Stellungnahme vom 29. Oktober 2010 gegenüber dem Bundeswirtschaftsministerium:

Telekommunikationsrecht – Nutzerinnen und Nutzer vor Datenmissbrauch schützen

Sicherheit der Verbraucher vor Datenlecks, Spionage und Datenhandel stärken

Missbräuchliche Offenlegung der Verbindungen von Aufsichtsräten und Journalisten (Deutsche Telekom), Verkauf Millionen von Privatanschriften und Privatnummern an kriminelle Kreise (T-Mobile), Werbemüll („Spam“) – noch nie waren Deutsche so vielen Datenpannen und Missbrauchsfällen ausgesetzt wie in den letzten Monaten und Jahren.

Die Folgen für die Telekommunikationsfreiheit und die Wirtschaft sind fatal: Sechs von sieben Menschen glauben nicht, dass sie ihre Daten Telefonanbietern noch ohne Sorge vor Missbrauch anvertrauen können.[1] 68% befürchten die Nutzung persönlicher Daten zu Werbezwecken, 66% den Missbrauch ihrer Angaben und 54% die Weitergabe der Angaben an andere Unternehmen ohne ihre Einwilligung. Jeder Zweite verzichtet deshalb „häufiger“ darauf, überhaupt etwas zu bestellen, wenn er dabei seine Daten preisgeben muss. 34.000 Menschen sind vor das Bundesverfassungsgericht gezogen, um die globale und pauschale Aufzeichnung ihrer Kontakte, Bewegungen und Internetverbindungen zu stoppen.

Vom Gesetzgeber ist vor diesem Hintergrund ein mutiges Einschreiten zu fordern: Zur Stärkung der Privatsphäre und des Nutzervertrauens ist es dringend erforderlich, durchzusetzen, dass Telekommunikationsdienste so wenige persönliche Nutzerdaten wie möglich sammeln und Nutzer über den Umgang mit ihren Daten wirklich frei entscheiden können. Der Gesetzgeber ist zudem aufgefordert, für mehr Transparenz bei der Aufzeichnung und Speicherung persönlicher Daten bei Kommunikationsdiensten zu sorgen.

Wirksamen Schutz vor Datendiebstahl und Datenmissbrauch gewährleisten

Den besten und einzig wirksamen Schutz vor Datendiebstahl und Datenmissbrauch stellt es dar, wenn von vornherein möglichst wenige persönliche Daten erhoben und gespeichert werden. Verbraucher erwarten daher, dass sie telefonisch und elektronisch ebenso anonym und überwachungsfrei kommunizieren können wie es postalisch und im unmittelbaren Gespräch miteinander möglich ist.

Unter anderem sind dazu die folgenden Gesetzesänderungen erforderlich:

1. Einbeziehung aller Kundendaten in den Schutz des Fernmeldegeheimnisses, Zulassung staatlicher Zugriffe nur noch auf richterliche Anordnung,
2. Einführung eines Rechts auf anonyme Telekommunikation, Aufhebung des Identifizierungszwangs für Prepaid-Mobiltelefonkarten,
3. Vollständige Aufhebung der Vorratsspeicherung von Kundendaten,
4. Information der Kunden über die Dauer der Aufbewahrung ihrer Daten,
5. Recht auf sofortige Löschung von Verbindungsdaten mit Verbindungsende,
6. Verbot der Zweckentfremdung von Verbindungsdaten,
7. Verbot der Vorratsdatenspeicherung zur „Störungserkennung“ und „Missbrauchsaufdeckung“,
8. Schutz vor Ausspionieren durch „Spyware“ und „Web-Bugs“,
9. Ablehnung der im Referentenentwurf vorgesehenen Außerlandesschaffung von Kommunikationsdaten.

[1] Allensbacher Institut für Demoskopie, „Einstellung der Deutschen zum Thema Datenschutz“ (August 2010), http://www.webcitation.org/5t9uDMnHb.

Konkrete Formulierungsvorschläge zu diesen Punkten werden in der vorliegenden Stellungnahme unterbreitet.

Schutz der Verbraucher und Entwicklung der ITK-Branche gewährleisten

Der Gesetzgeber muss den zunehmenden Datenskandalen mutig gegensteuern und die Anhäufung privater Informationen über Telefon-, Handy-, E-Mail- und Internetnutzer wirksam unterbinden. In einer Informationsgesellschaft sind Informationen über unsere Nutzung von Kommunikationsdiensten Schlüssel zu unserem Privatleben. Solche Daten dürfen nicht länger gehortet und dem Zugriff von Datendieben und Betrügern ausgesetzt werden.

Wenn wir uns telefonisch und im Internet ebenso anonym wie sonst auch politisch informieren, über religiöse Fragen oder unsere Krankheiten erkundigen und Erotikangebote nutzen können, gewährleistet dies nicht nur unsere Sicherheit vor Datenpannen und Missbrauch. Auch die wirtschaftliche Entwicklung der ITK-Branche als wichtiger Zukunftsbranche in Deutschland wird gesichert, wenn der Gesetzgeber aus den Datenskandalen, Datenpannen und Datenlecks der jüngsten Vergangenheit die richtigen Konsequenzen zieht.

Inhaltsverzeichnis

Zusammenstellung der Änderungsvorschläge

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
§ 88 Fernmeldegeheimnis	*(unverändert)*		*(unverändert)*
(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.	*(unverändert)*	1	(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und **die näheren Umstände des Fernmeldeverhältnisses**, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche **und auf Bestandsdaten**.

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
§ 92 Datenübermittlung an ausländische nicht öffentliche Stellen	*(unverändert)*		*(unverändert)*
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.	(1) An ausländische nicht öffentliche Stellen, **die sich nicht in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum befinden,** 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.	2	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.
	(2) Für andere Zwecke als in Absatz 1 dürfen personenbezogene Daten nur übermittelt werden, soweit dies entsprechend den Regelungen für eine Auftragsdatenverarbeitung gemäß § 11 Bundesdatenschutzgesetz erfolgt und schutzwürdige Interessen des Betroffenen am Ausschluss der Übermittlung gegenüber dem berechtigten Interesse des Diensteanbieters nicht überwiegen.		
§ 93 Informationspflichten	*(unverändert)*		*(unverändert)*
(1) Diensteanbieter haben ihre Teilnehmer bei Vertragsabschluss **über Art, Umfang, Ort und Zweck der Erhebung und Verwendung personenbezogener Daten** so zu unterrichten, dass die Teilnehmer in allgemein verständlicher Form Kenntnis von den grundlegenden Verarbeitungstatbeständen der Daten erhalten. Dabei sind die Teil-	*(unverändert)*	3	(1) Diensteanbieter haben ihre Teilnehmer bei Vertragsabschluss **1. darüber, welche personenbezogenen Daten wie lange, in welchem Umfang und zu welchen Zwecken erhoben, verarbeitet und genutzt werden, und** **2. über die Verarbeitung ihrer Daten in Staaten au-**

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
nehmer auch auf die zulässigen Wahl- und Gestaltungsmöglichkeiten hinzuweisen. Die Nutzer sind vom Diensteanbieter durch allgemein zugängliche Informationen über die Erhebung und Verwendung personenbezogener Daten zu unterrichten. Das Auskunftsrecht nach dem Bundesdatenschutzgesetz bleibt davon unberührt.			**ßerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31) und** **3. in Fällen, in denen der Diensteanbieter einen Beauftragten für Datenschutz bestellt hat, über Möglichkeiten zur schnellen elektronischen Kontaktaufnahme und unmittelbaren Kommunikation mit diesem, einschließlich seiner Adresse der elektronischen Post,** in allgemein verständlicher Form zu unterrichten. Dabei sind die Teilnehmer auch auf die zulässigen Wahl- und Gestaltungsmöglichkeiten hinzuweisen. Die Nutzer sind vom Diensteanbieter durch allgemein zugängliche Informationen über die Erhebung und Verwendung personenbezogener Daten zu unterrichten. Das Auskunftsrecht nach dem Bundesdatenschutzgesetz bleibt davon unberührt.
§ 95 Bestandsdaten	*(unverändert)*		*(unverändert)*
(2) Der Diensteanbieter darf die Bestandsdaten der in Absatz 1 Satz 2 genannten Teilnehmer zur Beratung der Teilnehmer, **zur Versendung von Informationen nach § 98 Abs. 1 Satz 3,** zur Werbung für eigene Angebote und zur Marktforschung nur verwenden, soweit dies für diese Zwecke erforderlich ist und der Teilnehmer eingewilligt hat. Ein Diensteanbieter, der im Rahmen einer bestehenden Kundenbezie-	(2) Der Diensteanbieter darf die Bestandsdaten der in Absatz 1 Satz 2 genannten Teilnehmer zur Beratung der Teilnehmer, ~~**zur Versendung von Informationen nach § 98 Abs. 1 Satz 3,**~~ zur Werbung für eigene Angebote und zur Marktforschung nur verwenden, soweit dies für diese Zwecke erforderlich ist und der Teilnehmer eingewilligt hat. Ein Diensteanbieter, der im **Rahmen einer bestehenden Kundenbe-**	4	(2) Der Diensteanbieter darf die Bestandsdaten der in Absatz 1 Satz 2 genannten Teilnehmer zur Beratung der Teilnehmer, zur Werbung für eigene Angebote und zur Marktforschung nur verwenden, soweit dies für diese Zwecke erforderlich ist und der Teilnehmer eingewilligt hat. Ein Diensteanbieter, der im **Zusammenhang mit dem Verkauf eines Produkts oder einer Dienst-**

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
hung rechtmäßig Kenntnis von der Rufnummer oder der Postadresse, auch der elektronischen, eines Teilnehmers erhalten hat, darf diese für die Versendung von Text- oder Bildmitteilungen an ein Telefon oder an eine Postadresse zu den in Satz 1 genannten Zwecken verwenden, es sei denn, dass der Teilnehmer einer solchen Verwendung widersprochen hat. Die Verwendung der Rufnummer oder Adresse nach Satz 2 ist nur zulässig, wenn der Teilnehmer bei der Erhebung oder der erstmaligen Speicherung der Rufnummer oder Adresse und bei jeder Versendung einer Nachricht an diese Rufnummer oder Adresse zu einem der in Satz 1 genannten Zwecke deutlich sichtbar und gut lesbar darauf hingewiesen wird, dass er der Versendung weiterer Nachrichten jederzeit schriftlich oder elektronisch widersprechen kann.	**ziehung** rechtmäßig Kenntnis von der Rufnummer oder der Postadresse, auch der elektronischen, eines Teilnehmers erhalten hat, darf diese für die Versendung von Text- oder Bildmitteilungen an ein Telefon oder an eine Postadresse **zu den in Satz 1 genannten Zwecken** verwenden, es sei denn, dass der Teilnehmer einer solchen Verwendung widersprochen hat. Die Verwendung der Rufnummer oder Adresse nach Satz 2 ist nur zulässig, wenn der Teilnehmer bei der Erhebung oder der erstmaligen Speicherung der Rufnummer oder Adresse und bei jeder Versendung einer Nachricht an diese Rufnummer oder Adresse zu einem der in Satz 1 genannten Zwecke deutlich sichtbar und gut lesbar darauf hingewiesen wird, dass er der Versendung weiterer Nachrichten jederzeit schriftlich oder elektronisch widersprechen kann.		**leistung** rechtmäßig Kenntnis von der Rufnummer oder der Postadresse, auch der elektronischen, eines Teilnehmers erhalten hat, darf diese für die Versendung von Text- oder Bildmitteilungen an ein Telefon oder an eine Postadresse **zur Beratung der Teilnehmer, zur Werbung für eigene ähnliche Angebote und zur Marktforschung** verwenden, es sei denn, dass der Teilnehmer einer solchen Verwendung widersprochen hat. Die Verwendung der Rufnummer oder Adresse nach Satz 2 ist nur zulässig, wenn der Teilnehmer bei der Erhebung oder der erstmaligen Speicherung der Rufnummer oder Adresse und bei jeder Versendung einer Nachricht an diese Rufnummer oder Adresse zu einem der in Satz 1 genannten Zwecke deutlich sichtbar und gut lesbar darauf hingewiesen wird, dass er der Versendung weiterer Nachrichten jederzeit schriftlich oder elektronisch widersprechen kann**, und wenn dem Teilnehmer unmittelbar und kostenfrei eine Widerspruchsmöglichkeit eingeräumt wird.**
(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.	*(unverändert)*	5	***(entfällt)***

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
(5) Die Erbringung von Telekommunikationsdiensten **darf nicht von einer Einwilligung des Teilnehmers in eine Verwendung seiner Daten für andere Zwecke abhängig gemacht werden,** wenn dem Teilnehmer ein anderer Zugang zu diesen Telekommunikationsdiensten **nicht oder in nicht** zumutbarer Weise möglich ist.		6	(5) **Der Diensteanbieter darf** die Erbringung von Telekommunikationsdiensten **nicht von der Angabe personenbezogener Daten abhängig machen, die zur Erbringung der Telekommunikationsdienste nicht erforderlich sind. Entsprechendes gilt für die Einwilligung des Teilnehmers in die Verarbeitung oder Nutzung der Daten für andere Zwecke. Die Sätze 1 und 2 gelten nicht,** wenn dem Teilnehmer ein anderer Zugang zu diesen Telekommunikationsdiensten in zumutbarer Weise möglich ist. **Im Fall des Satzes 3 hat der Diensteanbieter** **1. kenntlich zu machen, von welchen Angaben oder Einwilligungserklärungen die Erbringung der Telekommunikationsdienste abhängig gemacht wird und** **2. die Unterrichtung des Teilnehmers nach § 93 Abs. 1 auch darauf zu erstrecken, in welcher Weise ein anderer Zugang zu diesen Telekommunikationsdiensten möglich ist.**

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
		7	**(6) Der Diensteanbieter hat die Inanspruchnahme von Telekommunikationsdiensten und ihre Bezahlung anonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Die anonyme Bereitstellung ist zumutbar, wenn Telekommunikationsdienste dieser Art am Markt anonym angeboten werden, es sei denn, dass die besonderen Verhältnisse des Diensteanbieters entgegen stehen. Der Teilnehmer ist über die Möglichkeit der anonymen Inanspruchnahme zu informieren.**
§ 96 Verkehrsdaten	*(unverändert)*		*(unverändert)*
(1) Der Diensteanbieter darf folgende Verkehrsdaten erheben, soweit dies für die in diesem Abschnitt oder in § 2 oder § 4 des Zugangserschwerungsgesetzes genannten Zwecke erforderlich ist:	*(unverändert)*	8	(1) Der Diensteanbieter darf folgende Verkehrsdaten erheben, soweit dies für die in diesem Abschnitt oder in § 2 oder § 4 des Zugangserschwerungsgesetzes genannten Zwecke erforderlich ist:
1. 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,			1. 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,
2. den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,			2. den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
3. den vom Nutzer in Anspruch genommenen Telekommunikationsdienst,			3. den vom Nutzer in Anspruch genommenen Telekommunikationsdienst,
4. die Endpunkte von festge-			

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
schalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen, 5. sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten. Diese Verkehrsdaten dürfen nur verwendet werden, soweit **dies für die in Satz 1 genannten oder durch andere gesetzliche Vorschriften begründeten Zwecke oder zum Aufbau weiterer Verbindungen erforderlich ist.** Im Übrigen sind Verkehrsdaten vom Diensteanbieter **nach Beendigung der Verbindung unverzüglich zu löschen**.			4. die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen, 5. sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten. Diese Verkehrsdaten dürfen nur verwendet werden, soweit **sie zum Aufbau weiterer Verbindungen oder für die in den §§ 97, 99, 100 und 101 genannten Zwecke erforderlich sind.** Im Übrigen sind Verkehrsdaten vom Diensteanbieter **zu löschen, sobald die Verbindung beendet ist**. **Vorschriften in anderen Gesetzen, die sich ausdrücklich auf Telekommunikationsvorgänge beziehen, bleiben unberührt.**

Geltendes Telekommunikationsgesetz (TKG)	**Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen**	**Nr**	**Änderungsvorschlag**
§ 97 Entgeltermittlung und Entgeltabrechnung	*(unverändert)*		*(unverändert)*
(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. Diese Daten dürfen bis zu sechs Monate nach Versendung der Rechnung gespeichert werden. Für die Abrechnung nicht erforderliche Daten sind unverzüglich zu löschen**, soweit sie nicht nach § 113a zu speichern sind**. Hat der Teilnehmer gegen die Höhe der in Rechnung gestellten Verbindungsentgelte vor Ablauf der Frist nach Satz 2 Einwendungen erhoben, dürfen die Daten gespeichert werden, bis die Einwendungen abschließend geklärt sind.	(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. Diese Daten dürfen bis zu sechs Monate nach Versendung der Rechnung gespeichert werden. Für die Abrechnung nicht erforderliche Daten sind unverzüglich zu löschen~~, soweit sie nicht nach § 113a zu speichern sind~~. Hat der Teilnehmer gegen die Höhe der in Rechnung gestellten Verbindungsentgelte vor Ablauf der Frist nach Satz 2 Einwendungen erhoben, dürfen die Daten gespeichert werden, bis die Einwendungen abschließend geklärt sind.	9	(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. Für die Abrechnung nicht erforderliche Daten sind unverzüglich zu löschen. **Die Verkehrsdaten dürfen unter Kürzung der Zielnummer um die letzten drei Ziffern zu Beweiszwecken für die Richtigkeit der berechneten Entgelte – vorbehaltlich des Absatzes 4 – höchstens sechs Wochen 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 Daten gespeichert werden, bis die Einwendungen abschließend geklärt sind.

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
			(4) Auf Verlangen des Teilnehmers hat der rechnungstellende Diensteanbieter **1. die Zielnummer vollständig zu speichern oder** **2. das Entgelt zu berechnen und die Verkehrsdaten vollständig zu löschen, sobald die Verbindung beendet ist.** **Soweit ein Kunde zur vollständigen oder teilweisen Übernahme der Entgelte für bei seinem Anschluss ankommende Verbindungen verpflichtet ist, steht ihm das Wahlrecht nach Nummer 1 nicht zu. Die Sätze 1 und 2 gelten nicht für Diensteanbieter, die als Anbieter geschlossener Benutzergruppen ihre Dienste nur ihren Teilnehmern anbieten.**
(4) 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.	*(unverändert)*		*(wird zu Absatz 5)*

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
§ 100 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten	*(unverändert)*		*(unverändert)*
(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.**	*(unverändert)*	10	(1) **Liegen dem Diensteanbieter im Einzelfall zu dokumentierende tatsächliche Anhaltspunkte vor, dass bestimmte Nutzer seine zur Bereitstellung seines Dienstes genutzten technischen Einrichtungen stören, darf er Bestands- und Verkehrsdaten dieser Nutzer nur erheben, speichern und nutzen, soweit dies zur Beseitigung der Störung erforderlich ist; eine Verwendung der Daten für andere Zwecke ist unzulässig. Der Diensteanbieter hat die Daten unverzüglich zu löschen, wenn die Voraussetzungen nach Satz 1 nicht mehr vorliegen oder die Daten zur Störungsbeseitigung nicht mehr benötigt werden. Der betroffene Nutzer ist zu unterrichten, sobald dies ohne Gefährdung des mit der Maßnahme verfolgten Zweckes möglich ist.**
(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 erforderlich sind. Zu dem in Satz 1 genannten Zweck darf der Diensteanbieter die erhobenen Verkehrsdaten in der Weise verwenden, dass aus	*(unverändert)*		**(3) Liegen dem Diensteanbieter im Einzelfall zu dokumentierende tatsächliche Anhaltspunkte vor, dass seine Dienste von bestimmten Nutzern in der Absicht in Anspruch genommen werden, das Entgelt nicht oder nicht vollständig zu entrichten, darf er Bestandsdaten und nach § 97 TKG gespeicherte Verkehrsdaten dieser Nutzer nur verwenden, soweit dies zur Geltendmachung seiner Ansprüche gegen die Nutzer erforderlich ist. Der Diensteanbieter hat die Daten unver-**

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
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 Bundesnetzagentur und der oder die Bundesbeauftragte für den Datenschutz sind über Einführung und Änderung eines Verfahrens nach Satz 1 unverzüglich in Kenntnis zu setzen.			**züglich zu löschen, wenn die Voraussetzungen nach Satz 1 nicht mehr vorliegen oder die Daten für die Rechtsverfolgung nicht mehr benötigt werden. Der betroffene Nutzer ist zu unterrichten, sobald dies ohne Gefährdung des mit der Maßnahme verfolgten Zweckes möglich ist.**
§ 111 Daten für Auskunftsersuchen der Sicherheitsbehörden	*(unverändert)*	11	***(entfällt)***
§ 112 Automatisiertes Auskunftsverfahren	*(unverändert)*		***(entfällt)***

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
§ 113 Manuelles Auskunftsverfahren	*(unverändert)*	12	***(entfällt)***

Geltende Strafprozessordnung (StPO)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen		Änderungsvorschlag
§ 100g	*(unverändert)*		*(unverändert)*
(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer	*(unverändert)*		(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer
1. eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder			1. eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder
2. eine Straftat mittels Telekommunikation begangen hat,			2. eine Straftat mittels Telekommunikation begangen hat,
so dürfen auch ohne Wissen des Betroffenen Verkehrsdaten (§ 96 Abs. 1, § 113a des Telekommunikationsgesetzes) erhoben werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Im Falle des Satzes 1 Nr. 2 ist die Maßnahme nur zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Die Erhebung von Standortdaten in Echtzeit ist nur im Falle des Satzes 1 Nr. 1 zulässig.			so dürfen auch ohne Wissen des Betroffenen **Bestandsdaten und** Verkehrsdaten (§ 95 Abs. 1, § 96 Abs. 1~~, § 113a~~ des Telekommunikationsgesetzes) erhoben werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Im Falle des Satzes 1 Nr. 2 ist die Maßnahme nur zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Die Erhebung von Standortdaten in Echtzeit ist nur im Falle des Satzes 1 Nr. 1 zulässig.

Geltende Strafprozessordnung (StPO)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen		Änderungsvorschlag
(2) § 100a Abs. 3 und § 100b Abs. 1 bis 4 Satz 1 gelten entsprechend. Abweichend von § 100b Abs. 2 Satz 2 Nr. 2 genügt im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.	*(unverändert)*		(2) § 100a Abs. 3 und § 100b Abs. 1 bis 4 Satz 1 gelten entsprechend. Abweichend von § 100b Abs. 2 Satz 2 Nr. 2 genügt im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. **Im Fall von Bestandsdaten sind in der Anordnung abweichend von § 100b Abs. 2 anzugeben** **1. der Name und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet, oder die Rufnummer oder eine andere Kennung des Anschlusses, zu dem Auskunft erteilt werden soll,** **2. Art und Umfang der begehrten Auskunft.**
§ 101	*(unverändert)*		*(unverändert)*
(4) Von den in Absatz 1 genannten Maßnahmen sind im Falle ...	*(unverändert)*		(4) Von den in Absatz 1 genannten Maßnahmen sind im Falle ...
6. des § 100g die Beteiligten der betroffenen Telekommunikation,			6. des § 100g die Beteiligten der betroffenen Telekommunikation, **im Fall von Bestandsdaten die Inhaber der betroffenen Anschlüsse,**

Geltendes Telemediengesetz (TMG)	**Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen**	**Nr**	**Änderungsvorschlag**
§ 13 Pflichten des Diensteanbieters	*(unverändert)*		*(unverändert)*
		13	**(8) Die Speicherung von Daten im Endgerät des Nutzers und der Zugriff auf Daten, die im Endgerät des Nutzers gespeichert sind, ist nur zulässig, wenn der Nutzer darüber gemäß Absatz 1 unterrichtet worden ist und darin eingewilligt hat. Dies gilt nicht, wenn der alleinige Zweck der Speicherung oder des Zugriffs die Durchführung oder Erleichterung der Übertragung einer Nachricht über ein Telekommunikationsnetz ist oder soweit dies zwingend erforderlich ist, um einen vom Nutzer ausdrücklich gewünschten elektronischen Informations- und Kommunikationsdienst zur Verfügung zu stellen.**

Einzelerläuterung

1. Stärkung des Fernmeldegeheimnisses (§ 88 TKG)

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
§ 88 Fernmeldegeheimnis	*(unverändert)*		*(unverändert)*
(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.	*(unverändert)*	1	(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und **die näheren Umstände des Fernmeldeverhältnisses**, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche **und auf Bestandsdaten**.

Nach bisher überwiegender Meinung schützt das Fernmeldegeheimnis nicht alle Umstände des Fernmeldeverhältnisses, sondern nur Informationen über einzelne Verbindungen. Ungeschützt bleiben damit die Identität der Teilnehmer an Verbindungen (z.B. Internetverbindungen) und so sensible Informationen wie das Passwort zu einem E-Mail-Postfach und die PIN zu einem elektronischen Anrufbeantworter, aber auch Vertragsdaten wie die Bankverbindung des Kunden.

Aus den folgenden Gründen ist die Einbeziehung von Bestandsdaten in den Schutz des Fernmeldegeheimnisses geboten: Vorfälle wie der Verlust sämtlicher Kundendaten durch T-Mobile haben gezeigt, dass der bisherige Schutz von Bestandsdaten nicht ausreicht. Im Jahr 2006 verkaufte ein Mitarbeiter von T-Mobile die Daten der 17 Mio. Prepaid- und Postpaid-Kunden des Mobilfunkunternehmens. Die Daten umfassen den Namen, die Mobilfunknummer, die Anschrift, teils das Geburtsdatum und in einigen Fällen auch die E-Mail-Adresse. Die Daten wurden in kriminellen Kreisen angeboten. In den Daten fanden sich nicht nur viele Prominente aus Kultur und Gesellschaft wie Hape Kerkeling, Günther Jauch und Til Schweiger, sondern auch eine erstaunliche Anzahl geheimer Nummern und Privatadressen von bekannten Politikern, Ministern, Ex-Bundespräsidenten, Wirtschaftsführern, Milliardären und Glaubensvertretern, für die eine Verbreitung ihrer Kontaktdaten in kriminellen Kreisen eine Bedrohung ihrer Sicherheit darstellte (etwa Charlotte Knobloch, Präsidentin des Zentralrats der Juden). Das Bundeskriminalamt erstellte eine Gefährdungsanalyse, um Betroffene schützen zu können.

In Reaktion auf solche Vorfälle hat der Gesetzgeber eine Informationspflicht eingeführt (§ 93 Abs. 3 TKG). Er hat dabei die vergleichbare Schutzwürdigkeit von Verbindungs- und Bestandsdaten erkannt und Datenverluste in beiden Bereichen gleich behandelt. Jedoch fehlt im Bereich des Fernmeldegeheimnisses noch die erforderliche Gleichstellung. Die Einbeziehung aller Kundendaten in das Fernmeldegeheimnis ist erforderlich, um den Verlust, Verkauf oder Missbrauch dieser Informationen von vornherein zu verhindern.

Die Erweiterung des § 88 TKG ist auch verfassungsrechtlich geboten. Das Bundesverfassungsgericht hat bereits in frühen Entscheidungen klargestellt, dass das Fernmeldegeheimnis nicht nur den Inhalt geführter

Telefongespräche, sondern auch die „näheren Umstände des Fernmeldeverhältnisses“ umfasst.[2] Dazu gehört „insbesondere“ die Tatsache, ob und wann zwischen welchen Personen und Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist.[3] Ebenso bezeichnen aber Bestandsdaten „nähere Umstände des Fernmeldeverhältnisses“. Die Unterscheidung von Verkehrs- und Bestandsdaten ist für den Anwendungsbereich des Fernmeldegeheimnisses ohne Bedeutung. Selbst wenn man das Grundrecht auf einzelne Kommunikationsvorgänge beschränken wollte, bezeichnen Bestandsdaten durchaus nähere Umstände einzelner Verbindungen: über wessen Anschluss sie geführt wurden, wie für sie bezahlt wurde, mit welchen Passwort eine E-Mail abgerufen wurde usw. Das Beispiel des Inhabers einer IP-Adresse zeigt, dass es derzeit oft vom Zufall abhängt, ob die Vertraulichkeit der Telekommunizierenden § 88 TKG unterfällt („dynamische“ IP-Adresse)[4] oder nicht („statische“ IP-Adresse). Ähnliche Zufälligkeiten sind bei VPN- und Callthrough-Diensten („dynamische“ Anschlusskennungen) im Vergleich zu Internetzugangs- und Telefondiensten („statische“ Anschlusskennungen) zu beobachten. Diese sachlich nicht nachvollziehbare Unterscheidung muss aufgehoben werden.

Als Folgeänderung muss auch der strafrechtliche Schutz des Fernmeldegeheimnisses auf Bestandsdaten erstreckt werden.

2 BVerfGE 67, 157 (172); BVerfGE 86, 386 (396).

3 BVerfGE 67, 157 (172); BVerfGE 86, 386 (396).

4 BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 195.

2. Keine Außerlandesschaffung von Kommunikationsdaten (§ 92 TKG)

Geltendes Telekommunikationsgesetz (TKG)	**Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen**	**Nr**	**Änderungsvorschlag**
§ 92 Datenübermittlung an ausländische nicht öffentliche Stellen	*(unverändert)*		*(unverändert)*
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.	(1) An ausländische nicht öffentliche Stellen, **die sich nicht in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum befinden,** 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.	2	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.
	(2) Für andere Zwecke als in Absatz 1 dürfen personenbezogene Daten nur übermittelt werden, soweit dies entsprechend den Regelungen für eine Auftragsdatenverarbeitung gemäß § 11 Bundesdatenschutzgesetz erfolgt und schutzwürdige Interessen des Betroffenen am Ausschluss der Übermittlung gegenüber dem berechtigten Interesse des Diensteanbieters nicht überwiegen.		

Die geplanten Änderungen des § 92 TKG sind nicht akzeptabel und deshalb abzulehnen. Sie entzögen sensibelste Informationen über unsere Kontakte, Bewegungen und Internetnutzung faktisch dem Schutz des deutschen Fernmeldegeheimnisses:

Aus gutem Grund erlaubt das Telekommunikationsgesetz die Verbringung von Informationen über Fernmeldeverhältnisse und den Fernmeldeverkehr in das Ausland bisher nur, wenn dies aus besonderen Gründen erforderlich ist. Im Ausland, auch im europäischen Ausland, unterliegen Kommunikationsdaten nicht mehr unmittelbar dem hohen deutschen Schutzniveau, das geboten ist, um unbefangene elektronische Kommunikation auch in besonders vertraulichen Angelegenheiten zu gewährleisten. Die deutschen Aufsichtsbehörden können im Ausland keine Kontrollen mehr durchführen.

Hinzu kommt, dass die Daten im Ausland dem Zugriff ausländischer Behörden und Geheimdienste ausgesetzt sind, was auch im Hinblick auf geheimdienstliche Tätigkeit im Bereich der Wirtschaftsspionage (z.B. in Großbritannien, Frankreich) unannehmbar ist. Nach den Datenskandalen etwa bei der Deutschen Telekom und T-Mobile wäre die Legalisierung einer Außerlandesschaffung sensibelster Daten über die Telekommunikation in Deutschland genau das falsche Signal.

Entgegen der Gesetzesbegründung stellte § 93 Abs. 1 TKG-RefE keineswegs eine „Klarstellung", sondern eine gravierende Verschlechterung des Schutzniveaus dar. An § 93 Abs. 2 TKG-RefE ist zu kritisieren, dass sogar das Schutzniveau der §§ 4b ff. BDSG unterschritten wird, welche eine Datenverbringung in das außereuropäische Ausland nur ausnahmsweise gestattet. Auch ist vollkommen unklar, wann nach der vorgeschlagenen Formulierung ein Überwiegen des Interesses der Kommunikationsteilnehmer anzunehmen sein soll. Wie oben aufgezeigt, überwiegt das Interesse und Recht der Menschen auf vertrauliche Kommunikation immer und stets etwaige Geschäftsinteressen an einer Außerlandesschaffung, wo diese nicht ausnahmsweise erforderlich ist.

Deswegen muss § 92 TKG in seiner gegenwärtigen Fassung erhalten bleiben.

3. Mehr Transparenz über Datenspeicherung (§ 93 TKG)

Geltendes Telekommunikationsgesetz (TKG)	**Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen**	**Nr**	**Änderungsvorschlag**
§ 93 Informationspflichten	*(unverändert)*		*(unverändert)*
(1) Diensteanbieter haben ihre Teilnehmer bei Vertragsabschluss **über Art, Umfang, Ort und Zweck der Erhebung und Verwendung personenbezogener Daten** so zu unterrichten, dass die Teilnehmer in allgemein verständlicher Form Kenntnis von den grundlegenden Verarbeitungstatbeständen der Daten erhalten. Dabei sind die Teilnehmer auch auf die zulässigen Wahl- und Gestaltungsmöglichkeiten hinzuweisen. Die Nutzer sind vom Diensteanbieter durch allgemein zugängliche Informationen über die Erhebung und Verwendung personenbezogener Daten zu unterrichten. Das Auskunftsrecht nach dem Bundesdatenschutzgesetz bleibt davon unberührt.	*(unverändert)*	3	(1) Diensteanbieter haben ihre Teilnehmer bei Vertragsabschluss **1. darüber, welche personenbezogenen Daten wie lange, in welchem Umfang und zu welchen Zwecken erhoben, verarbeitet und genutzt werden, und** **2. über die Verarbeitung ihrer Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31) und** **3. in Fällen, in denen der Diensteanbieter einen Beauftragten für Datenschutz bestellt hat, über Möglichkeiten zur schnellen elektronischen Kontaktaufnahme und unmittelbaren Kommunikation mit diesem, einschließlich**

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
			seiner Adresse der elektronischen Post, in allgemein verständlicher Form zu unterrichten. Dabei sind die Teilnehmer auch auf die zulässigen Wahl- und Gestaltungsmöglichkeiten hinzuweisen. Die Nutzer sind vom Diensteanbieter durch allgemein zugängliche Informationen über die Erhebung und Verwendung personenbezogener Daten zu unterrichten. Das Auskunftsrecht nach dem Bundesdatenschutzgesetz bleibt davon unberührt.

Zu Ziff. 1. des Änderungsvorschlags:

Nach § 93 TKG ist der Nutzer über „Art, Umfang und Zwecke" der Verarbeitung seiner Daten zu unterrichten. Die Gewährleistung von Transparenz ist zur Wahrung des informationellen Selbstbestimmungsrechts und zur Stärkung des Nutzervertrauens von zentraler Bedeutung. In seiner bisherigen Formulierung ist § 93 Abs. 1 TKG jedoch zu unbestimmt und verfehlt sein Ziel in der Praxis daher regelmäßig. So wird oft nur in allgemeiner Form über die Art der verarbeiteten Daten unterrichtet, z.B. durch Verwendung der Begriffe „Bestandsdaten" oder „Abrechnungsdaten", ohne dass konkret darüber unterrichtet wird, welche Datentypen im Einzelnen verarbeitet werden.

Auch über den Umfang der Verarbeitung wird regelmäßig nur unzureichend aufgeklärt, insbesondere über den zeitlichen Umfang der Speicherung der einzelnen Datentypen. Dabei sah schon die Begründung zum damaligen § 91 TKG vor, dass sich die Unterrichtung auch auf „typische Speicherfristen" erstrecken muss.[5] Derselben Ansicht ist die EU-Datenschutzgruppe.[6] Ohne Zeitabgabe kann der Nutzer nicht erkennen, ob eine Speicherung einen Monat oder ein Jahr lang erfolgt, was nicht akzeptabel ist.

Bisher kann der Nutzer akkurate Informationen über die Speicherung von Daten zu seiner Person meist nur durch ein Auskunftsverlangen nach § 34 BDSG erhalten. Dieser Weg ist aber für beide Seiten aufwändig und unbefriedigend: Für den Nutzer, weil vollständige Auskünfte oft erst nach Monaten und nach Einschaltung der zuständigen Aufsichtsbehörde erteilt werden. Für den Diensteanbieter, weil er für das Zusammensuchen der Daten Zeit und Geld aufwenden muss.

Die allseits beste Lösung besteht folglich darin, zu gewährleisten, dass die nach § 93 Abs. 1 TKG vorgeschriebene Unterrichtung so genau und umfassend erfolgt, dass eine Auskunftsanforderung entbehrlich wird. Dazu muss der Nutzer in allgemein verständlicher Form darüber unterrichtet werden, „welche personenbezogenen Daten wie lange, in welchem Umfang und zu welchen Zwecken erhoben, verarbeitet und genutzt werden". Diese Formulierung sah schon der Entwurf der FDP-Fraktion eines Gesetzes zur Änderung des Telemediengesetzes vor.[7]

---

5 BT-Drs. 15/2316, 1 (88).

6 Vgl. Dokument WP 37 vom 21.11.2000, 65: „Die Betroffenen müssen klar und deutlich über den Verwendungszweck informiert werden, über die Art der erfassten Daten und die mögliche Dauer der Datenspeicherung."

7 BT-Drs. 16/11173, 4.

Eine solche Unterrichtung über die Dauer der Datenspeicherung ist auch europarechtlich geboten. Art. 6 Abs. 4 Hs. 1 RiL 2002/58/EG bestimmt: „*Der Diensteanbieter muss dem Teilnehmer oder Nutzer mitteilen, welche Arten von Verkehrsdaten für die in Absatz 2 genannten Zwecke verarbeitet werden und wie lange das geschieht*“. Diese Vorschrift ist bisher nicht vollständig umgesetzt.

Zu Ziff. 2. des Änderungsvorschlags:

Die Vorschrift entspricht § 13 Abs. 1 TMG. Wenn überhaupt eine Verbringung hochsensibler Kommunikationsdaten in Drittstaaten gestattet wird, dann muss der Teilnehmer darauf wenigstens hingewiesen werden, damit er solche Dienste meiden kann.

Zu Ziff. 3. des Änderungsvorschlags:

Das Bundesdatenschutzgesetz bestimmt: „*Betroffene können sich jederzeit an den Beauftragten für den Datenschutz wenden.*“ (§ 4f Abs. 5 S. 2 BDSG). Diese Absicht des Gesetzgebers wird bei Telekommunikationsdiensten regelmäßig dadurch vereitelt, dass der betriebliche Datenschutzbeauftragte vom Diensteanbieter nicht benannt wird und nicht erreichbar ist. Wenden sich Nutzer an die allgemeine Kontaktadresse, erhalten sie oftmals keine oder keine kompetente Antwort, selbst wenn ihr Schreiben ausdrücklich an den betrieblichen Datenschutzbeauftragten gerichtet ist. Es ist davon auszugehen, dass dieser Missstand nicht auf bösen Willen seitens der Kundendienstmitarbeiter der Unternehmen zurückzuführen ist, sondern dass ihnen die erforderliche Sachkompetenz fehlt, um Datenschutzanfragen ordnungsgemäß bearbeiten zu können.

Um zu gewährleisten, dass der betriebliche Datenschutzbeauftragte seine gesetzliche Aufgabe als Ansprechpartner der Betroffenen erfüllen kann, ist es erforderlich, dass Angaben verfügbar sind, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihm ermöglichen, einschließlich einer Email-Adresse. Die hier vorgeschlagene Formulierung orientiert sich an dem Wortlaut des § 5 Abs. 1 Nr. 2 TMG. Für die Anbieter ist kein nennenswerter Aufwand damit verbunden, Kontaktdaten zu veröffentlichen, über die der betriebliche Datenschutzbeauftragte erreichbar ist.

4. Einschränkung der Datennutzung zu Werbezwecken (§ 95 TKG)

Geltendes Telekommunikationsgesetz (TKG)	**Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen**	**Nr**	**Änderungsvorschlag**
§ 95 Bestandsdaten	*(unverändert)*		*(unverändert)*
(2) Der Diensteanbieter darf die Bestandsdaten der in Absatz 1 Satz 2 genannten Teilnehmer zur Beratung der Teilnehmer, **zur Versendung von Informationen nach § 98 Abs. 1 Satz 3,** zur Werbung für eigene Angebote und zur Marktforschung nur verwenden, soweit dies für diese Zwecke erforderlich ist und der Teilnehmer eingewilligt hat. Ein Diensteanbieter, der im Rahmen einer bestehenden Kundenbeziehung rechtmäßig Kenntnis von der Rufnummer oder der Postadresse, auch der elektronischen, eines Teilnehmers erhalten hat, darf diese für die Versendung von Text- oder Bild-	(2) Der Diensteanbieter darf die Bestandsdaten der in Absatz 1 Satz 2 genannten Teilnehmer zur Beratung der Teilnehmer, ~~**zur Versendung von Informationen nach § 98 Abs. 1 Satz 3,**~~ zur Werbung für eigene Angebote und zur Marktforschung nur verwenden, soweit dies für diese Zwecke erforderlich ist und der Teilnehmer eingewilligt hat. Ein Diensteanbieter, der im **Rahmen einer bestehenden Kundenbeziehung** rechtmäßig Kenntnis von der Rufnummer oder der Postadresse, auch der elektronischen, eines Teilnehmers erhalten hat, darf diese für die Versendung von Text- oder Bild-	4	(2) Der Diensteanbieter darf die Bestandsdaten der in Absatz 1 Satz 2 genannten Teilnehmer zur Beratung der Teilnehmer, zur Werbung für eigene Angebote und zur Marktforschung nur verwenden, soweit dies für diese Zwecke erforderlich ist und der Teilnehmer eingewilligt hat. Ein Diensteanbieter, der im **Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung** rechtmäßig Kenntnis von der Rufnummer oder der Postadresse, auch der elektronischen, eines Teilnehmers erhalten hat, darf diese für die Versendung von Text- oder

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
mitteilungen an ein Telefon oder an eine Postadresse zu den in Satz 1 genannten Zwecken verwenden, es sei denn, dass der Teilnehmer einer solchen Verwendung widersprochen hat. Die Verwendung der Rufnummer oder Adresse nach Satz 2 ist nur zulässig, wenn der Teilnehmer bei der Erhebung oder der erstmaligen Speicherung der Rufnummer oder Adresse und bei jeder Versendung einer Nachricht an diese Rufnummer oder Adresse zu einem der in Satz 1 genannten Zwecke deutlich sichtbar und gut lesbar darauf hingewiesen wird, dass er der Versendung weiterer Nachrichten jederzeit schriftlich oder elektronisch widersprechen kann.	mitteilungen an ein Telefon oder an eine Postadresse **zu den in Satz 1 genannten Zwecken** verwenden, es sei denn, dass der Teilnehmer einer solchen Verwendung widersprochen hat. Die Verwendung der Rufnummer oder Adresse nach Satz 2 ist nur zulässig, wenn der Teilnehmer bei der Erhebung oder der erstmaligen Speicherung der Rufnummer oder Adresse und bei jeder Versendung einer Nachricht an diese Rufnummer oder Adresse zu einem der in Satz 1 genannten Zwecke deutlich sichtbar und gut lesbar darauf hingewiesen wird, dass er der Versendung weiterer Nachrichten jederzeit schriftlich oder elektronisch widersprechen kann.		Bildmitteilungen an ein Telefon oder an eine Postadresse **zur Beratung der Teilnehmer, zur Werbung für eigene ähnliche Angebote und zur Marktforschung** verwenden, es sei denn, dass der Teilnehmer einer solchen Verwendung widersprochen hat. Die Verwendung der Rufnummer oder Adresse nach Satz 2 ist nur zulässig, wenn der Teilnehmer bei der Erhebung oder der erstmaligen Speicherung der Rufnummer oder Adresse und bei jeder Versendung einer Nachricht an diese Rufnummer oder Adresse zu einem der in Satz 1 genannten Zwecke deutlich sichtbar und gut lesbar darauf hingewiesen wird, dass er der Versendung weiterer Nachrichten jederzeit schriftlich oder elektronisch widersprechen kann**, und wenn dem Teilnehmer unmittelbar und kostenfrei eine Widerspruchsmöglichkeit eingeräumt wird.**

§ 95 Abs. 2 S. 2 TKG erlaubt die Verwendung von Bestandsdaten zu Werbezwecken bereits dann, wenn der Betroffene dem nicht widersprochen hat. Demgegenüber bestimmt Art. 13 Abs. 2 der RiL 2002/58/EG: *„Ungeachtet des Absatzes 1 kann eine natürliche oder juristische Person, wenn sie von ihren Kunden im Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung gemäß der Richtlinie 95/46/EG deren elektronische Kontaktinformationen für elektronische Post erhalten hat, diese zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen verwenden, sofern die Kunden klar und deutlich die Möglichkeit erhalten, eine solche Nutzung ihrer elektronischen Kontaktinformationen bei deren Erhebung und bei jeder Übertragung gebührenfrei und problemlos abzulehnen, wenn der Kunde diese Nutzung nicht von vornherein abgelehnt hat.“*

E-Mail-Werbung ist danach nur zulässig, wenn das Unternehmen die E-Mail-Adresse „im Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung [...] erhalten hat“. Es reicht also beispielsweise nicht, wenn sich ein Kunde wegen einer Reklamation per E-Mail an das Unternehmen wendet, denn in einem solchen Fall kann von einem Einverständnis mit Werbung nicht ausgegangen werden. Schließlich ist E-Mail-Werbung nach der Richtlinie nur für „eigene ähnliche Produkte oder Dienstleistungen“ zulässig. Die beworbenen Produkte müssen also denjenigen vergleichbar sein, für die sich der Verbraucher im Rahmen eines Verkaufsgesprächs interessiert hat. Zur korrekten Umsetzung dieser Einschränkungen ist § 95 Abs. 2 S. 2 TKG wie hier vorgeschlagen anzupassen.

Die Richtlinie erlaubt eine Datennutzung zu Werbezwecken zudem nur, wenn Kunden „die Möglichkeit erhalten, eine solche Nutzung ihrer elektronischen Kontaktinformationen bei deren Erhebung und bei jeder Übertragung gebührenfrei und problemlos abzulehnen“. Das nach deutschem Recht bestehende Widerspruchsrecht ermöglicht es nicht, die Nutzung der eigenen Daten zu Werbezwecken „problemlos abzulehnen“. Vielmehr setzt ein Widerspruch voraus, mit dem Anbieter umständlich in Verbindung zu treten, indem man eine gesonderte Nachricht an ihn verfasst, die oftmals mit Kosten verbunden ist (z.B. Brief, SMS). Wegen des damit verbundenen Aufwands gewährleistet § 95 Abs. 2 TKG das Recht auf informationelle Selbstbestimmung nicht hinreichend.

Die Möglichkeit der gebührenfreien und „problemlosen Ablehnung“ einer Nutzung der eigenen Daten zu Werbezwecken ist nur dann gegeben, wenn der Kunde bei jeder Datenerhebung und -nutzung unmittelbar widersprechen kann, etwa durch Klicken auf ein Auswahlfeld oder auf einen Link. Eine derartige unmittelbare Widerspruchsmöglichkeit wird dem Nutzer bereits heute verbreitet eingeräumt (z.B. bei der Anmeldung zu Internet-Diensten oder bei Email-„Newslettern“). Den Diensteanbietern ist es ohne weiteres zumutbar, dem Nutzer eine unmittelbare und kostenfreie Widerspruchsmöglichkeit einzuräumen. Dies sieht folglich der Änderungsvorschlag vor.

5. Keine Vorratsspeicherung von Bestandsdaten (§ 95 TKG)

Geltendes Telekommunikationsgesetz (TKG)	**Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen**	**Nr**	**Änderungsvorschlag**
§ 95 Bestandsdaten	*(unverändert)*		*(unverändert)*
(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.	*(unverändert)*	5	***(entfällt)***

§ 95 Abs. 3 TKG verpflichtet Kommunikationsmittler zur Vorratsspeicherung betrieblich nicht erforderlicher Bestandsdaten für die Dauer von 1-2 Jahren. Dabei handelt es sich um so sensible Daten wie Geburtsdatum, Privatanschrift, Gerätenummer von Mobilfunkgeräten, Datum des Vertragsbeginns, Bankverbindung, Kundennummer, Passwort, Inhalt eines elektronischen Telefonbuchs und Kurzwahlnummern. Sämtliche dieser Kundendaten sind nach § 95 Abs. 3 TKG auf Vorrat zu speichern.

Folgt man bei der verfassungsrechtlichen Würdigung des Bundesverfassungsgerichts mit Urteil vom 2. März 2010, so ist § 95 Abs. 3 TKG aus den folgenden Gründen verfassungswidrig:

- Die Sicherheit der anlasslos vorzuhaltenden Kommunikationsdaten genügt nicht den verfassungsrechtlichen Anforderungen.[8] Der Verlust sämtlicher 17 Mio. Kundendaten von T-Mobile (jetzt: Telekom Deutschland) beispielsweise setzte Politiker, Funktionäre und andere exponierte Personen erheblichen Gefahren aus, weil ihre geheimen Privatanschriften Unbefugten in die Hände gelangt waren.[9] Die Daten gelangten auch an die Moderation der Comedy-Sendung „Schmidt & Pocher“ in der ARD, die dies zum Anlass nahm, den Fernsehmoderator Günther Jauch vor laufender Kamera unter dessen Privatnummer anzurufen und öffentlich vorzuführen.[10]
- § 95 Abs. 3 TKG ist zweitens verfassungswidrig, weil schon die von der EU beschlossene Mindestspeicherfrist von sechs Monaten dem Bundesverfassungsgericht zufolge an der Grenze des verfas-

8 BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 221 ff.

9 Spiegel vom 04.10.2008, http://www.spiegel.de/wirtschaft/0,1518,581938,00.html.

10 Sendung Nr. 22 vom 9. Oktober 2008, http://www.schmidt-news.com/showguide_schmidt-pocher2008.php.

sungsrechtlich Vertretbaren liege,[11] Kundendaten gemäß § 95 Abs. 3 TKG aber mindestens doppelt so lange auf Vorrat zu speichern sind (1-2 Jahre).

- § 95 Abs. 3 TKG ist drittens verfassungswidrig, weil er über die europarechtlich vorgesehene Vorratsspeicherung von Name, Anschrift und Anschlusskennung der Nutzer öffentlicher Kommunikationsdienste hinaus geht. Das Bundesverfassungsgericht hat entschieden, dass die Beurteilung der grundsätzlichen Zulässigkeit der Vorratsspeicherung von Verkehrsdaten nicht auf andere Datensammlungen übertragen werden dürfe[12] und hat auch seine verfassungsrechtliche Zulassung einer Vorratsdatenspeicherung weitgehend auf die EU-Vorgaben beschränkt. Es heißt in dem Urteil wörtlich: „*Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt vielmehr voraus, dass diese eine Ausnahme bleibt.*“[13] § 95 Abs. 3 TKG betrifft keine „Telekommunikationsverkehrsdaten“.

Richtigerweise ergibt sich die Nichtigkeit des § 95 Abs. 3 TKG bereits daraus, dass das Prinzip einer anlasslosen, flächendeckenden Vorratsdatenspeicherung - unabhängig von ihrer Ausgestaltung - das Gebot der Verhältnismäßigkeit verletzt. Dementsprechend ist entsprechend dem Gebot der Datensparsamkeit eine unverzügliche Löschung der sensiblen Kundendaten vorzunehmen, sobald ihre Speicherung betrieblich nicht mehr erforderlich ist, wobei erforderlichenfalls stattdessen eine Sperrung vorzunehmen ist, wenn eine Löschung nicht zulässig ist. Dies ergibt sich bereits aus § 95 Abs. 1 TKG i.V.m. § 35 BDSG, so dass es einer besonderen Löschungsregelung in § 95 TKG nicht bedarf. § 95 Abs. 3 TKG kann ersatzlos wegfallen.

[11] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 215.

[12] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 218.

[13] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 218.

6. Schutz vor zwangsweiser Datenerhebung (Koppelungsverbot, § 95 TKG)

Geltendes Telekommunikationsgesetz (TKG)	**Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen**	**Nr**	**Änderungsvorschlag**
§ 95 Bestandsdaten	*(unverändert)*		*(unverändert)*
(5) Die Erbringung von Telekommunikationsdiensten **darf nicht von einer Einwilligung des Teilnehmers in eine Verwendung seiner Daten für andere Zwecke abhängig gemacht werden,** wenn dem Teilnehmer ein anderer Zugang zu diesen Telekommunikationsdiensten **nicht oder in nicht** zumutbarer Weise möglich ist.	*(unverändert)*	6	(5) **Der Diensteanbieter darf** die Erbringung von Telekommunikationsdiensten **nicht von der Angabe personenbezogener Daten abhängig machen, die zur Erbringung der Telekommunikationsdienste nicht erforderlich sind. Entsprechendes gilt für die Einwilligung des Teilnehmers in die Verarbeitung oder Nutzung der Daten für andere Zwekke. Die Sätze 1 und 2 gelten nicht,** wenn dem Teilnehmer ein anderer Zugang zu diesen Telekommunikationsdiensten in zumutbarer Weise möglich ist. **Im Fall des Satzes 3 hat der Diensteanbieter** **1. kenntlich zu machen, von welchen Angaben oder Einwilligungserklärungen die Erbringung der Telekommunikationsdienste abhängig gemacht wird und** **2. die Unterrichtung des Teilnehmers nach § 93 Abs. 1 auch darauf zu erstrecken, in welcher Weise ein anderer Zugang zu diesen Telekommunikationsdiensten möglich ist.**

Zur Vorbeugung von Missbrauch von Telekommunikationsdaten ist eine Neugestaltung des § 95 Abs. 5 TKG erforderlich. Der Bundesrat beklagte in seiner Stellungnahme zum ElGVG[14] zurecht: *„In der jetzigen Praxis gewähren die Anbieter von Online-Dienstleistungen den Verbrauchern häufig nur Zugang zu diesen Diensten, wenn eine Zustimmung zu einer weit reichenden Datenverwendung erteilt wird. [...] Es ist nicht ersichtlich, warum ein Verbraucher dem Anbieter von Online-Diensten als Voraussetzung zur Nutzung dieser Dienste persönliche Informationen zu einer umfangreichen Verwendung zugestehen sollte. Diese Zustimmung erfolgt somit nur, um den angebotenen Dienst nutzen zu können und entspricht nicht der Willensfreiheit des Zustimmenden.“* Dasselbe gilt für Telekommunikationsdienste.

[14] BR-Drs. 556/06 (B), 2.

In der Tat begegnen gerade Internetnutzern immer wieder Telekommunikationsdienste, deren Bereitstellung von der Offenbarung von Geburtsdatum, Beruf oder persönlichen Interessen abhängig gemacht wird (z.B. E-Mail-Dienste, Chatdienste). Entsprechende Angaben werden unter anderem zu Werbezwecken genutzt; sie sind auch schon illegal verkauft oder verloren worden. Aus einem Internet-Forum des ZDF-Kinderkanals konnten sich etwa beliebige Personen Klarnamen, Adresse, Telefonnummer und Geburtsdatum aller 1.000 registrierten Kinder verschaffen.[15] Wegen der vielen Fälle von Datenmissbrauch sind inzwischen 80% der Bundesbürger „sehr besorgt" um die Sicherheit ihrer Daten vor unbefugtem Zugriff oder Missbrauch.[16] Eine deutliche Mehrheit der Bevölkerung fordert eine Stärkung des gesetzlichen Datenschutzes.[17]

Zur Verhinderung von Datenmissbrauch und zur Stärkung des Nutzervertrauens muss die zwangsweise Erhebung überflüssiger Daten unterbunden werden. Davon profitiert auch die Wirtschaft, denn die daraus resultierende Missbrauchsgefahr hält viele Bürger von der Nutzung entsprechender Dienste ab.[18]

Neben der Angabe überflüssiger Daten wird die Erbringung von Telekommunikationsdiensten oft auch davon abhängig gemacht, dass der Nutzer eine – meist unklar formulierte und mehrere Seiten lange – Einwilligungserklärung abgibt. Insbesondere Internetunternehmen mit US-amerikanischen Muttergesellschaften nutzen diese Möglichkeit, um die gesetzlichen Regelungen quasi insgesamt abzubedingen: Sie verlangen bei der Anmeldung die Einwilligung des Kunden, jeden Klick und jede Eingabe des Nutzers auf Vorrat speichern zu dürfen, vorgeblich, um Missbrauch bekämpfen und eine bedarfsgerechte Gestaltung ihrer Dienste anbieten zu können. Bei nicht im Internet tätigen Unternehmen ist es unüblich, sich eine Einwilligung in die Verarbeitung personenbezogener Daten über das erforderliche Maß hinaus erteilen zu lassen. Da nicht im Internet tätige Unternehmen problemlos auch ohne eine solche Einwilligung auskommen, ist ein berechtigtes Interesse der Anbieter von Telekommunikationsdiensten hieran nicht ersichtlich. Es widerspricht dem Zweck des Telekommunikationsgesetzes, Internetanbietern über den Umweg der Einwilligung eine weiter gehende Datenverarbeitung zu erlauben als sie bei nicht im Internet tätigen Unternehmen derselben Branche üblich ist.

Es genügt nicht, Nutzer lediglich auf andere Anbieter zu verweisen, die auf die Erhebung und Verarbeitung unnötiger persönlicher Daten bzw. auf eine entsprechende Einwilligung verzichten. Diese alternativen Anbieter bieten nämlich nicht dieselben Dienstleistungen zu denselben Konditionen an, weshalb keine echte Wahlmöglichkeit des Nutzers besteht.

Zur Lösung des Problems ist eine Neufassung des § 95 Abs. 5 TKG erforderlich. Die hier vorgeschlagene Formulierung der Sätze 1 und 2 entspricht § 3 Abs. 2 S. 1 und 2 der ehemaligen Telekommunikations-Datenschutzverordnung (TDSV). [19] Die Formulierung des bisherigen § 95 Abs. 5 TMG ist unzureichend, weil sie den in der Praxis sehr verbreiteten Fall nicht erfasst, dass Diensteanbieter die Erbringung eines Telekommunikationsdienstes von der Angabe nicht erforderlicher personenbezogener Daten abhängig machen. Die Regelung des § 95 Abs. 1 TKG genügt zur Lösung des Problems nicht, weil sie sich durch Einsatz vorformulierter Einwilligungserklärungen aushebeln lässt.

Satz 3 des Änderungsvorschlags macht eine Ausnahme von den Sätzen 1 und 2. Eine Bestimmung, die eine alternative Zugangsmöglichkeit genügen lässt, fand sich zwar nicht in § 3 Abs. 2 TDSV. Jedoch stellt § 95 Abs. 5 TKG darauf ab, ob dem Nutzer ein anderer Zugang möglich ist. Die Klausel kann daher

---

15 Spiegel Online vom 16.10.2008: Kika stellt Daten von Kindern ungeschützt ins Web.

16 Unisys-Umfrage vom 01.10.2008, http://www.unisyssecurityindex.com/resources/reports/-Germany%20security%20index%20Oct%201-08.pdf.

17 Emnid-Umfrage vom 02.06.2008, http://www.presseportal.de/pm/13399/1204206/n24/rss.

18 Vgl. die Umfrage von Forrester Custom Consumer Research, http://www.bsa.org/germany/presse/newsreleases/upload/BSA-Forrester-Deutsch.ppt.

19 Die Bestimmung lautete: „(2) Diensteanbieter dürfen die Erbringung von Telekommunikationsdiensten nicht von der Angabe personenbezogener Daten abhängig machen, die nicht erforderlich sind, um diese Dienste zu erbringen. Entsprechendes gilt für die Einwilligung des Beteiligten in die Verarbeitung oder Nutzung der Daten für andere Zwecke. Erforderlich können auch Angaben sein, die mit einem Telekommunikationsdienst in sachlichem Zusammenhang stehen."

– wenn sich der Gesetzgeber nicht zu ihrer Streichung entschließt – in abgewandelter Form beibehalten werden. Allerdings muss eine Beweislastumkehr und eine Informationspflicht vorgesehen werden. Der Anbieter, der unnötige persönliche Daten erheben oder verarbeiten will, muss also darlegen und beweisen, dass dem Nutzer eine zumutbare Alternative zur Verfügung steht (Satz 3 des Änderungsvorschlags), und er muss den Nutzer darüber unterrichten, in welcher Weise ein anderer Zugang möglich ist (Satz 4 Nr. 2 des Änderungsvorschlags). Während diese Informationen dem Anbieter, der sich auf alternative Zugangsmöglichkeiten beruft, bekannt sein müssen, müssten Nutzer alternative Zugangsmöglichkeiten erst mühsam recherchieren.

Auch ist das informationelle Selbstbestimmungsrecht des Nutzers nur gewährleistet, wenn er bestimmen kann, ob er dem von ihm ausgewählten Dienst freiwillig die Erhebung oder Verarbeitung nicht erforderlicher persönlicher Daten erlaubt. Deswegen legt Satz 3 des Änderungsvorschlags fest, dass jeder Anbieter eine Zugangsmöglichkeit zu seinen Diensten anbieten muss, die ohne Erhebung oder Verarbeitung nicht erforderlicher persönlicher Daten auskommt. Unbenommen bleibt es den Anbietern, für solche Zugänge ein Entgelt oder eine zusätzliches Entgelt in zumutbarer Höhe zu erheben, um entgangene Einnahmen auszugleichen, die sie bei Angabe persönlicher Daten oder bei Abgabe einer Einwilligung durch den Nutzer oder ohne seinen Widerspruch hätten erzielen können (z.B. durch Werbung). Die daraus resultierende Möglichkeit der Nutzer, ihre persönlichen Daten „verkaufen“ zu können, ist freiheits- und marktgerechter als ein Recht der Anbieter, die Frage ohne Wahlrecht des Nutzers einseitig selbst zu entscheiden.

Weiter ist in Satz 4 Nr. 1 des Änderungsvorschlags vorgesehen, dass gegenüber dem Nutzer kenntlich zu machen ist, von welchen Angaben oder Einwilligungserklärungen die Erbringung des Dienstes anhängig gemacht wird. Während manche Telekommunikationsanbieter Pflichtangaben bereits heute kenntlich machen (z.B. durch ein Sternchen), erfährt man bei anderen Diensten die Pflichtangaben erst dadurch, dass man versucht, sich ohne die Angaben anzumelden. Dieser Aufwand ist den Nutzern nicht zumutbar. Den Diensteanbietern ist eine Kennzeichnung von Pflichtangaben ohne Weiteres möglich. Eine solche Kennzeichnung ermöglicht es den Nutzern, von ihrem Recht auf informationelle Selbstbestimmung Gebrauch zu machen. Die vorgeschlagene Regelung ist daher ein wichtiger Schritt zu mehr Transparenz.

7. Recht auf anonyme Telekommunikation (§ 95 TKG)

Geltendes Telekommunikationsgesetz (TKG)	**Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen**	**Nr**	**Änderungsvorschlag**
§ 95 Bestandsdaten	*(unverändert)*		*(unverändert)*
		7	**(6) Der Diensteanbieter hat die Inanspruchnahme von Telekommunikationsdiensten und ihre Bezahlung anonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Die anonyme Bereitstellung ist zumutbar, wenn Telekommunikationsdienste dieser Art am Markt anonym angeboten werden, es sei denn, dass die besonderen Verhältnisse des Diensteanbieters entgegen stehen. Der Teilnehmer ist über die Möglichkeit der anonymen Inanspruchnahme zu informieren.**

Der Grundsatz der Anonymität (vgl. § 13 Abs. 6 TMG) konkretisiert den allgemeinen Grundsatz der Datenvermeidung und Datensparsamkeit (§ 3a BDSG). Können Telekommunikationsdienste anonym genutzt werden, so brauchen sich Verbraucher keine Sorgen um einen Missbrauch ihrer Daten zu machen. Umfragen zeigen, dass gerade solche Sorgen bisher viele Verbraucher von der unbefangenen Nutzung der neuen Medien abhalten. Das Geschäft der Diensteanbieter wird durch anonyme Dienste also gefördert. Gerade das Geschäftsmodell kostenfreier Telekommunikationsdienste, wie sie im Internet verbreitet angeboten werden (z.B. E-Mail, Chat, Internettelefonie), basiert auf Werbung, zu deren Einblendung es keiner personenbezogenen Daten bedarf. Im „wirklichen" Leben bewegen sich die Bürger ganz regelmäßig anonym. Es gibt keinen Grund, warum dies im virtuellen Leben anders sein sollte.

Nach einer aktuellen Meinungsumfrage aus dem Jahr 2010[20] ist nur 14% der Bevölkerung der Meinung, sie könnten ihre Daten Telefonanbietern ohne die Gefahr von Missbrauch anvertrauen. 68% befürchten die Nutzung persönlicher Daten zu Werbezwecken, 66% den Missbrauch ihrer Angaben und 54% die Weitergabe der Angaben an andere Unternehmen. 50% der Befragten hat „schon häufiger" darauf verzichtet, etwas zu bestellen, weil sie ihre Daten nicht preisgeben wollten. 18% bestellen im Internet grundsätzlich nichts, weil sie ihre Daten nicht preisgeben wollen. Diese Ergebnisse zeigen, dass anonyme und datensparsame Dienste ein hohes Wirtschaftspotenzial aufweisen. Sie könnten Kreise von Kunden erschließen, die nur im Schutz der Anonymität zur Inanspruchnahme entsprechender Dienste bereit sind.

Vor diesem Hintergrund ist es wichtig, eine an § 13 Abs. 6 TMG angelehnte Anonymitätsgarantie auch für Telekommunikationsdienste einzuführen. Allerdings wird vorgeschlagen, den Verweis auf ein pseudonymes Angebot nicht zu übernehmen (Satz 1 des Änderungsvorschlags). Dieser Verweis birgt die Gefahr, dass Diensteanbieter die Vergabe von Pseudonymen als gleichwertige Alternative zu einem anonymen Angebot ansehen. Verfügt der Diensteanbieter jedoch über die Zuordnungsfunktion eines Pseudonyms, so bietet dieses keinen wirksamen Schutz der personenbezogenen Daten, was auch für den Verbraucher offensichtlich ist. Die Vergabe von Pseudonymen darf daher nicht als gleichwertige Alternative zu einem anonymen Angebot dargestellt werden. Vielmehr muss ein anonymes Angebot den Regelfall darstellen. Nur dies verhindert Datenmissbrauch effektiv und gewährleistet das Nutzervertrauen.

Auch ist eine Präzisierung des unbestimmten Begriffs der Zumutbarkeit und eine Umkehr der Darlegungs- und Beweislast erforderlich (Satz 2 des Änderungsvorschlags), um dem gewollten Regelfall eines anonymen Angebots zur Geltung zu verhelfen. Satz 2 des Änderungsvorschlags hat Dienste zum Gegenstand, die in der Praxis bereits erfolgreich anonym angeboten werden. Werden Dienste einer Art erfolgreich anonym angeboten, ist zunächst einmal kein Grund dafür ersichtlich, warum ein anonymes Angebot nicht auch anderen Anbietern von Diensten dieser Art zumutbar sein soll. In solchen Fällen muss es dem Anbieter obliegen, darzulegen, warum gerade ihm ein anonymes Angebot unzumutbar sein soll. Gründe hierfür können nur in seinen besonderen Verhältnissen liegen. In diese haben Außenstehende keinen Einblick, so dass eine Beweislastumkehr angemessen ist.

Unbenommen bleibt es den Anbietern, für anonyme Zugänge ein Entgelt oder ein zusätzliches Entgelt zu erheben, um entgangene Einnahmen auszugleichen, die sie bei Angabe persönlicher Daten durch den Nutzer hätten erzielen können (z.B. durch Werbung). Die daraus resultierende Möglichkeit der Nutzer, ihre persönlichen Daten „verkaufen" zu können, ist freiheits- und marktgerechter als ein Recht der Anbieter, die Frage ohne Wahlrecht des Nutzers einseitig selbst zu entscheiden. Die anonyme Bezahlung von Entgelten kann unschwer angeboten werden, nämlich insbesondere mittels vorausbezahlter Bezahlkarten (z.B. „Ukash", „Paysafecard").

[20] Allensbacher Institut für Demoskopie, „Einstellung der Deutschen zum Thema Datenschutz" (August 2010), http://www.webcitation.org/5t9uDMnHb.

8. Schutz vor Zweckentfremdung von Verbindungsdaten (§ 96 TKG)

Geltendes Telekommunikationsgesetz (TKG)	**Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen**	**Nr**	**Änderungsvorschlag**
§ 96 Verkehrsdaten	*(unverändert)*		*(unverändert)*
(1) Der Diensteanbieter darf folgende Verkehrsdaten erheben, soweit dies für die in diesem Abschnitt oder in § 2 oder § 4 des Zugangserschwerungsgesetzes genannten Zwecke erforderlich ist:	*(unverändert)*	8	(1) Der Diensteanbieter darf folgende Verkehrsdaten erheben, soweit dies für die in diesem Abschnitt oder in § 2 oder § 4 des Zugangserschwerungsgesetzes genannten Zwecke erforderlich ist:
1. 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,			1. 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,
2. den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,			2. den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
3. den vom Nutzer in Anspruch genommenen Telekommunikationsdienst,			3. den vom Nutzer in Anspruch genommenen Telekommunikationsdienst,
4. die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,			4. die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
5. sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.			5. sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.
Diese Verkehrsdaten dürfen nur verwendet werden, soweit **dies für die in Satz 1 genannten oder durch andere gesetzliche Vorschriften begründeten**			Diese Verkehrsdaten dürfen nur verwendet werden, soweit

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
Zwecke oder zum Aufbau weiterer Verbindungen erforderlich ist. Im Übrigen sind Verkehrsdaten vom Diensteanbieter **nach Beendigung der Verbindung unverzüglich zu löschen**.			**sie zum Aufbau weiterer Verbindungen oder für die in den §§ 97, 99, 100 und 101 genannten Zwecke erforderlich sind.** Im Übrigen sind Verkehrsdaten vom Diensteanbieter **zu löschen, sobald die Verbindung beendet ist**. **Vorschriften in anderen Gesetzen, die sich ausdrücklich auf Telekommunikationsvorgänge beziehen, bleiben unberührt.**

Zu § 96 Abs. 1 S. 2 TKG:

§ 96 Abs. 2 S. 1 TKG lautete bis Herbst 2006: „*Die gespeicherten Verkehrsdaten dürfen über das Ende der Verbindung hinaus nur verwendet werden, soweit sie zum Aufbau weiterer Verbindungen oder für die in den §§ 97, 99, 100 und 101 genannten Zwecke erforderlich sind.*“ Diese Vorschrift lautet aufgrund des Gesetzes zur Änderung telekommunikationsrechtlicher Vorschriften nun wie folgt: „*Die gespeicherten Verkehrsdaten dürfen über das Ende der Verbindung hinaus nur verwendet werden, soweit sie zum Aufbau weiterer Verbindungen oder für die in den §§ 97, 99, 100 und 101 genannten oder für die durch andere gesetzliche Vorschriften begründeten Zwecke erforderlich sind.*“ Zur Begründung ist angeführt worden, die bisherige Formulierung führe „*zu dem nicht beabsichtigten Rückschluss, dass die Daten nicht für die durch die §§ 100g, 100h StPO, § 8 Abs. 8 und 10 BVerfSchG, § 10 Abs. 3 MAD-Gesetz und § 8 Abs. 3a BND-Gesetz sowie durch Landesrecht geregelte Erteilung von Auskünften über Verkehrsdaten an die Strafverfolgungs- und Sicherheitsbehörden verwendet werden dürften.*“

So legitim das Anliegen ist, diese Frage klarzustellen, so ungeeignet und gefährlich ist die erfolgte Umformulierung. Es ist vollkommen unklar und unbestimmt, was „durch andere gesetzliche Vorschriften begründete Zwecke“ sein sollen. Diese Formulierung erlaubt die Auslegung, dass jegliche gesetzliche Auskunfts- oder Übermittlungsregelungen auch auf Telekommunikationsdaten Anwendung finden. Dies darf aber mitnichten der Fall sein, weil Verkehrsdaten dem Fernmeldegeheimnis unterliegen. § 88 Abs. 3 TKG erlaubt eine Verwendung zu anderen Zwecken deshalb nur, „soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht.“ Die gegenwärtige Formulierung des § 96 Abs. 1 S. 2 TKG hebelt diesen Schutz wieder aus.

Auch erlaubt es die gewählte Formulierung undifferenziert, Daten zu spezialgesetzlichen Zwecken zu „verwenden“, also auch etwa zu speichern. Dies würde die Interpretation erlauben, dass Daten, die an sich zu löschen wären, für den Fall auf Vorrat gespeichert werden dürfen, dass sie irgendwann einmal für „durch andere gesetzliche Vorschriften begründete Zwecke erforderlich sind“.

Schließlich steht mit der Entscheidung des Bundesverfassungsgerichts zum automatisierten Kontenabruf[21] nicht im Einklang, dass der Kreis der zugriffsberechtigten Behörden nicht bestimmt ist.[22]

§ 96 Abs. 2 TKG sollte stattdessen in seiner ursprünglichen Fassung wieder hergestellt und durch einen klarstellenden Satz ergänzt werden, wie es Gegenstand des vorliegenden Änderungsvorschlags ist. Mit dieser Formulierung wird ohne Weiteres das Ziel erreicht, klarzustellen, dass spezialgesetzliche Vorschriften unberührt bleiben. Gleichzeitig wird die Übereinstimmung mit § 88 Abs. 3 TKG gewährleistet

21 BVerfG NJW 2007, 2464.

22 Gola/Klug/Reif, NJW 2007, 2599 (2601).

und sichergestellt, dass Verkehrsdaten nur insoweit zu anderen Zwecken gespeichert oder übermittelt werden, wie es spezialgesetzlich auch vorgesehen ist.

Zu § 96 Abs. 1 S. 3 TKG:

§ 96 Abs. 1 S. 3 TKG bedarf der Anpassung an europarechtliche Vorgaben. In der gegenwärtigen Fassung ist § 96 Abs. 1 S. 3 TKG zu unbestimmt und führt zu divergierenden Auslegungen hinsichtlich der Frage, was unter einer „unverzüglichen" Löschung zu verstehen ist. Teilweise wird sogar eine Löschung erst nach sieben Tagen noch als „unverzüglich" angesehen,[23] was der Schutzwürdigkeit von Informationen über unsere Kommunikationspartner keinesfalls Rechnung trägt. Im Bereich des bürgerlichen Rechts sieht die Rechtsprechung sogar eine Frist von zwei Wochen als „unverzüglich" an, was noch weiter von Sinn und Zweck des § 96 TKG entfernt ist.

Demgegenüber bestimmt Art. 6 Abs. 1 RiL 2002/58/EG eindeutig: „*Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen Kommunikationsdienstes verarbeitet und gespeichert werden, sind unbeschadet der Absätze 2, 3 und 5 des vorliegenden Artikels und des Artikels 15 Absatz 1 zu löschen oder zu anonymisieren, **sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden***."

Zur korrekten Umsetzung dieser Vorschrift muss im deutschen Recht klargestellt werden, dass Verkehrsdaten zu löschen sind, „sobald" die Verbindung beendet ist. Dies entspricht nach richtiger Auffassung bereits der geltenden Rechtslage.[24]

[23] OLG Frankfurt, MMR 2010, 645.

[24] OLG Karlsruhe, MMR 2009, 412; LG Darmstadt, MMR 2006, 330; AG Darmstadt, MMR 2005, 634.

9. Recht auf sofortige Verbindungsdatenlöschung (§ 97 TKG)

Geltendes Telekommunikationsgesetz (TKG)	**Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen**	**Nr**	**Änderungsvorschlag**
§ 97 Entgeltermittlung und Entgeltabrechnung	*(unverändert)*		*(unverändert)*
(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. Diese Daten dürfen bis zu sechs Monate nach Versendung der Rechnung gespeichert werden. Für die Abrechnung nicht erforderliche Daten sind unverzüglich zu löschen**, soweit sie nicht nach § 113a zu speichern sind**. Hat der Teilnehmer gegen die Höhe der in Rechnung gestellten Verbindungsentgelte vor Ablauf der Frist nach Satz 2 Einwendungen erhoben, dürfen die Daten gespeichert werden, bis die Einwendungen abschließend geklärt sind.	(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. Diese Daten dürfen bis zu sechs Monate nach Versendung der Rechnung gespeichert werden. Für die Abrechnung nicht erforderliche Daten sind unverzüglich zu löschen~~, soweit sie nicht nach § 113a zu speichern sind~~. Hat der Teilnehmer gegen die Höhe der in Rechnung gestellten Verbindungsentgelte vor Ablauf der Frist nach Satz 2 Einwendungen erhoben, dürfen die Daten gespeichert werden, bis die Einwendungen abschließend geklärt sind.	9	(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. Für die Abrechnung nicht erforderliche Daten sind unverzüglich zu löschen. **Die Verkehrsdaten dürfen unter Kürzung der Zielnummer um die letzten drei Ziffern zu Beweiszwecken für die Richtigkeit der berechneten Entgelte – vorbehaltlich des Absatzes 4 – höchstens sechs Wochen 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 Daten gespeichert werden, bis die Einwendungen abschließend geklärt sind. **(4) Auf Verlangen des Teilnehmers hat der rechnungstellende Diensteanbieter** **1. die Zielnummer vollständig zu speichern oder** **2. das Entgelt zu berechnen und die Verkehrsdaten vollständig zu löschen, sobald die Verbindung beendet ist.** **Soweit ein Kunde zur vollständigen oder teilweisen Übernahme der Entgelte für bei seinem Anschluss ankommende Verbindungen verpflichtet ist, steht ihm das**

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
			Wahlrecht nach Nummer 1 nicht zu. Die Sätze 1 und 2 gelten nicht für Diensteanbieter, die als Anbieter geschlossener Benutzergruppen ihre Dienste nur ihren Teilnehmern anbieten.
(4) 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.	*(unverändert)*		*(wird zu Absatz 5)*

In vielen Situationen müssen sich Menschen beruflich (z.B. Geheimnisträger) oder wegen ihrer persönlichen Lebenssituation (z.B. Krankheit, Abhängigkeit, seelische Störung) darauf verlassen können, dass ihre Gesprächspartner – und damit oft auch Hinweise auf den Inhalt des Gesprächs – Dritten nicht zur Kenntnis gelangen. Deshalb ist es von hoher Bedeutung, Telekommunizierenden das Recht zu geben, die Aufzeichnung von Informationen über ihre Telekommunikation zu verhindern.

Vor Einführung digitaler Vermittlungsstellen sind Informationen über die einzelnen Verbindungen nicht erfasst worden. Es ist auf der Grundlage einer Taktung abgerechnet worden. Im Zeitalter der Digitalisierung ist es den Anbietern erst recht möglich, nach dem Ende einer Verbindung sogleich das darauf entfallende Entgelt zu ermitteln, dem Kundenkonto zu belasten und alle Verbindungsspuren zu löschen. § 7 TDSV sah wenigstens eine Verkürzung der Zielrufnummern und, auf Wunsch des Teilnehmers, eine Löschung aller Verbindungsdaten mit Rechnungsversand vor. § 97 TKG a.F. sah dann nur noch eine Löschung der Zielrufnummern auf Wunsch des Teilnehmers vor. Mit Einführung der Vorratsdatenspeicherung entfiel das Wahlrecht ohne Begründung ganz. Der nun vorliegende Referentenentwurf will daran – wiederum ohne Begründung – nichts ändern und nicht einmal die Rechtslage vor Einführung der verfassungswidrigen Vorratsdatenspeicherung wieder herstellen. Dies ist nicht hinnehmbar, zumal früher viele Teilnehmer eine frühestmögliche Verbindungsdatenlöschung gewählt hatten.

Das Bundesverfassungsgericht hat entschieden,[25] auch eine nur kurzfristige Speicherung von Verkehrsdaten berühre das Interesse des Betroffenen an der Wahrung seines Fernmeldegeheimnisses in nicht ganz unerheblichem Ausmaß. Aufgrund der Speicherung könne das Telekommunikationsunternehmen diese Daten zu eigenen Zwecken verwenden. Darüber hinaus bestehe die Möglichkeit eines staatlichen Zugriffs, etwa aufgrund des § 100 g StPO. Auch das Risiko eines Missbrauchs der Verkehrsdaten durch das Telekommunikationsunternehmen oder durch Dritte, die sich unbefugt Zugang zu ihnen verschaffen, sei nicht völlig auszuschließen. Anbieter müssten daher „eine datenschutzfreundliche technische Gestaltung“ wählen, wobei alle „allgemein möglichen und zumutbaren technischen Gestaltungen des Umgangs mit Verkehrsdaten“ zu berücksichtigen seien. Es sei nicht offenkundig, dass eine sofortige Löschung der Verkehrsdaten nach Gesprächsende nicht in Betracht komme. Bei Prepaid-Karten werde das geschuldete Entgelt unmittelbar nach Verbindungsende ermittelt und von dem Kartenguthaben abgezogen. Dementsprechend sei nicht ohne weiteres nachvollziehbar, warum eine bis zu einem fiktiven Abrechnungsdatum fortdauernde Speicherung der Verkehrsdaten erheblich kostengünstiger oder gar technisch erforderlich

[25] BVerfG, 1 BvR 1811/99 vom 27.10.2006.

sein soll. Weitere Speicherungsinteressen der Anbieter, die mit dem Löschungsinteresse der Teilnehmer kollidieren und im Rahmen einer Abwägung überwiegen müssten, seien nicht ersichtlich.

Gleiches gilt für andere Anbieter. Alle Anbieter können nach Verbindungsende sogleich das angefallene Entgelt ermitteln und dem Kundenkonto belasten, ohne Aufzeichnungen über die einzelnen Verbindungen führen zu müssen. Dementsprechend ist es verfassungsrechtlich geboten, Telekommunizierenden das Recht zu geben, die Speicherung von Verkehrsdaten zu untersagen, weil diese bei „datenschutzfreundlicher technischer Gestaltung“ zur Gebührenabrechnung nicht erforderlich ist. Zudem dürfen Zielrufnummern nur verkürzt gespeichert werden, weil die Kenntnis der genauen Zielrufnummer für Beweiszwecke nicht erforderlich ist. Der Anbieter ist insoweit nicht beweispflichtig (§ 45i Abs. 2 TKG).

Der hier unterbreitete Vorschlag zur Neufassung des § 97 TKG orientiert sich an § 7 TDSV, berücksichtigt aber die neuere Rechtsprechung des Bundesverfassungsgerichts. Außerdem wird die zulässige Speicherfrist auch sechs Wochen nach Rechnungsversand verkürzt. Die Frist entspricht etwa der im Bankenwesen anerkannten Frist für Beanstandungen und gibt den Teilnehmern ausreichend Gelegenheit zur Prüfung der Rechnung. Eine kürzere Frist als bisher dient nicht nur dem Datenschutz, sondern auch dem Rechtsfrieden und der Vermeidung von Streitigkeiten.

10. Schutz vor Missbrauch von Verbindungsdaten (§ 100 TKG)

Geltendes Telekommunikationsgesetz (TKG)	**Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen**	**Nr**	**Änderungsvorschlag**
§ 100 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten	*(unverändert)*		*(unverändert)*
(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.**	*(unverändert)*	10	(1) **Liegen dem Diensteanbieter im Einzelfall zu dokumentierende tatsächliche Anhaltspunkte vor, dass bestimmte Teilnehmer oder Nutzer seine zur Bereitstellung seines Dienstes genutzten technischen Einrichtungen stören, darf er Bestands- und Verkehrsdaten dieser Teilnehmer oder Nutzer nur erheben, speichern und nutzen, soweit dies zur Beseitigung der Störung erforderlich ist; eine Verwendung der Daten für andere Zwecke ist unzulässig. Der Diensteanbieter hat die Daten unverzüglich zu löschen, wenn die Voraussetzungen nach Satz 1 nicht mehr vorliegen oder die Daten zur Störungsbeseitigung nicht mehr benötigt werden. Die betroffenen Teilnehmer oder Nutzer sind zu unterrichten, sobald dies**

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
			ohne Gefährdung des mit der Maßnahme verfolgten Zweckes möglich ist.
(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 erforderlich 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 Bundesnetzagentur und	*(unverändert)*		**(3) Liegen dem Diensteanbieter im Einzelfall zu dokumentierende tatsächliche Anhaltspunkte vor, dass seine Dienste von bestimmten Teilnehmern oder Nutzern in der Absicht in Anspruch genommen werden, das Entgelt nicht oder nicht vollständig zu entrichten, darf er Bestandsdaten und nach § 97 TKG gespeicherte Verkehrsdaten dieser Teilnehmer oder Nutzer nur verwenden, soweit dies zur Geltendmachung seiner Ansprüche gegen die Teilnehmer oder Nutzer erforderlich ist. Der Diensteanbieter hat die Daten unverzüglich zu löschen, wenn die Voraussetzungen nach Satz 1 nicht mehr vorliegen oder die Daten für die Rechtsverfolgung nicht mehr benötigt werden. Die betroffenen Teilnehmer oder Nutzer sind zu unterrichten, sobald dies ohne Gefährdung des mit der Maßnahme verfolgten Zweckes möglich ist.**

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
der oder die Bundesbeauftragte für den Datenschutz sind über Einführung und Änderung eines Verfahrens nach Satz 1 unverzüglich in Kenntnis zu setzen.			

In vielen Situationen müssen sich Menschen beruflich (z.B. Geheimnisträger) oder wegen ihrer persönlichen Lebenssituation (z.B. Krankheit, Abhängigkeit, seelische Störung) darauf verlassen können, dass ihre Gesprächspartner – und damit oft auch der Grund des Gesprächs – Dritten nicht zur Kenntnis gelangen. Zeichnet der Anbieter Kontakte, Standorte und Internetverbindungen auf, so begründet dies die Besorgnis von Missbrauch, falschem Verdacht, unberechtigten Abmahnungen und Strafverfolgungsmaßnahmen und Datenverlust. Um eine freie und unbefangene Kommunikation zu gewährleisten, muss deshalb nach Möglichkeit verhindert werden, dass Anbieter Kontakte, Standorte und Internetverbindungen festhalten.

§ 100 TKG bewirkt das Gegenteil hiervon:

- Die Vorschrift legt fest nicht, aus welchem Anlass Anbieter zur „Störungserkennung“ oder „Missbrauchsaufdeckung“ Verbindungsprotokolle erstellen dürfen. Der unbestimmte Wortlaut des § 100 TKG leistet einer Auslegung Vorschub, wonach sämtliche Anbieter von Telekommunikationsdiensten berechtigt wären, die Telefon-, Handy-, E-Mail- und Internetnutzung ihrer Kunden ohne Anlass aufzuzeichnen. Es dürfte nämlich nie auszuschließen sein, dass diese Daten einmal zum „Erkennen“ denkbarer zukünftiger „Störungen“ oder „rechtswidriger Inanspruchnahmen“ „erforderlich“ sein könnten. Damit wird zur potenziell unbegrenzten und unbefristeten Speicherung jedes Telefonats, jeder SMS, jeder E-Mail und jeder Internetverbindung ermächtigt, zu einer Vorratsdatenspeicherung. § 100 TKG macht den Grundsatz der §§ 96, 97 TKG, demzufolge Verkehrsdaten nicht über die Dauer der Verbindung hinaus aufbewahrt werden dürfen, bedeutungslos. Die Vorschrift ist nicht auf eine Erfassung „im Einzelfall“ bei Vorliegen einer konkreten Störung oder eines konkreten Verdachts beschränkt, sondern erlaubt eine anlasslose, globale und pauschale Aufzeichnung unserer Kontakte, Bewegungen und Internetverbindungen.
- § 100 TKG schließt eine Verwendung der gesammelten Informationen zu ganz anderen Zwecken nicht aus. Die Verwendung der Verbindungsprotokolle wird „zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern“ gestattet, aber eben nicht „nur“ dazu (vgl. hingegen § 15 Abs. 1 TMG). Die für bestimmte Zwecke erstellten Verbindungsprotokolle sind daher auf Anfrage beispielsweise an Polizei, Geheimdienste sowie an die Unterhaltungsindustrie herauszugeben, wo sie zu ganz anderen Zwecken genutzt werden.
- § 100 TKG gewährleistet die Vertraulichkeit der Telekommunikation nicht. Die vorgeschlagene Ermächtigung der Anbieter zum „Verwenden“ von Verkehrsdaten deckt auch deren Übermittlung ab (§ 3 Abs. 4 BDSG). Die Vorschrift ermächtigt daher zur Offenlegung unserer Verbindungen gegenüber Dritten zur „Störungserkennung“ oder „Missbrauchsaufdeckung“.

§ 100 TKG wird den verfassungsrechtlichen Mindestanforderungen und dem Verhältnismäßigkeitsgebot nicht gerecht. Nach der Rechtsprechung des Bundesverfassungsgerichts darf eine automatisierte Datenerfassung „nicht anlasslos erfolgen oder flächendeckend durchgeführt werden“.[26] Begriffe wie „erforderlich“ oder „sachdienlich“ stellen keine hinreichende Eingrenzung dar.[27] Das „strikte Verbot der Samm-

[26] BVerfG, MMR 2008, 308, 308; BVerfG, NVwZ 2007, 688, 691.

[27] BVerfG, MMR 2007, 93, 94; BVerfG, NVwZ 2007, 688, 691.

lung personenbezogener Daten auf Vorrat“ ist zu gewährleisten.[28] Eine „enge und konkrete Zweckbindung“ muss gesetzlich angeordnet werden.[29] Anbieter haben Verkehrsdaten mit Verbindungsende zu löschen; Speicherungsinteressen, die mit dem Löschungsinteresse der Teilnehmer kollidieren und im Rahmen einer Abwägung überwiegen müssten, sind nicht ersichtlich.[30]

Der Bundesrat hat dementsprechend ausgeführt: „*Dies erscheint insbesondere deshalb veranlasst, weil die zu § 100 Absatz 1 TKG ergangene Rechtsprechung in verfassungsrechtlich bedenklicher Weise die vorbeugende Speicherung von IP-Adressen zur Störungseingrenzung und -beseitigung zulässt, ohne dass tatsächliche Anhaltspunkte bei einem bestimmten Nutzer vorliegen (vgl. LG Darmstadt, Urteil vom 06.06.2007 - 10 O 562/03 -, CR 2007, 574).*“[31] Nur in Teilen der Rechtsprechung wird § 100 TKG einschränkend dahin ausgelegt, dass eine Datensammlung tatsächliche Anhaltspunkte für einen Missbrauch bei einem bestimmten Nutzer[32] oder eine konkrete Funktionsstörung[33] voraus setze. Der hohe Stellenwert des Fernmeldegeheimnisses und das Gebot der Normenklarheit erfordern, dass der Gesetzgeber die Reichweite der Ermächtigung selbst und eindeutig regelt.

In seiner jetzigen Fassung verletzt § 100 TKG auch Art. 6 Abs. 1 RiL 2002/58/EG. Anders als die Vorgängervorschrift des § 9 TDSV erlaubt § 100 TKG die Erhebung und Speicherung von Verkehrsdaten zur Störungs- und Missbrauchsbekämpfung nicht mehr nur „im Einzelfall“. In Erwägungsgrund 29 der Richtlinie 2002/58/EG heißt es demgegenüber eindeutig: „*Der Diensteanbieter kann Verkehrsdaten in Bezug auf Teilnehmer und Nutzer* ***in Einzelfällen*** *verarbeiten, um technische Versehen oder Fehler bei der Übertragung von Nachrichten zu ermitteln.* ***Für Fakturierungszwecke notwendige Verkehrsdaten*** *dürfen ebenfalls vom Diensteanbieter verarbeitet werden, um Fälle von Betrug, die darin bestehen, die elektronischen Kommunikationsdienste ohne entsprechende Bezahlung nutzen, ermitteln und abstellen zu können.*“ § 100 TKG trägt weder der danach gebotenen Beschränkung auf den Einzelfall, noch der Beschränkung auf „für Fakturierungszwecke notwendige Verkehrsdaten“ Rechnung.

§ 100 Abs. 3 TKG verletzt überdies Art. 15 Abs. 1 RiL 2002/58/EG. Nach dieser Vorschrift dürfen Ausnahmen von dem Verbot von Verbindungsaufzeichnungen zur „Verhütung, Ermittlung, Feststellung und Verfolgung [...] des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen“ eingeführt werden. Die Generalanwältin bei dem Europäischen Gerichtshof hat klargestellt, dass diese Ausnahme „nur den systemwidrigen Gebrauch“ elektronischer Kommunikationssysteme, „nicht aber den Gebrauch zu unzulässigen Zwecken“ erfasst.[34] Auch die Europäische Kommission hat bekräftigt, die Ausnahmeklausel erfasse nur systemwidrigen Gebrauch, der die Integrität oder die Sicherheit des Kommunikationssystems gefährde.[35] § 100 Abs. 3 TKG ist auf diese Fälle demgegenüber nicht beschränkt. Als rechtswidrig im Sinne des § 100 Abs. 3 TKG wird eine Inanspruchnahme schon dann angesehen, wenn sie gegen einen zwischen dem Nutzer und dem Diensteanbieter geschlossenen Vertrag verstößt.[36] Auch soll der Versand von Spam oder Viren eine rechtswidrige Inanspruchnahme darstellen.[37] Selbst die Nutzung eines Telefons zur Bedrohung oder Belästigung Dritter soll eine rechtswidrige Inanspruchnahme darstellen[38], ebenso wie jegliche sonstige Straftat.[39] All diese Fälle haben mit einer Gefährdung der Integrität oder

---

28 BVerfG, MMR 2006, 531.

29 BVerfGE 100, 313, 385 f.

30 BVerfG, 1 BvR 1811/99 vom 27.10.2006.

31 BR-Drs. 62/09, 10.

32 LG Darmstadt, Urteil vom 07.12.2005, 25 S 118/2005.

33 OLG Karlsruhe, MMR 2009, 412.

34 Kokott, Schlussanträge vom 18.07.2007, Az. C-275/06, Rn. 98.

35 Kokott, Schlussanträge vom 18.07.2007, Az. C-275/06, Rn. 92.

36 LG München, MMR 2010, 111; BeckTKG-Wittern, § 100 TKG, Rn. 10.

37 LG Darmstadt, CR 2007, 574; AG Bonn, MMR 2008, 203; BeckTKG-Wittern, § 100 TKG, Rn. 10; Säcker, § 100 TKG, Rn. 15.

38 BeckTKG-Wittern, § 100 TKG, Rn. 10; a.A. Säcker, § 100 TKG, Rn. 14.

39 LG Köln, MMR 2008, 197.

Sicherheit des Kommunikationsnetzes offenkundig nichts zu tun. Eine so weite Fassung des § 100 Abs. 3 TKG ist mit Art. 15 RiL 2002/58/EG nicht vereinbar.

§ 100 TKG muss vor diesem Hintergrund einschränkend formuliert werden. Dass sich Störungen und Leistungserschleichung im Wege eines einzelfallbezogenen Vorgehens ausreichend begegnen lässt, zeigen die vielen Anbieter, die darauf verzichten, unter Berufung auf § 100 TKG eine flächendeckende Vorratsdatenspeicherung vorzunehmen. Die hier vorgeschlagene Neufassung orientiert sich an § 15 Abs. 8 TMG und der aufgezeigten Rechtsprechung des Bundesverfassungsgerichts. Absatz 1 Satz 1 des Vorschlags verhindert eine permanente, generelle und anlasslose Protokollierung und erlaubt Aufzeichnungen nur, wenn „im Einzelfall" tatsächlich konkrete Anhaltspunkte für eine Störung oder für Leistungserschleichung durch bestimmte Nutzer eines Dienstes vorliegen. Dies dient dem Schutz der überwältigenden Mehrheit rechtstreuer Nutzer, die keinen Anlass für eine Aufzeichnung ihres Kommunikationsverhaltens gegeben haben. Die Weitergabe der Daten an Dritte wird ausgeschlossen. Eine Zweckbindung wird angeordnet. Die in Satz 3 vorgesehene Benachrichtigung ermöglicht betroffenen Nutzern effektiven Rechtsschutz (Art. 19 Abs. 4 GG) gegen rechtswidrige Aufzeichnungsverfahren, was wiederum Datenskandalen vorbeugt.

11. Recht auf anonyme Telekommunikation und Schutz vor ausufernden staatlichen Zugriffen (§§ 111, 112 TKG)

Geltendes Telekommunikationsgesetz (TKG)	**Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen**	**Nr**	**Änderungsvorschlag**
§ 111 Daten für Auskunftsersuchen der Sicherheitsbehörden	*(unverändert)*	11	***(entfällt)***
§ 112 Automatisiertes Auskunftsverfahren	*(unverändert)*		***(entfällt)***

Die §§ 111, 112 TKG sind verfassungswidrig[40] und zu streichen.

§ 111 Abs. 1 S. 1 und Abs. 2 S. 1 TKG verpflichtet Telekommunikationsanbieter zur Identifizierung von Anschlussinhabern, selbst wenn dies betrieblich nicht erforderlich ist. Die Vorschrift verbietet dadurch die anonyme Überlassung von Telekommunikationsanschlüssen und sieht eine globale, pauschale „Vorratsdatengewinnung" ohne jeden Anlass vor. Der massive Grundrechtseingriff eines Quasi-Verbots anonymer Telekommunikation ist nicht gerechtfertigt: Der Gesetzesvorbehalt des Art. 10 Abs. 2 GG, der Eingriffe nur auf besondere Anordnung zulässt, ist überschritten. Das Zitiergebot ist verletzt. Vor allem ist ein allgemeines Verbot der Überlassung anonymer Telekommunikationsanschlüsse unverhältnismäßig. Es dient Allgemeininteressen wegen vielfältiger Umgehungsmöglichkeiten (z.B. falsch registrierte Handykarten, Weitergabe von Prepaidkarten, ausländische Karten) kaum, setzt auf der anderen Seite aber ohne jeden Anlass die gesamte Bevölkerung dem ständigen Risiko eines Missbrauchs oder Verlustes vertraulicher Daten sowie dem Risiko eines falschen Verdachts aufgrund der irrtumsanfälligen Telekommunikationsdaten aus und schreckt dadurch unzumutbar von freier Fernkommunikation ab, gerade wo einzelne Menschen oder die Allgemeinheit auf anonyme Informationen oder Beratung dringend angewiesen sind. Soweit das Bundesverfassungsgericht mit Urteil vom 2. März 2010 erwogen hat, dass eine Vorratsspeicherung ohnehin anfallender Daten in Einklang mit dem Grundgesetz zu bringen sein könne, lassen sich diese Erwägungen auf eine „Vorratsdatengewinnung" nicht übertragen. Umgekehrt soll nach dem Willen des Bundesverfassungsgerichts seine Entscheidung zur Vorratsspeicherung von Verkehrsdaten auf andere Datensammlungen nicht übertragen werden. Die Zulassung der Verkehrsdatenspeicherung soll eine „Ausnahme" bleiben.[41] Deshalb kann die allgemeine Identifizierungspflicht, die selbst in der EG-Richtlinie zur Vorratsdatenspeicherung nicht vorgesehen ist, keinen Bestand haben. Die meisten europäi-

[40] Verfassungsbeschwerde anhängig unter Az. 1 BvR 1299/05.

[41] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 218.

schen Staaten kennen keine Identifizierungspflicht, ohne dass sich dies auf die Sicherheit der Bürger dieser Staaten nachteilig auswirken würde.

Der staatliche Online-Zugriff auf Kundendaten nach § 112 TKG greift zu weit in die Grundrechte unbescholtener Bürger ein. Im Jahr 2009 ist die Zahl der staatlichen Kenntnisnahmen von Kommunikationsdaten nach § 112 TKG auf 4,5 Mio. und damit erneut stark angestiegen,[42] so dass nunmehr 1.000 zugriffsberechtigte Behörden täglich mindestens 12.000 Fernmeldeverhältnisse offen legen. Gegenüber 2001 hat sich die Zahl der staatlichen Kenntnisnahmen bereits verdreifacht, gegenüber früheren Jahren exponentiell gesteigert. Diese anhaltende Zugriffsexplosion lässt sich nicht durch veränderte Rahmenbedingungen erklären und verdeutlicht vielmehr, dass die Eingriffsvoraussetzungen des § 112 TKG dem verfassungsrechtlichen Stellenwert der Vertraulichkeit der Telekommunikation keine Rechnung tragen.

Die näheren Umstände eines Fernmelde-Vertragsverhältnisses sind integraler Bestandteil der in diesem Rahmen vermittelten Telekommunikation. Insbesondere die Information, wer unter welcher Kennung kommuniziert (hat), ist der Schlüssel zur Vertraulichkeit der Telekommunikation auch im Verhältnis zum Kommunikationspartner und ist nicht typischerweise weniger schutzwürdig als Inhalt und Umstände der einzelnen Kommunikationsvorgänge selbst. Deswegen muss die Aufdeckung der Identität eines Kommunikationsteilnehmers oder der Kennung, unter welcher eine Person kommuniziert, denselben Voraussetzungen unterworfen werden wie sonstige Eingriffe in das Fernmeldegeheimnis (etwa §§ 100a, 100g StPO). Dass Identifikations- und Verbindungsdaten eine vergleichbare Sensibilität aufweisen, hat der Gesetzgeber inzwischen mit der Regelung zur Meldepflicht von Datenpannen in § 93 Abs. 3 TKG anerkannt. Der Verlust von Bestands- und Verkehrsdaten begründet danach gleichermaßen eine Informationspflicht. Die Begründung des Gesetzentwurfs zu § 93 Abs. 3 TKG führt dazu aus, die Meldepflicht beziehe sich „auf besonders sensible personenbezogene Daten“[43], wozu der Gesetzgeber Bestands- und Verkehrsdaten gleichermaßen zählt.

§ 112 TKG genügt den verfassungsrechtlichen Anforderungen des Verhältnismäßigkeitsgebots nicht:

- Erstens beschränkt er die Durchbrechung des Fernmeldegeheimnisses nicht auf die Aufklärung schwerer Straftaten[44] und die Abwehr von Gefahren für wichtige Rechtsgüter[45]. Er legt nicht einmal fest, zu welchen konkreten, klar definierten Zwecken Kenntnisnahmen überhaupt zugelassen werden sollen.
- Zweitens beschränkt § 112 TKG die Datenerhebung nicht auf Beschuldigte/Störer oder solche Personen, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für einen Beschuldigten/Störer bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte/Störer ihren Anschluss benutzt (vgl. § 100a StPO).
- Drittens versäumt es § 112 TKG, eine richterliche Prüfung zur Voraussetzung für den Zugriff zu machen.[46] Der durch § 112 TKG eröffnete direkte staatliche Zugriff auf ein Verzeichnis sämtlicher Anschlussinhaber Deutschlands begünstigt die jährlich millionenfache Aufhebung der Anonymität von Fernmeldeverhältnissen und genügt dem Verhältnismäßigkeitsgebot nicht. Mit Urteil vom 2. März hat das Bundesverfassungsgericht betont, dass der Prüfung und Bearbeitung von Auskunftsersuchen durch den Telekommunikationsmittler als einzigem Garant des Fernmeldegeheimnisses in diesem Verfahrensstadium eine zentrale Bedeutung zukomme. Deswegen sei „durch entsprechende Regelungen und technische Vorkehrungen sicherzustellen“, dass staatliche Stellen „keinen direkten Zugriff auf die Daten“ haben.[47] Die Daten dürften dem Staat „unmittelbar als Gesamtheit nicht zur Verfügung“ stehen – eben dies ist aber die Folge des § 112 TKG. Auch zur Gewährleistung eines effektiven Rechtsschutzes und adäquater Sanktionen gehört es dem Bundesverfassungsgericht zufolge, „dass die Daten aufgrund der Anordnung von den Telekommunikationsunternehmen als speicherungsverpflichteten Drit-

42 Bundesnetzagentur, Jahresbericht 2009, 127 f.

43 Bundesregierung, BT-Drs. 16/12011, 34.

44 Vgl. BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 228.

45 Vgl. BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 231.

46 Vgl. BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 247 ff.

47 BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 214.

ten herausgefiltert und übermittelt werden, das heißt den Behörden also nicht ein Direktzugriff auf die Daten eröffnet wird. Auf diese Weise wird die Verwendung der Daten auf das Zusammenwirken verschiedener Akteure verwiesen und damit in sich gegenseitig kontrollierende Entscheidungsstrukturen eingebunden."[48] Selbst eine richterliche Anordnung ermächtige die Behörden nicht zu einem Direktzugriff auf die Daten.[49] Wenngleich sich diese Ausführungen des Bundesverfassungsgerichts unmittelbar nur auf anlasslos gespeicherte Verkehrsdaten bezogen haben, müssen sie für anlasslos gespeicherte oder sogar anlasslos erhobene Identifizierungsdaten nach § 111 TKG ebenso gelten. Insoweit steht die grundrechtlich geschützte Anonymität der Telekommunikation auf dem Spiel.

- Ohne Richtervorbehalt kommt einer manuellen Prüfung und Erledigung von Auskunftsersuchen durch die Verpflichteten eine noch größere Bedeutung zu. Ohne vorherige richterliche Prüfung stellen die Kommunikationsmittler nämlich die einzige Stelle dar, die wenigstens offensichtlich rechtswidrige Auskunftsersuchen zurückweisen können. Das automatisierte Abrufverfahren nach § 112 TKG stellt eine effektive Vorabkontrolle demgegenüber nicht sicher und führt zu einer zunehmenden Ausuferung und Zweckausweitung des Zugriffsverfahrens. Dies trägt dem verfassungsrechtlichen Schutz des Fernmeldegeheimnisses nicht Rechnung. Ein manuelles Auskunftsverfahren sichert die Rechtmäßigkeit und Verhältnismäßigkeit von Durchbrechungen des Fernmeldegeheimnisses auch dadurch, dass manuelle Auskünfte einen Entschädigungsanspruch begründen (§ 23 Abs. 1 JVEG) und der Abfragende seinen Grundrechtseingriff dadurch in erhöhtem Maße rechtfertigen muss.
- Viertens gewährleistet § 112 TKG nicht die verfassungsrechtlich gebotene Zweckbindung erlangter Informationen, die Kennzeichnung erhobener Daten[50] und die Benachrichtigung der Betroffenen.

Selbst wenn man nur die vom Bundesverfassungsgericht zur Identifizierung von Internetnutzern entwickelten Maßstäbe anlegen wollte, änderte dies nichts an der Verletzung des Verhältnismäßigkeitsgebots:

- Das Bundesverfassungsgericht hat identifizierende Auskünfte nur für die Verfolgung von Straftaten, für die Verfolgung auch im Einzelfall besonders gewichtiger und ausdrücklich zu benennender Ordnungswidrigkeiten, für die Gefahrenabwehr und die Aufgabenwahrnehmung der Nachrichtendienste auf der Grundlage der allgemeinen fachrechtlichen Eingriffsermächtigungen zugelassen.[51] § 112 Abs. 2 TKG geht hierüber sowohl hinsichtlich des Kreises der abrufberechtigten Stellen wie auch hinsichtlich der zugelassenen Erhebungszwecke („zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich") weit hinaus. § 112 Abs. 2 TKG versäumt es, überhaupt konkret die Verwendungszwecke übermittelter Daten zu benennen. § 112 TKG umreißt nur in generalisierender Weise die Aufgabenfelder, für die ein Datenabruf möglich sein soll. Dass § 112 TKG die Weitergabe personenbezogener Daten an bestimmte Behörden pauschal „zur Erfüllung ihrer gesetzlichen Aufgaben" erlaubt,[52] anstatt klar festzulegen, „um welche konkreten, klar definierten Zwecke es sich dabei handelt", verstößt gegen das Gebot der Normenklarheit.[53]
- § 112 TKG versäumt es auch, sicherzustellen, dass Auskünfte nicht ins Blaue hinein eingeholt werden, sondern nur aufgrund eines Anfangsverdachts oder einer konkreten Gefahr auf einzelfallbezogener Tatsachenbasis.[54] Eine solche Anforderung kann der Norm selbst im Wege der Auslegung nicht entnommen werden. Auch das Fachrecht gewährleistet die Einhaltung dieser Eingriffsschwelle nicht: § 112 TKG bestimmt erstens nicht normenklar, dass Zugriffe nur nach Maßgabe fachgesetzlicher Ermächtigungen zulässig sein sollen. Zweitens sieht das Fachrecht vielfach selbst nicht die erforderliche Eingriffsschwelle vor (z.B. für Nachrichtendienste, Notrufabfragestellen, Finanzdienstleistungsaufsicht, Zollverwaltung).

---

48 BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 250.

49 BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 283.

50 BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 236.

51 BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 261 f.

52 Vgl. BVerfGE 65, 1 (66 f.) zu einer vergleichbaren Formulierung.

53 BVerfG a.a.O.

54 BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 261.

- § 112 TKG stellt ferner – anders als etwa das österreichische Recht – nicht sicher, dass die rechtlichen und tatsächlichen Grundlagen entsprechender Abfragen aktenkundig gemacht werden, wie es verfassungsrechtlich geboten ist.[55]
- § 112 TKG versäumt es weiter, Benachrichtigungspflichten jedenfalls dann vorzusehen, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird oder sonst überwiegende Interessen Dritter oder des Betroffenen selbst entgegenstehen, wie es verfassungsrechtlich geboten ist.[56] § 112 TKG gewährleistet nicht, dass der Grund für ein Absehen von der erforderlichen Benachrichtigung aktenkundig gemacht wird.[57]
- § 112 TKG fehlt schließlich die verfassungsrechtlich gebotene[58] Anordnung, dass die Verwendung erlangter Daten nur zur Verfolgung derjenigen Zwecke zulässig ist, zu deren Erreichung die Daten nach dem Gesetz erhoben werden durften, und dass die Daten zu löschen sind, wenn sie zu diesen Zwecken nicht mehr benötigt werden (Zweckbindungsgebot).

Hinsichtlich der in § 112 Abs. 3 TKG vorgesehenen „Ähnlichkeitssuche“ ist der Parlamentsvorbehalt verletzt. § 112 verletzt Parlamentsvorbehalt und Gebot der Normenklarheit, weil die Vorschrift nicht selbst festgelegt, welche Angaben Suchanfragen mindestens enthalten müssen und über wie viele Personen Auskunft verlangt werden darf. Wegen der Grundrechtswesentlichkeit dieser Frage sind Regelungen in einer Rechtsverordnung (§ 112 Abs. 3 TKG), deren Erlass überdies freigestellt ist, nicht ausreichend.

Insgesamt sind die Regelungen der §§ 111, 112 TKG verfassungswidrig und verfehlt. Ein vergleichbares Verfahren gibt es in kaum einem anderen europäischen Staat. Es ist verzichtbar, weil betrieblich erforderliche Kundendaten ohnehin gespeichert und durch manuelle Auskunftsersuchen in Erfahrung gebracht werden können. Die §§ 111, 112 TKG sind folglich ersatzlos zu streichen.

12. Schutz von Kundendaten vor ausufernden staatlichen Zugriffen (§ 113 TKG)

Geltendes Telekommunikationsgesetz (TKG)	**Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen**	**Nr**	**Änderungsvorschlag**
§ 113 Manuelles Auskunftsverfahren	*(unverändert)*	12	***(entfällt)***
Geltende Strafprozessordnung (StPO)	**Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen**		**Änderungsvorschlag**
§ 100g	*(unverändert)*		*(unverändert)*
(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer	*(unverändert)*		(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer
1. eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu be-			1. eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat, begangen hat, in Fällen, in

[55] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 261.

[56] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 263.

[57] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 263.

[58] BVerfGE 65, 1 (46).

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
gehen versucht hat oder durch eine Straftat vorbereitet hat oder 2. eine Straftat mittels Telekommunikation begangen hat, so dürfen auch ohne Wissen des Betroffenen Verkehrsdaten (§ 96 Abs. 1, § 113a des Telekommunikationsgesetzes) erhoben werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Im Falle des Satzes 1 Nr. 2 ist die Maßnahme nur zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Die Erhebung von Standortdaten in Echtzeit ist nur im Falle des Satzes 1 Nr. 1 zulässig.			denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder 2. eine Straftat mittels Telekommunikation begangen hat, so dürfen auch ohne Wissen des Betroffenen **Bestandsdaten und** Verkehrsdaten (§ 95 Abs. 1, § 96 Abs. 1~~, § 113a~~ des Telekommunikationsgesetzes) erhoben werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Im Falle des Satzes 1 Nr. 2 ist die Maßnahme nur zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Die Erhebung von Standortdaten in Echtzeit ist nur im Falle des Satzes 1 Nr. 1 zulässig.

Geltendes Telekommunikationsgesetz (TKG)	Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen	Nr	Änderungsvorschlag
(2) § 100a Abs. 3 und § 100b Abs. 1 bis 4 Satz 1 gelten entsprechend. Abweichend von § 100b Abs. 2 Satz 2 Nr. 2 genügt im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.	*(unverändert)*		(2) § 100a Abs. 3 und § 100b Abs. 1 bis 4 Satz 1 gelten entsprechend. Abweichend von § 100b Abs. 2 Satz 2 Nr. 2 genügt im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. **Im Fall von Bestandsdaten sind in der Anordnung abweichend von § 100b Abs. 2 anzugeben** **1. der Name und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet, oder die Rufnummer oder eine andere Kennung des Anschlusses, zu dem Auskunft erteilt werden soll,** **2. Art und Umfang der begehrten Auskunft.**
§ 101	*(unverändert)*		*(unverändert)*
(4) Von den in Absatz 1 genannten Maßnahmen sind im Falle ...	*(unverändert)*		(4) Von den in Absatz 1 genannten Maßnahmen sind im Falle ...
6. des § 100g die Beteiligten der betroffenen Telekommunikation,			6. des § 100g die Beteiligten der betroffenen Telekommunikation, **im Fall von Bestandsdaten die Inhaber der betroffenen Anschlüsse,**

§ 113 TKG ist verfassungswidrig[59] und zu streichen.

§ 113 TKG verletzt das verfassungsrechtliche Zitiergebot, weil die Einschränkung des Fernmeldegeheimnisses verkannt wurde, und vor allem das Verhältnismäßigkeitsgebot. Informationen über Fernmelde-Vertragsverhältnisse sind integraler Bestandteil der in diesem Rahmen vermittelten Telekommunikation. Insbesondere die Information, wer unter welcher Kennung kommuniziert (hat), ist der Schlüssel zur Vertraulichkeit der Telekommunikation auch im Verhältnis zum Kommunikationspartner und ist nicht typischerweise weniger schutzwürdig als Inhalt und Umstände der einzelnen Kommunikationsvorgänge

[59] Verfassungsbeschwerde anhängig unter Az. 1 BvR 1299/05.

selbst. Deswegen muss die Aufdeckung der Identität eines Kommunikationsteilnehmers oder der Kennung, unter welcher eine Person kommuniziert, denselben Voraussetzungen unterworfen werden wie sonstige Eingriffe in das Fernmeldegeheimnis (etwa § 100g StPO). Dassselbe gilt, soweit § 113 TKG den Zugriff auf Schlüssel zu Kommunikationsinhalten erlaubt (z.B. Zugriffscode für elektronischen Anrufbeantworter oder E-Mail-Postfach).

§ 113 TKG genügt den verfassungsrechtlichen Anforderungen des Verhältnismäßigkeitsgebots nicht:

- Er beschränkt die Durchbrechung des Fernmeldegeheimnisses nicht auf die Aufklärung schwerer Straftaten[60] und die Abwehr von Gefahren für wichtige Rechtsgüter[61].
- § 113 TKG beschränkt die Datenerhebung nicht auf Beschuldigte/Störer oder solche Personen, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für einen Beschuldigten/Störer bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte/Störer ihren Anschluss benutzt (vgl. §§ 100a, 100g StPO).
- § 113 TKG versäumt es ferner, eine richterliche Prüfung zur Voraussetzung für den Zugriff zu machen.[62] Der derzeitige § 113 TKG begünstigt die massenhafte Aufhebung der Anonymität von Fernmeldeverhältnissen und genügt dem Verhältnismäßigkeitsgebot nicht. Schon im Jahr 2006 identifizierte alleine die Deutsche Telekom AG 94.417 Inhaber von IP-Adressen, während es im Jahr 2003 noch 3.170 Personen waren.[63] Die unzureichenden Voraussetzungen des § 113 TKG ermöglichen erst diese ausufernde Aufhebung der Vertraulichkeit der Internetnutzung.
- § 113 TKG gewährleistet schließlich nicht die verfassungsrechtlich gebotene Zweckbindung erlangter Informationen, die Kennzeichnung erhobener Daten und die Benachrichtigung der Betroffenen.

Selbst wenn man nur die vom Bundesverfassungsgericht zur Identifizierung von Internetnutzern entwickelten Maßstäbe anlegen wollte, änderte dies nichts an der Verletzung des Verhältnismäßigkeitsgebots durch § 113 TKG:

- Das Bundesverfassungsgericht hat identifizierende Auskünfte nur für die Verfolgung von Straftaten, für die Verfolgung – auch im Einzelfall – besonders gewichtiger und ausdrücklich zu benennender Ordnungswidrigkeiten, für die Gefahrenabwehr und die Aufgabenwahrnehmung der Nachrichtendienste auf der Grundlage der allgemeinen fachrechtlichen Eingriffsermächtigungen zugelassen.[64] § 113 TKG stellt demgegenüber keine Anforderung an die Schwere der Ordnungswidrigkeit, deren Aufklärung den Eingriff rechtfertigen soll.
- § 113 TKG versäumt es auch, sicherzustellen, dass Auskünfte nicht ins Blaue hinein eingeholt werden, sondern nur aufgrund eines Anfangsverdachts oder einer konkreten Gefahr auf einzelfallbezogener Tatsachenbasis.[65] Eine solche Anforderung kann der Norm im Wege der Auslegung nicht entnommen werden, ohne das Gebot der Normenklarheit zu verletzen. Auch das Fachrecht gewährleistet die Einhaltung der verfassungsrechtlich gebotenen Eingriffsschwellen nicht: § 113 TKG bestimmt erstens nicht normenklar, dass Zugriffe nur nach Maßgabe fachgesetzlicher Ermächtigungen zulässig sein sollen. Zweitens sieht das Fachrecht vielfach selbst nicht die erforderliche Eingriffsschwelle vor. So setzen die §§ 8a Abs. 1 BVerfSchG, 4a MAD-G, 2a BND-G keine konkrete Gefahr auf einzelfallbezogener Tatsachenbasis voraus, sondern nur die „Erforderlichkeit“ der Datenerhebung zur Aufgabenerfüllung. Gleiches gilt für § 21 BPolG, §§ 20b, 22 BKAG und eine Vielzahl von Datenerhebungsbefugnissen der Länder.

---

60 Vgl. BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 228.

61 Vgl. BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 231.

62 Vgl. BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 247 ff.

63 Köbele, Wirtschaftsunternehmen – Verlängerter Arm der Strafverfolgungsbehörden?, https://www.datenschutzzentrum.de/sommerakademie/2007/sak2007-koebele-wirtschaftsunternehmen-verlaengerter-arm-der-sicherheitsbehoerden.pdf, 7.

64 BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 261 f.

65 BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 261.

- § 113 TKG stellt ferner – anders als etwa das österreichische Recht – nicht sicher, dass die rechtlichen und tatsächlichen Grundlagen entsprechender Abfragen aktenkundig gemacht werden, wie es verfassungsrechtlich geboten ist.[66]
- § 113 TKG ist auch deswegen verfassungswidrig, weil der Gesetzgeber versäumt hat, die zur Gewährleistung der Zweckbindung erforderlichen Folgeregelungen verbindlich festzulegen. § 113 TKG fehlt namentlich die verfassungsrechtlich gebotene[67] Anordnung, dass die Verwendung erlangter Daten nur zur Verfolgung derjenigen Zwecke zulässig ist, zu deren Erreichung die Daten nach dem Gesetz erhoben werden durften, und dass die Daten zu löschen sind, wenn sie zu diesen Zwecken nicht mehr benötigt werden (Zweckbindungsgebot).

§ 113 TKG ist danach aufzuheben. Mindestens geboten ist die Erstreckung des Schutzniveaus des § 100g StPO auf Bestandsdaten. Dazu sind die §§ 100g, 101 StPO auf Bestandsdaten zu erweitern. Dies ist Gegenstand des hier unterbreiteten Änderungsvorschlags. Dadurch wird die Beschränkung von Auskünften auf Tatverdächtige und Nachrichtenmittler erheblicher oder mittels Telekommunikation begangener Straftaten, eine richterliche Prüfung, eine Zweckbindung erlangter Informationen, die Kennzeichnung erhobener Daten und eine Benachrichtigung der Betroffenen sichergestellt.

13. Schutz von Internetnutzern vor „Spyware“, „Web-Bugs“ usw. (§ 13 TMG)

Geltendes Telemediengesetz (TMG)	**Referentenentwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen**	**Nr**	**Änderungsvorschlag**
§ 13 Pflichten des Diensteanbieters	*(unverändert)*		*(unverändert)*
		13	**(8) Die Speicherung von Daten im Endgerät des Nutzers und der Zugriff auf Daten, die im Endgerät des Nutzers gespeichert sind, ist nur zulässig, wenn der Nutzer darüber gemäß Absatz 1 unterrichtet worden ist und darin eingewilligt hat. Dies gilt nicht, wenn der alleinige Zweck der Speicherung oder des Zugriffs die Durchführung oder Erleichterung der Übertragung einer Nachricht über ein Telekommunikationsnetz ist oder soweit dies zwingend erforderlich ist, um einen vom Nutzer ausdrücklich gewünschten elektronischen Informations- und Kommunikationsdienst zur Verfügung zu stellen.**

Der hier vorgeschlagene § 13 Abs. 8 TMG-E ist europarechtlich geboten. Art. 5 Abs. 3 der RiL 2002/58/EG bestimmt: „*Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder*

66 BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 261.

67 BVerfGE 65, 1 (46).

der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann."

Diese Bestimmung ist bisher in Deutschland nicht umgesetzt, weswegen bei der Europäischen Kommission bereits eine Beschwerde eingereicht wurde. Zwar sehen TKG und TMG Informationspflichten vor. Sie machen die Zulässigkeit der „Speicherung von Informationen oder den Zugriff auf Informationen, die im Endgerät eines Teilnehmers oder Nutzers gespeichert sind", aber nicht von einer ordnungsgemäßen Information abhängig, wie es Art. 5 Abs. 3 RiL 2002/58/EG vorschreibt. Es existiert bisher auch nicht das in der Richtlinie vorgesehene Einwilligungserfordernis. Zudem ist der Anwendungsbereich des Art. 5 Abs. 3 RiL 2002/58/EG nicht auf personenbezogene Daten beschränkt.

Eine Umsetzung des Art. 5 Abs. 3 der RiL 2002/58/EG ist nicht nur rechtlich geboten, sondern auch aus Gründen des Datenschutzes erforderlich. Die Richtlinie führt in ihrem Erwägungsgrund 24 dazu aus: „*Die Endgeräte von Nutzern elektronischer Kommunikationsnetze und in diesen Geräten gespeicherte Informationen sind Teil der Privatsphäre der Nutzer, die dem Schutz aufgrund der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten unterliegt. So genannte ‚Spyware', ‚Web-Bugs', ‚Hidden Identifiers' und ähnliche Instrumente können ohne das Wissen des Nutzers in dessen Endgerät eindringen, um Zugang zu Informationen zu erlangen, oder die Nutzeraktivität zurückzuverfolgen und können eine ernsthafte Verletzung der Privatsphäre dieser Nutzer darstellen. Die Verwendung solcher Instrumente sollte nur für rechtmäßige Zwecke mit dem Wissen der betreffenden Nutzer gestattet sein.*"

Schon der Entwurf der FDP-Fraktion eines Gesetzes zur Änderung des Telemediengesetzes sah eine Umsetzung des Art. 5 Abs. 3 RiL 2002/58/EG in § 13 TMG vor.[68] Zu regeln ist, unter welchen Bedingungen Diensteanbieter den Computer des Benutzers als „Datenspeicher" verwenden oder Informationen daraus auslesen dürfen. § 13 Abs. 8 TMG-E unterwirft speziell den Zugriff auf das Endgerät des Nutzers besonderen Einschränkungen. Demgegenüber stellt die Vorschrift keinen zusätzlichen Erlaubnistatbestand für die Erhebung oder Verwendung personenbezogener Daten dar. Inwieweit personenbezogene Daten erhoben oder verwendet werden dürfen, richtet sich nach den übrigen Vorschriften des Telemediengesetzes. Um dies klarzustellen, sollte – wie in der Richtlinie auch – der Begriff des „Zugriffs" auf Daten gewählt werden und nicht die Begriffe der „Erhebung" oder „Verwendung" von Daten.

Der hier vorgeschlagene § 13 Abs. 8 TMG-E setzt Art. 5 Abs. 3 der RiL 2002/58/EG inhaltsgleich um und passt lediglich die Terminologie dem deutschen Sprachgebrauch an.

29. Oktober 2010

Arbeitskreis Vorratsdatenspeicherung

www.AK-Vorrat.de

[68] BT-Drs. 16/11173, 4.