisse bezüglich möglicher präventiver Wirkungen des Strafrechts zusammen, so ist festzuhalten, dass solche Wirkungen auf keinem Gebiet zweifelsfrei empirisch belegbar sind[376]. Ob man daraus den Schluss ziehen

373 Kunz, Kriminologie, § 30, Rn. 20.

374 Feltes, MschrKrim 1993, 341 (350); vgl. auch Sherman u.a.-MacKenzie, Preventing Crime, 430 f.

375 Eckhardt, CR 2002, 770 (774); **Fehler! Textmarke nicht definiert.** ff.

376 Niggli, Kriminologische Überlegungen zur Strafzumessung (I), 7.

kann, das Strafrecht sei überhaupt sinnlos[377], kann dahinstehen. Jedenfalls sind im Bereich der Strafverfolgung angesichts der genannten Erkenntnisse nur entschieden mildere Eingriffsbefugnisse angemessen als bei der Abwehr konkreter Gefahren[378]. Der Gesetzgeber muss diese Abstufung auch abstrakt nachvollziehen. Bei der Einräumung von Befugnissen darf er nicht allzu sehr generalisieren, sondern muss bereichsspezifisch unterschiedliche Eingriffsschwellen vorsehen.

Die unterschiedlichen Anforderungen dürfen auch nicht dadurch umgangen werden, dass die Verwendung von Erkenntnissen, die im Rahmen der Gefahrenabwehr gewonnen wurden, ohne Weiteres auch für Zwecke der Strafverfolgung erlaubt wird[379]. Es ist ein Wertungswiderspruch, wenn die Kenntnisnahme personenbezogener Informationen mit Gefahren für höchste Rechtsgüter legitimiert wird, die Verwendung der Kenntnisse aber dann schon zur Verfolgung von geringwertigen Zwecken zulässig sein soll[380]. Aus Sicht der Betroffenen macht es keinen Unterschied, ob bereits erhobene Daten zu einem „Sekundärzweck" verwertet werden oder ob die Daten überhaupt erst zu diesem Zweck erhoben werden („Primärzweck"). In beiden Fällen ist der Betroffene gleichermaßen belastet, beispielsweise durch Verwicklung in ein strafrechtliches Ermittlungsverfahren, möglicherweise auch zu Unrecht. Die Sicht des Betroffenen ist die maßgebliche, wenn es um die Beurteilung der Verhältnismäßigkeit einer Maßnahme geht, denn dabei ist die Belastung der Betroffenen gegen den Nutzen der Maßnahme abzuwägen. Das wiederum zwingt zu dem Schluss, dass ein Eingriff in Art. 10 Abs. 1 Var. 3 GG durch Zweitverwertung von Daten nur zulässig ist, wenn auch die erstmalige Erhebung der Daten allein zu diesem Zweck und auf dieselbe Weise verhältnismäßig gewesen wäre[381]. Dem tragen bestehende Normen bisher keine Rechnung.

(ii) Möglicher Nutzen einer Erweiterung der Befugnisse der Strafverfolgungsbehörden

377 Nachweise bei Kaiser, Kriminologie, 103; Eisenberg, Kriminologie, § 41, Rn. 17 und § 42, Rn. 11.

378 Vgl. BVerfGE 100, 313 (394 ff.); vgl. auch Art. 13 Abs. 3 und 4 GG; ebenso Schenke, AöR 125 (2000), 1 (29); Schenke, JZ 2001, 997 (997); dagegen AK-GG-Bizer, Art. 10, Rn. 95.

379 BVerfGE 100, 313 (389 f.).

380 So aber das BVerfG in E 100, 313 (373 ff.); vgl. auch Art. 13 Abs. 5 S. 2 GG.

381 Gusy, KritV 2000, 52 (63); L/D³-Bäumler, J 719; so jetzt auch BVerfGE 109, 279 (377) und BVerfG, NJW 2004, 2213 (2221).

Fraglich ist, ob und in welchem Maße erweiterte informationelle Eingriffsbefugnisse in Strafverfahren den Rechtsgüterschutz stärken können. Vorab ist festzuhalten, dass eine Ausweitung informationeller Eingriffsbefugnisse hohe Kosten verursachen kann, etwa Fortbildungskosten oder Kosten für die Anschaffung technischer Einrichtungen. Soweit der Staat die Kosten trägt, können der originären Kriminalpräventionsarbeit auf diese Weise Mittel vorenthalten werden. Weil die Bekämpfung der Ursachen von Kriminalität vielversprechender ist als Maßnahmen der Strafverfolgung[382], sind Mittelverlagerungen in den Bereich der Strafverfolgung kontraproduktiv. Zwar lässt sich vortragen, ohne die Möglichkeit einer Bestrafung könne keine alternative Vorbeugungsstrategie auskommen[383]. Die Strafverfolgung kann aber stets nur das letzte Mittel der Kriminalitätskontrolle sein[384]. Alles andere wäre eine Überschätzung ihrer präventiven Wirkungen, denn Strafverfolgung ist per definitionem primär auf nachträgliche Repression in einzelnen Fällen angelegt[385]. Dies wird etwa an den Vorschriften des Strafgesetzbuches über die Strafzumessung deutlich, die in erster Linie auf die Schuld des Täters abstellen (§ 46 Abs. 1 S. 1 StGB) und erst in zweiter Linie auf die Auswirkungen der Strafe (§ 46 Abs. 1 S. 2 StGB).

Gegen die Annahme, dass eine Erweiterung der Eingriffsbefugnisse im Strafverfahren eine kriminalitätssenkende Wirkung haben könnte, sprechen zunächst die in Deutschland auf politischer Ebene gemachten Erfahrungen. Nach der Auflösung des Polizeistaates des Dritten Reiches wurden in Deutschland vorhandene Überwachungsstrukturen zunächst zerschlagen. Seit 1968 wurde das Maß an informationellen Eingriffsbefugnissen wieder zusehends gesteigert, unter anderem um die Durchsetzung des Strafrechts zu erleichtern. Fundamentale Prinzipien wie die Unschuldsvermutung, das Trennungsprinzip, die Offenheit staatlicher Ermittlungen und die Konzentration von Maßnahmen auf Verdächtige sind immer weiter eingeschränkt worden[386], ohne dass jedoch ein Einfluss dieser Änderungen auf das Kriminalitätsniveau feststellbar wäre. Strafverfolgungsbehörden verweisen zwar auf – teilweise spektakuläre – Einzelfälle, die mit Hilfe der verschiedenen Befugnisse gelöst worden seien. Jedoch können solche Einzelfälle oder Erledigungsstatistiken nichts über die

382 Travis Hirschi, zitiert bei Kunz, Kriminologie, § 34, Rn. 3; Schneider, Kriminologie, 325; Diekmann, Die Befolgung von Gesetzen, 151.

383 Schneider, Kriminologie, 336.

384 Schneider, Kriminologie, 336.

385 Kunz, Kriminologie, § 31, Rn. 41; Hassemer, Strafen im Rechtsstaat, 277.

386 Hassemer, Strafen im Rechtsstaat, 255.

Frage aussagen, ob Auswirkungen von Befugniserweiterungen auf das Kriminalitätsniveau spürbar sind.

Dies ist, soweit ersichtlich, nicht der Fall. Trotz aller bisher erfolgten Befugniserweiterungen bestehen die gravierenden Strafverfolgungsdefizite, die allseits beklagt werden, unverändert fort. Als chronische Strafverfolgungsdefizite sind die großen Dunkelfelder und die geringen Aufklärungsquoten zu nennen, besonders auf den zentralen Gebieten modernen Strafrechts wie in den Bereichen der organisierten Kriminalität und Wirtschaftskriminalität[387]. Gerade Fälle der schwersten und folgenreichsten Kriminalität kommen höchst selten zur Anklage und zur Verurteilung, obwohl sie am sozialschädlichsten sind[388]. Selbst wenn es zu einer Anklage kommt, dauern Prozesse oft jahrelang und ziehen in den allermeisten Fällen allenfalls Geld- oder Bewährungsstrafen nach sich[389]. Auf dem Gebiet der Betäubungsmittelkriminalität ist es der Strafverfolgung offensichtlich nicht gelungen, eine merkliche Eindämmung des Drogenhandels und damit auch der Begehung entsprechender Straftaten zu erreichen. Im Bereich der Computerkriminalität kommt ein deutsches Gutachten zum Thema Datenpiraterie zu dem Ergebnis, „dass rechtliche Instrumentarien die Verbreitung der Raubkopien [...] nicht nennenswert verhindern. Das Ausmaß der in der Praxis festzustellenden Raubkopien steht in eklatantem Widerspruch zu den bisherigen rechtlichen Erfolgen"[390].

Eine Ursache für die Vollzugsdefizite kann darin liegen, dass die Strafverfolgung aus politischen Gründen auf vorweisbare Erfolge angewiesen ist, wobei in der Statistik jeder erledigte Fall gleich viel zählt. Dadurch kann es zu einer Konzentration auf leicht zu erledigende Kleinkriminalität kommen, wohingegen Fälle der schwersten, folgenreichsten und sozial schädlichsten Kriminalität nur höchst selten zur Anklage und Verurteilung gebracht werden[391].

Als weitere Ursache für die Vollzugsdefizite kommt die ständige Ausdehnung des Strafrechts in Betracht. Das Strafrecht beschränkt sich nicht mehr auf die klassische

387 Hassemer, Freiheitliches Strafrecht, 226 f.

388 Kunz, Kriminologie, § 35, Rn. 2; Hassemer, Freiheitliches Strafrecht, 226 f.

389 Albrecht, Die vergessene Freiheit, 168.

390 Sieber, Gutachten zum Thema Datenpiraterie (I).

391 Kunz, Kriminologie, § 35, Rn. 2 ff.; DG Research, Economic risks arising from the potenzial vulnerability of electronic commercial media to interception (I); Hassemer, Freiheitliches Strafrecht, 226 f.

Sicherung eines „ethischen Minimums"[392], also den Schutz konkreter Rechtsgüter. Es soll Rechtsgüter vielmehr bereits im Vorfeld vor vielfältigen Gefahren schützen und wird damit zu einem politischen Steuerungsinstrument auf nahezu allen Gebieten, etwa der Subventions- und Umweltpolitik, der Gesundheits- und Außenpolitik[393]. Kaum ein neues Gesetz kommt ohne einen Annex von Strafnormen zu seiner Durchsetzung aus. Dabei wird das Strafrecht oft nicht als letztes Mittel, sondern häufig als erstes oder sogar einziges Mittel zur Durchsetzung von Normen vorgesehen[394]. Obwohl den Ermittlungsbehörden, denen oft keine ausreichende Sachkenntnis und keine hinreichenden Mittel zur Verfügung stehen, Straftaten auf solchen Nebengebieten nur ganz ausnahmsweise bekannt werden und diese damit nur selten verfolgt werden können, scheint der Glaube an das Strafrecht als „Allzweckwaffe"[395] zur Lösung gesellschaftlicher Konflikte fortzubestehen und die Flut neuer Strafnormen nicht nachzulassen. Unter dem Aspekt des Grundsatzes der Gleichmäßigkeit der Strafverfolgung kann es nicht angehen, dass unter einer Masse rechtswidrig handelnder Personen nur wenige exemplarisch abgestraft werden, die übrigen dagegen nicht erreichbar sind.

Die Folgerung liegt nahe, dass das Strafrecht schlicht nicht in der Lage ist, in großflächigen Problemlagen Abhilfe zu schaffen, wie sie beispielsweise auf den Gebieten Drogen, Wirtschaft und Umwelt existieren[396]. Es ist als Instrument insoweit vergleichsweise schlecht geeignet[397]: Das Strafrecht ist vergangenheitsgerichtet und erlaubt keine konkreten Maßnahmen zur Vorbeugung von Schäden. Es ist auf die Bestrafung einzelner Täter gerichtet und in seinen Wirkungen entsprechend beschränkt. Das Strafverfahren braucht Zeit; rasche Reaktionen sind kaum möglich. Vielfältige Beschränkungen bei der Sachverhaltsermittlung und die Unschuldsvermutung führen dazu, dass das strafrechtliche Instrumentarium in den weitaus meisten Fällen nicht zum Zug kommt.

Das Strafrecht kann die hohen Erwartungen an seine Wirksamkeit daher zwangsläufig nicht erfüllen. Zur Prävention ist es schon seiner Eigenart nach – wenn überhaupt

---

392 Hassemer, Strafen im Rechtsstaat, 185.

393 Hassemer, Strafen im Rechtsstaat, 185.

394 Hassemer, Strafen im Rechtsstaat, 197.

395 Hassemer, Strafen im Rechtsstaat, 197.

396 Albrecht, Die vergessene Freiheit, 74 und 168.

397 Zum Folgenden Hassemer, Strafen im Rechtsstaat, 185 f. und 275 ff.

– nur sehr beschränkt und mittelbar in der Lage. Die meisten Faktoren, die in der Wissenschaft als mögliche Entstehungsgründe für Kriminalität diskutiert werden, sind in Strafverfahren nicht oder kaum beeinflussbar[398], und entsprechend der oben genannten Forschungsergebnisse verspricht eine gegenüber dem bestehenden Maß verschärfte Strafverfolgung weder in general- noch in spezialpräventiver Hinsicht nennenswerten Erfolg[399].

Dieser Befund steht nicht im Widerspruch zu der Annahme, dass die völlige Entkriminalisierung eines sozial schädlichen Verhaltens dessen Ausweitung zur Folge hätte. Diese Hypothese lässt ebenso wenig auf die Wirkung erweiterter Ermittlungsbefugnisse schließen wie auf den Nutzen härterer Strafen: Empirisch widerlegt ist bekanntlich der – von der Alltags- und Lebenserfahrung nahe gelegte und von vielen Bürgern als richtig unterstellte – Schluss, dass eine härtere Bestrafung das Kriminalitätsniveau senken könnte. Wenn zum Beleg für die Behauptung, dass die Einführung neuer Ermittlungsbefugnisse typischerweise einen positiven Einfluss auf die Aufklärungsquote habe, auf die Erfahrungen der Eingriffsbehörden verwiesen wird, ist daher zu entgegnen, dass subjektive Einschätzungen keine zuverlässige Beurteilungsgrundlage darstellen. Überdies hat ein internationaler Vergleich der Telekommunikationsüberwachung ergeben, dass „Struktur und Entwicklungen der von der Überwachung der Telekommunikation besonders betroffenen Kriminalitätsbereiche [...] im Vergleich der Länder keine Rückschlüsse darauf [zulassen], dass die Häufigkeit der Anordnung der Überwachung der Telekommunikation mit einer effizienteren Kontrolle der davon erfassten Kriminalitätsbereiche korreliert."[400]

Dieses Ergebnis widerlegt auch die Annahme, dass Ermittlungsbefugnisse, wenn sie die Kriminalität schon nicht eindämmen, wenigstens ihre Ausweitung verhinderten. Im zeitlichen und internationalen Vergleich ist nicht feststellbar, dass geringere Ermittlungsbefugnisse ein höheres Kriminalitätsniveau zur Folge haben. Plausibel – wenn auch mangels praktischer Beispiele nicht erwiesen – ist lediglich die Annahme, dass ein höheres Kriminalitätsniveau zu befürchten wäre, wenn potenzielle Straftäter den Eindruck hätten, eine Strafverfolgung sei in bestimmten Bereichen

398 BMI/BMJ, Sicherheitsbericht 2001, 462.

399 Travis Hirschi, zitiert bei Kunz, Kriminologie, § 34, Rn. 3; Feltes, Fehlerquellen im Ermittlungsverfahren (I).

400 Albrecht/Arnold/Demko/Braun, Rechtswirklichkeit und Effizienz der Telekommunikationsüberwachung, 437.

generell ausgeschlossen. Mehr als ein Mindestmaß an Eingriffsbefugnissen lässt sich damit aber nicht legitimieren.

Soweit ersichtlich hat noch niemand auch nur einen Einfluss der Aufklärungsquote auf die Anzahl der registrierten Straftaten feststellen können. Das bedeutet, dass man selbst dann nicht selbstverständlich von einem Nutzen zusätzlicher Ermittlungsbefugnisse ausgehen könnte, wenn fest stünde, dass diese die Aufklärungsquote erhöhten. Ist schon eine Korrelation zwischen der Aufklärungsquote in Bezug auf eine Straftat und der registrierten Anzahl ihrer Begehung nicht festzustellen, dann kann erst recht nicht davon ausgegangen werden, dass weiter gehende Ermittlungsbefugnisse das tatsächliche Kriminalitätsniveau senken könnten, obwohl gerade dies von Politikern und Bürgern verbreitet angenommen wird.

Realistischerweise können neue Ermittlungsbefugnisse die Aufklärungsquote bestenfalls um einige Prozentpunkte steigern. Ob eine Steigerung der Aufklärungsquote in dieser Größenordnung einen negativen Einfluss auf das Kriminalitätsniveau haben könnte, ist – auch angesichts des großen Dunkelfeldes von staatlich nicht registrierten Straftaten – äußerst fragwürdig. Gerade bei rational geplanten und auf dauernde Gewinnerzielung gerichteten Straftaten wie der Wirtschaftskriminalität und der organisierten Vermögenskriminalität, bei denen ein Einfluss des Entdeckungsrisikos auf den Tatentschluss noch am ehesten zu erwarten wäre, ist anzunehmen, dass die Inhaftierung einiger der Straftäter lediglich dazu führt, dass andere Bandenmitglieder ihr Werk fortführen, dass nicht inhaftierte Straftäter infolge der mangelnden Konkurrenz vermehrt Straftaten begehen oder dass Personen die lukrative Begehung der Straftaten neu aufnehmen.

Angesichts dessen spricht viel für die Annahme, dass Befugniserweiterungen – „more of the same" – keinen merklichen Einfluss auf die Kriminalität haben. Soweit die Kriminalität eine Ausprägung struktureller sozialer Probleme wie etwa von Arbeitslosigkeit oder übergreifender Entwicklungen wie der Globalisierung ist, ist anzunehmen, dass sie sich durch politische und erst recht durch lediglich kriminalpolitische Maßnahmen nicht merklich beeinflussen lassen wird[401]. Noch weniger als das Kriminalitätsniveau von Entdeckungsrisiko oder Strafhöhe abhängt, kann es vom Aus-

401 Hassemer, Strafen im Rechtsstaat, 261.

maß abstrakter Eingriffsbefugnisse abhängen. Auf dem Gebiet der Telekommunikationsüberwachung hat eine internationale Untersuchung ergeben, dass ein Einfluss der rechtlichen Ausgestaltung der Eingriffsbefugnisse auf das Kriminalitätsniveau nicht erkennbar sei[402]. Auch Vergleichsuntersuchungen zwischen den einzelnen Bundesstaaten der USA konnten keinen Zusammenhang zwischen den – je nach Staat unterschiedlichen – Ermittlungsbefugnissen und der Kriminalitätsentwicklung feststellen[403]. Im Vergleich zu Deutschland zeigen die Beispiele anderer Staaten, dass das Instrument der Telekommunikationsüberwachung erheblich seltener oder – wie etwa in Japan – überhaupt nicht zum Einsatz kommen kann[404], ohne dass die Sicherheit dieser Staaten unter diesem Umstand erkennbar leiden würde.

Generell weisen Staaten mit erheblich weiter gehenden Eingriffsbefugnissen, Diktaturen aber auch Demokratien wie die USA[405], im Vergleich zu Deutschland keineswegs eine niedrigere Kriminalitätsrate auf. Wenn selbst totalitäre Staaten, in denen der Überwachung keine Grenzen gesetzt sind, die Kriminalität durch Kontrollmaßnahmen nicht spürbar senken können, dann scheint dies in einem Rechtsstaat erst recht nicht möglich zu sein. Aus den genannten Gründen ist anzunehmen, dass erweiterte informationelle Eingriffsbefugnisse keinen nennenswerten Beitrag zum Rechtsgüterschutz erwarten lassen.

(iii) Nutzen einer Vorratsspeicherung im Speziellen

Im vorliegenden Zusammenhang ist von Bedeutung, in welchem Maße gerade eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten zum Rechtsgüterschutz geeignet ist. Zunächst lässt sich daran denken, dass gespeicherte Verkehrsdaten dazu verwendet werden könnten, noch unbekannte Straftaten oder Gefahren aufzudecken. Insoweit kommt etwa eine automatische Durchsuchung und Analyse der Datenbestände auf bestimmte Merkmale hin in Betracht, die geeignet sind, das Vorliegen einer Straftat oder Gefahr zu indizieren. Allerdings erscheint es aufgrund des Aussagegehalts von Verkehrsdaten unwahrscheinlich, dass aus deren Analyse gänzlich neue Anhaltspunkte für Gefahren gewonnen

402 Albrecht/Arnold/Demko/Braun, Rechtswirklichkeit und Effizienz der Telekommunikationsüberwachung, 437.

403 Rohe, Verdeckte Informationsgewinnung mit technischen Hilfsmitteln zur Bekämpfung der Organisierten Kriminalität, 47.

404 Für Japan wik-Consult, Studie (I), 103 f. und 110.

405 Vgl. Bottger/Pfeiffer, ZRP 1994, 7 (14): Die Kriminalität in den USA sei laut Statistik erheblich höher als in Deutschland.

werden könnten. Solche Projekte, die manchmal als „fishing expeditions"[406] oder als „Stochern im Nebel"[407] bezeichnet werden, sind ohne vorherige Anhaltspunkte rechtsstaatlich bedenklich, erfordern ein großes Maß an Ressourcen und versprechen kaum Erfolg. Gerade die Bekämpfung organisierter Kriminalität erfordert stattdessen gezielte kriminalistische Arbeit[408].

Dies bestätigt die mit großem Aufwand im Jahre 2002 durchgeführte Rasterfahndung, die der Identifizierung potenzieller Terroristen dienen sollte. Nicht mehr als fünf Verdächtige wurden auf diesem Weg herausgefiltert, wobei mehrere davon bereits zuvor unter polizeilicher Beobachtung standen[409]. Die Rasterfahndung hat damit im Wesentlichen lediglich zur Aufdeckung einiger Fälle von Sozialhilfebetrug geführt[410]. Auch die Initiatoren der Rasterfahndung mussten schließlich eingestehen, dass sich „Schläfer" gerade dadurch auszeichnen, dass sie ein äußerlich vollkommen normales Leben führen[411]. Viele Terroristen leben über Jahre hinweg in westlichen Ländern und sind dort vollständig integriert. Eine der zentralen Figuren der al-Quaida war beispielsweise Sergeant bei der US-Armee und hatte in dieser Funktion sogar Zugang zu Geheimdokumenten[412]. Führen Terroristen aber ein äußerlich normales Leben, dann ist es aussichtslos, sie anhand äußerlicher Merkmale identifizieren zu wollen – so das Ergebnis einer wissenschaftlichen Vergleichsstudie zu Soziologie und Psychologie des Terrorismus[413]. Dies aber entzieht Verfahren, die – wie die Rasterfahndung – erst der Verdachtsgewinnung dienen sollen, den Boden. Gründe für die Annahme, dass dies bei anderen Kriminalitätszweigen oder speziell im Bereich von Telekommunikations-Verkehrsdaten substanziell anders sein könnte, sind nicht ersichtlich. Eine hinreichende Eignung solcher Filterverfahren zur Verdachtsgewinnung kann somit nicht angenommen werden.

---

406 GILC, Global Internet Liberty Coalition u.a.: Open letter to the European Parliament, gilc.org/cox_en.html.

407 Weichert, Terror und Informationsgesellschaft (I); ähnlich L/D³-Lisken, C 83: „Suchen im Nebel"; Schütte, ZRP 2002, 393 (397) zur Schleierfahndung spricht von einem Stochern „mit der Nadel im Heuhaufen".

408 Weichert, Terror und Informationsgesellschaft (I).

409 Klink, Manfred (BKA-Direktor), zitiert in BKA: Rasterfahndung bringt kaum Erfolge, Handelsblatt vom 09./10.05.2003, S. 4; vgl. auch Heise Verlag: Rasterfahndung führt nicht zum Erfolg, Meldung vom 09.04.2004, www.heise.de/newsticker/meldung/46416/.

410 Weichert, Thilo: Beängstigende Bilanz der Terrorismusbekämpfung, 10.09.2002, www.datenschutzverein.de/-Pressemitteilungen/2002_07.html.

411 Krischer, Markus: In den Köpfen der Krieger Allahs, FOCUS 37/2002, S. 52-58, 52 (54).

412 Krischer, Markus: In den Köpfen der Krieger Allahs, FOCUS 37/2002, S. 52-58, 52 (61).

413 Krischer, Markus: In den Köpfen der Krieger Allahs, FOCUS 37/2002, S. 52-58, 52 (54); vgl. auch AG Wiesbaden, DuD 2003, 375 (375 ff.).

Von Bedeutung können angesichts dessen vor allem Fälle sein, in denen ein Verdacht bezüglich des Vorliegens einer bestimmten Straftat oder Gefahr bereits besteht oder das Vorliegen einer Straftat oder Gefahr bereits gewiss ist. Hier könnten Strafverfolgungsbehörden beispielsweise versuchen, anhand von Telekommunikations-Verkehrsdaten zu klären, ob eine vermutete Straftat begangen wurde und wenn ja, an welchem Ort und durch wen sie begangen wurde. Gefahrenabwehrbehörden könnten versuchen, mit Hilfe von Telekommunikations-Verkehrsdaten zu klären, ob eine vermutete Gefahr besteht und welche Rechtsgüter an welchem Ort durch wen gefährdet sind.

Die Einführung einer obligatorischen Vorratsspeicherung von Telekommunikations-Verkehrsdaten ist grundsätzlich geeignet, die Verdachtssteuerung und Verdachtsverdichtung zu erleichtern. Durch eine Vorratsspeicherung wird vermieden, dass sich Kommunikationsvorgänge nicht nachvollziehen lassen, weil ihre Umstände nicht aufgezeichnet wurden oder die Aufzeichnungen gelöscht wurden. Allerdings ist nicht bekannt, in wie vielen und in welchen Fällen tatsächlich ein Bedarf nach Verkehrsdaten besteht, die gegenwärtig nicht gespeichert oder gelöscht werden und die im Fall einer Vorratsspeicherung verfügbar wären. Zu beachten ist nämlich, dass eine Vorratsspeicherung die Quantität der zu staatlichen Zwecken verfügbaren Verkehrsdaten nur in begrenztem Maße steigern würde: Schon bisher kann die Aufzeichnung von Telekommunikations-Verkehrsdaten in Einzelfällen angeordnet werden (§ 100a StPO). Was Verkehrsdaten aus der Vergangenheit angeht, so wird schon bisher eine Vielzahl von Verkehrsdaten zu Abrechnungs- und Beweiszwecken bis zu sechs Monate lang gespeichert. Eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten würde diese Zeitdauer allenfalls auf 1-2 Jahre erhöhen können. In Großbritannien ist sogar eine Aufbewahrungsfrist von nur sechs Monaten und für Internet-Verkehrsdaten von nur vier Tagen geplant[414].

Angesichts dessen wird teilweise bezweifelt, ob eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten nennenswerten Nutzen für die staatliche Aufgabenerfüllung entfalten kann, und es werden nähere Untersuchungen über

[414] FIPR (foundation for information policy research): FIPR welcomes Commissioners' rejection of data retention, Pressemeldung vom 16.09.2002, www.fipr.org/press/020916Commissioners.html.

den Bedarf danach gefordert[415]. In der Praxis gebe es nur sehr wenige Fälle, in denen ein Auskunftverlangen daran scheitere, dass die Daten bereits gelöscht wurden[416]. Auf die meisten dieser Fälle wiederum seien die Sicherheitsbehörden erst nach so langer Zeit aufmerksam geworden, dass selbst nach den aktuellen Plänen für eine Vorratsspeicherung, die eine Speicherungsdauer von ein bis zwei Jahren vorsehen, die Daten bereits gelöscht worden wären[417].

Vertreter italienischer Sicherheitsbehörden sind der Ansicht, Untersuchungen im Bereich der Netzkriminalität begönnen nur selten vor Ablauf eines Jahres nach Begehung der Straftat[418]. Ihnen sind keine oder nur wenige Fälle bekannt, in denen eine Ermittlung an der fehlenden Vorratsspeicherung von Telekommunikations-Verkehrsdaten scheiterte[419]. Auch die schwedischen Strafverfolger sehen insoweit keinen Handlungsbedarf[420], wohingegen die britischen Behörden eine „zunehmende Anzahl" von Fällen vermelden, in denen es an Verkehrsdaten mangele[421]. Deutsche Stimmen behaupten, dass die Zuordnung von IP-Adressen zu einer Person im Internet „oftmals" scheitere, wenn nicht zeitnah ermittelt werde[422]. Die Bundesregierung sah im Jahr 2002 dagegen noch keine Notwendigkeit einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten[423].

Der Internet-Access-Provider AOL Großbritannien gibt an, 99,9% der an Sicherheitsbehörden erteilten Auskünfte hätten ausschließlich Bestandsdaten zum Gegenstand[424]. Verkehrsdaten sind also in weniger als 0,1% der Fälle erfragt worden, was

---

415 ISPA, Internet Service Providers' Association (UK): Memorandum by the Internet Services Providers' Association (ISPA), 19 November 2001, www.parliament.the-stationery-office.co.uk/pa/cm200102/cmselect/cmhaff/351/351ap10.htm; eco, Electronic Commerce Forum e.V., Verband der deutschen Internetwirtschaft: Vorratsdatenspeicherung ist verfassungswidrig! Pressemitteilung vom 17.12.2003, www.eco.de/servlet/PB/menu/1236462_pcontent_l1/content.html.

416 ECTA, European Competitive Telecommunications Association: ECTA position on data retention in the EU, August 2002, https://www.ectaportal.com/uploads/1412ECTAdataretentionstatement.DOC.

417 APIG, Communications Data, 25; vgl. auch Uhe/Herrmann, Überwachung im Internet (I), 111, wonach die vollständige Auswertung einer Computerausrüstung in einem deutschen Bundesland im Schnitt ein bis zwei Jahre dauere; a.A. Finnland in MDG, EU-Questionnaire (I), 24: In den meisten Fällen sei eine zweijährige Speicherung ausreichend.

418 Italien in MDG, EU-Questionnaire (I), 8.

419 Italien in MDG, EU-Questionnaire (I), 19.

420 Schweden in MDG, EU-Questionnaire (I), 19.

421 Großbritannien in MDG, EU-Questionnaire (I), 19.

422 BMI/BMJ, Sicherheitsbericht 2001, 203 f.

423 Deutschland in MDG, EU-Questionnaire (I), 24. Schon in BT-Drs. 13/4438, 39 sah die Bundesregierung keinen „aktuellen Bedarf" für eine Vorratsspeicherung.

424 De Stempel, Camille in APIG, All Party Parliamentary Internet Group (UK): Internet Service Providers Association (UK), APIG Communications Data Inquiry Oral Evidence, 11.12.2002, www.apig.org.uk/ispa_oral_evidence.htm.

gegen die Bedeutung speziell von Internet-Verkehrsdaten für die Sicherheitsbehörden spricht. Es ist bekannt, dass die meisten Auskunftsersuchen Telefon-Verbindungsdaten zum Gegenstand haben und dass Internet-Verkehrsdaten eher selten angefordert werden[425]. In Deutschland sollen Internet-Daten nur in etwa 0,5-1% der Fälle von Telekommunikationsüberwachung betroffen sein[426]. Ähnliche Zahlen sind aus den Niederlanden bekannt, wo Internet-Provider zu Investitionen in dreistelliger Millionenhöhe verpflichtet wurden, um die Telekommunikationsüberwachung im Internet sicher zu stellen, wo aber seit 1998 nicht mehr als fünf Internet-Überwachungsmaßnahmen angeordnet wurden[427].

Der mögliche Zusatznutzen einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten reduziert sich weiter dadurch, dass eine Vorratsspeicherung nur die Quantität, nicht aber die Qualität von Verkehrsdaten verbessern würde. Telekommunikations-Verkehrsdaten sind bedeutungslos, sobald die Kommunikationsnetze anonym genutzt werden[428]. Verhalten in den Kommunikationsnetzen nachvollziehen zu können, ist weitgehend sinnlos, wenn es sich nicht auch den jeweiligen Personen zuordnen lässt. Gerade dies ist heutzutage aber nicht gewährleistet; es gibt kostengünstige, leicht erreichbare und effektive Mittel zur anonymen Nutzung der Kommunikationsnetze. Dies führt dazu, dass aus technischer Sicht nahezu jede behördliche Maßnahme unter dem Vorbehalt steht, dass der jeweilige Täter nicht das gewisse Maß an krimineller Energie und technischem Geschick aufwendet, das erforderlich ist, um sich einer Identifizierung zu entziehen[429].

Für die Zukunft ist mit der Neu- und Fortentwicklung von Möglichkeiten zur anonymen Telekommunikation zu rechnen[430], was deren Verbreitung weiter fördern wird. Es ist anzunehmen, dass zunehmend komfortable und preisgünstige Lösungen auf den Markt kommen werden oder dass Anonymisierungstechniken sogar standardmäßig angeboten werden, besonders im Internet. Es dauert erfahrungsgemäß nur

---

425 NCIS Submission (I), Punkt 6.1.1.

426 Schulzki-Haddouti, Lauscher unter Beschuss, c't 09/2001, 24 ff.; Welp, TKÜV, 3 (4).

427 Ermert, Monika: Jedem Bundesland sein Lauschgesetz, 23.11.2002, Heise Newsticker, www.heise.de/newsticker/data/gr-23.11.02-001/.

428 Lenz, Karl-Friedrich: Stellungnahme zur Anhörung der Kommission über die Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität, europa.eu.int/ISPO
/eif/InternetPoliciesSite/Crime/Comments/kf_lenz.html.

429 Germann, 325 für das Internet.

430 Hamm, NJW 2001, 3100 (3101).

drei bis vier Jahre, bis sich neue Technik im Bereich von Endgeräten durchsetzt[431]. Vertreter von Sicherheitsbehörden erkennen an, dass sich die Verbreitung von Datenverschlüsselung im Zusammenhang mit Internetanwendungen weder aufhalten noch nationalstaatlich begrenzen lässt[432]. Nicht anders verhält es sich auf dem Gebiet von Anonymisierungstechniken.

Die anonyme Nutzung von Kommunikationsnetzen lässt sich in weiten Bereichen nicht verhindern. Denkbar wäre es zwar, in Deutschland oder vielleicht sogar Europa vorzusehen, dass sich jeder Käufer eines Mobiltelefons oder einer Telefonkarte, jeder Benutzer eines Hoteltelefons oder Internet-Cafés mit einem Ausweis identifizieren muss. Abgesehen von den damit verbundenen Freiheitseinbußen, die bisher nur totalitäre Staaten wie China und Pakistan[433] in Kauf nehmen, würde der Versuch der Abschaffung anonymer Telekommunikation spätestens an den Grenzen Europas scheitern. Der Umweg über Drittstaaten würde es weiterhin ohne größere Schwierigkeiten ermöglichen, sich anonym ein Mobiltelefon zu kaufen, Callback-Dienste zu nutzen, E-Mail-Konten einzurichten und Proxies zu verwenden, auch von Ländern aus, in denen eine Identifizierungspflicht existiert. Gerade die Divergenzen der nationalen Rechtsordnungen werden von Straftätern häufig ausgenutzt, um einer Strafverfolgung zu entgehen[434]. So haben Terroristen aus dem Umfeld der Anschläge auf das World Trade Center am 11. September 2001 unter anderem mit Schweizer SIM-Karten in ihren Handys telefoniert[435], weil bei dem Kauf von Schweizer SIM-Karten keine Personalien angegeben werden mussten. In vielen Staaten werden international einsetzbare SIM-Karten anonym verkauft[436].

Die vorliegenden Vorschläge zur Einführung einer Vorratsspeicherung sehen keine wirksamen Einschränkungen der anonymen Nutzung der Netze vor. Sich der ver-

---

431 Pfitzmann, Andreas in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 40.

432 Zwingel (Leiter des BKA-Referates IT-Nutzung und Telekommunikationsüberwachung), Technische Überwachungsmaßnahmen aus Sicht der Polizei, 37 (42).

433 Dazu Rötzer, Florian: Pakistan: Ausweis für Benutzung von Internetcafés, Telepolis, Heise-Verlag, 05.08.2002, www.heise.de/tp/deutsch/inhalt/te/13040/1.html.

434 BMI/BMJ, Sicherheitsbericht 2001, 204.

435 taz, Die Tageszeitung: Terroristen nutzten SIM-cards, 09.08.2002, www.taz.de/pt/2002/08/09/a0131.nf/text.name,askeVQpje.n,66.

436 taz, Die Tageszeitung: Terroristen nutzten SIM-cards, 09.08.2002, www.taz.de/pt/2002/08/09/a0131.nf/text.name,askeVQpje.n,66; Spanische Delegation in der Gruppe „Drogenhandel" des Rates der Europäischen Union: Entwurf von Schlussfolgerungen des Rates zur Notwendigkeit der Einführung einer gemeinsamen Regelung auf EU-Ebene für die Identifizierung von Guthabenkartenbenutzern zur Erleichterung der Ermittlungen im Bereich der organisierten Kriminalität insbesondere mit Blick auf den illegalen Drogenhandel, 05.06.2002, register.consilium.eu.int/pdf/de/02/st05/05157-r2d2.pdf.

fügbaren Möglichkeiten zur anonymen Nutzung der Netze nicht zu bedienen, wäre für einen Kriminellen aber so leichtsinnig wie eine Erpressung unter Benutzung des eigenen Telefonanschlusses oder wie ein Bankraub mit dem eigenen Nummernschild am Fluchtwagen[437]. Bekannt ist, dass sich die Nutzung von Möglichkeiten anonymer Telekommunikation in kriminellen Kreisen immer weiter durchsetzt[438]. Die Verwendung einer Vielzahl von anonym oder unter falschem Namen angemeldeten Mobiltelefonkarten sowie mehrerer Mobiltelefone abwechselnd ist heute bereits unter Kleinkriminellen verbreitet[439]. Die sicherheitsbewusstesten Großkriminellen sollen jedes Mobiltelefon und jede Mobiltelefonkarte gar nur einmal benutzen[440]. Selbst im Bereich redlicher Kunden werden etwa 50% der Mobiltelefonkarten innerhalb eines Jahres verschenkt[441], was eine Identifizierung des jeweiligen Nutzers vereiteln kann. Im Bereich der Internetkriminalität ist bekannt, dass in vielen Fällen gestohlene Internet-Zugangsdaten eines Dritten genutzt werden[442]. Auch die übrigen Möglichkeiten des Internet zur Wahrung der Anonymität und zur Erschwerung der Nachvollziehbarkeit von Absenderadressen werden nach Einschätzung des Ersten Sicherheitsberichts der Bundesregierung ausgenutzt[443]. Nach Angaben des Bayerischen Landeskriminalamts wurden bei 7-8% der dort durchgeführten Untersuchungen mit Internetrelevanz Anonymisierungsdienste eingesetzt[444].

Darüber hinaus ist anzunehmen, dass eine Vorratsspeicherung zu einer erheblich höheren Verbreitung anonymer Telekommunikation als bisher führen würde, weil dadurch ein konkreter Bedarf nach diesen Techniken entstünde[445]. Dieser kontraproduktive Effekt schlägt im Rahmen der Verhältnismäßigkeitsprüfung negativ zu Buche.

---

437 Lenz, Karl-Friedrich: Stellungnahme zur Anhörung der Kommission über die Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität, europa.eu.int/
ISPO/eif/InternetPoliciesSite/Crime/Comments/kf_lenz.html.

438 Jeserich (Leitender Oberstaatsanwalt bei der Generalstaatsanwaltschaft in Celle), TK-Überwachung, 63 (69).

439 Heise Verlag: IMSI-Catcher zur Mobilfunküberwachung bald legal, Meldung vom 30.11.2001, www.heise.de/newsticker/-data/hod-30.11.01-000/.

440 Fairbrother, Peter: Defeating traffic analysis, www.apig.org.uk/fairbrother.pdf.

441 BMWi-Ressortarbeitsgruppe, Eckpunkte zur Anpassung der Regelungen des § 90 TKG (I), 7.

442 Hong Kong Inter-departmental Working Group on Computer Related Crime, Report (I), 61.

443 BMI/BMJ, Sicherheitsbericht 2001, 205.

444 Gerling/Tinnefeld, DuD 2003, 305 (305).

445 Fairbrother, Peter: Defeating traffic analysis, www.apig.org.uk/fairbrother.pdf.

Angesichts der vielfältigen Möglichkeiten anonymer Telekommunikation ist fraglich, ob gerade gegen besonders gefährliche Personen wie Hintermänner organisierter Kriminalität effektiv im Wege des Zugriffs auf Telekommunikations-Verkehrsdaten vorgegangen werden kann. Teilweise wird vorgetragen, dass selbst professionelle Zielpersonen immer einmal wieder auch identifizierbare Anschlüsse benutzten[446]. Viele Straftäter seien zu bequem, um verfügbare Möglichkeiten anonymer Telekommunikation zu nutzen. Dies gelte jedenfalls außerhalb des Internetbereichs, in dem die Sicherheitsbehörden – wohl wegen der zahlenmäßig seltenen Überwachung in diesem Feld – noch keine Erfahrungen sammeln konnten[447].

Inwieweit die Hoffnung der Strafverfolgungsbehörden, auch Großkriminelle gelegentlich identifizieren zu können, berechtigt ist, lässt sich nicht sicher sagen. Immerhin steht fest, dass sich die Erfahrungswerte der Strafverfolgungsbehörden[448] nur auf die von ihnen tatsächlich erfassten Kommunikationsdaten und nur auf ihnen bekannte Täter beziehen können. Wie viel Telekommunikation und wie viele Personen ihnen dagegen entgehen, können sie kaum beurteilen. Es ist eine allgemeine Erkenntnis moderner Kriminologie, dass das Dunkelfeld unerkannter Straftaten allgemein sehr groß ist und dass, wenn eine Straftat einmal entdeckt und aufgeklärt wird, meistens nur „kleine Fische" überführt werden können[449].

Auch auf dem Gebiet der Telekommunikationsüberwachung konzedieren Vertreter der Sicherheitsbehörden, dass in den Kreisen wirklich gefährlicher Personen „gewichtige Überwachungsdefizite" bestehen und dass sich gerade besonders gefährliche Personen die Möglichkeiten der anonymen Telekommunikationsnutzung in hohem Maße zunutze machen[450]. Wirklich gefährliche Kriminelle suchten immer nach Wegen, um einer Überwachung vorzubeugen, beispielsweise durch die Benutzung vorausbezahlter Handys, von Internet-Cafés oder von pauschalen Ab-

446 Jeserich (Leitender Oberstaatsanwalt bei der Generalstaatsanwaltschaft in Celle), TK-Überwachung, 63 (68); so zu den Möglichkeiten der Verschlüsselung auch Graf, Jürgen (Generalbundesanwalt) in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 12 f.; Lorenz, GA 97, 51 (69).

447 Graf, Jürgen (Generalbundesanwalt) in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 14.

448 Zu deren Maßgeblichkeit BVerfGE 100, 313 (374 f.).

449 Hassemer, Strafen im Rechtsstaat, 278.

450 Jeserich (Leitender Oberstaatsanwalt bei der Generalstaatsanwaltschaft in Celle), TK-Überwachung, 63 (71); für den Internetbereich auch Gehde (LKA Berlin), c't 19/2002, 127.

rechnungsmodellen[451]. Wenn einige Telekommunikationsunternehmen Verkehrsdaten freiwillig speichern, dann würden organisierte Kriminelle andere Unternehmen nutzen[452]. Im Falle einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten würde diese Gruppe von Kriminellen sofort Gegenmaßnahmen ergreifen, um einer Überwachung zu entgehen[453].

Da es für professionelle Kriminelle, die viel zu verlieren haben, geradezu leichtsinnig wäre, sich vorhandener Möglichkeiten anonymer Kommunikation nicht zu bedienen, spricht viel dafür, dass sich der unsichere Gebrauch von Mobiltelefonen im Wesentlichen auf Kleinkriminalität beschränkt[454]. Organisierte Täterkreise sind demgegenüber bekannt dafür, mit äußerster Professionalität vorzugehen. Sie werden daher selbst hohe Kosten und Unbequemlichkeiten in Kauf nehmen, um ihre lukrativen und oft langfristig aufgebauten Geschäfte nicht zu gefährden. Aus diesen Gründen ist anzunehmen, dass sich ernsthafte Kriminelle regelmäßig einer Identifizierung entziehen werden[455] und dass der Zugriff auf Telekommunikations-Verkehrsdaten daher kein geeignetes Mittel ist, gegen diese Täterkreise effektiv vorzugehen[456].

Angesichts dieser Situation ist zwar ein kurzfristiger Handlungsvorteil der Behörden nach Einführung einer Vorratsspeicherung denkbar[457]. Dieser kann aber durch Prob-

---

451 Gamble, Jim (Assistant Chief Constable in the UK National Crime Squad) in APIG, All Party Parliamentary Internet Group (UK): UK Law Enforcement, APIG Communications Data Inquiry Oral Evidence, 18.12.2002, www.apig.org.uk/-law_enforcement_
oral_evidence.htm.

452 Gamble, Jim (Assistant Chief Constable in the UK National Crime Squad) in APIG, All Party Parliamentary Internet Group (UK): UK Law Enforcement, APIG Communications Data Inquiry Oral Evidence, 18.12.2002, www.apig.org.uk/-law_enforcement_oral_
evidence.htm.

453 Gamble, Jim (Assistant Chief Constable in the UK National Crime Squad) in APIG, All Party Parliamentary Internet Group (UK): UK Law Enforcement, APIG Communications Data Inquiry Oral Evidence, 18.12.2002, www.apig.org.uk/-law_enforcement_ oral_
evidence.htm.

454 Fairbrother, Peter: Defeating traffic analysis, www.apig.org.uk/fairbrother.pdf.

455 Snape, Tim (Managing Director des britischen ISP West Dorset Internet), zitiert bei McCue, Andy: Government rethinks data policy, 10.10.2001, www.vnunet.com/News/
1126012: „Any competent technician can bypass logging procedures"; Robinson, James K.: Vortrag auf der International Computer Crime Conference „Internet as the Scene of Crime" in Oslo, Norwegen, 29.-31.05.2000, www.usdoj.gov/criminal/-cybercrime/
roboslo.htm: „While less sophisticated cybercriminals may leave electronic ‚fingerprints,' more experienced criminals know how to conceal their tracks in cyberspace."

456 So Pfitzmann, Andreas in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 10 angesichts von Verschlüsselungsmöglichkeiten: eher zweifelhaft; a.A. Graf, Jürgen (Generalbundesanwalt) in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 12 f. und 44.

457 Fairbrother, Peter: Defeating traffic analysis, www.apig.org.uk/fairbrother.pdf.

leme in der Einführungsphase der Technik gemindert werden[458]. Nach einigen Monaten wird sich überdies jedenfalls ein großer Teil der gefährlichen Kriminellen auf die neue Situation eingestellt haben und von den Möglichkeiten anonymer Telekommunikation Gebrauch machen[459]. Es liegt daher nahe, dass eine Vorratsspeicherung zur Überführung einiger Unachtsamer führen könnte und Kleinkriminelle wie schon bisher überführt werden könnten, dass sie gegen umsichtige und ernsthafte Kriminelle aber nahezu gänzlich wirkungslos wäre[460] und dass insoweit nach wie vor nur in Einzelfällen Erfolge erzielt werden könnten.

Angesichts der Möglichkeiten zur anonymen Nutzung der Telekommunikationsnetze muss man daher davon ausgehen, dass eine Vorratsspeicherung von Verkehrsdaten regelmäßig allenfalls bei geringen Gefahren Abhilfe schaffen kann[461]. Die Eignung zur Bekämpfung organisierter Kriminalität oder zur Verhütung terroristischer Anschläge ist demgegenüber als gering einzuschätzen. Die Schaffung besonders eingriffsintensiver Befugnisse, die regelmäßig nur im Bereich der kleinen und mittleren Kriminalität Nutzen entfalten können, steht im Widerspruch zu dem Grundsatz der gleichmäßigen Strafverfolgung und führt zu einer weiteren Konzentration der Strafverfolgung auf die Bekämpfung der „kleinen Fische".

Die Bedeutung des Zugriffs auf Verkehrsdaten im Rahmen von Ermittlungsverfahren darf auch nicht überschätzt werden: Zu Recht warnen Behördenvertreter, dass es eine Überschätzung der Möglichkeiten der Telekommunikationsüberwachung wäre, diese allein als „Schlüssel zur inneren Sicherheit" anzusehen[462]. Während plausibel ist, dass der Zugriff auf Verkehrsdaten im Rahmen von Ermittlungsverfahren nützlich sein kann, bedeutet das noch nicht, dass Verkehrsdaten das entscheidende,

---

458 Fairbrother, Peter: Defeating traffic analysis, www.apig.org.uk/fairbrother.pdf.

459 Fairbrother, Peter: Defeating traffic analysis, www.apig.org.uk/fairbrother.pdf.

460 Fairbrother, Peter: Defeating traffic analysis, www.apig.org.uk/fairbrother.pdf; BITKOM: Stellungnahme zur Gesetzesinitiative des Bundesrates vom 31.05.2002 (BR-Drs. 275/02), 12.08.2002, www.bitkom.org/files/documents/Position_BITKOM_Vorrats datenspeicherung_u.a._12.08.2002.pdf, 9; o2 (Germany): Schriftliche Stellungnahme zur öffentlichen Anhörung am 09.02.2004 in Berlin zum Entwurf eines Telekommunikationsgesetzes (TKG), in Ausschussdrucksache 15(9)961, www.bundestag.de/gremien
15/a09/004Anhoerungen/TKG/materialeingeladene.pdf, 140 (146).

461 Fairbrother, Peter: Defeating traffic analysis, www.apig.org.uk/fairbrother.pdf; BITKOM: Stellungnahme zur Gesetzesinitiative des Bundesrates vom 31.05.2002 (BR-Drs. 275/02), 12.08.2002, www.bitkom.org/files/documents/-Position_BITKOM_Vorratsdaten
speicherung_u.a._12.08.2002.pdf, 9.

462 Bansberg (Abteilung Grundsatzangelegenheiten des Bundesamtes für Verfassungsschutz), Staatsschutz im Internet, 48 (54).

zur Aufklärung der Straftat führende Element darstellen[463]. Außerhalb des Gebiets der Netzkriminalität stellen Verkehrsdaten nur einen kleinen Teil des Puzzles dar, welches die Ermittler zusammen setzen müssen[464]. Ein Fehlen von Verkehrsdaten kann oft durch andere Informationsquellen ausgeglichen werden[465], deren Erschließung zwar aufwändiger sein kann, dafür aber zielgerichteter erfolgen und infolgedessen effektiver sein kann[466]. Selbst wenn die erforderlichen Verkehrsdaten zur Verfügung stehen, kann die Aufklärung einer Straftat immer noch aus einer Vielzahl von anderen Gründen scheitern.

Es ist daher nicht klar, ob eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten einen merklichen Einfluss auf die Aufklärungsrate oder gar das Kriminalitätsniveau haben könnte. Angesichts der beschriebenen Bedenken gegen die präventive Wirksamkeit der Strafverfolgung allgemein, besonders gegen den Nutzen der Erweiterung ihrer Befugnisse, sowie gegen die Wirksamkeit gerade einer Vorratsspeicherung von Verkehrsdaten ist ein merklicher Einfluss dieser Maßnahme auf die Kriminalitätsrate nicht anzunehmen.

Im Übrigen sollte auch die Bedeutung des Arguments nicht überschätzt werden, dass der verstärkte Zugriff auf Verkehrsdaten dazu dienen könnte, Unschuldige von falschen Verdachtsmomenten zu entlasten[467]. Nur in Einzelfällen kann davon ausgegangen werden, dass Verkehrsdaten mit Hilfe von anderen Ermittlungsmethoden gewonnene Verdachtsmomente entkräften können. Ihre Aussagekraft ist wegen der vielen Manipulationsmöglichkeiten zu gering. Demgegenüber ist mit einer Vielzahl von Massenverdächtigungen durch Verkehrsdaten-Rasterung der oben genannten Art zu rechnen, was den möglichen Entlastungseffekt bei Weitem überwiegt. Als konkretes Beispiel lässt sich der Fall eines Nigerianers in Österreich anführen, der mehrere Monate lang in Untersuchungshaft genommen wurde, weil er wegen seiner zahlreichen Telefonkontakte als Führer einer Rauschgiftbande in Ver-

---

463 De Stempel, Camille in APIG, All Party Parliamentary Internet Group (UK): Internet Service Providers Association (UK), APIG Communications Data Inquiry Oral Evidence, 11.12.2002, www.apig.org.uk/ispa_oral_evidence.htm.

464 De Stempel, Camille in APIG, All Party Parliamentary Internet Group (UK): Internet Service Providers Association (UK), APIG Communications Data Inquiry Oral Evidence, 11.12.2002, www.apig.org.uk/ispa_oral_evidence.htm.

465 Bansberg (Abteilung Grundsatzangelegenheiten des Bundesamtes für Verfassungsschutz), Staatsschutz im Internet, 48 (54).

466 Weichert, DuD 2001, 694 (694).

467 So NCIS, APIG-Submission (I), Punkt 3.0; zu diesem Argument ausführlich Seiten 120-121.

dacht geraten ist[468]. Später stellte sich der Verdacht als unbegründet und der Nigerianer einfach als gefragter Ratgeber für die schwarze Gemeinschaft in Wien heraus[469]. In den USA sollen 800 Personen nur deshalb in Untersuchungshaft sitzen, weil sie im Vorfeld des 11. September besonders viel kommuniziert haben[470].

(cc) Zusammenfassung: Nutzen einer Vorratsspeicherung von Telekommunikationsdaten

Festzuhalten ist, dass eine vorsorgliche, generelle Speicherung von Telekommunikations-Verkehrsdaten notwendig vergangenheitsbezogen ist und daher im Wesentlichen nur der Aufklärung bereits begangener Straftaten dienen kann. Nach den obigen Ausführungen kann nicht davon ausgegangen werden, dass Strafverfahren den Entschluss von Personen zur Begehung von Straftaten beeinflussen können. Der Verfolgung bereits begangener Straftaten können präventive Effekte nur insoweit zugeschrieben werden, als Straftäter im Wege des Freiheitsentzugs von der Gefährdung von Rechtsgütern abgehalten werden oder als infolge eines Strafverfahrens eine Restitution oder Entschädigung der Opfer einer Straftat erfolgen kann. In wie vielen Fällen gerade eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten dabei von Nutzen wäre, ist nicht bekannt. Die vielfältigen Möglichkeiten zur anonymen Telekommunikation, von denen bei Einführung einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten vermutlich verstärkt Gebrauch gemacht würde, stellen den möglichen Nutzen der Maßnahme allerdings grundlegend in Frage.

Insgesamt ist anzunehmen, dass eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten nur in wenigen und regelmäßig wenig bedeutenden Einzelfällen den Schutz von Rechtsgütern fördern könnte[471]. Ein dauerhafter, negativer Effekt auf das Kriminalitätsniveau ist selbst im Bereich der Netzkriminalität nicht zu erwarten. Die Eignung einer Vorratsspeicherung zur Bekämpfung organisierter Krimi-

---

468 Krempl, Stefan: Die totale Informationsüberwachung, die Demokratie und die Hacker, Telepolis, Heise-Verlag, 28.12.2002, www.heise.de/tp/deutsch/inhalt/te/13870/1.html.

469 Krempl, Stefan: Die totale Informationsüberwachung, die Demokratie und die Hacker, Telepolis, Heise-Verlag, 28.12.2002, www.heise.de/tp/deutsch/inhalt/te/13870/1.html.

470 Krempl, Stefan: Die totale Informationsüberwachung, die Demokratie und die Hacker, Telepolis, Heise-Verlag, 28.12.2002, www.heise.de/tp/deutsch/inhalt/te/13870/1.html.

471 Earl of Northesk: Debatte im House of Lords, 27.11.2001, www.parliament.the-stationery-office.co.uk/pa/ld199900/-ldhansrd/pdvn/lds01/text/11127-13.htm; vgl. auch BVerfGE 103, 21 (31) zu vorsorglich gespeicherten DNA-Profilen: „Künftige Straftaten können sie im Regelfall auch tatsächlich nicht verhindern".

nalität oder zur Verhütung terroristischer Anschläge ist als äußerst gering bis nicht gegeben einzuschätzen.

(dd) Betroffene Grundrechtsträger nach Art und Zahl, Identifizierbarkeit der Betroffenen, Eingriffsvoraussetzungen

Für die Bemessung des Verlusts an grundrechtlich geschützter Freiheit infolge einer generellen Speicherung von Verkehrsdaten ist zunächst maßgeblich, welche und wie viele Grundrechtsträger von einer solchen Maßnahme negativ betroffen wären. Während konkrete Nachteile von staatlicher Seite regelmäßig erst durch den staatlichen Zugriff auf die gespeicherten Daten drohen, ist bereits die vorbereitende Erfassung der Verkehrsdaten durch die Telekommunikationsunternehmen als Eingriff in Art. 10 Abs. 1 Var. 3 GG zu qualifizieren, von dem, wie auszuführen sein wird, auch ohne späteren staatlichen Zugriff auf die Daten erhebliche Gefahren ausgehen können.

Von einer Vorratsspeicherung betroffen wären daher alle Personen, die sich der Fernmeldetechnik bedienen. Eine größere Zahl betroffener Grundrechtsträger infolge einer Grundrechtsbeschränkung ist kaum denkbar. Es gäbe praktisch keine unbeeinträchtigte Telekommunikation mehr[472]. Der EU-Vorschlag ist zwar insoweit eingeschränkt, wie er nur auf solche Kommunikationsvorgänge Anwendung finden soll, die über öffentliche Kommunikationsnetze oder öffentliche Kommunikationsdienste abgewickelt werden (Art. 1 Abs. 1 RSV-E), während Kommunikationsvorgänge, die beispielsweise über Firmennetzwerke oder Nebenstellenanlagen abgewickelt werden, nicht erfasst sein sollen. Diese Einschränkung kann im Rahmen des Art. 10 Abs. 1 Var. 3 GG aber nicht von großem Gewicht sein, weil die Betroffenen regelmäßig keine Wahl zwischen dem Einsatz öffentlicher und privater Kommunikationsnetze haben.

Als weiteres Kriterium für die Verhältnismäßigkeitsprüfung fragt das Bundesverfassungsgericht nach der Identifizierbarkeit der Betroffenen. Werden Daten anonym erhoben, so ist der Eingriff nämlich von geringerem Gewicht. Entsprechend dem

[472] So auch Bäumler, Helmut, zitiert bei Wagner, Marita: Intimsphäre - lückenlos überwacht? Telepolis, Heise-Verlag, 28.06.2002, www.heise.de/tp/deutsch/inhalt/te/12813/1.html.

Zweck einer Vorratsspeicherung müssen die gespeicherten Telekommunikationsdaten jedoch in jedem Fall personenbezogen sein, um der Gefahrenabwehr oder Strafverfolgung förderlich sein zu können. Bei der gewöhnlichen Telekommunikationsnutzung besteht ein Personenbezug regelmäßig insoweit, als sich der Inhaber des genutzten Telekommunikationsanschlusses anhand von Auskünften des jeweiligen Telekommunikationsunternehmens feststellen lässt. Zwar gibt es vielfältige Möglichkeiten der anonymen Telekommunikation, welche die Herstellung eines Personenbezugs verhindern können und deren Einsatz sich für Kriminelle lohnen mag. Dem Normalbürger ist die ausschließliche Nutzung anonymer Formen von Telekommunikation aber wegen des damit verbundenen Aufwands auf Dauer nicht möglich oder jedenfalls unzumutbar. Die Möglichkeiten anonymer Telekommunikation bewirken daher nur eine geringfügige Minderung der Eingriffsintensität einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten.

Für die Verhältnismäßigkeit einer Grundrechtsbeschränkung sind weiterhin die Voraussetzungen, unter denen ein Eingriff zulässig ist, von Bedeutung. Je niedriger die Eingriffsschwelle, desto höher ist die Intensität des Eingriffs. Im vorliegenden Zusammenhang ist bereits die staatlich angeordnete Speicherung oder Aufbewahrung von Verkehrsdaten durch Telekommunikationsunternehmen als Eingriff in Art. 10 Abs. 1 Var. 3 GG anzusehen, soweit sie nicht für Zwecke der Vertragsabwicklung erforderlich ist. Für diesen Eingriff sind im Rahmen der Pläne zur Einführung einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten keine Voraussetzungen vorgesehen. Vielmehr sollen unterschiedslos und unabhängig vom Bestehen eines Verdachts Verkehrsdaten aller Nutzer von Kommunikationsnetzen gespeichert werden. Fast durchgängig betrifft der Eingriff dabei Personen, die sich nichts zuschulden kommen lassen haben. Der Eingriff könnte daher kaum schwerwiegender sein.

(ee) Gefahrennähe

Maßnahmen wie eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten, die bereits im Vorfeld einer konkreten Gefahr oder eines Verdachts wegen einer Straftat getroffen werden, werden als Vorfeldmaßnahmen bezeichnet. In der Sache handelt es sich um Eingriffe in die Grundrechte von Personen, die

nicht aufgrund bestimmter Anhaltspunkte verdächtig sind, Rechtsgüter zu gefährden oder eine Straftat begangen zu haben. Letztlich geht es also um verdachtsunabhängige Eingriffe.

Dass allein der Rechtsgüterschutz Grundrechtseingriffe legitimieren kann, wurde bereits ausgeführt. Dass ein Eingriff potenziell geeignet ist, Rechtsgüter zu schützen, kann ihn aber nicht in jedem Fall legitimieren. Ansonsten wäre zur Aufdeckung von Gefahren und Straftaten eine allgemeine Überwachung und Kontrolle der Bürger zulässig und die Grundrechte obsolet. Das Bundesverwaltungsgericht formuliert diesen Gedanken in einer Entscheidung auf dem Gebiet des Strafprozessrechts wie folgt: „Ausgangspunkt hat die Feststellung zu sein, daß nach dem Menschenbild des Grundgesetzes die Polizeibehörde nicht jedermann als potenziellen Rechtsbrecher betrachten und auch nicht jeden, der sich irgendwie verdächtig gemacht hat (‚aufgefallen ist') oder bei der Polizei angezeigt worden ist, ohne weiteres ‚erkennungsdienstlich behandeln' darf. Eine derart weitgehende Registrierung der Bürger aus dem Bestreben nach möglichst großer Effektivität der Polizeigewalt und Erleichterung der polizeilichen Überwachung der Bevölkerung widerspräche den Prinzipien des freiheitlichen Rechtsstaates."[473]

Gerade Vorfeldmaßnahmen sind daher nicht uneingeschränkt zulässig[474]. Der grundsätzliche Freiheitsanspruch des Einzelnen verlangt, dass der Einzelne von solchen Eingriffen verschont bleibt, die nicht durch eine hinreichende Beziehung oder Nähe zwischen ihm und einer Gefahr legitimiert sind[475]. Ob der insoweit erforderliche „Zurechnungszusammenhang"[476] gegeben ist, ist im Wege einer Abwägung der einschlägigen Interessen zu entscheiden. Letztlich handelt es sich um nichts anderes als die Prüfung der Verhältnismäßigkeit im engeren Sinne. Im Rahmen der Verhältnismäßigkeitsprüfung ist also die Gefahrennähe der betroffenen Grund-

---

473 BVerwGE 26, 169 (170 f.); vgl. dazu Hohmann-Schwan, Freiheitssicherung durch Datenschutz, 276 (298): „Dies gilt selbstverständlich nicht nur für die Aufbewahrung erkennungsdienstlicher Unterlagen, sondern auch für die Speicherung aller anderen personenbezogenen Daten"; ähnlich wie das BVerwG die abweichende Meinung in BVerfGE 109, 279 (391).

474 SächsVerfGH, DuD 1996, 429 (436): informationelle Vorfeldmaßnahmen seien nur ausnahmsweise zulässig; Hohmann-Schwan, Freiheitssicherung durch Datenschutz, 276 (300): Vorfeldbefugnisse seien nur punktuell und in besonderen Gefährdungslagen zulässig.

475 Für gesetzliche Eingriffe auf dem Gebiet des Polizeirechts MVVerfG, LKV 2000, 149 (153); VG Trier, MMR 2002, 698 (699); vgl. auch Lisken, NVwZ 2002, 513 (515). Für das Gebiet der Straftatenverhütung vgl. BVerfG, NJW 2004, 2213 (2216), wonach das „Risiko einer Fehlprognose" „hinnehmbar" erscheinen müsse. Ähnliche Kriterien leitet Waechter, DÖV 1999, 138 (145) aus dem Gesichtspunkt der Indienstnahme Privater zu öffentlichen Zwecken ab, die nur bei deren besonderer Sachnähe zulässig sei.

476 Für gesetzliche Eingriffe auf dem Gebiet des Polizeirechts MVVerfG, LKV 2000, 149 (153); VG Trier, MMR 2002, 698 (699).

rechtsträger zu berücksichtigen, so dass im vorliegenden Zusammenhang fraglich ist, welche Nähe zwischen den von einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten betroffenen Personen und den Gefahren, denen mit Hilfe der Vorratsspeicherung begegnet werden soll, besteht.

Wie gezeigt, kann man diese Gefahren in zwei Gruppen einteilen, nämlich in Gefahren, die aus der rechtswidrigen Nutzung von Telekommunikationsnetzen resultieren einerseits und in sonstige Gefahren, denen mit Hilfe einer Überwachung der Telekommunikation begegnet werden kann, andererseits. Fraglich ist zunächst, welche Nähe zwischen den von einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten betroffenen Personen und den Gefahren infolge von Netzkriminalität besteht.

Eine hinreichende Gefahrennähe liegt grundsätzlich dann vor, wenn eine Person aufgrund konkreter Umstände im Einzelfall im Verdacht steht, Rechtsgüter zu verletzen oder eine strafbare Handlung begangen zu haben[477]. Allgemeines Erfahrungswissen und Vermutungen genügen zur Begründung eines Verdachts nicht[478]. Dementsprechend hat das Bundesverwaltungsgericht in der oben zitierten Entscheidung geurteilt, dass angesichts des Menschenbildes des Grundgesetzes erkennungsdienstliche Unterlagen nur von Beschuldigten angefertigt und aufbewahrt werden dürfen und auch nur von solchen Beschuldigten, bei denen „nach der konkreten Sachlage [...] Anhaltspunkte dafür vor[liegen], daß die erkennungsdienstlich behandelte Person zukünftig strafrechtlich in Erscheinung treten [wird]"[479]. Demnach genügt es beispielsweise nicht, wenn sich die Polizeibehörden auf die generelle Wiedereinlieferungsquote in den Strafvollzug berufen, selbst wenn diese mit 50%[480] außerordentlich hoch liegt.

In die gleiche Richtung geht eine Entscheidung des Bundesverfassungsgerichts über einen Fall, in dem zur Aufklärung einer Straftat angeordnet worden war, dass allen männlichen Porschefahrern mit Münchener Kennzeichen eine Blutprobe zu ent-

477 Vgl. etwa SächsVerfGH, DuD 1996, 429 (437).

478 SächsVerfGH, DuD 1996, 429 (437).

479 BVerwGE 26, 169 (171); vgl. dazu Hohmann-Schwan, Freiheitssicherung durch Datenschutz, 276 (298): „Dies gilt selbstverständlich nicht nur für die Aufbewahrung erkennungsdienstlicher Unterlagen, sondern auch für die Speicherung aller anderen personenbezogenen Daten."

480 Kunz, Kriminologie, § 31, Rn. 40.

nehmen sei, um die Proben mit am Tatort gefundenen Spuren vergleichen zu können. Diese Vorgehensweise sah das Gericht trotz des großen Adressatenkreises als verhältnismäßig an, führte aber aus, die Grenze der Zumutbarkeit sei überschritten, wenn die Ermittlungsmaßnahme gegen so viele Personen angeordnet werde, dass ein konkreter Tatverdacht im Sinne des § 152 Abs. 2 StPO gegen die von der Anordnung Betroffenen nicht mehr bestehe[481]. Sobald jemand also nicht aufgrund besonderer Merkmale verdächtiger ist als sonstige Personen, hat er Eingriffe grundsätzlich nicht hinzunehmen. Die bloße allgemeine Möglichkeit, dass Daten einmal zu Zwecken der Strafverfolgung oder der Gefahrenabwehr benötigt werden könnten, begründet danach grundsätzlich nicht die von Verfassungs wegen zur Rechtfertigung von Eingriffen erforderliche Gefahrennähe.

Auch für den Zugriff auf Verkehrsdaten zu Strafverfolgungszwecken hat das Bundesverfassungsgericht in einem neueren Urteil einen konkreten Tatverdacht gegen die betroffene Person oder eine hinreichend sichere Tatsachenbasis für die Annahme, dass die Person als Nachrichtenmittler für einen Straftäter tätig wird, gefordert[482]. Das Urteil betraf zwar nicht die generelle Vorratsspeicherung von Verkehrsdaten, sondern die Übermittlung bestimmter Verkehrsdaten an Strafverfolgungsbehörden im Einzelfall. Das Gericht spricht in diesem Zusammenhang aber allgemein von der „Erfassung der Verbindungsdaten"[483] und stellt ausdrücklich fest: „Voraussetzung der Erhebung von Verbindungsdaten ist ein konkreter Tatverdacht."[484] Dies spricht für die Annahme, dass die Verdachtsschwelle für jede dem Staat als Eingriff zuzurechnende Erfassung und Speicherung von Verkehrsdaten gelten soll.

Eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten würde verdachtsunabhängig erfolgen, so dass sich eine Gefahrennähe der Betroffenen nicht über einen konkreten Verdacht gegen sie herleiten lässt. Allerdings hat der Gesetzgeber in bestimmten Bereichen schon bisher zu Vorfeldeingriffen ermächtigt. Dies gilt etwa für die Einrichtung des Bundeszentralregisters, die Daten über Straftäter speichert. Immerhin setzt eine Eintragung in dieses Register, ebenso wie die meisten anderen strafprozessualen Eingriffe, voraus, dass gegen den Betroffenen zu ei-

481 BVerfG JZ 1996, 1175 (1176).
482 BVerfGE 107, 299 (322).
483 BVerfGE 107, 299 (321).
484 BVerfGE 107, 299 (322).

nem früheren Zeitpunkt einmal ein Tatverdacht vorgelegen hat. Diese Voraussetzung ist bei einer generellen Verkehrsdatenspeicherung nicht gegeben, so dass sich auch hieraus keine Gefahrennähe herleiten lässt.

Weiterhin können diejenigen Personen, die eine besondere Gefahrenquelle in ihrer Obhut haben, besonderen Kontrollen unterworfen sein, etwa Kraftfahrzeugführer (§ 36 Abs. 5 StVO) oder Betreiber emittierender Anlagen (§ 52 Abs. 2 BImSchG). Noch einen Schritt weiter geht der Gesetzgeber, wenn er Personen allein schon deshalb Kontrollen unterwirft, weil sie sich an Orten aufhalten, an denen typischerweise Gefahren auftauchen sollen, etwa an Grenzen (§ 2 BGSG; vgl. auch die Landespolizeigesetze). Darüber hinaus muss der Bürger an allen öffentlichen Orten mit Identitätskontrollstellen rechnen, wenn dies zur Verfolgung von Mitgliedern einer terroristischen Vereinigung oder in Fällen schweren Raubes erforderlich ist (§ 111 StPO). Auch eine Inanspruchnahme Unbeteiligter zur Gefahrenabwehr ist nach den Landespolizeigesetzen in Ausnahmefällen zulässig („polizeilicher Notstand").

Unabhängig von der Frage, inwieweit diese Befugnisse jeweils mit der Verfassung vereinbar sind, ist jedenfalls festzustellen, dass eine allgemeine Vorratsspeicherung von Telekommunikations-Verkehrsdaten selbst im Vergleich zu diesen Befugnissen eine gänzlich neue Qualität hätte[485]. Bisher sind Vorfeldeingriffe nur punktuell und in besonderen Gefährdungslagen zulässig[486]. Bei der generellen Speicherung von Verkehrsdaten aber geht es um eine umfassende und generelle Überwachung bisher ungekannten Ausmaßes. Weder ist der Nutzer von Telekommunikationsdiensten für eine Gefahrenquelle verantwortlich, noch hält er sich an einem besonders gefährlichen Ort auf, noch wird er ausschließlich hinsichtlich konkreter, in der Vergangenheit vermutlich begangener Straftaten kontrolliert, noch besteht im Einzelfall ein polizeilicher Notstand. Der einzige Anknüpfungspunkt besteht in der Benutzung von Telekommunikationsnetzen.

Als Vergleichsfall kommt weiterhin das Waffenrecht in Betracht. Auf diesem Gebiet hat der Gesetzgeber angenommen, dass der Besitz von Waffen eine abstrakte Gefahr von solcher Art und von solchem Ausmaß begründet, dass ein weitgehendes Verbot und im Übrigen eine strenge Überwachung des Waffenbesitzes gerechtfer-

485 Eckhardt, CR 2002, 770 (774).

tigt ist. Im Unterschied zu Telekommunikationsnetzen ist allerdings erstens zu beachten, dass Waffen höchstrangige Rechtsgüter, nämlich Leib und Leben von Personen, gefährden. Außerdem werden diese Rechtsgüter durch den Einsatz von Waffen unmittelbar, also nicht erst in Verbindung mit anderen Faktoren, gefährdet. Ein weiterer Unterschied im Rahmen der grundrechtlich gebotenen Abwägung liegt in dem unterschiedlichen gesellschaftlichen Nutzen der Werkzeuge. Während Waffen nur im Einzelfall, etwa zur Selbstverteidigung oder zur Jagd, nützlich sein können, ihr weitgehendes Fehlen aber auch nicht zu untragbaren Nachteilen führt, baut unsere Gesellschaft immer mehr auf Telekommunikationsnetzen auf. Diese entfalten daher einen großen Nutzen, sowohl materiell-wirtschaftlicher Art wie auch ideell-politischer Art, wenn beispielsweise das Internet zur verstärkten Ausübung von Grundrechten genutzt wird. Die Wertungen des Waffenrechts lassen sich auf das Gebiet der Telekommunikation daher nicht übertragen.

In den Begründungen beider Vorschläge des Bundesrats zur Einführung einer generellen Telekommunikationsdatenspeicherung wird ausgeführt, eine Pflicht zur Speicherung von Daten zu staatlichen Zwecken sei dem geltenden Recht nicht fremd, wie das Geldwäschegesetz (GwG) zeige[487]. Das Geldwäschegesetz[488] sieht vor, dass Kreditinstitute, Versicherungen und gewisse andere Stellen fremde Vermögensangelegenheiten erst nach Identifizierung des Kunden anhand eines amtlichen Ausweises wahrnehmen dürfen (§§ 2-4 und 6 GwG), selbst wenn eine Identifizierung für die Durchführung der Geschäfte nicht erforderlich ist. Im Unterschied zu einer Vorratsspeicherung von Telekommunikations-Verkehrsdaten betrifft die Aufbewahrungspflicht nach dem Geldwäschegesetz allerdings nur die Personalien der Kunden, nicht die einzelnen von ihnen vorgenommenen Transaktionen. Daten über die einzelnen Transaktionen mögen zwar nach anderen Vorschriften aufzubewahren sein. Anders als Telekommunikationsunternehmen sind die aufbewahrungspflichtigen Personen im Finanzbereich aber nicht verpflichtet, den Strafverfolgungs- und Gefahrenabwehrbehörden einschließlich der Nachrichtendienste Auskünfte über ihre Aufzeichnungen zu erteilen. Hierin liegt der entscheidende Unterschied zu Telekommunikations-Verkehrsdaten. Auch auf die nach dem Geldwäschegesetz

---

486 Hohmann-Schwan, Freiheitssicherung durch Datenschutz, 276 (300).

487 Beschluss des Bundesrates vom 31.05.2002, BR-Drs. 275/02, 25; Beschluss des Bundesrates vom 19.12.2003, BR-Drs. 755/03, 34.

488 Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten vom 25.10.1993 (BGBl. I 1993, 1770), zuletzt geändert durch Art. 1 des Gesetzes vom 08.08.2002 (BGBl I 2002, 3105).

aufzuzeichnenden Personalien dürfen nur sehr eingeschränkt weitergegeben und verwendet werden (§ 10 GwG), insbesondere zur Verfolgung von Geldwäschedelikten. Aus den genannten Gründen ist eine Vorratsspeicherung von Telekommunikations-Verkehrsdaten vielfach eingriffsintensiver als das Geldwäschegesetz.

Eine weitgehende Überwachung auf dem Gebiet der Telekommunikation erlaubt das G10[489], das in seinem § 5 zu einer anlassunabhängigen („strategischen") Überwachung internationaler Telekommunikationsbeziehungen zur Abwehr schwerster Gefahren ermächtigt. Zwar erlaubt das G10 auch die Kenntnisnahme von Kommunikationsinhalten, während eine Verkehrsdatenspeicherung auf die Kommunikationsumstände beschränkt ist. Jene Beschränkung verhindert aber lediglich, dass eine generelle Aufhebung des Fernmeldegeheimnisses zu besorgen ist. Ansonsten sind Telekommunikations-Verkehrsdaten nicht generell weniger schutzwürdig als Kommunikationsinhalte[490], so dass darin kein maßgeblicher Unterschied zu § 5 G10 zu sehen ist.

Das Bundesverfassungsgericht hat eine globale und pauschale Überwachung selbst zur Abwehr größter Gefahren ausdrücklich als verfassungswidrig bezeichnet[491] und damit eine „flächendeckende Erfassung [...] des [...] Fernmeldeverkehrs"[492] gemeint. Weil eine Vorratsspeicherung grundsätzlich jeglichen Telekommunikationsverkehr einer Überwachung unterwerfen würde, könnte sie als eine solche „globale und pauschale Überwachung" des Telekommunikationsverkehrs angesehen werden. In der strategischen Überwachung nach dem G10 hat das Bundesverfassungsgericht nur deswegen keine solche Globalüberwachung gesehen, weil nur der internationale Fernmeldeverkehr betroffen sei, es tatsächlich nur selten zu einer Erfassung komme, der Satelliten-Downlink nicht immer erfasst würde, nur die Überwachung bestimmter Fernmeldeverkehrsbeziehungen angeordnet würde und die Überwachung wegen begrenzter Kapazitäten faktisch beschränkt sei[493]. All diese Gesichtspunkte treffen auf die gegenwärtigen Vorhaben zur Einführung einer Vorratsspeicherung nicht zu, zumal es auf tatsächliche Begrenzungen – wie bereits

489 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses vom 26.06.2001 (BGBl I 2001, 1254, 2298), zuletzt geändert durch Art. 4 des Gesetzes vom 09.01.2002 (BGBl I 2002, 361).

490 Hierzu ausführlich die Seiten 178-184.

491 BVerfGE 313, 100 (376 und 383).

492 BVerfGE 313, 100 (377).

493 BVerfGE 313, 100 (377 f.).

gezeigt – ohnehin nicht ankommen kann. Eine beachtliche Begrenzung der Überwachung im Fall der Vorratsspeicherung lässt sich auch nicht durch Verweis auf die Möglichkeiten anonymer Telekommunikation konstruieren, weil die ausschließliche Nutzung anonymer Formen von Telekommunikation auf Dauer nicht möglich oder jedenfalls unzumutbar ist.

§ 5 G10 ist insoweit weniger belastend als eine generelle Vorratsspeicherung, als das Bundesverfassungsgericht festgestellt hat, dass ein „verfassungswidriger Missbrauch" der Befugnis vorliege, wenn sie „zur Einzelüberwachung von Personen oder zur Sammlung von Nachrichten über [...] Gefahren für die innere Sicherheit" verwendet würde[494]. Auch zur Strafverfolgung darf dieses Instrument nicht eingesetzt werden. Das Mittel der strategischen Überwachung darf vielmehr nur ausnahmsweise zur Aufrechterhaltung der Sicherheit der Bundesrepublik Deutschland gegenüber Gefahren aus dem Ausland, die nicht vornehmlich personenbezogen sind, eingesetzt werden[495]. Nur dieser besondere Zweck rechtfertigt es, dass die Eingriffsvoraussetzungen im G10 anders bestimmt werden als es im Polizei- oder Strafprozessrecht verfassungsrechtlich zulässig ist[496]. Die generelle Aufbewahrung von Verkehrsdaten ist demgegenüber auf ein nachträgliches Einschreiten in Einzelfällen zugeschnitten. Ansonsten wäre, wie im Bereich des § 5 G10, lediglich eine einmalige Prüfung der Daten erforderlich und nicht auch deren Aufbewahrung. Auch die Vorschläge des Bundesrats zielen, wie schon die Begründung zum ErmittlungsG-Entwurf zeigt, vornehmlich auf eine verbesserte Strafverfolgung. Der EU-Vorschlag ist von vornherein auf diesen Bereich beschränkt. In Anbetracht der weiten Verwendungsmöglichkeiten greift eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten daher in erheblich höherem Maße in die Grundrechte ein als § 5 G10.

Darüber hinaus sind selbst die „strategischen" Kontrollmaßnahmen nach dem G10 nicht ebenso pauschal und allumfassend wie es eine Vorratsspeicherung wäre. Sie sind auf den internationalen Telekommunikationsverkehr beschränkt und werden auch nur im Einzelfall angeordnet, betreffen also nur den Telekommunikationsverkehr mit einzelnen Ländern. Außerdem ist ein Verfahren unter Einschaltung von Kon-

494 BVerfGE 67, 157 (180 f.).
495 BVerfGE 100, 313 (383).
496 BVerfGE 100, 313 (383).

trollorganen vorgesehen, das die Eignung der Maßnahme fördern kann[497]. Voraussetzung einer Anordnung ist die begründete (vgl. § 9 Abs. 3 G10) Annahme, dass durch die Maßnahme Kenntnisse erlangt werden können, die zur Abwehr schwerster Gefahren für die Sicherheit Deutschlands erforderlich sind. Demnach besteht bei Maßnahmen nach § 5 G10 ein erheblich höherer Eignungsgrad als bei einer generellen Vorratsspeicherung sämtlicher Verkehrsdaten.

Im Ergebnis ist festzuhalten, dass die einzige Verbindung zwischen den von einer Vorratsspeicherung betroffenen Personen und den Gefahren, die aus der Nutzung von Telekommunikationsnetzen zu rechtswidrigen Zwecken erwachsen, darin besteht, dass das gleiche Medium benutzt wird. Es liegen auch nicht die Voraussetzungen vor, unter denen eine allgemeine Telekommunikationsüberwachung bisher für zulässig erachtet worden ist.

Während Telekommunikationsnetze dort, wo sie als Werkzeug zur Begehung von Straftaten genutzt werden, noch eine eigenständige Rechtsgutsgefahr darstellen könnten, ist dies im Übrigen von vornherein ausgeschlossen. Gleichwohl greifen Eingriffsbehörden oftmals auf die Umstände auch von solchen Telekommunikationsvorgängen zu, die in keinem Zusammenhang mit der Begehung von Straftaten standen, sondern der alltäglichen Kommunikation dienten. Beispielsweise kann die Standortkennung des Mobiltelefons eines Straftäters von Strafverfolgungsbehörden abgefragt werden, um dessen Aufenthaltsort zu ermitteln, selbst wenn der Straftäter sein Mobiltelefon zu keiner Zeit zu rechtswidrigen Zwecken genutzt hat. Die Beziehung zwischen dem durchschnittlichen Telekommunikationsnutzer und den Gefahren, die einzelne Telekommunikationsnutzer allgemein verursachen, ist noch entfernter als in dem Bereich, in dem die Eigenschaften der Telekommunikationsnetze, von denen alle Telekommunikationsbenutzer profitieren, zur Begehung von Straftaten ausgenutzt werden.

Aufschlussreich für die Bemessung der Gefahrennähe ist auch das zahlenmäßige Verhältnis der Gesamtheit aller Telekommunikationsvorgänge zu der Anzahl von Telekommunikationsvorgängen, welche später zu Gefahrenabwehr- oder Strafverfolgungszwecken nachvollzogen werden müssen. Die Wahrscheinlichkeit, dass ein be-

497 BVerfGE 100, 313 (373).

liebiger Telekommunikationsvorgang zu einem späteren Zeitpunkt einmal zu Gefahrenabwehr- oder Strafverfolgungszwecken nachvollzogen werden muss, ist angesichts der Vielzahl an Telekommunikationsvorgängen als verschwindend gering anzusehen[498]. Im Jahr 2002 wurden in Deutschland täglich 216 Millionen Telefonverbindungen hergestellt[499], im gesamten Jahr also etwa 79 Milliarden Verbindungen. Die Zahl von Telekommunikations-Verkehrsdatensätzen, die jährlich an Gefahrenabwehr- oder Strafverfolgungsbehörden übermittelt werden, ist zwar nicht bekannt. Es wird sich aber allenfalls um einige tausend Datensätze handeln. Die Wahrscheinlichkeit, dass eine Telefonverbindung zu einem späteren Zeitpunkt einmal nachvollzogen werden muss, läge damit bei einer Größenordnung von 0,00001%. Im Internetbereich wird diese Zahl noch erheblich geringer sein, weil hier ein Vielfaches an Verkehrsdaten anfällt, Internet-Verkehrsdaten von Gefahrenabwehr- oder Strafverfolgungsbehörden aber vergleichsweise selten angefordert werden. Berechnungen des Internet-Access-Providers T-Online haben ergeben, dass derzeit nur 0,0004% der insgesamt dort anfallenden Verkehrsdaten von den Strafverfolgungsbehörden angefordert werden[500].

Angesichts dieser geringen Größenordnung ist fraglich, ob auf dem Gebiet der Telekommunikation die Wahrscheinlichkeit, dass ein beliebiger Kommunikationsvorgang zu einem späteren Zeitpunkt einmal zu Gefahrenabwehr- oder Strafverfolgungszwecken nachvollzogen werden muss, größer ist als im Bereich der traditionellen Kommunikation. Ob dies der Fall ist, ist empirisch noch nicht geprüft worden. Jedenfalls soweit Telekommunikation nicht im unmittelbaren Zusammenhang mit der Begehung von Straftaten erfolgt, ist kein Grund ersichtlich, warum Verkehrsdaten zu Gefahrenabwehr- oder Strafverfolgungszwecken nützlicher sein sollten als die Kenntnis der Umstände von Kommunikationsvorgängen außerhalb von Telekommunikationsnetzen. Während der Zugriff auf Verkehrsdaten bei Straftaten, die mittels Telekommunikationsnetzen begangen werden, oft das einzige Mittel zur Aufklärung der Tat sein wird, wird dies bei anderweitig begangenen Straftaten nur ausnahmsweise der Fall sein. In diesem Bereich stellen Verkehrsdaten eine Informati-

498 Dix, Alexander: Schriftliche Stellungnahme zur öffentlichen Anhörung am 09.02.2004 in Berlin zum Entwurf eines Telekommunikationsgesetzes (TKG), in Ausschussdrucksache 15(9)961, www.bundestag.de/gremien15/a09/004Anhoerungen/-TKG/materialeingeladene.
pdf, 217 (219).

499 BVerfGE 107, 299 (327).

500 Uhe/Herrmann, Überwachung im Internet (I), 161.

onsquelle wie jede andere dar. Dass sich nur Telekommunikations-Verkehrsdaten generell erfassen und speichern lassen und dass die finanziellen Kosten einer solchen Vorratsspeicherung begrenzt sind, erhöht den durchschnittlichen Nutzen dieser Daten nicht und ist daher unbeachtlich. Es ist sogar denkbar, dass Telekommunikations-Verkehrsdaten von geringerem Erkenntnisinteresse sind als die näheren Umstände sonstiger Kommunikation, weil Straftätern die Überwachbarkeit der Telekommunikationsnetze bekannt ist und sie die Nutzung dieses Mediums für ihre Zwecke aus diesem Grunde möglichst vermeiden werden.

Soweit Telekommunikationsnetze zur Begehung von Netzkriminalität im engeren Sinne genutzt werden, ist zu beachten, dass sich Angriffe auf Computersysteme auch ohne Telekommunikationsnutzung vornehmen lassen. Insbesondere Angriffe von Mitarbeitern eines Unternehmens, die besonders schadensträchtig sind, werden vermutlich meist mittels eines Computers des angegriffenen Unternehmens selbst vorgenommen, weil die Angreifer dadurch vermeiden können, dass aufgrund der Zwischenschaltung von Telekommunikationsnetzen Datenspuren entstehen, die sie verraten könnten. Es lässt sich daher ohne nähere Untersuchung nicht sagen, ob im Bereich der Telekommunikation die Wahrscheinlichkeit, dass ein beliebiger Computerbenutzungsvorgang zu einem späteren Zeitpunkt einmal zu Gefahrenabwehr- oder Strafverfolgungszwecken nachvollzogen werden muss, größer ist als im Bereich der unmittelbaren Computernutzung.

Im Bereich der Netzkriminalität im weiteren Sinne wird die Telekommunikation letztlich zum Zweck des Austauschs von Informationen zwischen Menschen eingesetzt. Hier ist also zu fragen, ob der durchschnittliche Kommunikationsvorgang auf dem Gebiet der Telekommunikation öfter der Begehung einer Straftat dient als außerhalb dieses Gebiets, etwa bei der unmittelbar menschlichen Kommunikation oder der Kommunikation per Post. Die verfügbaren Kriminalitätsstatistiken erlauben es leider nicht, Anzahl und Schädlichkeit von Straftaten, die menschliche Kommunikation voraussetzen, inner- und außerhalb von Telekommunikationsnetzen zu vergleichen. Damit ist auch auf diesem Gebiet ein Vergleich der Gefahrennähe nicht möglich.

Lässt man die tatsächlichen Unsicherheiten außer Acht und nimmt man an, dass die Kenntnis der Umstände eines durchschnittlichen Telekommunikationsvorgangs

für die Eingriffsbehörden nicht interessanter ist als die Kenntnis der Umstände sonstiger Kommunikationsvorgänge, so fragt es sich, ob schon die allgemeine Möglichkeit, dass Kommunikationsvorgänge zu einem späteren Zeitpunkt einmal von Eingriffsbehörden nachvollzogen werden müssen, deren generelle Aufzeichnung rechtfertigt. Gemessen an der nahezu unbegrenzten Anzahl von Gesprächen, Briefen und anderen Kommunikationsvorgängen liegt es auf der Hand, dass die Wahrscheinlichkeit, dass eine beliebiger Kommunikationsvorgang zu einem späteren Zeitpunkt einmal zu Gefahrenabwehr- oder Strafverfolgungszwecken nachvollzogen werden muss, verschwindend gering ist. Wollte man trotz dieser geringen Wahrscheinlichkeit eine hinreichende Nähe jedes Kommunizierenden, also im Grunde jedes Menschen, zur Begehung von Straftaten mittels menschlicher Kommunikation annehmen, dann wäre der Gesetzgeber zur Aufzeichnung der näheren Umstände jedes Informationsaustausches legitimiert, allein schon wegen der Tatsache des Informationsaustausches. Dies würde beispielsweise zum Aufbau eines allgemeinen Spitzelsystems berechtigen, wie es durch die Stasi organisiert wurde.

Fraglich ist, ob Derartiges mit dem Menschenbild des Grundgesetzes zu vereinbaren wäre. Das Bundesverfassungsgericht betont in ständiger Rechtsprechung, dass der Mensch ein gemeinschaftsbezogenes und gemeinschaftsgebundenes Wesen ist[501]. Er „ist eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit"[502]. Seiner besonderen Bedeutung entsprechend wird der Informationsaustausch auch durch das Grundgesetz besonders geschützt. So garantiert das Recht auf informationelle Selbstbestimmung den Schutz personenbezogener Informationen vor staatlichen Zugriffen. Das Gleiche gilt für Art. 10 GG. Art. 5 Abs. 1 und 2 GG gewährleistet die Meinungs-, Informations-, Presse- und Rundfunkfreiheit, deren Ausübung notwendig den Austausch von Informationen voraussetzt. Art. 4 Abs. 1 und 2 GG gewährleistet die ungestörte Religionsausübung, die oftmals in Gemeinschaft mit anderen erfolgt und dementsprechend auf einem Gedankenaustausch basiert. In der Tat lässt sich kaum ein Grundrecht denken, dessen Ausübung nicht einen Informationsaustausch erforderlich machen kann. Die Grundrechtsordnung des Grundgesetzes basiert darauf, dass die Grundrechte grundsätzlich ungestört von staatlichen Eingriffen ausgeübt werden kön-

501 St. Rspr. des BVerfG seit E 4, 7 (15).

502 BVerfGE 65, 1 (44).

nen[503]. Jedenfalls muss der Einzelne keine unzumutbaren Eingriffe in seine Freiheiten dulden[504]. Außerdem gewährleistet Art. 19 Abs. 2 GG einen unantastbaren Bereich der ungestörten Grundrechtsausübung.

Dieser Konzeption des Grundgesetzes würde es widersprechen, wenn man bereits in dem bloßen Austausch von Informationen eine abstrakte Gefahr sehen würde, die den Staat zu Eingriffen berechtigte. Dass ein Informationsaustausch in manchen Fällen konkrete Gefahren begründet oder erhöht, muss vielmehr dem Bereich des allgemeinen Lebensrisikos zugeordnet werden. Der Austausch von Informationen allgemein begründet daher für sich genommen noch keine hinreichende Gefahrennähe der Kommunizierenden, so dass eine Vorratsspeicherung der näheren Umstände beliebiger Kommunikationsvorgänge unzulässig wäre.
Angesichts dessen kann eine generelle Verkehrsdatenspeicherung nur dann gerechtfertigt sein, wenn die näheren Umstände der Telekommunikation für den Schutz von Rechtsgütern von größerer Relevanz sind als die Umstände sonstiger Kommunikation. Ob dies der Fall ist, ist – wie bereits ausgeführt – unbekannt.

(ff) Aussagekraft der Daten, die erhoben werden können, unter Berücksichtigung ihrer Nutzbarkeit und Verwendungsmöglichkeit; den Betroffenen drohende Nachteile nach Ausmaß und Wahrscheinlichkeit ihres Eintritts

Die vorliegenden Vorschläge zur Einführung einer Vorratsspeicherung sind vage, was die genaue Art der zu speichernden Daten angeht. Der Grund dafür wird darin zu sehen sein, dass Widerstände sowohl von Bürgern wie auch von der Wirtschaft zu erwarten sind, sobald diese klar vor Augen haben, was die Regelungen tatsächlich bedeuten. Es wird daher für politisch klüger erachtet, zunächst die generelle Befugnisnorm zu schaffen. Wenn es dann später um die konkrete Umsetzung geht und den Betroffenen die konkrete Bedeutung der Norm bewusst wird, ist es für sie schon zu spät, über das „Ob" der Regelung noch zu diskutieren. Diese „Scheibchentaktik" wurde im Bereich des § 88 TKG a.F. (jetzt § 110 TKG), der erst 2001 durch die TKÜV konkretisiert wurde, erfolgreich angewandt. Auch in EU-Ländern, in denen die Ein-

503 BVerfGE 65, 1 (44): „Grundrechte [...] als Ausdruck des allgemeinen Freiheitsanspruchs des Bürgers gegenüber dem Staat".
504 St. Rspr. des BVerfG; für Art. 10 GG vgl. nur BVerfGE 67, 157 (178); BVerfGE 100, 313 (391).

führung einer generellen Vorratsspeicherung von Verkehrsdaten geplant ist, ist auf diese Weise verfahren worden.

Dem RSV-Entwurf zufolge sollen insbesondere solche Telekommunikationsdaten gespeichert werden, welche die Identifizierung von Ursprung, Ziel, Zeit und Ort eines Informationsaustausches, des eingesetzten Kommunikationsgeräts (bei Mobiltelefonen etwa die IMEI) sowie des Kunden und des Benutzers des elektronischen Kommunikationsdienstes erlauben (Art. 2 Abs. 2 RSV-E). Der ErmittlungsG-Entwurf enthielt keine nähere Konkretisierung der zu speichernden Daten und umfasste daher potenziell alle zur Verfügung stehenden Telekommunikationsdaten. Die Stellungnahme des Bundesrats vom 19.12.2003 sieht vor, dass die Aufbewahrungspflicht für alle Verkehrsdaten gelten soll, die „erhoben worden sind"[505]. Dies umfasst alle zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung von Telekommunikationsdiensten notwenigen Verkehrsdaten (vgl. § 96 Abs. 1 Nr. 5 TKG).

Hinsichtlich der betroffenen Dienste schließt der RSV-Entwurf öffentliche Internetangebote ein (Art. 2 Abs. 3 Buchst. c RSV-E). Auch die Vorschläge des Bundesrats nehmen die Nutzung öffentlicher Internetangebote nicht aus.

Der RSV-Entwurf erstreckt sich weiterhin auch auf den Informationsaustausch zwischen einem nur empfangsbereiten Mobiltelefon und der Basisstation, so dass die Telekommunikationsunternehmen komplette Bewegungsprofile ihrer Kunden speichern müssten. Gleichermaßen stellt sich die Lage nach den Vorschlägen des Bundesrats dar. Die Tatsache, dass beide Vorschläge die Aufzeichnung von Bewegungsprofilen und die Aufzeichnung der Nutzung von Massenmedien über das Internet einschließen, erhöht ihre Eingriffsintensität erheblich.

Bei der Bemessung der Eingriffsintensität einer Vorratsspeicherung ist zudem der Vergleich mit bestehenden Eingriffsbefugnissen von Nutzen. Dieser ergibt zunächst, dass die Verarbeitung von Verkehrsdaten mit erheblich größeren Gefahren verbunden ist als die automatische Verarbeitung personenbezogener Daten generell; die allgemeinen Gefahren einer automatisierten Datenverarbeitung erhalten im

505 BR-Drs. 755/03, 33.

Bereich der Telekommunikationsnetze eine neue Dimension[506], denn hier besteht die Möglichkeit, Persönlichkeitsbilder mit einer noch nie da gewesenen Genauigkeit zu gewinnen. Das liegt zum einen daran, dass Daten über jede Telekommunikationsnutzung eines Teilnehmers anfallen, das Telekommunikationsverhalten einer Person also vollständig dokumentiert werden kann. In anderen Bereichen müsste ein solcher Datenberg erst aus unterschiedlichen Quellen zusammen getragen werden, etwa in dem aufwändigen Verfahren der Rasterfahndung. Eine weitere, besondere Gefahr auf dem Gebiet der Telekommunikation ergibt sich daraus, dass die Speicherung von Verkehrsdaten entweder schon in der Struktur der Systeme angelegt ist oder sich mit begrenztem Aufwand durchführen lässt. Nicht zuletzt sind Verkehrsdaten auch inhaltlich äußerst aussagekräftig und geben selbst über intime Details Auskunft, etwa im Bereich der Internet-Nutzung. Es lässt sich sagen, dass sich der Mensch nirgendwo im dem Maße, in all seinen Facetten und in so konstanter und aussagekräftiger Weise offenbart wie in den Telekommunikationsnetzen.

Vergleicht man weiterhin beispielsweise den Zugriff auf Mobiltelefon-Positionsdaten mit dem klassischen Mittel der Observation, so ergeben sich gravierende Unterschiede[507]: Standortdaten können auch für die Vergangenheit abgefragt werden, was eine Observation nicht leisten kann. Standortdaten können zeitlich lückenlos aufgezeichnet werden, was bei einer Observation nicht gewährleistet ist. Die Abfrage von Standortdaten bleibt dem Betroffenen – anders als eine Observation – mit Sicherheit verborgen. Schließlich ist der Zugriff auf Verkehrsdaten für die Behörden mit einem viel geringeren Einsatz von Personal und Kosten möglich als die Vornahme einer Observation, so dass Informationseingriffe tendenziell öfter stattfinden werden. Auch dieses Beispiel zeigt die erheblich höhere Eingriffsintensität einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten gegenüber bestehenden Eingriffsbefugnissen.

506 Zum Folgenden Gridl, Datenschutz in globalen Telekommunikationssystemen, 74 ff.

507 Schenke, AöR 125 (2000), 1 (28).

(i) Vergleich mit der Aussagekraft von Kommunikationsinhalten

Weit verbreitet ist die Behauptung, der staatliche Zugriff auf die näheren Umstände der Telekommunikation wiege weniger schwer als der Zugriff auf ihren Inhalt[508]. Gegen die Richtigkeit dieser meist ohne Begründung angeführten These, die an die Art des jeweiligen Datums anknüpft, spricht die Feststellung des Bundesverfassungsgerichts, dass bei der Bemessung der Intensität eines Informationseingriffs „nicht allein auf die Art der Angaben abgestellt werden [kann]. Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses' Datum mehr."[509]

Konkret liegt beispielsweise auf der Hand, dass die Kenntnisnahme des Inhalts eines belanglosen Telefonats mit dem Nachbarn weniger belastend ist als die Kenntnisnahme sämtlicher Positionsdaten eines Mobiltelefons, anhand derer sich ein Bewegungsprofil des Besitzers erstellen lässt. Verkehrsdaten sind also keineswegs zwangsläufig weniger aussagekräftig als Kommunikationsinhalte. Sie können es im Einzelfall sein, oft verhält es sich aber auch umgekehrt.

Wie bereits erwähnt, sind bei der Beurteilung der Intensität eines Informationseingriffs auch die Möglichkeiten der Verarbeitung oder Verknüpfung erlangter Daten zu berücksichtigen[510]. Kommunikationsinhalte – mit Ausnahme unverschlüsselter Textübertragungen wie E-Mail oder SMS – liegen regelmäßig nicht in maschinenlesbarer Form vor (z.B. akustische Gespräche, Telefaxe). In absehbarer Zukunft werden keine Computer zur Verfügung stehen, die ausreichend leistungsfähig sind, den Inhalt solcher Kommunikationsvorgänge automatisch zu analysieren oder eine Vielzahl von Kommunikationsvorgängen nach bestimmten Inhalten zu durchsuchen. Eine Auswertung wird vielmehr stets durch Menschen erfolgen müssen, so dass Inhalte be-

508 BVerfGE 107, 299 (322); BVerfGE 109, 279 (345); Bundesregierung in BT-Drs. 14/7008, 6 für Verbindungsdaten: „regelmäßig"; Bundesrat in BT-Drs. 14/7258, 1 für Verbindungsdaten: „bei weitem"; Thüringen in BR-Drs. 513/02, 3 für Mobilfunkstandortdaten; BGH-Ermittlungsrichter, MMR 1999, 99 (101) für Verbindungsdaten; Weichert, Bekämpfung von Internet-Kriminalität (I), Punkt 3: „regelmäßig"; Germann, 620: „deutlich".

509 BVerfGE 65, 1 (45).

510 BVerfGE 65, 1 (45).

reits aus diesem Grund nur punktuell erfasst werden können. Auch ist im Bereich der E-Mail-Kommunikation eine effektive, kostengünstige und einfache Verschlüsselung der Kommunikationsinhalte möglich[511], so dass eine staatliche Vorratsspeicherung insoweit nutzlos wäre. Selbst unverschlüsselte, maschinenlesbare Kommunikationsinhalte könnten wegen der unüberschaubaren Datenmengen kaum auf Vorrat gespeichert werden. Die Entlastung, welche die Ausnahme von Kommunikationsinhalten von einer Vorratsspeicherung bewirkt, darf daher nicht überschätzt werden[512].

Im Vergleich zu Inhaltsdaten sind die Verarbeitungsmöglichkeiten von Verkehrsdaten weit höher. Da Verkehrsdaten von vornherein als computerlesbare Datensätze gespeichert werden, eignen sie sich in hohem Maße zur Speicherung, Übermittlung und Verknüpfung mit anderen Datenbeständen. Sie können automatisch analysiert und auf bestimmte Suchmuster hin durchkämmt[513], nach bestimmten Kriterien geordnet und ausgewertet[514] werden. All diese Möglichkeiten bestehen bei Inhaltsdaten nicht, was für eine höhere Sensibilität von Verkehrsdaten spricht.

In vielen Fällen ist der Staat auch von vornherein oder jedenfalls zunächst nur an den Umständen eines Telekommunikationsvorgangs interessiert. Geht es etwa darum, heraus zu finden, von welchem Telefonanschluss aus zu einer bestimmten Zeit ein bestimmter anderer Anschluss angerufen wurde (beispielsweise in einem Erpressungsfall), dann müssen alle bei einem Telekommunikationsunternehmen gespeicherten Verbindungsdaten daraufhin durchgesehen werden, ob sie mit diesen Suchmerkmalen übereinstimmen. Was in den einzelnen Gesprächen gesagt wurde, ist den Behörden gleichgültig. Bei dieser Maßnahme geht es nicht um den Inhalt der Gespräche, so dass es falsch wäre, dem Eingriff geringes Gewicht zuzumessen, weil „nur" Verkehrsdaten betroffen sind. Der Eingriff hat vielmehr umgekehrt ein besonders großes Gewicht, da er die Daten einer Vielzahl unbeteiligter Personen betrifft.

---

511 BMI/BMJ, Sicherheitsbericht 2001, 200, wonach PGP-chiffrierte Daten derzeit mit unter Kostengesichtspunkten vertretbaren Mitteln nicht entschlüsselbar seien.

512 Weinem (Diplom-Informatiker beim Bundeskriminalamt), TK-Überwachung, 451 (453).

513 DSB-Konferenz, Freie Telekommunikation (I); Omega Foundation, Report (I) mit der Forderung, den Einsatz solcher Techniken denselben Tatbestandsvoraussetzungen zu unterwerfen wie das Abfangen von Telekommunikationsinhalten.

514 Gridl, Datenschutz in globalen Telekommunikationssystemen, 61.

Während die Eingriffsbehörden häufig nur oder jedenfalls zunächst nur an Verkehrsdaten interessiert sind, kommt der umgekehrte Fall praktisch nicht vor. Selbst im Fall der strategischen Telekommunikationsüberwachung durch den BND ist ein Zugriff auf Verkehrsdaten erforderlich, um festzustellen, mit welchem Land kommuniziert wird. Die strategische Überwachung nach dem G10 kann nämlich nur für bestimmte Länder angeordnet werden. Aus diesem Grund ist ein Abhören von Kommunikationsinhalten praktisch bedeutungslos, wenn nicht zugleich festgestellt werden kann, wer an dem Kommunikationsvorgang beteiligt ist. Die Aussage, Verkehrsdaten seien für die Arbeit der Sicherheitsbehörden ebenso wichtig wie Kommunikationsinhalte[515], ist daher eine Untertreibung. An der fehlenden praktischen Nutzbarkeit von Kommunikationsinhalten ohne die zugehörigen Verkehrsdaten zeigt sich die essenzielle Bedeutung von Telekommunikations-Verkehrsdaten.

Hinzu kommt, dass die Unterscheidung von Inhalts- und Verkehrsdaten besonders im Internetbereich unklar ist[516]. Im Bereich öffentlich zugänglicher Internet-Inhalte erlaubt es die Kenntnis der Verkehrsdaten (URLs) etwa regelmäßig, den Inhalt der Kommunikation selbst nachzuvollziehen[517]. Dazu genügt es, die URL in einen Internet-Browser einzugeben. Dementsprechend ist eine niedrigere Eingriffsschwelle als für den unmittelbaren Zugriff auf Kommunikationsinhalte nicht gerechtfertigt[518]. Teilweise werden WWW-Nutzungsdaten – die als Kommunikationsumstände an sich zu den Verkehrsdaten zu zählen sind[519] – schon dem Kommunikationsinhalt zugerechnet[520].

---

515 Weinem (Diplom-Informatiker beim Bundeskriminalamt), TK-Überwachung, 451 (453).

516 Kommission, Discussion Paper for Expert's Meeting on Retention of Traffic Data (I); Artikel-29-Gruppe der EU, Privatsphäre im Internet (I), 55.

517 Schaar, Cybercrime und Bürgerrechte (I), 11; Queen Mary (University of London), Studie über Netzkriminalität (I); Kommission, Discussion Paper for Expert's Meeting on Retention of Traffic Data (I); Weßlau, ZStW 113 (2001), 681 (703); Weichert, Thilo: BigBrotherAward 2002 in der Kategorie „Kommunikation", 25.10.2002, www.big-brother-award.de/2002/.comm. Laut EPIC/PI, Privacy and Human Rights 2002 (I), Teil I, 58 und Queen Mary (University of London), Studie über Netzkriminalität (I) sind in Großbritannien für den Zugriff auf URLs stärkere Schutzvorkehrungen vorgesehen als für den Zugriff auf sonstige Verkehrsdaten, soweit nicht nur auf den Namen des Servers zugegriffen wird.

518 Artikel-29-Gruppe der EU, Privatsphäre im Internet (I), 55.

519 Schaar, Retention (I), 1.

520 Schaar, Datenschutz im Internet, Rn. 143; EPIC/PI, Privacy and Human Rights 2002 (I), Teil I, 57: dem Kommunikationsinhalt ähnlicher als Verbindungsdaten; laut Dänemark in MDG, EU-Questionnaire (I), 13 f. unterliegt dort der Zugriff auf Verkehrsdaten denselben Voraussetzungen wie der Zugriff auf Inhaltsdaten; Gridl, Datenschutz in globalen Telekommunikationssystemen, 74: „Aufgrund der verschwimmenden Grenzen zwischen diesen beiden Daten im Internet und in Online-Netzen kann die klassische Unterscheidung zwischen dem Inhalt einer Kommunikation und der Information darüber, dass eine solche Kommunikation stattgefunden hat, nicht mehr aufrecht erhalten werden."

Das Verschwimmen der Grenzen von Verkehrs- und Inhaltsdaten ist nicht auf das Internet begrenzt. Auch wo die Telefontastatur zur Eingabe von Kontonummern und anderen Inhaltsdaten genutzt wird, ist eine technische Abgrenzung zur Eingabe von Telefonnummern nicht möglich[521]. Dabei erlaubt es die Kenntnis der „Verkehrsdaten", die bei der Kommunikation mit dem Telefoncomputer einer Bank anfallen („Telefonbanking"), den gesamten Kommunikationsvorgang nachzuvollziehen: Werden die aufgezeichneten Ziffern im Rahmen eines Anrufs des Telefoncomputers durch die Polizei erneut gewählt, dann kann ihre Bedeutung anhand der Ansagen des Telefoncomputers ohne Weiteres nachvollzogen werden. Auch insoweit fehlt jeder Unterschied zu einer direkten Aufzeichnung des Inhalts des Gesprächs, so dass unterschiedliche Eingriffsschwellen nicht gerechtfertigt sind.

Besonders im Bereich der neuen Technologien können Verkehrsdaten aussagekräftiger sein als die Kenntnis von Inhalten. Während Verkehrsdaten traditionell allenfalls im Bereich der Individualkommunikation zur Verfügung standen und dort nur besagen, ob, wann und wie oft zwischen welchen Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist[522], hat die Feststellung der jeweiligen Position eines Mobiltelefons oder der von einer Person abgerufenen Internet-Inhalte eine völlig neue Qualität[523]. Schon quantitativ entstehen durch ein eingeschaltetes Mobiltelefon oder während einer Internetsitzung laufend neue Verkehrsdaten, während im Bereich der Sprachtelefonie nur ein Datensatz pro Kommunikationsvorgang anfällt. Gerade im Bereich der neuen Netze fällt eine so große Menge an Verkehrsdaten an, dass die Bildung umfassender Persönlichkeits- und Verhaltensprofile möglich ist[524].

In geringerem Maße ist dies auch im Bereich der Individualkommunikation der Fall. Zwar bilden Verbindungsdaten in diesem Bereich insgesamt gesehen nicht einen ebenso großen Bereich des täglichen Lebens ab. Im Einzelfall kann die Kenntnis der Tatsache, ob, wann und wie oft zwischen bestimmten Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist, für den Betroffenen aber belastender sein als die Kenntnis von Internet-Verkehrsdaten oder

---

521 Queen Mary (University of London), Studie über Netzkriminalität (I).

522 Vgl. BVerfGE 100, 313 (358).

523 Schaar, Retention (I), 2 für Positionsdaten; Gridl, Datenschutz in globalen Telekommunikationssystemen, 74: „neue Dimension"; Meade, Retention of Communications Traffic Data (I): „far more personal and revealing".

524 Gridl, Datenschutz in globalen Telekommunikationssystemen, 61.

Gesprächsinhalten. Dies gilt nicht nur für das Verbindungsdatum der Position eines Mobiltelefons, dessen Aufzeichnung weitgehende Schlüsse über das Verhalten des Benutzers erlaubt. Auch die Kenntnis des Gesprächspartners (z.B. Anwalt für internationales Steuerrecht, Drogenhilfe, auf Geschlechtskrankheiten spezialisierter Arzt), der sich anhand des Verkehrsdatums der Anschlussnummer ermitteln lässt, ermöglicht Rückschlüsse auf das Privatleben einer Person[525]. Bereits aus solchen Verbindungsdaten können – auch falsche – Folgerungen über Gesundheitszustand, kriminelle Verstrickungen oder sonstige Eigenschaften einer Person gezogen werden[526]. Das Bundesverfassungsgericht stellt daher fest, dass „Verbindungsdaten ein detailliertes Bild über Kommunikationsvorgänge und Aufenthaltsorte" ermöglichen[527] und Rückschlüsse etwa auf das soziale Umfeld einer Person erlauben[528]. Die Eingriffsintensität, so das Gericht, würde durch die Datenmenge weiter verstärkt, da Auskunftsanordnungen über Verbindungsdaten meist eine Vielzahl von Verbindungen und Personen erfassten[529].

Weil Telekommunikation in immer mehr Bereichen des täglichen Lebens zum Einsatz kommt, hat sich auch die Menge der anfallenden Verkehrsdaten erhöht. Im Jahr 2002 wurden täglich 216 Millionen Telefonverbindungen hergestellt[530]. 1997 fielen allein im Festnetz der Deutschen Telekom AG 54 Milliarden Verbindungsdatensätze an[531]. Nimmt man den Mobilfunkbereich und den Internetbereich hinzu, dann wird deutlich, dass gespeicherte Telekommunikations-Verkehrsdaten eine Datensammlung unermesslichen Ausmaßes darstellen[532]. Teilweise wird angenommen, dass es sich schon bei den bisher von Telekommunikationsunternehmen gespeicherten Verkehrsdaten um die größte Sammlung personenbezogener Daten in Deutschland handele[533].

Bei genauer Betrachtung ist auch der Inhalt eines Kommunikationsvorgangs nichts anderes als ein näherer Umstand der Kommunikation[534], weil er den Kommunikati-

525 Gridl, Datenschutz in globalen Telekommunikationssystemen, 73 f.
526 Gridl, Datenschutz in globalen Telekommunikationssystemen, 74.
527 BVerfGE 107, 299 (322).
528 BVerfGE 107, 299 (320).
529 BVerfGE 107, 299 (320 f.).
530 BVerfGE 107, 299 (327).
531 Welp, TKÜV, 3 (9).
532 Welp, TKÜV, 3 (9).
533 Welp, TKÜV, 3 (9).
534 Vgl. schon Seite **Fehler! Textmarke nicht definiert.**.

onsvorgang näher beschreibt. Die Unterscheidung von Verkehrs- und Inhaltsdaten ist daher rein technischer und begrifflicher Art, ohne dass daraus auf eine unterschiedliche Aussagekraft der jeweiligen Daten geschlossen werden könnte. Verkehrsdaten bilden vielmehr einen mindestens ebenso großen Ausschnitt des täglichen Lebens ab wie Kommunikationsinhalte[535].

Die anfängliche Plausibilität der These, der Zugriff auf Verkehrsdaten wiege weniger schwer als der Zugriff auf Inhalte, beruht allein auf der Tatsache, dass die Kenntnisnahme der äußeren Umstände eines Kommunikationsvorgangs weniger belastend ist als wenn zusätzlich noch der Kommunikationsinhalt abgehört wird. Hierbei handelt es sich aber um keine Besonderheit im Verhältnis von Verkehrs- zu Inhaltsdaten. Der Zugriff auf eine quantitativ größere Datenmenge ist für den Betroffenen vielmehr immer belastender als der Zugriff auf nur einige dieser Daten. Wollte man bei der rechtlichen Ausgestaltung der Eingriffsschwellen auf diesen Unterschied abstellen, so müsste man die Eingriffsvoraussetzungen von der Menge wahrgenommener Daten abhängig machen. Es kann demgegenüber nicht angehen, dass das Kommunikationsverhalten einer Vielzahl von Personen anhand derer Telekommunikations-Verkehrsdaten unter geringeren Voraussetzungen nachvollzogen werden darf als der Inhalt eines Telefongesprächs zwischen Nachbarn.

Dem Bundesverfassungsgericht zufolge ist für die Beurteilung der Schwere eines Informationseingriffs die Nutzbarkeit und Verwendungsmöglichkeit des jeweiligen Datums entscheidend. Nach dem Gezeigten kann, abhängig von den jeweiligen Umständen des Einzelfalls, die Aussagekraft von Telekommunikations-Verkehrsdaten die Aussagekraft von Inhalten erreichen oder übersteigen[536]. Ein Grundsatz, wonach Verkehrsdaten typischerweise weniger schutzbedürftig seien als Inhaltsdaten, lässt sich nicht aufstellen[537]. Da sich die Schwere der Belastung eines Grundrechtsträgers durch die Kenntnisnahme von Aspekten seiner Telekommunikation jeweils nur im Einzelfall bestimmen lässt, die Voraussetzungen eines zulässigen Eingriffs in das

---

535 Walden, Ian in APIG, All Party Parliamentary Internet Group (UK): Dr. Ian Walden, APIG Communications Data Inquiry Oral Evidence, 11.12.2002, www.apig.org.uk/walden_oral_evidence.htm.

536 DSB-Konferenz, Datenschutzbeauftragte des Bundes und der Länder: Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation, Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08.10.1999, BT-Drs. 14/5555, 217; so auch bereits 1984 der Richter am EGMR Pettiti in seiner zustimmenden Meinung zu EGMR, Malone-GB (1984), Publications A82: „It is known that, as far as data banks are concerned, the processing of 'neutral' data may be as revealing as the processing of sensitive data."

Fernmeldegeheimnis aber durch abstrakt-generelle Rechtsnormen zu regeln sind, ist ein unterschiedliches Schutzniveau für Inhaltsdaten einerseits und Verkehrsdaten andererseits nicht gerechtfertigt[538], wie es in den Rechtsordnungen einer Reihe von Ländern bereits anerkannt ist[539].

(ii) Besonders sensible Verkehrsdaten

Auch wenn die Bedeutung einer Unterscheidung von Daten ihrer Art nach im Allgemeinen gering ist, ist sie doch in den Fällen relevant, in denen ein Datum seiner Natur nach in besonders belastender Weise verwendet werden kann[540]. Dies gilt insbesondere für sensible Daten etwa über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben (vgl. § 3 Abs. 9 BDSG). Solche Daten können im Bereich von Telekommunikations-Verkehrsdaten etwa insoweit anfallen, wie die Identität eines Kommunikationspartners – insbesondere bei dauerhaften Kommunikationsbeziehungen – Rückschlüsse auf derartige Tatsachen erlaubt. Das Internet etwa wird im Bereich von Diskussionsforen (Newsgroups) und Beratungsangeboten spezifisch zur Preisgabe und Diskussion von Details des Sexual- und Intimlebens und von Tatsachen genutzt, deren Kenntnis und Zuordnung durch Dritte die Gefahr sozialer Abstempelung (etwa als Drogensüchtiger, Vorbestrafter, Geisteskranker, Asozialer)[541] mit sich bringt. Das Gleiche gilt für Telekommunikation außerhalb des Internet. Insbesondere die Rufnummern der Gesprächspartner und der jeweilige Aufenthaltsort, der sich aus Telekommunikations-Verkehrsdaten ermitteln lässt, kann derartige Rückschlüsse erlauben.

Während sich bei der bisherigen Erfassung von Daten im Einzelfall meistens feststellen lässt, wie sensibel ein Datum ist (vgl. § 100h Abs. 2 StPO), würde eine Vorratsspeicherung unterschiedslos die gesamte Nutzung von Telekommunikationsnetzen

537 Allitsch, CRi 2002, 161 (164).

538 Internationale Konferenz der Datenschutzbeauftragten, Fernmeldegeheimnis (I); Schaar, Retention (I), 2 für Standortdaten; Queen Mary (University of London), Studie über Netzkriminalität (I); Welp, Die strafprozessuale Überwachung des Post- und Fernmeldeverkehrs, 129; ders., Überwachung und Kontrolle, 91; Omega Foundation, Working document (I), Punkt 4.vii. für die automatische Auswertung von Telefongesprächen; Data Protection Commissioner (UK), RIP (I), Punkt 8; Allitsch, CRi 2002, 161 (164 und 166): „outdated and artificial distinction"; IWGDPT, Standortdaten für Standortdaten.

539 G8 Workshop, Workshop A (I); für Österreich Lücking, Die strafprozessuale Überwachung des Fernmeldeverkehrs.

540 Vgl. Bizer, Forschungsfreiheit, 148 f.

541 BVerfGE 65, 1 (48); BVerfGE 78, 78 (87).

abbilden. Es ist technisch unmöglich, sensible Daten von der Aufzeichnung auszunehmen[542]. Dies erhöht die Eingriffsintensität einer Vorratsspeicherung von Telekommunikationsdaten weiter.

Das Leben des modernen Menschen verlagert sich zunehmend in den Bereich der Telekommunikationsnetze[543], wie bereits die Schlagworte Telearbeit, Telemedizin, Telebanking, Telelernen, Teleshopping und Telematik deutlich machen. Betroffen von diesem Trend ist nicht nur das öffentliche, sondern auch das Privatleben. Eine Vorratsspeicherung von Telekommunikations- und Internet-Nutzungsdaten würde weite – und weiterhin steigende – Teile des Privatlebens erfassen. Dementsprechend groß sind auch die Nachteile, die mit einer Vorratsspeicherung einher gehen könnten.

(iii) Staatliche Fehlurteile

Ein Nachteil, den eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten mit sich bringen könnte, ist eine erhöhte Anzahl von Fehlentscheidungen in Ermittlungs- und Gerichtsverfahren. Wie verbreitet Irrtümer in Ermittlungsverfahren allgemein sind, zeigt sich daran, dass 1998 in den alten Bundesländern 2.728 strafmündige Personen von der Polizei ermittelt wurden, welche die Polizei für überführt hielt, ein vorsätzliches Tötungsdelikt begangen zu haben. Wegen eines vorsätzlichen Tötungsdelikts rechtskräftig verurteilt wurden im selben Jahr aber nur 875 Personen[544], also etwa ein Drittel der vorgenannten Zahl. Für die Annahme einer erheblichen Zahl von Fehlurteilen der Staatsanwaltschaft spricht, dass 1998 in den alten Bundesländern 947.187 Personen strafrechtlich angeklagt wurden, davon aber 176.000 Personen freigesprochen wurden oder das Verfahren gegen sie durch das Gericht eingestellt wurde[545].

Dass auch gerichtliche Fehlentscheidungen nicht selten sind, zeigen beispielsweise wissenschaftliche Untersuchungen in den USA, wo immer wieder Fälle von zu Unrecht ausgesprochenen Todesurteilen an das Licht der Öffentlichkeit gelangen. In

542 Weichert, Bekämpfung von Internet-Kriminalität (I), Punkt 6.
543 DSB-Konferenz, Freie Telekommunikation (I).
544 BMI/BMJ, Sicherheitsbericht 2001, 4 f.
545 BMI/BMJ, Sicherheitsbericht 2001, 360.

der Tat liegt bei genauer Betrachtung jedem erfolgreichen Rechtsmittel eine gerichtliche Fehlentscheidung in der Vorinstanz zugrunde. Rechtsmittel sind in unzähligen Fällen erfolgreich, und auch wenn sie nicht eingelegt werden oder werden können, garantiert das nicht die Richtigkeit einer Entscheidung. Vielmehr ist anzunehmen, dass eine substanzielle Anzahl rechtskräftiger Gerichtsentscheidungen falsch ist. Es ist daher von großer Bedeutung, eine angemessen hohe Einschreitschwelle für strafprozessuale Ermittlungen vorzusehen, um Fehlurteilen vorzubeugen. Insgesamt muss davon ausgegangen werden, dass viele Personen unschuldig in Ermittlungs- und Strafverfahren verwickelt werden und dass es in einer erheblichen Anzahl von Fällen zu ungerechtfertigten Verurteilungen kommt. Zahlenmäßig ist von Hunderttausenden auszugehen, die jedes Jahr unschuldig von Eingriffen betroffen sind[546]. Nicht nur staatskritische Personen wie Globalisierungskritiker müssen staatliche Vor- und Fehlurteile fürchten, wenn sie in einen falschen Verdacht geraten. Selbst der unauffälligste Kleinstadtbürger, der an sich „nichts zu verbergen"[547] hat, kann unschuldig belangt werden, wenn er zur falschen Zeit am falschen Ort war.

Zugriffsmöglichkeiten der Behörden auf Telekommunikations-Verkehrsdaten erhöhen die allgemeine Gefahr, unschuldig verdächtigt zu werden[548]. Erstens beziehen sich Verkehrsdaten stets nur auf den Inhaber eines Anschlusses. Wird der Anschluss ohne Wissen des Inhabers missbraucht, dann kann dieser leicht in einen falschen Verdacht geraten. Zweitens ermöglicht es der Zugriff auf Verkehrsdaten den Behörden, nach dem Eliminierungsprinzip zu arbeiten. Dabei wird nicht, wie traditionell üblich, eine „heiße Spur" verfolgt, sondern es werden – etwa mit Hilfe von Verkehrsdaten – eine (oft große) Gruppe von Personen ermittelt, die aufgrund bestimmter Merkmale als Täter in Betracht kommen (beispielsweise alle Personen, die innerhalb eines bestimmten Zeitraums das Opfer einer Straftat angerufen haben). Es kommt dadurch quasi zu einer Inflation an Verdächtigungen, aus der sich die so Erfassten nur noch im Wege einer Art Beweislastumkehr befreien können[549]. Weil ein Verkehrsdatensatz ein Indiz gegen den Angeklagten bilden kann, muss dieser unter Umständen den Richter von seiner Unschuld überzeugen (vgl. § 261 StPO), um nicht

546 Albrecht, Die vergessene Freiheit, 139.

547 Vgl. Wagner, Marita: Intimsphäre - lückenlos überwacht? Telepolis, Heise-Verlag, 28.06.2002, www.heise.de/tp/deutsch/inhalt/te/12813/1.html.

548 BVerfGE 107, 299 (321).

549 Hamm, TKÜV, 81 (86).

zu Unrecht verurteilt zu werden[550]. Mangels eines Alibis wird Unschuldigen der Beweis des Gegenteils keineswegs immer gelingen.

Aber auch, wenn sich die Unschuld einer Person noch im Ermittlungsverfahren herausstellt, kann ein falscher Verdacht ausreichen, um zu Hausdurchsuchungen, Untersuchungshaft, Bewegungseinschränkungen oder Aus- und Einreiseverboten zu führen, was mit erheblichen Belastungen für die Betroffenen verbunden ist. Dies verdeutlicht ein Blick auf die Rasterfahndung zum Auffinden von Terroristen, die allein in Nordrhein-Westfalen Informationen über 250.000 Personen erbracht hat[551]. „Verdächtige" Personen wurden von der Polizei überprüft, wobei die Überprüfung die Befragung von Nachbarn, Hausmeister und Arbeitgeber ebenso einschließen konnte wie das Durchsuchen des Mülleimers[552].

Folgende Fälle von Fehlurteilen aufgrund einer Analyse von Telekommunikations-Verkehrsdaten sind in Europa bereits bekannt geworden: In Österreich wurde ein Nigerianer mehrere Monate lang in Untersuchungshaft genommen, weil er wegen seiner zahlreichen Telefonkontakte als Anführer einer Rauschgiftbande in Verdacht geraten war[553]. Später stellte sich der Verdacht als unbegründet und der Nigerianer lediglich als gefragter Ratgeber in der schwarzen Gemeinschaft in Wien heraus[554]. In Schweden gab es Fälle, in denen unschuldige Personen im Zusammenhang mit Ermittlungen wegen Netzkriminalität festgenommen wurden. Später stellte sich heraus, dass die wirklichen Straftäter den Internet-Zugangscode der festgenommenen Personen ohne deren Kenntnis missbraucht hatten[555].

Aufgrund des begrenzten Aussagegehalts von Telekommunikations-Verkehrsdaten und der Tatsache, dass der Zugriff auf Verkehrsdaten oft eine Vielzahl von Personen betrifft, birgt der Zugriff auf Verkehrsdaten ein besonderes Risiko falscher Verdächtigungen. Weil eine generelle Vorratsspeicherung eine erheblich umfangreichere

---

550 L/D³-Lisken, C 26.

551 Albrecht, Die vergessene Freiheit, 137 f.

552 Albrecht, Die vergessene Freiheit, 137 f.

553 Krempl, Stefan: Die totale Informationsüberwachung, die Demokratie und die Hacker, Telepolis, Heise-Verlag, 28.12.2002, www.heise.de/tp/deutsch/inhalt/te/13870/1.html.

554 Krempl, Stefan: Die totale Informationsüberwachung, die Demokratie und die Hacker, Telepolis, Heise-Verlag, 28.12.2002, www.heise.de/tp/deutsch/inhalt/te/13870/1.html.

Speicherung von Verkehrsdaten als bisher zur Folge hätte, ist zu erwarten, dass auch die Anzahl der Zugriffe auf Verkehrsdaten erheblich steigen würde. Damit würde sich auch das Risiko von Fehlentscheidungen in Ermittlungs- und Gerichtsverfahren erhöhen.

(iv) Staatlicher Gebrauch und Missbrauch von Verkehrsdaten

Aufgrund der hohen Aussagekraft von Telekommunikations-Verkehrsdaten birgt eine Sammlung dieser Daten zudem die Gefahr staatlichen Missbrauchs. Die Artikel-29-Datenschutzgruppe stellt fest: „Allein dadurch, dass es sie gibt, ermöglichen es Verkehrsdaten, persönliches Verhalten in einem bisher ungekannten Maße zu überwachen und zu kontrollieren."[556] Telekommunikation wird heute längst nicht mehr nur zur persönlichen Kommunikation genutzt, sondern zur Bewältigung fast beliebiger Alltagsaktivitäten, seien sie intimer, privater oder beruflicher Art. Dies lässt die Telekommunikationsüberwachung zu einem Mittel der Totalkontrolle werden[557]. Die Datenschutzbeauftragten des Bundes und der Länder wiesen schon 1996 auf diese Gefahr hin[558]: „Bei digitalen Kommunikationsformen läßt sich anhand der Bestands- und Verbindungsdaten nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Eine staatliche Überwachung dieser Vorgänge greift tief in das Persönlichkeitsrecht der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse (z.B. Arztgeheimnis, anwaltliches Vertrauensverhältnis)." Die mit einer Vorratsspeicherung von Telekommunikationsdaten verbundene „Gefahr der Sammlung, Verwertung und Weitergabe der Informationen zu anderen Zwecken"[559] nimmt mit der zunehmenden Verlagerung des Lebens

555 Kronqvist, Stefan (Leiter der IT-Kriminalitätsgruppe der nationalen schwedischen Strafverfolgungsbehörde): Submission to the European Commission for the Public Hearing on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/PublicHearingPresentations/Kronqvist.html.

556 Artikel-29-Gruppe der EU, Anonymität, 5.

557 Weichert, Bekämpfung von Internet-Kriminalität (I), Punkt 5; ders., BigBrotherAward 2002; vgl. auch LINX, User Privacy (I), Punkt 1 für das Internet.

558 DSB-Konferenz, Datenschutzbeauftragte des Bundes und der Länder: Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich, Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23.10.1996, BT-Drs. 13/7500, 200.

559 BVerfGE 85, 386 (399).

in die Welt der neuen Medien[560] weiter zu. In Zukunft wird möglicherweise in jedes Kleidungsstück ein mittels Telekommunikation vernetzter Computer eingebaut sein („Ubiquitous Computing").

Das Ausmaß der Gefahr eines staatlichen Missbrauchs von Verkehrsdaten hängt von der Ausgestaltung der Vorratsspeicherung ab. Besonders wenn sämtliche Verkehrsdaten in einer zentralen, staatlichen Datenbank gespeichert würden, wäre der staatliche Zugriff auf sie kaum kontrollierbar, so dass dem Missbrauch Tür und Tor geöffnet wäre. Aber auch wenn den Eingriffsbehörden die Möglichkeit eines automatischen Online-Zugriffs auf Verkehrsdaten-Datenbanken von privaten Telekommunikationsunternehmen eingeräumt würde, bestünde eine erhebliche Missbrauchsgefahr.

Die britischen Eingriffsbehörden forderten bereits im Jahr 2000 die Einrichtung eines zentralen „Datawarehouse", in dem sämtliche britischen Verkehrsdaten gespeichert werden sollten, um den Behörden das zeitgleiche Durchsuchen und Analysieren des gesamten Datenbestands zu ermöglichen[561]. Bei Einrichtung eines derartigen Datawarehouse in Deutschland würde selbst die geringe Missbrauchskontrolle entfallen, die durch die derzeit noch notwendige Einschaltung der Telekommunikationsunternehmen gewährleistet ist. Bisher müssen Telekommunikationsunternehmen schriftlich um Auskunft ersucht werden, so dass sie immerhin regelmäßig einige formelle Voraussetzungen überprüfen werden, etwa ob ein Ersuchen von einer zuständigen Stelle gestellt wurde. Ein automatisiertes Abrufverfahren würde dagegen die mit schriftlichen Auskunftsersuchen verbundenen Verfahrensschritte und den damit einher gehenden Arbeitsaufwand überflüssig machen, der bisher als faktische Begrenzung der Inanspruchnahme dieser Befugnisse wirkt.

Die moderne Technik erleichtert die Gewinnung vielfältiger Informationen anhand von Telekommunikations-Verkehrsdaten ungemein. Systeme der Firma Harlequin etwa ermöglichen es, automatisch Kommunikationsprofile auf der Basis von Telefon-Verbindungsdaten erstellen zu lassen, um Freundschaftsnetzwerke darzustellen[562]. Solche Software wird etwa in Großbritannien routinemäßig von allen Sicher-

560 Ruhmann/Schulzki-Haddouti, Abhör-Dschungel (I); Artikel-29-Gruppe der EU, Anonymität, 5.

561 NCIS Submission (I), Punkt 6.6.5.

562 Omega Foundation, Working document (I), 10.

heitsbehörden verwendet[563]. Mit etwas Mühe lässt sich das soziale Umfeld einer Person auch ohne diese Software identifizieren. Erforderlich ist nur eine Zugriffsmöglichkeit auf Verkehrs- und Bestandsdaten, wie sie schon heute in Deutschland gegeben ist. Mit Hilfe von Computern ist es auch ein Leichtes, anhand von Telekommunikations-Verkehrsdaten allgemein nach „abnormalem" Kommunikationsverhalten Ausschau zu halten. Mit Hilfe einer Analyse von Verkehrsdaten sind sogar automatisierte Vorhersagen von Verhaltensweisen durchführbar[564].

Die abstrakten Bezeichnungen für die verschiedenen Arten von Verkehrsdaten wie „Ursprung und Ziel einer Kommunikation" sind insoweit irreführend, als sie die Daten als harmlos erscheinen lassen. Die tatsächlichen Verwendungsmöglichkeiten von Verkehrsdaten sind heutzutage jedoch enorm, gerade angesichts der moderner „Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten"[565]. Im Vergleich zu 1983 ist es heute ungleich leichter, verschiedene Informationen zu einem „weitgehend vollständigen Persönlichkeitsbild"[566] zusammen zu fügen. Gerade Telekommunikations-Verkehrsdaten ermöglichen die Gewinnung mannigfaltiger Informationen über Menschen bis hin zur Bildung von Persönlichkeitsprofilen[567]. Im Vergleich zu Telekommunikations-Verkehrsdaten gibt es wohl keine andere Methode, die auf ähnlich billige und bequeme Weise die Erforschung der privaten, geschäftlichen und öffentlichen Beziehungen einer Person ermöglicht[568].

Anhand von Verkehrsdaten lassen sich etwa Fragen der folgenden Art beantworten: Hat eine Person bestimmte Beratungsgespräche per Telefon geführt? Hat sie bei muslimischen Vereinigungen angerufen oder deren Internetseiten betrachtet? Welche Personen surfen überdurchschnittlich oft auf afghanischen Webseiten? Wer benutzt oft die „Online-Banking"-Funktion von schweizer oder liechtensteiner Banken? Hat eine Person an Internet-Foren von Globalisierungskritikern teilgenommen? Wer erhält regelmäßig E-Mails von palästinensischen Menschenrechtsorganisatio-

563 NCIS Submission (I), Punkt 2.1.5.

564 DSB-Konferenz, Datenschutzbeauftragte des Bundes und der Länder: Data Warehouse, Data Mining und Datenschutz, Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15.03.2000, BT-Drs. 14/5555, 232.

565 BVerfGE 65, 1 (45).

566 BVerfGE 65, 1 (42).

567 Bundesregierung, BT-Drs. 14/9801, 14 (15); Schaar, Datenschutz im Internet, 3.

568 Welp, TKÜV, 3 (9).

nen? Die Beispiele machen deutlich, welchen Sprengstoff für eine Demokratie der staatliche Zugriff auf Verkehrsdaten darstellt.

Was Staaten mit Informationen der genannten Art anfangen können, zeigt ein Bericht über die Möglichkeiten des Einsatzes von „Technologien zur politischen Kontrolle", den das Europäische Parlament erstellen ließ[569]. Der Bericht führt aus, dass ein Großteil moderner Überwachungstechnologie in Teilen der Welt eingesetzt wird, um die Aktivitäten von Dissidenten, Menschenrechtsaktivisten, Journalisten, Studentenführern, Minderheiten, Gewerkschaftsführern und politischen Gegenspielern zu überwachen[570]. Selbst der britische Geheimdienst GCHQ soll Organisationen wie Amnesty International und Christian Aid überwachen[571].

Die Möglichkeit von Missbräuchen staatlicher Befugnisse darf man in Anbetracht weitgehend fehlender Kontrollmöglichkeiten auch in Deutschland nicht unterschätzen. Dies lehrt bereits die geschichtliche Erfahrung. Bezeichnenderweise erwogen bereits die Verfasser des Grundgesetzes, in dem späteren Art. 10 GG eine Telekommunikationsüberwachung „zu Zwecken der politischen Überwachung" ausdrücklich auszuschließen[572]. Die Erfahrung lehrt auch, dass einmal etablierte Überwachungsstrukturen im Laufe der Zeit in immer größerem Maße genutzt zu werden pflegen, auch infolge von rechtlichen Erweiterungen. Dies relativiert mögliche rechtliche Begrenzungen, die in Verbindung mit einer Vorratsspeicherung von Telekommunikationsdaten vorgesehen werden könnten.

Hinzu kommen die offiziellen Zugriffsmöglichkeiten ausländischer Staaten nach der Cybercrime-Konvention. Dieser Vereinbarung zufolge darf Deutschland anderen Vertragsstaaten den Zugriff auf hierzulande gespeicherte Verkehrsdaten nicht verwehren, selbst wenn in diesen Staaten keine auch nur annähernd vergleichbaren Sicherungsmechanismen existieren. Davon ist angesichts der Vielzahl von Vertragsstaaten (darunter Albanien, Azerbaijan und Russland) auszugehen. Sobald ausländische Staaten Zugriff auf deutsche Verkehrsdaten erhalten, kann von deutscher Seite nicht mehr verhindert werden, dass die Daten im Ausland in einer Weise ein-

569 Omega Foundation, Report (I).
570 Omega Foundation, Report (I), Punkt 7.
571 Omega Foundation, Report (I).
572 AK-GG-Bizer, Art. 10, Rn. 10, Fn. 57.

gesetzt werden, die in Deutschland als exzessiv und rechtswidrig anzusehen wäre. Als Beispiel für ein solches Vorgehen lässt sich anführen, dass in den USA 800 Menschen nur deshalb monatelang inhaftiert worden sein sollen, weil sie im Vorfeld des 11. September 2001 besonders viel kommuniziert haben[573]. Aussicht auf ordnungsgemäße Gerichtsverfahren hatten diese Menschen nicht[574]. Man hüte sich auch vor der leichtfertigen Aussage, in Europa sei ein solcher Vorgang nicht denkbar. Eine solche Prognose würde die Veränderlichkeit von Werten außer Betracht lassen.

In diesem Zusammenhang ist zu beachten, dass auch Interessen der Wirtschaft geeignet sind, Tendenzen zur Überwachung der Nutzung von Telekommunikationsnetzen zu bestärken. Unternehmen, die im Bereich der Telekommunikationsnetze aktiv sind, sind regelmäßig an der Gewährleistung eines geschützten Bereiches für ihre Kunden und sie selbst interessiert, in dem ungestört konsumiert werden kann. Kritische Aktivitäten im Netz können dabei etwa insoweit stören, wie Eltern ihren Kindern bestimmte Inhalte im Internet vorenthalten wollen und die Kinder deswegen insgesamt von der Nutzung des Internet ausschließen könnten, wodurch diese auch kommerzielle Angebote nicht mehr nutzen könnten. Von Seiten der Wirtschaft bestehen daher Tendenzen, Aktivitäten außerhalb des Gewöhnlichen oder sogar am Rand des Illegalen aus den Telekommunikationsnetzen zu verdrängen und nur wirtschaftlich und politisch erwünschtes Verhalten zuzulassen[575]. Dieser Gefahr muss vorgebeugt werden, und es muss stets im Auge behalten werden, dass Freiheitsbeschränkungen durch andere Interessen motiviert sein können als es öffentlich vorgetragen wird.

Staatlichen Überwachungsbefugnissen wohnt stets die Gefahr inne, gezielt gegen Personen eingesetzt zu werden, die dem Staat missliebig sind. Dass auch hierzulande gegen staatskritische Personen bislang gezielt vorgegangen wird, zeigt etwa der Fall einer bayerischen Lehrerin, die wegen ihrer „Tätigkeit in organisierten Friedensbewegungen" Repressalien seitens ihres Dienstherrn hinzunehmen hatte[576]. Weil sie das Hauptquartier des Palästinenserpräsidenten Jassir Arafat in Ramallah besucht

---

573 Krempl, Stefan: Die totale Informationsüberwachung, die Demokratie und die Hacker, Telepolis, Heise-Verlag, 28.12.2002, www.heise.de/tp/deutsch/inhalt/te/13870/1.html.

574 Krempl, Stefan: Die totale Informationsüberwachung, die Demokratie und die Hacker, Telepolis, Heise-Verlag, 28.12.2002, www.heise.de/tp/deutsch/inhalt/te/13870/1.html.

575 Zur Parallele bei der Videoüberwachung Achelpöhler/Niehaus, DuD 2002, 731 (734 f.).

576 Eckert, Dirk: Ist eine Tätigkeit in der Friedensbewegung verfassungskonform?, 20.05.2002, Telepolis, Heise-Verlag, www.heise.de/tp/deutsch/inhalt/co/12578/1.html.

hatte, an einer Demonstration für „Solidarität mit Palästina" teilgenommen hatte und Mitglied bei der globalisierungskritischen Nichtregierungsorganisation Attac war, äußerte die Regierung von Oberbayern Zweifel an ihrer Verfassungstreue[577]. Derartige Zweifel hätten sich auch aus der Analyse von Telekommunikations-Verkehrsdaten ergeben können, etwa aufgrund bestimmter Kontakte oder eines Interesses an bestimmten Internetangeboten. Als weiteres Beispiel politischer Kontrolle ist ein Fall zu nennen, in dem – noch in den 80er Jahren – das Land Niedersachsen eine Lehrerin namens Vogt vom Dienst suspendierte, nachdem sich diese als Kandidatin für die Kommunistische Partei hatte aufstellen lassen. Erst der Europäische Gerichtshof für Menschenrechte stellte fest, dass in diesem Vorgehen ein Verstoß gegen die Meinungsfreiheit der Lehrerin (Art. 10 EMRK) lag[578]. Dass der deutsche Staat bisweilen versucht ist, in demokratisch bedenklicher Weise seine Muskeln spielen zu lassen, zeigten auch die internationalen Spitzengipfel in Salzburg und Genua im Jahre 2001. In deren Vorfeld hat man auf deutscher Seite die Befugnisse, die ursprünglich als Maßnahmen gegen Hooligans präsentiert und in das Passgesetz eingefügt worden waren, gegen Globalisierungskritiker eingesetzt[579].

Weiterhin haben die Praktiken einiger Staaten, Kommunikationsüberwachung zum Zwecke von Wirtschaftsspionage einzusetzen, traurige Berühmtheit erlangt[580]. In Großbritannien und den USA z.B. ist Wirtschaftsspionage im Ausland legal[581]. Auch im Zusammenhang mit der Ausforschung wissenschaftlicher Forschungserkenntnisse könnten Zugriffe auf Verkehrsdaten erfolgen, die auf Vorrat gespeichert wurden.

Es existiert mithin eine Vielzahl von Fällen, in denen staatliche Eingriffsbefugnisse – gemessen an dem Standard des Grundgesetzes und der Menschenrechtskonvention – missbraucht wurden, gerade im Bereich der Telekommunikationsüberwachung und des Zugriffs auf Verkehrsdaten. Deshalb und wegen der enormen Ver-

---

577 Eckert, Dirk: Ist eine Tätigkeit in der Friedensbewegung verfassungskonform?, 20.05.2002, Telepolis, Heise-Verlag, www.heise.de/tp/deutsch/inhalt/co/12578/1.html.

578 EGMR, Vogt-D (1995), Publications A323.

579 Kaleck, Wolfgang u.a.: Stellungnahme von Bürgerrechtsorganisationen zur Anhörung des Innenausschusses des Deutschen Bundestages am 30.11.2001 zum Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz), www.cilip.de/terror/atg-stell-281101.pdf, 6.

580 Dazu nur EP, Echelon-Bericht (I), 102 ff.; Omega Foundation, Report (I); Garstka/Dix/Walz/Sokol/Bäumler, Hintergrundpapier (I), Punkt II.

581 Schulzki-Haddouti, Christiane: Widerstände gegen Cybercrime-Abkommen aus eigenen Reihen, 09.11.2000, Telepolis, Heise-Verlag, www.heise.de/tp/deutsch/inhalt/te/4228/1.html.

wendungsmöglichkeiten von Telekommunikations-Verkehrsdaten sind missbräuchliche Zugriffe gerade auch auf vorratsgespeicherte Verkehrsdaten zu erwarten.

Was die rechtlich zulässigen Verwendungsmöglichkeiten von mittels einer generellen Vorratsspeicherung erlangten Telekommunikations-Verkehrsdaten angeht, sehen weder der RSV-Entwurf noch die Vorschläge des Bundesrats nennenswerte Einschränkungen vor. In dem ErmittlungsG-Entwurf holte der Bundesrat zum „Rundumschlag" aus, indem er alle Gefahrenabwehr- und Strafverfolgungsbehörden, einschließlich der Nachrichtendienste, zum Zugriff ermächtigen wollte. Die Stellungnahme des Bundesrats vom 19.12.2003 knüpft an die bestehenden Zugriffsrechte von Strafverfolgungsbehörden und Nachrichtendiensten sowie, nach Maßgabe der Landesgesetze, auch Gefahrenabwehrbehörden an. Der RSV-Entwurf erlaubt den Zugriff mindestens für Zwecke der „Prävention, Erforschung, Ermittlung und Verfolgung von Kriminalität und Straftaten". Dies entspricht dem einschlägigen Kompetenztitel, Art. 29 EU, der Maßnahmen zur präventiven „Verhütung" und repressiven „Bekämpfung der [...] Kriminalität" abdeckt.

Während die Vorschläge des Bundesrats im Zusammenhang mit Zugriffsnormen wie den §§ 100g, 100h StPO zu lesen sind, bestimmt der RSV-Entwurf selbst, dass auf gespeicherte Daten nur „fallweise" zugegriffen werden darf (Art. 6 Buchst. a RSV-E). Dies dürfte es ausschließen, dass Behörden „ins Blaue hinein" auf die gespeicherten Daten zugreifen, also losgelöst vom Einzelfall den gesamten Datenbestand durchsuchen und auswerten, um überhaupt erst Anhaltspunkte für begangene oder geplante Straftaten zu gewinnen. Aufgrund der unvorstellbar großen Datenmengen könnte dabei zwangsläufig nur nach dem Muster der Rasterfahndung vorgegangen werden, indem nach bestimmten, auffälligen Merkmalen gesucht wird. Gerade diese Vorgehensweise würde der freien Kommunikation in unserer Gesellschaft großen Schaden zufügen. Jeder, dessen Kommunikationsverhalten von dem des europäischen Durchschnittsbürgers abweicht, hätte dann nämlich zu befürchten, allein wegen dieses abweichenden Verhaltens von den Behörden unter die Lupe genommen zu werden und weiteren Ermittlungen, die zwangsläufig das Risiko von Vor- und Fehlurteilen mit sich bringen, ausgesetzt zu werden.

Abgesehen von dem Verbot des Zugriffs „ins Blaue hinein" sieht der RSV-Entwurf keine Eingriffsschwelle vor. Er überlässt es vielmehr den Mitgliedstaaten, zu welchen

„bestimmten, [...] legitimen Zwecken" ihre Behörden auf die gespeicherten Verkehrsdaten zugreifen dürfen (Art. 6 Buchst. a RSV-E). Welche Zwecke die Umschreibung „Prävention, Erforschung, Ermittlung und Verfolgung" von Straftaten im Einzelnen abdeckt, ist offen. Eine Erheblichkeitsschwelle ist nicht vorgesehen, so dass auch wegen Bagatelldelikten eine umfassende Untersuchung des Kommunikationsverhaltens erlaubt werden kann. Unbestimmt ist ferner die Formulierung „Kriminalität und Straftaten", der offenbar die Annahme zugrunde liegt, dass Kriminalität auch außerhalb strafbaren Verhaltens existieren können soll.

(v) Risiko des Missbrauchs durch Private

Neben dem Risiko einer missbräuchlichen oder exzessiven Verwendung von Verkehrsdaten durch den Staat besteht die Gefahr, dass der Staat, wo er wegen eigener Überwachungsinteressen einen effektiven Schutz personenbezogener Daten verhindert, auch Dritten den missbräuchlichen Zugriff auf diese Daten erleichtert. Beispielsweise sind die gegenwärtig nach § 110 TKG einzurichtenden Überwachungsschnittstellen Schwachstellen im Sicherheitssystem der Telekommunikationsunternehmen, weil sie den Einbruch unbefugter Personen und das unbefugte Abhören durch Mitarbeiter des Anlagenbetreibers ermöglichen[582]. Teilweise wird davon ausgegangen, dass es nur eine Frage von Monaten sei, bis diese Schnittstellen von ausländischen Geheimdiensten und der organisierten Kriminalität genutzt würden[583]. Im Fall der Einführung einer Vorratsspeicherung von Telekommunikations-Verbindungsdaten würde sich diese Problematik erheblich verschärfen[584]. Wegen der Sicherheitsprobleme und der Kosten für die Wirtschaft hat man in den USA auf die für die Behörden bequeme und preiswerte Schnittstellenlösung verzichtet, ohne dass dies zu erkennbaren Erfolgseinbußen geführt hätte[585].

---

582 VATM: 15 Punkte zur TKG-Novelle, 17.12.2002, www.vatm.de/images/dokumente/15_punkte_tkg.pdf: „[...] beabsichtigtes und unbeabsichtigtes Eindringen Unbefugter [wird] erleichtert mit dem Risiko schwerster Schäden an innerbetrieblicher bzw. vertraulicher Information"; AK-GG-Bizer Art. 10, Rn. 17 und 114; Garstka/Dix/Walz/Sokol/Bäumler, Hintergrundpapier (I), Punkt II; Germann, 323: wie wenn die Polizei nach einer gewaltsamen Wohnungsöffnung die Tür offen lassen würde; Weichert, Bekämpfung von Internet-Kriminalität (I); Pernice, Ina (Deutscher Industrie- und Handelskammertag) in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 14.

583 Pfitzmann, Andreas in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 24.

584 ULD-SH, Kampagne, Hintergrund (I).

585 Schulzki-Haddouti, Internationale Abhörpolitik, 125 (130).

Große Bestände von personenbezogenen Daten, wie sie eine Vorratsspeicherung von Telekommunikationsdaten zur Folge hätte, bilden stets einen Anreiz für technisch versierte Hacker[586]. Sogar deutsche Kreditinstitute, deren Anlagen in hohem Maße gesichert sein sollten, erlagen in der Vergangenheit wiederholt Angriffen von Hackern. Organisationen wie der Chaos Computer Club demonstrierten immer wieder Sicherheitslücken von Online-Banking, Telefonkarten, Geldkarten-PINs usw. Wenn selbst der Großkonzern Microsoft laufend Sicherheitsverbesserungen seiner Internet-Produkte veröffentlichen muss, weil ständig neue Sicherheitslücken bekannt werden, dann ist kaum zu erwarten, dass es hunderte von Telekommunikationsunternehmen in Deutschland verstehen werden, ihre Daten ausreichend zu sichern. Das Risiko eines unbefugten Datenzugriffs steigt allgemein mit der Anzahl von Daten speichernden Stellen. Im Fall einer Vorratsspeicherung wäre eine Vielzahl von Telekommunikationsunternehmen mit der Datenvorhaltung betraut, so dass das Missbrauchsrisiko entsprechend groß wäre. Verbände von Internet-Service-Providern warnen ausdrücklich, dass ihnen die Gewährleistung der Datensicherheit aller Wahrscheinlichkeit nach unmöglich sein würde, sollten sie zu einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten verpflichtet werden[587]. Durch Absicht oder unbeabsichtigterweise könnten gespeicherte Daten vielmehr jederzeit in falsche Hände gelangen[588].

Tatsächlich ist es in der Praxis immer wieder vorgekommen, dass wegen technischer Fehler plötzlich ganze Kundendateien einschließlich Kreditkartennummern für jedermann über das Internet abrufbar waren[589]. Sogar die Firma Microsoft, die für die

---

586 Etwa Heise Verlag: Kreditkarten-Nummern bei Online-Händler erbeutet, Meldung vom 19.05.2001, www.heise.de/-newsticker/data/em-19.05.01-000/.

587 EuroISPA, Internet Service Providers' Association (Europe) / US ISPA, Internet Service Providers' Association (U.S.A.): Position on the Impact of Data Retention Laws on the Fight against Cybercrime, 30.09.2002, www.euroispa.org/docs/-020930eurousispa_
dretent.pdf, 2; Bernhard Rohleder (Bitkom-Geschäftsführer) in Heise Verlag: IT-Branchenverband gegen Vorratsspeicherung von Verbindungsdaten, Meldung vom 19.08.2002, www.heise.de/newsticker/data/hod-19.08.02-001/; Deutsche Telekom AG: Schriftliche Stellungnahme zur öffentlichen Anhörung am 09.02.2004 in Berlin zum Entwurf eines Telekommunikationsgesetzes (TKG), in Ausschussdrucksache 15(9)961, www.bundestag.de/gremien15/a09/004Anhoerungen/TKG/-materialeingeladene.pdf, 150 (163): „potentiell wesentlich erhöhte Gefahr des Missbrauchs personenbezogener Daten".

588 EuroISPA, Internet Service Providers' Association (Europe) / US ISPA, Internet Service Providers' Association (U.S.A.): Position on the Impact of Data Retention Laws on the Fight against Cybercrime, 30.09.2002, www.euroispa.org/docs/-020930eurousispa_
dretent.pdf, 2.

589 Vgl. etwa Darstellung bei EPIC/PI, Privacy and Human Rights 2002 (I), Teil I, 79; für Deutschland etwa Heise Verlag: Versicherungsgruppe HUK-Coburg legte Kundendaten offen ins Netz, Meldung vom 06.11.2002, www.heise.de/newsticker/data/-jk-06.11.02-001/; Heise Verlag: Schwerwiegende Sicherheitsmängel bei T-Com, Meldung vom 26.07.2004, www.heise.de/-newsticker/meldung/49424; für die USA Heise Verlag: Daten von mehr als acht Millionen US-Kreditkarten geklaut, Meldung vom 19.02.2003, www.heise.de/newsticker/data/jk-19.02.03-000/.

Sicherheit der meisten Heimcomputer verantwortlich ist, hat in der Vergangenheit versehentlich interne Geschäftsgeheimnisse und persönliche Daten von Millionen von Kunden öffentlich zugänglich ins Internet gestellt[590]. Das Internet hat bekanntlich die Eigenschaft, dass sich alle Daten, die dort einmal verfügbar waren, beliebig oft vervielfältigen lassen, so dass Inhalte, einmal veröffentlicht, meistens nicht mehr entfernt werden können. Zu welchen Schäden die unfreiwillige Veröffentlichung von Telekommunikations-Verkehrsdaten führen könnte, lässt sich kaum abschätzen. Außer durch Hacking könnten Telekommunikations-Verkehrsdaten auch auf dem Übertragungsweg zwischen Telekommunikationsunternehmen und Sicherheitsbehörden abgefangen werden. Schon die nach der bestehenden TKÜV in Verbindung mit der zugehörigen technischen Richtlinie geforderten Sicherheitsmechanismen entsprechen aus Sicht von Sachverständigen bei weitem nicht dem, was technisch möglich und zumutbar ist[591]. Die vorgesehenen Sicherheitsfunktionen schützten allenfalls vor Angriffsversuchen durch Unbedarfte[592]. Wie allgemein bei den hier diskutierten Missbrauchsrisiken liegt die besondere Gefahr dieser Einbruchstelle darin, dass ein Abhören regelmäßig unbemerkt bleiben wird.

Ein Grund dafür, dass Private großen Aufwand treiben könnten, um illegal an Verkehrsdaten zu gelangen, liegt in dem hohen kommerziellen Wert von Persönlichkeitsprofilen, die durch die Auswertung von Telekommunikations-Verkehrsdaten erstellt werden können[593]. Nach den Erfahrungen der Datenschutz-Aufsichtsbehörden genügen zur Erstellung eines Persönlichkeitsprofils schon die Verkehrsdaten, die bei dem Besuch weniger Internetseiten durch eine Person anfallen[594]. Ein Online-Nutzerprofil erspart jedem Unternehmen Marketingausgaben in Höhe von ca. 100 Euro pro Kunde[595], insbesondere wegen der darin enthaltenen detaillierten Hinweise auf die Interessen, Vorlieben und Gewohnheiten einer Person, die ihre gezielte

590 Heise Verlag: Microsoft mit offenem ftp-Server, Meldung vom 19.11.2002, www.heise.de/newsticker/data/ps-19.11.02-000/; Heise Verlag: Microsoft veröffentlicht unfreiwillig Kundendaten, c't 25/2002, S. 25.

591 Federrath, Schwachstelle Schnittstelle, 115 (122).

592 Federrath, Schwachstelle Schnittstelle, 115 (122).

593 Feather, Clive, zitiert bei Loney, Matt: ISPs spell out true cost of data retention, 12.12.2002, news.zdnet.co.uk/story/0,,t295-s2127408,00.html.

594 Bäumler, Helmut / Leutheusser-Schnarrenberger, Sabine / Tinnefeld, Marie-Theres: Grenzenlose Überwachung des Internets? Steht die freie Internetkommunikation vor dem Aus? Stellungnahme zum Gesetzesentwurf des Bundesrates vom 31. Mai 2002, www.rainer-gerling.de/aktuell/vorrat_stellungnahme.html, Punkt 1.

595 Schaar, DuD 2001, 383 (384).

Ansprache ermöglichen. Die Kenntnis von Verkehrsdaten ermöglicht es damit, Menschen unbemerkt in ihrem Konsumverhalten zu steuern[596].

Wegen des hohen Wertes von Verkehrsdaten wäre die Versuchung von Telekommunikationsunternehmen groß, die äußerst aussagekräftigen und umfangreichen Verkehrsdaten, die sie zu staatlichen Zwecken auf Vorrat speichern müssten, anderweitig zu nutzen. Ein solcher Missbrauch wäre von außen kaum feststellbar. Zurecht wird darauf hingewiesen, dass eine Vorratsspeicherung insoweit Straftaten nicht bekämpfen, sondern umgekehrt ihre Begehung begünstigt würde (vgl. §§ 206 StGB, 44, 43 BDSG)[597]. Wenn für die Daten von 10.000 Kunden nach der oben genannten Wertschätzung bis zu eine Million Euro locken, sind derartige Befürchtungen nicht aus der Luft gegriffen. Gerade bei kleineren Anbietern, die keinen Ruf zu verlieren haben oder sich wirtschaftlich am Rande der Insolvenz bewegen, wäre das Risiko eines solchen Missbrauches hoch. Schon heute gibt es immer wieder Gerüchte, wonach Internetfirmen persönliche Daten ihrer Kunden gewinnbringend weitergegeben haben sollen[598]. In den USA steht ein Mitarbeiter des Internet-Zugangsanbieters AOL im Verdacht, 92 Millionen Kundendatensätze des Unternehmens für 152.000 US$ verkauft zu haben[599].

Selbst wenn ein Unternehmen guten Willens wäre, könnte es nicht immer verhindern, dass einzelne Mitarbeiter unbefugt Daten heraus geben, wie es etwa im Rahmen der Bonusmeilen-Affäre mit den Daten von Abgeordneten des Deutschen Bundestags geschehen ist. Dieses Beispiel zeigt, dass im Fall einer Vorratsspeicherung von Telekommunikationsdaten nicht nur die Herausgabe gesamter Datenbestände etwa an Direktmarketingunternehmen zu befürchten wäre, sondern auch die – im Einzelfall ebenfalls lukrative – Erteilung einzelner Auskünfte an Presse, Wirtschaftsauskunfteien, Detektivbüros, Banken, Arbeitgeber oder sonstige interessierte

596 Gridl, Datenschutz in globalen Telekommunikationssystemen, 61.

597 Bäumler, Helmut / Leutheusser-Schnarrenberger, Sabine / Tinnefeld, Marie-Theres: Grenzenlose Überwachung des Internets? Steht die freie Internetkommunikation vor dem Aus? Stellungnahme zum Gesetzesentwurf des Bundesrates vom 31. Mai 2002, www.rainer-gerling.de/aktuell/vorrat_stellungnahme.html, Punkt 1.

598 Bager/Bleich/Heidrich, c't 22/2002, 150 (150 f.).

599 Heise Verlag: AOL-Mitarbeiter wegen Verkaufs von Kundendaten verhaftet, 24.06. 2004, www.heise.de/newsticker/meldung/48542.

Stellen[600]. Auch Mitarbeiter staatlicher Stellen missbrauchen ihre Zugriffsbefugnisse mitunter[601].

Dass Wissen eine Machtposition verleiht, weiß schon der Volksmund. Das Wissen um eine Person, etwa um ihre persönlichen Schwächen, kann zu ihrer Manipulation verwendet werden[602]. Teilweise wird sogar angenommen, dass man nahezu jeden Menschen inkriminieren kann, wenn man ihn nur lange genug unbemerkt in seinem Tun beobachten kann[603]. Das Wissen um Telekommunikations-Verkehrsdaten einer Person eignet sich wegen der hohen Aussagekraft der Daten in besonderem Maße zur Manipulation von Menschen.

Zu welchen Konsequenzen es führen kann, wenn Daten in die falschen Hände gelangen, zeigt in neuester Zeit der bereits erwähnte „Bonusmeilen-Skandal". Deutsche Politiker, die mit dienstlich erworbenen Bonusmeilen Privatflüge bezahlt haben, sahen sich infolge der Veröffentlichung dieser Tatsache zum Rücktritt gezwungen. Auch infolge der „Hunzinger-Affäre" standen plötzlich alle im Rampenlicht der Öffentlichkeit, die Beziehungen zu diesem PR-Berater hatten.

Das Informationspotenzial der Spuren aller deutschen Telekommunikationsnutzer ist nur schwer einzuschätzen. Wer mit Herrn Hunzinger per Telefon, Fax oder E-Mail in Kontakt stand, ließe sich mit ihrer Hilfe unschwer ermitteln. Unzählige Tatsachen über das Privatleben von Prominenten könnten enthüllt werden[604]. Politiker könnten zum Rücktritt gezwungen, Amtsträger könnten erpresst werden. Informationen über das Sexualleben ließen sich mit Hilfe von Telekommunikations-Verkehrsdaten ebenso ausbeuten wie Hinweise auf Kontakte mit bestimmten Personen oder Ländern.

Nicht nur im öffentlichen und privaten, sondern auch im geschäftlichen Bereich bringt eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten erhebliche Gefahren mit sich[605]. Unter dem Gesichtspunkt der Wirtschaftsspionage

---

600 Gridl, Datenschutz in globalen Telekommunikationssystemen, 39 und 61.

601 Vgl. nur Landesbeauftragter für den Datenschutz in Baden-Württemberg, 7. Tätigkeitsbericht, LT-Drs. 9/4015, 45-49 mit Fällen von absichtlichem und fahrlässigem Datenmissbrauch bei der Polizei.

602 Buxel, DuD 2001, 579 (581).

603 Fairbrother, Peter: Defeating traffic analysis, www.apig.org.uk/fairbrother.pdf, 3.

604 Königshofen, Thomas, zitiert bei Krempl, Stefan: Datenschutz ade? Telepolis, Heise-Verlag, 29.12.2001, www.heise.de/tp/deutsch/inhalt/te/11456/1.html.

605 ULD-SH, Sichere Informationsgesellschaft (I), Punkt 7a.

kann es beispielsweise von großem Interesse sein, wo sich ein Vorstandsmitglied aufhält und mit welchen Firmen es Kontakte pflegt. Anfällig für Wirtschaftsspionage sind auch Verhandlungen über die Vergabe großer Aufträge. Für geschäftliche Verhandlungen ist Anonymität nach außen oft vital. Die Speicherung von Verkehrsdaten stellt diese Anonymität in Frage. Angesichts der hohen Summen, um die es im Bereich der internationalen Wirtschaft geht, wird selbst großer Aufwand nicht gescheut werden, um an auf Vorrat gespeicherte Datenbestände zu gelangen. In dementsprechend hohem Maße wären solche Datenbestände gefährdet.

Einen effektiven Schutz vor Missbräuchen ermöglichen letztlich nur Verfahren, die es zur Speicherung von Daten von vornherein nicht kommen lassen (Datensparsamkeitsprinzip, vgl. § 3a BDSG). Eine Vorratsspeicherung von Telekommunikationsdaten würde dem Datensparsamkeitsprinzip diametral zuwider laufen. Insofern spiegelt sich bei den Plänen zur Vorratsspeicherung von Verkehrsdaten ein allgemeiner Konflikt im Bereich der Telekommunikationsüberwachung wider. Die Konfliktlinie verläuft nicht streng zwischen den Sicherheitsbehörden einerseits und Datenschützern andererseits. Vielmehr hat sich auch im staatlichen Bereich bei nicht wenigen Personen die Ansicht durchgesetzt, dass der Aufbau einer sicheren Infrastruktur und der damit einher gehende präventive Schutz von persönlichen Daten und Geschäftsgeheimnissen Vorrang haben muss vor kurzfristigen Ermittlungsvorteilen für die Sicherheitsbehörden, die eine Schwächung der informationstechnischen Sicherheit mit sich bringen[606]. In Anbetracht dieser Tatsache hat die Politik in der Vergangenheit davon abgesehen, die Nutzung von Verschlüsselungstechnologien einzuschränken. Im Bereich der anonymen Telekommunikationsnutzung ist die Interessenlage vergleichbar[607]. Eine generelle Vorratsspeicherung von Verkehrsdaten würde demgegenüber ein unkontrollierbares Missbrauchspotenzial begründen.

(vi) Verursachung von Hemmungen seitens der Grundrechtsträger

Wie gezeigt, müsste der Bürger im Falle einer Vorratsspeicherung seiner Telekommunikationsdaten ständig mit dem Risiko staatlicher Fehlentscheidungen oder eines staatlichen oder privaten Missbrauchs seiner Daten rechnen. Aus diesem Grund ist

606 Etwa Tauss/Kelber, DuD 2001, 694 (694); vgl. auch Pfitzmann, Andreas in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 24.

607 Fox/Bizer, DuD 1998, 616 (616).

eine Vorratsspeicherung von Telekommunikationsdaten geeignet, die Unbefangenheit der zwischenmenschlichen Kommunikation in unserer Gesellschaft zu gefährden. Wer ständig damit rechnen muss, sein Kommunikationsverhalten könnte in Zukunft einmal gegen ihn verwendet werden, wird im Zweifel versuchen, sich möglichst unauffällig zu verhalten oder Kommunikationsvorgänge gänzlich zu unterlassen. Dies jedoch wäre unserem demokratischen Staatssystem (Art. 20 Abs. 1 GG) abträglich, das auf die aktive und unbefangene Mitwirkung der Bürger angewiesen ist[608]. Jede Demokratie lebt von der Meinungsfreude und dem Engagement der Bürger und setzt daher Furchtlosigkeit voraus[609]. Dort, wo „ein Klima der Überwachung und Bespitzelung herrscht, [kann] ein freier und offener demokratischer Prozess nicht stattfinden"[610]. Gerade eine Vorratsspeicherung von Telekommunikationsdaten wäre ein großer Schritt hin zu mehr Überwachung, weil die Überwachung über Einzelfälle hinaus auf die gesamte Telekommunikation der Gesellschaft ausgedehnt würde. Dies wäre auch für diejenigen Bürger, die sich mit den Feinheiten der gesetzlichen Regelungen nicht auskennen, deutlich erkennbar, so dass ein deutlicher Einfluss auf das Kommunikationsverhalten der gesamten Gesellschaft zu befürchten ist.

In besonderem Maße gilt dies dort, wo staatlicher Missbrauch besonders nahe liegt, nämlich bei staatskritischen Organisationen, deren Aktivitäten in einer Demokratie besonders wichtig sind. Beispielsweise waren die anlässlich des letzten Deutschlandbesuches des US-Präsidenten Bush angekündigten Demonstrationen der Bundesregierung aus Gründen des „außenpolitischen Ansehens" ein Dorn im Auge. In solchen Situationen könnten Organisatoren von Demonstrationen durchaus Anlass sehen, ihre Telekommunikation einzuschränken, um einer missbräuchlichen Überwachung zu entgehen. Von jeher ein besonders legitimes Interesse an Anonymität haben Journalisten, Menschenrechtsaktivisten, Minderheitenvertreter und Oppositionelle. Dies gilt heute besonders in totalitären Staaten[611]. Aber auch westliche Staa-

608 Vgl. BVerfGE 65, 1 (43); BVerfGE 100, 313 (381).

609 Limbach, Jutta: Ist die kollektive Sicherheit Feind der individuellen Freiheit? 10.05.2002, www.zeit.de/reden/-Deutsche%20Innenpolitik/200221_limbach_sicherheit. html.

610 Kutscha, Martin, zitiert bei Limbach, Jutta: Ist die kollektive Sicherheit Feind der individuellen Freiheit? 10.05.2002, www.zeit.de/reden/Deutsche%20Innenpolitik/
200221_limbach_sicherheit.html; DG Research, Economic risks arising from the potenzial vulnerability of electronic commercial media to interception (I); vgl. zu Maßnahmen der Terrorismusbekämpfung auch Weichert, Terror und Informationsgesellschaft (I); Schwimmer, Anti-terrorist measures and Human Rights (I).

611 Artikel-29-Gruppe der EU, Anonymität, 5.

ten wie Deutschland sind, wie gezeigt, gegen Missbräuche bezüglich dieser Personen nicht von vornherein immun.

Um Anhaltspunkte für die Frage zu gewinnen, wie sich eine generelle Vorratsspeicherung von Verkehrsdaten auf das Kommunikationsverhalten in Deutschland auswirken könnte, hat der Verfasser im April 2003 einen kurzen Fragenkatalog an Personen und Organisationen versandt, die aufgrund ihrer politisch teilweise brisanten Arbeit besonders sensibel auf staatliche Überwachung reagieren könnten. Im Einzelnen wurde der Fragebogen an die Organisationen Attac, BUND, Deutsches Rotes Kreuz, Eirene, GFBV, Greenpeace, ILMR, IPPNW, Misereor, PDS, Terre des Hommes und X1000malquer sowie an die Journalistin Schulzki-Haddouti versandt. In dem Fragebogen wurden folgende Fragen gestellt: „Berücksichtigen Sie bei Ihren Anrufen, Telefaxen, Emails usw. die Möglichkeit, dass staatliche Stellen (z.B. Geheimdienste) Ihre Telekommunikation abhören oder aufzeichnen könnten? Ergreifen Sie in bestimmten Fällen Gegenmaßnahmen (z.B. Ausweichen auf persönliche Gespräche, Ausweichen auf Briefe, Benutzung öffentlicher Telefonzellen, Verschlüsselung von Nachrichten)? Würde es Sie zu (verstärkten) Gegenmaßnahmen veranlassen, wenn der Staat die äußeren Umstände jedes Telefonanrufs, Telefaxes, jeder Email und jeder Internetnutzung durch die Telekommunikationsunternehmen speichern lassen würde, um im Bedarfsfall darauf zugreifen zu können (Rufnummern/Emailadressen/Internetadressen der Beteiligten, Uhrzeit, bei eingeschalteten Mobiltelefonen auch der jeweilige Standort)?"

Drei der angeschriebenen Stellen antworteten auf die Anfrage. Die PDS-Bundesgeschäftsstelle erklärte, dass die PDS eine weitgehend öffentliche Partei sei, in der alle Gremien öffentlich tagten und deren Beschlüsse und Diskussionen zum Beispiel über das Internet öffentlich gemacht würden. Aus diesem Grund beantworte man die gestellten Fragen mit „Nein".

Die Antwort der Journalistin und Autorin Christiane Schulzki-Haddouti weist demgegenüber darauf hin, dass die Einführung einer Vorratsspeicherung von Telekommunikationsdaten Beeinträchtigungen der Telekommunikationsnutzung mit sich bringen könnte. Frau Schulzki-Haddouti beschäftigt sich kritisch mit politischen Themen wie etwa der staatlichen Telekommunikationsüberwachung. In der Vergangenheit hat sie unter anderem Informationen über das geheime weltweite Überwachungs-

system Echelon recherchiert und veröffentlicht. In Anbetracht solcher Aktivitäten lässt sich sicherlich sagen, dass Frau Schulzki-Haddouti Nachteile infolge einer Vorratsspeicherung der näheren Umstände ihrer Telekommunikation nicht ohne Grund befürchtet. In ihrer Antwort auf die Fragen des Verfassers gab Frau Schulzki-Haddouti an, bereits gegenwärtig in bestimmten Angelegenheiten auf die Nutzung von Telekommunikationsnetzen zu verzichten und stattdessen auf persönliche Gespräche zurückzugreifen. Für den Fall einer generellen Vorratsspeicherung von Telekommunikationsdaten kündigte sie an, im Bereich des Internet nur noch anonym zu kommunizieren und im Übrigen nur noch unbedenkliche Aktivitäten über die Telekommunikationsnetze abzuwickeln. Teilweise würde sie auch auf die Kommunikation per Briefpost ausweichen.

Auch die Hilfsorganisation Misereor gab an, bei ihrer Telekommunikation zu berücksichtigen, welche Staaten den Telekommunikationsverkehr generell aufzeichnen, besonders, wenn es sich um sensible Themenbereiche wie die Menschenrechtsarbeit handele. Gegebenenfalls würden sensible Informationen in persönlichen direkten Gesprächen oder per Briefpost übermittelt, anstatt Telekommunikationsnetze einzusetzen.

Diese Angaben machen deutlich, dass eine Vorratsspeicherung von Telekommunikationsdaten teilweise einen Verzicht auf die Nutzung des Mediums der Telekommunikation zur Folge hätte. Dieser Verzicht könnte weder durch einen Einsatz anonymer Telekommunikation noch durch eine Nutzung alternativer Kommunikationsformen wie Briefkommunikation oder persönliche Gespräche voll ausgeglichen werden, weil diese Möglichkeiten nur in bestimmten Bereichen praktikabel sind. Letztlich würde eine Vorratsspeicherung daher die gesamtgesellschaftliche Kommunikation beeinträchtigen, was wiederum zur Einschränkung politischer Aktivitäten und damit zu gravierenden Nachteilen für unser demokratisches System führen kann.

Wenn 60% der Deutschen darauf vertrauen, dass die Polizei gespeicherte Daten absolut richtig und zuverlässig verwendet[612], handelt es sich dabei möglicherweise nur um die „schweigende Mehrheit". Zu den übrigen 40% gehören möglicherweise

612 Opaschowski, DuD 2001, 678 (679).

gerade solche Personen, die sich politisch engagieren und daher für eine funktionierende Demokratie von besonderer Bedeutung sind. Bereits wenn 40% der Bevölkerung Bedenken im Hinblick auf die korrekte Verwendung ihrer Daten durch die Polizei hätten, begründete dies eine reale Gefahr für unser freiheitliches demokratisches Gemeinwesen[613]. Im Jahr 2003 waren 20% der im Rahmen einer Umfrage befragten Deutschen der Ansicht, es sei besser, vorsichtig zu sein, wenn man in Deutschland seine politische Meinung äußern wolle[614].

Auch außerhalb des öffentlichen Lebens, wo die Funktionsfähigkeit der Demokratie nicht unmittelbar bedroht ist, muss der Einzelne grundsätzlich sicher sein können, seine Grundrechte unbeschwert und frei von Überwachung oder auch nur der Möglichkeit der Überwachung wahrnehmen zu können. Der Mensch ist ein gemeinschaftsbezogenes Wesen, und der Schutz seiner Würde (Art. 1 Abs. 1 GG) verlangt ein gewisses Maß an unbeobachteter Kommunikation mit anderen Personen, beispielsweise in besonderen Notlagen. Der Schutz der Privatsphäre bildet die Grundlage der Handlungsfreiheit[615]. Nur wer sich vor Beobachtung sicher sein kann, kann ohne Druck zur Konformität und zur Anpassung an vorgegebene soziale, gesellschaftliche und moralische Standards handeln[616]. Dementsprechend stellt das Bundesverfassungsgericht in einer neueren Entscheidung – interessanterweise ohne auf die Funktionsfähigkeit der Demokratie abzustellen – allgemein fest: „Es gefährdet die Unbefangenheit der Nutzung der Telekommunikation und in der Folge die Qualität der Kommunikation einer Gesellschaft, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen."[617]

Gerade das Medium der Telekommunikation dient in besonderem Maße der Grundrechtsverwirklichung, so dass sich Überwachungsmaßnahmen in diesem Bereich besonders nachteilig auf die Kommunikation in einer Gesellschaft auswirken. Wie die folgende Aufzählung[618] zeigt, sind gerade die vielfältigen Tätigkeiten auf den „Datenautobahnen" mindestens ebenso reichhaltig wie das „wirkliche" Leben

613 Vgl. BVerfGE 65, 1 (43).

614 Institut für Demoskopie Allensbach: Der Wert der Freiheit, Ergebnisse einer Grundlagenstudie zum Freiheitsverständnis der Deutschen, Oktober/November 2003, www.ifd-allensbach.de/pdf/akt_0406.pdf, 48.

615 Buxel, DuD 2001, 579 (581).

616 Buxel, DuD 2001, 579 (581).

617 BVerfGE 107, 299 (328).

außerhalb von Telekommunikationsnetzen: Surfen im Web (Recht auf informationelle Selbstbestimmung, Art. 1 und 2 GG; Informationsfreiheit, Art. 5 Abs. 1 GG; Fernmeldegeheimnis, Art. 10 Abs. 1 Var. 3 GG), E-Mail-Versand und Internet-Telefonie (Fernmeldegeheimnis, Art. 10 Abs. 1 Var. 3 GG), Elektronische Presse, Chatrooms und Newsgroups (Presse- und Meinungsfreiheit, Art. 5 Abs. 1 GG), Elektronischer Handel, E-Commerce (Berufsfreiheit, Art. 12 GG), virtuelle Kunstausstellungen (Kunstfreiheit, Art. 5 Abs. 3 GG), Recherchen für wissenschaftliche Veröffentlichungen (Forschungsfreiheit, Art 5 Abs. 3 GG), elektronische Beichten (Glaubensfreiheit, Art. 4 GG), Beschwerden bei Behörden mittels E-Mail (Petitionsrecht, Art. 17 GG), virtuelle Demonstrationen (Versammlungsfreiheit, Art. 8 GG), virtuelle „Ortsvereine" (Vereinigungs- und Koalitionsfreiheit, Art. 9 GG; Parteienprivileg, Art. 21 GG), behindertengerechte Internetangebote staatlicher Behörden (Diskriminierungsverbot, Art. 3 Abs. 3 GG).

In den Kommunikationsnetzen werden auch viele private und vertrauliche Gespräche und Tätigkeiten abgewickelt. Gerade was Kommunikationsvorgänge privaten Inhalts anbelangt, so geht die Globalisierung an engen persönlichen Beziehungen zu Familienmitgliedern oder Freunden nicht spurlos vorbei und führt zunehmend zu örtlicher Trennung. Das Bedürfnis nach der Möglichkeit, im Familien- und Freundeskreis vertrauliche Gespräche führen zu können, nimmt dabei nicht ab, sondern eher noch zu, so dass privater Telekommunikation in Zukunft zunehmende Bedeutung zukommen wird.

Was besondere Vertrauensverhältnisse zu Vertretern bestimmter Berufsgruppen angeht, so bieten die neuen Medien ideale Voraussetzungen dafür, sich schnell und anonym jemandem anvertrauen zu können, ohne Konsequenzen befürchten zu müssen. Die Bedeutung dieser Möglichkeit für Menschen in Not ist in der heutigen, von Beziehungsdesintegration geprägten Zeit noch gewachsen. Die lange Liste besonderer Vertrauensverhältnisse, in deren Rahmen sich die Beteiligten zunehmend telekommunikativer Mittel bedienen, umfasst Abgeordnete, Geistliche, Rechtsanwälte, Wirtschaftsprüfer, Steuerberater, Ärzte, Psychotherapeuten, Volksvertreter, Journalisten, aber auch Einrichtungen der Schwangerschaftsberatung und der Drogenhilfe (vgl. § 53 StPO). Damit wird das Fernmeldegeheimnis zunehmend zur

618 Nach Schaar, Sicherheit und Freiheitsrechte (I), 2 ff.

Vorbedingung einer Vielzahl von Vertrauensverhältnissen und seine zunehmende Durchlöcherung zu einer Gefahr für weite Bereiche der Gesellschaft[619].

Auch über die Privatsphäre im engeren Sinne hinaus kann schließlich ein legitimes Interesse an Geheimhaltung bestehen, etwa was das eigene Vermögen angeht oder den Schutz von Geschäftsgeheimnissen[620]. Würde für die Kommunikation in all diesen Situationen nicht das Medium der Telekommunikation genutzt, so würde regelmäßig in einer Wohnung oder einem Geschäftsraum kommuniziert werden, so dass Art. 13 GG einschlägig wäre. Auch tatsächlich werden die Telekommunikationsnetze regelmäßig von abgeschlossenen Räumen aus genutzt, was weiter verdeutlicht, dass die Telekommunikation einer Person oftmals dem Bereich ihrer Privatsphäre zuzuordnen ist. Schon 1983 hat die internationale Konferenz der Datenschutzbeauftragten erklärt, dass die Erfassung von Telekommunikations-Verkehrsdaten das Recht der Unverletzlichkeit der Wohnung berühre[621]. Auch wenn man so weit nicht gehen möchte, so ist die Schutzwürdigkeit von Telekommunikation derjenigen von Gesprächen in einer Wohnung jedenfalls vergleichbar.

Eine Vorratsspeicherung von Telekommunikationsdaten würde unterschiedslos alle Verkehrsdaten erfassen, also auch die Umstände von Kommunikationsvorgängen mit privatem und vertraulichem Inhalt. Damit müssten sich die an solchen Kommunikationsvorgängen Beteiligten stets mit dem Gedanken tragen, dass ihre Kommunikation jederzeit nachvollzogen werden könnte und dass es zur missbräuchlichen Kenntnisnahme dieser Informationen durch Dritte kommen könnte. Es ist daher nicht unwahrscheinlich, dass eine Vorratsspeicherung von Telekommunikationsdaten zu Kommunikationsanpassungen führen würde, dass also auf die Nutzung des Mediums Telekommunikation für private oder vertrauliche Kommunikationsvorgänge teilweise verzichtet würde, ohne dass den Beteiligten immer Alternativen zur Verfügung stünden. Unerwünschte Beeinträchtigungen der gesamtgesellschaftlichen Kommunikation wären die Folge.

Angesichts der besonderen Bedeutung von Vertrauensverhältnissen hat der sächsische Verfassungsgerichtshof entschieden, dass es unzulässig sei, zum Zwecke der

619 Ruhmann/Schulzki-Haddouti, Abhör-Dschungel (I).

620 Ruhmann/Schulzki-Haddouti, Abhör-Dschungel (I).

621 Internationale Konferenz der Datenschutzbeauftragten, Neue Medien (I).

Gefahrenabwehr Daten über unbeteiligte Personen aus Vertrauensverhältnissen zu erheben[622]. Unbeteiligt sind Personen, bei denen nicht aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass von ihnen eine Gefahr ausgeht oder dass sie Nachrichtenmittler eines Störers sind. Erst recht muss all dies im Bereich der Strafverfolgung gelten, die einen verfassungsrechtlich geringeren Stellenwert hat als die unmittelbare Abwehr von Gefahren.

Im Bereich der Telekommunikation dagegen tragen die Normen, die zum Zugriff auf Telekommunikationsdaten ermächtigen, der Bedeutung von Vertrauensverhältnissen nicht oder, wie in § 100h Abs. 2 StPO, nicht ausreichend Rechnung. Zu der neuen Lösung des § 100h Abs. 2 StPO ist kritisch anzumerken, dass die mittelbare Verwertung einer rechtswidrig erlangten Auskunft darin nicht verboten wird[623]. Dadurch besteht für die Behörden stets der Anreiz, unter § 100h Abs. 2 StPO fallende Daten rechtswidrig zur Ermittlung weiterer Beweise zu verwenden, weil diese von dem Verwertungsverbot nicht mehr erfasst sind. Dies stellt deswegen eine gravierende Gesetzeslücke dar, weil sich zumeist erst im Prozess herausstellen wird, ob das ursprüngliche Auskunftverlangen rechtswidrig war. Die Kenntnis der an einer Kommunikation beteiligten Anschlussinhaber oder auch zusätzlich der Verbindungsdaten erlaubt nämlich keine Rückschlüsse darauf, ob beispielsweise ein Vertrauensverhältnis vorlag und wie weit daher „das Zeugnisverweigerungsrecht in den Fällen des § 53 Abs. 1 Satz 1 Nr. 1, 2 und 4 reicht"[624]. Aus diesem Grund ist § 100h Abs. 2 StPO praktisch von geringem Wert. Überdies erscheint die Auswahl der in § 100h Abs. 2 StPO geschützten Vertrauensverhältnisse willkürlich und unvollständig, auch gemessen an den Entscheidungen des Europäischen Gerichtshofs für Menschenrechte und des Bundesverfassungsgerichts.

Für eine Drogenberatungsstelle hat das Bundesverfassungsgericht ausdrücklich entschieden, dass der Schutz von Vertrauensverhältnissen schwerer wiege als das allgemeine Interesse an der Aufklärung von Straftaten[625]. In der Umgehung des Zeugnisverweigerungsrechts durch eine Beschlagnahmeanordnung sah es einen unver-

622 SächsVerfGH, DuD 1996, 429 (439).

623 Gegen ein Verwertungsverbot in einem solchen Fall allerdings BVerfGE 44, 353 (384); für ein umfassendes Verwertungsverbot im Bereich der Art. 1 und 13 GG BVerfGE 109, 279 (331 f. und 377 f.).

624 BR-Drs. 275/02 (Beschluss), 13.

625 BVerfGE 44, 353 (380).

hältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung[626]. Nur wenn im Einzelfall spezifische Anhaltspunkte dafür bestünden, dass Unterlagen zur Verfolgung besonders schwerer Straftaten benötigt werden, sei eine Beschlagnahme zulässig[627]. Diese Erwägungen des Bundesverfassungsgerichts müssen für Eingriffe in den Fernmeldeverkehr erst recht gelten, weil solche Eingriffe – im Unterschied zu einer Beschlagnahme – geheim erfolgen und daher tendenziell schwerer wiegen. Ob damit eine pauschale Erhebung von Verkehrsdaten aus Vertrauensverhältnissen, wie sie mit einer Vorratsspeicherung verbunden wäre, zu vereinbaren ist, erscheint fragwürdig.

Wegen der Vielzahl von privilegierten Kommunikationsvorgängen, die über wechselnde Anschlüsse von Telefon, Fax, E-Mail, WWW usw. abgewickelt werden, ist es nicht möglich, solche Kommunikationsvorgänge zuverlässig von einer Vorratsspeicherung auszunehmen. Zeugnisverweigerungsberechtigte Stellen pauschal von einer Speicherung auszunehmen, könnte einerseits dazu führen, dass nicht privilegierte Kommunikationsvorgänge, etwa Privatgespräche von Rechtsanwälten (§ 53 Abs. 1 Nr. 3 StPO), die über den beruflichen Telefonanschluss geführt würden, von einer Überwachung ausgenommen wären. Andererseits wäre etwa ein Gespräch des Bruders eines Beschuldigten, das von einer öffentlichen Telefonzelle aus geführt wird, nicht geschützt.

Daraus ergibt sich, dass man bei sämtlichen Verkehrsdaten von der Möglichkeit ausgehen muss, dass es sich um Daten über besondere Vertrauensverhältnisse handelt. Die einzige Möglichkeit eines wirksamem Schutzes von Vertrauensverhältnissen im Bereich der Telekommunikationsnetze ist daher ein generell hohes Schutzniveau. Eine generelle Vorratsspeicherung von Telekommunikations-Verkehrsdaten ist mit einem wirksamen Schutz von Vertrauensverhältnissen demnach nicht in Einklang zu bringen.

Die Pläne zur Einführung einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten sind auch im Zusammenhang mit anderen Bestrebungen zur Verbesserung der Sicherheit zu sehen. In der jüngeren Vergangenheit Deutschlands wurden etwa die Instrumente der Rasterfahndung, der akustischen Wohnraum-

626 BVerfGE 44, 353 (380).

überwachung und der Ortung von Mobiltelefonen eingeführt. Einen Blick in die mögliche Zukunft erlauben die schon heute existierenden technischen Möglichkeiten: So gibt es Software, die von Überwachungskameras aufgenommene Bilder zeitgleich auswertet und bei „abnormalen Bewegungen" Alarm schlägt[628]. Auch Bewegungen bestimmter Personen lassen sich so analysieren, dass für jede Person ein unverwechselbares Bewegungsprofil entsteht und dass Personen folglich für entsprechend eingerichtete Überwachungssysteme überall und schon von weitem an ihrem Laufstil erkennbar sind[629]. Aufnahmen, die Überwachungskameras von Gesichtern anfertigen, lassen sich unter Anwendung eines modernen biometrischen Verfahrens automatisch analysieren und mit einem Datenbestand – etwa aus Fahndungsfotos gewonnen – vergleichen. Das derartige Auffinden und Überwachen von Personen findet in Städten Großbritanniens und der USA bereits statt[630].

Stets lassen sich die aus den unterschiedlichen Quellen gewonnenen Daten mit Hilfe von Computern ohne Weiteres verknüpfen, so dass sich der Bürger insgesamt einem immer dichter werdenden Netz von Überwachungs-, Kontroll- und Überprüfungsmöglichkeiten ausgesetzt sieht[631], das ihn veranlassen kann, jedes Verhalten zu meiden, mit dem er sich verdächtig machen könnte. Auch wenn jeder einzelne Eingriff für sich genommen eine gewisse Berechtigung haben mag, so dürfen die gesellschaftlichen Auswirkungen einer insgesamt zunehmenden Überwachung der Bevölkerung nicht unbeachtet bleiben. Leider ist kaum messbar, wie sehr das unbefangene Gebrauchmachen von Grundrechten in einer Demokratie unter staatlichen Überwachungsmöglichkeiten leidet. Es spricht allerdings einiges für die Annahme, dass der Schaden für unsere demokratische Gesellschaft infolge einer zunehmenden Überwachung des Bürgers durch den graduellen Effizienzgewinn, den viele Befugniserweiterungen bestenfalls bewirken können, nicht aufgewogen werden kann. Jedenfalls muss bei der Abwägung von Sicherheit und Freiheit heutzutage besonders vorsichtig vorgegangen und jede einzelne, für sich genommen vielleicht unbedeutende Regelung in ihrer Gesamtwirkung bedacht werden[632].

---

627 BVerfGE 44, 353 (379).

628 Spiegel Online: Software warnt vor Verbrechen, 01.05.2002, www.spiegel.de/wissenschaft/mensch/0,1518,194325,00.html.

629 Spiegel Online: Übeltäter verraten sich durch ihren Gang, 05.11.2001, www.spiegel.de/wissenschaft/mensch/0,1518,166107,00.html.

630 Achelpöhler/Niehaus, DuD 2002, 731 (734) für die Stadt Tampa in Florida.

631 DSB-Konferenz, Zehn Jahre nach dem Volkszählungsurteil (I).

632 Ähnlich schon BVerfGE 34, 238 (249); vgl. auch Weßlau, ZStW 113 (2001), 681, 691.

(vii) Kontraproduktive Effekte

Auch die kontraproduktiven Effekte auf das Kriminalitätsniveau, die mit der insgesamt zunehmenden Ausweitung von Eingriffsbefugnissen einher gehen können, sind zu beachten[633]: Vieles spricht für die Annahme, dass die absolute Achtung der Menschenwürde einer Gemeinschaft nach innen und nach außen zu einer moralischen Anziehungs- und Überzeugungskraft verhilft[634], welche auf lange Sicht einzelne Vorteile, die durch exzessive Eingriffe erzielt werden könnten, überwiegt. Wissenschaftler haben als wichtiges Motiv von Terroristen die Erfahrung von Demütigung ausgemacht[635]. Schädliche Auswirkungen kann auch eine ausländerfeindliche Einstellung oder ein Klima des Misstrauens haben[636]. Gerade dies sucht ein Rechtsstaat zu vermeiden. Die Aufgabe rechtsstaatlicher Prinzipien ist demgegenüber geeignet, Fundamentalisten und Extremisten im In- und Ausland Auftrieb zu geben[637]. Nur der entschiedene Eintritt für Menschenrechte auch in Krisenzeiten sichert die Unterstützung der öffentlichen Meinung im In- und Ausland[638]. Die Einigkeit über die Achtung der Rechte anderer stärkt soziale Normen in der Gesellschaft und reduziert so zugleich das Maß an Kriminalität[639]. Maßnahmen staatlicher Überwachung, die diesen sozialen Zusammenhalt gefährden können, sollten daher gerade im Interesse der Sicherheit sehr genau überlegt sein.

Des Weiteren geht mit der Erweiterung staatlicher Ermittlungsbefugnisse auf dem Gebiet der Telekommunikation stets auch die verstärkte Entwicklung von Gegenmaßnahmen, insbesondere von Verschlüsselungs- und Anonymisierungstechniken einher[640]. Es ist zu erwarten, dass die Einführung einer Vorratsspeicherung von Telekommunikationsdaten über die schon bisher vorsichtigen Kreise organisierter Kriminalität hinaus auch bei Normalnutzern ein Problembewusstsein entstehen lassen

633 Schieder, Anti-Terrorist Measures and Human Rights (I).

634 Hassemer, Freiheitliches Strafrecht, 173.

635 Rötzer, Florian: Armut ist keine Ursache für den Terrorismus, Telepolis, Heise-Verlag, 01.08.2002, www.heise.de/tp/-deutsch/inhalt/co/13015/1.html; Limbach, Jutta: Ist die kollektive Sicherheit Feind der individuellen Freiheit? 10.05.2002, www.zeit.de/reden/
Deutsche%20Innenpolitik/200221_limbach_sicherheit.html.

636 Weichert, Terror und Informationsgesellschaft (I): „So wird die Terroristenbekämpfung selbst zum Sicherheitsrisiko".

637 Schieder, Anti-Terrorist Measures and Human Rights (I); Schwimmer, Anti-terrorist measures and Human Rights (I).

638 Schwimmer, Anti-terrorist measures and Human Rights (I).

639 Hassemer, Strafen im Rechtsstaat, 262.

640 Hamm, NJW 2001, 3100 (3101).

würde und dass dadurch auch in diesen Kreisen verstärkt Möglichkeiten zur anonymen und verschlüsselten Netznutzung eingesetzt würden[641]. Beispielsweise könnten sich Firmen zu Maßnahmen des technischen Selbstschutzes genötigt sehen, wenn sie den Schutz ihrer Geschäftsgeheimnisse und Kontakte auf andere Weise nicht mehr gewährleisten können. Auf dem Gebiet der Verschlüsselung beobachten die Strafverfolgungsbehörden bereits jetzt, dass von diesen Möglichkeiten zunehmend Gebrauch gemacht wird und dass die Nutzung von Verschlüsselungstechniken mit steigendem Benutzerkomfort der verfügbaren Werkzeuge zunimmt[642]. Dasselbe wird auf dem Gebiet von Anonymisierungstechniken, deren Entwicklung sich momentan teilweise noch in den Kinderschuhen befindet, zu beobachten sein.
Wenn der Staat mit einer erweiterten Telekommunikationsüberwachung indirekt die anonyme Telekommunikation fördert, dann schneidet er sich mittelfristig selbst in Fällen größter Gefahr die Möglichkeit eines Abhörens ab. Selbst die schon bisher zulässige Telekommunikationsüberwachung in Einzelfällen würde damit unmöglich. Ähnlich wie im Falle des Volkszählungsgesetzes[643] sind zu weite Eingriffsbefugnisse daher kontraproduktiv, weil sie die Überwachung der Telekommunikation letztlich insgesamt in Frage stellen[644]. Vor dem Hintergrund, dass die Eingriffsbehörden nicht müde werden, die Bedeutung der Telekommunikationsüberwachung für die Wahrnehmung ihrer Aufgaben zu betonen, stimmt dies bedenklich. Im Rahmen der Verhältnismäßigkeitsprüfung ist dieser kontraproduktive Effekt negativ zu bewerten.
Eine Minderung der Effektivität bestehender Befugnisse ist auch im Hinblick auf die Kosten einer Vorratsspeicherung für die Wirtschaft abzusehen[645]: Internationale Telekommunikationskonzerne zentralisieren ihre Informationsverarbeitung schon heute zunehmend und verlagern sie beispielsweise in die USA. Dieser Trend würde durch eine Verpflichtung zu einer kostenträchtigen Vorratsspeicherung erheblich beschleunigt. Die Speicherung von Verkehrsdaten im Ausland würde nicht nur dazu führen, dass eine nationale Pflicht zur Vorratsspeicherung leer laufen würde. Sie würde außerdem die bestehenden Zugriffsbefugnisse im Einzelfall gefährden, weil auf Verkehrsdaten im Ausland in der Praxis nicht oder nur nach langer Zeit zugegrif-

641 Lenz, Karl-Friedrich: Stellungnahme zur Anhörung der Kommission über die Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität, europa.eu.int/
ISPO/eif/InternetPoliciesSite/Crime/Comments/kf_lenz.html.

642 Zwingel (Leiter des BKA-Referates IT-Nutzung und Telekommunikationsüberwachung), Technische Überwachungsmaßnahmen aus Sicht der Polizei, 37 (42).

643 BVerfGE 65, 1 (64 und 50).

644 Bonitz, Sylvia (MdB) in Bundestag, Öffentliche Anhörung zum Thema Cyber-Crime/TKÜV (I), 47.

fen werden könnte. Dadurch kann die Einführung einer Vorratsspeicherung letztlich dazu führen, dass weniger Verkehrsdaten verfügbar wären als zuvor.

(viii) Zwischenergebnis

Zusammenfassend ist festzuhalten, dass die Aussagekraft von Verkehrsdaten, gemessen an ihrer Nutzbarkeit und Verwendungsmöglichkeit, äußerst hoch ist und mindestens der Aussagekraft von Kommunikationsinhalten entspricht. Zwar kann mangels einschlägiger Forschung nicht in seriöser Weise angegeben werden, mit welcher Wahrscheinlichkeit eine Vorratsspeicherung wie viele Fehlentscheidungen, Missbräuche und Mitwirkungshemmungen seitens der Bürger hervorrufen würde. Dies hindert aber nicht die Berücksichtigung dieser Faktoren, denn auch ein möglicher Nutzen einer Vorratsspeicherung ist nicht durch konkrete Daten belegt. Anhand von Erfahrungswerten, die nur den öffentlich bekannten Ausschnitt aller Fälle betreffen können, lässt sich jedenfalls sagen, dass die Gefahr von Fehlentscheidungen, Missbräuchen und Mitwirkungshemmungen infolge einer Vorratsspeicherung real und nicht nur unerheblich ist.

Fraglich ist, ob sich argumentieren lässt, dass wesentliche Nachteile für die Betroffenen nicht schon mit der Speicherung von Verkehrsdaten, sondern erst infolge eines anschließenden staatlichen Zugriffs darauf drohten und dass diesen Nachteilen daher durch eine Beschränkung der staatlichen Zugriffsrechte hinreichend begegnet werden könne[646]. Dieser Argumentation ist entgegenzuhalten, dass Zugriffsbeschränkungen nur Nachteile infolge eines legalen Zugriffs auf Verkehrsdaten abwenden können, etwa Nachteile infolge staatlicher Fehlurteile. Demgegenüber besteht selbst dann, wenn der Zugriff auf gespeicherte Daten verboten ist, die Gefahr von Missbräuchen der Daten von staatlicher oder privater Seite sowie das Risiko von Kommunikationsanpassungen auf Seiten der Betroffenen. Diesen für die Betroffenen und die Gesellschaft insgesamt wesentlichen Nachteilen lässt sich allein dadurch effektiv vorbeugen, dass bereits die Vorratsspeicherung von Telekommunikationsdaten unterbleibt. Es wäre daher unzutreffend, zu behaupten, dass den Betroffenen aufgrund einer bloßen Datenvorhaltung keine Nachteile drohten.

---

645 Zum Folgenden APIG, Communications Data, 26 f.

646 Ähnlich BVerfGE 100, 313 (384) für die vorbereitende Erfassung von Telekommunikation durch den BND.

(gg) Zusammenfassung: Eingriffstiefe und negative Auswirkungen einer Vorratsspeicherung von Telekommunikationsdaten

Unabhängig von der Ausgestaltung einer Vorratsspeicherung von Telekommunikationsdaten im Einzelnen wäre die Beeinträchtigung der betroffenen Grundrechtsträger außerordentlich schwerwiegend. Dies ergibt sich aus folgenden Umständen:

- Nicht nur einzelne Personen, sondern grundsätzlich jeder Bürger wäre von der Aufzeichnung seines Telekommunikationsverhaltens betroffen.

- In vielen Fällen können Personen die Nutzung von Telekommunikationsnetzen nicht oder nur unter unzumutbaren Nachteilen meiden. Dementsprechend könnte im Fall einer Vorratsspeicherung von Telekommunikationsdaten einer Überwachung des eigenen Kommunikationsverhaltens oft nicht entgangen werden[647].

- Nicht nur vermutete Straftäter oder Störer oder deren vermutete Kontaktpersonen wären betroffen, sondern jeder Telekommunikationsnutzer, ohne dass er einen Grund für die Überwachung geliefert hat[648] oder in einer besonderen Nähebeziehung zu kriminellem Verhalten steht, dessentwegen die Vorratsspeicherung vorgenommen wird. Die Aufzeichnung wäre weder sachlich auf gefahrenträchtige Situationen noch zeitlich auf Sondersituationen noch auf Fälle begrenzt, in denen Anhaltspunkte für das Vorliegen oder Bevorstehen einer konkreten Straftat oder Gefahr gegeben sind.

- Jede Inanspruchnahme der Medien Festnetztelefon, Mobiltelefon, Fax, SMS, E-Mail, WWW usw. würde nach Beteiligten, Zeit, Ort usw. festgehalten, ohne dass es eine Eingriffsschwelle gäbe. Eine Einzelfallprüfung mit Verhältnismäßigkeitskontrolle fände nicht statt. Betroffen wären auch sämtliche Vertrauensverhältnisse und Ge-

---

647 Vgl. dazu MVVerfG, LKV 2000, 149 (156).

648 Zur rechtlichen Bewertung solcher Maßnahmen vgl. BVerfGE 100, 313 (383) zum G10: „Entgegen der Auffassung des Beschwerdeführers zu 1) folgt die Unverhältnismäßigkeit der Überwachungs- und Aufzeichnungsbefugnisse und der gesetzlich vorgesehenen Maßnahmen nicht schon aus dem Fehlen von Einschreitschwellen [...] Die unterschiedlichen Zwecke rechtfertigen es [...], daß die Eingriffsvoraussetzungen im G 10 anders bestimmt werden als im Polizei- oder Strafprozeßrecht. Als Zweck der Überwachung durch den Bundesnachrichtendienst kommt wegen der Gesetzgebungskompetenz des Bundes aus Art. 73 Nr. 1 GG nur die Auslandsaufklärung im Hinblick auf bestimmte außen- und sicherheitspolitisch relevante Gefahrenlagen in Betracht"; SächsVerfGH, DuD 1996, 429 (432): Generell gegen unbeteiligte Dritte mit informationellen Eingriffsmaßnahmen vorzugehen, wäre mit dem freiheitlichen Menschenbild der Verfassung unvereinbar; L/D³-Lisken, C 40: Heimliche Vorfeldbefugnisse sind nur den Ämtern für Verfassungsschutz gestattet; ders., C 31: Inanspruchgenommene Nichtbeteiligte müssen ansonsten in irgendeiner besonderen Nähe zu der polizeilichen Situation stehen; L/D³-Rachor, F 182: Vorfeldbefugnisse heben das Verhältnismäßigkeitsprinzip aus den Angeln; L/D³-Bäumler, J 546: Die Verarbeitung von Daten über Nichtverdächtige oder Nichtbeteiligte ist unzulässig; ders., J 607 und 671: Zu repressiven Zwecken dürfen Daten nur über Verdächtige gespeichert werden; Albers, ZRP 1990, 147 (149): Nichtstörer dürfen jedenfalls nicht in gleichem Maße in Anspruch genommen werden wie Störer.

schäftsbeziehungen. Entsprechend der fehlenden Eingriffsschwelle würde nur ein verschwindend geringer Teil der gespeicherten Daten später tatsächlich benötigt[649]. Es würde damit im Wesentlichen keine unbeobachtete Telekommunikation mehr geben[650].

- Erfasst würden nicht etwa nur öffentlich zugängliche Daten oder Adressdaten, sondern unmittelbar die Privatsphäre betreffende Daten über das Verhalten des Einzelnen[651]. Die Aussagekraft der Daten ist extrem hoch. Eine missbräuchliche Auswertung könnte daher großen Schaden anrichten und beispielsweise zur öffentlichen Diskreditierung oder zum Verlust der beruflichen Stellung von Personen führen.

- Verkehrsdaten würden nicht nur aus öffentlichen oder geschäftlichen Räumen erhoben. Vielmehr werden Telekommunikationsnetze von Privatpersonen regelmäßig im Schutz der eigenen Wohnung, also innerhalb ihrer räumlichen Privatsphäre, genutzt. Das Verhalten der Bürger in diesem Bereich unterliegt ansonsten nur ausnahmsweise staatlichem Zugriff (vgl. Art. 13 GG).

- Die Verkehrsdaten würden nicht etwa als Akten, sondern in maschineller Form gespeichert. Sie können daher potenziell unbegrenzt gespeichert, abgerufen, übermittelt, vervielfältigt oder mit anderen Daten verknüpft werden.

- Verkehrsdaten würden bei einer Vielzahl verschiedener Unternehmen dezentral gespeichert werden und zwar in vielen Fällen auf Datenverarbeitungsanlagen, die mit Telekommunikationsnetzen verbunden wären. Beides erhöht die Gefahr, dass missbräuchlich auf gespeicherte Verkehrsdaten zugegriffen wird.

- Verkehrsdaten würden nicht anonym oder nur zur statistischen Nutzung gespeichert, sondern sie wären dazu bestimmt, für den Verwaltungsvollzug eingesetzt zu werden. Ihre Speicherung und staatliche Verwendung könnte daher einschneidende Folgen für die Betroffenen haben, bis hin zum lebenslänglichen Freiheitsentzug, unter Umständen auch zu Unrecht aufgrund eines falschen Verdachts.

- Die Daten würden nicht offen erhoben, sondern im Geheimen. Dadurch könnten die Betroffenen keine rechtzeitige Überprüfung der Richtigkeit der Daten oder der

---

649 Vgl. dazu BVerfGE 109, 279 (354); MVVerfG, LKV 2000, 149 (153).

650 Vgl. Bäumler, zitiert bei Wagner, Marita: Intimsphäre - lückenlos überwacht? Telepolis, Heise-Verlag, 28.06.2002, www.heise.de/tp/deutsch/inhalt/te/12813/1.html: Der Datenschutz für Internet und Telekommunikation würde fast vollkommen ausgehebelt.

651 Vgl. dazu L/D³-Bäumler, J 742: In aller Regel ist die Speicherung von das Privatleben oder die Persönlichkeit betreffenden Daten über Personen, die weder Verdächtige noch Störer sind oder waren, unverhältnismäßig.

Rechtmäßigkeit des Zugriffs veranlassen[652]. Eine Überprüfung der Richtigkeit der Daten ist den Betroffenen angesichts der enormen Datenmassen realistischerweise ohnehin nicht möglich.

- Die Daten würden nicht etwa durch die Betroffenen persönlich angegeben, sondern unabhängig von deren Willen und deren Kenntnis automatisch aufgezeichnet und gegebenenfalls an Behörden weiter übermittelt.

- Im Gegensatz zu bisher bekannten Maßnahmen würden nicht nur ursprünglich zu einem anderen Zweck erfasste Daten auf Vorrat gespeichert, bei denen wegen eines früheren Verfahrens eine erhöhte Wahrscheinlichkeit besteht, dass sie in Zukunft erneut benötigt werden. Vielmehr erfolgt bei einer Vorratsspeicherung von Verkehrsdaten bereits die Erhebung ohne konkreten Anlass[653]. Der Bürger würde also rein vorsorglich überwacht[654].

- Den zuständigen Behörden entstünden durch Zugriffe auf die gespeicherten Daten kaum Kosten, und es wäre kaum Personal nötig. Damit entfallen faktische Begrenzungen der Eingriffshäufigkeit, die bei traditionellen Befugnissen stets bestanden[655].

- Mit der Einführung einer Vorratsspeicherung von Telekommunikations-Verkehrsdaten sind gravierende Änderungen und Einschränkungen des Kommunikationsverhaltens zu befürchten, besonders auf Seiten regierungskritischer Personen, deren Aktivitäten in einer Demokratie besonders wichtig sind.

- Es würde zu Gegenmaßnahmen auf Seiten der Telekommunikationsnutzer und der Telekommunikationsunternehmen kommen. Dadurch könnten Maßnahmen der Telekommunikationsüberwachung selbst bei Vorliegen eines konkreten Verdachts unmöglich werden.

Abhängig von der Ausgestaltung der Regelung im Einzelnen können sich noch weiter gehende Belastungen ergeben:

- Wenn den Behörden ein Online-Zugriff auf die Datenbestände eingeräumt würde, fiele auch die faktische Begrenzung der Anzahl von Eingriffen durch den bürokratischen, mit Anfragen verbundenen Aufwand weg. Zugriffe blieben selbst vor den Telekommunikationsunternehmen geheim, was eine Rechtmäßigkeitskontrolle

652 Vgl. dazu SächsVerfGH, JZ 1996, 957 (963).

653 Vgl. zu dieser Unterscheidung L/D³-Bäumler, J 537 f.

654 DSB-Konferenz, Vorratsspeicherung (I).

655 Vgl. dazu Albrecht/Arnold/Demko/Braun, Rechtswirklichkeit und Effizienz der Telekommunikationsüberwachung, 192, wonach das das Ausmaß an Telefonüberwachung fiskalisch weit mehr begrenzt wird als durch das Gesetz.

durch diese ausschließt. Außerdem würden solche Schnittstellen eine große Angriffsfläche für Hacker bieten.

- Der Zugriff kann rechtlich auf die Verkehrsdaten solcher Personen beschränkt sein, die aufgrund bestimmter, bereits bekannter Tatsachen als Täter einer Straftat oder Verursacher einer Störung in Betracht kommen. Der Zugriff kann sich aber auch auf mögliche Nachrichtenmittler oder gar auf jede Person erstrecken. Abhängig von der Zugriffsschwelle kann auch eine Durchsuchung ganzer Datenbestände nach bestimmten Merkmalen möglich sein, um Verdachtsmomente überhaupt erst zu gewinnen, ähnlich dem Verfahren der Rasterfahndung. Unter Umständen wäre die Erstellung von Bewegungsbildern, Interessenprofilen, die Abbildung sozialer Beziehungen und die Erstellung weitgehend vollständiger Persönlichkeitsabbilder zulässig.

- Die Zugriffsschwelle kann niedrig ausgestaltet sein, etwa wenn bereits tatsächliche Anhaltspunkte oder polizeiliche Erfahrungswerte, die für das Vorliegen einer beliebigen Straftat oder Gefahr sprechen, genügen und nicht nur der auf konkreten Tatsachen im einzelnen Fall beruhende Verdacht einer im Einzelnen bestimmten schweren Straftat oder Gefahr.

- Wenn nicht nur Individualkommunikation, sondern auch der Abruf öffentlich zugänglicher Informationen über Telekommunikationsnetze – insbesondere das Internet – aufgezeichnet würde, ließen sich auch das Informationsverhalten und die Interessen einzelner Personen und der Bevölkerung insgesamt in weitem Umfang überwachen und auswerten.

- Wenn der Standort eines Mobiltelefons nicht nur bei dessen Benutzung zum Telefonieren, sondern stets aufgezeichnet würde, ließen sich die Bewegungen der Benutzer von Mobiltelefonen nachvollziehen und überwachen.

- Wenn auch ausländischen Staaten Zugriff auf die Datenbestände eröffnet würde, wäre nicht gewährleistet, dass der Zugriff auf die Daten und die Nutzung der Daten durch den ausländischen Staat unter denselben grundrechtssichernden Bedingungen erfolgen wie sie in Deutschland bestehen mögen.

-

(hh) Ergebnis

Wie gezeigt, lassen sich sowohl die positiven wie auch die negativen Auswirkungen, die eine Vorratsspeicherung von Telekommunikationsdaten hätte, auf der Basis der

gegenwärtigen Erkenntnisse nicht sicher beurteilen. Auch ohne die experimentelle Einführung einer solchen Regelung ließen sich die maßgeblichen Tatsachen aber durch Auswertungen und Untersuchungen in vielerlei Hinsicht klären. Weil eine Vorratsspeicherung von Telekommunikationsdaten zu schweren und irreparablen Einbußen auf Seiten der Betroffenen führen könnte, ist der Gesetzgeber grundsätzlich verpflichtet, die ihm zugänglichen Erkenntnisquellen vor Einführung einer Vorratsspeicherung auszuschöpfen.

Vor Klärung der für die Beurteilung der Angemessenheit maßgeblichen Tatsachen ist die Einführung einer Vorratsspeicherung von Telekommunikationsdaten nur zulässig, wenn sie ausnahmsweise zum Schutz vor hinreichend wahrscheinlichen Gefahren für wichtige Rechtsgüter erforderlich ist und die beeinträchtigten Rechtsgüter dahinter zurücktreten müssen. Wie dargelegt, wäre ein erweiterter Zugriff auf Telekommunikations-Verkehrsdaten vorwiegend im Rahmen der Strafverfolgung von Nutzen. Im Gegensatz zur Netzkriminalität betreffen die allgemeinen Kriminalitätsrisiken auch höchstwertige Rechtsgüter. Die allgemeine Eignung einer Grundrechtsbeschränkung zur Erleichterung der Strafverfolgung kann jedoch noch nicht genügen, um eine besondere Dringlichkeit zu begründen, die ein sofortiges Handeln erforderlich macht. Gegen eine besondere Dringlichkeit einer Vorratsspeicherung von Telekommunikationsdaten spricht auch, dass der Gesetzgeber die Einführung einer Vorratsspeicherung über lange Zeit abgelehnt hat. Zudem lässt eine generelle Verkehrsdatenspeicherung den Schutz von Rechtsgütern nur in wenigen und regelmäßig wenig bedeutenden Einzelfällen erwarten. Sie kann sogar in erheblichem Maße kontraproduktiv wirken.

Die Einführung einer Vorratsspeicherung von Telekommunikationsdaten ohne vorheriges Ausschöpfen der verfügbaren Erkenntnisquellen kann daher nicht als ausnahmsweise zum Schutz wichtiger Rechtsgüter erforderlich angesehen werden. Erst recht nicht müssen die beeinträchtigten Rechtspositionen hinter das Vollzugsinteresse zurücktreten, da eine Vorratsspeicherung unabsehbar große Schäden für die betroffenen Grundrechtsträger und für die gesellschaftliche Kommunikation insgesamt befürchten lässt. Angesichts dessen ist den Betroffenen die experimentelle Einführung einer Vorratsspeicherung unzumutbar. Der Gesetzgeber ist stattdessen verpflichtet, zunächst die ihm bereits jetzt zugänglichen Erkenntnisquellen auszuschöpfen.

Wägt man die verfassungsrechtlichen Interessen auf der Grundlage bisheriger Erkenntnisse gegeneinander ab, so ergibt sich, dass der zu erwartende Nutzen einer Vorratsspeicherung von Telekommunikations-Verkehrsdaten in einem deutlichen Missverhältnis zu den damit verbundenen Nachteilen für die Betroffenen und die Gesellschaft insgesamt steht[656]. Während der drohende Schaden für unser demokratisches Gemeinwesen unabsehbar groß wäre, ist der zu erwartende Zusatznutzen einer Vorratsspeicherung von Telekommunikationsdaten insgesamt gering. Eine Vorratsspeicherung von Telekommunikations-Verkehrsdaten lässt den Schutz von Rechtsgütern nur in wenigen und regelmäßig wenig bedeutenden Einzelfällen erwarten, ohne dass mit einem dauerhaften, negativen Einfluss auf das Kriminalitätsniveau zu rechnen wäre. Etwas anderes lässt sich auf der Grundlage der gegenwärtigen Erkenntnisse nicht vertretbar annehmen, so dass der Gesetzgeber seinen Beurteilungsspielraum in verfassungswidriger Weise überschreiten würde, wenn er eine Vorratsspeicherung von Telekommunikationsdaten gleichwohl anordnete. Dass nähere Untersuchungen der maßgeblichen Tatsachen an diesem Ergebnis etwas ändern könnten, ist nicht zu erwarten.

---

656 Artikel-29-Gruppe der EU, Stellungnahme 5/2002 (I); Bäumler/v. Mutius-Bäumler, Anonymität im Internet, 8; BfD, 19. Tätigkeitsbericht, BT-Drs. 15/888, 78; BITKOM: Stellungnahme zur Gesetzesinitiative des Bundesrates vom 31.05.2002 (BR-Drs. 275/02), 12.08.2002, www.bitkom.org/files/documents/Position_BITKOM_Vorratsdatenspeicherung_u.a._12.08.2002.pdf, 10; Covington & Burling, Memorandum (I), 3; Bundesregierung in BT-Drs. 13/4438, 39; Dix, Alexander, zitiert bei LDA Bbg.: Datenschutzbeauftragte kritisieren Entwurf für neues Telekommunikationsgesetz, 21.11.2003, www.lda.brandenburg.de/sixcms/detail.php?id=112968&template=lda_presse; DSB-Konferenz, Vorratsspeicherung (I); DSB-Konferenz, Datenschutzbeauftragte des Bundes und der Länder: Entschließung zur systematischen verdachtslosen Datenspeicherung in der Telekommunikation und im Internet der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25.10.2002, BT-Drs. 15/888, 199; eco, Electronic Commerce Forum e.V., Verband der deutschen Internetwirtschaft: Vorratsdatenspeicherung ist verfassungswidrig! Pressemitteilung vom 17.12.2003, www.eco.de/servlet/PB/menu/1236462_pcontent_l1/content.html; Empfehlung des Europäischen Parlaments zu der Strategie zur Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität (2001/2070(COS)) vom 06.09.2001, Dokument Nr. T5-0452/2001; EDSB-Konferenz, Europäische Datenschutzbeauftragte: Statement at the International Conference in Cardiff (09.-11.09.2002) on mandatory systematic retention of telecommunication traffic data, BT-Drs. 15/888, 176; EDSB-Konferenz, Europäische Datenschutzbeauftragte: Statement at the International Conference in Athens (10.-11.05.2001) on the retention of traffic data by Internet Service Providers (ISP's), BT-Drs. 15/888, 178; EDSB-Konferenz, Europäische Datenschutzbeauftragte: Statement at the International Conference in Stockholm (06.-07.04.2000) on the retention of traffic data by Internet Service Providers (ISP's), BT-Drs. 14/5555, 211; GDD, Gesellschaft für Datenschutz und Datensicherung e.V.: Bundesratsinitiative zur Vorratsdatenspeicherung verstößt gegen elementare Grundsätze des Datenschutzes, Pressemitteilung vom 05.06.2002, www.rainer-gerling.de/aktuell/-vorrat.html; Krader, DuD 2001, 344 (347); Kugelmann, DuD 2001, 215 (220); Queen Mary (University of London), Studie über Netzkriminalität (I): „arguable"; Schaar, Forderungen an Politik und Gesetzgebung (I); Schaar, zitiert bei Hänel, Oberster Datenschützer kritisiert TKG-Novelle (I); Schaar, Retention (I), 4; Uhe/Herrmann, Überwachung im Internet (I), 164 m.w.N.; Unabhängiges Landeszentrum für den Datenschutz Schleswig-Holstein, Tätigkeitsbericht 2002, LT-Drs. 15/1700, 112; ULD-SH, Sichere Informationsgesellschaft (I), Punkt 6; Vertreterin des Bundesministeriums für Wirtschaft und Arbeit für die Bundesregierung, zitiert in der Niederschrift über die Sitzung des Rechtsausschusses des Bundesrates vom 12.11.2003, 16, www.spindoktor.de/vorratsspeicherung1103.pdf; Weichert, Bekämpfung von Internet-Kriminalität (I); Weßlau, ZStW 113 (2001), 681 (703); für Bestandsdaten schon Rieß, DuD 1996, 328 (333); vgl. auch BAG, 1 ABR 21/03 vom 29.06.2004, Absatz-Nrn. 38 ff., www.bundesarbeitsgericht.de zur Unverhältnismäßigkeit einer allgemeinen Videoüberwachung und -aufzeichnung am Arbeitsplatz.

(b) Angemessenheit eines Vorratsspeicherungsrechts für Telekommunikationsunternehmen

Als Alternative zur Einführung einer obligatorischen Vorratsspeicherung kommt die Ermächtigung von Telekommunikationsunternehmen in Betracht, die Verkehrsdaten ihrer Kunden freiwillig länger als für ihre Zwecke erforderlich speichern zu dürfen[657]. In den USA liegt es beispielsweise im Ermessen der Telekommunikationsunternehmen, wie lange sie die Verkehrsdaten ihrer Kunden speichern[658]. Offenbar werden Daten dort oft auf freiwilliger Basis länger gespeichert als es für Abrechnungszwecke erforderlich ist, was für die dortigen Eingriffsbehörden von Vorteil ist. Diese tragen vor, die von den Unternehmen freiwillig gespeicherten Daten deckten sich weitgehend mit den zu staatlichen Zwecken benötigten[659]. Für die Unternehmen kann dieses Arrangement mit weit geringeren Kosten verbunden sein, weil die Entscheidung über eine Vorratsspeicherung in ihrem Ermessen liegt.

Auch für die Kunden ist ein Vorratsspeicherungsrecht für Telekommunikationsunternehmen gegenüber einer generellen Vorratsspeicherung vorzugswürdig, solange Höchstspeicherfristen vorgesehen sind. Zum einen wird eine freiwillige Vorratsspeicherung wegen der Kosten einer Datenvorhaltung regelmäßig in geringerem Umfang erfolgen als es den Unternehmen erlaubt ist. Zum anderen haben Kunden die Möglichkeit, auf spezielle Dienste zuzugreifen, die ausdrücklich auf die Speicherung von Verkehrsdaten verzichten. Derartige Dienste können etwa im Rahmen besonderer Vertrauensverhältnisse oder zum Schutz von Geschäftsgeheimnissen eingesetzt werden.

Solche Dienste werden allerdings größtenteils nur gegen Bezahlung angeboten, während die Benutzung kostenloser Dienste regelmäßig ein gewisses technisches Vorverständnis erfordert. Mittellose und unbedarfte Personen könnten daher von

---

657 EuroISPA, Internet Service Providers' Association (Europe) / US ISPA, Internet Service Providers' Association (U.S.A.): Position on the Impact of Data Retention Laws on the Fight against Cybercrime, 30.09.2002, www.euroispa.org.

658 Richard, Mark: Statement of the United States of America presented at the EU Forum on Cybercrime in Brussels, 27.11.2001, cryptome.org/eu-dataspy.htm; ETNO / EuroISPA / ECTA: The Implications of „Data Retention" in Article 15.1 of the Common Position on the Electronic Communications Data Protection Directive, Joint Industry Memo in view of the 2nd Reading of the Cappato Report, 16.04.2002, www.euroispa.org/docs/160402_dataretent.doc; EuroISPA, Internet Service Providers' Association (Europe) / US ISPA, Internet Service Providers' Association (U.S.A.): Position on the Impact of Data Retention Laws on the Fight against Cybercrime, 30.09.2002, www.euroispa.org/docs/020930eurousispa_dretent.pdf, 1.

659 Richard, Mark: Statement of the United States of America presented at the EU Forum on Cybercrime in Brussels, 27.11.2001, cryptome.org/eu-dataspy.htm.

der Benutzung derartiger Telekommunikationsdienste ausgeschlossen werden. Zudem müssen zur Abwicklung der Bezahlung kostenpflichtiger Dienste doch wieder personenbezogene Daten erhoben werden. Angesichts von Gerüchten, dass einige US-amerikanische Anonymisierungsdienste in Wirklichkeit von dortigen Eingriffsbehörden betrieben werden sollen[660], wird es staatskritischen Personen auch schwer fallen, ihre Daten solchen privaten Diensten, deren Aktivitäten für Kunden intransparent sind, anzuvertrauen. Damit besteht die Gefahr eines veränderten Kommunikationsverhaltens der Bevölkerung ebenso wie im Fall einer Verkehrsdatenspeicherungspflicht. Die mit einer Datenvorhaltung stets verbundene Missbrauchsgefahr besteht ebenfalls unabhängig davon, ob die Speicherung von Verkehrsdaten auf einer Entscheidung des Staates oder des jeweiligen Unternehmens beruht.

Vor allem liegt es auf der Hand, dass ein System teilweiser Datenvorratshaltung dem Gebot gleichmäßiger Strafverfolgung gravierend zuwider läuft. Während einige Kleinkriminelle, die auf die Verdeckung ihrer Spuren keinen Wert legen, auf diese Weise überführt werden könnten, wächst die Wahrscheinlichkeit, dass anonyme Dienste eingesetzt werden, mit dem Ausmaß an Gefahr, das von einer Person ausgeht. Damit aber ist eine freiwillige Datenspeicherung zum Schutz von Rechtsgütern noch weniger geeignet als eine obligatorischen Vorratsspeicherung. Ist diese Eignung bereits bei einer obligatorischen Vorratsspeicherung so gering, dass sie Eingriffe nicht rechtfertigen kann, dann gilt dies erst recht in Bezug auf eine teilweise Vorratsspeicherung.

In Bezug auf die Option eines Vorratsspeicherungsrechts für Telekommunikationsunternehmen ist daher zu resümieren, dass eine solche Regelung für die betroffenen Bürger im Vergleich zu einer Vorratsspeicherungspflicht zwar weniger belastend ist, wenn insgesamt weniger Verkehrsdaten gespeichert werden. Dem stehen aber erhebliche Nachteile entgegen, insbesondere Effektivitätseinbußen bei der Arbeit der Sicherheitsbehörden. Die Abwägungsentscheidung kann daher im Ergebnis nicht anders ausfallen als hinsichtlich einer obligatorischen Vorratsspeicherung. Demnach ist auch die Einräumung eines Vorratsspeicherungsrechts mit Art. 10 Abs. 1 Var. 3 GG oder, soweit das Fernmeldegeheimnis nicht einschlägig ist, Art. 2 Abs. 1, 1

660 Cryptome.org: Meldung vom 16.02.2002, cryptome.org/g8-isp-e-spy.htm.

Abs. 1 GG unvereinbar. Folglich sehen insbesondere die §§ 97 Abs. 3 S. 3, 97 Abs. 4 S. 1 Nr. 2, 100 Abs. 1 und 3 TKG und die §§ 6 Abs. 7 S. 1 TDDSG, 19 Abs. 8 S. 1 MDStV unzulässige Vorratsspeicherungsrechte vor.

(c) Angemessenheit einer einzelfallbezogenen Speicherung von Telekommunikations-Verkehrsdaten

Die von Deutschland unterzeichnete Cybercrime-Konvention des Europarates sieht vor, dass die Vertragsstaaten die für die Strafverfolgung zuständigen Stellen dazu ermächtigen, in einzelnen Fällen die Aufbewahrung (Art. 16, 17 CCC) oder Erhebung von Verkehrsdaten (Art. 20 CCC) anordnen zu können. Eine solche Befugnis könnte auch für andere als computervermittelte Telekommunikationsvorgänge eingeführt werden.

In Deutschland soll bereits der bestehende § 100a StPO die Anordnung der Erhebung und Aufzeichnung von Telekommunikations-Verkehrsdaten erlauben[661]. Allerdings können nur geschäftsmäßige Anbieter von Telekommunikationsdiensten in Anspruch genommen werden (§ 100b Abs. 3 S. 1 StPO), also nur Anbieter von Telekommunikationsdiensten für Dritte (vgl. § 3 Nr. 10 TKG)[662]. Während diese Voraussetzung bei Telekommunikationsunternehmen ohne Weiteres gegeben ist, könnten Anbieter eigener Inhalte von dieser Definition nicht erfasst sein.

Die Problematik verdeutlicht das plastische Beispiel einer Wahrsagerin, die Anrufern am Telefon ihre Wahrsagedienste anbietet. Die Wahrsagerin bietet Dritten zwar bestimmte Dienste an, und diesen Diensten liegt auch eine Übermittlung mittels Telekommunikation zugrunde. Angeboten werden den Kunden aber nicht Telekommunikationsdienste (eine Fernübermittlung von Informationen), sondern bestimmte Inhalte. Telekommunikationsanbieter des anrufenden Kunden ist nicht die Wahrsagerin am Telefon, sondern die Telefongesellschaft des Kunden, denn diese übernimmt die Fernübermittlung der ausgetauschten Inhalte.

---

661 BGH-Ermittlungsrichter, DuD 2001, 297 (297); Begründung der Bundesregierung zu Entwurf der §§ 100g, h StPO in BT-Drs. 14/7008, 6 zu § 100g Abs. 1 S. 3 StPO.

662 BeckTKG-Büchner, § 85, Rn. 4.

Daran ändert sich auch dadurch nichts, dass die Wahrsagerin ein Telefon betreibt[663]. Bei diesem Telefon handelt es sich zwar um eine Telekommunikationsanlage, weil das Telefon eine technische Einrichtung ist, „die als Nachrichten identifizierbare [...] Signale senden [und] empfangen" kann (§ 3 Nr. 23 TKG). Die Wahrsagerin verwendet ihr Telefon aber im eigenen Interesse und nicht zu dem Zweck, Dritten Telekommunikationsdienste anzubieten. Dementsprechend kann die Wahrsagerin auch nicht gemäß § 100b Abs. 3 S. 1 StPO verpflichtet werden, die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen.

Vorstellbar ist weiterhin der Fall, dass die Wahrsagerin expandiert und das Wahrsagen von Mitarbeitern erledigen lässt. Auch wenn die Wahrsagerin nun eine Telefonanlage mit mehreren Anschlüssen betreibt, die von ihren Mitarbeitern genutzt werden, liegt kein Angebot von Telekommunikation an Dritte vor, weil die Nutzung der Telekommunikationsanlage durch die Mitarbeiter unter der Kontrolle der Wahrsagerin erfolgt. Dies ändert sich erst, wenn den Mitarbeitern erlaubt wird, ihr Telefon auch zu Privatgesprächen zu nutzen[664].

Dieser Sachverhalt lässt sich auf den Internetbereich übertragen. Denkbar ist beispielsweise, dass die Wahrsagerin täglich aktualisierte Horoskope im Internet veröffentlicht, und zwar mittels eines eigenen Webservers. In diesem Fall könnte die Wahrsagerin der Staatsanwaltschaft zwar die Überwachung und Aufzeichnung der Zugriffe auf ihr Angebot ermöglichen, etwa indem sie Zugriffsprotokolle zur Verfügung stellt. Sie kann derzeit aber nicht gemäß § 100b Abs. 3 S. 1 StPO hierzu verpflichtet werden[665], weil sie keine Telekommunikationsdienste für Dritte anbietet, sondern Inhalte. Ihr Server ist also nicht anders zu behandeln als ihr Telefon im oben diskutierten Fall.

Fraglich ist, ob anders zu entscheiden ist, wenn sich die Wahrsagerin zur Veröffentlichung ihres Angebots eines fremden Unternehmens bedient (Webhosting-Unternehmen). Dieses Unternehmen betreibt einen Server für Dritte, nämlich für die Wahrsagerin. Weil der Server über Internet-Verbindungsnetze „als Nachrichten identifizierbare [...] Signale senden [und] empfangen" kann (§ 3 Nr. 23 TKG), könnte

663 Vgl. BeckTKG-Büchner, § 85, Rn. 4.

664 So allgemein zu betrieblich genutzten Telekommunikationsanlagen BeckTKG-Büchner, § 85, Rn. 4.

665 A.A. in solchen Fällen wohl Schaar, Cybercrime und Bürgerrechte (I), 11.

man in dieser Tätigkeit ein geschäftsmäßiges Angebot von Telekommunikationsdiensten sehen[666]. Dies hätte zur Folge, dass das Unternehmen verpflichtet werden könnte, die Überwachung und Aufzeichnung der vermittelten Telekommunikation zu ermöglichen.

Dies ist im Bereich von Individualkommunikation über das Internet (z.B. E-Mail, Chat) anerkannt[667]. Dem liegt wohl der Gedanke zugrunde, dass eine Ungleichbehandlung zu den klassischen Formen der Individualkommunikation (z.B. Sprachtelefondienst, Telefax) wegen der sachlichen Vergleichbarkeit nicht einleuchten würde. Dieser Umstand bedeutet aber noch nicht, dass eine Gleichbehandlung in Deutschland auch gesetzlich vorgesehen ist, vor allem mit der nach dem Bestimmtheitsgebot erforderlichen Regelungsdichte. Zu beachten ist auch, dass eine Abgrenzung von Individualkommunikation und Massenkommunikation im Internet auf technischer Ebene nicht möglich ist, weil auch Dienste wie E-Mail zur Verbreitung von Massenkommunikation genutzt werden können (z.B. regelmäßiger Informationsbrief)[668]. Selbst bei inhaltlicher Prüfung einer Kommunikation wird man oft zu keinem eindeutigen Ergebnis kommen[669].

Umstritten ist die Geltung traditioneller Telekommunikationsregelungen vor allem in Bezug auf Internetdienste, die vorwiegend dem Angebot öffentlich zugänglicher Informationen dienen (z.B. WWW-Seiten, FTP-Dateien)[670]. Bei diesen Diensten handelt es sich unbestritten um Tele- oder Mediendienste (vgl. etwa § 2 Abs. 2 TDG). Das technische Anbieten solcher Dienste ist ebenso unbestritten nur mittels Telekommunikation möglich, weil Tele- und Mediendiensten definitionsgemäß eine Übermittlung mittels Telekommunikation zugrunde liegt (§ 2 Abs. 1 TDG). Diese telekommunikative Übermittlung kann auch geschäftsmäßig erfolgen, wie es etwa bei Webhosting-Unternehmen der Fall ist, die Telekommunikationsdienste an Dritte, nämlich an ihre Kunden, anbieten[671]. Man könnte daher vertreten, dass diese Unternehmen

---

666 So Germann, 569.

667 Weßlau, ZStW 113 (2001), 681 (699 f.) m.w.N.; Bizer, Rechtsfragen beim Einsatz von Email, Newsgroups und WWW in Schulen (I); BeckTKG-Schuster, § 85, Rn. 4c; BeckTKG-Büchner, § 85, Rn. 4; Germann, 139 und 619 f.

668 Ruhmann/Schulzki-Haddouti, Abhör-Dschungel (I).

669 BeckTKG-Schuster, § 4, Rn. 4

670 Klug, RDV 2001, 311 (312): Auf dem zweiten BfD-Symposium „Datenschutz in der Telekommunikation" sei man zu dem Ergebnis gekommen, das Surfen im Internet sei keine Telekommunikation und unterliege daher nicht der Telekommunikationsüberwachung; ebenso Koenig/Koch/Braun, K&R 2002, 289 (291) m.w.N.; Weßlau, ZStW 113 (2001), 681 (699 f.); a.A. Bär, MMR 2000, 472 (473); Kudlich JA 2000, 227 (231).

671 Germann, 569.

zur Aufzeichnung und Überwachung der Telekommunikation verpflichtet werden könnten und dass davon auch die Nutzung der Tele- und Mediendienste durch Dritte erfasst sei[672].

Dagegen spricht allerdings, dass der Inhalteanbieter in diesen Fällen nur zufällig zugleich ein Anbieter von Telekommunikation für Dritte ist. Betreibt ein Inhalteanbieter die erforderlichen Telekommunikationsanlagen selbst, dann kann er nicht verpflichtet werden, die Überwachung der Nutzung seiner Inhalte zu ermöglichen. Warum ein Outsourcing daran etwas ändern soll, ist nicht verständlich. In beiden Fällen müsste gleichermaßen erst das nächste Glied in der Kette, nämlich der Internet-Access-Provider des Inhalteanbieters, zur Ermöglichung einer Überwachung verpflichtet sein. So verhält es sich auch bei privaten Internetnutzern und bei Tele- und Mediendiensten, die telefonisch erbracht werden.

Begründen kann man die Ausnahme von Inhalteanbietern damit, dass nach dem Schwerpunkt einer Tätigkeit abzugrenzen sei[673]: Bietet ein Unternehmen schwerpunktmäßig Tele- oder Mediendienste an, dann wird das Angebot der notwendig zugrunde liegenden Telekommunikation von dieser Tätigkeit überlagert. Es liegt dann kein geschäftsmäßiges Angebot von Telekommunikationsdiensten vor. In der Tat bieten Webhosting-Unternehmen ihren Kunden nicht vorwiegend die Erbringung von Telekommunikationsdiensten an; zentral geht es vielmehr um das Angebot eines Tele- oder Mediendienstes. Für diese Auffassung kann man auch anführen, dass das Teledienstegesetz nicht für das geschäftsmäßige Erbringen von Telekommunikationsdiensten gilt (§ 2 Abs. 4 Nr. 1 TDG)[674] und dass das Gesetz daher von einer Ausschließlichkeit ausgeht. Weiterhin wurde argumentiert, dass TDG und MDStV als spätere Gesetze das ältere TKG verdrängten[675]. Dieses Argument kann nach der Neufassung des TKG im Jahre 2004 jedoch nicht mehr aufrecht erhalten werden.

Unbestritten verpflichtet das geltende Recht nur Anbieter von Telekommunikationsdiensten, nicht aber auch Anbieter von Tele- und Mediendiensten, zur Ermögli-

672 Germann, 569.
673 BeckTKG-Schuster, § 4, Rn. 4.
674 BeckTKG-Schuster, § 4, Rn. 4.
675 BeckTKG-Schuster, § 4, Rn. 4; Roßnagel-Spindler, § 2 TDG, Rn. 37.

chung der Aufzeichnung und Überwachung übermittelter Inhalte[676]. Auch Art. 1 Nr. 3 Buchst. a.bb des ErmittlungsG-Entwurfs des Bundesrates hätte daran nichts geändert, sondern nur zu einer Absenkung der Eingriffsschwelle geführt. Wie gezeigt, sind Anbieter von Tele- und Mediendiensten nicht oder jedenfalls nicht immer zugleich auch Anbieter von Telekommunikationsdiensten und als solche zur Mitwirkung bei Überwachungsmaßnahmen verpflichtet. Zwar kann in solchen Fällen eine Überwachung durch das nächste Glied in der Kommunikationskette erfolgen. Technisch ist es beispielsweise möglich, den Internetverkehr erst beim Internet-Access-Provider abzugreifen und aufzuzeichnen. Dies ist aber mit erheblichem Aufwand verbunden und daher praktisch nur in Ausnahmefällen realisierbar.

Vor diesem Hintergrund und angesichts der Tatsache eines wohl steigenden Maßes an Internetkriminalität mag man diesen Zustand für unbefriedigend halten. Die adäquate Reaktion bestünde dann aber nicht in der extremen Lösung[677] der Einführung einer generellen Vorratsspeicherung von Telekommunikations-Verkehrsdaten. Vielmehr müsste zunächst festgestellt werden, inwieweit es ausreicht, den zuständigen Stellen in einzelnen Fällen Zugriffsmöglichkeiten auf Internet-Verkehrsdaten einzuräumen[678]. Insoweit stehen insbesondere die Logfiles der Betreiber von Internet-Servern zur Verfügung, die sich von diesen regelmäßig ohne Kostenaufwand erstellen lassen oder – nach geltendem Recht meist illegal (§ 6 Abs. 1 S. 1 TDDSG, § 19 Abs. 2 S. 1 MDStV) – bereits erstellt werden. Mit Art. 12 GG wäre eine derartige Befugnis jedenfalls dann zu vereinbaren, wenn sie auf die Nutzung bereits vorhandener technischer Mittel eines gewerblichen Serverbetreibers beschränkt würde und wenn dessen Kosten im Wesentlichen erstattet würden.

Auch mit dem Recht auf informationelle Selbstbestimmung wäre eine solche Befugnis nicht von vornherein unvereinbar. Allerdings müssten hinreichend hohe Zugriffsschwellen vorgesehen sein[679], wobei eine Differenzierung zwischen Bestands-

---

676 Etwa Roßnagel-Dix/Schaar, § 6 TDDSG, Rn. 151.

677 EuroISPA, Internet Service Providers' Association (Europe) / US ISPA, Internet Service Providers' Association (U.S.A.): Position on the Impact of Data Retention Laws on the Fight against Cybercrime, 30.09.2002, www.euroispa.org/docs/-020930eurousispa_
dretent.pdf, 3: „Mandatory data retention is a drastic step".

678 EUROISPA/US ISPA; dafür auch Kommission, Sichere Informationsgesellschaft (I), 35; Queen Mary (University of London), Studie über Netzkriminalität (I).

679 Kommission, zitiert bei MDG, Entwurf für Schlussfolgerungen des Rates zur Informationstechnologie vom 28.11.2002, 3: Die Verwendung elektronischer Kommunikationsdaten sollte in Anbetracht des Grundsatzes der Verhältnismäßigkeit streng auf die Bekämpfung organisierter Kriminalität beschränkt sein.

‚Verkehrs- und Inhaltsdaten nicht gerechtfertigt ist. Die Ermächtigungsgrundlage müsste hinreichend normenklar und detailliert formuliert sein, und es müsste – anders als es derzeit bei den §§ 100a, 100g StPO der Fall ist – ein tatsächlich wirksames Verfahren zur Gewährleistung des Grundrechtsschutzes vorgesehen werden. Bei Beachtung dieser Erfordernisse wäre die Schaffung einer entsprechenden Befugnis als angemessene Beschränkung der Art. 2 Abs. 1, 1 Abs. 1 GG anzusehen. Art. 10 Abs. 1 Var. 3 GG ist nicht betroffen, weil Anbieter von Tele- und Mediendiensten Verkehrsdaten erst nach Abschluss der telekommunikativen Übermittlung aufzeichnen können.

Sollte der Gesetzgeber Anbieter von Tele- und Mediendiensten im Zuge einer Umsetzung der Cybercrime-Konvention in die Pflicht nehmen wollen, so ist zusätzlich zu beachten, dass diese Konvention eine weit reichende Zusammenarbeit der Vertragsstaaten untereinander vorsieht und dass Deutschland ein ausländisches Ersuchen um Amtshilfe nur unter sehr eingeschränkten Voraussetzungen verweigern dürfte. Übermittelt eine deutsche Behörde Verkehrsdaten an einen anderen Vertragsstaat, dann liegt darin ein rechtfertigungsbedürftiger Eingriff in das Fernmeldegeheimnis oder, soweit dieses nicht einschlägig ist, in das Recht auf informationelle Selbstbestimmung, der nur unter den oben bezeichneten, unabdingbaren formellen und materiellen Erfordernissen des deutschen Verfassungsrechts zulässig ist. Da sich die Vertragsstaaten der Cybercrime-Konvention grundsätzlich uneingeschränkt zur internationalen Amtshilfe verpflichten müssen, ausreichende Garantien dagegen weder ausdrücklich vorgesehen noch Vorbehalte in ausreichendem Maße zugelassen werden[680], ist die Ratifizierung der Konvention mit dem Grundgesetz unvereinbar.

Auch ob und inwieweit die übermittelten Daten von dem ersuchenden Staat genutzt oder weiter gegeben werden, ist im Hinblick auf das deutsche Verfassungsrecht nicht unerheblich. Ohne ein transparentes, rechtlich abgesichertes Verfahren in dem ersuchenden Staat kann nämlich nicht davon ausgegangen werden, dass die aus dem Recht auf informationelle Selbstbestimmung und Art. 10 Abs. 1 Var. 3 GG abzuleitenden Mindestanforderungen dort eingehalten werden. Ist die Beachtung dieser Garantien im Ausland aber nicht sicher gestellt, dann birgt die Übermitt-

680 Breyer, DuD 2001, 592 (598).

lung von Daten an einen ausländischen Staat eine besondere Gefahr der Verletzung des Rechts auf informationelle Selbstbestimmung in sich, die sich jederzeit verwirklichen kann. Bereits die Datenübermittlung durch eine deutsche Behörde würde in solchen Fällen einen verfassungswidrigen Eingriff in das Fernmeldegeheimnis oder das Recht auf informationelle Selbstbestimmung darstellen. Daraus ergibt sich, dass eine Datenübermittlung ins Ausland – ebenso wie die Gestattung oder Duldung von Eingriffen ausländischer Staaten auf deutschem Hoheitsgebiet – nur dann verfassungsmäßig gerechtfertigt sein kann, wenn die nach deutschem Verfassungsrecht unabdingbaren Garantien auch in dem ausländischen Staat gewährleistet werden. Dies stellt die Cybercrime-Konvention nicht auch nur ansatzweise sicher. Dass hinreichende Sicherungen etwa in den USA nicht existieren, ergibt sich schon daraus, dass Rechtsnormen über den Umgang von Nachrichtendiensten mit Daten ausländischer Bürger dort entweder nicht existieren oder geheim gehalten werden[681], was dem Bestimmtheitsgebot mangels Vorhersehbarkeit von Eingriffen nicht genügt

Berlin, den 20.06.2005

Starostik
Rechtsanwalt

681 EP, Echelon-Bericht (I), 94.