

Astrid Schalk
stud. jur. 7. Semester

**Seminar im Datenschutzrecht
SS 2001
Prof. Dr. Zeschwitz**

**Besonderer Datenschutz bei Telekommunikation und
Telediensten**

A. Einführung

Die aktuellen Statistiken über die Eingriffe in die Telekommunikation zeigen, daß die Bedeutung dieser Eingriffsmaßnahmen im Ermittlungsverfahren in den vergangenen Jahren weiter zugenommen hat. Wurden im Jahr 1995 noch 4.674 Überwachungsmaßnahmen registriert, stieg diese Zahl bis zum Jahr 1998 auf 9.802 und hat sich damit mehr als verdoppelt.¹ Betroffen waren sowohl Telefonanschlüsse, als auch Mobiltelefone. Eingriffe in die Telekommunikation haben folglich eine besondere Bedeutung im strafrechtlichen Ermittlungsverfahren. Um so wichtiger sind die gesetzlichen Regelungen, die diese Eingriffe ermöglichen beschränken und oder auch teilweise verbieten. Im Folgenden wird hierauf näher eingegangen.

B. Eingrenzung des Themas:

Dieses Referat beschränkt sich auf die geschäftsmäßige Erbringung von Telekommunikationsdiensten und die Abgrenzung zu den Telediensten im Inland. Intranetze werden unberücksichtigt gelassen. Auch werden die Probleme in Bezug auf das EU Ausland und Drittländer außer acht gelassen. Für Europa gilt sei neustem die AIP Richtlinie, die hier aus Platzgründen auch nicht näher dargestellt wird.² Auch das Telefonieren mittels eines Computers wird hier nicht näher erläutert.

C. Anwendbarkeit des deutschen Rechtes

Da es in diesem Referat unter anderem auch um Internet geht, soll kurz vorweggenommen werden, wann deutsches Recht überhaupt anwendbar ist. Das deutsche Datenschutzrecht³ kommt zur Anwendung wenn 1.) ein Unternehmen mit Sitz in Deutschland Daten im Ausland verarbeiten läßt oder ein Unternehmen mit Sitz im Ausland Daten über deutsche Terminals verarbeitet.

I. Telekommunikation nach dem TKG

1. Allgemeine Definitionen

Telekommunikation

Telekommunikation im Sinne von § 3 Nr. 16 TKG ist der technische Vorgang des Aussendens, Übermittels und Empfangen von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen⁴, die wiederum in § 3 Nr. 17 TKG als technische Einrichtungen oder Systeme beschrieben werden, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können. Telekommunikationsanlagen im Sinne dieses Gesetzes sind somit alle Rechner, die über ein ISDN-Karte oder ein Modem mit dem Telefonnetz verbunden sind.⁵ Hierzu gehören Mailboxen, Online-Dienste und auch Internet-Server. Aufgrund dieser Definition wird in der Literatur davon ausgegangen, daß auch Online-Provider teilweise in den Geltungsbereich des TKG, d.h. datenschutzrechtlich unter § 89 TKG fallen und es insoweit Überschneidungen in den persönlichen Anwendungsbereichen des TKG einerseits und des TDG andererseits gebe.⁶ Näher hierzu wird jeweils bei der Anwendbarkeit von TDSV, TKG, TDG und TDDSG eingegangen.

2. Spezielle Definitionen der TDSV

a) Beteiligte am Fernmeldeverkehr

Bei den Beteiligten unterscheidet man gem. § 2 Nr. 1 TDSV zwischen den Kunden und den Diensteanbietern von Telekommunikationsdienstleistungen. Kunden im Sinne von § 2 Nr. 1a

¹ Bär, MMR 2000, S. 472.

² vertiefend hierzu: Köhler, Recht des Internet, Rdnr. 396 f; Hoeren, Rechtsfragen des Internet, Rdnr. 369 f;

³ Hoeren, Rechtsfragen des Internet, Rdnr. 374.

⁴ Moritz/Winkler, NJW-CoR 1997, S.43, 44.

⁵ Schick, NJW-CoR 1998, S. 486, 487.

⁶ Löw, Datenschutz im Internet, S. 51.

TDSV können dabei sowohl natürliche Personen, als auch juristische Personen⁷ und Personengesellschaften gem. § 1 I TDSV sein. Die Personengesellschaften können dies aber nur insoweit, als sie Rechte erwerben oder Verbindlichkeiten eingehen können. § 2 Nr. 1 b TDSV umfaßt auch Mitbenutzer, also etwa Familienangehörige des Kunden, die in die Nutzung eines Anschlusses eingeschlossen werden.

Dienstleister sind solche Anbieter, die Telekommunikationsdienstleistungen mit Gewinnerzielungsabsicht anbieten.⁸

b) Besonderheiten im Internet

Gem. § 1 TDSV fallen unter die Dienstleister aber nur Access, Service und Presence Provider und somit fallen auch nur diese in den Anwendungsbereich der TDSV. Ebenfalls fallen auch nur diese unter das TKG.⁹ Die Content-Provider werden vom TDSV und TKG nicht umfaßt.¹⁰ Für sie gelten das TDG, das TDDSG sowie gegebenenfalls die allgemeinen Regeln des BDSG. Zudem kommt das TKG bei dem Betrieb der technischen Einrichtungen wie beispielsweise Server, Gateway (Schnittstelle zwischen 2 Netzen), Router (Gerät das Anfragen aus dem Computernetz weiterleitet) und Telekommunikationskabel zur Anwendung.¹¹

aa) Access Provider sind die sogenannten Zugangsprovider.¹² Über diese wählt man sich in das Internet ein und bekommt ein Zugang zu diesem. Z. B. T-Online, AOL, CompuServe usw. Wobei diese Anbieter meist schon wieder mehr anbieten als den reinen Internetzugang.

bb) Service- oder Presence Provider, sind Inhaltsvermittler, die im Internet fremde Inhalte zur Nutzung bereit halten oder technisch die Verteilung fremder Inhalte ermöglichen.¹³ Sie stellen für Nutzer Web Seiten bereit. An sie kann sich quasi jeder wenden, der eine eigene Webseite haben möchte. Diese steht dann jederzeit im Internet und ist grundsätzlich für jeden Internetnutzer abrufbar.

cc) Content Provider hingegen halten eigene oder fremde Inhalte zum Abruf bereit.¹⁴ Zum Beispiel Datenbanken. Sie können aber abgesehen von Informationen auch Waren, und Dienstleistungen anbieten. Beispiele hierfür wären Web.de, Gmx.de, Altavista.de, Amazon.de, Bol.de, Buecher.de usw.

3. Einwilligung

Die Verarbeitung und Nutzung nach vorstehenden Grundsätzen erhobenen Daten unterliegt gem. § 3 I S. 2 TDSV einem Verbot mit Erlaubnisvorbehalt. § 89 X TKG erhebt den Grundsatz aus § 3 II TDSV in Gesetzesrang.

Danach darf die Erbringung von Telekommunikationsdiensten nicht von der Angabe personenbezogener Daten abhängig gemacht werden, die hierfür nicht erforderlich sind.¹⁵ Dies gilt auch für die Entgeltfestlegung.¹⁶ Zusätzlich wird die Aufklärungspflicht für die datenschutzrechtliche Einwilligung abweichend von § 4 a BDSG dahin konkretisiert, daß in sachgerechter Weise über Inhalt und Reichweite der Einwilligung zu informieren ist, und die vorgesehenen Zwecke und Nutzungszeiten zu nennen sind. Die Einwilligung umfaßt keinesfalls Datenübermittlungen an unbekannte Dritte, etwa Adreßverkäufer im Ausland.¹⁷ Die Einwilligung soll in der Regel schriftlich erfolgen. Nach h. M. reicht es nicht aus, wenn dies in den AGB steht und lediglich durch Unterzeichnung des sonstigen Vertrages mit

⁷ Moritz/Winkler, NJW-CoR 1997, S.43, 44.

⁸ Büchner/Büchner, TKG, Anh. § 89 Rdnr. 3.

⁹ Determann, Kommunikationsfreiheit im Internet, S. 522.

¹⁰ Strömer, Online§Recht, S. 189.

¹¹ Determann, Kommunikationsfreiheit im Internet, S. 522.

¹² Löw, Datenschutz im Internet, S.37.

¹³ Determann, Kommunikationsfreiheit im Internet, S. 70.

¹⁴ Löw, Datenschutz im Internet, S.37.

¹⁵ Strömer, Online§Recht, S. 189.

¹⁶ Büchner, TKG, § 89, Rdnr. 53.

¹⁷ Koch, Internet-Recht, S.304.

unterzeichnet wird.¹⁸ Erstmals wird jedoch auch ausdrücklich die Erteilung der Einwilligung im elektronischen Verfahren erlaubt.¹⁹ § 4 TDSV regelt die Voraussetzungen für die Einwilligung im elektronischen Verfahren. Diese sind:

1. die Einwilligung darf nur durch eine eindeutige und bewußte Handlung des Nutzers erfolgen können.
2. die Einwilligung muß protokolliert werden
3. der Inhalt der Einwilligung muß jederzeit vom Beteiligten abgerufen werden können
4. es muß eine Rücknahmemöglichkeit für einen Zeitraum von mindestens einer Woche vorgesehen sein

4. Verbindungsdaten

§ 89 II Nr. 1 b TKG gestattet die Erhebung und Verarbeitung von Daten für das Herstellen und Aufrechterhalten einer Kommunikationsverbindung.²⁰ Diese Verbindungsdaten gehören aus der Sicht des Datenschutzes zu den sensibelsten Informationen, die bei der Erbringung von Telekommunikationsdiensten anfallen.²¹ Hierbei handelt es sich um die Rufnummer des Anrufers und des Angerufenen, Datum, Uhrzeit und Dauer der Verbindung sowie die Art der vom Kunden in Anspruch genommenen Telekommunikationsdienstleistungen.²² Sie dürfen gem. § 6 TDSV nur insoweit gespeichert und ausgewertet werden, wie es insbesondere für Abrechnungszwecke notwendig ist.²³ Über das Ende der Verbindung hinaus werden diese Daten zur Entgeltermittlung und –abrechnung benötigt. Strittig ist dabei, inwieweit die Zielnummer und die Uhrzeit der Verbindung erforderlich sind, wenn nicht ein Einzelverbindungs nachweis vereinbart ist. Die Notwendigkeit dieser Daten muß bejaht werden, da beide Daten nach praktisch allen gängigen Tarifmodellen maßgeblich für die Entgeltermittlung sind.

Problematisch ist, ob und welche Verbindungsdaten in welcher Form wie lange gespeichert bleiben dürfen. Da Verbindungsdaten Rückschlüsse über die näheren Umstände stattgefundener Telekommunikationsvorgänge erlauben, fallen sie zugleich unter das Fernmeldegeheimnis im Sinne von § 85 TKG.²⁴ § 6 TDSV schreibt vor, daß sobald die Daten nicht mehr zum Verbindungsaufbau, zur Entgeltermittlung bzw. Abrechnung gem. § 7 TDSV, zum Einzelverbindungs nachweis gem. § 8 oder zur Ermittlung von Störungen gem. § 9 TDSV benötigt werden, sind sie spätestens am Tag nach Beendigung der Verbindung unverzüglich zu löschen.

5. Besonderheiten fürs Internet

Rechnet ein Internet Provider pauschal ab, dann darf er das Nutzerverhalten nur insoweit in Logdateien speichern, wie er solche Informationen für das Erbringen seiner Leistungen benötigt.²⁵ Denkbar ist zum Beispiel, daß der Kunde bestimmte Newsgroups abonniert hat. Hier muß der Provider unter Umständen festhalten, um welche Diskussionsgruppen es sich handelt.²⁶ Logdateien sind Dateien, die die Vorgänge protokollieren welche ein Nutzer vornimmt. Zum Beispiel wann er sich ins Internet einloggt, und wann er sich wieder abmeldet.

6. Bestandsdaten

Die Verarbeitung von Daten ist gem. § 89 II Nr. 1 a) TKG für das Begründen, inhaltliche Ausgestalten und Ändern eines Vertragsverhältnisses zulässig. Dies betrifft die im

¹⁸ Löw, Datenschutz im Internet, S. 64.

¹⁹ Büchner/Büchner, TKG, § 89, Rdnr. 53.

²⁰ Büchner/Büchner, TKG, § 89, Rdnr. 25.

²¹ Büchner/Büchner, TKG, § 89, Rdnr. 25.

²² Büchner/Büchner, TKG, § 89, Rdnr. 25.

²³ Strömer, Onlin§Recht, S. 189.

²⁴ Büchner/Büchner, TKG, § 89, Rdnr. 25.

²⁵ Strömer, Onlin§Recht, S. 189.

²⁶ Strömer, Onlin§Recht, S. 189.

Zusammenhang mit den für die Erbringung von Telekommunikationsdiensten begründeten Vertragsbeziehungen zu erhebenden Bestandsdaten, also insbesondere Name und Anschrift des Kunden gegebenenfalls auch die Bankverbindung, Art des kontrahierten Dienstes und die dem Kunden zum Gebrauch überlassenen Einrichtungen.²⁷ Gem. § 5 I TDSV dürfen aber nur Informationen erhoben, verarbeitet und genutzt werden die zur inhaltlichen Ausgestaltung des Vertragsverhältnisses unbedingt erforderlich sind.²⁸ Es wird teilweise für möglich gehalten, daß auch Verbindungsdaten unter die Definition des § 89 II Nr. 1 TKG fallen. Dies widerspricht aber der eindeutigen Intention des Gesetzgebers und ist daher abzulehnen.²⁹ Dies wird durch die eindeutige Gegenüberstellung der hier geregelten Daten und der gem. § 89 II Nr. 1 b) TKG für das Herstellen und Aufrechterhalten einer Telekommunikationsverbindung erforderlichen Daten deutlich. Nach Beendigung des Vertragsverhältnisses muß der Diensteanbieter die Bestandsdaten gem. § 5 III TDSV mit Ablauf des auf die Beendigung folgenden Kalenderjahres löschen. § 35 III BDSG gilt entsprechend.

7. Auskunftspflicht

§ 89 VI TKG sieht die Verpflichtung der Diensteanbieter vor, die Bestandsdaten, auf entsprechendes Ersuchen an Strafverfolgungsbehörden, Verfassungsschutz, BND, MAD oder Zollkriminalamt zu übermitteln, wenn dies für die Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die nicht näher konkretisierte Erfüllung der gesetzlichen Aufgaben der genannten Behörden erforderlich ist.³⁰

Zum Beispiel wurden auf Basis dieser Vorschrift Auskunftsersuchen an Online-Service-Provider zur Identifizierung von Anbietern von Kinderpornographie im Internet gerichtet, die unter Pseudonymen agierten. Erfasst werden von dieser Vorschrift nur personenbezogene Daten, die nicht dem Fernmeldegeheimnis unterliegen, also insbesondere nicht Verbindungsdaten, die die näheren Umstände der Telekommunikation gemäß § 85 I TKG betreffen. Hier wird im Hinblick auf die Verfassungsmäßigkeit der Norm eine einschränkende Auslegung gefordert. Ansonsten würde ein Eingriff in das Recht auf informationelle Selbstbestimmung vorliegen. Zudem wird durch § 89 I TKG der Verhältnismäßigkeitsgrundsatz gefordert.³¹ Demnach dürfte ein speziell telekommunikationsorientiertes vereinfachtes Auskunftsverfahren dieser Art sich jedenfalls nur auf personenbezogene Daten mit spezifischem Telekommunikationsbezug erstrecken, nicht aber auf Bankverbindungen, Beruf, eventuelle Mahnungen usw.³² Problematisch ist zudem, ob § 89 VI überhaupt einen Auskunftsanspruch der Sicherheitsbehörden konstitutiv begründet, oder ob er nicht vielmehr nur die Auskunftserteilung, die aufgrund anderer Befugnisnormen verlangt wird, datenschutzrechtlich sanktioniert.³³ Für die Strafverfolgung gibt § 12 FAG i. V. m. § 99 I Nr. 2 TKG eine Befugnis zur Auskunftseinholung über zurückliegende Telekommunikationsvorgänge unter bestimmten Voraussetzungen.³⁴ Diese Norm bezieht sich aber nur auf die Überprüfung von Vorgängen, die vom Beschuldigten ausgehen, oder an ihn gerichtet sind. Andererseits erfaßt diese Norm die Verbindungsdaten, die dem Telekommunikationsgeheimnis unterliegen. Ferner gibt es noch die 98 a und b StPO, die bei bestimmten Straftaten von erhebliche Bedeutung einen maschinellen Abgleich personenbezogener Daten erlauben.³⁵

²⁷ Büchner, TKG, § 89, Rdnr. 24.

²⁸ Strömer, Online§Recht, S. 189.

²⁹ Büchner/Büchner TKG, § 89, Rdnr. 24.

³⁰ Büchner/Büchner TKG, § 89, Rdnr. 44.; LG Hamburg, MMR 8/1998, S. 419.

³¹ Büchner/Büchner TKG, § 89, Rdnr. 44.

³² Büchner/Büchner TKG, § 89, Rdnr. 45.

³³ Büchner/Büchner TKG, § 89, Rdnr. 44.

³⁴ Büchner/Büchner TKG, § 89, Rdnr. 44.

³⁵ Büchner, TKG, § 89, Rdnr. 44.

Wäre § 89 VI TKG nur für solche anderweitig normierte Herausgabefälle gedacht, dann wäre er überflüssig. Er geht daher in seinem Anwendungsbereich über diese Fälle hinaus. Im Falle strafrechtlicher Ermittlung ist aber entsprechend § 98 b StPO zumindest zu fordern, daß ein Auskunftsverlangen auch im Rahmen des § 89 VI TKG grundsätzlich nur durch den Richter und lediglich bei Gefahr im Verzug auch durch den Staatsanwalt erhoben werden darf. § 89 VI S. 2 TKG verbietet ausdrücklich eine Mitteilung an den Kunden über die erteilte Auskunft. Dadurch wird allerdings ein effektiver Rechtsschutz gegen eventuelle ungerechtfertigte Auskunftsersuchen ausgehebelt. Hier bieten allenfalls besondere Unterrichtungspflichten an Datenschutzinstitutionen, wie etwa gem. § 98 b IV S.2 StPO einen gewissen Schutz.³⁶ Grundsätzlich hat die Auskunftserteilung gem. § 89 VI TKG i. V. m. § 17 a ZSEG nur unter Kostenersatz zu erfolgen. Eine Ausnahme hiervon bildet § 90 I TKG. Hier werden auf Ersuchen der Behörde von der Regulierungsbehörde in einem automatisierten Verfahren Daten abgerufen. Der Aufwand hierfür wurde als gering eingestuft. Nach § 90 TKG sind Anbieter verpflichtet, Kundendateien zu führen, in die unverzüglich die Rufnummern und Rufnummernkontingente aufzunehmen sind, auch soweit diese nicht in öffentliche Verzeichnisse eingetragen sind. Soweit es zur Erfüllung der gesetzlichen Aufgaben erforderlich ist, darf die Regulierungsbehörde dies Daten auf Anfrage der Gerichte, der Ermittlungsbehörden und des Verfassungsschutzes gem. § 90 III TKG, abrufen. Der verpflichtete hat auf seine Kosten dafür zu sorgen, daß ein solcher Abruf von ihm unbemerkt erfolgen kann.³⁷

8. Inhalte

Unter Inhaltsdaten sind die jeweiligen konkreten Gesprächsinhalte zu verstehen.³⁸ Ein Zugriff auf Inhalte der Kommunikation ist nur bei einer Anordnung zur Überwachung des Fernmeldeverkehrs gem. § 100a StPO möglich. Es muß sich um eine der Überwachung zugängliche Form der Telekommunikation handeln. Zum zweiten muß der konkrete Verdacht einer der aufgeführten Katalogtaten vorliegen und zum Dritten der Adressat eines solchen Eingriffs zum Kreis der in § 100a S. 2 StPO ausdrücklich genannten Personen gehören.³⁹ Zu den Daten auf die gem. § 100a StPO zugegriffen werden kann gehören auch die technisch bedingten Positionsmeldungen nicht telefonierender Mobiltelefone.⁴⁰ Es muß dann gegebenenfalls auch der Standort eines Mobiltelefones den Ermittlungsbehörden mitgeteilt werden. Dies ist technisch möglich, weil ein empfangsbereites Handy zur ständigen Erreichbarkeit im Fall einer Verbindung seine Position der nächstliegenden Sendestation ständig mitteilt. Ausgeschlossen bleiben Abhörmaßnahmen von Bildschirmen, da es sich zwar um Ausnutzung des technischen Phänomens der Abstrahlung, aber nicht um einen Vorgang der Telekommunikation handelt.⁴¹ Umstritten ist der Zugriff auf Mails. Sie werden im 1. Schritt vom Rechner des Absenders auf den Mailserver des Internetanbieters, bei dem der Adressat ein Postfach hat übertragen. In einem zweiten Schritt werden die Daten solange bei dem (Empfänger) Mailserver zwischengespeichert, bis sie abgerufen werden. Ein Zugriff auf die Mails in Phase 1 und Phase 3 ist den Ermittlungsbehörden nur aufgrund des § 100a StPO gestattet. Phase 2 ist umstritten. Die Befürworter, daß auch hier nur über § 100a StPO ein Eingriff zulässig sein soll, begründen dies damit, daß es sich um einen einheitlichen Vorgang handle, der nicht getrennt werden dürfe. Die Gegner und der BGH wollen hier § 94 StPO anwenden. Phase 2 sei keine Telekommunikation mehr. Die Zwischenspeicherung auf einer Festplatte sei ähnlich wie ein Text auf einem Anrufbeantworter, der auch nicht unter die

³⁶ Bühren/Büchner, TKG, § 89, Rdnr. 44.

³⁷ Schick, NJW-CoR 1998, S. 486, 487; LG Hamburg, MMR 1998 S. 419.

³⁸ Bär, MMR 2000, S. 472.

³⁹ Bär, MMR 2000, S. 472.

⁴⁰ Bär, MMR 2000, S. 472.

⁴¹ Bär, MMR 2000, S. 472, 473.

Telekommunikation fällt. Aus Sicht der Praxis würden zudem die Möglichkeiten zur Kontrolle von Mails auf ein für die Strafverfolgung nicht akzeptables Minimum reduziert.⁴² Zur Mißbrauchsbekämpfung im Sinne von § 89 II Nr. 1 e) TKG erlaubt § 89 III TKG keine Erhebung, Verarbeitung oder Nutzung von Nachrichteninhalten mehr, sondern vielmehr nur noch diejenige von Steuersignalen, und dies auch nur, wenn dies im Einzelfall für Mißbrauchsbekämpfungsmaßnahmen unerlässlich ist.⁴³ Dies bedeutet, daß Aufzeichnen von Nachrichteninhalten, also das Hineinhören in Gespräche, zur Mißbrauchsbekämpfung nicht mehr erlaubt ist. Die Eingriffsmöglichkeiten sind auf das maschinelle Erfassen von Steuersignalen ohne Kenntnisnahme vom gesprochenen Wort herabgesetzt. Allerdings verspricht das hiermit erlaubte „Abtasten“ des Sprachkanals im ISDN-Netz durchaus Erfolg bei der Aufdeckung und Unterbindung unberechtigter Manipulationen etwa durch Computerhacker.⁴⁴ § 89 II TKG schreibt ausdrücklich die Unterrichtung der Regulierungsbehörde vor, die einheitlich an die Stelle des BMPT und der Datenschutzkontrollbehörde tritt, denen gegenüber nach der TDSV entsprechende Unterrichtungspflichten bestehen. Der von der Überwachungsmaßnahme Betroffene muß hiervon benachrichtigt werden, sobald dies ohne Gefährdung des Zwecks der Überwachungsmaßnahme möglich ist.

Die Aufzeichnung und Zugänglichmachung von Nachrichteninhalten gegenüber Dritten bzw. ihre sonstige Verarbeitung erlaubt § 89 IV TKG nur, soweit sie Gegenstand eines Telekommunikationsdienstes oder aus verarbeitungstechnischen Gründen Bestandteil desselben ist und, wie sich aus § 89 III Nr. 4 TKG ergibt, insoweit notwendig ist.⁴⁵ Hierbei handelt es sich etwa um „Mailbox-Dienste“ der Mobilfunkanbieter oder die von der Deutschen Telekom im Festnetz angebotenen Voice-Mail-Funktionen, bei denen individuelle Nachrichten von Teilnehmer zu Teilnehmer vermittelt werden. Der hiermit verbundene Eingriff in das Telekommunikationsgeheimnis (§ 85 TKG) ist durch Einwilligung der am Kommunikationsvorgang beteiligten gedeckt. Auf Seiten des Angerufenen ist durch Aktivierung des Voice-Mail-Services eine Einwilligung erteilt und auf Seiten des Anrufers durch Inanspruchnahme des Dienstes.⁴⁶

9. Aufschalten auf bestehende Verbindungen

Zur Durchführung von Umschaltungen, zur Störungserkennung und –Beseitigung im Netz ist gem. § 89 V TKG das Aufschalten auf bestehende Verbindungen erlaubt, soweit dies betrieblich erforderlich ist.⁴⁷ Die Erforderlichkeit ist eng auszulegen.⁴⁸ Dies ergibt sich aus § 89 III S. 4 TKG, wo die Erhebung, Verarbeitung und Nutzung anderer Nachrichteninhalte (als Steuersignale) als unzulässig bezeichnet wird, sofern sie nicht im Einzelfall für Maßnahmen nach V unerlässlich ist. Die Aufschaltung muß sich im Rahmen des § 85 II TKG bewegen wonach es den Diensteanbietern untersagt ist, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste erforderliche Maß hinaus Kenntnisse über den Inhalt oder die näheren Umstände der Telekommunikation zu verschaffen. Aus diesem Grund ist in § 89 V S. 2 TKG auch vorgeschrieben, daß das Aufschalten den betroffenen Gesprächsteilnehmern durch ein akustisches Signal angezeigt und ausdrücklich mitgeteilt werden muß.⁴⁹ Diese Formulierung bedeutet wörtlich genommen, daß über die Anzeige des Aufschaltens durch ein akustisches Signal hinaus eine ausdrückliche Mitteilung an den Teilnehmer erfolgen muß. Gemeint ist aber wohl unter Berücksichtigung des Gesetzeszweckes, daß das akustische Signal in dem Sinne unmißverständlich sein muß,

⁴² Bär, MMR 2000, S. 473, 475.

⁴³ Büchner/Büchner, TKG, § 89, Rdnr. 41.

⁴⁴ Büchner/Büchner, TKG, § 89, Rdnr. 41.

⁴⁵ Büchner/Büchner, TKG, § 89, Rdnr. 42.

⁴⁶ Büchner/Büchner, TKG, § 89, Rdnr. 42.

⁴⁷ Büchner/Büchner, TKG, § 89, Rdnr. 43.

⁴⁸ Büchner/Büchner, TKG, § 89, Rdnr. 43.

⁴⁹ Büchner/Büchner, TKG, § 89, Rdnr. 42.

daß es vom Teilnehmer als entsprechende Mitteilung verstanden wird. Ein leicht überhörbarer Pfeif- oder Piepton wird somit den gesetzlichen Anforderungen nicht gerecht.⁵⁰ Ein Mithören im Rahmen des § 89 V TKG ohne entsprechende ausdrückliche Mitteilung dürfte den Straftatbestand des § 206 StGB Verletzung des Fernmeldegeheimnisses erfüllen.⁵¹

10. Entgeltdaten

§ 89 II Nr. 1 c) TKG erlaubt die Verwendung von Daten für die Ermittlung und den Nachweis der Entgelte einschließlich der auf andere Netzbetreiber und Anbieter entfallenden Leistungsanteile: dabei ist dem Nutzer hinsichtlich des Entgeltnachweises eine Wahlmöglichkeit in bezug auf die Dauer der Speicherung und den Umfang der Speicherung einzuräumen.⁵² Zur Entgeltermittlung werden zunächst die Verbindungsdaten benötigt. Unter der Geltung der TDSV alter Fassung bzw. der UDSV war ein wesentlicher Kritikpunkt, daß die Zielnummern während des gesamten für die Entgeltermittlung verfügbaren Zeitraums unverkürzt gespeichert werden konnten.⁵³ § 6 III TDSV hat insofern eine Verbesserung gebracht, als sie die Speicherung der Zielrufnummern generell nur unter Verkürzung um die letzten drei Ziffern erlaubt. Damit wird dem informationellen Selbstbestimmungsrecht des Angerufenen Rechnung getragen. Die so gespeicherten Verbindungsdaten sind sodann den rechnungsrelevanten Bestandsdaten des Kunden zuzuordnen.⁵⁴ Schließlich sind noch sonstige entgeltrelevante Umstände wie etwa Vorauszahlungen, Zahlungsrückstände, Anschlußsperrern, Stundungsgewährungen Ratenzahlungsvereinbarungen etc. zu berücksichtigen. Die in § 89 II Nr.1 c) TKG nun gesetzlich vorgeschriebene Wahlmöglichkeit des Kunden muß dahin gehen, entweder nach Rechnungsversendung eine Löschung der Verbindungsdaten zu verlangen, damit aber in Kauf zu nehmen, daß diese bei Meinungsverschiedenheiten über die Rechnungshöhe nicht mehr zur Verfügung stehen, oder eine längerfristige Speicherung zu verlangen um Rechnungsansätze notfalls verifizieren zu können. Indem das Gesetz von Wahlmöglichkeiten hinsichtlich Speicherdauer und Speicherumfang spricht, zielt der Gesetzgeber allerdings abweichend von § 6 IV TDSV darauf ab, daß die TDSV neuer Fassung nicht eine Regelhandlung vorschreibt und der Kunde für eine Ausnahme hiervon votieren kann, sondern er vielmehr zwischen mehreren Optionen wählen kann, wie dies in § 89 VIII TKG für die Eintragung in öffentliche Verzeichnisse vorgesehen ist. Besonders sensibel ist die Möglichkeit, Verbindungsdaten nach Zielrufnummern auszuwerten. Sie muß auf das im Rahmen der Entgeltbemessung notwendige Minimum beschränkt bleiben.⁵⁵

11. Überwachungsmaßnahmen:

Gemäß § 88 I TKG haben die Betreiber von Telekommunikationsanlagen die technischen Einrichtungen zur Umsetzung von gesetzlich vorgesehenen Maßnahmen zur Überwachung der Telekommunikation auf eigene Kosten zu gestalten und vorzuhalten.⁵⁶ Die gesetzlich vorgesehenen Maßnahmen zur Überwachung der Telekommunikation ergeben sich dabei vor allem aus dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, den §§ 100a, 100b StPO und dem § 39 des Außenwirtschaftsgesetzes (AWG). Nach § 88 IV TKG ist jeder Betreiber einer Telekommunikationsanlage, der anderen den Netzgang zu seiner Telekommunikationsanlage geschäftsmäßig überläßt, verpflichtet den gesetzlich zur Überwachung der Telekommunikation berechtigten Stellen auf deren Aufforderung einen Netzzugang für die Übertragung der im Rahmen einer Überwachungsmaßnahme anfallenden Informationen unverzüglich und vorrangig bereitzustellen.⁵⁷

⁵⁰ Büchner/Büchner, TKG, § 89, Rdnr. 42.

⁵¹ Büchner/Büchner, TKG, § 89, Rdnr. 42.

⁵² Büchner/Büchner, TKG, § 89, Rdnr. 26.

⁵³ Büchner/Büchner, TKG, § 89, Rdnr. 26.

⁵⁴ Büchner/Büchner, TKG, § 89, Rdnr. 26.

⁵⁵ Büchner/Büchner, TKG, § 89, Rdnr. 26.

⁵⁶ Schick, NJW-CoR 1998, S. 486, 487; Holznapel, Bysikiewicz, Enaux, Nienhaus, S. 196.

⁵⁷ Schick, NJW-CoR 1998, S. 486, 487.

12. Technische Schutzmaßnahmen

Die Betreiber von Telekommunikationsmaßnahmen, und somit auch Internet Provider, sofern sie wie oben bereits erläutert unter TKG fallen haben gem. § 87 TKG technische Schutzmaßnahmen einzurichten, durch die die Daten vor unberechtigten Zugriffen geschützt werden sollen. Je nach Dienst wie z. B. beim Internet telefonieren, oder aber auch bei E-Mails hat der Provider keinen Einfluß darauf, auf welchem Wege die Daten übermittelt werden, und auf welchen Rechnern diese zwischengespeichert werden. Es ist sogar durchaus denkbar, daß die Zwischenspeicherungen auf Rechnern vorgenommen werden, die sich außerhalb des Geltungsbereiches des TKG befinden. Auf diese Rechner hat der inländische Provider keinen Einfluß. Für dritte dürfte es demnach relativ einfach sein, auf die zwischengespeicherten Daten unbefugt zuzugreifen.⁵⁸ Allerdings ist der geforderte Schutzaufwand auch davon abhängig, in welchem Umfang der Benutzer davon ausgehen kann, daß sein Fernmeldegeheimnis gewahrt und Dritten die Möglichkeit einer Verletzung dieses Rechts erschwert wird. Weiß der Benutzer, daß technisch ein Abhören mit vergleichsweise einfachen Mitteln möglich ist, so kann er nicht darauf vertrauen, daß jede nur erdenkliche Maßnahme getroffen wird, um den Schutzstandard zu verbessern.⁵⁹ Gem. § 87 I TKG dürfte es derzeit ausreichen, wenn der Service Provider dafür Sorge trifft, daß zumindest auf seine Rechner nicht unbefugt zugegriffen werden kann.⁶⁰ Der Internetnutzer muß damit rechnen, daß Dritte an seine Daten gelangen, und daß er im Zweifel nicht davon erfährt.

13. Sanktionen

Das TKG enthält keine datenschutzrechtliche Sanktionsnormen. Allerdings enthält § 17 TDSV in der neusten Fassung einen Katalog über Ordnungswidrigkeiten.

Während sich die Strafvorschriften des § 44 BDSG vorwiegend auf Datenverarbeitungsvorgänge beziehen, wird die Verletzung wichtiger Verfahrensregelungen gem. § 43 II BDSG als Ordnungswidrigkeit mit Geldbußen bis zu 50.000 DM geahndet. Z.B wäre die Unterlassung der Bestellung eines Datenschutzbeauftragten entgegen § 36 I BDSG eine Ordnungswidrigkeit gem. § 44. Gem. § 30 OwiG kann eine Geldbuße auch gegen juristische Personen und Handelsgesellschaften festgesetzt werden, also auch gegen die speichernde Stelle selbst. Dabei besteht die Möglichkeit der Verdoppelung der Geldbuße gem. § 30 II OwiG.

Andere Beispiele finden sich in § 17 TDSV.

14. Datenschutzkontrolle

Für den Bereich des Schutzes personenbezogener Daten im Rahmen der geschäftsmäßigen Erbringung von Telekommunikationsdiensten weist § 91 IV TKG die Zuständigkeit, abweichend von § 38 BDSG, nicht den Aufsichtsbehörden der Länder, sondern dem Bundesbeauftragten für den Datenschutz zu.⁶¹ Dessen Kontrollbefugnisse beschränken sich auf die Datenverarbeitung im Zusammenhang mit der Erbringung von Telekommunikationsdiensten. Für sonstige Datenverarbeitungsmaßnahmen, also etwa die Verarbeitung von Mitarbeiterdaten bleiben die Aufsichtsbehörden der Länder gem. § 38 BDSG zuständig.⁶² Im Falle der Feststellung von Verstößen gegen Datenschutzvorschriften beanstandet der Bundesbeauftragte für den Datenschutz diese nach § 25 BDSG gegenüber dem zuständigen Bundesministerium, d.h. in Bezug auf privatwirtschaftlich organisierte Telekommunikationsunternehmen gegenüber dem Bundesministerium für Wirtschaft, das insoweit an die Stelle des aufgelösten Bundesministeriums für Post und Telekommunikation getreten ist. Hoheitliche Maßnahmen im Falle von Datenschutzverletzungen fallen dagegen in die Zuständigkeit der Regulierungsbehörde. Der Bundesbeauftragte für den Datenschutz wird

⁵⁸ Schick, NJW-CoR 1998, S. 486, 488.

⁵⁹ Schick, NJW-CoR 1998, S. 486, 488.

⁶⁰ Schick, NJW-CoR 1998, S. 486, 488.

⁶¹ Büchner/Büchner, TKG, § 89, Rdnr. 57.

⁶² Büchner/Büchner, TKG, § 89, Rdnr. 57.

insbesondere auf Beschwerden von Kunden von Telekommunikationsunternehmen tätig oder wenn er auf andere Weise Anhaltspunkte für Verstöße erhält.⁶³ Gem. § 91 IV TKG in Verbindung mit § 24 I 1 BDSG ist aber auch eine rein Präventive Kontrolle möglich, über die der Bundesbeauftragte für den Datenschutz im eigenen pflichtgemäßen Ermessen zu entscheiden hat.⁶⁴

II. Teledienste

1. TDG Anwendbarkeit

Im Geltungsbereich des TDG (Teledienstegesetz) sind, wie es in § 2 I TDG positiv formuliert wird all diejenigen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt.⁶⁵ Es wird hieraus der Schluß gezogen, daß kein Teledienst im Sinne des TDG vorliegt, wenn eines der folgenden Merkmale fehlt: 1.) Die Übermittlung 2.) Die Bestimmung zur individuellen Nutzung 3.) Das Angebot.⁶⁶ Die Übermittlung von Daten wird hier im technischen Sinne und nicht im rechtlichen verstanden. Eine Übermittlung von Daten kann daher auch im Intranet stattfinden. Das TDG und das TDDSG sind gem. § 3 Nr. 2 TDG und § 2 Nr. 2 TDDSG grundsätzlich auch dann anwendbar, wenn es sich bei dem Nutzer um eine Juristische Person handelt. Das TDG ist gem. § 2 IV Nr. 1 TDG nicht anwendbar, wenn das TKG anwendbar ist.⁶⁷ Gem. § 2 IV Nr. 2 TDG ist das TDG auch nicht anwendbar, wenn es sich um Rundfunk im Sinne des § 2 Rundfunkstaatsvertrag handelt, oder es gem. § 2 Mediendienste-Staatsvertrag hierunter fällt. § 2 II Nr. 3 TDG bestimmt allerdings ausdrücklich, daß Angebote zur Nutzung des Internets oder weiterer Netze als Teledienst im Sinne TDG angesehen werden sollen. Dem Wortlaut nach könnte man auch die Zugangsvermittlung zum Internet (wird von Access Providern übernommen) als ein Angebot zur Nutzung des Internet ansehen und damit als Teledienst.⁶⁸ Allerdings stellt die Gewährung von Zugang zum Internet, also die Tätigkeit der Zugangsvermittler (Access Provider) und Inhaltsvermittler (Service Provider) eine Telekommunikationsdienstleistung im Sinne von § 3 Nr. 18 TKG dar, auf die das TDG nach § 2 IV Nr. 1 TDG gerade keine Anwendung finden soll.⁶⁹ Hinweise darauf, daß der Bundesgesetzgeber im TDG das früher erlassene TKG abändern wollte, liegen nicht vor.⁷⁰ Die Gesetzesbegründung benennt auch die Zugangsvermittlung gerade nicht als Beispiel eines Angebotes zur Nutzung des Internet im Sinne von § 2 II Nr. 3 TDG.⁷¹ Es ist vielmehr von Angeboten zur Nutzung der neuen Dienste (Navigationshilfen), nicht des gesamten Netzes die Rede. Vermittlungsdienste innerhalb des Netzes, sogenannte Content Provider, zum Beispiel Suchmaschinen, sind deshalb Teledienste und fallen unter das TDG. Access Provider fallen speziell im Rahmen ihre Tätigkeit der Zugangsvermittlung nur unter das TKG.⁷² Sie können aber in Bezug auf andere Tätigkeiten auch unter das TDG fallen. Es ist immer streng nach den jeweiligen Diensten und Tätigkeiten zu trennen.⁷³

2. Regelungsgehalt des TDDSG

Das TDDSG regelt gem. § 1 I TDDSG den Schutz personenbezogener Daten bei Telediensten im Sinne des Teledienstegesetzes. Nicht erfaßt werden daher Angaben über juristische

⁶³ Büchner/Büchner TKG, § 89, Rdnr. 57.

⁶⁴ Büchner/Büchner, TKG, § 89, Rdnr. 57.

⁶⁵ Löw, Datenschutz im Internet, S.18 ; Determann, Kommunikationsfreiheit im Internet, S. 521.

⁶⁶ Löw, Datenschutz im Internet, S.18 ; Determann, Kommunikationsfreiheit im Internet, S. 521.

⁶⁷ Löw, Datenschutz im Internet, S. 50.

⁶⁸ Determann, Kommunikationsfreiheit im Internet, S. 522.

⁶⁹ Determann, Kommunikationsfreiheit im Internet, S. 522.

⁷⁰ vgl. auch die Geganansich, Löw, Datenschutz im Internet, S. 36, 51.

⁷¹ Determann, Kommunikationsfreiheit im Internet, S. 522.

⁷² Determann, Kommunikationsfreiheit im Internet, S. 522.

⁷³ Engel-Flehsig/Maennel/Tettenborn, NJW 1997, S. 2981, 2986; Tinnefeld/Ehmann, Einführung in das Datenschutzrecht, S. 148.

Personen und Personenmehrheiten oder Personenvereinigungen, insoweit sich das Gesetz auf personenbezogene Daten im Sinne des § 3 I BDSG bezieht.⁷⁴

§ 3 I TDDSG regelt grundsätzlich inwieweit personenbezogene Daten vom Anbieter zur Durchführung von Telediensten verarbeitet werden dürfen. Sobald personenbezogene Daten aus anderen Gründen verarbeitet werden richtet sich die Zulässigkeit der Datenverarbeitung nach den allgemeinen Vorschriften des BDSG.⁷⁵

a) Prinzipien des TDDSG

aa) Verbotsprinzip

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist gem. § 3 II TDDSG grundsätzlich untersagt, sofern nicht das TDDSG oder das BDSG dies ausnahmsweise erlauben.⁷⁶

bb) Prinzip der Datenvermeidung

Hierbei gilt der Grundsatz, daß wenn schon personenbezogene Daten erhoben werden müssen, deren Erhebung, Verarbeitung und Nutzung gem. § 3 IV TDDSG möglichst gering gehalten werden soll.⁷⁷ Gem. § 4 I TDDSG ist dem User die Inanspruchnahme des Internet und die Bezahlung beim E-Commerce anonym oder unter einem Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist.

cc) Prinzip des selbst bestimmten Nutzers

Der Nutzer muß umfassend über Art, Umfang, Ort und Zwecke der Erhebung, Verarbeitung, und Nutzung personenbezogener Daten unterrichtet werden, vgl. § 3 V S. 1 TDDSG.⁷⁸ Der Inhalt der Unterrichtung muß gem. § 7 TDDSG für den Nutzer jederzeit kostenlos abrufbar sein. Eine erfolgte Unterrichtung bzw. ein Verzicht des Nutzers sind zu protokollieren, vgl. § V S. 5 TDDSG.⁷⁹

dd) Einwilligungserfordernis

Die Erhebung und Verarbeitung ist folglich nur zulässig, soweit sie gesetzlich gestattet ist oder der Betroffene gem. § 3 VI TDDSG schriftlich (gem. § 4a BDSG) einwilligt. Eine konkludente Einwilligung die in Form einer Akzeptierung von AGB`s abgegeben wird ist grundsätzlich nicht zulässig.⁸⁰ Es muß ausdrücklich auf die Einwilligung hingewiesen werden. Die Dienste dürfen auch hier wie beim TKG nicht von der Einwilligung abhängig gemacht werden. Es gilt der Grundsatz der Zweckbindung. Der Betroffene ist über Art, Umfang, Ort und Zweck der Erhebung und Nutzung seiner Daten vor deren Erhebung zu informieren. Auch hat der Nutzer das Recht, die zu seiner Person gespeicherten Daten unentgeltlich einzusehen.⁸¹ Die Voraussetzungen für eine wirksame elektronische Einwilligung sind in § 3 VII TDDSG ausführlich geregelt. Die in den ersten drei Punkte enthaltene erforderliche Zurechenbarkeit und Verlässlichkeit ist auf jeden Fall gewahrt, wenn der Einwilligende sich einer digitalen Signatur im Sinne des Signaturgesetzes bedient.⁸²

ee) Verbot von personenbezogenen Nutzungsprofilen und Trennungsgebot

Die Zulässigkeit von Nutzerprofilen ist in § 4 IV TDDSG geregelt. Hiernach ist die Erstellung von Nutzerprofilen nur unter Verwendung von Pseudonymen zulässig⁸³ Immer dann, wenn derartige Daten auf die Träger des Pseudonyms zurückgeführt werden können oder mit

⁷⁴ Engel-Flehsig/Maennel/Tettenborn, NJW 1997, S. 2981, 2986.

⁷⁵ Löw, Datenschutz im Internet, S. 58.

⁷⁶ Köhler/Arndt, Recht des Internet, Rdnr. 388; Engel-Flehsig/Maennel/Tettenborn, NJW 1997, S. 2981, 2986.

⁷⁷ Köhler/Arndt, Recht des Internet, Rdnr. 388.

⁷⁸ Löw, Datenschutz im Internet, S. 58.

⁷⁹ Löw, Datenschutz im Internet, S. 58.

⁸⁰ Löw, Datenschutz im Internet, S.64.

⁸¹ Hoeren, Rechtsfragen des Internet, Rdnr. 381.

⁸² Eichborn, Internet-Recht, S. 113.

⁸³ Köhler/Arndt, Recht des Internet, Rdnr. 395.

solchen Daten zusammen geführt werden können, führt dies zur Unzulässigkeit eines Nutzerprofils.⁸⁴

Technisch ist es den Anbietern leicht möglich ein solches Nutzerprofil zu erstellen. Greift man auf die Seite eines Internetanbieters zu, z. B. bei Amazon.de, dann braucht dieser nur ein Cookie zu setzen. Cookies sind Internet Softwareprogramme, die auf die Festplatten der Benutzer PC`s übertragen werden. Jedesmal wenn man wieder auf die Seite zugreift kann dieser Anbieter den PC über das Cookie identifizieren. Gibt man jetzt einmal bei Amazon seine Adresse und Bankverbindung ein, dann kann der Anbieter diese dem Cookie zuordnen. So weiß der Anbieter dann immer ganz genau, wann und wie lange Frau Müller sich auf der Seite aufhält, welche Angebote sie studiert und was sie kauft. Genau dies ist unzulässig.

b) Bestandsdaten § 5 TDDSG

Bestandsdaten sind solche Daten, die zur Begründung, inhaltlichen Ausgestaltung oder Änderung eines Vertragsverhältnisses über die Nutzung von Telediensten erforderlich sind.⁸⁵ Diese dürfen erhoben, verarbeitet und genutzt werden, sofern dies erforderlich ist. Eine darüber hinausgehende Nutzung gem. § 3 VII TDDSG, beispielsweise für Werbung, Marktforschung bei der Gestaltung des Teledienstes, ist nur nach ausdrücklicher Einwilligung des Betroffenen gestattet.⁸⁶

c) Nutzungs- und Abrechnungsdaten gem. § 6 TDSG

Nutzungsdaten, also Personenbezogene Daten, die nicht für die Abrechnung erforderlich sind müssen gem. § 6 I Nr. 1 TDDSG unmittelbar nach Ende der Nutzung gelöscht werden.⁸⁷

Die Abrechnungsdaten dürfen auch nicht länger gespeichert werden, als es für die Abrechnung erforderlich ist. Sie sind grundsätzlich nach Erfüllung der Forderung zu löschen.⁸⁸ Die Weitergabe der Daten an Dritte ist prinzipiell ausgeschlossen.

3. Datenschutzrechtliche Kontrolle

Die Einhaltung der Datenschutzvorschriften bei Telediensteanbietern überwacht gem. § 8 I TDDSG, die nach § 38 BDSG, für nicht öffentliche verarbeitende Stellen zuständige Landes Aufsichtsbehörde,. Es sind auch anlaßunabhängige Kontrollen zulässig.⁸⁹

III. Anwendungsbereich des Bundesdatenschutzgesetzes

Das Bundesdatenschutzgesetz tritt subsidiär hinter den speziellen Regelungen der TDSV, des TKG, des TDG und des TDDSG zurück und kommt gem. § 1 III BDSG immer dann zur Anwendung, wenn die speziellen Rechtsvorschriften wie TKG, TDSV, TDG, TDDSG Regelungslücken enthalten.⁹⁰

Zum Beispiel ist die Verwendung von Daten nichtnutzender Dritter im Online-Bereich von den neuen Regelwerken nicht umfaßt.⁹¹ Hier kommt das BDSG zur Anwendung.⁹² Für Kommunen gilt insoweit das Landesdatenschutzgesetz, für die Privatwirtschaft ebenfalls das BDSG.

Das BDSG gilt aber nur für Daten natürlicher Personen.⁹³ Auch kommt das Gesetz gem. § 1 II Nr.3 nicht zur Anwendung, soweit das Internet für ausschließlich private Zwecke genutzt wird.⁹⁴ Dies zeigt wie wichtig die speziellen Vorschriften des TKG, TDSV, TDG und TDDSG sind.

⁸⁴ Köhler/Arndt, Recht des Internet, Rdnr. 395.

⁸⁵ Köhler/Arndt, Recht des Internet, Rdnr. 390.

⁸⁶ Köhler/Arndt, Recht des Internet, Rdnr. 390.

⁸⁷ Löw, Datenschutz im Internet, S. 71; Köhler/Arndt, Recht des Internet, Rdnr. 390.

⁸⁸ Engel-Flehsig/Maennel/Tettenborn, NJW 1997, S. 2981, 2987.

⁸⁹ Löw, Datenschutz im Internet, S. 74.

⁹⁰ Moritz/Winkler, NJW 1997, S 43.

⁹¹ Hoeren, Rechtsfragen des Internet, Rdnr. 383; Engel-Flehsig/Maennel/Tettenborn, NJW 1997, S. 2981, 2985.

⁹² Köhler/Arndt, Recht des Internet, Rdnr. 393.

⁹³ Köhler/Arndt, Recht des Internet, Rdnr. 392.

⁹⁴ Hoeren, Rechtsfragen des Internet, Rdnr. 376; Köhler/Arndt, Recht des Internet, Rdnr. 392.

D. Beispiel⁹⁵

Die Vertraulichkeit des Datentransfers im Internet wird sowohl durch die an den Übermittlungsvorgängen Beteiligten, als auch durch Dritte bedroht. Im Rahmen des E-Mail-Verkehr sowie bei Nutzung der meisten WWW-Anwendungen werden Daten unverschlüsselt transportiert und zwischengespeichert. Zwar werden die zwischengespeicherten Daten auch wieder gelöscht. Löschen bedeutet aber für die meisten Rechnersysteme nur, daß ein Speicherplatz zum Überschreiben freigegeben wird. Wann die freigegebenen Daten tatsächlich überschrieben werden, hängt davon ab, wann der Speicherplatz benötigt wird. In der Zwischenzeit bleiben die Daten für Interessenten mit Informatikkenntnissen zugänglich. Im Rahmen der Nutzung von WWW-Angeboten sind zwar die Inhalte nicht vertraulich, wohl aber die Verbindungsdaten, die wie bei herkömmlichen Telefonaten anfallen. Durch systematisches Sammeln dieser Daten können die Inhalts- und Zugangsvermittler umfangreiche Statistiken, aber auch individuelle Persönlichkeitsbilder für Werbeagenturen erstellen. So werden über das Internet Softwareprogramme, sogenannte „Cookies“, auf die Festplatten der Benutzer-PCs übertragen, die automatisch Daten über Nutzergewohnheiten speichern. Diese Daten kann der Versender des Cookies bei Bedarf von der Festplatte des Benutzers abrufen. Auch Geheimdienste interessieren sich für die Internet-Kommunikation. Es wird berichtet, daß auf diesem Wege auch systematisch Wirtschaftsspionage zu Lasten europäischer Unternehmen und zugunsten von US-Unternehmen betrieben wird. Dies erscheint insbesondere deshalb problematisch, weil auch Großbritannien am Echelon System beteiligt ist und dadurch möglicherweise gemeinschaftrechtliche Pflichten verletzt. Auch der deutsche Bundesnachrichtendienst überwacht die Kommunikation im Internet. Die Bewältigung der Datenschutzprobleme im Internet durch nationale Gesetze ist angesichts der internationalen dezentralen Netzstruktur nur eingeschränkt möglich. Strenge Datenschutzgesetze in Deutschland veranlassen international agierende Unternehmen, ihre Rechner im Ausland aufzustellen. Auch Internet-Kommunikation zwischen Deutschen wird deshalb zum Teil von Rechnern in den USA abgewickelt, die an weit weniger strikte Regeln gebunden sind..

E. Fazit

Hier wird deutlich, daß diese noch relativ jungen Regeln der TKG, des TDSV und der TDG sowie des TDDSG noch nicht perfekt aufeinander abgestimmt sind. In der Literatur gibt es doch noch Meinungsverschiedenheiten darüber, wie zum Beispiel die einzelnen Internet Provider zu behandeln sind. An dieser Stelle kann nur gehofft werden, daß hier bald eine eindeutige Klärung stattfindet.

Andererseits sind gerade die deutschen Regeln schon sehr weitreichend. Man mag sich die Frage stellen, wie viel Sinn das macht, wenn die Unternehmen dann in die USA abwandern und dort ihre Rechner aufstellen, um nicht den strengen deutschen Regeln unterworfen zu sein. So gibt es Mail Provider die die deutschen Mails über Rechner in den USA laufen lassen. Hier wäre es sinnvoll sich international zu einigen.

Außerdem ist die Durchsetzung der Vorschriften wohl das größte Problem. Kaum einer wird merken, wenn irgendwo im Internet seine Daten weitergeleitet wurden. Man fragt sich zwar vielleicht wieso man schon wieder einen Katalog über Ski-Urlaube bekommt, obwohl man das Unternehmen gar nicht kennt, aber beweisen könnte man es nicht. Wenn alle die Verdacht hätte, dies beim Datenschutzbeauftragten anzeigen würden, dann wäre dieser völlig überlastet. Weiterhin stellt sich hier dann auch die Frage, wie er die einzelnen Verstöße überprüfen soll. Hier werden wohl noch viele Fragen und Regelungslücken offen bleiben, zumal uns die Technik derzeit laufend mit ihren Fortschritten einholt.

⁹⁵ Determann, Kommunikationsfreiheit im Internet, S. 91.