Telekommunikationsrecht

*CHRISTIAN KOENIG/ERNST RÖDER**

Die EG-Datenschutzrichtlinie für Telekommunikation – Verpflichtungen auch für Internetdienstleister

Der europäische Gesetzgeber hat mit der Richtlinie 97/66/EG die Voraussetzungen für ein einheitliches Datenschutzniveau in der Europäischen Gemeinschaft und damit für einen Binnenmarkt für Telekommunikationsdaten geschaffen. Die Umsetzungsfrist des Großteils der Verpflichtungen ist am 24. 10. 1998 abgelaufen, die wesentliche Aufgabe der Sicherstellung der Vertraulichkeit der Kommunikation muss bis zum 24. 10. 2000 umgesetzt werden. Der Titel der Richtlinie ist zwar weiter gefasst als die noch heute häufig verwendete ursprüngliche Bezeichnung »ISDN-Richtlinie«, er verdeckt aber immer noch, dass die Richtlinie auch Verpflichtungen für Internetdienstleister schafft. Zusammen mit den anwendbaren Regelungen der allgemeinen Datenschutzrichtlinie 95/46/EG ergeben sich umfangreiche Anforderungen, sei es für den Vertrieb von Daten im herkömmlichen Internet, sei es für Dienste, die sich des neuen Wireless Application Protocols (WAP) bedienen. Zugleich zeigt sich aber, dass die Richtlinie noch sehr dem herkömmlichen Verständnis von Telekommunikation als Sprachtelefonie verhaftet ist, was die Anwendung der Richtlinie im Bereich von Internetdienstleistungen verkompliziert. Die Autoren untersuchen die wesentlichen Verpflichtungen und stellen dar, inwieweit die Richtlinie noch mehr auf Internetdienstleistungen zugeschnitten werden sollte.

* Professor Dr. Christian Koenig, LL.M., ist Direktor am Zentrum für Europäische Integrationsforschung (ZEI) an der Universität Bonn. Ernst Röder, LL.M., ist wissenschaftlicher Mitarbeiter am ZEI (*http://www.zei.de*).

I. Internetdienstleister als Telekommunikationsanbieter

Die Telekommunikations-Datenschutzrichtlinie[1] schafft die Grundlage für eine Harmonisierung der Vorschriften für die Verarbeitung personenbezogener Daten im Zusammenhang mit der Erbringung öffentlich zugänglicher Telekommunikationsdienste über öffentliche Telekommunikationsnetze in der Gemeinschaft, insbesondere über das diensteintegrierende digitale Telekommunikationsnetz (ISDN) und öffentliche digitale Mobilfunknetze.[2] Hierbei sind Telekommunikation und Mobilfunk nicht lediglich mit Sprachtelefonie gleichzusetzen, wie dies auch die Kommission zu früheren Zeitpunkten implizit getan hat.[3] Vielmehr bezieht sich entsprechend der schon in der ONP-Richtlinie verwendeten Definition »Telekommunikationsdienst« auf Dienste, die ganz oder teilweise aus der Übertragung und Weiterleitung von Signalen über das Telekommunikationsnetz bestehen, mit Ausnahme von Hör- und Fernsehfunk.[4] Schon die Ausnahme von Hör- und Fernsehfunk muss jedoch eng verstanden werden. Schließlich umfasst die Richtlinie ausdrücklich Dienste wie Video auf Abruf und interaktives Fernsehen, die als neue Telekommunikationsdienste zur Entwicklung der Informationsgesellschaft eingeordnet werden.[5] Somit sind nur herkömmliche Rundfunkangebote vom Anwendungsbereich der Richtlinie ausgenommen.

Nicht ausdrücklich als Teil des Anwendungsbereiches der Richtlinie erwähnt werden Internetdienstleistungen wie E-Mail und das Anbieten von Homepages im World Wide Web (WWW).[6] Die Anwendbarkeit ergibt sich jedoch aus einer systematischen Auslegung der Begriffsdefinitionen der Richtlinie. So wird das öffentliche Telekommunikationsnetz[7] in der Richtlinie definiert als »Übertragungs- und gegebenenfalls Vermittlungssysteme sowie sonstige Betriebsmittel, mit denen Signale zwischen definierten Abschlusspunkten über Draht, über Funk, auf optischem oder anderem elektromagnetischen Wege übertragen werden und die ganz oder teilweise der Erbringung öffentlich zugänglicher Telekommunikationsdienste dienen«.[8] Ein traditionelles Verständnis des Begriffes Telekommunikation verleitet, das Telekommunikationsnetz lediglich mit den Netzen der Sprachtelefonie gleichzusetzen.[9] Schon der Verweis auf in denselben Netzen vorgenommene Faxübertragung und allgemeine Datenübertragung stellt jedoch klar, dass diese Beschränkung auf Sprachtelefonie nicht vom Wortlaut gedeckt ist. Auch hier handelt es sich schließlich um die Übertragung und Weiterleitung von Signalen über Draht, über Funk, auf optischem oder anderem elektromagnetischen Wege. Für die Einordnung von Internetdienstleistungen ist das Zusatzkriterium »zwischen definierten Abschlusspunkten«[10] entscheidend. In der Mitteilung zur Einordnung der Internettelefonie[11] hatte die Kommission dargelegt, dass es hierbei entscheidend auf die Möglichkeit ankommt, dass jeder Nutzer in einem öffentlichen Telekommunikationsnetz jeden anderen Nutzer erreichen kann. In der Mitteilung wurde darüber hinaus darauf abgestellt, dass die Abschlusspunkte als Telefonnummern aus dem nationalen Nummerierungsplan definiert seien. Im Kontext der Mitteilung erklärt sich dies damit, dass es hier um die mögliche Einordnung von Internettelefonie als Sprachtelefonie im Sinne der einschlägigen Richtlinien ging. Internet-Protokoll-Adressen sind zwar nicht mit Rufnummern in diesem Sinne gleichzusetzen,[12] dennoch ist das Internet ein öffentliches Telekommunikationsnetz, da insoweit die grundsätzlich vorhandene Erreichbarkeit der IP-Adressen im Internet ausreicht, um eine Erreichbarkeit jedes Nutzers durch jeden Nutzer zu bejahen. Damit ist die Telekommunikations-Datenschutzrichtlinie insbesondere auch anwendbar auf die Übertragung von E-Mail

1) Richtlinie 97/66/EG des Europäischen Parlaments und des Rates v. 15.12.1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, ABl. EG Nr. L 24 v. 30.1.1998, S. 1–8 (Telekommunikations-Datenschutzrichtlinie).

2) Art. 3 (1) Telekommunikations-Datenschutzrichtlinie (FN 1).

3) Weder der Vorschlag (ABl. EG 1990 Nr. C 277/12) noch der Geänderte Vorschlag (ABl. EG 1994 Nr. C 200/4) der Telekommunikations-Datenschutzrichtlinie (FN 1) beziehen sich auf weiter gehende Dienste der Informationsgesellschaft. Erst der gemeinsame Standpunkt vom 20.2.1995 (Abl. EG 1995 Nr. C 93/1) erwähnt die Möglichkeit, dass auch personenbezogene Ton- oder Bilddaten erfasst werden sollen. Die Formulierung in ihrer heutigen Form findet sich dann im Gemeinsamen Standpunkt v. 12.9.1996 (ABl. EG 1996 Nr. C 315/30).

4) Art. 2 Nr. 2 und 3 Richtlinie 90/387/EWG des Rates v. 28.6.1990 zur Verwirklichung des Binnenmarktes für Telekommunikationsdienste durch Einführung eines offenen Netzzugangs (Open Network Provision – ONP), geändert durch Richtlinie 97/51/EG (ABl. EG Nr. L 295 v. 29.10.97, 23).

5) Erwägungsgründe 3 und 10 Telekommunikations-Datenschutzrichtlinie (FN 1). Die Erwähnung dieser Dienste könnte auch vom Wunsch der Kommission geprägt sein, bereits jetzt klarzustellen, dass diese Dienste bei Marktfähigkeit nach Ansicht der Kommission als Telekommunikationsdienste anzusehen sind. Ähnliche Gesichtspunkte dürften auch der jüngst angenommenen Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt (2000/31 EG), ABl. EG Nr. L 178 v. 17.7.2000 (*E-Commerce-Richtlinie*) zugrunde liegen, die explizit in Erwägungsgrund 18 lediglich traditionelle Rundfunkangebote aus dem Anwendungsbereich ausnimmt, kritisch hierzu *Hamann*, Der Entwurf einer E-Commerce-Richtlinie 98/586 unter rundfunkrechtlichen Gesichtspunkten, ZUM 2000, 290 f. Kompetenzstreitigkeiten mit den Mitgliedstaaten dürften sich dennoch nicht vermeiden lassen.

6) Zu diesen und anderen Diensten im Internet vgl. z. B. *Gralla*, So funktioniert das Internet, München, 1999.

7) Die Telekommunikations-Datenschutzrichtlinie (FN 1) findet nur auf öffentliche, nicht auf für die Öffentlichkeit nicht zugängliche Telekommunikationsnetze Anwendung, Art. 3 (1) Telekommunikations-Datenschutzrichtlinie (FN 1). In nicht-öffentlichen Telekommunikationsnetzen wie z. B. Firmen-Intranets gilt die allgemeine Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. 10. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG Nr. L 281 v. 23.11.1995, 31–50 (Datenschutzrichtlinie).

8) Art. 2 lit. c Telekommunikations-Datenschutzrichtlinie (FN 1).

9) Zu kurz greift hier auch *Gundermann*, K&R 2000, 225 (227), Fußn. 21.

10) Art. 2 lit. c Telekommunikations-Datenschutzrichtlinie (FN 1).

11) Notice on the status of voice communications on the Internet under Community law and, in particular, pursuant to Directive 90/388/EEC, Supplement to the 1995 Commission Communication on the Status and Implementation of Directive 90/388/EEC.

12) Vgl. *Koenig/Neumann*, K&R 1999, 145 ff.

und anderen Internet-Diensten.[13] Dabei ist es irrelevant, welche Infrastruktur – z. B. das Festnetz, internetspezifische Backbones, das Stromnetz – dem Internet im Einzelnen zugrunde liegt, da unabhängig von dem konkreten Weg der Datenpakete eine Erreichbarkeit jeden Nutzers durch jeden Nutzer gegeben ist. Schließlich zeigt die Tatsache, dass im Anhang der Telekommunikations-Datenschutzrichtlinie unter den Datenarten, deren Verarbeitung gestattet ist,[14] neben Rufnummer und Verbindungsdauer auch explizit die Datenmenge erwähnt wird, dass auch Datenübermittlung jenseits von Sprach- und Faxtelefonie berücksichtigt werden sollte. Damit sind nicht nur Internetdienste, die im Internetfestnetz oder über Satellit mit TCP/IP erbracht werden, erfasst. Die Erwähnung von mobilen Telekommunikationsnetzen neben öffentlichen Telekommunikationsnetzen[15] ist insoweit historisch bedingt. Auch in anderen Telekommunikations-Richtlinien wird der Mobilfunk aus historischen oder auch inhaltlichen Gründen getrennt behandelt. Doch erfüllen auch öffentliche Mobilfunknetze die Eigenschaften eines öffentlichen Telekommunikationsnetzes. Damit sind auch im Mobilfunknetz über WAP[16] erbrachte Internetdienstleistungen erfasst, die folglich ebenfalls in den Anwendungsbereich der Richtlinie fallen.

Die Anwendbarkeit ist dabei nicht auf den Schutz der bei der Datenübertragung anfallenden Daten beschränkt. Zwar wurde schon in der allgemeinen Datenschutzrichtlinie klargestellt, dass bei der Übermittlung einer personenbezogene Daten enthaltenden Nachricht über Telekommunikationsdienste oder durch elektronische Post in der Regel die Person, von der die Nachricht stammt, und nicht die Person, die den Übermittlungsdienst anbietet, als Verantwortlicher für die Verarbeitung der in der Nachricht enthaltenen personenbezogenen Daten gilt. Dabei gelten die Anbieter der Übermittlungsdienstleistungen in der Regel lediglich als Verantwortliche für die Verarbeitung der personenbezogenen Daten, die zusätzlich für den Betrieb des Dienstes erforderlich sind.[17] In der Telekommunikations-Datenschutzrichtlinie wird jedoch darüber hinaus die Vertraulichkeit der Kommunikation selbst geschützt.[18] Damit sind durch die Richtlinie anders als im deutschen Teledienstedatenschutzgesetz (TDDSG)[19] und dem Mediendienstestaatsvertrag[20] nicht nur Bestandsdaten[21] sowie Nutzungs- und Abrechnungsdaten[22] geschützt,[23] sondern auch die Inhalte der Kommunikation selbst.[24]

II. Die Regelungen im Einzelnen

1. Terminologie

Auch wenn die Formulierungen der Telekommunikations-Datenschutzrichtlinie offensichtlich auf Teilnehmer an Sprach- und Faxtelefonie ausgerichtet sind, sind sie auch für Internetdienste, -anbieter und -nutzer tauglich. So differenziert die Telekommunikations-Datenschutzrichtlinie zwischen dem »Teilnehmer« – eine natürliche oder juristische Person, die mit einem Anbieter öffentlich zugänglicher Telekommunikationsdienste einen Vertrag über die Inanspruchnahme dieser Dienste geschlossen hat – und dem »Benutzer« – eine natürliche Person, die einen öffentlich zugänglichen Telekommunikationsdienst für private oder geschäftliche Zwekke nutzt, ohne diesen Dienst zwangsläufig abonniert zu haben.[25] Internetnutzer, die fest bei einem Provider abonniert sind, und auch Internetnutzer, die sich des Internet-by-Calls bedienen, sind daher Teilnehmer. Nut-

13) Zum gleichen Ergebnis kommt auch *Schild*, Die Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, EuZW 1999, 69 (70), der allerdings darauf abstellt, dass Internetdienste und Telekommunikation »schwer voneinander zu trennen sind«. Die Ansicht der Kommission hierzu ist nicht eindeutig zu ermitteln. Der Überarbeitungsvorschlag der Kommission zur Telekommunikations-Datenschutzrichtlinie (Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (KOM [2000] 385) v. 12.7.2000) geht zwar davon aus, dass Änderungen notwendig sind, um Zweifel zu beseitigen, es wird jedoch nicht eindeutig gesagt, dass nach dem jetzigen Wortlaut eine Anwendbarkeit der Richtlinie auf Internetdienstleistungen abgelehnt würde, vgl. Arbeitspapier der GD Informationsgesellschaft zu KOM/239/2000, abrufbar unter *http://www.ispo.cec.be/infosoc/telecompolicy/review99/*wdprot.pdf (Stand 15.6.2000). Für eine Bejahung der Anwendbarkeit schon der jetzigen Fassung auch durch die Kommission spricht dabei, dass die vorgeschlagene Änderung an der Telekommunikations-Datenschutzrichtlinie im Gegensatz zu den im Zusammenhang mit dem einheitlichen Rahmen für alle elektronischen Kommunikationsdienste und -netze vorgeschlagenen weiter reichenden Änderungen an anderen Richtlinien sich im Wesentlichen auf den Ersatz des Begriffes »Telekommunikationsdienst« durch den Begriff »elektronischen Kommunikationsdienst« beschränkt. Der Begriff »elektronischer Kommunikationsdienst« ist dabei lediglich klarstellend, da es sich hierbei nur um einen in seiner Substanz ernst genommenen Telekommunikationsbegriff handelt.

14) Verarbeitet werden dürfen laut Art. 6 Abs. 2 i.V.m. dem Anhang der Telekommunikations-Datenschutzrichtlinie (FN 1) die Nummer oder die Identifikation des Teilnehmerendgerätes; die Anschrift des Teilnehmers und die Art des Endgerätes; die Gesamtzahl der für den Abrechnungszeitraum zu berechnenden Einheiten; die Nummer des angerufenen Teilnehmers; Art, Beginn und Dauer der Anrufe *und/oder die übermittelte Datenmenge*; Datum des Anrufs/der Dienstleistung; andere Zahlungsinformationen, beispielsweise Vorauszahlung, Ratenzahlung, Sperren des Anschlusses und Mahnungen (Hervorhebung durch die Autoren).

15) Art. 3 (1) Telekommunikations-Datenschutzrichtlinie (FN 1).

16) Zum Wireless Application Protocol (WAP), dem Versuch einer Vielzahl von Produzenten u.a. aus dem Bereich Software und Endgeräte, einen de facto Industriestandard zu schaffen, vergleiche *http://www.wapforum.org* (Stand 15.6.2000).

17) Erwägungsgrund 47 Datenschutzrichtlinie (FN 7).

18) Erwägungsgrund 1 und Art. 5 Telekommunikations-Datenschutzrichtlinie (FN 1).

19) Artikel 2 des Informations- und Kommunikationsdienste-Gesetz (IuKDG) in der Fassung des Beschlusses des Deutschen Bundestages v. 13. 6. 1997 (BT-Drucks. 13/7934 v. 11.6.1997).

20) Staatsvertrag über Mediendienste (Mediendienstestaatsvertrag), abrufbar unter *http://www.iid.de/iukdg/mdstv.html* (Stand 15.6.2000).

21) Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erforderlich sind, vgl. § 5 (1) TDDSG und § 14 MDStV.

22) Daten über die Inanspruchnahme von Diensten, die erforderlich sind, um die Nutzung bzw. die Abrechnung der Nutzung zu ermöglichen, vgl. § 6 TDDSG und § 15 MDStV.

23) Zur diesbezüglichen Diskussion über den Anwendungsbereich des TDDSG (FN 19) und des MDStV (FN 20) vgl. *Imhof*, CR 2000, 110.

24) Im Einzelnen hierzu unten unter II. 3.

25) Art. 2 lit. a und b Telekommunikations-Datenschutzrichtlinie (FN 1).

zer, die sich von öffentlichen Zugangspunkten wie z. B. Internet-Cafes in das Internet einloggen, sind dagegen Benutzer.[26]

Des Weiteren werden in der Richtlinie die Begriffe »öffentliches Telekommunikationsnetz« und »Telekommunikationsdienst« definiert.[27] Wie oben ausgeführt, umfassen diese Begriffe auch das Internet bzw. Internetdienste.

2. Datensicherheit

Der »gläserne Nutzer« ist in besonders hohem Maße des Datenschutzes bedürftig.[28] Das Stichwort hier lautet Datensicherheit: der Schutz personenbezogener Daten gegen zufällige oder unautorisierte Zerstörung oder zufälligen Verlust sowie unautorisierten Zugang, Veränderung oder Verbreitung.[29] Nebenbegriff zur Datensicherheit ist die Netzsicherheit,[30] die den Begriff der Datensicherheit um die netzspezifische Sichtweise erweitert. Internetdiensteanbieter müssen geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit ihrer Dienste zu gewährleisten, insoweit davon die Netzsicherheit betroffen ist, notwendigenfalls zusammen mit dem Betreiber der zugrunde liegenden Netzinfrastruktur.[31] Dabei wird der Grad der Sicherheit unter Berücksichtigung des Artikel 17 der Datenschutzrichtlinie[32] bewertet. Dieser Vorschrift zufolge müssen personenbezogene Daten gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang sowie gegen jede andere Form der unrechtmäßigen Verarbeitung geschützt werden. Die Datensicherheit muss nicht in jedem Fall gewährleistet werden. Vielmehr werden der Stand der Technik und die Kosten der Sicherungsmaßnahmen in Betracht gezogen. Diesen gegenüber muss lediglich ein »angemessenes« Sicherheitsniveau angesichts des bestehenden Risikos gewährleistet werden.[33] Besteht ein besonderes Risiko der Verletzung der Netzsicherheit, muss der Betreiber eines öffentlich zugänglichen Telekommunikationsdienstes die Teilnehmer über dieses Risiko und über mögliche Abhilfen einschließlich deren Kosten unterrichten.[34]

Der Stand der Technik ist in der Richtlinie nicht definiert. Allerdings kann davon ausgegangen werden, dass sich für die Datensicherheit von E-Mails die digitale Unterschrift,[35] durch die E-Mails vor unbemerkbaren Veränderungen durch Dritte geschützt werden, als technischer Standard durchgesetzt hat. Diese Prämisse liegt einer Vielzahl von Gesetzen[36] und der Richtlinie über Digitale Signaturen[37] zugrunde. Noch kein Standard hat sich für das Verschlüsseln von E-Mails auf der Übertragungsebene durchgesetzt.[38] Auch von den Verschlüsselungsprogrammen, die auf Ebene der Nutzeranwendungen arbeiten,[39] hat sich noch keines als De-facto-Standard etabliert.

Für die Übertragung von Daten im Rahmen von WWW-Angeboten ist das Verwenden von SSL[40] als Verschlüsselung auf der Übertragungsebene oder ähnlicher Systeme als Stand der Technik anzusehen. Da Verschlüsselung insoweit auch zum gegenwärtigen Stand der Technik zählt, sind Internetdienstleister nach der Telekommunikations-Datenschutzrichtlinie verpflichtet, bei der Übertragung von personenbezogenen Daten neben unverschlüsselten Verbindungen auch verschlüsselte Verbindungen für die Nutzer, deren Browser und TCP/IP-Stacks verschlüsselte Verbindungen verarbeiten können, anzubieten.

3. Vertraulichkeit

Die Telekommunikations-Datenschutzrichtlinie verpflichtet die Mitgliedstaaten zur Sicherstellung der Vertraulichkeit der Kommunikation. Die Mitgliedstaaten sollen durch innerstaatliche Vorschriften auch die Vertraulichkeit der über das Internet und mit Internetdiensten erfolgenden Kommunikation sicherstellen. Insbesondere müssen die Mitgliedstaaten das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Kommunikation durch andere Personen als die Benutzer, wenn keine Einwilligung der betroffenen Benutzer vorliegt, untersagen,[41]

26) Um die Lesbarkeit zu erleichtern, soll nachfolgend, wenn es nicht auf diese Unterscheidung ankommt, vom Nutzer der Dienstleistung gesprochen werden.

27) Art. 2 lit. c und d Telekommunikations-Datenschutzrichtlinie (FN 1).

28) Vgl. schon 1996 die Empfehlungen der International Working Group on Data Protection in Telecommunications, Report and Guidance on Data Protection and Privacy on the Internet adopted at the 20th Meeting in Berlin, Germany, 15. und 16. 4. 1996 (»Budapest – Berlin Memorandum«).

29) Art. 17 Datenschutzrichtlinie, auf den Erwägungsgrund 15 der Telekommunikations-Datenschutzrichtlinie (FN 1) in Bezug auf den Begriff der Sicherheit verweist. Vgl. auch schon Art. 7 der Council of Europe Convention 108/81-Convention for the protection of individuals with regard to automatic processing of personal data, geändert am 15. 6. 1999 mit Appendix 3, Punkt 10.3b, um der EG den Beitritt zur Konvention zu ermöglichen.

30) Art. 4 Telekommunikations-Datenschutzrichtlinie (FN 1).

31) Art. 4 Telekommunikations-Datenschutzrichtlinie (FN 1).

32) Erwägungsgrund 15 Telekommunikations-Datenschutzrichtlinie (FN 1).

33) Die weitere Ausnahme des Art. 17 (2) Telekommunikations-Datenschutzrichtlinie (FN 1), die es darüber hinaus noch gestattet, die Art der Daten zu berücksichtigen, um das angemessene Sicherheitsniveau zu ermitteln, wird als lex generalis von der lex specialis des Art. 4 (1) Satz 2 Telekommunikations-Datenschutzrichtlinie (FN 1) verdrängt.

34) Art. 4 (2) Telekommunikations-Datenschutzrichtlinie (FN 1).

35) So auch *Geis*, NJW 1997, 288 (291 f.).

36) Z. B. das Signaturgesetz als Art. 3 des IuKDG (FN 17) in Deutschland und ähnliche Gesetze in den USA, ein Überblick zu Letzteren findet sich beim Internet Law and Policy Forum, *http://www.ilpf.org/digsig/digrep.htm* (Stand 16.6.2000).

37) Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. 12. 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. EG Nr. L 13 v. 19.1.2000, 12–20.

38) Verschlüsselte Verbindungen sind bisher regelmäßig nur für das Abfragen von E-Mails über POP, nicht für das Versenden von E-Mails über SMTP möglich.

39) Z. B. Pretty Good Privacy (pgp), erhältlich unter *http://www.pgpi.org* (Stand 15.6.2000), zu dem Problem für deutsche Nutzer vgl. *Borngießer*, PGP – Wie geht das?, abrufbar unter *http://www.sicherheit-im-internet.de/showdoc.php3?doc=bmwi_theme_doc_1999938285080&page=1* (Stand 15.6.2000).

40) Secure Socket Layer, zu dieser und anderen Verschlüsselungsmethoden s. auch IT-Security, *http://pweb.uunet.de/shn-cs.es/firewall.htm* (Stand 15.6.2000). Erkennbar ist die Verwendung von SSL auf der Anwendungsebene durch den Beginn der Adresse (URL) mit https:// statt http://.

41) Art. 5 (1) Telekommunikations-Datenschutzrichtlinie (FN 1).

wobei Ausnahmen z. B. zum Schutz der nationalen Sicherheit gemacht werden können.[42]
Kommunikation ist hierbei nicht definiert. Es wird jedoch zu Recht angenommen, dass dies nicht nur die übermittelten Inhalte, sondern auch die Transaktionsdaten umfasst,[43] und zwar insbesondere bei Diensten wie E-Mail oder Chats, als auch Online-Banking und E-Commerce. Insoweit umfasst der Schutz der Vertraulichkeit nicht nur den Schutz personenbezogener Daten, sondern auch sonstige Kommunikationsinhalte. Problematisch hierbei ist, dass der unverschlüsselte Internet-Datenaustausch durch gezielte Angriffe[44] relativ einfach mitzulesen ist. Für E-Mail werden daher Verschlüsselungsprogramme[45] empfohlen. Derzeit bieten kaum E-Mail-Anbieter Verschlüsselung an,[46] so dass sich der Nutzer selbst um ein Programm wie PGP[47] kümmern muss, um seine E-Mails verschlüsseln zu können.
Die Regelung der Vertraulichkeit scheint im Unterschied zu der der Datensicherheit lediglich von Maßnahmen auf der normativen Ebene (»insbesondere untersagen ...«) auszugehen. Die Verpflichtung zur Sicherung der Vertraulichkeit nach dem jeweiligen technischen Stand muss jedoch in die Vorschrift mit hineingelesen werden. Zum einen ist Rechtsgut der Richtlinie neben dem Datenschutz auch der Schutz der Privatsphäre. Zum anderen ist Vertraulichkeit der Schutz der kommunizierten Daten vor unautorisiertem Zugang. Somit ist Vertraulichkeit ein Unterfall der Datensicherheit, nach der die Daten der Nutzer jeweils technisch bestmöglich (mit den erwähnten Ausnahmen) zu schützen sind. Verschlüsselung wird überraschenderweise nicht expressis verbis in der Richtlinie gefordert.[48]
Noch zählt Verschlüsselung, wie oben ausgeführt, nicht bei allen Internetdienstleistungen zum gegenwärtigen Stand der Technik. Sollten schon mit der Richtlinie selbst auch Anbieter von E-Mail verpflichtet werden, Verschlüsselung anzubieten, müsste die Richtlinie dementsprechend angepasst werden. Die Mitgliedstaaten können jedoch jetzt schon Internetdienstleister zur Erfüllung der Vorschrift zur Sicherstellung der Vertraulichkeit verpflichten, auf Verschlüsselungsmöglichkeiten hinzuweisen und diese dem Nutzer zugänglich zu machen.
Die Richtlinie lässt eine Ausnahme für das rechtlich zulässige Aufzeichnen von Kommunikation im Rahmen einer rechtmäßigen Geschäftspraxis zum Nachweis einer kommerziellen Transaktion oder einer sonstigen geschäftlichen Kommunikation zu.[49] Hier können die Mitgliedstaaten bestimmen, dass eine Aufzeichnung auch ohne vorherige Zustimmung zulässig sein soll. Diese Ausnahme ist lex specialis zu der Vorschrift zur Datenerhebung in der allgemeinen Datenschutzrichtlinie, die wie das bisherige deutsche Recht[50] die Einwilligung der anderen Partei verlangt. In der spezifischen Interessenlage des Geschäftsverkehrs über Fernkommunikation ist diese Ausnahme aber gerechtfertigt.[51]
Der Begriff »Aufzeichnung« zeigt, dass hier vor allem an den Geschäftsverkehr über Sprachtelefonie gedacht ist. Für Geschäftsverkehr über E-Mail erübrigt sich eine derartige Regelung auch, da dem Verfasser einer E-Mail bewusst ist, dass seine Mitteilung gespeichert werden kann und in der Regel auch gespeichert wird. Für Geschäftskontakte über interaktive Dienste im WWW könnte die Vorschrift jedoch Bedeutung gewinnen.

4. Verkehrsdaten und Daten für die Gebührenabrechnung

Verkehrsdaten, also Daten, die sich auf Nutzer beziehen und die für den Verbindungsaufbau verarbeitet und vom Internetdienstanbieter gespeichert werden, müssen nach Beendigung der Verbindung gelöscht oder anonymisiert werden.[52] Lediglich zum Zwecke der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen ist es zulässig, spezifische, im Anhang der Richtlinie genannte Daten zu verarbeiten. In dieser Aufzählung zeigt sich wieder die enge Fixierung der Richtlinie auf Sprachtelefonie, da, wie oben ausgeführt, mit dem Begriff der Datenmenge nur ein zukunftstaugliches Kriterium angeführt wird.[53] Die Verarbeitung dieser Daten ist nur bis zum Ablauf der Frist zulässig, innerhalb deren die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann. Der Internetdienstanbieter kann diese Daten zum Zwecke der Vermarktung seiner eigenen Telekommunikationsdienste verarbeiten, wenn der Teilnehmer seine Einwilligung gegeben hat.
Für die Nutzung des WWW scheint damit problematisch, dass Diensteanbieter zwar die der Verbindung zugrunde liegenden Daten löschen müssen, eine Erstellung von Nutzerprofilen etwa nach benutzten Websites aber zulässig zu sein scheint,[54] da es sich hier ja nicht um Daten, die für die Abrechnung notwendig sind, und auch nicht um den Inhalt der Kommunikation handelt. Bei der Verarbeitung dieser Daten handelt es sich jedoch nicht um Datenverarbeitung personenbezogener Daten im Zusammenhang mit der Erbringung von Te-

42) Art. 14 Telekommunikations-Datenschutzrichtlinie (FN 1).
43) Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes, 7. 9. 1999, 5085/99/en/final WP 25 und Recommendation 2/99 on the Respect of Privacy in the context Interception of Telecommunications, 3. 5. 1999, 5005/99/en/final WP 18.
44) Bei Dazuschalten auf Routerebene ist es möglich, den Datenstrom mitzuloggen und lesbar zu machen.
45) Vgl. Rfc 2504, 3.3 Email Pitfalls, *http://www.faqs.org/rfcs/rfc2504.html* (Stand 15.6.2000).
46) Eine Ausnahme ist beispielsweise web.de, vgl. *http://trust.web.de* (Stand 15.6.2000).
47) Pretty Good Privacy (FN 39).
48) Dies kritisiert auch *Schild*, EuZW 1999, 69 (70) m.w.N. in Fußn. 14.
49) Art. 5(2) Telekommunikations-Datenschutzrichtlinie (FN 1).
50) § 201 StGB verlangt die Einwilligung der anderen Partei.
51) *Schild*, EuZW 1999, 69 (71).
52) Art. 6 Telekommunikations-Datenschutzrichtlinie (FN 1).
53) Vgl. FN 14. Der Vorschlag der Kommission zur Überarbeitung der Telekommunikations-Datenschutzrichtlinie (FN 13) sieht vor, den gesamten Anhang als nicht technologieneutral zu streichen.
54) Diese sind bisher nach deutschen Regelungen in § 4 (4) TDDSG (FN 19) und § 12 (4) MDStV (FN 20) nur unter Verwendung von Pseudonymen zulässig.

lekommunikationsdiensten,[55] sondern um Daten, die lediglich bei Gelegenheit der Telekommunikation entstehen. Damit ist hier nicht die Telekommunikations-Datenschutzrichtlinie einschlägig, sondern die allgemeine Datenschutzrichtlinie anwendbar. Eine Verarbeitung von Datenspuren zur Erstellung von Nutzerprofilen ist daher nur mit Einwilligung des Nutzers möglich.[56]
Weiter gehende generelle Speichererfordernisse der Verkehrsdaten, wie sie als präventive Maßnahme der Verbrechensbekämpfung erwogen wurden, sind streng am Kriterium der Verhältnismäßigkeit auszurichten. Dabei sind generelle Verpflichtungen, alle Verkehrsdaten über den Abrechnungszeitraum hinaus zur Verbrechensbekämpfung aufzubewahren, nicht zulässig.[57]

55) Vgl. Art. 3 (1) Telekommunikations-Datenschutzrichtlinie (FN 1).
56) Art. 7 lit. a Datenschutzrichtlinie, die anderen Ausnahmen (Verarbeitung ist erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen; Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt; die Verarbeitung ist erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person; die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde; die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden) sind hier nicht einschlägig.
57) So auch Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes, 7. 9. 1999, 5085/99/EN/FINAL WP 25.
58) Art. 8 und 9 Telekommunikations-Datenschutzrichtlinie (FN 1).
59) Erwägungsgründe 18 und 19 Telekommunikations-Datenschutzrichtlinie (FN 1), hierzu auch Working Party on the Protection of Individuals with regard to the Processing of Personal Data Recommendation 3/97 Anonymity on the Internet, Adopted by the Working Party on 3 December 1997.
60) Vgl. dazu unten II. 7.
61) »In einigen Newsgruppen, in denen es um sehr sensible Themen geht (zum Beispiel sexuelle Gewohnheiten etc.), werden Pseudonyme bzw. Artikel, die über sogenannte Anonymous-Remailer (auch »Anon-Server« genannt) gepostet wurden, in Ausnahmefällen geduldet.«, Punkt 14 der Netiquette unter *http://www.kirchwitz.de/~amk/dni/netiquette* (Stand 15.6.2000), vgl. z. B. die Charta der Newsgruppe de.etc.selbsthilfe.missbrauch unter *http://www.wolfgang-kopp.de/de-chartas.txt* (Stand 15.6.2000).
62) Vgl. für de.newsgroups Netiquette unter *http://www.kirchwitz.de/~amk/dni/netiquette* (Punkt 14: Benutzen Sie Ihren wirklichen Namen, kein Pseudonym!), für das gesamte Usenet z. B. Netiquette Guidelines 3.1.3. unter *http://www.faqs.org/rfcs/rfc1855.html* (Stand 15.6.2000).
63) Hierzu auch Arbeitskreis »Technische und organisatorische Datenschutzfragen« der Datenschutzbeauftragten des Bundes und der Länder, vom 17.11.1997, abrufbar unter *http://www.datenschutz-bayern.de/home.htm* (Stand 15.6.2000).
64) Hierzu *Ermer*, Systemdatenschutz und Chipkarten, CR 2000, 126.
65) Art. 2 Abs. 1 lit. e des Vorschlags der Kommission zur Überarbeitung der Telekommunikations-Datenschutzrichtlinie (FN 13). Abgesehen von der altertümlich anmutenden Verwendung des Begriffes »Telefondienst« zeigt schon das Beispiel der Konferenzschaltung, die bei ISDN möglich ist und vom Schutzzweck her auch unter diese Definition fallen müsste, dass die Definition nicht sonderlich geglückt ist.
66) Art. 11 Telekommunikations-Datenschutzrichtlinie (FN 1).

5. Anonyme Nutzung des Internets

Auch die Möglichkeit der Vermeidung von Verkehrsdaten muss gewährleistet sein. Die Telekommunikations-Datenschutzrichtlinie geht umfangreich auf das Regel-Ausnahmeverhältnis der Anrufnummernanzeige bzw. -unterdrückung ein (CLIP bzw. CLIR).[58] Hierbei werden die Verkehrsdaten zwar nicht vermieden, dem Partner der Telekommunikation sind sie jedoch nicht zugänglich. Damit liegt der Richtlinie insoweit der allgemeine Gedanke zugrunde, dass Punkt-zu-Punkt-Kommunikation anonym möglich sein sollte. Schon frühzeitig wurde eine mögliche anonyme Nutzung des Internets diskutiert. Sachgerecht wurde dabei vorgeschlagen, Anonymität dort zu ermöglichen, wo sie in parallel gelagerten Fällen auch eingeräumt würde.[59] So ist das Versenden eines Briefes, das Anbringen eines Zettels an ein schwarzes Brett oder auch das Anrufen eines Sorgentelefons von einem Münzfernsprecher anonym möglich.
Hier sind jedoch die Vorschriften der Richtlinie nicht direkt anwendbar, da die Formulierungen für Anrufernummernanzeigenunterdrückung dem Wortlaut nach nur auf Sprachtelefonie anwendbar sind. Auch wenn man E-Mails unter »Anrufe« subsumieren möchte, was teleologisch möglich wäre,[60] so führt doch der Unterschied in der technischen Machbarkeit der Anonymisierung dazu, dass die Regelungen der Richtlinie nicht greifen können. Bei Telefonanrufen kann Anonymität schon durch die Unterdrückung der Rufnummernanzeige einfach gewährleistet werden. Anders ist es bei E-Mails. Hier ist entweder der anonyme Zugang zum Internet oder Remailing über einen spezifischen Provider notwendig, um Anonymität zu gewährleisten. In entsprechenden Newsgroups[61] wird auch entgegen der Usenet-Netiquette[62] das Beitragen von Artikeln (Posten) unter einem anderen als dem Realnamen gestattet. Trotz der angesprochenen ausdrücklichen Erwähnung von neuen Diensten in der Richtlinie sind diese Regelungen damit nur vom Sinn, nicht jedoch vom Wortlaut für E-Mails relevant. Möglichkeiten anonymer Nutzung von E-Mail und anderen Internetdiensten,[63] z. B. durch Remailing, Internet-by-Call oder durch die Inanspruchnahme von Internetdiensten unter Verwendung einer Chipkarte[64], wären in einer überarbeiteten Form der Richtlinie zu fordern. Der Änderungsvorschlag der Kommission sieht hierzu jedoch noch keine Änderungen vor, sondern beschränkt die Gewährung von Anonymität auf »Anrufe«, die definiert werden sollen als »eine über einen öffentlichen Telefondienst aufgebaute Verbindung, die eine zweigleisige Echtzeit-Kommunikation ermöglicht«.[65]

6. Verzeichnisse

Die Telekommunikations-Datenschutzrichtlinie regelt das Anlegen von Teilnehmerverzeichnissen.[66] Teilnehmer ist bei Inanspruchnahme von Internetdienstleistungen sowohl derjenige Nutzer, der sich bei einem Internetdiensteanbieter fest für einen Zugang zum Internet angemeldet hat, als auch derjenige, der sich über Internet-by-Call einwählt. Im Falle der Führung eines

Teilnehmerverzeichnisses durch Telekommunikationsanbieter[67] müssen Teilnehmer die Möglichkeit haben, einer Aufnahme ins Verzeichnis ganz zu widersprechen. Im Falle der Zustimmung zur Eintragung ins Verzeichnis dürfen lediglich zur Identifizierung des Teilnehmers notwendige Daten ins Verzeichnis aufgenommen werden, außer der Teilnehmer stimmt der Aufnahme darüber hinausgehender Informationen zu. Der Überarbeitungsvorschlag der Kommission sieht hier die Umkehrung des Regel-Ausnahme-Verhältnisses dahin gehend vor, dass der Eintragung nicht gegebenenfalls widersprochen werden muss, sondern eine Einwilligung des Nutzers nötig ist.[68] Viele Teilnehmerverzeichnisse im Internet sehen schon jetzt eine Eintragung nur bei Einwilligung vor.[69]

7. Unerwünschte Werbezusendungen

Direktvermarkter bedienen sich verstärkt des Internets, um mit potenziellen Kunden Kontakt aufzunehmen. Dies ist zwar primär keine Frage des Datenschutzes, sondern des Schutzes der Privatsphäre, jedoch auch von der Richtlinie umfasst. Für diese unerwünschten Werbe-E-Mails (Spam) legt die Richtlinie auf den ersten Blick keine Verpflichtungen fest. Lediglich für Kommunikation mit Automaten als Gesprächspartner (Voice-Mail-System) oder Fernkopien (Telefax) für die Zwecke des Direktmarketings wird die Verpflichtung geschaffen, dass diese Art der Kontaktaufnahme nur bei vorheriger Einwilligung der Teilnehmer gestattet werden darf (sog. Opt-In-Lösung).[70] Unerbetene Anrufe, die nicht über Voice-Mail-Systeme oder Telefax erfolgen, können ebenfalls im Wege des Opt-Ins geregelt werden, hier ist aber auch eine Opt-Out-Lösung (der Nutzer muss mitteilen, dass er diese Art von Anrufen nicht möchte) möglich.[71] Da die Richtlinie »Anruf« nicht definiert, sondern lediglich von unerbetenen Anrufen, die nicht mit Voice-Mail oder Telefax erfolgen, spricht, wäre eine Anwendung bei weiter Interpretation des Begriffes »Anruf« auch für unerwünschte Werbe-E-Mails möglich.[72] Damit müssten die Mitgliedstaaten auch hier entweder Opt-In- oder Opt-Out-Möglichkeiten schaffen. Eine solche Interpretation wird zwar z. B. in der britischen Umsetzung der Richtlinie nahegelegt, die »Direktmarketing« als »Kommunikation mit beliebigem Kommunikationsmittel«[73] definiert. Gegen diese weite Interpretation der in der Telekommunikations-Datenschutzrichtlinie aufgestellten Verpflichtung spricht aber, dass an dieser Stelle speziell von »Anrufen« und nicht, wie an anderen Stellen in der Richtlinie, von »Kommunikation« die Rede ist.[74] Gegen eine weite Auslegung des Begriffes »Anruf« spricht insoweit auch die Verwendung des Begriffes »Anruf« in anderen Artikeln der Richtlinie, die sich zweifellos nur auf Telefon- oder Faxanrufe beziehen.[75] In einer ähnlichen Vorschrift in der Fernabsatzrichtlinie, die unerbetene Anrufe ausschließt, wird dagegen an entsprechender Stelle nicht von anderen Anrufen, sondern von »Fernkommunikationstechniken, die eine individuelle Kontaktaufnahme erlauben«,[76] gesprochen. Während die Fernabsatzrichtlinie unerwünschte Werbe-E-Mails mit umfasst, wird die Frage der Anwendbarkeit der Datenschutzrichtlinie auf Werbe-E-Mails aber in jedem Fall mit dem Erlass der E-Commerce-Richtlinie[77] obsolet. Nach der E-Commerce-Richtlinie muss unerwünschte kommerzielle Kommunikation wie unerwünschte Werbe-E-Mails klar und eindeutig als solche erkennbar sein.[78] Darüber wurde auf Drängen des Europäischen Parlamentes in den geänderten Vorschlag der Richtlinie die Verpflichtung aufgenommen, auch hier Opt-Out-Register zu schaffen, in die sich diejenigen eintragen können, die keine unerwünschten Werbe-E-Mails empfangen wollen.[79] Die Mitgliedstaaten müssen sicherstellen, dass Direktvermarkter regelmäßig diese Verzeichnisse heranziehen und sich danach richten. Darüber hinaus steht es den Mitgliedstaaten offen, Spam weiter gehenden Regeln zu unterwerfen.[80] Sachgerecht ist hier der Überarbeitungsvorschlag der Kommission, in diesem Zusammenhang die Vorschrift von der Anwendbarkeit auf »Anrufe« auf »Unerbetene Nachrichten« zu erweitern. Unter Berücksichtigung der Verbraucherinteressen sollen E-Mails dabei als eine solche Form der Kommunikation eingestuft werden, für welche die Mitgliedstaaten lediglich eine Opt-In-Lösung vorsehen dürfen.[81]

8. Datentransfer in Drittländer

Die Telekommunikations-Datenschutzrichtlinie enthält keine speziellen Vorschriften zum Datenexport. Damit sind die Regeln der allgemeinen Datenschutzrichtlinie zum Export von personenbezogenen Daten zur Verarbeitung in Länder außerhalb der EG einschlägig. Dies ist problematisch, da diese Vorschriften sich sehr am Gedanken von zentraler, hierarchischer Daten-

67) Verzeichnisanbieter im Internet, die keine Telekommunikationsdienste erbringen, werden hiervon nicht erfasst, sind aber mit Art. 6 (1) lit. d der Datenschutzrichtlinie ebenfalls zur Datenpflege, also z. B. zu Sicherstellung der Richtigkeit der gespeicherten Daten verpflichtet.

68) Art. 12 des Vorschlags der Kommission zur Überarbeitung der Telekommunikations-Datenschutzrichtlinie (FN 13).

69) Vgl. z. B. das E-Mail-Verzeichnis des Deutschen Forschungsnetz e.V., abrufbar unter *http://www.directory.dfn.de/ambix/* (Stand 16.6.2000).

70) Art. 12 (1) Telekommunikations-Datenschutzrichtlinie (FN 1).

71) Art. 12 (2) Telekommunikations-Datenschutzrichtlinie (FN 1).

72) Eine Anwendbarkeit der Richtlinie hält auch für möglich *Rowe*, Telecoms Data Protection – UK Implementation, Computer Law and Security Report 1999, S. 407 (408, 409).

73) »Communication (by whatever means) of any advertising or marketing material which is directed to particular individuals«, Data Protection Act UK 1998, unsere Übersetzung, zitiert nach *Rowe*, Computer Law and Security Report 1999, 407 (410).

74) Diese Ansicht vertritt auch das britische Department of Trade and Industry nach *Rowe*, Computer Law and Security Report 1999, 407 (409).

75) Z. B. ist »Anrufweiterschaltung« in Art. 10 Telekommunikations-Datenschutzrichtlinie (FN 1) eine Vorschrift, deren Übertragung auf E-Mails keinen Sinn machen würde, da die Interessenlage eine andere ist.

76) Richtlinie 97/7/EG des Europäischen Parlaments und des Rates vom 20. 5. 1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz, ABl. EG Nr. L 144 v. 4.6.1997, 19.

77) *E-Commerce-Richtlinie* (FN 5). Hierzu *Röder*, European Business Law Review 2000, 472.

78) Art. 7 (1) E-Commerce Richtlinie (FN 5).

79) Art. 7 (2) E-Commerce Richtlinie (FN 5) wurde hinzugefügt.

80) Art. 3 (3) i.V.m. Anhang E-Commerce Richtlinie (FN 5).

81) Art. 13 des Vorschlags der Kommission zur Überarbeitung der Telekommunikations-Datenschutzrichtlinie (FN 13).

verarbeitung in Mainframe-Rechnern orientieren.[82] Im weltumspannenden Internet finden ständig Datentransfers von und zu Rechnern in verschiedensten Ländern statt. Innerhalb der EG ist das unproblematisch, da hier mit Umsetzung der Richtlinien von einem einheitlichen Datenschutzniveau auszugehen ist. Exporte von Daten in Länder außerhalb der EG sind nach der Datenschutzrichtlinie nur zulässig, wenn im Drittland ein adäquates Datenschutzniveau besteht.[83] Die Einstufung des Schutzniveaus im Drittland wird dabei letztlich von der Europäischen Kommission getroffen. Diese Vorschrift ist einschlägig für personenbezogene Daten, die »Gegenstand einer Verarbeitung sind«.[84] Verarbeitung ist hierbei jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten.[85] Schon personenbezogene Daten, die vom Nutzer z. B. bei der Nutzung von WWW-Angeboten auf einem Server in einem Drittland oder bei der Übersendung eines E-Mails an einen Server im Drittland übertragen werden, sind daher von der Vorschrift umfasst. Mit zunehmender internationaler Etablierung von direktem E-Commerce, dem Vertrieb von virtuellen Gütern wie Software oder digitalisierten Musikstücken über das Internet und indirektem E-Commerce, dem Vertrieb von Gütern und Dienstleistungen auf herkömmlichem Wege, die über das Internet bestellt wurden, sowie der Einrichtung von Firmenextranets für globale Unternehmen auch unter Verwendung der Internetinfrastruktur, werden diese Datenströme stetig zunehmen. Besonders ansteigen werden sie durch den verstärkten Einsatz von Business-to-Business-Vertriebsplätzen im Internet (sogenanntes B2B), wie sie von großen Unternehmen oft in internationaler Kooperation geplant sind.[86] Hierbei sind verschiedene Konstellationen denkbar. Der Datenempfänger im Drittland kann z. B. für die Verarbeitung verantwortlich sein, es kann aber auch ein im Inland Verantwortlicher die Daten zur Verarbeitung ins Drittland schicken, oder Rechner in einem Mitgliedstaat lassen den Zugriff aus einem Drittland zu.[87] Damit gewinnt das grundsätzliche Verbot des Datenexportes in ein Drittland ohne angemessenes Schutzniveau gerade im Internet an Bedeutung.

Die Übertragung in ein nicht sicheres Drittland ist zulässig, wenn der Nutzer der Datenübertragung zustimmt. Damit müsste theoretisch ein Anbieter, der die Übertragung von Daten in ein Drittland veranlasst, in seinen Server eine Funktion einbauen, die den Nutzer auf die Übertragung seiner Daten in ein Drittland ohne angemessenes Datenschutzniveau hinweist, ihn über die vorgesehene Weiterverwendung informiert[88] und den Datenübertragungsvorgang ohne erteilte Zustimmung abbricht.

Über die Ausnahme der Einwilligung des Nutzers hinaus steht der Regel des Verbotes der Übertragung in ein Drittland ohne angemessenes Schutzniveau aber ein umfangreicher Ausnahmenkatalog gegenüber. Insbesondere ist eine Übertragung auch bei fehlendem angemessenen Datenschutzniveau im Drittland möglich, wenn die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse der betroffenen Person vom für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wurde oder geschlossen werden soll. Außerdem ist eine Übermittlung zulässig, die entweder für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben ist oder für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist oder aus einem Register erfolgt, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.[89]

Darüber hinaus kann ein Mitgliedstaat eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland genehmigen, das kein angemessenes Schutzniveau bietet, wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet.[90] Diese Garantien können sich insbesondere aus entsprechenden Vertragsklauseln ergeben.[91] Problematisch bei der Vertragslösung ist, dass diese

82) Nachw. bei *Swire/Litan*, None of your Business, Washington, 1998, S. 50 ff.

83) Art. 25 und 26 Datenschutzrichtlinie (FN 15), hierzu *Draf*, Die Regelung der Übermittlung personenbezogener Daten in Drittländer nach Art. 25, 26 der EG-Datenschutzrichtlinie, Frankfurt 1999.

84) Art. 25 (1) Datenschutzrichtlinie (FN 15). Der Zusatz »oder nach der Übermittlung verarbeitet werden sollen« ist redundant, da die Übermittlung schon eine Verarbeitung darstellt, vgl. Art. 2 lit. b Datenschutzrichtlinie (FN 15) und dazu *Draf*, Die Regelung der Übermittlung personenbezogener Daten in Drittländer nach Art. 25, 26 der EG-Datenschutzrichtlinie, Frankfurt 1999, S. 58.

85) Art. 2 lit. b Datenschutzrichtlinie (FN 15).

86) *Kuri*, Geldbäume im Online-Land, c't 2000, Heft 7, 190 f. Z.B. haben *Ford*, *GM* und *DaimlerChrysler* den weltweit größten Internet-basierten virtuellen Markt geplant, vgl. *http://www.ford.com/default.asp*?pageid=106&storyid=695 (Stand 15.6.2000).

87) *Tröndle*, CR 1999, 717 (720).

88) Ähnlich *Tröndle*, CR 1999, 717 (722 f).

89) Art. 26 (1) Telekommunikations-Datenschutzrichtlinie (FN 1).

90) Diese Lösung wurde mit dem »Safe-Harbour-Agreement« der EG mit den USA gewählt. Eine Liste der einzuhaltenden Prinzipien findet sich unter U.S. Department of Commerce, Draft International Safe Harbour Privacy Principles, November 15, 1999, *http://www.ita.doc.gov/td/ecom/* USPrinciplesJune2000.htm (Stand 15.6.2000). Die Ausgangslage könnte sich jedoch ändern, wenn auch die USA Datenschutzgesetze erlassen, wie jüngst in einem Report eines Beratungskommitees der Federal Trade Commission empfohlen wurde, vgl. FTC Advisory Committee on Online Access and Security, Final Report of the FTC Advisory Committee on Online Access and Security, May 15, 2000, *http://www.ftc.gov/acoas/papers/finalreport.htm* (Stand 15.6.2000).

91) Art. 26 (2)–(4) Telekommunikations-Datenschutzrichtlinie (FN 1).

sinnvoll nur für ständige Kommunikationsbeziehungen ist, nicht für einmalige Kommunikationsbeziehungen, wie sie für das Internet typisch sind.[92] Eine mögliche sachgerechte Lösung ist damit die Internationalisierung der vorgesehenen Verhaltenskodizes über den Bereich der EG hinaus.[93] Es ist jedoch offensichtlich, dass das Internet bei der Schaffung der Datenexportregeln nicht genügend berücksichtigt wurde. Wünschenswert wäre daher entweder eine Neuorientierung der Datenexportregeln der Datenschutzrichtlinie oder die Erarbeitung spezifischer Regelungen in der Telekommunikations-Datenschutzrichtlinie bei einer Überarbeitung der Richtlinie, um sie insgesamt mehr an die Gegebenheiten des Internets anzupassen. Hierzu sieht der Änderungsvorschlag der Kommission leider keine Änderungen vor.[94]

III. Anpassungsbedarf der Richtlinie

Auch wenn sich schon jetzt für Internetdienstleister umfangreiche Verpflichtungen aus den Datenschutzrichtlinien ergeben, beziehen sich die Formulierungen der bereichsspezifischen Telekommunikations-Datenschutzrichtlinie doch noch zu deutlich auf Sprachtelefoniebetreiber. Eine Ergänzung zur Klarstellung der Anwendbarkeit der Richtlinie auf Internetdienstleister wäre also wünschenswert.

Eine Ergänzung der Telekommunikations-Datenschutzrichtlinie ist insbesondere notwendig, um einheitliche Kriterien für Daten- und Netzsicherheit im Binnenmarkt sicherzustellen. Auch zur Erzielung eines einheitlichen Niveaus des Schutzes der Privatsphäre wäre eine konkreter auf Internetdienstleistungen zugeschnittene Verpflichtung zum Schutz der Vertraulichkeit erstrebenswert.

Die Regelungen der Speicherung von Verkehrsdaten erfassen zwar nicht das Anlegen von Nutzerprofilen, dies ist jedoch unproblematisch, da ein Anlegen von Nutzerprofilen schon nach den Vorschriften der allgemeinen Datenschutzrichtlinie nur mit Einverständnis des Nutzers möglich ist.

Zur Ermöglichung von Anonymität im Internet wären weiter gehende Regelungen wünschenswert, da die Ansätze in der Telekommunikations-Datenschutzrichtlinie hier zu einseitig auf herkömmliche Sprachtelefonie zugeschnitten sind.

Nicht besonders auf Internetdienstleistungen zugeschnitten werden muss die Regelung von Teilnehmerverzeichnissen, da diese schon in der jetzigen Form sachgerecht sind.

Eine eigene Regelung zu unerwünschten Werbe-E-Mails (Spam) in der Richtlinie wäre eigentlich nicht notwendig. Zwar thematisch auch mit dem Themenkreis der Privatsphäre verwandt, ist dieses Problem schon sachgerecht im Rahmen des Fernabsatzes und demnächst auch im Rahmen des elektronischen Handels geregelt worden. Jedoch wäre eine Überarbeitung der Richtlinie, die unerwünschte Werbe-E-Mails in den Rahmen der Kommunikationsformen einbringt, die nur nach einem Opt-In des Nutzers erfolgen dürfen, ein sinnvoller Schritt zu mehr Verbraucherschutz.

Wichtig bleibt es weiterhin, entweder im Rahmen einer Überarbeitung der allgemeinen Datenschutzrichtlinie oder der Telekommunikations-Datenschutzrichtlinie adäquate Regeln für den Datentransfer in Drittländer über das Internet zu schaffen.

Der Änderungsvorschlag der Kommission beschränkt sich leider weitgehend auf den Ersatz des Begriffes »Telekommunikation« durch den der »elektronischen Kommunikation«, ohne in den hier angesprochenen Problemkreisen wesentliche Verbesserungsvorschläge zu machen.

In Zukunft wird über den Schutz der Übertragung personenbezogener Daten im Internet hinaus verstärkt der allgemeine Schutz der Privatsphäre im Internet an Bedeutung gewinnen. In diesem Zusammenhang sind auch die Vorhaben zur Ausarbeitung eines Europäischen Grundrechtskatalogs zu bedenken. Sollte hiernach der Internet-Datenschutz umfassender geregelt werden, könnte eine Erweiterung der Gemeinschaftskompetenzen auf Belange der Inhaltsregulierung notwendig werden.

92) *Geis*, NJW 1997, 288 (293).
93) *Geis*, NJW 1997, 288 (293) mit Hinweis auf *Ehmann*, zitiert in *Bachmann*, NJW 1996, 1805 f.
94) Vorschlag der Kommission zur Überarbeitung der Telekommunikations-Datenschutzrichtlinie (FN 13).