

Speicherung von Nutzungsdaten bei Flatrates als datenschutzrechtliches Problem

Seminararbeit bei Prof. Dr. Jürgen Kühling,
Universität Karlsruhe

von

Jens Müller

22. Juni 2005

Karlsruhe, Juni 2005

Inhaltsverzeichnis

§ 1	Einleitung	1
§ 2	Technischer und wirtschaftlicher Hintergrund	3
	I. Technischer Hintergrund	3
	1. Übertragungsprotokolle	3
	2. IP-Adressen	4
	3. Zugang zum Internet	4
	II. Wirtschaftlicher Hintergrund	4
§ 3	Rechtliche Einordnung der Internet-Nutzung	7
§ 4	Anfallende Daten	9
	I. Zeit und Dauer von Verbindungen	9
	II. Übertragenes Datenvolumen	9
	III. IP-Adresse	9
§ 5	Verfassungsrechtliche Grundlagen	11
	I. Datenschutz	11
	II. Fernmeldegeheimnis	12
§ 6	Datenschutzgesetze	13
	I. Bundesdatenschutzgesetz	13
	II. Teledienstschutzgesetz	14
	1. Datenarten	15
	a) Bestandsdaten	15
	b) Nutzungsdaten	15
	c) Abrechnungsdaten	16
	III. Telekommunikationsgesetz	16
	1. Datenarten	17
	a) Bestandsdaten	17
	b) Verkehrsdaten	17
§ 7	Verwaltungszuständigkeiten	19
§ 8	Rechtliche Bewertung der Speicherung von Nutzungsdaten bei Flat-rates	21
	I. Anwendbarkeit der einzelnen Gesetze auf Internet-Provider	21
	1. Bundesdatenschutzgesetz	21

2.	Teledienststedatenschutzgesetz	21
3.	Telekommunikationsgesetz	22
II.	Bewertung hinsichtlich der verschiedenen anfallenden Daten	22
1.	Zeit und Dauer von Verbindungen	22
a)	Bewertung nach dem TDDSG	22
b)	Bewertung nach dem TKG	23
2.	IP-Adresse	23
a)	Bewertung nach dem BDSG	23
b)	Bewertung nach dem TDDSG	23
c)	Bewertung nach dem TKG	23
3.	Übertragenes Datenvolumen	24
a)	Bewertung nach TDDSG und TKG	24
III.	Fazit	24
§ 9	Schlußbemerkungen	25

§ 1 Einleitung

Das Internet als weltweites Datennetz ist inzwischen allgegenwärtig. Es ist zu einem bedeutenden Wirtschaftsfaktor geworden und erfreut sich auch und gerade bei privaten Nutzern großer Beliebtheit. **1**

Zunehmende Verbreitung finden sogenannte Flatrates, Pauschalangebote zur Nutzung des Internets hauptsächlich über Breitbandanschlüsse. **2**

Wie im digitalen Zeitalter schon „gewohnt“, fallen auch beim Internet-Zugang unterschiedlichste Daten, die sich in ihrer Sensibilität stark unterscheiden.

Ob, wie lange und wofür solche Daten erhoben, gespeichert und genutzt werden sollen und dürfen, war und ist Gegenstand intensiver rechtspolitischer Diskussionen.

Um das Thema umfassend verstehen zu können, ist es notwendig, die technischen und wirtschaftlichen Hintergründe zu begreifen sowie die Internet-Nutzung und die dabei anfallenden Daten in das vielfältige Geflecht von allgemeinen und bereichsspezifischen Datenschutzregelungen sowie das Telekommunikations- und Teledienstrecht einzuordnen. **3**

Außerdem beschäftigt sich diese Arbeit mit den verfassungsrechtlichen Grundlagen von Datenschutz und Telekommunikationsgeheimnis und nimmt schließlich eine detaillierte rechtliche Bewertung vor. **4**

§ 2 Technischer und wirtschaftlicher Hintergrund

I. Technischer Hintergrund

Das Internet ist ein öffentlich verfügbares, weltweites System untereinander verbundener Computer-Netzwerke, die Daten mittels Paketvermittlung unter Benutzung des standardisierten Internet-Protokolls und anderer Protokolle übermitteln¹. 5

Anfangs nur vom US-amerikanischen Militär und wenigen Forschungseinrichtungen benutzt, hat das Internet heute kommerzielle und private Nutzer, deren Anzahl die Milliardengrenze überschritten hat. Dazu beigetragen haben vielfältige auf dem Internet aufbauende Dienste in Bereichen wie Multimedia und eCommerce.

1. Übertragungsprotokolle

Die Übertragung im Internet erfolgt durch eine Familie von Übertragungsprotokollen, die insgesamt unter der Bezeichnung *TCP/IP* bekannt sind. 6

Das *Internet Protocol*² (IP) sorgt dabei für eine Ende-zu-Ende-Übertragung von Paketen (Schicht 3 (Vermittlung) des OSI-Modells³), das *Transport Control Protocol* (TCP) übernimmt die transparente Übertragung von Datenströmen (Schicht 4 (Transport) des OSI-Modells). Die darüberliegenden Schichten 5 bis 7 betreffen die Kommunikationsaspekte von Anwendungen⁴.

Die Koordinierung der technischen Standards für das Internet ist Aufgabe der *Internet Engineering Task Force* (IETF), einer nicht rechtsfähigen Organisation, die von verschiedenen Forschungseinrichtungen getragen wird⁵. 7

Die Vergabe von Protokollparametern ist nicht Aufgabe der IETF, sondern wird von einer als *Internet Assigned Numbers Authority* (IANA) bezeichneten Stelle getragen.

¹ nach <http://en.wikipedia.org/wiki/Internet>, 24. April 2005, eigene Übersetzung

² RFC 791 (Standard), Internet Engineering Task Force, 1981

³ DIN ISO 7498 (Standard): Information technology - Open Systems Interconnection - Basic Reference Model: The basic model

⁴ vgl. Abeck/Lockemann/Schiller/Seitz, *Verteilte Informationssysteme*, dpunkt.verlag 2003, S. 48: „Für die Kooperationsaspekte sind dann die anwendungsorientierten Schichten zuständig; dabei werden allerdings nur solche Kooperationsaspekte behandelt, die zum einen einen unmittelbaren Bezug zur Kommunikation haben und die zum anderen in formaler (d.h. verallgemeinerbarer) Weise behandelbar sind. Darunter fallen beispielsweise die Steuerung des Ablaufs und die Informationsdarstellung.“

⁵ Die IETF bezeichnet sich selbst als *formally established in 1986*. Die Rechtsnatur dieser Gründung ist nicht vollständig klar. Am ehesten dürfte sie einem nicht-ingetragenen Verein oder einer BGB-Gesellschaft entsprechen.

2. IP-Adressen

- 8 Zur Adressierung der Endpunkte einer Datenübertragung im Internet dienen Adressen, die im Standard als Internet-Adresse bezeichnet werden und allgemein unter der Bezeichnung IP-Adresse bekannt sind.
- 9 Wenn man die Datenübertragung im Internet als Telekommunikation ansieht (zu Abgrenzungsfragen s. § 3), handelt es sich dabei um *Nummern* i.S.d. §3 Ziffer 13 TKG 2004.
- 10 IP-Adressen werden von ICANN (*Internet Corporation for Assigned Names and Numbers*), einer Gesellschaft nach dem Recht des US-Bundesstaates Kalifornien, die inzwischen neben weiteren Aufgaben der Netzverwaltung die Funktionen der IANA wahrnimmt, blockweise an regionale Registrierungsstellen und von diesen ebenfalls blockweise hauptsächlich an Internet-Provider, aber auch an institutionelle Nutzer mit größerem Adreßbedarf vergeben. Trotz einer angeblichen Knappheit an IP-Adressen (theoretisch existieren zwei Mrd. IP-Adressen; durch Verschnitt und reservierte Bereiche ist diese Zahl wesentlich geringer) ist Europa recht gut versorgt. Ein Mangel ist am ehesten in den aufstrebenden Regionen Südostasiens zu erwarten.

3. Zugang zum Internet

- 11 Institutionelle Nutzer sind in der Regel über Standleitungen mit dem Internet verbunden. Bis vor einigen Jahren waren bei Privatanutzern fast ausschließlich analoge oder ISDN-Wählverbindungen im Einsatz. Dabei wird über die Telefonleitung eine Verbindung zum Internet hergestellt, für deren Dauer aus dem Bereich des Internet-Zugangsanbieters eine IP-Adresse dynamisch zugewiesen wird.
- 12 Die DSL-Technologie ermöglichte dann für Privathaushalte erschwingliche Breitbandanbindungen über herkömmliche Telefonleitungen aus Kupfer. Mit der Entwicklung dieser Technologie kommen auch im Privatbereich zunehmend Standleitungen vor. Allerdings wird der Zugang auf logischer Ebene auch hier meist als Wählverbindung realisiert.

II. Wirtschaftlicher Hintergrund

- 13 In der Bevölkerung sind Internet-Anschlüsse schon recht weit verbreitet. 2003 hatten 47,3 % (früheres Bundesgebiet) bzw. 40,7 % (Beitrittsgebiet) der Haushalte einen Internet-Anschluß bzw. -Zugang⁶.
- Allerdings sind ISDN-Anschlüsse im Vergleich dazu nur recht schwach verbreitet: 25,6 % im früheren Bundesgebiet und 13,8 % im Beitrittsgebiet. Es ist davon auszugehen, daß die meisten Haushalte, die nicht über einen ISDN-Anschluß verfügen, erst recht keinen DSL-Anschluß verfügen. Die Internet-Nutzung erfolgt dort also per Modem über die analoge Telefonleitung. Wegen der vergleichsweise hohenzeitabhängigen Kosten im Vergleich zu DSL dürfte die Nutzung hier nur sehr sporadisch erfolgen.
- 14 Das Nutzungsverhalten ist in den verschiedenen Bevölkerungsgruppen sehr unterschiedlich. So nutzen 97 % der Studierenden das Internet, aber nur 12 % der Personen im Ruhestand. Insgesamt ist die Nutzung bei Jüngeren stärker als bei Älteren, anteilmäßig am stärksten in der Gruppe der 16-24jährigen.
- 15 Die Verbraucherpreise für Internetnutzung haben (wie die für andere Telekommunikations-

⁶ Quelle für diese und alle weiteren statistischen Angaben, soweit nicht anders angegeben: Statistisches Bundesamt, Statistiken zu Informations- und Kommunikationstechnologien, Band 1, Wiesbaden 2004

dienstleistungen) stark abgenommen. 2003 betragen sie noch 65,9 % des Wertes von 2000. Dieser Preisverfall dürfte in Zukunft weiter anhalten.

Trotzdem hat zum Beispiel der Marktführer T-Online seinen Umsatz 2004 auf 2,01 Mrd. Euro (gegenüber 1,84 Mrd. Euro in 2003) gesteigert. Der Umsatz pro Kunde nahm dabei allerdings leicht ab⁷. **16**

Die einzige Möglichkeit, bei fallenden Preisen pro Zeiteinheit den Umsatz zu halten oder gar zu steigern, ist, entweder neue Kunden zu gewinnen oder die vorhandenen Kunden zu verstärkter Nutzung zu bewegen. **17**

Eine Möglichkeit dafür sind Pauschalpreismodelle, bei denen der Kunde monatlich einen festen Betrag entweder für eine bestimmte Anzahl von Stunden, für ein maximales Datentransfervolumen oder vollkommen pauschal für eine beliebig starke Inanspruchnahme seines Zugangs bezahlt. Insbesondere die vollkommen pauschalen Modelle sowie inzwischen auch die Modelle mit einer Beschränkung des Datenvolumens sind als *Flatrates* (englisch: flacher Tarif, also ein Tarif, der unabhängig von der Dauer der Inanspruchnahme des Dienstes ist) bekannt. **18**

Zwei Anbieter versuchten sich 2000 an einer Flatrate für die Internet-Nutzung über ISDN-Zugang. Hier muß der Anbieter des Internet-Zugangs dem Betreiber des Teilnehmeranschlusses für die Originierung ein zeitabhängiges Entgelt entrichten. Eine Vielzahl von Kunden, die ihre Verbindung ständig, teilweise auch über Nacht, aufrechterhielten, führten beim Anbieter NGI zu hohen, in der Kalkulation nicht erwarteten Kosten, daß er das Angebot drei Monate nach dem Start einstellen mußte und danach mit gravierenden wirtschaftlichen Problemen zu kämpfen hatte. **19**

T-Online setzte sein Angebot noch eine Weile fort, obwohl dort ein ähnliches Nutzungsverhalten vorgelegen haben dürfte. Es wurde vermutet, daß die von T-Online zu zahlenden Entgelte in Form von Werbeschaltungen auf dem Portal von T-Online wieder zurückflossen. Die Regulierungsbehörde für Telekommunikation und Post verpflichtete die Deutsche Telekom AG schließlich, eine „Großhandelsflatrate“ allen interessierten Internet-Zugangsanbietern anzubieten, solange die eigene Tochtergesellschaft T-Online ihre Flatrate anbot. T-Online kündigte daraufhin alle noch bestehenden Verträge fristgemäß und stellte das Angebot ein. **20**

Zu erwähnen ist noch, daß auch zahlreiche Unternehmen, die nicht über den Zugang zur DSL-Teilnehmeranschlußleitung verfügen, Internetzugang über DSL anbieten. Diese lassen den entsprechenden Verkehr entweder regional in ihr eigenes IP-Datennetz leiten oder nutzen entsprechende Vorleistungen, zum Beispiel die IP-Plattform der Deutschen Telekom AG. **21**

⁷ Quelle für die Angaben zu T-Online: http://www.medienmaerkte.de/artikel/internet/050303_t-online.html, Stand: 20. Juni 2005

§ 3 Rechtliche Einordnung der Internet-Nutzung

Das Teledienstegesetz gilt nach seinem § 2 Abs. 1 „für alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt (Teledienste)“.

Nach Abs. 2 Ziffer 3 sind das insbesondere auch „Angebote zur Nutzung des Internets oder weiterer Netze“.

Damit ist jedenfalls der *Zugang* zum Internet ein Teledienst. Es ergeben sich allerdings Abgrenzungsfragen zu Telekommunikationsdiensten.

Diese werden in Rechtspraxis und Literatur zum Teil sehr unterschiedlich wahrgenommen und beantwortet.

So nimmt das Regierungspräsidium Darmstadt dieses Problem in seiner Flatrate-Entscheidung¹ überhaupt nicht wahr, sondern wendet stillschweigend die Vorschriften des TDDSG an, ohne die damit implizite Einordnung des Internet-Zugangs als Teledienst, geschweige denn die mögliche Einordnung als Telekommunikation, auch nur zu erwähnen.

In seiner Anmerkung zu dieser Entscheidung weist Alexander Dix² auf neuere Gerichtsentscheidungen hin, die das Angebot des Internet-Zugangs als Telekommunikationsdienstleistung qualifizieren.

So stellt das OLG Hamburg³ fest, daß Online-Diensteanbieter jedenfalls als Anbieter von TK-Dienstleistungen für die Öffentlichkeit i. S. v. § 3 Nr. 18 TKG und § 3 TKV gelten, soweit sie die Zuführung zu Inhalten im Internet übernehmen.

„Telekommunikation“ ist nach § 3 Nr. 22 TKG „der technische Vorgang des Aussendens, Übermittels und Empfangens von Signalen mittels Telekommunikationsanlagen“. Telekommunikationsanlagen (Nr. 23) sind „technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können“. Telekommunikation meint damit den rein technischen, vom Inhalt unabhängigen Vorgang der Übertragung von Nachrichten in Form von Signalen.

Dieser Vorgang ist schon nach dem Wortlaut des TDG Grundlage für Teledienste.

„Telekommunikation“ und „Teledienst“ können sich also durchaus auf denselben Vorgang beziehen und beschreiben dann unterschiedliche konzeptuelle Ebenen dieses Vorgangs (ähnlich dem bereits erwähnten OSI-Schichtenmodell, vgl. Rn. 6). Fraglich ist dann nicht, ob ein Vorgang Teledienst oder Telekommunikation ist, sondern wo die jeweils betrachtete konzeptuelle Ebene

¹ Regierungspräsidium Darmstadt, Schreiben vom 14.01.2003, II 21.4-3v-04/03-043/02, JurPC-Web-Dok. 43/2003

² A. Dix: Vorratsspeicherung vomn IP-Adressen?, DuD 2003, 234

³ Urteil vom 23. März 2000, MMR 10/2000, 611

dieses Vorgangs anzusiedeln ist.

- 29** Es ist also zu klären, auf welcher „Höhe“ der Schichtenarchitektur der Teledienst beginnt. Klar ist dies auf jeden Fall dann, wenn eine inhaltsbezogene, vom Kommunikationsvorgang abgekoppelte Verarbeitung der übertragenen Daten stattfindet. Dies ist aber nicht hinreichend. Nach dem Wortlaut des Gesetzes meint Telekommunikation zwar nur das Übertragen von Nachrichten und verwandte Vorgänge, nicht aber die Steuerung des Ablaufs einer Kommunikation, die aus dem wechselseitigen Versand von Nachrichten besteht.
- 30** Allerdings ist davon auszugehen, daß der Gesetzgeber diese Sachverhalte nicht streng technisch, sondern umfassend betrachtet wissen wollte.
- 31** Als abschließendes Beispiel sei hier die eMail-Kommunikation genannt. Die Weiterleitung von Nachrichten zwischen Mailservern erfolgt mittels Nachrichten, ist also Telekommunikation. Die Zwischenspeicherung einer eMail auf einem Mailserver wäre bei dieser Betrachtung keine Telekommunikation mehr. Allerdings dient sie der Übertragung der eMail-*Nachricht*. Der Telekommunikationsdienst *eMail übertragen* benutzt hier also den Telekommunikationsdienst *Datenübertragung im Internet*. Dieses Ergebnis deckt sich mit der herrschenden Meinung, daß der eMail-Dienst Telekommunikation darstellt.
- 32** Daraus ergibt sich, daß der reine Datenübertragungsdienst im Internet Telekommunikation darstellt⁴. Da nach dem Wortlaut des Gesetzes der *Zugang* zum Internet einen Teledienst darstellt und die hier untersuchte Datenspeicherung bei Flatrates einen solchen Internet-Zugang betrifft, kann letztendlich dahingestellt bleiben, ob die reine Datenübertragung im Internet *auch* ein Teledienst ist (was der Autor dieser Arbeit tendenziell verneint).
- 33** Problematisch könnte noch sein, daß das TDG nach seinem § 2 Abs. 4 nicht für „Telekommunikationsdienstleistungen und das geschäftsmäßige Erbringen von Telekommunikationsdiensten“ gilt. Dieses Problem kann aufgelöst werden, indem man die Vorschrift so auslegt, daß das TDG keine Anwendung für die Aspekte einer Dienstleistung findet, die nach obigen Ausführungen als Telekommunikation anzusehen sind (so auch das OLG Hamburg, das davon ausgeht, daß „TKG und TDG funktionsbezogen differenziert nebeneinander zur Anwendung“ kommen⁵).

⁴ So auch das OLG Hamburg in seinem Urteil vom 23. März 2000, MMR 10/2000 611

⁵ Leitsatz der Redaktion

§ 4 Anfallende Daten

I. Zeit und Dauer von Verbindungen

Wenn der Internetzugang zumindest logisch als Einwahlzugang realisiert ist, fallen Daten über Uhrzeit und Dauer der Wählverbindungen an. **34**

Für Abrechnungszwecke benötigt der Diensteanbieter diese nicht, wenn der Kunde den Zugang pauschal bezahlt hat. Allenfalls sind sie für die Abrechnung von Vorleistungen notwendig. **35**

Jedenfalls bei ISDN-Flatrates (vgl. Rn. 19f.) hat der Anbieter aber ggf. ein starkes wirtschaftliches Interesse, Vielnutzer zu identifizieren, um ihnen ggf. (ordentlich) zu kündigen und so eine für ihn vorteilhaftere Nutzerstruktur zu erreichen. **36**

Das Interesse, die Nutzung zu begrenzen, um eine effiziente Nutzung von IP-Adressen sicherzustellen, dürfte dagegen gering sein (vgl. Rn. 10). **37**

II. Übertragenes Datenvolumen

Besonders relevant bei DSL-Flatrates ist das übertragene Datenvolumen. Es ist Grundlage für die Entgelte, die der Zugangsanbieter an den Betreiber des IP-Backbones zu zahlen hat. **38**

Erlaubt der Tarif zeitlich eine beliebige Nutzung, ist aber nur ein bestimmtes Datenvolumen inclusive, so wird dieses Datum außerdem für Abrechnungszwecke benötigt. **39**

Eine ständige volle Auslastung der DSL-Verbindung bei einem völlig pauschalen Zugang würde zu einer derart hohen Datenmenge führen, daß die Kalkulation des Anbieters, die von einem Nutzungsverhalten, das im Normalfall wenig intensiv ist und zeitweise einzelne Spitzen zeigt, ausgeht, jedenfalls in Bezug auf den jeweiligen Kunden nicht aufgeht. Auch hier könnte der Anbieter also ein Interesse haben, entsprechende Kunden „loszuwerden“. **40**

III. IP-Adresse

Bei Einwahlzugängen existieren in der Regel weniger IP-Adressen, als es insgesamt Kunden gibt. Dementsprechend werden dem Nutzer mit hoher Wahrscheinlichkeit bei zwei aufeinanderfolgenden Einwahlen unterschiedliche IP-Adressen zugewiesen. Die Speicherung der IP-Adresse kann also sinnvollerweise nur in Verbindung mit Zeit und Dauer der Verbindung, für die diese Adresse zugewiesen war, erfolgen. **41**

Anhand dieser Informationen könnten Daten bei anderen Stellen (oder auch dem Diensteanbieter selbst), die sich auf Verbindungen von einer bestimmten Adresse zu einer bestimmten Uhrzeit beziehen, wieder einer (natürlichen) Person, nämlich dem jeweiligen Nutzer (bzw. zunächst demjenigen, der den Vertrag mit dem Zugangsanbieter abgeschlossen hat), zugeordnet werden. **42**

- 43** Praktisch relevant ist dies bei der Bekämpfung der mißbräuchlichen Nutzung des Internets, zum Beispiel dem Versand unerwünschter eMail-Werbung.

§ 5 Verfassungsrechtliche Grundlagen

I. Datenschutz

Der Datenschutz findet seine verfassungsrechtliche Grundlage in dem „Recht auf informationelle Selbstbestimmung“, das das Bundesverfassungsgericht beginnend mit dem Volkszählungsurteil¹ aus dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG entwickelt hat. 44

Unter den Bedingungen der modernen Datenverarbeitung umfaßt dieses Grundrecht den „Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten“. Es „gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“². 45

Eine Einschränkung dieses Grundrechts ist nur aufgrund gesetzlicher Grundlage, die „die Voraussetzungen und den Umfang der Beschränkungen klar und für den Bürger erkennbar“ und den "Verwendungszweck bereichsspezifisch und präzise bestimmt“. 46

Diese Grundsätze aus der verfassungsgerichtlichen Rechtsprechung wurden für den Fall der Datenerhebung durch den Staat entwickelt. Es besteht jedoch weitgehend Einigkeit, daß aus den Grundrechten auch staatliche Schutzpflichten folgen³. Als Schutzpflicht wird „das rechtlich gebotene Verhalten des Staates, Gefährdungen und Verletzungen grundrechtlich geschützter Güter abzuwehren“ bezeichnet. Dies schließt auch Verletzungen und Gefährdungen durch vorsätzliche und fahrlässige Handlungen Privater mit ein. 47

Der Gesetzgeber ist also verpflichtet, einen effektiven Schutz der Grundrechte sicherzustellen. In der Wahl der Mittel und der Abwägung gegensätzlicher Rechtspositionen hat er dabei ein weites Ermessen, wegen des Grundsatzes der Gewaltenteilung ist dieser legislative Spielraum nur eingeschränkt verfassungsgerichtlich überprüfbar. 48

Allerdings darf ein gewisses Mindestschutzniveau nicht unterschritten werden. Die getroffenen Maßnahmen müssen dabei geeignet sein, einen angemessenen Schutz strukturell sicherzustellen. So genügt eine reine Verbotsnorm nicht, wenn mangels Durchsetzungsmöglichkeiten nicht damit zu rechnen ist, daß diese eine schützende Wirkung entfalten kann. 49

Vor dem Hintergrund dieser verfassungsrechtlichen Vorgaben hat der Gesetzgeber ein ausdifferenziertes System allgemeiner und bereichsspezifischer (so für die Bereiche Telekommunikation und Teledienste) Regelungen entwickelt, die den Umgang mit personenbezogenen Daten durch Private regulieren und umfangreiche institutionelle Vorkehrungen treffen, um ihre Einhaltung sicherzustellen. 50

Bei der Auslegung dieser Regelungen sind die genannten verfassungsrechtlichen Vorgaben zu berücksichtigen. 51

¹ BVerfG, 1. Senat, Urteil vom 15. Dezember 1983, BVerfGE 65,1

² ebenda, Leitsätze des Gerichts, Nr. 1

³ zur Problematik vgl. <http://www.student-online.net/Publikationen/296/> (16. Juni 2005)

II. Fernmeldegeheimnis

- 52** Das Fernmeldegeheimnis ist gemäß Art. 10 Abs. 1 GG unverletzlich⁴. Grund für diesen spezifischen Schutz der Telekommunikation ist, daß die Gesprächspartner anders als bei einem unmittelbaren persönlichen Gespräch bei einem Gespräch über eine räumliche Distanz, das durch Telekommunikationseinrichtungen vermittelt wird, eine Kenntnisnahme der Kommunikation durch Dritte regelmäßig weder bemerken noch kontrollieren können.
- 53** Durch die Gewährleistung des Fernmeldegeheimnisses werden also die fehlenden Eigenschutzmöglichkeiten ausgeglichen.
- 54** Der Schutzbereich umfaßt den Inhalt und die näheren Umstände fernmeldetechnisch übertragener individueller Kommunikation. Soweit Verkehrsdaten über den Abschluß des einzelnen Telekommunikationsvorgangs hinaus gespeichert werden, wirkt der Schutz auch nach und schützt insofern die Daten vor staatlichem Zugriff. Die Anforderungen entsprechen dabei denen, die sich aus dem Recht auf informationelle Selbstbestimmung generell für die Verarbeitung personenbezogener Daten ergeben („datenschutzrechtliche Dimension des Fernmeldegeheimnisses“).
- 55** Eine Fortwirkung des Fernmeldegeheimnisses ergibt sich selbst dann noch, wenn sich Daten über Kommunikation nicht im Machtbereich des Erbringers der Telekommunikationsdienstleistung befinden, sondern in dem des Teilnehmers. So hat das Bundesverfassungsgericht⁵ entschieden, daß die Beschlagnahme eines Mobiltelefons, um die darin gespeicherten Informationen über geführte Gespräche zu gewinnen, mit der in §§ 100g und 100h StPO normierten, auf Art. 10 Abs. 2 GG beruhenden Begrenzungsfunktion nicht zu vereinbaren ist. Das Gericht hat hier zwar Art. 10 GG nicht direkt angewandt, wohl aber eine gewisse Ausstrahlungswirkung des Fernmeldegeheimnisses auf die Rechtsordnung bejaht.
- 56** Beschränkungen dürfen nach Art. 10 Abs. 2 S. 1 GG nur aufgrund eines Gesetzes angeordnet werden, wobei das Zitiergebot des Art. 19 Abs. 1 S. 2 GG zu beachten.
- 57** Während sich das Fernmeldegeheimnis früher hauptsächlich an den Staat in Form der Deutschen Bundespost als Träger der Verwaltung im Fernmeldewesen richtete. Mit der Privatisierung ist die Bedeutung dieser Schutzrichtung fast vollständig verlorengegangen, da die Privaten, die nun Telekommunikationsdienstleistungen nunmehr erbringen, nicht unmittelbar an Art. 10 GG gebunden sind. In diesem Umfeld entfaltet das Fernmeldegeheimnis seine Wirkung einerseits gegenüber staatlichen Überwachungsmaßnahmen, andererseits in Form einer Schutzpflicht gegenüber Beeinträchtigungen durch Private. Dem ist der Gesetzgeber u.a. durch die Verpflichtung der privaten Leistungserbringer auf ein einfachrechtliches Fernmeldegeheimnis (§ 88 TKG) nachgekommen.
- 58** Auch im Bereich des Fernmeldegeheimnisses umfaßt die Schutzpflicht die Sicherstellung eines *effektiven* Schutzes vor Beeinträchtigungen durch Private, indem die oben erwähnte Verpflichtung durch geeignete institutionelle Vorkehrungen durchgesetzt wird.

⁴ Zu den Ausführungen dieses Abschnitts vgl. Koenig/Loetz/Neumann: Telekommunikationsrecht, 3. Kapitel, C.I.

⁵ Bundesverfassungsgericht, 2 BvR 308/04, Urteil vom 4. Februar 2005, http://www.bverfg.de/entscheidungen/rk20050204_2bvr030804.html

§ 6 Datenschutzgesetze

Die Schutzwirkung der Grundrechte aus Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG (informationelle Selbstbestimmung) und Art. 10 Abs. 1 GG (Fernmeldegeheimnis) verlangt vom Gesetzgeber, einen ausreichenden und effektiven Schutz dieser Grundrechte vor Beeinträchtigungen durch Private sicherstellen. **59**

Staatliche Eingriffe bedürfen einer gesetzlichen Grundlage, die zur Erreichung eines legitimen Ziels erforderlich und geeignet ist und die Verhältnismäßigkeit im engeren Sinne wahrt. **60**

In beiden Fällen muß der Staat eine effektive Kontrolle vorsehen, um Mißbrauchsmöglichkeiten jedenfalls struktureller Art weitestgehend auszuschließen. **61**

Die unterschiedlichen Gegebenheiten in unterschiedlichen Rechts- und Lebensgebieten führen zu einer Vielzahl von datenschutzrechtlichen Regelungen aus unterschiedlichen Rechtsquellen (Bundes- und Landesgesetze, Rechtsverordnungen, Satzungen, Tarifverträge, Betriebs- und Dienstvereinbarungen). **62**

Das allgemeine Datenschutzrecht besteht aus dem Bundesdatenschutzgesetz (BDSG) und den Datenschutzgesetzen der Länder, die als Auffanggesetze fungieren¹. **63**

Daneben existieren bereichsspezifische Regelungen. Diese können einerseits in Form von Gesetzen auftreten, die sich ausschließlich mit dem Datenschutz in einem bestimmten Bereich auftreten (so zum Beispiel das Teledienststedatenschutzgesetz (TDDSG)). **64**

Andererseits verteilen sich datenschutzrechtliche Regelungen über eine Vielzahl von Fachgesetzen, so etwa SGB I, SGB X, TKG, StGB und StPO. Datenschutzrecht stellt damit eine Querschnittsmaterie dar, ist also kein in seinem Anwendungsbereich genau abgrenzbares Rechtsgebiet, sondern entfaltet Auswirkungen auf die gesamte Rechtsordnung. **65**

Grund für die bereichsspezifischen Regelungen ist, daß allgemeine Datenschutzvorschriften, die zwangsläufig abstrakt gefaßt sein müssen, die sich aus dem Volkszählungsurteil ergebenden Anforderungen nach Normenklarheit nicht erfüllen können (vgl. Rn. 46). **66**

Für die vorliegende Fragestellung sind im wesentlichen folgende Gesetze relevant:

I. Bundesdatenschutzgesetz

Wie bereits erwähnt, ist das BDSG datenschutzrechtliches Auffanggesetz. Sein Zweck ist es, „den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.“ (§ 1 Abs. 1). **67**

Es gilt „für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten“ durch „nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien **68**

¹ vgl. Gola/Klug, Grundzüge des Datenschutzrechts, Verlag C. H. Beck 2003, S. 7

verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten“ (§ 1 Abs. 2 Nr. 3).

69 Das Verhältnis des BDSG zu anderen, bereichsspezifischen Rechtsnormen wird in § 1 Abs. 3 geregelt: „Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor“ (Grundsatz der Subsidiarität, *lex specialis derogat legi generali*). Die Vorschriften des BDSG treten dabei nur zurück, *soweit* andere Rechtsvorschriften des Bundes anwendbar sind. Für Sachverhalte, die vom spezielleren Gesetz nicht erfaßt werden, ist also ein Rückgriff auf das BDSG notwendig.

70 Jegliche Art Datenerhebung, -verarbeitung und -nutzung steht unter dem Vorbehalt der Erlaubnis durch das BDSG oder andere Rechtsvorschriften. Auch eine Einwilligung durch den Betroffenen reicht aus (bei einer informierten, ohne Zwang erfolgten Einwilligung liegt schon tatbestandsmäßig kein Eingriff in die informationelle *Selbstbestimmung* vor) (§ 4 Abs. 1).

71 Im Ersten Abschnitt des Gesetzes werden Regelungen getroffen, die für nicht-öffentliche und öffentliche Stellen gleichermaßen gelten. So werden bestimmte Rechte des Betroffenen für unabdingbar erklärt (§ 6), technische und organisatorische Maßnahmen vorgeschrieben (§ 9) und ein Anspruch auf Schadenersatz normiert (§ 7).

72 Die Datenverarbeitung durch nicht-öffentliche Stellen regelt der Dritte Abschnitt. Er legt verschiedene Rechtsgrundlagen für die Datenverarbeitung fest, regelt die Rechte der Betroffenen (Benachrichtigung, Anspruch auf Auskunft, Berichtigung, Löschung und Sperrung) und schreibt die Einrichtung von Aufsichtsbehörden durch Landesrecht vor.

73 Nach Landesrecht zuständig sind entweder die auch für den öffentlichen Bereich zuständigen unabhängigen Datenschutzbeauftragten oder aber Innenministerien, Bezirksregierungen oder ähnliche Stellen. Der letztgenannte Fall begegnet in Datenschutzkreisen zunehmend Bedenken, da die hinreichende Unabhängigkeit solcher Stellen von politischer Einflußnahme bezweifelt wird.

II. Teledienstedatenschutzgesetz

74 Das Gesetz über den Datenschutz bei Telediensten (Teledienstegesetz – TDDSG) gilt nach seinem § 1 Abs. 1 „für den Schutz personenbezogener Daten bei Telediensten im Sinne des Teledienstegesetzes“ (vgl. Rn. 22 ff.). In den Anwendungsbereich wird auch der Schutz von Daten einbezogen, die nicht in Dateien verarbeitet oder genutzt werden (§ 1 Abs. 2).

75 Diensteanbieter und damit Verpflichtete nach diesem Gesetz sind solche, „die Teledienste zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln“ (§ 2 Nr. 1).

76 In seinem § 3 stellt das Gesetz Grundsätze für die Verarbeitung personenbezogener Daten auf. Der Erlaubnis- und Einwilligungsvorbehalt (Abs. 1) und der Zweckbindungsgrundsatz (Abs. 2) unterscheiden sich dabei nicht vom allgemeinen Datenschutzrecht.

77 Interessant ist das Verbot, die Erbringung von Telediensten davon abhängig zu machen, daß der Nutzer der Verarbeitung oder Nutzung für andere Zwecke zustimmt. Dieses Verbot gilt nur dann, wenn dem Nutzer ein anderer Zugang nicht oder nicht in zumutbarer Weise möglich ist. Damit soll das „Abpressen“ einer Zustimmungserklärung durch einen Monopolanbieter oder durch entsprechendes übereinstimmendes Verhalten mehrerer marktbeherrschender Anbieter verhindert werden.

78 Weiter wird der Grundsatz der Datensparsamkeit aufgestellt (Abs. 4): „Die Gestaltung und Auswahl technischer Einrichtungen für Teledienste hat sich an dem Ziel auszurichten, keine

oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen“. Konkretisiert wird dies durch die Verpflichtung, „dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist“ (§ 4 Abs. 1 S. 1). In diesem Fall entfällt die Personenbindung der Daten, die Eingriffsintensität sinkt damit dramatisch.

Da der Nutzer nicht unmittelbar erkennen kann, welche Daten gerade erhoben werden und vor allem, für welchen Zweck dies geschieht, stellt das Gesetz eine Unterrichtungspflicht auf (§ 3 Abs. 5). Dabei schreibt es die Protokollierung der Unterrichtung vor. Der Nutzer kann auf die Unterrichtung auch verzichten (was ebenfalls zu protokollieren ist). Dies birgt die Gefahr, daß Nutzer sich von ständigen Unterrichtungen derart gestört oder überfordert fühlen, daß sie sie irgendwann überhaupt nicht mehr wahrnehmen. In gewisser Weise wird dem durch den Grundsatz der Datensparsamkeit begegnet, indem die Zahl der Datenerhebungsvorgänge und damit der Unterrichtungen des Nutzers möglichst gering gehalten soll. Langfristig wird man sich aber Gedanken über eine automatische Form Unterrichtung und Zustimmung, zum Beispiel durch Abgleich der Privacy Policies von Anbieter und Nutzer, Gedanken machen müssen. Auch Datenverarbeitungsvorgänge, die der einzelne schon aufgrund der schiereren Menge nicht mehr überblicken kann, beeinträchtigen nämlich sein Recht auf informationelle Selbstbestimmung.

Das Gesetz stellt datenschutzrechtliche Pflichten für Diensteanbieter (§ 4) auf, die durch die Besonderheiten von Telediensten (Nutzung aus räumlicher Distanz mittels Telekommunikation) notwendig werden. So müssen Nutzungsdaten bis auf Abrechnungsdaten unmittelbar nach Beendigung der Nutzung gelöscht werden (§ 4 Abs. 2 Nr. 2) und der Teledienst gegen Kenntnisnahme Dritter geschützt in Anspruch genommen werden können (Nr. 3). Außerdem dürfen Daten über die Nutzung verschiedener Teledienste nicht gemeinsam verarbeitet werden, eine Zusammenführung ist nur zulässig, wenn dies für Abrechnungszwecke erforderlich ist (Nr. 4). Diese Verpflichtungen müssen durch technische und organisatorische Vorkehrungen sichergestellt werden. Dies stellt eine Konkretisierung von § 9 BDSG dar, allerdings ohne den dort noch enthaltenen Vorbehalt der Verhältnismäßigkeit.

1. Datenarten

Das Teledienstedatenschutzgesetz definiert unterschiedliche Kategorien von Daten, deren Verarbeitung ein unterschiedlich starkes Gefährdungspotential für das Grundrecht auf informationelle Selbstbestimmung mit sich bringt und an deren Verarbeitung daher auch jeweils unterschiedliche Anforderungen gestellt werden.

a) Bestandsdaten

Bestandsdaten sind Daten, die „für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses“ mit dem Diensteanbieter „über die Nutzung von Telediensten erforderlich sind“ (§ 5 Abs. 1). Diese Daten dürfen vom Diensteanbieter erhoben, verarbeitet und genutzt werden, *soweit* diese Erforderlichkeit reicht.

Für andere Zwecke (Beratung, Werbung, Marktforschung, bedarfsgerechte Gestaltung der Teledienste) dürfen die Daten nur mit ausdrücklicher Einwilligung des Nutzers gespeichert werden.

b) Nutzungsdaten

Nutzungsdaten sind Daten, die dem Nutzer die Inanspruchnahme von Telediensten ermögli-

chen sollen. Diese Daten dürfen nur erhoben, verarbeitet und genutzt werden, soweit es für diesen Zweck erforderlich ist (§ 6 Abs. 1 Nr. 1). Sie sind frühstmöglich zu löschen, *spätestens* unmittelbar nach dem Ende der jeweiligen Nutzung², soweit es sich nicht um Abrechnungsdaten handelt. Soweit Daten nicht notwendig sind, um die Inanspruchnahme des Teledienstes zu ermöglichen, handelt es sich nicht um Nutzungsdaten im Sinne dieser Vorschrift, damit dürfen sie erst gar nicht (jedenfalls nicht personenbezogen) erhoben werden.

c) Abrechnungsdaten

85 Abrechnungsdaten sind Daten, die erforderlich sind, um die Nutzung von Telediensten abzurechnen (§ 6 Abs. 1 Nr. 2). Auch diese Daten dürfen nur soweit dafür erforderlich erhoben, verarbeitet und genutzt werden. Sie sind zu löschen, sobald sie für Zwecke der Abrechnung nicht mehr erforderlich sind. Ein Einzelnachweis wird nur auf Verlangen des Nutzers erstellt (§ 6 Abs. 5), dementsprechend ist die Speicherung von Daten über Anbieter, Zeitpunkt, Dauer, Art und Häufigkeit von in Anspruch genommenen Telediensten nicht erforderlich, falls der Nutzer einen Einzelnachweis nicht verlangt hat.

86 Nutzerbezogene Abrechnungsdaten, die zur Erstellung von Einzelnachweisen benutzt wurden, sind spätestens 80 Tage nach Versendung des Einzelnachweises zu löschen, es sei denn, die Entgeltforderung wurde bestritten oder nicht beglichen.

87 Der Anbieter kann Abrechnungsdaten an Dritte übermitteln, wenn er mit diesen einen Vertrag über die Abrechnung geschlossen hat (§ 6 Abs. 4). Er hat den Dritten dabei zur Wahrung des *Fernmeldegeheimnisses* zu verpflichten. Trotz der Abgrenzung von Telediensten und Telekommunikation geht der Gesetzgeber also offenbar davon aus, daß die Nutzung von Telediensten vom Schutzbereich des Fernmeldegeheimnisses erfaßt wird.

88 Anders als im allgemeinen Datenschutzrecht hat der Nutzer auch bei kurzfristiger Speicherung ein Auskunftsrecht, die Auskunft muß auf Verlangen elektronisch erfolgen (§ 7)

89 Schließlich verweist das Gesetz (§ 8 Abs. 1) bezüglich der Aufsicht auf § 38 BDSG. Auch im Teledienstebereich sind also nach Landesrecht bestimmte Stellen für die Aufsicht zuständig (vgl. Rn. 73). Überprüfungen dürfen diese auch verdachtsunabhängig vornehmen.

III. Telekommunikationsgesetz

90 Fernmeldegeheimnis und Datenschutz werden in Abschnitt 1 bzw. Abschnitt 2 von Teil 7 des TKG³ geregelt.

91 Dem Fernmeldegeheimnis unterliegen „der Inhalt der Telekommunikation und ihre näheren Umstände“ (§ 88 Abs. 1). Verpflichteter ist jeder Diensteanbieter (§ 88 Abs. 2).

92 Zunächst ist es den Verpflichteten untersagt, „sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen“ (§ 88 Abs. 3 S. 1). Soweit sie unter diesen Voraussetzungen Kenntnisse erlangen, unterliegen diese einer strengen Zweckbindung (Satz 2).

93 Dementsprechend sind die Datenschutzvorschriften in Abschnitt 2 ebenfalls unter Berücksichtigung des Fernmeldegeheimnisses zu betrachten, da sie auch den Umgang mit Daten regeln,

² Daraus ergibt sich die Verpflichtung, Nutzungsdaten ggf. auch schon während der Nutzung wieder zu löschen, wenn ihre weitere Speicherung nicht mehr erforderlich ist!

³ Telekommunikationsgesetz vom 22. Juni 2004, BGBl. I 2004, 1190

die sich auf die näheren Umstände der Telekommunikation beziehen und damit dem Fernmeldegeheimnis unterliegen.

In den Anwendungsbereich dieses Abschnitts fallen personenbezogene Daten der Teilnehmer und Nutzer von Telekommunikation, einschließlich juristischer Personen. **94**

Den Diensteanbietern werden umfangreiche Informationspflichten über Erhebung und Verwendung personenbezogener Daten auferlegt (§ 93). **95**

Ähnlich der Regelung im TDG ist eine Einwilligung im elektronischen Verfahren möglich (§ 94). **96**

1. Datenarten

Auch das TKG unterscheidet verschiedene Arten von Daten und verbindet damit jeweils unterschiedliche rechtliche Regelungen. **97**

a) Bestandsdaten

Bestandsdaten sind „Daten, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienstleistungen erhoben werden“ (§ 3 Nr. 3 TKG). Der Diensteanbieter darf sie erheben und verwenden, soweit es für diesen Zweck erforderlich ist (§ 95 Abs. 1 S. 1). Soweit zur Vertragserfüllung erforderlich, darf er sie auch an Dritte übermitteln. **98**

Wie auch im Teledienstegesetz (vgl. Rn. 83) ist die Verwendung zur Werbung, Marktforschung und Beratung nur mit Einwilligung zulässig. Ebenfalls ähnlich wie im TDDSG (Rn. 77) wurde ein Kopplungsverbot geregelt, nach dem die Erbringung der Dienstleistung nicht von der Einwilligung in die Verwendung für diese Zwecke abhängig gemacht werden darf, wenn ein anderer Zugang nicht oder nicht in zumutbarer Weise möglich ist. **99**

b) Verkehrsdaten

Verkehrsdaten sind „Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden“ (§ 3 Nr. 30 TKG). Das Gesetz legt fest, welche Verkehrsdaten überhaupt erhoben und verwendet werden dürfen. Dazu gehören (§ 96 Abs. 1) Anschlußkennungen der beteiligten Anschlüsse, Beginn und Ende von Verbindungen, übermittelte Datenmengen, soweit davon Entgelte abhängen und welcher Telekommunikationsdienst in Anspruch genommen wurde. Diese Daten dürfen erhoben verwendet werden, soweit es für die im Abschnitt genannten Zwecke erforderlich ist. Zulässig ist außerdem die Erhebung und Verwendung „sonstige[r] zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige[r] Verkehrsdaten“ (§ 96 Abs. 1 Nr. 5). **100**

Über das Ende der Verbindung hinaus dürfen die Verkehrsdaten nur verwendet werden, soweit sie zum Aufbau weiterer Verbindungen oder für die in den §§ 97 (Entgeltermittlung und -abrechnung), 99 (Einzelverbindungsachweis), 100 (Störungsbeseitigung, Mißbrauchsbekämpfung) und 101 („Fangschaltung“) genannten Zwecke erforderlich sind. Ansonsten sind sie nach Beendigung der Verbindung unverzüglich zu löschen (§ 96 Abs. 2). **101**

Zur Entgeltermittlung dürfen die in § 96 Abs. 1 Nr. 1 genannten Daten (v.a. Kennungen der beteiligten Anschlüsse) verwendet werden, soweit sie dafür benötigt werden. **102**

Aus den Verkehrsdaten sind nach dem Ende der Verbindung unverzüglich die für die Berechnung des Entgelts erforderlichen Daten zu ermitteln, nicht mehr benötigte Daten sind dann zu löschen (§ 97 Abs. 3). „Unverzüglich“ im Rechtssinne bedeutet „ohne schuldhaftes Zögern“. **103**

- 104** Zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen darf der Diensteanbieter die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden (§ 100 Abs. 1).
- 105** „Bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte“ darf der Diensteanbieter, soweit erforderlich, die Bestandsdaten erheben und verwenden, „die zum Aufdecken sowie Unterbinden von Leistungerschleichungen und sonstigen rechtswidrigen Inanspruchnahmen der Telekommunikationsnetze und -dienste erforderlich sind“ (§ 100 Abs. 3).
- 106** Zu nennen ist außerdem noch die Verpflichtung, die Anzeige der Rufnummer zu unterdrücken (§ 102). Rufnummern sind allerdings Nummern, „durch deren Wahl im öffentlichen *Telefondienst* eine Verbindung zu einem bestimmten Ziel aufgebaut werden kann“ (§ 3 Nr. 18). Damit ist diese Vorschrift auf IP-Adressen keinesfalls anwendbar.

§ 7 Verwaltungszuständigkeiten

- Die Regelungen der Datenschutzgesetze, die die Aufsicht über die Einhaltung der materiellen Datenschutzvorschriften regeln, haben zum Ziel, eine möglichst effektive, von politischer Einflußnahme unabhängige Kontrolle sicherzustellen. **107**
- Die Kontrolle über *öffentliche* Stellen wird daher stets durch unabhängige Datenschutzbeauftragte wahrgenommen. Für den Bereich des Bundes ist dies der Bundesbeauftragte für den Datenschutz, dessen Rechtsstellung in § 22 BDSG geregelt ist. Er unterliegt keiner Fachaufsicht und ist von Weisungen unabhängig. Ähnliches gilt für die Datenschutzbeauftragten der Länder, die für die Aufsicht über deren öffentliche Stellen zuständig sind. **108**
- Hingegen ist die Aufsicht über nicht-öffentliche Stellen sehr unterschiedlich geregelt. In den meisten Ländern sind dafür Verwaltungsbehörden auf Landes- oder Regierungsbezirkebene zuständig. Vieles spricht dafür, dieses Modell kritisch zu betrachten. So können diese (weisungsgebundenen) Stellen versucht sein, zum Beispiel aus standortpolitischen oder anderen sachfremden Erwägungen heraus bei der Aufsicht weniger strenge Maßstäbe anzuwenden. **109**
- Dementsprechend haben einige Länder sich entschieden, auch die Aufsicht über die Privatwirtschaft von den Landesbeauftragten für den Datenschutz ausüben zu lassen.
- Für die Aufsicht im Teledienstebereich sind von den Ländern bestimmte Stellen zuständig (§ 8 Abs. 1 TDDSG i. V. m. § 38 BDSG), also in der Regel dieselben Stellen, die die allgemeine Datenschutzaufsicht ausüben. Der Bundesbeauftragte für den Datenschutz hat lediglich die Aufgabe, die Entwicklung des Datenschutzes in diesem Bereich zu beobachten und darüber zu berichten. **110**
- Die Regulierungsbehörde für Telekommunikation und Post kann auch zur Sicherstellung der datenschutzrechtlichen Vorschriften des TKG (Abschnitt 2 des Teils 7) Anordnungen und andere Maßnahmen treffen (§ 115 Abs. 1 TKG). **111**
- „Soweit für die geschäftsmäßige Erbringung von Telekommunikationsdiensten Daten von natürlichen oder juristischen Personen erhoben, verarbeitet oder genutzt werden“, ist zuständige Aufsichtsbehörde der Bundesbeauftragte für den Datenschutz (§ 115 Abs. 4 TKG). Die Telekommunikationsanbieter unterliegen damit einer bundesweit einheitlichen Datenschutzaufsicht. **112**
- Interessant ist in diesem Zusammenhang, daß, soweit der Internet-Zugang Telekommunikationsdienst ist, das Regierungspräsidium Darmstadt nicht die zuständige Aufsichtsbehörde für T-Online war. Das mag erklären, warum es in seiner Entscheidung auf diese Abgrenzungsproblematik nicht eingegangen ist. **113**

§ 8 Rechtliche Bewertung der Speicherung von Nutzungsdaten bei Flatrates

Um zu bestimmen, unter welchen Bedingungen die Speicherung oder Verwendung von Nutzungsdaten bei Flatrates zulässig ist, ist zunächst zu bestimmen, unter welche gesetzlichen Regelungen dieser Zugang einzuordnen ist. **114**

Außerdem muß jeweils bestimmt werden, unter welche in den bereichsspezifischen Gesetzen definierte Datenart die verschiedenen Nutzungsdaten jeweils einzuordnen sind. **115**

Zu beachten ist, daß das BDSG zurücktritt, soweit TDDSG oder TKG anwendbar sind und eine andere Regelung treffen (vgl. Rn. 69). Diese Verdrängungswirkung tritt aber nicht zwangsläufig vollständig ein. **116**

I. Anwendbarkeit der einzelnen Gesetze auf Internet-Provider

Zunächst ist – unabhängig von den einzelnen Daten – zu prüfen, ob Internet-Provider Normadressaten der Datenschutzgesetze sind. **117**

1. Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz gilt „für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch“ „nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten“ (§ 1 Abs. 2 Nr. 3 BDSG). Internet-Provider sind in der Regel nicht-öffentliche Stellen (der Fall, daß ein Internet-Provider öffentliche Stelle ist, soll hier nicht betrachtet werden), und ausnahmslos alle anfallenden Nutzungsdaten werden unter Einsatz von Datenverarbeitungsanlagen erhoben. Eine persönliche oder familiäre Tätigkeit liegt ebenfalls nicht vor. Das BDSG ist damit grundsätzlich anwendbar. **118**

2. Teledienstedatenschutzgesetz

Das Teledienstedatenschutzgesetz gilt „für den Schutz personenbezogener Daten der Nutzer von Telediensten im Sinne des Teledienstegesetzes bei der Erhebung, Verarbeitung und Nutzung dieser Daten durch Diensteanbieter“ (§ 1 Abs. 1 S. 1 TDDSG). **119**

„Diensteanbieter“ ist „jede natürliche oder juristische Person, die eigene oder fremde Teledienste zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt“ (§ 2 S. 1 Nr. 1 **120**

TDDSG). Soweit der Internetzugang Teledienst ist, wird ein eigener oder (bei Reselling) fremder Teledienst zur Nutzung bereitgehalten, jedenfalls wird aber über diesen Zugang die Nutzung anderer Teledienste vermittelt. Das TDDSG ist daher grundsätzlich anwendbar.

3. Telekommunikationsgesetz

- 121** Im Sinne des TKG ist Diensteanbieter „jeder, der ganz oder teilweise geschäftsmäßig a) Telekommunikationsdienste erbringt“ (§ 3 Nr. 6 TKG). Soweit die Datenübertragung im Internet Telekommunikation ist, werden Telekommunikationsdienste erbracht. „Geschäftsmäßig“ werden diese erbracht, wenn es sich um ein „nachhaltige[s] Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht“ handelt (§ 3 Nr. 10 TKG). Das trifft für die allermeisten Internetprovider zu. Damit ist das TKG einschließlich seiner datenschutzrechtlichen Vorschriften grundsätzlich anwendbar.

II. Bewertung hinsichtlich der verschiedenen anfallenden Daten

- 122** Da die Einordnung des Internet-Zugangs als Teledienst oder Telekommunikation umstritten ist, die meisten Zugangsanbieter aber aufbauend auf dem reinen Zugang auch Dienste anbieten, die unstreitig als Teledienste einzuordnen sind (z. B. Webmail, Portal mit Suchmaschine, etc.), sollen im folgenden beide Annahmen untersucht werden. Die Untersuchung orientiert sich dabei an den verschiedenen oben genannten Datenarten.
- 123** Alle genannten Gesetze stellen für den Umgang mit personenbezogenen Daten ein grundsätzliches Verbot unter dem Vorbehalt durch Rechtsvorschrift gegebener Erlaubnistatbestände oder einer qualifizierten Einwilligung auf. Solche Erlaubnistatbestände können sich dann auch aus dem BDSG ergeben, selbst wenn primär zum Beispiel das TDDSG einschlägig ist. Es werden daher möglicherweise einschlägige Erlaubnistatbestände untersucht.

1. Zeit und Dauer von Verbindungen

- 124** Bestimmte Erlaubnistatbestände machen nur in Zusammenhang mit der IP-Adresse Sinn. Sie werden im folgenden Unterabschnitt untersucht.

a) Bewertung nach dem TDDSG

- 125** Nach § 6 Abs. 4 TDDSG darf der Anbieter Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus speichern, soweit sie für Zwecke der Abrechnung *mit dem Nutzer* erforderlich sind.
- Eine Notwendigkeit für die Abrechnung mit dem Erbringer von Vorleistungen ist für diese Vorschrift unbeachtlich. Für die Abrechnung mit dem Nutzer ist die Nutzungsdauer nicht erforderlich, eine weitere Speicherung ist also nach dieser Vorschrift nicht erlaubt.
- Anderer Ansicht ist das Regierungspräsidium Darmstadt, das für diesen Zweck sogar eine Speicherung der IP-Adresse für zulässig erachtet (s. u. unter Rn. 130).
- 126** Wenn der Nutzer nicht widerspricht, dürfen pseudonymisierte Nutzungsprofile für Zwecke der Werbung, der Marktforschung oder der bedarfsgerechten Gestaltung der Teledienste erstellt werden (§ 6 Abs. 3 TDDSG).
- Allerdings muß hier eine Unterrichtung erfolgen, der Nutzer kann dann jederzeit widersprechen. Soweit die Unterrichtung erfolgt ist und der Nutzer nicht widersprochen hat, ist hiernach eine Nutzung zulässig.

b) Bewertung nach dem TKG

Auch nach § 97 TKG dürfen Diensteanbieter Beginn und Ende von Verbindungen erheben, soweit sie zur Ermittlung des Entgelts sind. Für die Entgeltermittlung ist die Nutzungsdauer nicht erforderlich, eine weitere Speicherung ist also nach dieser Vorschrift nicht erlaubt. **127**

Nach § 96 Abs. 3 TKG dürfen teilnehmerbezogene Verkehrsdaten „zum Zwecke der Vermarktung von Telekommunikationsdiensten, zur bedarfsgerechten Gestaltung von Telekommunikationsdiensten oder zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Zeitraum“ verwendet werden, sofern der Betroffene eingewilligt hat. **128**

In diesem Fall ist also eine entsprechende Nutzung zulässig.

2. IP-Adresse**a) Bewertung nach dem BDSG**

Das Regierungspräsidium Darmstadt sieht die Speicherung der IP-Adresse als zur Gewährleistung der Datensicherheit erforderlich vor Hacker-Angriffen und damit nach §9 BDSG zulässig an. **129**

Eine Norm, die Maßnahmen zum Schutz personenbezogener Daten vorschreibt, als Einfallstor für einen weiteren *Eingriff* in das Recht auf informationelle Selbstbestimmung in Form einer Ermächtigung zur Datenerhebung anzusehen, begegnet erheblichen verfassungsrechtlichen Bedenken. Eine solche nicht gerade naheliegende Lesart verletzt den für Eingriffe in dieses Grundrecht in besonderer Weise geltenden Grundsatz der Normenklarheit.

Außerdem ist die Maßnahme auch nicht erforderlich, da geeignete technische Maßnahmen zum Schutz der Datenverarbeitungsanlagen existieren. Eine Speicherung ist daher nicht nach dieser Vorschrift zulässig.

b) Bewertung nach dem TDDSG

Noch weniger als die Nutzungszeiten ist die IP-Adresse für Abrechnungszwecke erforderlich. Anderer Ansicht ist das Regierungspräsidium Darmstadt. Danach ist die „Speicherung der IP-Nummer [...] gerechtfertigt, damit die T-Online International AG im Zweifelsfall die kostenpflichtige Erbringung ihrer Leistung wirklich korrekt und durchsetzbar nachweisen kann“¹. Diese Ansicht begegnet in der Literatur erheblichem Widerstand². Ein „Qualitätsverlust“ bei der Nachweisbarkeit und Durchsetzbarkeit von Forderungen ist danach für die Frage der Erforderlichkeit im datenschutzrechtlichen Sinne ohne Belang. Zusätzliche Befugnisse für die Aufklärung mißbräuchlicher Nutzung regelt § 6 Abs. 8 TDDSG abschließend. **130**

c) Bewertung nach dem TKG

Bezüglich der Erforderlichkeit für Abrechnungszwecke gelten auch nach dem TKG die für das TDDSG angestellten Betrachtungen. **131**

Gemäß § 111 TKG hat ein Diensteanbieter, der „Rufnummern vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern bereitstellt“, „für die Auskunftsverfahren nach den §§ 112 und 113 die Rufnummern, den Namen und die Anschrift des Rufnummerninhabers, das Datum des Vertragsbeginns“ (und andere Daten) zu erheben und unverzüglich **132**

¹ Regierungspräsidium Darmstadt, Schreiben vom 14. Januar 2004, JurPC Web-Dokument 43/2003, Abs. 5

² so bei A. Dix, DuD 2003, 234

zu speichern, bei Bekanntwerden auch das Datum des Vertragsendes. Das LG Stuttgart³ hat die Verpflichtung eines Internet-Providers, den Strafverfolgungsbehörden Auskunft über die zu einer IP-Adresse zu einer bestimmten Uhrzeit gehörigen Bestandsdaten zu erteilen, nach § 113 TKG bejaht. § 113 bezieht sich auf nach § 111 zu erhebende Daten. Das LG Stuttgart verkennt dabei, daß sich § 111 TKG auf Rufnummern, nicht auf Nummern bezieht. IP-Adressen sind unstreitig Zeichenfolgen, die in Telekommunikationsnetzen Zwecken der Adressierung dienen, sind also Nummern im Sinne des § 3 Nr. 13 TKG. Allerdings werden sie nicht im öffentlichen *Telefondienst* verwendet, sind also keine Rufnummern im Sinne des § 3 Nr. 18 TKG. Daher kann § 111 TKG keine Rechtsgrundlage für die Speicherung der IP-Adresse sein.

3. Übertragenes Datenvolumen

a) Bewertung nach TDDSG und TKG

133 Soweit der Flatrate-Tarif nur ein begrenztes Übertragungsvolumen zuläßt, ist die Speicherung dieses Datums unstreitig für Abrechnungszwecke erforderlich.

134 Bei einer „echten“ Flatrate könnte man argumentieren, daß mit Hilfe dieses Datums der Anbieter die tatsächliche Erbringung seiner Leistung belegen kann, wenn der Nutzer geltend macht, daß zwar eine Verbindung zustande kam, Daten aber gar nicht oder nur sehr langsam übertragen wurden. Die Speicherung ist dafür aber weder erforderlich noch geeignet. Sie ist nicht erforderlich, weil der Anbieter Informationen über eventuelle Überlastungen auch systemweit erheben kann und dies nicht nutzerspezifisch tun muß. Sie ist auch nicht geeignet, weil ein niedriges Datenvolumen nicht bedeutet, daß der Kunde die vertraglich vereinbarte Bandbreite aus technischen Gründen nicht nutzen konnte. Wahrscheinlicher ist, daß er die Verbindung gar nicht ständig voll ausgelastet hat. Beweiswert käme insofern nur einem Datenvolumen zu, daß annähernd dem maximal möglichen entspricht.

III. Fazit

135 Aus diesen Betrachtungen ergibt sich, daß eine Speicherung von Nutzungsdaten stets nur mit Einwilligung des Nutzers zulässig ist.

136 Soweit die Speicherung zu bestimmten Zwecken rechtspolitisch als sinnvoll angesehen wird, ist eine klare gesetzliche Regelung erforderlich, um dem verfassungsmäßig gebotenen Grundsatz der Normenklarheit gerecht zu werden. Ein „Hineininterpretieren“ in bestehende Vorschriften wird den diesbezüglichen Anforderungen nicht gerecht.

³ LG Stuttgart, Beschluß vom 4. Januar 2005, 13 Qs 89/04, NJW 9/2005 614

§ 9 Schlußbemerkungen

- Die Betrachtungen des vorherigen Abschnitts haben gezeigt, daß nach gegenwärtiger Rechtslage bei Flatrates die Speicherung von Nutzungsdaten ohne Einwilligung des Nutzers nicht zulässig ist. **137**
- Gleichwohl bestehen bei Sicherheitsorganen erhebliche Begehrlichkeiten nach solchen Nutzungsdaten, insbesondere seit den terroristischen Anschlägen vom 11. September 2001. **138**
- Auch wenn es sich hierbei oftmals um Populismus handelt, sind solche Forderungen nicht vollständig von der Hand zu weisen. Allerdings muß hier angesichts der Tragweite der berührten Rechtsgüter mit Augenmaß agiert werden. Auch ernste terroristische Bedrohungen rechtfertigen nicht eine grenzenlose Beschränkung der Freiheitsrechte des Einzelnen, die Grundlage einer freiheitlichen rechtsstaatlichen Ordnung sind, unter der sich Demokratie erst entfalten kann. **139**
- Insbesondere bedürfen solche Eingriffe (wie schon dargelegt) einer klaren gesetzlichen Grundlage, machen also ein Tätigwerden des Gesetzgebers erforderlich und dürfen nicht durch die ausübende und rechtsprechende Gewalt in bestehende Gesetze hineininterpretiert werden. **140**
- Angesichts einer immer weiter zunehmenden Verbreitung von Informations- und Kommunikationstechnologien, die sich in Richtung einer allgegenwärtigen Datenverarbeitung (Ubiquitous Computing) entwickelt, gewinnt der Schutz des Einzelnen bei dieser Datenverarbeitung eine immer stärkere Bedeutung. **141**
- Ob die gegenwärtigen Instrumente ausreichen, um einen hinreichenden Schutz sicherzustellen, bleibt abzuwarten. **142**

