Johann Bizer
Schutz der Vertraulichkeit in der Telekommunikation[1]

1. Problemstellung

Telekommunikation[2] steht in der modernen Informationsgesellschaft für einen technisch vermittelten Nachrichtenaustausch über Entfernungen mit Hilfe von Fernmeldetechnik,[3] d. h. mit Hilfe von elektromagnetischen Wellen über Kabel, Funk oder Lichtwellen.[4] Fernmeldetechnisch übermittelte Nachrichten sind, verglichen mit herkömmlichen Mitteln, in hohem Maß verletzlich: Während die mündliche Alltagskommunikation durch die Wahl der örtlichen Kommunikationsbedingungen (Vier-Augen-Prinzip) und die Briefpost durch einen physischen Umschlag gegen unbefugte Kenntnisnahme geschützt werden kann, sind fernmeldetechnisch übermittelte Nachrichten dem Zugriff des Netzbetreibers und Dienstleistungsanbieters preisgegeben. Aber nicht nur das: Auch Dritte können mit technischen Hilfsmitteln Leitungen oder Server öffentlicher Netzwerke anzapfen oder Funkstrecken scannen und auf diese Weise gezielt Nachrichten abhören.

Darüber hinaus hat die Digitalisierung der Kommunikationstechnik zu einer Integration von Nachrichtenübertragung und Datenverarbeitung geführt, die die Übermittlung von Sprachen, Bildern und Texten in Datenform getrennt oder multimedial in großen Mengen, hoher Qualität und kürzester Zeit ermöglicht. Die neuen technischen Möglichkeiten begünstigen den Boom der Telekommunikation.[5] Während einerseits die technische Entwicklung die Möglichkeiten der Nachrichten- und Datenübertragung verbessert hat, haben sich andererseits aber auch die Risiken erhöht, Nachrichten spurenlos abzuhören.[6] Mit ausreichenden Rechnerkapazitäten stehen die technischen Mittel zur Verfügung, wenige Nachrichten aus einer Vielzahl von Kommunikationsakten zu erfassen und nach bestimmten Merkmalen zu selektieren.[7]

1 Schriftliche Fassung eines Vortrags des Verf. auf dem Kongreß »5 vor 2000« des Berufsverbandes der Datenschutzbeauftragten (BvD) am 25. 10. 1995 in Ulm.

2 Seit dem 3. September 1994 ist im GG nunmehr ausdrücklich von Telekommunikation und nicht mehr vom Fernmeldewesen die Rede, vgl. Art. 73 Nr. 7 und den nunmehr neuen Art. 87 f., Gesetz zur Änderung des GG vom 30. August 1994, BGBl. I, S. 2245.

3 Nicht gemeint ist mit Telekommunikation also die Nachrichtenübertragung mit Hilfe von Buschtrommeln, Leuchtfeuer oder optischen Signalmasten etc.

4 Zum Begriff der Fernmeldetechnik Kammerer/Eidenmüller, Post- und Fernmeldewesen, Loseblatt, Mai 1991, § 1 FAG, Anm. 4 f., BT-Drs. 5/1880, 7.

5 So betrug bspw. die Anzahl der in Deutschland im In- und ins Ausland geführten Telefongespräche 1990: 36,2 Mrd. und 1993 51,4 Mrd Zahlen aus Geschäftsbericht der DBP Telekom 1993, zitiert nach Jahrbuch Telekommunikation und Gesellschaft 1995, 395.

6 Vgl. Bundesregierung vom 10. 4. 1995, BT-Drs. 12/1110, S. 2, wonach »Sicherheitslücken« in digitalen Vermittlungsstellen das »unbefugte Aufschalten auf Anschlußleitungen« und »unbefugtes Eindringen in das Computersystem über Einrichtungen des Fernwirkens und Fernwartens« sein können.

7 Vgl. nur die Befugnis des BND nach § 3 Abs. 2 G 10 G i. d. F. des Art. 13 des Verbrechensbekämpfungsgesetzes vom 28. Oktober 1994, BGBl. I, S. 3195.

Die wirtschaftliche Brisanz einer ungeschützten Telekommunikation liegt auf der Hand: Schutzbedürftig sind vornehmlich, aber nicht nur, Betriebs- und Geschäftsgeheimnisse gegen in- und ausländische Konkurrenten (Wirtschaftsspionage) und andere, auch rechtlich geschützte Berufsgeheimnisse wie die ärztliche oder die anwaltliche Schweigepflicht oder das Steuergeheimnis.[8] Aber auch im täglichen »elektronischen Geschäft«, bei der elektronischen Bestellung im Teleshopping oder Video on Demand, der elektronischen Überweisung im Electronic Banking und anderen Rechtsgeschäften sollte ein ausreichender Vertraulichkeitsschutz gewährleistet sein, um Mißbrauch durch Dritte abzuwehren.

Neben diesen mehr wirtschaftlichen Gesichtspunkten wirkt sich der fehlende Vertraulichkeitsschutz der Telekommunikation aber auch auf die kommunikative Entfaltung der Teilnehmer störend aus: Wer damit rechnen muß, daß seine Kommunikation mit anderen von Dritten mitgehört wird, ist in seiner Entfaltungsfreiheit erheblich eingeschränkt und wird sein Kommunikationsverhalten entsprechend verändern.[9] Die latente Möglichkeit, von Dritten belauscht zu werden, beeinträchtigt die Offenheit und Spontanität des wechselseitigen Austauschs. Gemeintes wird nicht offen ausgesprochen, und Inhalte werden unterdrückt, weil die Kommunikationssituation sich an den Ohren des Lauschers ausrichtet. Daß eine solche Beeinträchtigung nicht nur die Entfaltungschancen der Einzelnen betrifft, sondern auch das Gemeinwohl, hat das BVerfG erst jüngst wieder hervorgehoben.[10]

2. Technische Schutzkonzepte

Vor diesem Hintergrund gewinnen die technischen Möglichkeiten, die Anlagen der Telekommunikation gegen Angriffe auf die Vertraulichkeit zu schützen, neue Bedeutung. Kryptographische Verschlüsselungsverfahren, ehemals nur eine Domäne der Instanzen des staatlichen Geheimschutzbereichs und dort zum Schutz der Übermittlung geheimgehaltener Informationen (Verschlußsachen) ebenso wie zur Analyse verschlüsselter Nachrichten fremder Dienste und innerstaatlicher Organisationen verwendet,[11] gewinnen zunehmend auch für zivile Zwecke an Bedeutung.[12] Sicherheit in offenen Netzen wird in Zukunft ohne die Verwendung kryptographischer Verfahren nicht zu gewährleisten sein.[13]

In der Telekommunikation können Verschlüsselungstechniken von den *Betreibern der Fernmeldeanlagen* eingesetzt werden, um ihre ungesicherten Übertragungsstrecken zu schützen. Heute werden auf diese Weise lediglich die Funkstrecken des Mobilfunknetzes im GSM-Standard, nicht aber die Übertragung über Festleitungen (Kabel) gesichert.[14] Nicht geschützt ist auch der übrige Funkverkehr wie z. B. die

8 Vgl. die exemplarische Darstellung von 10 Ermittlungsfällen bei Bär, Der Zugriff auf Computerdaten im Strafverfahren, 1992, 37 ff.

9 BVerfG, EuGRZ 1995, 355.

10 BVerfG, EuGRZ 1995, 355 unter ausdrücklichem Hinweis auf das Volkszahlungsurteil BVerfGE 65, 1, 43.

11 Rihaczek, Datensicherheit amerikanisch, DuD 1987, 240 ff.; ders., Kryptoalgorithmen in offenen Kommunikationssystemen, DuD 1993, 220 ff.; Folsing, Die Hohe Schule der Kryptologie, Kursbuch 66, 1981, 92 mwN.; Bauer, Kryptologie, 1994, 156.

12 Allerdings stehen einer innovativen Entwicklung noch einschrankende Exportbestimmungen und in bestimmten Landern wie Frankreich auch Verwendungsverbote entgegen.

13 Hessischer Datenschutzbeauftragter, 22. Tatigkeitsbericht 1993, 159 f. Auch fur die Umsetzung der in der Anlage zu § 9 BDSG geforderten Datensicherheitsmaßnahmen gewinnen kryptographische Verfahren unter den heutigen Bedingungen der dezentralen Datenverarbeitung neue Bedeutung.

14 Dies ist beispielsweise auf der Mobilfunkstrecke des D-Netzes der Fall; Beheim, Sicherheit und Vertraulichkeit bei europaweiter Mobilkommunikation, DuD 1994, 327 ff.

Funkkommunikation von Behörden und Organisationen mit Sicherheitsaufgaben (BOS)[15] oder die gebündelten Richtfunkstrecken der Netzbetreiber.
Die Vertraulichkeit von Nachrichten in der Telekommunikation kann aber auch durch die *Teilnehmer* selbst geschützt werden, indem sie unabhängig und autonom vom Netzbetreiber mit Hilfe von Verschlüsselungstechniken ihre Individualkommunikation verschlüsseln, so daß sie nur vom Empfänger entschlüsselt werden kann.[16]

Teilnehmer können ihre Nachrichten mit symmetrischen und mit asymmetrischen Schlüsseln verschlüsseln.[17] Symmetrische Schlüssel eignen sich für geschlossene Benutzergruppen, denn die Kommunikationspartner müssen den jeweiligen Entschlusselungsschlüssel vor ihrer Kommunikation festlegen. Demgegenüber können Nachrichten mit asymmetrischen Schlüsselverfahren auch außerhalb geschlossener Benutzergruppen verschlüsselt übertragen werden, ohne vorher mit dem Kommunikationspartner in Kontakt getreten zu sein.[18]
Asymmetrische Schlüsselverfahren verwenden mathematisch zusammenhängende Schlüsselpaare mit je einem geheimen und einem öffentlichen Schlüssel.[19] Der geheime Schlüssel wird unausforschbar auf einer Chipkarte gespeichert, der öffentliche Schlüssel ist allgemein, beispielsweise über ein elektronisches Register, verfügbar.[20] Der Nachrichtenaustausch mit Hilfe eines asymmetrischen Verfahrens erfolgt, indem der Absender seine Nachricht mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und diese verschlüsselte Nachricht an den Empfänger übermittelt. Nunmehr kann nur der Empfänger mit Hilfe seines »geheimen« Schlüssels die verschlüsselte Nachricht entschlüsseln und im Klartext lesen.
Allerdings setzen asymmetrische Schlusselverfahren eine vertrauenswürdige Sicherungsinfrastruktur voraus,[21] denn die Schlüssel müssen sicher erzeugt, Personen zugeordnet, zertifiziert und gegen einen kompromittierenden Zugriff Dritter geschützt sein. Aber auch symmetrische Schlüsselverfahren funktionieren nicht voraussetzungslos, sie müssen ebenfalls sicher erzeugt, verwaltet und zwischen den Kommunikationspartnern ausgetauscht werden konnen.

3. Vertraulichkeit versus Innere Sicherheit

Weil die Verwendung von Verschlüsselungsverfahren aus naheliegenden Gründen das Abhören von Nachrichten erschwert, haben beide Optionen, die Verschlüsselung durch die Netzbetreiber und die autonome Verschlüsselung durch die Teilnehmer, das besondere Interesse der Behörden der Inneren Sicherheit geweckt. Ein Blick in die jüngere Geschichte der Kryptologie zeigt, daß staatliche Sicherheitsinteressen schon immer in der Versuchung waren, den Schutz der Vertraulichkeit zu ihren Gunsten zu kompromittieren.

Beispielsweise hat die amerikanische Geheimdienstbehörde NSA (National Security Agency) Ende der 70er Jahre erheblichen Einfluß auf die Entwicklung und Standardisierung des welt-

15 Vgl. die Entschließung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 in Berlin zur Gefahrdung der Vertraulichkeit der Funkkommunikation von Sicherheitsbehörden und Rettungsdiensten. Dazu auch der Hessische Datenschutzbeauftragte, 21. Tätigkeitsbericht 1992, 118.

16 Zu den einzelnen Verfahren siehe Bizer, Die Kryptokontroverse, in: V. Hammer, Die Gestaltung von Sicherungsinfrastrukturen für eine offene Telekooperation 1995, 179 f. mwN.

17 Bauer (Fn. 11), 148 mwN; Beutelspacher, Kryptologie 1993, 133 ff.

18 Das bekannteste asymmetrische Schlusselsystem lautet nach seinen Erfindern Rivest/Shamir/Adleman RSA, C.ACM 1978, 120 ff.; dazu auch Bauer (Fn. 11), 148 mwN. Weitere Verfahren sind in: Der Hessische Datenschutzbeauftragte, 23. Tätigkeitsbericht, 1994, 166 f., aufgezählt.

19 Ausführlicher provet/GMD, Die Simulationsstudie Rechtspflege, Eine neue Methode zur Technikgestaltung für Telekooperation, 1994, 56 ff. mwN.

20 Wegen der allgemeinen Verfügbarkeit des öffentlichen Schlussels wird auch von einem öffentlichen Schlusselsystem gesprochen.

21 Zum Begriff der Sicherungsinfrastruktur siehe V. Hammer, Gestaltungsbedarf und Gestaltungsoptionen für Sicherungsinfrastrukturen, in V. Hammer (Fn. 16); zu den Anforderungen und Gestaltungsmöglichkeiten Roßnagel, Institutionell-organisatorische Gestaltung informationstechnischer Sicherungsinfrastrukturen, DuD 1995, 259 ff.

weit bedeutsamen DES (Data Encryption Standard) genommen, nur um ein starkes Verschlüsselungsverfahren zu verhindern.[22] Angenommen wird, daß mit dem DES verschlüsselte Nachrichten für gut ausgestattete Dienste wie die NSA beherrschbar sind.[23] Staatliche Sicherheitsinteressen spielten in den USA auch in dem für zivile Zwecke vorgesehenen Verschlüsselungskonzept eines »Clipper-Chip« eine große Rolle. Sein Verschlüsselungsalgorithmus »Skipjack« ist von der NSA entwickelt, wird aber geheimgehalten.[24]

In der Bundesrepublik Deutschland ist für die Entwicklung, Überprüfung und Zulassung von Verschlüsselungsverfahren im Bereich der Verarbeitung oder Übermittlung amtlich geheimgehaltener Informationen das Bundesamt für Sicherheit in der Informationstechnik (BSI) zuständig.[25] Vorläufer war die im Umfeld der Geheimdienste angesiedelte Zentralstelle für das Chiffrierwesen (ZfCH), von der berichtet wird, ihr sei es zu verdanken gewesen, daß die Normung des DES vom DIN ersatzlos eingestellt worden ist.[26] Problematisch an der rechtlichen Konstruktion des heutigen BSI ist seine Funktion als Diener zweier Herren, auf der einen Seite von Polizei und Staatsanwaltschaft, auf der anderen Seite der Verfassungsschutzbehörden, die es mit seiner Fachkompetenz »unterstützen« soll, § 3 Abs. 1 Nr. 6 BSIG.[27] Gleichzeitig soll das BSI aber auch Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik »beraten« können, § 3 Abs. 1 Nr. 7.[28] Und nicht nur das, auf das Marktgeschehen kann das BSI indirekt Einfluß nehmen, indem es auf Antrag der Hersteller und Vertreiber Sicherheitszertifikare für informationstechnische Systeme oder Komponenten (Produktzertifikate) ausstellt, § 4 Abs. 1 BSIG.

Schließlich läßt sich die Brisanz der zivilen Verwendung von Kryptoverfahren auch aus den jeweils geltenden Ausfuhrbeschränkungen für Kryptotechniken ablesen, die einen Vertraulichkeitsschutz grenzüberschreitender Kommunikation erheblich erschweren. So sind beispielsweise eine Reihe von Sicherungsanwendungen des PEM (Privacy Enhanced Mail), die für e-mail im Internet angeboten werden könnten, wegen geltender Exportbeschränkung nur in Kanada und den USA verfügbar.[29] In Deutschland unterliegen der Export von Kryptotechniken zur Gewährleistung der Informationssicherheit sowie Techniken zur Ausführung kryptoanalytischer Funktionen einem Genehmigungsvorbehalt.[30]

Die nunmehr auch in Deutschland beginnende Kontroverse über den Schutz der Vertraulichkeit und die Interessen der Inneren Sicherheit bietet Anlaß genug, ihren (verfassungs)rechtlichen Rahmen abzustecken.

22 Fumy/Rieß, Kryptographie, 1994, 219; Folsing (Fn. 11), 102 f.; Coy, Geheime Schriften – geheime Dienste, in: Kursbuch 66 (1981), S. 83 ff. Statt einem 64 Bit Schlussel wurde nur ein 56 Bit Schlussel entwickelt. Aus diesem Grund wird der DES haufig auch als Triple-DES mit einer Schlussellange von 112 Bit angeboten und verwendet, Hessischer Datenschutzbeauftragter (Fn. 18), S. 165.

23 Rihaczek (Fn. 11), DuD 1993, 221; Rueppel, »Clipper« – Der Krypto-Konflikt am Beispiel der amerikanischen ESCROW-Technologie in: Tinnefeld/Philipps/Weis, Institutionen und Einzelne im Zeitalter der Informationstechnik 1994, 187 (auch in DuD 1994, 443 ff.).

24 Naher Rueppel (Fn. 23), S. 186; Hessischer Datenschutzbeauftragter (Fn. 18), S. 166.

25 BSI-Errichtungsgesetz – BSIG, vom 17. Dezember 1990, BGBl. I, S. 2834.

26 Waidner/Pfitzmann/Pfitzmann, Uber die Notwendigkeit genormter kryptographischer Verfahren, DuD 1987, 293 ff., 298.

27 Kritisch bereits Bizer/Hammer/Pordesch/Roßnagel, Ein Bundesamt fur die Sicherheit in der Informationstechnik, DuD 1990, 179.

28 Bereits im Gesetzgebungsverfahren wurde gefordert, das BSI als rein »zivile« Behorde zu konzipieren und weisungsunabhangig zu stellen. Bizer/Roßnagel, Bundesamt fur die Sicherheit in der Informationstechnik, KJ 1990, 441 f sowie Bizer/Hammer/Pordesch/Roßnagel (Fn. 27), DuD 1990, 179.

29 So Horster/Portz, Privacy Enhanced Mail, DuD 1994, 440; die Kontroverse um den Export von PGP (Pretty Good Privacy) scheint jedoch mittlerweile ausgeraumt zu sein.

30 § 7 Abs. 1 AWG i. V. m. § 5 Abs. 1 AWV i. V. m. Teil I Abschnitt C 5A011 i. V. m. 5E011 der Ausfuhrliste. Ausgenommen sind lediglich einzelne Anwendungen, bspw. in pay-TV fur den allgemeinen Gebrauch, wenn die digitale Entschlusselung auf die Bild-, Ton- oder Bedienfunktion beschrankt ist, oder in Mobilfunktelefonen fur den zivilen Einsatz, die Verschlusselung enthalten, wenn sie ihren Anwender begleiten, Ausfuhrliste Teil I, Abschnitt C, 5E011 Ziff. 1 c und d. Abgedruckt in Hocke/Berwald/Maurer Außenwirtschaftsrecht, 1994. Einfuhrbeschrankungen bestehen, soweit ersichtlich, nicht.

Das als Grundrecht in Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis gilt dem Schutz der Vertraulichkeit einer fernmeldetechnisch vermittelten Kommunikation.[31] Es gewährleistet die freie Entfaltung der Persönlichkeit durch einen privaten, vor den Augen der Öffentlichkeit verborgenen Austausch von Nachrichten, Gedanken und Meinungen.[32] Letztlich ist das Fernmeldegeheimnis eine rechtliche Reaktion auf die besondere Schutzbedürftigkeit einer mit technischen Hilfsmitteln vermittelten Kommunikation, deren Sicherheit außerhalb der Verfügungsmöglichkeiten der Kommunikationspartner liegt.[33]

Grundrechtlichen Schutz genießt in erster Linie der Kommunikations*inhalt*.[34] Ob dieser für Dritte verständlich ist (Klartext) oder durch kryptographische Verfahren verfremdet und damit Dritten als unverständlicher »Ziffernsalat« erscheint, ist für den Grundrechtsschutz unerheblich. Letztlich ist es das Wesen eines Geheimnisses, daß es vor Dritten – auf welche Weise auch immer – verborgen wird. Also unterliegt auch eine verschlüsselte Nachricht dem Schutz des Fernmeldegeheimnisses.

Geschützt ist aber auch die Bestimmungsbefugnis der am Kommunikationsvorgang Beteiligten, »wer von dem Inhalt Kenntnis erlangen soll«.[35] Notwendigerweise erstreckt sich das Fernmeldegeheimnis damit auch auf die Entscheidungs- und Verfügungsbefugnis der Beteiligten, ein Geheimnis mit technischen Mitteln zu schützen. Insoweit besteht kein Unterschied zum Briefgeheimnis, das ebenfalls die Freiheit schützt, Nachrichten im verschlossenen Umschlag zu versenden und sie dadurch vor dem Zugriff Dritter zu schützen.[36] Damit schützt das Fernmeldegeheimnis aber auch die Entscheidungsfreiheit des Empfängers, eine verschlüsselte Nachricht zu entschlüsseln oder als (verschlüsseltes) Geheimnis dauerhaft zu bewahren.[37]

Neben dem Kommunikationsinhalt schützt das Fernmeldegeheimnis auch den Kommunikations*vorgang*, insbesondere die Tatsache, ob und wann zwischen welchen Personen und Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist.[38] Demnach fallen in den Schutzbereich des Fernmeldegeheimnisses auch die *Umstände* einer verschlüsselten Nachrichtenübermittlung, nämlich die Tatsache, ob und wer an wen verschlüsselte Nachrichten übermittelt hat.

Während der verfassungsrechtliche Schutz des Fernmeldegeheimnisses primär gegen staatliche Eingriffe gerichtet ist, konkretisiert § 10 FAG die objektiv-rechtliche Verpflichtung des Staates, die Vertraulichkeit der Telekommunikation zu gewährleisten, als Geheimhaltungsverpflichtung im Privatrechtsverkehr.[39] Danach ist zur Wahrung des Fernmeldegeheimnisses jeder verpflichtet, der eine Fernmeldeanlage betreibt, beaufsichtigt, bedient oder sonst bei ihrem Betrieb tätig ist.[40] Außerdem verpflichtet § 10a Abs. 1 FAG die Betreiber öffentlicher Fernmeldeanlagen, »technische Vorkehrungen oder sonst geeignete Maßnahmen zum Schutz (1.) des Fernmeldegeheimnis-

31 BVerfGE 67, 152, 172; naher Bizer (Fn. 16) S. 184.
32 BVerfGE 67, 157, 171.
33 Ähnlich Rohlf, Der grundrechtliche Schutz der Privatsphäre, 1980, 165 f.; Evers, Privatsphäre und Ämter für Verfassungsschutz, 1960, 180 f.; Gusy, Das Grundrecht des Post- und Fernmeldegeheimnisses, JuS 1986, 90; Roßnagel, Das Recht auf (tele)kommunikative Selbstbestimmung, KJ 1990, 273 f.
34 BVerfGE 85, 386, 396.
35 BVerfGE 85, 386, 396 und BVerfGE 67, 157, 172.
36 Lower in: v. Münch/Kunig, Kommentar zum GG, 1992, Art. 10 Rn. 10; Schuppert in: AK-GG 1989, Art. 10, Rn. 23.
37 Naher Bizer (Fn. 16), S. 186.
38 BVerfGE 85, 386, 396; BVerfGE 67, 157, 171.
39 Unter den Bedingungen einer deregulierten Telekommunikation gewinnt diese und die folgenden Bestimmungen erheblich an praktischer Bedeutung.
40 Eine vergleichbare Geheimhaltungspflicht besteht für den Funkverkehr, § 11 FAG und § 6 AFuG.

ses (...) zu treffen«.[41] Strafrechtlich ist das Fernmeldegeheimnis durch § 354 StGB abgesichert. Das Ausspähen besonders gesicherter Daten ist nach § 202a StGB strafbar.

5. Staatliche Abhörbefugnisse

Demnach ist das Fernmeldegeheimnis zwar umfassend rechtlich geschützt, jedoch ist es den Behörden der Inneren Sicherheit nach den auf der Grundlage des Gesetzesvorbehalts in Art. 10 Abs. 2 GG erlassenen, im folgenden kurz skizzierten gesetzlichen Regelungen nicht verwehrt, den Fernmeldeverkehr unter näher festgelegten Voraussetzungen abzuhören.[42]

Nach *§ 100a StPO* darf der Fernmeldeverkehr nur für Zwecke der Straftatverfolgung von der Staatsanwaltschaft und Polizei »überwacht und aufgezeichnet« werden. Abgehört werden darf nur zur Verfolgung sogenannter »Katalogstraftaten«, d. h. im Gesetz ausdrücklich benannter Straftaten[43], wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre, § 100a Satz 1 StPO. Verfahrensrechtlich ist das Abhören zu Zwecken der Straftatverfolgung durch einen Richtervorbehalt gesichert, bei Gefahr im Verzug darf es auch durch den Staatsanwalt angeordnet werden, § 100b Abs. 1 StPO.[44] Die Anordnung ergeht schriftlich, muß Namen und Anschrift des Betroffenen enthalten, Art, Umfang und Dauer der Maßnahmen bestimmen und darf höchstens auf drei Monate mit einer Verlangerungsmöglichkeit befristet sein, § 100b Abs. 2 StPO. Die Anordnung einer Überwachungsmaßnahme richtet sich gegen den Beschuldigten oder gegen Personen (also unverdächtige Personen), von denen auf Grund bestimmter Tatsachen anzunehmen ist, daß sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder daß der Beschuldigte ihren Anschluß benutzt, § 100a Satz 2 StPO.

§ 39 Abs. 1 AWG: De lege lata ist das »Überwachen und Aufzeichnen« des Fernmeldeverkehrs zu präventiv-polizeilichen Zwecken unzulässig.[45] Eine Ausnahme bildet die 1992 eingefuhrte Abhörbefugnis des Zollkriminalamts[46], nach der das Abhören zur Verhütung von Straftaten nach dem Außenwirtschaftsgesetz oder dem Kriegswaffenkontrollgesetz, also bereits im Vorfeld strafbaren Handelns, zulässig ist. Die Verfahrensvorschriften dieser Abhorbefugnis entsprechen weitgehend § 100a StPO.

Nach dem *G 10 Gesetz* ist das »Überwachen und Aufzeichnen« zur Abwehr drohender Gefahren für die freiheitlich demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes sowie der in der Bundesrepublik Deutschland stationierten NATO-Truppen möglich, § 1 Abs. 1 G 10.[47] Zur Kontrolle *individueller Anschlüsse* ermachtigt das G 10, wenn tatsachliche Anhaltspunkte für den Verdacht bestimmter, im Gesetz näher bezeichneter Straftaten gegen die innere und äußere Sicherheit bestehen, § 2 G 10.[48]

41 Allerdings ist die entsprechende Verordnungsermachtigung nach § 10a Abs. 2 FAG bislang von der Bundesregierung noch nicht ausgefullt worden.

42 Vgl. im einzelnen die Darstellung der Abhorbefugnisse bei Bizer (Fn. 16) S. 191 ff mwN., Andeutungsweise auch Bar (Fn. 8), S 323, 464 ff., 503 f. und ders., Die Uberwachung des Fernmeldeverkehrs, CR 1993, 583.

43 Vgl. § 100a Abs. 1 Nr 1 bis 5 StPO (i. d. Fassung des Art. 4 des Verbrechensbekampfungsgesetzes vom 28. Oktober 1994, BGBl. I, S. 3186), dazu zahlen u. a. die Staatsschutzdelikte, Geld- und Wertpapierfalschung, schwerer Menschenhandel, Mord, Totschlag oder Volkermord, Erpressung, gewerbsmaßige Hehlerei und Bandenhehlerei, bestimmte Straftaten gegen das Waffengesetz, das Außenwirtschaftsgesetz, das Betaubungsmittelgesetz sowie das Auslander- und Asylverfahrensgesetz.

44 1993 wurden in der Bundesrepublik 3964 Genehmigungen erteilt, BT-Drs. 12/8306. Im selben Zeitraum wurden in der USA lediglich 821 Abhorgenehmigungen erteilt, vgl. Bottger/Pfeiffer, Der Lauschangriff in Deutschland und den USA, ZRP 1994, 7 f.

45 Nicht gemeint ist hier das Abhoren eines Raumes mit Hilfe eines entsprechend manipulierten Telephons, vgl dazu naher Mann/Muller, Praventiver Lauschangriff via Telephon?, ZRP 1995, 180 ff.

46 Fruher Zollkriminalinstitut, BGBl. 1992 I 1222.

47 Arndt, Die Fernmeldekontrolle im Verbrechensbekampfungsgesetz, NJW 1995, 169 ff.; Riegel, Der Quantensprung des Gesetzes zu Art. 10 GG, ZRP 1995, 176 ff.

48 Angaben uber die Anzahl der von den Geheimdiensten abgehorten Anschlusse sind nicht bekannt.

Im Rahmen der sogenannten *strategischen Kontrolle* darf darüber hinaus der BND den internationalen, nicht leitungsgebundenen Fernmeldeverkehr abhören, § 3 G 10.[49] Strategische Kontrolle bedeutet, daß der Fernmeldeverkehr rechnergestützt nach bestimmten Suchbegriffen abgehört wird, § 3 Abs. 2 G 10. Diese Suchbegriffe dürfen keine Identifizierungsmerkmale enthalten, die zu einer gezielten Erfassung bestimmter Fernmeldeanschlüsse führen.[50] Diese Einschränkung gilt allerdings nur für Anschlüsse deutscher Staatsangehöriger oder von Gesellschaften mit Sitz im Ausland mit überwiegend deutscher Beteiligung, näher § 3 Abs. 2 G 10.[51] Die durch Maßnahmen der strategischen Kontrolle gewonnenen personenbezogenen Daten dürfen nach einer die bisherige gesetzliche Regelung einschränkenden einstweiligen Anordnung des BVerfG nur verwendet und übermittelt werden, »wenn *bestimmte Tatsachen den Verdacht* begründen, daß jemand eine in der Vorschrift genannte Straftat plant, begeht oder begangen hat.«[52]

Die Abhörmaßnahme wird angeordnet durch die jeweils zuständigen Landes- bzw. Bundesminister, § 5 Abs. 1 G 10, und unterliegt der Kontrolle durch eine parlamentarische Kontrollkommission, § 9 G 10. Dem Betroffenen ist die Beschränkung mitzuteilen, sobald eine Gefahrdung des Zwecks der Beschränkung der Verwendung ausgeschlossen werden kann. § 3 Abs. 8 G 10.[53]

Nur zur Vollständigkeit soll hier außerdem noch auf die ebenfalls das Fernmeldegeheimnis berührende Auskunftspflicht *im strafgerichtlichen Untersuchungsverfahren* nach *§ 12 FAG* hingewiesen werden. Danach kann der Richter und bei Gefahr im Verzug auch die Staatsanwaltschaft in strafgerichtlichen Untersuchungen *Auskunft* uber den an den Beschuldigten gerichteten und von ihm ausgehenden Fernmeldeverkehr verlangen.

Einschränkungen wie etwa einen in § 100a StPO enthaltenen Katalog schwerwiegender Straftaten, die diese Befugnis auslösen, enthält § 12 FAG nicht.[54] Allgemein wird auf der Grundlage dieser Vorschrift auch die Auskunft über betriebsbedingt gespeicherte Daten für zulässig gehalten und zwar auch fur den in der Vergangenheit bereits abgewickelten Fernmeldeverkehr.[55] Mit der Umstellung auf digitale Vermittlungstechniken haben sich Art und Umfang der den Betreibern zur Verfügung stehenden Daten erheblich vermehrt,[56] so daß die 1927 ursprünglich nur als Komplementarvorschrift zur Postbeschlagnahme gedachte Vorschrift nunmehr neue Bedeutung erhalten hat, ohne selbst ausreichende verfahrensrechtliche Beschränkungen zu bieten.[57]

Die Befugnis, den Fernmeldeverkehr zu überwachen, bedeutet seinem Wortsinn nach zunächst nur Kenntnisnahme der Kommunikation, beinhaltet aber auch das Moment des kontrollierenden Beobachtens und damit auch das *Entschlüsseln* verschlüsselter Fernmeldekommunikation.[58] Insofern besteht kein Unterschied zu sonst sprachlich codierten Nachrichten wie beispielsweise die Verwendung einer Fremdsprache, die ebenfalls von Sicherheitsbehörden übersetzt und damit entschlüsselt werden darf, wenn die gesetzlichen Voraussetzungen des Abhörens vorliegen. Allerdings kann das erfolgreiche Abhören verschlüsselter Kommunikation die Si-

49 Naher Arndt (Fn. 47), NJW 1995, 169 ff.; Riegel (Fn. 47), ZRP 1995, 176 ff.
Ziel ist die Gewinnung von Erkenntnissen uber die Gefahr eines bewaffneten Angriffs auf die Bundesrepublik, aber auch uber den internationalen Terrorismus, Rauschgiftschmuggel nach Deutschland, den illegalen Handel mit Kriegswaffen und uber internationale Geldwasche- und Geldfalschungsaktivitaten. Zur Abwehr eines bewaffneten Angriffs durfen auch leitungsgebundene Fernmeldeverkehrsbeziehungen abgehort werden, § 3 Abs. 1 Satz 3 G 10.

50 Nach BVerfG EuGRZ 1995, 355, gehen einige Datenschutzbeauftragte »von Zahlen in sechsstelliger Hohe taglich fur die rechnergestützte Überwachung und von taglich viertausend aufgezeichneten Gesprachen aus«.

51 Zur globalen Geltung des Art. 10 Abs. 1 GG Gropl, Das Fernmeldegeheimnis des Art. 10 GG vor dem Hintergrund des internationalen Aufklarungsauftrages des Bundesnachrichtendienstes, ZRP 1995, 13 ff.; Arndt (Fn. 47), NJW 1995, 169 ff.

52 § 3 Abs. 3 bis 5 G 10, BVerfG EuGRZ 1995, 353; Hervorhebung durch mich, J. B.

53 Zu den Ausnahmen § 3 Abs. 8 Satz 2 G 10; dazu kritisch Riegel (Fn. 47), ZRP 1995, 179.

54 Kritisch Bar (Fn. 8), S. 352 mwN.

55 OLG Koln NJW 1970, 1857; Bar (Fn. 8), S. 353 mwN.

56 Nach § 6 TDSV ist eine Loschung der Verbindungsdaten spatestens nach 80 Tagen vorgesehen. Langstens bis zu diesem Zeitraum sind diese Daten technisch zugriffsfahig.

57 Kritisch auch Bar (Fn. 8), S. 352 ff. mwN.; Walz, Datenschutz und Telekommunikation II, CR 1990, 140 ff.

58 Naher Bizer (Fn. 16), S. 193.

cherheitsbehörde vor erhebliche Schwierigkeiten stellen. Das Knacken von Verschlüsselungsverfahren kann (zeit)aufwendig sein und muß nicht immer erfolgreich verlaufen, zumal wenn starke Verschlüsselungsverfahren mit relativ großer Schlüssellänge verwendet werden. Überwachungsmaßnahmen verschlüsselter Kommunikation könnten den Diensten allerdings erheblich erleichtert werden, wenn ihnen von den Netzbetreibern und Dienstleistungsanbietern die Kommunikation unverschlüsselt zur Verfügung gestellt werden müßte.

6. Mitwirkungspflichten der Netzbetreiber

Tatsächlich sind die Betreiber öffentlicher Fernmeldeanlagen[59] auf Grund der Anordnung einer Abhörmaßnahme rechtlich verpflichtet, die Überwachung und Aufzeichnung des Fernmeldeverkehrs zu ermöglichen.

Nach § 100b Abs. 3 StPO hat jeder »Betreiber von Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind«, also auch private Betreiber[60], auf Grund der (richterlichen oder bei Gefahr im Verzug der staatsanwaltlichen) Anordnung »die Überwachung und Aufzeichnung des Fernmeldeverkehrs zu ermöglichen«.[61]
Eine entsprechende Mitwirkungspflicht gilt nach § 1 Abs. 2 Satz 2 G 10 auch gegenüber den Geheimdiensten sowie in Verbindung mit § 39 Abs. 5 AWG auch gegenüber dem Zollkriminalamt. Nach § 1 Abs. 2 Satz 3 G 10 haben die Betreiber sogar das für die Durchführung der Anordnung erforderliche Personal »bereitzuhalten«.

Komplementär zu dieser Mitwirkungspflicht verpflichtet der im Rahmen der Novelle zur Postreform II in das FAG aufgenommene § 10a Satz 1 FAG die Betreiber von Fernmeldeanlagen, die Gestaltung der technischen Einrichtungen zur Umsetzung von Überwachungsmaßnahmen des Fernmeldeverkehrs nach dem G 10, § 100a StPO und § 39 AWG »im Einvernehmen mit dem Bundesministerium für Post und Telekommunikation festzulegen«. Darüber hinaus enthält § 10b Satz 2 FAG eine Verordnungsermächtigung für die Bundesregierung, »die technische Umsetzung von Überwachungsmaßnahmen in den Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind, zu regeln.« Diese Ermächtigung hat die Bundesregierung mittlerweile durch Erlaß der Fernmeldeüberwachungsverordnung (FÜV) umgesetzt.[62]
Diese Verordnung ist in mehrfacher Hinsicht verfassungsrechtlich bedenklich.

Sie verpflichtet die Betreiber, Rufnummern, Leistungsmerkmale und andere Informationen über die näheren Umstände eines Fernmeldegesprächs dem Bedarfsträger[63] bereitzustellen, und zwar auch dann, »wenn keine Verbindung zustande gekommen ist«, § 3 Abs. 2 Nr. 1, 2 FÜV.
Die Betreiber haben nicht nur die über Mobilfunk geführten Gespräche bereitzustellen, sondern nach § 3 Nr. 4 FÜV auch die »Funkzellen, über die die Verbindung abgewickelt wird«. Damit wird der gesetzlich definierte Rahmen einer bloßen Überwachung des Fernmeldeverkehrs überschritten, weil über die Funkzellen des Mobilfunks ein Bewegungsprofil des Teilnehmers während der Dauer des Gesprächs erstellt werden kann. Zudem ist die Ermächtigungsgrundlage des § 10b Satz 2 FAG keinesfalls eine ausreichend bestimmte Ermächtigungsgrundlage für die Erstellung von Bewegungsprofilen.

59 Gemeint sind Anlagen, die für den öffentlichen Verkehr bestimmt sind.
60 Rutter, Die Telekommunikationsdienstleistungsfreiheit und ihre rechtlichen Rahmenbedingungen, jurpc 1991, 1362; Walz (Fn. 57), CR 1990, 139.
61 In der Fassung des Art. 12 Nr. 24 des PTNeuOG vom 14. September 1994, BGBl. I, S. 2325.
62 Vom 18. Mai 1995, BGBl. I, S. 722.
63 Bedarfsträger sind die Sicherheitsbehörden, die nach § 100a StPO, § 39 AWG und dem G 10 zum Überwachen und Aufzeichnen des Fernmeldeverkehrs berechtigt sind, vgl. § 2 Nr. 3 FÜV.

Ferner muß der Betreiber den zu überwachenden Fernmeldeverkehr für die gesamte Dauer der Maßnahme dem Bedarfsträger an einer festgelegten technischen Schnittstelle bereitstellen, § 8 Abs. 1 FÜV, damit er zeitgleich an den Bedarfstrager in dessen Räumlichkeiten übermittelt werden kann, § 4 Abs. 3, § 5 Abs. 2, § 8 Abs. 2 FÜV. Diese technische Gestaltung begünstigt einen mißbrauchsfördernden »Abfluß« an Daten durch die Bedarfsträger eher als daß sie ihn durch eine zusätzliche Kontrolle durch den Betreiber verhindert (Vier-Augen-Kontrolle), zumal der Betreiber zu einer umfassenden Vertraulichkeit verpflichtet ist, § 12 FÜV. Darüber hinaus treibt diese Regelung den Betreiber in das Dilemma, dem Bedarfsträger möglicherweise mehr Daten bereitzustellen, als er nach »Art und Umfang« der Abhöranordnung gegenüber seinem Kunden berechtigt ist, und damit das Fernmeldegeheimnis zu verletzen.

Schließlich ist der Betreiber nach § 8 Abs. 4 FÜV verpflichtet, die ihm zur Übermittlung anvertrauten Nachrichten, die er »durch technische Maßnahmen« (beispielsweise eine Verschlüsselung) gegen die unbefugte Kenntnisnahme durch Dritte geschützt hat, dem Bedarfsträger *ungeschützt* an der oben erwähnten Schnittstelle nach § 8 FÜV bereitzustellen. Diese Bereitstellungspflicht ist rechtlich zwar durch die gesetzlich angeordnete Mitwirkungspflicht der Betreiber gedeckt, weil diese das Überwachen und Aufzeichnen des Fernmeldeverkehrs ermöglichen müssen. Mehr als fraglich ist jedoch, ob die Verordnungsermächtigung des § 10b Satz 2 FAG nach Art. 80 Abs. 1 Satz 2 GG ausreichend bestimmt ist, da diese die Bundesregierung lediglich zur Regelung der »technischen Umsetzung von Überwachungsmaßnahmen« ermächtigt.

7. Individualverschlüsselung

Neben der Sicherung der Vertraulichkeit durch den Anlagenbetreiber könnten die Teilnehmer ihre Telekommunikation aber auch durch betreiberunabhängige Kryptoverfahren sichern. Kontrovers ist jedoch die Frage, welche Zugriffsmöglichkeiten die Sicherheitsbehörden de lege lata haben und vor allem de lege ferenda haben können, wenn die Teilnehmer selbst ihre Telekommunikation mit eigenen Kryptoalgorithmen verschlüsseln.[64] Dabei sind zwei Fallkonstellationen zu unterscheiden, nämlich Verschlüsselungssysteme, deren Erzeugung ausschließlich in der Hand der Teilnehmer liegt, und solche, deren Erzeugung von Instanzen einer Schlüsselverwaltung übernommen wird, die als Dienstleistung angeboten werden.[65]

Im ersten Fall sind die Dienste mehr oder weniger ohnmächtig: Sie können die verschlüsselten Nachrichten »knacken«, was zeitaufwendig oder in Abhängigkeit von der »Härte« des Algorithmus auch erfolglos sein kann. Eine Beschlagnahme der Entschlüsselungsschlüssel ist zwar theoretisch möglich, wird aber durch technisch-organisatorische Schutzmaßnahmen von den Teilnehmern unterlaufen werden können, zumal sie als Beschuldigte nicht einmal gegenüber den Strafverfolgungsbehörden zur Mitwirkung gezwungen werden können. Schließlich würde eine Beschlagnahme das Ziel der Überwachungsmaßnahme, nämlich die Kommunikation gerade von den Teilnehmern unbemerkt abhören zu können, konterkariert.

Einfacher stellt sich aus der Sicht der Sicherheitsbehörden die zweite Konstellation dar, in der ein Dienstleistungsanbieter Kryptoverfahren öffentlich anbietet, mit deren Hilfe Teilnehmer ihre Nachrichten selbst verschlüsseln können. Hier könnten, so die Überlegung, aufwendige Versuche, Verschlüsselungsverfahren zu knacken,

64 Die zweite Fragestellung bildet den Kern der Diskussion uber die »Kryptogesetzgebung«.

65 Beispielhaft sind offentliche Schlusselsysteme, die auf asymmetrischen Schlusselverfahren wie dem RSA beruhen. Zu den technischen, organisatorischen und rechtlichen Voraussetzungen der Sicherungsinfrastruktur vgl. die Beitrage in: Hammer (Fn. 16).

vermieden werden, wenn die Sicherheitsbehörden bei den Dienstleistungsanbietern Zugriff auf die Schlüsselduplikate nehmen, um mit ihrer Hilfe die Nachrichten unbemerkt von den Kommunikationspartnern zu dechiffrieren.[66]
Diese Alternative mitsamt ihren sicherheitspolitischen Implikationen spiegelt sich auch in der Diskussion einer ISDN-Richtlinie der Europäischen Union wider. Noch nach dem ersten Entwurf dieser Richtlinie galt eine Verpflichtung, »eine Verschlüsselung von Endgerät zu Endgerät anzubieten«.[67] In der nunmehr geänderten Fassung von 1994 ist aus sicherheitspolitisch naheliegenden Gründen nur noch allgemein von Verschlüsselungsmöglichkeiten die Rede.[68]

7.1 Geltende Rechtslage

In Deutschland sind jedoch nach geltendem Recht die Anbieter von Verschlüsselungsverfahren rechtlich nicht verpflichtet, Schlüsselduplikate ihrer Kunden aufzubewahren und für Zwecke der Sicherheitsbehörden zur Verfügung zu halten.
Die gesetzlich verankerte Mitwirkungspflicht, Staatsanwaltschaft und Polizei nach § 100b Abs. 3 StPO sowie den Diensten nach § 1 Abs. 2 Satz 2 G 10 das Abhören des Fernmeldeverkehrs zu ermöglichen, ist auf die *Betreiber von Fernmeldeanlagen* beschränkt. Ebenfalls nur die Betreiber von Fernmeldeanlagen sind verpflichtet, die Gestaltung der technischen Einrichtungen zur Umsetzung von Überwachungsmaßnahmen des Fernmeldeverkehrs im Einvernehmen mit dem Bundesminister für Post und Telekommunikation festzulegen, § 10b Satz 1 FAG. Verschlüsselungsverfahren sind jedoch keine Fernmeldeanlagen, mit denen Nachrichten übertragen werden, sondern lediglich ein Mittel zur Verfremdung von Daten *vor* ihrer Übermittlung.[69] Aus diesem Grund besteht selbst dann keine Mitwirkungspflicht, Schlüsselduplikate aufzubewahren, wenn neben der Übermittlungsleistung von dem Betreiber gleichzeitig auch ein Verschlüsselungsverfahren angeboten wird, das den Teilnehmern unabhängig vom Übertragungsdienst selbständig das Verschlüsseln von Endgerät zu Endgerät ermöglicht. Ebensowenig wie das Schreiben eines Briefes mit Geheimtinte Bestandteil des Postverkehrs ist, ist das Chiffrieren von Sprache, Bildern und Dateien Bestandteil des Fernmeldeverkehrs.
Eine anderslautende Vorschrift besteht jedoch nunmehr mit § 8 Abs. 4 Satz 2 FÜV. Danach muß der Betreiber einer Fernmeldeanlage, falls er *dem Teilnehmer* Verschlüsselungsmöglichkeiten für die Nachrichten bereitstellt, dem Bedarfsträger die entschlüsselten Nachrichten an der Schnittstelle oder die für eine Entschlüsselung erforderlichen Informationen zeitgerecht zur Verfügung stellen. Allerdings ist diese Verpflichtung verfassungswidrig: Sie verletzt die unternehmerische Freiheit des Betreibers, weil die Bereitstellungspflicht keine ausreichende Rechtsgrundlage weder in der bereits erwähnten Verordnungsermächtigung des § 10b Satz 2 FAG (Art. 80 Abs. 1 Satz 2 GG) hat noch sich eine derartige Verpflichtung aus der gesetzlichen Mitwirkungspflicht der Betreiber ergibt, da sich diese lediglich auf Fernmeldeanlagen, nicht aber auf davon unabhängige Dienstleistungen der Nachrichtenverschlüsselung bezieht. Diese Verpflichtung der Betreiber verletzt auch das Fernmeldege-

66 Naher dazu Bizer (Fn. 16), S. 195 ff.
67 Art. 8 Abs. 2 der Richtlinie zum Schutz personenbezogener Daten und der Privatsphäre in digitalen Telekommunikationsnetzen, insbesondere im dienstintegrierenden digitalen Telekommunikationsnetz (ISDN) und digitalen Mobilfunk, vom 11. 3. 1992, KOM (90) 314 – SYN 288.
68 Art. 4 der ISDN-Richtlinie, abgedruckt bei Rihaczek, DuD 1994, 499, und ders. S. 491.
69 Bizer (Fn. 16), S. 199.

heimnis der Teilnehmer, die zwar im angeordneten Umfang das Überwachen ihres Fernmeldeverkehrs dulden müssen, nicht aber, daß ihre Verschlüsselungsschlüssel, die auch zu anderen Zwecken als zur Sicherung ihres Fernmeldegeheimnisses verwendet werden können, offengelegt werden müssen.

Denkbar wäre allenfalls, daß die Anbieter von Verschlüsselungsverfahren von sich aus, freiwillig, Schlüsselduplikate ihrer Kunden aufbewahren. Datenschutzrechtlich ist dies jedoch nur mit Einwilligung des betroffenen Schlüsselinhabers zulässig. Dies ergibt sich aus § 3 Abs. 1 TDSV/UDSV, wenn das Verschlüsselungsverfahren Bestandteil der Übermittlungsdienstleistung ist, aus § 4 Abs. 1 BDSG, wenn es selbständig angeboten wird.[70]

Die Annahme, Kunden von Verschlüsselungsverfahren hätten ein Interesse, Schlüsselduplikate von dem Anbieter des Verschlüsselungsverfahren aufbewahren zu lassen, ist wegen der Mißbrauchsgefahren wenig wahrscheinlich. Regelmäßig wird sich das Sicherungsinteresse eines Kunden auf den Verlust eines Entschlüsselungsschlüssels beschränken, mit dem er selbst zum Zwecke der Datensicherung verschlüsselt *gespeicherte* Daten entschlüsseln kann. Das Risiko, verschlüsselt *übermittelte* Nachricht nicht entschlüsseln zu können, weil der Entschlüsselungsschlüssel verloren gegangen ist, läßt sich hingegen mit der Bitte, die Übermittlung zu wiederholen, einfacher reduzieren, ohne die Vertraulichkeit der Nachrichtenübermittlung durch eine Aufbewahrung von Schlüsselduplikaten durch den Dienstleistungsanbieter gefährden zu müssen.

7.2 Handlungsoptionen des Gesetzgebers

Da nach geltendem Recht der Zugriff auf Schlüsselduplikate rechtlich auf den Fall einer freiwilligen Aufbewahrung durch den Dienstleistungsanbieter mit Einverständnis des Schlüsselinhabers beschränkt und damit praktisch ausgeschlossen ist, stellt sich die Frage, welche Möglichkeiten der Gesetzgeber hat, den Interessen der Sicherheitsbehörden nachzugeben.[71] Dabei stehen neben der Option, die Verwendung von Kryptoverfahren ohne Einschränkung zu liberalisieren, zwei weitere Möglichkeiten zur Diskussion, die Gegenstand einer bislang kaum öffentlich geführten »Kryptokontroverse« sind.[72] Der Gesetzgeber könnte einmal die Verwendung von Verschlüsselungsverfahren verbieten, zum anderen aber sie nach Anforderungen lizenzieren, die den Sicherheitsbehörden den Zugriff auf Schlüsselduplikate erlauben.

Beide Optionen sind mit Grundrechtseingriffen verbunden und bedürfen daher einer ausreichenden gesetzlichen Grundlage. Betroffen ist zunächst das Fernmelde-

70 Naher Bizer (Fn. 16), S. 195 ff.

71 Die Einschrankung der individuellen Verschlusselungsoption bildet den eigentlichen Hintergrund der derzeitigen Prufung einer Kryptogesetzgebung, vgl. Antwort der Bundesregierung, BT-Drs. 13/1676. Außerdem ist die Debatte mit der noch nicht gelosten Frage der europaweiten Liberalisierung von Kryptoverfahren für zivile Zwecke verbunden.
Daruber hinaus konnte eine restriktive Kryptogesetzgebung auch die Rechtssicherheit beeintrachtigen, wenn nämlich die Sicherheitsbehorden mit dem Zugriff auf die Verschlusselungsschlussel eines asymmetrischen Verfahrens wie RSA gleichzeitig auch die geheimen Signierschlussel besitzen wurden, mit denen Teilnehmer die Authentizitat und Urheberschaft digitaler Dokumente sichern. Naher dazu mwN. Bizer (Fn. 16), S. 212 ff.; ders., Das Schriftformprinzip im Rahmen rechtsverbindlicher Telekooperation, DuD 1992, 175.

72 Vgl. zum folgenden ausfuhrlich Bizer (Fn. 16); und die Kontroverse zwischen Bizer und Heuser in: Kubicek/Muller/Neumann/Raubold/Roßnagel (Hrsg.), Jahrbuch Telekommunikation und Gesellschaft, 1995, 214 ff. und S. 224 ff. (Heuser ist Abteilungsleiter im BSI); außerdem Pordesch, Wieviel Sicherheit ist erlaubt? in: Wechselwirkung Juni/Juli 1995, 48 f.; Rihaczek (Fn. 11), DuD 1993, 220 ff.

geheimnis nach Art. 10 Abs. 1 GG der Teilnehmer, denen untersagt wird, ihre individuelle Kommunikation selbst zu schützen, bzw. denen vorgeschrieben wird, nur zugelassene Verfahren zum Schutz ihrer Nachrichten im Fernmeldeverkehr zu verwenden. Zum anderen betreffen beide Optionen die unternehmerische Handlungsfreiheit nach Art. 2 Abs. 1 GG[73] bzw. die Berufsausübungsfreiheit der Hersteller und Anbieter von Verschlüsselungsverfahren nach Art. 12 Abs. 1 GG, die in ihrer Marktfreiheit durch ein Verbot von oder die Beschränkung auf lizenzierte Verschlüsselungsverfahren behindert werden. Verfassungsrechtlich gerechtfertigt sind die Eingriffe nur, wenn sie den Anforderungen des Verhältnismäßigkeitsgrundsatzes genügen, d. h. ein verfassungsrechtlich legitimes Ziel verfolgen und zur Erfüllung dieses Ziels geeignet, erforderlich und zumutbar sind.[74]

7.2.1 Verbot

Mit dem Verbot von Kryptoverfahren soll den Sicherheitsbehörden das Abhören des Fernmeldeverkehrs im Rahmen ihrer gesetzlichen Befugnisse erleichtert werden. Dieses Ziel ist verfassungsrechtlich legitim, soweit mit dem Überwachen und Aufzeichnen des Fernmeldeverkehrs auch selbst verfassungsrechtlich zulässige Ziele verfolgt werden.[75]

Faktisch würde ein Verbot von Verschlüsselungsverfahren bewirken, daß flächendeckend allen Grundrechtsträgern verboten werden würde, ihr Fernmeldegeheimnis mit technischen Hilfsmitteln autonom gegen den Zugriff Dritter zu sichern, um in wenigen Einzelfällen das staatliche Abhören zu ermöglichen. Problematisch an einem solchen Totalverbot ist vor allem seine »präventive« Zielrichtung, die individuelle Sicherung des grundrechtlich geschützten Fernmeldegeheimnisses mit technischen Mitteln von vorneherein als »verdächtig« zu diskreditieren, indem es unter einen Ausübungsvorbehalt gestellt wird.

Ein Verbot wäre auch unter den historischen Entstehungsbedingungen des Fernmeldegeheimnisses verhängnisvoll. Unter den Bedingungen einer technisch vermittelten Kommunikation ermöglichen öffentliche Schlüsselsysteme den Teilnehmern erstmals in der Geschichte des Fernmeldegeheimnisses, den Verlust an persönlicher Verfügungsmöglichkeit über die Vertraulichkeit ihrer Nachricht durch die Verwendung einer End-zu-Ende Verschlüsselung auszugleichen und damit ihr Fernmeldegeheimnis technisch selbst zu sichern.[76] Mit einer derartigen Schutzmöglichkeit wird das Fernmeldegeheimnis wieder auf seinen ursprünglichen Grund zurückgeführt, nämlich ein *individuelles* Schutzrecht gegen staatliche Eingriffe in die Vertraulichkeit der Kommunikation zu sein. Ein Verbot von Kryptoverfahren unter den heutigen Bedingungen der Telekommunikation würde jedoch das Fernmeldegeheimnis just in dem Moment preisgeben, in dem sich die Teilnehmer von den Schutzmöglichkeiten, die die Betreiber von Fernmeldeanlagen anbieten, emanzipieren können.

Zweifelhaft ist hier insbesondere die *Eignung* eines Kryptoverbots, denn praktisch kann es ohne großen Aufwand von den Teilnehmern unterlaufen werden. Auch trotz eines Verbotes können die für das Verschlüsseln erforderlichen Schlüssel mit einem gewissen Aufwand erworben oder selbst hergestellt und eingesetzt werden.

73 BVerfGE 50, 290, 366; 65, 196, 210.
74 Zum folgenden ausführlich Bizer (Fn. 16), S. 203 ff.
75 Zur verfassungsrechtlichen Bewertung des G 10 Gesetzes: BVerfGE 30, 1 ff. Der Frage kann hier nicht weiter nachgegangen werden.
76 Provet/GMD (Fn. 19), S. 218.

Ein Verbot von Kryptoverfahren würde lediglich das öffentliche Angebot von Verschlüsselungsdienstleistungen verhindern können. Es kann aber unterstellt werden, daß gerade die für die staatliche Überwachung interessanten und im Sinne der Sicherheitsbehörden gefährlichen oder verdächtigen Personen über die erforderlichen Mittel verfügen, um ihre Kommunikation ausreichend gegen staatlichen Zugriff zu schützen.[77] Sie könnten, wenngleich verbotswidrig, hochwertige Schlüsselverfahren verwenden oder aber andere Methoden der elektronischen Tarnung benutzen wie beispielsweise die der Steganographie.[78] Die einschlägigen Tätergruppen werden sich auch durch strafrechtliche Sanktionen nicht von der Verwendung auch aufwendiger Verschlüsselungsverfahren abhalten lassen, solange nur die Gewinnerzielungsmöglichkeiten ausreichend attraktiv sind.[79]

Selbst die Identifizierung »verdächtiger«, weil verbotswidrig verschlüsselter Kommunikation, ist kein ausreichender Sicherheitsgewinn. Zwar könnte das verbotswidrige Verschlüsseln straf- oder ordnungsrechtlich sanktioniert werden, jedoch müßten die verschlüsselten Geheimnisse, um deren Kenntnis es den Sicherheitsbehörden doch letztlich geht, erst entschlüsselt werden, bevor weitere Überwachungs- oder Verfolgungsmaßnahmen möglich wären. Müssen aber auch die verbotswidrig verschlüsselten Nachrichten erst entschlüsselt werden, dann kann ebensogut auf das Verbot verzichtet werden.

Selbst die Beschlagnahme verbotswidrig verwendeter Schlüssel bei den Verdächtigen nach § 94 Abs. 1 StPO im Rahmen der Straftatverfolgung[80] würde wenig weiterhelfen, denn gerade die Straftäter der einschlägigen Gruppen werden die erforderlichen Schlüssel löschen, nachdem sie ihre Nachrichten entschlüsselt und im Klartext zur Kenntnis genommen haben. Im übrigen wird ein Zugriff auf Schlüssel auch daran scheitern, daß der Inhaber als Beschuldigter einer Straftat aus Rechtsgründen nicht zur Mitwirkung an seiner Überführung gezwungen werden kann,[81] d. h. auch nicht zur Herausgabe seines Schlüssels oder der für den Zugriff auf die Chipkarte notwendigen PIN (Personal Identification Number).

7.2.2 Lizenzierung

Erhebliche verfassungsrechtliche Bedenken sprechen auch gegen das Verbot nicht staatlich lizenzierter Kryptoverfahren. Sinn und Zweck solcher Lizenzierungsverfahren ist es, im Interesse der Inneren Sicherheit Teilnehmer nur solche Kryptoverfahren verwenden zu lassen, die den Sicherheitsbehörden Zugriff auf die Schlüssel zum Dechiffrieren der Nachrichten ermöglichen.[82]

Ein solches Modell ist der in den USA diskutierte Clipper-Chip, bei dem die Schlüs-

77 So auch Seidel, Signaturverfahren und elektronische Dokumente, in: Herda/Seidel/Struif, 1992, S. 74 f., 90. In anderem Zusammenhang auch Pfeiffer, Telefongespräche im Visier der elektronischen Rasterfahndung, ZRP 1994, 254; dieses Risiko wird auch von Heuser (Fn. 72), S. 227, gesehen.

78 Z. B. Moller/Pfitzmann/Stierand, Rechnergestützte Steganographie, DuD 1994, 318: Digitale Datenübertragung (bspw. im ISDN) ermöglicht, im Rauschen der übertragenen Hintergrundgeräusche Daten »zu verstecken«.

79 Positiver beurteilt Heuser (Fn. 72), S. 227, einen möglichen Abschreckungseffekt, denn ein Verstoß bedeute immerhin einen »Schritt in die offene Illegalität«.

80 Beschlagnahmt werden kann nach § 94 StPO als Gegenstand nur der Datenträger, vgl. ausführlich Bar (Fn. 8), S. 240 ff., 248 f.; Kleinknecht/Meyer, StPO 1992, § 94, Rn. 4; Rudolphi in: SK-StPO 1994, § 94, Rn. 11; jedoch können auf einem Datenträger gespeicherte Daten nach § 94 Abs. 1 StPO durch Kopieren sichergestellt werden, näher zu den Voraussetzungen Bar (Fn. 8), S. 248 ff., 266 ff.

81 Rudolphi (Fn. 80), § 95, Rdnr. 5; Kleinknecht/Meyer (Fn. 80), § 95 Rdnr. 5.

82 Aus diesem Grund werden derartige Verfahren auch als Escrow-Systeme bezeichnet.

sel treuhänderisch von staatlichen Stellen verwaltet werden sollen.[83] Das technisch-organisatorische Konzept sieht vor, daß sich die Sicherheitsbehörden auf der Grundlage eines richterlichen Beschlusses über eine spezielle, in dem verschlüsselten Dokument enthaltene Kennung den Schlüssel zum Dechiffrieren der Nachricht bei den Treuhändern verschaffen können.[84]

Unbestritten besteht der Vorteil derartiger Lizenzierungsverfahren darin, daß der Einzelne seine Kommunikation zumindest gegen private Eingriffe schützen kann. Andererseits sind seine Schutzmaßnahmen nur solange wirksam, wie die Verwaltung der Schlüssel nicht kompromittiert ist. Dieses Risiko wird aber durch die Verpflichtung der Anbieter, Schlüsselduplikate aufzubewahren, erheblich erhöht. Mit wachsendem Sicherungsbedürfnis der Teilnehmer werden sich die Instanzen, die über die Schlüsselduplikate verfügen, zu höchst sicherheitsempfindlichen Stellen entwickeln. Insider könnten einem beträchtlichen Bestechungsdruck ausgesetzt sein, was wiederum das Vertrauen in die Vertrauenswürdigkeit zugelassener Verschlüsselungsverfahren nicht stärken wird. Dieses Risiko könnte zwar durch organisatorische und technische Vorkehrungen in der Schlüsselverwaltung reduziert werden,[85] jedoch werden sie gegenüber wirtschaftlich oder ideell motivierten Tätern nur einen bedingten Schutz bieten können. Welche Bank, welcher Autokonzern, welche Entwicklungsfirma würde schließlich die Übermittlung von Betriebs- und Geschäftsgeheimnissen mit einem Verschlüsselungsverfahren sichern wollen, auf dessen Schlüsselverwaltung Externe direkt oder indirekt Zugriff haben können? Schließlich wäre die Aufbewahrung von Schlüsselduplikaten auch unter dem Gesichtspunkt der Kontrolle der freien Kommunikation der Bürger und der politischen Willensbildung problematisch, denn die zuständigen Instanzen der Schlüsselverwaltung könnten letztlich die kommunikativen Prozesse innerhalb der Gesellschaft kontrollieren.

Das Lizenzierungsmodell ist zudem auch datenschutzrechtlich problematisch, weil es voraussetzt, daß die Anbieter von Kryptoverfahren die geheimen Verschlüsselungsschlüssel ihrer Kunden allein nur für den Fall aufbewahren, daß sie möglicherweise in der Zukunft von den Sicherheitsbehörden benötigt werden könnten, ohne daß heute nähere Verdachtsmomente die Speicherung rechtfertigen müßten. Eine flächendeckende Speicherungspflicht »zu unbestimmten oder noch nicht bestimmbaren Zwecken« steht aber im Widerspruch zum Verbot der »Vorratshaltung personenbezogener Daten.«[86]

Bemerkenswert in diesem Zusammenhang ist die Einschätzung von Bundesforschungsminister J. Rüttgers (CDU). Seiner Auffassung nach lehrt die Erfahrung,

> »daß jede Abhörmöglichkeit für öffentliche Stellen innerhalb kurzer Zeit auch von nichtautorisierten Personen genutzt werden kann. Übertragen auf neue Infonetze bedeutet dies, daß ein Abhorprivileg für öffentliche Stellen im Zweifel nicht eingeführt werden sollte.«[87]

Auch das Lizenzierungsmodell ist mit dem Makel belastet, die Ausübung des Fern-

83 Naher Rueppel (Fn. 23), S. 183 ff. Zu fruheren Uberlegungen Rihaczek (Fn. 11), DuD 1987, 240 ff. Zu einem europaweiten Vorschlag: Heuser, Grenzuberschreitende Verschlusselung und nationale Souveranitat: ein Losungsvorschlag, in: Horster (Hrsg), Trust Center 1995, 227 ff.

84 Besondere Implikation dieses Verfahrens ist, daß der einmalige Zugriff auf die Schlussel sowohl das Entschlusseln vergangener als auch zukunftiger Verschlusselungen ermoglicht. Zu einem technischen Losungsvorschlag, der ein unbeschranktes Abhoren durch ein »Zeitabhangiges Key Escrowing« losen will, Fox in: Horster (Hrsg) Trust Center 1995, 232 ff.

85 Im Clippers Chip Konzept ist vorgesehen, daß zum Berechnen eines geheimen Schlussels zwei Schlussel notwendig sind, die von zwei verschiedenen Personen verwaltet werden, vgl. Rueppel (Fn. 23), S. 191 ff

86 BVerfGE 65, 1 (46).

87 »Das Reprasentationsprinzip darf nicht ersetzt werden. Wie sich die Politik auf den Wandel von der Industrie- zur Informationsgesellschaft vorbereiten muß«, FR vom 12. September 1995, S. 18. Ebenso in: Bulletin der Bundesregierung vom 27. Juni 1995, Nr. 52, S. 471.

meldegeheimnisses staatlich zu lizenzieren und damit den grundrechtlichen Schutz des Fernmeldegeheimnisses in eine vorbeugende Offenbarungspflicht zu verkehren: Das Fernmeldegeheimnis wäre zwar durch staatlich lizenzierte Kryptoverfahren gegen den Zugriff Dritter geschützt, aber um den Preis der Zugriffsmöglichkeit der staatlichen Sicherheitsbehörden, gegen das es doch »historisch und aktuell«[88] schützen soll.

Zwar könnte der Zugriff auf die Schlüsselduplikate verfahrensrechtlich und organisatorisch durch eine richterliche Anordnung und öffentliche Berichts- und Rechtfertigungspflichten, wie sie in den USA bei Abhörmaßnahmen vorgeschrieben sind,[89] beschränkt werden, gleichwohl ist diese Sicherung unzureichend, wenn einmal kompromittierte Schlüssel technisch das Entschlüsseln aller vergangenen und zukünftigen Nachrichten an den Empfänger ermöglichen.[90] Da der Betroffene nach deutschem Recht erst über die Abhörmaßnahmen informiert wird, wenn ihr Zweck nicht mehr gefährdet ist,[91] kann er die Vertraulichkeit seiner Kommunikation erst sehr viel später durch neue Schlüssel wieder herstellen. Aber auch in diesem Fall kann er nicht sicher sein, ob seine Schlüssel erneut diskreditiert sind. Das Lizenzierungsmodell wird daher zu einer prinzipiellen Verunsicherung der Kommunikation der Teilnehmer führen.

Schließlich ist das Lizenzierungsverfahren auch nicht geeignet, den Sicherheitsbehörden das Abhören der Kommunikation einschlägiger Kreise zu sichern. Straftäter, »Verfassungsfeinde« und andere Objekte staatlicher Überwachung werden ihre Kommunikation auch trotz Verbot mit nicht zugelassenen Kryptoverfahren sichern können.[92] Letztlich würde auch das Lizenzierungsmodell nur dazu führen, daß das Fernmeldegeheimnis normaler Teilnehmer dem staatlichen Zugriff preisgegeben ist, die einschlägige und eigentliche Klientel sich aber durch eigene Kryptoverfahren erfolgreich schützt.

Auch straf- oder ordnungsrechtliche Sanktionen werden gemessen am Sicherungsbedürfnis der Anwender keine ausreichende Abschreckungswirkung haben. Regelmäßig werden die Sanktionen niedriger sein als der immaterielle oder materielle Wert der vertraulichen, aber verbotenen Kommunikation. Unter dieser Voraussetzung ist auch ein staatliches Lizenzierungsverfahren von Kryptoverfahren unverhältnismäßig, weil es für die angestrebten Zwecke untauglich ist.

8. Rechtspolitischer Ausblick

Eine öffentliche Diskussion über die verschiedenen Handlungsoptionen einer Kryptogesetzgebung steht in Deutschland erst an den Anfängen, ist aber längst überfällig.[93] Möglicherweise wird sie durch den Entwurf einer Europaratsempfehlung angestoßen, der sich aus sicherheitspolitischen Gründen für eine Beschränkung des Besitzes, des Vertriebs und des Gebrauches kryptographischer Verfahren

88 BVerfGE 85, 386, 396.

89 Vgl. naher Bottger/Pfeiffer (Fn 44), ZRP 1994, 7ff.

90 Vgl. zum Clipper-Chip Modell Rueppel (Fn. 23), S. 196.

91 BVerfGE 30, 1, 31; § 101 Abs. 1 StPO; § 3 Abs. 8, § 5 Abs. 5 G 10.

92 So auch Rueppel (Fn. 23), S. 196; auf Abschreckung setzt Heuser (Fn. 72), S. 227.

93 Ausnahmen sind die Rezeption der US-amerikanischen Diskussion um den Clipper-Chip in Deutschland, bspw. S. Levy, Bericht vom Kryptokrieg, in DIE ZEIT vom 30. Dezember 1994, S. 54, G von Randow, Schlussel fur Abhorer, DIE ZEIT vom 24. September 1993, S 49. Offentlich ist die Diskussion allenfalls in den discussion groups des internets bzw. in den Kommentarspalten der diversen Computerzeitschriften.

ausspricht, ohne allerdings die Erfolglosigkeit solcher Maßnahmen zu diskutieren.[94]

Dabei dürfen zwei Gesichtspunkte nicht verkannt werden: Zum einen betrifft der Konflikt von Vertraulichkeitsschutz und Sicherheitsinteresse nicht nur allein das Verhältnis der privaten Kommunikation im Sinne einer individuellen Freiheitsentfaltung versus den Interessen der Inneren Sicherheit. Von der Kryptokontroverse und seiner politischen Lösung sind vielmehr auch wirtschaftliche Interessen, wiederum differenziert nach denen der Hersteller, der Dienstleistungsanbieter und der Anwender betroffen, die in Teilbereichen zu Interessenkonvergenzen zwischen einer kommunikationsrechtlich motivierten Interpretation des Fernmeldegeheimnisses als Voraussetzung für einen offenen politischen Willensbildungsprozeß und den Entfaltungsmöglichkeiten unternehmerischer Freiheit führen können.

Zum anderen wirft der hier vertretene und begründete Verzicht auf eine restriktive Kryptogesetzgebung unnachsichtig die Frage nach anderen Mitteln einer effektiven, auch vorbeugenden Verbrechensbekämpfung auf. Nicht von ungefähr stellen Befürworter des Lizenzierungsmodells, mit den Einwänden gegen eine restriktive Kryptogesetzgebung konfrontiert, die (listige) Alternative Kryptogesetzgebung versus Großer Lauschangriff. Ebensogut (oder – schlecht) könnte der Große Lauschangriff auch eine restriktive Kryptogesetzgebung entbehrlich machen. Gleichwohl sollten die Alternativen nicht falsch gestellt werden: Da eine restriktive Kryptogesetzgebung keinen Erfolg verspricht, ist sie kein geeignetes Mittel einer effektiven Verbrechensbekämpfung oder gar Vorfeldaufklärung.[95] Statt der Formulierung scheinbarer Alternativen tut vielmehr Transparenz über die Effektivität der bereits bislang durchgeführten Abhörmaßnahmen aller Sicherheitsdienste Not. Hier genügen nicht nur pauschale Behauptungen, sondern es sind nachprüfbare Zahlen über den betriebenen Aufwand an Technik und Personal, die abgehörten Personen und schließlich den Erfolg der Abhörmaßnahmen erforderlich. Doch das sind alte Fragen.

94 Die schwacher formulierte Empfehlung lautet in der Entwurfsfassung (Stand: 44. Plenarsitzung vom 29. Mai bis 2. Juni 1995): »Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary«. Die im Text zitierte Schlußfolgerung (conclusion) stammt aus der Erläuterung Nr. 175, Satz 3.

95 Nicht von ungefähr wird aus der Ministerialbürokratie der Satz kolportiert »Die Katze ist schon auf dem Baum«.