Fredrik Roggan

Moderne Telekommunikationsüberwachung: Eine kritische Bestandsaufnahme*

I. Bundesrechtliche TKÜ-Regelungen

Inzwischen müsse jeder Mensch bei einem Fernmeldekontakt mit dem Ausland mit einer Erfassung durch den Bundesnachrichtendienst rechnen, so sinngemäß das *Bundesverfassungsgericht* in seiner jüngsten Abhörentscheidung[1]. Aber auch bei inländischen Telekommunikationskontakten ist Überwachung längst Normalität und betrifft täglich tausende Individuen – auch Unverdächtige. »Zuwachs« haben zwar nicht nur die für strafprozessuale Datenerhebungen einschlägigen Vorschriften der §§ 100 a, b StPO erhalten. Auch im Außenwirtschaftsgesetz (AWG)[2] und im Gesetz zur Beschränkung von Artikel 10 des Grundgesetzes (G10)[3] finden sich Ermächtigungen zum heimlichen Überwachen des Telekommunikationsverkehrs[4]. Im Folgenden beschränkt sich die Darstellung aber auf die – auch in der Praxis vor allem bedeutsamen – strafprozessualen Regelungen.

1. Die Überwachung der Telekommunikation (TKÜ) nach den §§ 100 a, b StPO

Seit 1968 sieht die Strafprozeßordnung in § 100 a StPO eine Befugnis zur Überwachung und Aufzeichnung der Telekommunikation (TK) zu Zwecken der Strafverfolgung vor. Demnach dürfen entsprechende Maßnahmen angeordnet werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer[5] bestimmte Katalogtaten begangen, zu begehen versucht oder vorbereitet hat. Diesbezüglich reicht ein einfacher Tatverdacht[6]. Diese Verdachtsschwelle entspricht derjenigen bei anderen heimlichen Datenerhebungen, so etwa bei (strafverfolgenden) großen Lauschangriffen (§ 100 c I Nr. 3 StPO).

Entsprechend dem allgemeinen Verhältnismäßigkeitsgrundsatz darf eine TKÜ nur subsidiär durchgeführt werden. § 100 a S.1 a.E. StPO bestimmt insoweit, dass die

---

* Der Beitrag erscheint in erweiterter Form und mit weiterem Material als Kapitel im *Handbuch zum Recht der Inneren Sicherheit* (voraussichtlich Frühjahr 2003).

1 *BVerfGE* 100, 313 (377).

2 § 39 AWG.

3 § 1 I i.V.m. § 3 G10.

4 Eine knappe Übersicht hierzu findet sich etwa bei *Kloepfer* in: Holznagel/Nelles/Sokol, Die neue TKÜV, München 2002, S. 98 f.

5 Zur Kritik, dass die Strafprozeßordnung die Begriffe des »Täters« und »Teilnehmers« verwendet vgl. *Zaczyk*, StV 1993, 491.

6 KK-*Nack*, 4. Aufl., München 1999, § 100 a Rdnr. 24.

Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

§ 100 b StPO regelt die Einzelheiten der Anordnung einer TKÜ, insbesondere eine verfahrensmäßige Grundrechtssicherung in Gestalt des Richtervorbehalts. Nur bei Gefahr im Verzug ist auch die Staatsanwaltschaft anordnungsberechtigt. Inwieweit das Rechtsinstitut des Richtervorbehalts eine wirksame Begrenzung von heimlichen Datenerhebungen darstellt, ist an anderer Stelle eingehend dargestellt[7], weshalb auf die dortigen Ausführungen hier zu verweisen ist.

In § 100 b III StPO wird bestimmt, dass aufgrund einer richterlichen Anordnung jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, dem Richter, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Hilfsbeamten (§ 152 GVG) die Überwachung und Aufzeichnung der TK zu ermöglichen hat. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, ergibt sich aus § 88 des Telekommunikationsgesetzes (TKG) und der auf seiner Grundlage erlassenen Rechtsverordnung zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen. Aufgrund dieser Ermächtigung hat die Bundesregierung die Telekommunikations-Überwachungsverordnung (TKÜV) vom 22. Januar 2002 erlassen. Diesem Erlaß waren z.T. heftige rechtspolitische Diskussionen vorausgegangen. Das erscheint mit Blick auf die genannte Ermächtigung zum Verordnungserlaß (§ 100 b III S. 2 StPO i.V.m. § 88 II S. 2 TKG) jedenfalls verspätet, denn die Ermächtigung zur Telekommunikationsüberwachung datiert mitnichten aus dem Jahre 2002[8]. Als Erklärung für den »verspäteten Protest« darf gelten, dass vielen erst durch eine Rechtsverordnung ein gesetzlich vorgesehener Eingriff in Freiheitsrechte bewußt wird[9].

1.1. Überwachung der unmittelbaren Kommunikation

Das Fortschreiten der Möglichkeiten der modernen Kommunikation, auch unter Verwendung von elektronischen Medien, hat den Anwendungsbereich des § 100 a StPO in entsprechender Weise »mitwachsen« lassen. Längst findet der Austausch von menschlichen Gedankenerklärungen auch über Mobilfunknetze und insbesondere auch das Internet statt[10]. Im Zusammenhang mit den modernen Medien stellen sich damit Rechtsfragen, die bei traditioneller Kommunikation via (leitungsgebundenem) Telefonieren unbekannt waren.

Was unter Telekommunikation im Sinne des § 100 a StPO zu verstehen ist, ergibt sich aus § 3 Nr. 16 und 17 des Telekommunikationsgesetzes (TKG). Demnach handelt es sich dabei um den technischen Vorgang des Aussendens, Übermittelns und Emp-

---

7 *Asbrock*, KritV 1997, 255 ff.; *ders*., ZRP 1998, 17 ff.; *Paeffgen*, in: FS-Roxin (Hrsg.: Schünemann u.a.), Berlin 2001, S. 1308 ff.; zusammenfassend auch *Roggan*, Auf legalem Weg in einen Polizeistaat, Bonn 2000, S. 54 ff..

8 Vgl. dazu ausführlicher *Dix*, in: Polizei und Datenschutz (Hrsg.: Bäumler), Neuwied 1999, S. 257.

9 Auch zur Vorgeschichte vgl. *Kloepfer* (o. Fn. 4), S. 93 ff.

10 Zur wachsenden Bedeutung der Telekommunikationsüberwachung ausführlich *Bizer* in: Polizei und Datenschutz (Hrsg.: Bäumler), Neuwied 1999, S. 131 ff.

fangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels technischer Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können. Es bedarf an dieser Stelle keiner näheren Erörterung, dass demnach z.B. Gespräche über Mobilfunktelefone, der Fernschreib- und Telefaxverkehr von der Befugnis des § 100 a StPO erfaßt werden. Unproblematisch ist auch, daß der Austausch von e-mails, der in bestimmten Bereichen persönliche Gespräche und Briefverkehr – z. T. weitgehend – ersetzt hat, von der Regelung erfaßt wird[11].

1.2. Der Zugriff auf in Mailboxen zwischengespeicherte Informationen

Weniger unproblematisch und daher umstritten ist dagegen, ob auch auf Mailboxen von überwachten Anschlüssen gespeicherte Nachrichten dem Zugriff der Strafverfolgungsbehörden nach § 100 a StPO unterliegen. Mailbox-Dienste werden sowohl im Festnetz als auch im Mobilfunk-Verkehr als externe Anrufbeantworter häufig genutzt. Im Internet erfüllen sie für e-mails die Funktion eines »Briefkastens«, in dem die Daten bis zum Abruf durch den Berechtigten bereitgehalten werden.

Der *BGH* (Ermittlungsrichter) hat die Zulässigkeit des (heimlichen) Zugriffs auf die Informationen einer Mailbox mit der Begründung angenommen, dass § 100 a StPO vor dem Hintergrund des technischen Fortschrittes in der Weise ausgelegt werden müsse, dass er auch den über das öffentliche Leitungsnetz erfolgenden Zugriff auf die in einer Mailbox abrufbereit gespeicherten Informationen zulasse. Auch insofern liege eine Überwachung des Fernmeldeverkehrs vor, weil der technische Bereich der Fernmeldeanlage nicht verlassen werde und der Vorgang der Nachrichtenübermittlung noch nicht abgeschlossen sei. Auch gewährleiste die hohe Zulässigkeitsschwelle des § 100 a StPO, dass der Eingriff auf Verfahren wegen besonders schwerwiegender oder gefährlicher Delikte beschränkt bleibe[12].

Im Gegensatz zum *BGH* geht das Schrifttum[13] davon aus, dass der technische Fortschritt durchaus rechtliche Probleme schaffen kann, die nicht ohne weiteres durch die extensive Auslegung vorhandener Normen zu bewältigen sind. Dieses Phänomen der »Befugnisnormen auf Zuwachs« zeigt die höchstrichterliche Rechtsprechung allerdings nicht nur in Fällen der TKÜ, sondern auch bei anderen »modernen« Ermittlungsmethoden[14]. Dogmatisch konsequent ist die Auffassung des *BGH* schon aufgrund der Nichtbeachtung des natürlichen Wortsinns der Begriffe der »Übermittlung« und »Überwachung« nicht. Beim Zugriff auf gespeicherte Nachrichten findet keine Datenübermittlung zwischen (mindestens) zwei Partnern statt. Von Kommunikation ist nur beim Vorgang der Inanspruchnahme des Speicherplatzes einer Mailbox

11 Einhellige Auffassung, vgl. nur KK-*Nack* (o. Fn. 6), § 100 a Rdnr. 6; HK-*Lemke*, 3. Aufl., Heidelberg 2001, § 100 a Rdnr. 5; *Paeffgen* (o. Fn. 7), S. 1315 und die weiteren Nachweise bei *Weßlau*, ZStW 113 (2001), 700 (dort: Fn. 65).

12 NJW 1997, 1934.

13 *Palm*/*Roy*, NJW 1997, 1904 sowie KK-*Nack* (o. Fn. 6), § 100 a Rdnr. 7 ff., jeweils m.w.N..

14 *Roggan* (o. Fn. 7), S. 146 ff.

durch den Absender der Informationen auszugehen, während der Zeit der Speicherung aber nicht mehr. Es ist deswegen dogmatisch konsequent, hier § 94 StPO anzuwenden und die ruhenden Nachrichten der Beschlagnahme zu unterwerfen[15]. Auch bedeutet das Einwählen auf einen fremden Mail-Server einen selbständigen Kommunikationsvorgang, an dem die Polizei teilnimmt. Von »Überwachung«, also der passiven Kontrolle eines Kommunikationsvorganges, kann dabei nicht ausgegangen werden[16]. Erst mit dem Abrufen der auf dem Speichermedium gespeicherten Daten findet der Kommunikationsvorgang seine Fortsetzung und damit gleichsam seine Beendigung. Zu konstatieren ist lediglich, dass die Rechtsprechung des *BGH* dazu führt, dass die in Mailboxen gespeicherten Daten jedenfalls nicht nur durch die tatbestandlichen Voraussetzungen des § 94 StPO, der weder einen im Vergleich zum Anfangsverdacht gesteigerten Verdachtsgrad noch eine Katalogtat voraussetzt, geschützt werden[17].

Zusammenfassend ist festzustellen, dass auch die auf Mailboxen zwischengespeicherte Daten – unabhängig von der Befugnisnorm – dem Zugriff der Polizei unterliegen und es sich dort nach keiner vertretenen Auffassung um eine »überwachungsfreie Enklave« handelt.

1.3. Mobiltelefone als »Bewegungsmelder«

Mit der Verbreitung der Mobilfunktechnik (Handys) ergeben sich nicht nur für die Nutzer solcher Telefone neue Möglichkeiten der Kommunikation. Während diese nämlich nahezu überall und ohne Bindung an eine feste Station erreichbar sind, werden auch den Strafverfolgungsorganen neue Möglichkeiten eröffnet.

Es ist unbestritten, dass die Daten zur Standortbestimmung des telefonierenden Teilnehmers zur Auskunftspflicht des Netzbetreibers gehört, da es sich hierbei um die näheren Umstände einer Kommunikation handelt[18].

Umstritten war dagegen lange, ob es sich auch bei der Standortbestimmung des lediglich empfangsbereiten Handys um ein überwachtes Datum handelt. Dagegen haben Teile des Schrifttums eingewendet, dass schon der Normzweck des § 100 a StPO nicht auf Observation gerichtet sei. Daher seien als nähere Umstände der TK nur Informationen über wirklich abgewickelte Kommunikationsvorgänge anzusehen, also über tatsächlich geführte (oder wenigstens versuchte) Gespräche[19]. Auch weise der Wortbegriff der (Tele-)Kommunikationsüberwachung eher darauf hin, dass es um die Erlangung von Informationen bei der Verständigung zwischen Menschen gehe und nicht um eine solche beim Datenaustausch zwischen Maschinen[20] (hier: Einwahl des Handys bei der Sendestation). Die Positionsmeldungen fielen völlig unabhängig von transportierten Inhalten an[21]. Schließlich wurde mitunter gegen die Zulässigkeit der

15 KK-*Nack* (o. Fn. 6), § 100 a Rdnr. 8.
16 Ebenso *Bär*, CR 1996, 491 m.w.N.; *Paeffgen* (o. Fn. 7), S. 1315.
17 *Weßlau*, ZStW 113 (2001), 696 f.
18 Einhellige Auffassung: *BGH*, StV 2001, 215 m.w.N. auf höchstrichterliche Rspr.; *Dix* (o. Fn. 8), S. 259 f.; *Bär*, MMR 2000, 473; *Eckhardt*, CR 2001, 387.
19 *Weßlau*, ZStW 113 (2001), 690.
20 *Bernsmann/Jansen*, StV 1999, 592.
21 *Eckhardt*, CR 2001, 386 u. 387; krit. auch *Gehrken*, Forum Recht 2002, 99.

beschriebenen Nutzung von Mobiltelefonen auf der Basis von § 100 a StPO eingewandt, dass damit die Grenze zu § 100 c I Nr. 1b StPO verwischt werde, der den Einsatz technischer Observationsmittel regele[22].

Die entsprechende Frage ist zunächst von der Rechtsprechung der *Landgerichte*[23] und später auch vom *BGH*[24] anders entschieden worden. § 100 a StPO eröffne ausdrücklich die Möglichkeit zur Aufenthaltsermittlung des Beschuldigten. Bemerkenswerter war hier, dass die Gerichte vom Schutzbereich des vermeindlich betroffenen Grundrechts aus Art. 10 GG her argumentieren: Da die §§ 100 a, 100 b StPO mit ihrem weiteren Anwendungsbereich eine gesetzliche Ermächtigung zu Eingriffen in das durch Art. 10 GG geschützte Fernmeldegeheimnis (moderner: Telekommunikationsgeheimnis[25]) darstellten, müsse sich ihre Auslegung, insbesondere des nunmehr maßgebenden Begriffs der Telekommunikation, in erster Linie an diesem Grundrecht orientieren. Das Grundrecht des Fernmeldegeheimnisses sei gegenüber den technischen Entwicklungen, wie sie z.B. in den heutigen Möglichkeiten der Speicherung und Verarbeitung von Informationen jeglicher Art durch Digitalisierung zeige, offen und dynamisch[26]. Kurz: ein durch neuartige Gefährdungen wachsender Schutzbereich eines Grundrechts soll gleichsam mitwachsende Eingriffsbefugnisse nach sich ziehen.

Ein solches Argumentationsmuster ist bemerkenswert und war hier darzustellen, weil die Rechtsprechung alles von einer auf das Grundrecht zugeschnittenen Eingriffsnorm für erfaßt erklärt, was in den Schutzbereich des Grundrechts fällt. Eine solche Auslegung der §§ 100 a f. StPO fällt aus dem bisherigen Verständnis des verfassungsrechtlichen Verhältnisses von Schutzbereich und Beschränkungsmöglichkeiten eines Grundrechts heraus. Keineswegs wurde bisher der Eingriffsumfang einer Rechtsgrundlage durch den Umfang des Schutzbereichs definiert. Vielmehr betrafen einschlägige Eingriffsermächtigungen regelmäßig nur eine Teilmenge des Schutzbereiches eines Grundrechts[27].

Auch kann der Verweis auf die von § 100 a StPO bezweckte Möglichkeit zur Aufenthaltsermittlung nicht überzeugen, denn dies wiederum führte zu einer Ablösung der Auslegung vom Wortbegriff der »Kommunikation«, bei deren Überwachung der Standort des Beschuldigten ermittelt werden soll. Kommunikation setzt den Transport von Nachrichten voraus. Da die Positionsmeldungen eines Handys aber völlig unabhängig von tatsächlich stattfindendem Austausch von Inhalten sind, kann die Aufenthaltsermittlung des Handybesitzers ohne jeden Versuch des Kontakts zu einem anderen Teilnehmer vorgenommen werden. Das mag unter kriminalistischen Gesichtspunkten nützlich sein, denn der sein Handy mitführende Beschuldigte ist damit von Funkzelle zu Funkzelle zu verfolgen. Diesen Umstand aber als (Teil-)

22 *Eckhardt*, CR 2001, 387; vgl. auch *Bernsmann*/*Jansen*, StV 1999, 593.
23 *LG Aachen*, StV 1999, 590; *LG Ravensburg*, NStZ-RR 1999, 84; *LG Dortmund*, NStZ 1998, 577.
24 *BGH* StV 2001, 214 = CR 2001, 385.
25 *Löwer* in: von Münch/Kunig, GG-Komm., München 2001, Art. 10 Rdnr. 18.
26 Stellvertretend *BGH* StV 2001, 215.
27 *Eckhardt*, CR 2001, 387; vgl. auch *Bernsmann*/*Jansen*, StV 1999, 592.

Bereich von Kommunikation zu begreifen, mißachtet die Wortbedeutung eines an sich denknotwendig zwischen mindestens zwei Individuen stattfindenden Vorgangs.

Dagegen vermag der Hinweis auf das Verhältnis von § 100 a StPO zu § 100 c I Nr. 1b StPO nicht ohne weiteres zu überzeugen. § 100 c I Nr. 1b StPO ermächtigt ausdrücklich zum *Einsatz* von besonderen *für Observationszwecke bestimmte* technische Mittel zur Aufenthaltsermittlung. Beim durch die Positionsmeldungen registrierten Mitführen eines Kommunikationsgeräts kann aber schon nicht von einem Einsatz durch die Strafverfolgungsbehörden ausgegangen werden, denn dies setzt nach bisherigem Verständnis ein ihrerseitiges (aktives) Tun voraus[28]. Das kann z.B. im – gezielten (!) – Verwenden von Bewegungsmeldern, Nachtsichtgeräten oder Peilsendern[29] der Fall sein. Auch sind Mobilfunk-Telefone keine *zu Observationszwecken bestimmte* technische Mittel. Ihr Sinn liegt vielmehr in der festnetz-unabhängigen Möglichkeit zur Kommunikation. Dass sie im Stand-By-Modus nebenbei jeweils den Standort des Besitzers mitteilen, macht sie noch nicht zu Observationsmitteln. Ein nicht zu nivellierender Unterschied der beiden Befugnisnormen liegt also darin, dass ausschließlich § 100 a StPO die strafverfolgerische Nutzung von Gegenständen aus der Sphäre des Beschuldigten zu Zwecken der Strafverfolgung erlaubt. Dagegen meint § 100 c I Nr. 1b StPO die Zulässigkeit des Einsatzes von *staatlichen* technischen Mitteln zur Aufenthaltsermittlung.

Unabhängig davon läßt sich als – dogmatisch keineswegs überzeugendes – Ergebnis der skizzierten Rechtsprechung festhalten, dass ein originär kommunikationsunabhängiger Lebenssachverhalt, nämlich das bloße Beisichführen eines Mobiltelefons, für Observationszwecke herangezogen werden darf. Auf diese Weise werden angeschaltete Handys zu permanenten »Bewegungsmeldern«.

1.4. Überwachungsfreies »Surfen« im Internet?

Umstritten ist auch, ob das bloße »Surfen« im Internet, also das Aufrufen von Seiten des World-Wide-Web, von § 100 a StPO erfaßt wird. Dies wird teilweise unter Verweis auf § 3 Nr. 16 TKG (siehe oben) angenommen[30]. Das erscheint zweifelhaft, denn die Betreiber von Mediendiensten gehören nicht zum Kreis der nach § 100 b III StPO verpflichteten Institutionen, die technische Einrichtungen zur Umsetzung der TKÜ vorzuhalten und vorbereitende organisatorische Vorkehrungen für die Umsetzung solcher Maßnahmen zu treffen haben. Das stellt § 2 II Nr. 4 der Telekommunikationsüberwachungsverordnung (TKÜV) unmißverständlich klar: Danach gehören u.a. die Betreiber von solchen Telekommunikationsanlagen nicht zum Kreis der Verpflichteten, deren Anlagen der Verteilung von Rundfunk oder anderen für die Öffentlichkeit bestimmten Diensten, dem Abruf von allgemein zugänglichen Informationen oder der

28 So wohl auch *Gundermann*, K&R 1998, 54.

29 Vgl. nur *Kleinknecht*/*Meyer-Goßner*, StPO, 45. Aufl., München 2001, § 100 c Rdnr. 2 m.w.N.

30 *Kudlich*, JA 2000, 231; *Bär*, MMR 2000, 473 m.w.N.; auch KK-*Nack* (o. Fn. 6), § 100 a Rdnr. 6, geht davon aus, dass die Nutzung von »Online-Diensten« pauschal unter § 100 a fällt.

Übermittlung von Messwerten, nicht individualisierten Daten usw. dienen. Um solche handelt es sich jedenfalls bei den Anbietern von redaktionellen Informationsangeboten im Internet (»Homepages«)[31].

Aber auch der Bereich der Teledienste fällt aus der Überwachung nach § 100 a StPO heraus, weil für solche Dienste nicht das TKG, sondern das Teledienstegesetz (TDG) gilt. Die Betreiber von Telebanking-Diensten oder auch e-commerce-Angeboten werden damit nicht durch § 100 b III StPO i.V.m. § 88 TKG i.V.m. der TKÜV zur Ermöglichung der Erfassung der Daten ihrer Nutzer verpflichtet. Es wäre ein Widerspruch innerhalb der einschlägigen Regelungen, wenn einerseits die Inanspruchnahme der Angebote solche Anbieter überwacht werden dürfte, diese Betreiber aber nicht verpflichtet wären, die dafür erforderlichen Vorkehrungen zu treffen. Es erscheint deshalb richtig, mit *Weßlau* u.a. davon auszugehen, dass das Surfen im Internet *de lege lata* überwachungsfrei ist[32].

1.5. TKÜ als flächendeckend eingesetzte Standardmaßnahme der Strafverfolgungsbehörden

Die Gründe für die jährlichen Zuwachsraten bei den richterlich angeordneten TK-Überwachungen sind vielschichtig: Schon der von § 100 a I StPO verlangte Verdachtsgrad ist keineswegs eine wirksame Schwelle für solche Maßnahmen. Der verlangte einfache Tatverdacht in Gestalt der *bestimmten Tatsachen, die den Verdacht begründen* liegt allenfalls knapp oberhalb des Anfangsverdachts. Von diesem hat das *Bundesverfassungsgericht* erst jüngst wieder betont, dass dessen Schwelle niedrig liegt[33]. Wie wenig höher der einfache Tatverdacht anzusiedeln ist, zeigt ein Blick in die Kommentierung zu § 100 a StPO. Dort wird der Begriff des einfachen Tatverdachts etwa damit umschrieben, dass »Gerüchte und Gerede« nicht ausreichten. Es müßten vielmehr Umstände vorliegen, die nach der Lebenserfahrung, auch der kriminalistischen Erfahrung, in erheblichem Maße darauf hindeuten, dass jemand als Täter oder Teilnehmer eine Katalogtat begangen hat[34]. Das Bundesverfassungsgericht spricht in der G10-Entscheidung von einer »sicheren Basis«[35]. Dass eine solche Hürde aber leicht zu nehmen ist, zeigt der Umstand, dass nicht einmal eine überwiegende Wahrscheinlichkeit für das Vorliegen einer Katalogtat vorliegen muß (hinreichender Tatverdacht, vgl. § 170 I StPO)[36].

Die einschränkend gemeinte Subsidiaritätsklausel des § 100 a S.1 StPO ist schon aufgrund des technischen Fortschritts eine immer weniger ernstzunehmende Barriere vor ausufernder TKÜ. Die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten muß auf andere Weise nur wesentlich erschwert sein.

---

31 Siehe § 2 Mediendienste-Staatsvertrag (MDStV).

32 ZStW 113 (2001), 699 f.; entsprechend z.B. auch die *Datenschutzbeauftragten* des Bundes und der Länder, siehe die Entschließung vom 10.5.2001 zum damaligen Entwurf einer Telekommunikationsüberwachungsverordnung unter http://www.bfd.bund.de/aktuelles.

33 *BVerfG,* wistra 2002, 135 (136).

34 Vgl. nur KK-*Nack* (o. Fn. 6), § 100 a Rdnr. 24; HK-*Lemke* (o. Fn. 11), § 100 a Rdnr. 10.

35 *BVerfG* NJW 2000, 55 (65 f.).

36 *Kleinknecht/Meyer-Goßner* (o. Fn. 29), § 100 a Rdnr. 6.

Es wird also ein Vergleich von verschiedenen Ermittlungsmethoden verlangt. Wie z.B. *Kloepfer* richtig feststellt, bereitet die Überwachung der TK aufgrund der Weiterentwicklung der Digitaltechnik und nicht zuletzt wegen der nach der TKÜV bereitzustellenden technischen Vorkehrungen durch die TK-Anbieter immer geringere Schwierigkeiten. Eine Anwendung anderer Methoden würden aufgrund der Leichtigkeit der TKÜ die Ermittlungen daher regelmäßig »erheblich erschweren«. Das zeigt sich gerade hinsichtlich der Ermittlung des Aufenthaltsortes eines Beschuldigten: Die Bestimmung der Funkzelle, in der sich ein Mobiltelefon befindet, ist flächendeckend und ohne größeren Aufwand realisierbar[37]. Auf diese Weise gerät eine Abwägung der Schwere des Grundrechtseingriffs mit den Belangen der Strafverfolgung (Verhältnismäßigkeit) leicht in den Hintergrund.

Der Richtervorbehalt als präventiver verfahrensmäßiger Grundrechtsschutz läuft weitgehend leer. Auf diese Weise konnte die Bundesrepublik in der Vergangenheit zum Weltmeister in Sachen TKÜ werden[38]. Erst in seinem jüngsten Bericht für die Jahre 1999 und 2000 beklagte der Bundesbeauftragte für den Datenschutz einen ständigen Anstieg der nach der StPO angeordneten TKÜ: Im Jahr 1995 seien 4.674, in 1996 bereits 6.428, in 1997 dann 7.776 und in 1998 insgesamt 9.802 Anordnungen erlassen worden. 1999 schließlich sei die Zahl auf 12.651 richterliche Beschlüsse gestiegen. Auf das Jahr 1995 bezogen bedeutet dies eine Steigerung von 175 %, für das Jahr 1999 allein 30 %[39]. Im Jahr 2000 wurden 15.751 entsprechende Beschlüsse gefaßt[40] und der (leider wohl wieder nur ein Jahr geltende) Höchststand von 19.896 Maßnahmen[41] wurde im Jahr 2001 erreicht.

Das Ausmaß der TKÜ in der Bundesrepublik bestimmt sich aber nicht nur nach der Zahl der Anordnungen, sondern auch nach der Zahl der dabei überwachten Anschlüsse. Im Jahr 2000 sollen 17.140 Anschlüsse betroffen gewesen sein, was im Vergleich zum Vorjahr einen Anstieg um 28 % bedeutet[42]. Auch im Bereich der von den Anordnungen betroffenen Personen ist also ein signifikanter Anstieg zu registrieren. Dabei handelt es sich bei den Betroffenen keineswegs ausschließlich um Beschuldigte, vgl. § 100 a S. 2 StPO. Die Anordnungen sollen sich vielmehr in der Mehrzahl nicht auf Anschlüsse des Beschuldigten beziehen, sondern auf solche von Dritten[43]. Die Zahl der in jeder Hinsicht unverdächtigen Bürger, deren Wort heimlich registriert wird, dürfte damit in die Hunderttausende gehen: Jeder, der mit einer solchen Kontaktperson per Telefon kommuniziert, wird zunächst einmal polizeilich erfaßt.

Es zeigt sich, dass die geltenden Tatbestände der Strafprozeßordnung eine immer flächendeckendere Überwachung des individuellen Nachrichtenaustauschs nicht zu verhindern vermögen. Im Gegenteil: Der gesetzgeberische Wille scheint – wie im folgenden zu verdeutlichen ist – in die entgegengesetzte Richtung zu weisen.

---

37 *Kloepfer* (o. Fn. 4), S. 96 f.
38 *Paeffgen* (o. Fn. 7) , S. 1299 m.w.N.; ausführlich auch *Bizer* (o. Fn. 10), S. 130 ff.
39 BT-Drucks. 14/5555, S. 50; siehe auch die Grafik bei *Fox*, DuD 2002, 194.
40 So die Berechnungen von *Bizer*, DuD 2002, 217.
41 Quelle: Der Spiegel 50/2002, S. 84.
42 Ausführlich *Bizer*, DuD 2002, 216 ff.
43 *Kloepfer* (o. Fn. 4), S. 101.

2. Auskunftsansprüche über zurückliegende und zukünftige Verbindungsdaten nach den §§ 100 g, h StPO

Seit dem 1.1. 2002 sind an die Stelle des § 12 des Fernmeldeanlagengesetzes (FAG) die §§ 100 g, h StPO getreten[44]. Sie regeln die Mitteilungspflichten der TK-Anbieter über die sogenannten *Verbindungsdaten*, die bei jeder Telekommunikation anfallen.

2.1. Verbindungsdaten des Beschuldigten

§ 100 g I S.1 StPO bestimmt, dass diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, unverzüglich Auskunft über die Verbindungsdaten zu erteilen haben, wenn bestimmte Tatsachen den Verdacht einer Straftat von erheblicher Bedeutung, insbesondere einer Katalogtat des § 100 a S.1 StPO, begründen[45]. Dasselbe gilt beim Verdacht von Straftaten, die mittels einer Endeinrichtung (Telefon, Fax, Computer etc.) begangen wurden. Nach § 100 g I S.3 StPO darf die Auskunft auch über zukünftige Verbindungsdaten angeordnet werden. Wie auch bei der TKÜ nach § 100 a StPO wird eine richterliche Anordnung verlangt (§ 100 h I S.3 StPO).

Bemerkenswert an der Regelung ist, dass § 100 g I i.V.m. III StPO die TK-Anbieter zur Auskunft über Daten ihrer Kunden verpflichtet, die sie z.T. von sich aus überhaupt nicht erheben oder speichern würden. Von welcher Funkzelle aus etwa ein Gespräch stattfindet, bräuchte ein TK-Unternehmen nicht zu interessieren. *Eckhardt* fragt deshalb zu Recht, ob die TK-Anbieter fortan alle in § 100 g III StPO genannten Verbindungsdaten zu erfassen und zu speichern haben: Eine Regelung darüber, dass eine Anordnung nach den §§ 100 g I, 100 h I S.3 StPO die TK-Unternehmen zwingt, sämtliche dort genannten Verbindungsdaten zu erheben und zu speichern wurde nicht ausdrücklich getroffen[46]. Sinn und Zweck der Vorschrift sprechen dafür. *De lege ferenda* sollte diese Frage in den die TK-Unternehmen betreffenden Datenschutzregelungen gelöst werden.

Noch problematischer ist die Formulierung im Gesetz, wonach die Auskunft *auch* über zukünftige TK-Verbindungsdaten angeordnet werden darf. Das impliziert ihre Pflicht zur Auskunft über Daten aus der Vergangenheit. Dass die Unternehmen solche aus der Zeit vor einer Anordnung mitzuteilen haben, ist unproblematisch. Die Mitteilung von planmäßig erhobenen und gespeicherten Daten bereitet insoweit zwar keine Schwierigkeiten. Fraglich ist aber, ob das Gesetz auch hier wiederum sämtliche in § 100 g III StPO genannten Verbindungsdaten meint. Eine Auskunft hierüber könnten die Unternehmen nur dann erteilen, wenn sie generell bei sämtlichen Kunden alle in § 100 g III StPO genannten Daten für eine eventuelle spätere Strafverfolgung auf Vorrat erheben und speichern würden. Hier jedenfalls fallen die bei den TK-Unternehmen rechtmäßig vorhandenen und die im Falle eines Strafverfahrens mitzuteilenden Ver-

44 BGBl. 2001, Teil I, S. 3879.

45 Im Verhältnis zu § 12 FAG stellt die Voraussetzung von bestimmten Straftaten eine (unwesentliche) Anhebung der tatbestandlichen Anforderungen dar.

46 *Eckhardt*, DuD 2002, 199.

bindungsdaten auseinander. Die Frage darf deshalb nur in der Weise beantwortet werden, dass nur rechtmäßig vorhandene Verbindungsdaten aus der Vergangenheit von einer Anordnung erfaßt sein können.

2.2. Verbindungsdaten von Unverdächtigen: Die Zielwahlsuche

In § 100 g II StPO wird unter Subsidiaritätsvoraussetzungen die sog. *Zielwahlsuche* legalisiert. Danach darf auch die Auskunft darüber verlangt werden, wer mit den in § 100 a S.2 StPO genannten Zielpersonen via Telekommunikation Kontakt aufgenommen hat. Absatz II stellt insoweit eine (im Ergebnis freilich nicht zu überschätzende) Anhebung der tatbestandlichen Anforderungen im Verhältnis zu Absatz I Satz 2 dar: Die Einbeziehung der Verbindungsdaten von Dritten, die von sich aus Kontakt zu der Zielperson aufgenommen haben, ist nur zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Hinsichtlich der Effektivität solcher »Restriktion« ist auf die Ausführungen zur Subsidiaritätsklausel im vorangegangenen Abschnitt zu verweisen.

Zweck des § 100 g II StPO ist es, ein vollständiges Kommunikationsprofil eines Beschuldigten zu erfassen: Mit wem hatte ein Beschuldigter wie oft und von wo aus wie lange Kontakt etc. ? Eine Auskunft durch die TK-Anbieter hierüber ist nicht ohne weiteres möglich, denn die TK-Unternehmen dürfen nicht jedwedes Datum einer Person – also ohne Rücksicht darauf, wer der Anrufer ist – überhaupt speichern. In der Regel ist das nur für solche Verbindungsdaten der Fall, für die der Kunde (der Beschuldigte) gegenüber dem Unternehmen der Kostenschuldner ist. Es werden demnach überhaupt nur solche Verbindungsdaten gespeichert, bei denen der Beschuldigte der Initiator der Kommunikation ist. Dagegen ist es für die Anbieter der TK-Dienstleistungen in der Regel ohne Belang, wer mit ihrem Kunden (auf dessen Rechnung) Kontakt aufgenommen hat. Entsprechende Daten werden deshalb zu Abrechnungsgründen erst gar nicht erhoben. Die Zielwahlsuche kann daher nur in der Weise erfolgen, dass die aufgrund von § 100 b III StPO Verpflichteten in der Weise an der Strafverfolgung des Beschuldigten mitzuwirken haben, dass sie durch einen Abgleich sämtlicher Verbindungsdaten ihrer Kunden herauszufinden haben, wer mit dem Beschuldigten (von sich aus) Kontakt aufgenommen hat. Bei einem solchen Suchlauf werden ca. 450 Millionen Datensätze durchsucht[47]. Es ist naheliegend, hierbei von einer Art »Rasterfahndung« zu sprechen, die von den Kommunikationsunternehmen *für die Strafverfolgungsbehörden* durchzuführen ist[48].

Festzustellen ist damit zunächst, dass hier Private erstmals *de lege lata* verpflichtet werden, Ermittlungsergebnisse für die Polizei zu produzieren[49] und damit per Gesetz zu Gehilfen der Strafverfolgungsbehörden mutieren. Mindestens ebenso problematisch ist es aber, dass die TK-Unternehmen bei ihrer Zielwahlsuche *für die Polizei* (gezielt) in die Grundrechte sämtlicher TK-Nutzer eingreifen. *Welp* geht deshalb rich-

47 *Welp*, Überwachung und Kontrolle, Berlin 2000, S. 107.
48 *Weßlau*, ZStW 113 (2001), 693.
49 *Welp* (o. Fn. 47), S. 102.

tigerweise davon aus, dass damit der grundrechtliche Geheimnisschutz der Verbindungsdaten gegenüber den Strafverfolgungsbehörden praktisch beseitigt und damit – nach Art. 19 II GG unzulässig – in den Wesensgehalt von Art. 10 I GG eingegriffen wird[50]. Es bestehen damit nicht zu beseitigende verfassungsrechtliche Bedenken gegen die Eingriffsermächtigung des § 100 g II StPO.

3. Exkurs: Der IMSI-Catcher

Durch das Gesetz zur Änderung der Strafprozeßordnung vom 6. August 2002 ist der sog. IMSI-Catcher als § 100 i in die StPO eingefügt worden[51]. Für das Bundesamt für Verfassungsschutz ist er bereits durch das Terrorismusbekämpfungsgesetz vom 9.1.2002[52] legalisiert worden[53]. Die Regelung dieser Methode war von datenschutzrechtlicher Seite seit längerem angemahnt worden[54]. Dagegen war die Bundesregierung noch im September 2001 der Auffassung, dass der Einsatz des IMSI-Catchers im strafprozessualen Bereich durch die §§ 100 a ff., 161 StPO gedeckt sei[55].

3.1. Die Funktionsweise des IMSI-Catchers

Bei dem IMSI-Catcher handelt es sich um ein Gerät[56], das in der Lage ist die IMSI (International Mobile Subsciber Identity) eines Mobilfunk-Telefons (Handy) zu erfassen. Ist die IMSI eines Geräts festgestellt, können die Sicherheitsbehörden von den Mobilfunkbetreibern nach § 89 VI TKG den Namen und die Anschrift des Nutzer erfahren, dem die IMSI zugeordnet ist.

Der IMSI-Catcher simuliert eine Funkzelle mit starker Feldstärke, so dass sich alle Handys in einem bestimmten Umkreis nicht bei der echten Funkzelle ihres Netzes, sondern bei der des IMSI-Catchers anmelden[57]. Außerdem besteht Möglichkeit, eine Funkzelle mit geringer Leistung und damit geringer Ausdehnung zu simulieren, so dass der Aufenthaltsort eines bereits bekannten Handys stark eingegrenzt und damit quasi geortet werden kann[58]. In modifizierter Bauart ermöglicht es auch ein Abhören von abgehenden Gesprächen eines »gefangenen« Handys[59]. Während des Einsatzes des Geräts sind sämtliche Handys im entsprechenden Bereich nicht funktionsfähig[60].

Die Strafverfolgungs- und Sicherheitsbehörden waren an diesem Gerät deshalb besonders interessiert, weil es auch die Feststellung von unbekannten Anschlußnum-

---

50 *Welp* (o. Fn. 47), S. 107.
51 BGBl. I, S. 3018.
52 BGBl. I, S. 361 ff.
53 Eine kritische Würdigung hierzu liefert *Rublack*, DuD 2002, 204.
54 *Löwnau-Iqbal*, DuD 2001, 578; BT-Drucks. 14/5555, S. 88.
55 BT-Drucks. 14/6885.
56 Es handelt sich hierbei um ein Gerät der Firma Rhode & Schwarz (»GA 090«), das ursprünglich ein Test- und Messsystem war und für den Zweck der Bestimmung der Endgerätekennung eines Handys weiter entwickelt wurde, vgl. *Fox*, DuD 2002, 212.
57 Vgl. zu den technischen Einzelheiten *Kiper*/*Ruhmann*, DuD 1998, 160.
58 *Fox*, DuD 2002, 213 f.
59 *Gundermann*, K&R 1998, 55; *Fox*, DuD 2002, 212.
60 *Rublack*, DuD 2002, 204.

mern einer Zielperson ermöglicht. Vor diesem Problem stehen die Sicherheitsbehörden u.a. deshalb, weil u.a. durch die weite Verbreitung von sog. Pre-Paid-Handys eine unmittelbare Feststellung des Nutzers – mangels festen Vertrages mit einer Telefongesellschaft – nicht immer möglich ist. Darüber hinaus werden vorsichtige Kriminelle tunlichst den Abschluß von Mobilfunk-Verträgen unter ihrem eigenen Namen vermeiden[61].

3.2. Tatbestandliche Voraussetzungen

Unter dem Vorbehalt einer richterlichen Anordnung ist der Einsatz eines IMSI-Catchers unter Subsidiaritätsvoraussetzungen zulässig zur Vorbereitung einer – zulässigen – TKÜ nach § 100 a StPO (§§ 100 i I Nr. 1 i.V.m. II S.1 StPO). Im Fall einer Straftat von erheblicher Bedeutung ist er auch, wenn die Ermittlung des Aufenthaltsorts eines Beschuldigten oder Verurteilten (nicht: Täters[62]) auf andere Weise weniger erfolgversprechend oder erschwert wäre, zur vorläufigen Festnahme nach § 127 II StPO oder zur Vollstreckung eines Haftbefehls oder Unterbringungsbefehls anwendbar (§§ 100 i I Nr.2 i.V.m. II S.2 StPO). Im letztgenannten Fall ist er schließlich zur Sicherung von eingesetzten Polizeibeamten zulässig (§ 100 i I Nr.2 i.V.m. II S.3 StPO).

§ 100 i III S.1 StPO regelt, dass personenbezogene Daten Dritter, also die IMSI deren Handys, nur erhoben werden dürfen, wenn dies aus technischen Gründen zur Erreichung des Zwecks nach Absatz I unvermeidbar ist. Diesbezüglich stellt sich die Frage, ob die Datenerhebung von Dritten nicht *der Normalfall* des Einsatzes des IMSI-Catchers ist. Das wäre nur dann nicht der Fall, wenn sich polizeilicherseits ausschließen ließe, dass sich Handys von Unbeteiligten im Bereich der von dem Gerät imitierten Funkzelle aufhalten. Das erscheint schon aufgrund der inzwischen weiten Verbreitung der Mobiltelefone mehr als unwahrscheinlich. Es wird sich praktisch nie vermeiden lassen, dass die Daten Unverdächtiger von dem IMSI-Catcher »mitgefangen« werden. Die Vermeidbarkeit der Inanspruchnahme Dritter ist damit eher theoretischer Natur.

§ 100 i III S.2 bestimmt eine Verwendungsbegrenzung und eine unverzügliche Löschung nach Beendigung der Maßnahme. Dabei stellt sich das Problem, in welchem Zeitraum die Daten Dritter zur Verfügung der Polizei stehen. Mit »Beendigung der Maßnahme« kann jedenfalls nicht der Zeitpunkt des Abschlusses des unmittelbaren Einsatzes des IMSI-Catchers, also der Vorgang der Feststellung der sich im Bereich dessen »Funkzelle« befindlichen Handys, gemeint sein. Dann würde sein Einsatz im Regelfall nutzlos sein. Vielmehr kann die entsprechende Wendung nur so zu verstehen sein, dass erst nach den entsprechenden Abgleichen und dem Ausschluß von »gefangenen Handynutzern« aus dem Kreis der Verdächtigen eine Löschung vorzunehmen ist. Erst wenn die tatsächliche Zielperson identifiziert ist und etwa eine TKÜ-Maßnahme nach § 100 a StPO gegen den Beschuldigten möglich ist, sind die TK-(Bestands-)Daten der anderen uninteressant und unterliegen damit der unverzüglichen Vernichtung. Je nach Ermittlung kann es sich bei diesem Zeitraum um mehrere Tage

61 *Fox*, DuD 2002, 212.
62 So aber der Wortlaut des Gesetzes.

oder gar Wochen handeln, in denen sich die Unbeteiligten im Visier der Ermittler befinden. So lange kommen sie auch als Verdächtige in Frage. Der Wortlaut des Gesetzes könnte insoweit den falschen Eindruck erwecken, dass Dritte nur kurzfristig von den entsprechenden polizeilichen Nachforschungen betroffen sind. Schon aus diesem Grunde ist von einem nicht unbeträchtlichen Eingriff in die Sphäre von Unverdächtigen auszugehen.

3.3. Der Zugriff auf eine Vielzahl Unverdächtiger

Aus dem zuvor Gesagten ergibt sich: Der IMSI-Catcher greift technisch bedingt tief in die Grundrechte einer Vielzahl von unbeteiligten Dritten ein, deren Aufenthaltsort zwangsläufig mit registriert wird[63]. Angesichts der weiten Verbreitung der Mobiltelefone steht zu befürchten, dass die Erstellung von Bewegungsbildern von Personen mit aktiv geschaltetem Handy zu einer Standardmethode der Polizei wird[64]. Die Entwicklung der Zahlen der Telekommunikationsüberwachungen nach § 100 a StPO lassen eine solche Prognose zu.

Rechtspolitisch bedeutungsvoll ist der Einsatz des IMSI-Catcher aber vor allem deshalb, weil (auch) mit ihm die *Einbeziehung von Unverdächtigen zum Normalfall polizeilicher Tätigkeit* wird. Je nach Art des Einsatzes besteht auch die Möglichkeit, dass Unbeteiligte in die Verlegenheit geraten zu Objekten polizeilicher Nachforschungen zu werden bzw. ihren Aufenthalt im Bereich der simulierten Funkzelle erklären zu müssen[65]. Das kann dann der Fall sein, wenn der IMSI-Catcher als Methode zur Feststellung der in einem bestimmten Gebiet befindlichen Mobiltelefone verwendet wird. Damit wird auch im Bereich der Telekommunikation eine *de facto*-Mitwirkungspflicht aller Handy-Nutzer statuiert. Ein fehlender Zusammenhang mit einer aufzuklärenden Straftat schützt nicht mehr vor ihrer Registrierung für einen für sie nicht zu bestimmenden Zeitraum.

3.4. Verstoß gegen Zitiergebot?

Im Nachklang zur Verabschiedung des Gesetzes zur Einführung des IMSI-Catchers ist von Seiten einiger Datenschützer die Behauptung erhoben worden, dass es gegen das Zitiergebot des Art. 19 I S.2 GG verstoße[66]. In der Tat enthält das Gesetz keinen Hinweis auf eine Einschränkung des Fernmeldegeheimnisses aus Art. 10 GG.

Dem Zitiergebot zufolge muß ein förmliches Gesetz, das ein Grundrecht einschränkt oder dazu ermächtigt, ausdrücklich darauf hinweisen, dass das Grundrecht eingeschränkt wird. Geschieht dies nicht, verletzt das Gesetz nach einhelliger Meinung das eingeschränkte Grundrecht in Verbindung mit Art. 2 I GG und ist nichtig[67]. Es ist deshalb zu erörtern, ob der Einsatz des IMSI-Catchers durch seine beiden Einsatzmöglichkeiten (Ermittlung von Geräte- und Kartennummern sowie Aufenthaltser-

63 Bundesbeauftragter für den Datenschutz, BT-Drucks. 14/5555, S. 88.
64 *Rublack*, DuD 2002, 204.
65 *Gundermann*, K&R 1998, 55.
66 Siehe unter http://www.datenschutzzentrum.de/material/themen/divers/imsicat.htm .
67 Vgl. nur *BVerfGE* 5, 13 (15f.) und *Jarass*/*Pieroth*, GG, München 2002, Art. 19 Rdnr. 2.

mittlung einer Zielperson) in den Schutzbereich des Telekommunikationsgeheimnisses überhaupt eingreift. Hierzu bedarf es der Bestimmung seines Schutzbereiches.

Das bisherige Schrifttum stellt auf den Schutz von tatsächlich zustande gekommenen Kommunikationsvorgängen und deren nähere Begleitumstände ab: Das Grundrecht des Telekommunikationsgeheimnisses soll die durch unkörperliche Signale transportierte räumlich distanzierte individuelle Kommunikation schützen[68]. Unbestritten ist insoweit, dass nicht nur der traditionelle Telefon-, Telegramm- und Funkverkehr, sondern auch die Kommunikation mittels neuer Medien, wie zum Beispiel Mobilfunk und Internet geschützt wird[69]. Auch das Bundesverfassungsgericht spricht in seiner jüngsten Abhör-Entscheidung nur vom Schutz vor der staatlichen Kenntnisnahme von Telekommunikationskontakten[70]. Der Schutzbereich betrifft demnach unbestritten tatsächlich zustande gekommene oder wenigstens versuchte Kontakte[71]. Genau diesen Umfang definiert im übrigen auch § 85 I S.2 TKG. Dort heißt es: »Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche«.

In Ergänzung zu diesen Definitionen wollen *Schenke* und andere den Schutzbereich des TK-Geheimnisses aus Art. 10 GG weiter fassen. Die Privatheit der Kommunikation werde bereits durch die Ausforschung der Kommunikations*bereitschaft* gefährdet. Im Bereich des Mobilfunks sei eine Kommunikation ohne vorherige Aufnahme der Betriebsbereitschaft nicht denkbar. Die Grundrechte seien in ihrem Freiheitsgehalt entscheidend darauf angelegt, dass die Grundrechtsträger nicht befürchten müßten, wegen oder aus Anlaß der Grundrechtsausübung Objekt staatlicher Beaufsichtigung und möglicher nachteiliger Maßnahmen zu werden[72]. Schutz verdiene dann aber nicht nur der eigentliche Kommunikationsvorgang, sondern ebenso die dem vorgelagerte Kommunikations*anbahnung*[73] *(Hervorhebungen F.R.).* Demzufolge würde auch das Datum des sich an einem bestimmten Ort im Stand-By-Modus aufhaltenden Mobilfunkgeräts den Schutz des Art. 10 GG genießen[74]. Das Ausnutzen dieser Betriebsbereitschaft durch den IMSI-Catcher bedeutete dann einen Eingriff in das TK-Geheimnis.

Dass insoweit die Termini in der Eingriffsbefugnis des § 100 a StPO (dort: enge Auslegung, s.o.[75]) und im Schutzbereich auseinanderfallen können, steht dem nicht entgegen: Im Sinne eines möglichst umfassenden Grundrechtsschutzes sind die Schutzbereiche der Grundrechte weit zu interpretieren. Zwar ist zuzugeben, dass die bloße Feststellung einer Geräte- und Kartennummer oder die Aufenthaltserfassung einer Zielperson durch einen IMSI-Catcher originär unabhängig von irgendeiner tatsächlich stattfindenden oder wenigstens versuchten Kontaktaufnahme zwischen Indi-

68 Statt vieler vgl. nur *Löwer* (o. Fn. 27), Art. 10 Rdnr. 18.
69 Statt vieler vgl. nur *Pieroth/Schlink*, Grundrechte/Staatsrecht II, Heidelberg 2001, S. 192.
70 *BVerfGE* 100, 313 (358) m.w.N.
71 AK-GG-*Bizer* (Stand: 2001), Art. 10 Rdnr. 40 m.w.N.
72 *Schenke*, AöR 2000, 20 f.; *Gercke*, Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren, Berlin 2002, S. 68 ff.
73 *Schenke*, AöR 2000, 21; ebenso *Gundermann*, K&R 1998, 55.
74 AK-GG-*Bizer* (o. Fn. 71), Art. 10 Rdnr. 40.
75 Vgl. oben Punkt 1.3.

viduen ist. Die Betriebsbereitschaft eines Handys ihrerseits ist aber *eine technisch notwendige Vorstufe zur Anbahnung* einer späteren Kommunikation. Bereits die Erfassung der Standortdaten von Mobilfunktelefonen ist – unabhängig von konkreten (auch: versuchten) Gesprächen – ein Eingriff in das Grundrecht aus Art. 10 GG[76].

Der Einsatz des IMSI-Catchers bedeutet daher nicht nur einen Eingriff in den Schutzbereich des Art. 10 GG, sondern auch in denjenigen des Grundrechts auf informationelle Selbstbestimmung[77]. Als Ergebnis der eingangs dargestellten verfassungsrechtlichen Frage ist festzustellen, dass wegen der Nicht-Erwähnung des Art. 10 GG als eingeschränktem Grundrecht von einem Verstoß gegen das Zitiergebot des Art. 19 I S.2 GG durch das Gesetz zur Änderung der Strafprozeßordnung vom 6. August 2002 auszugehen ist. Es unterfällt dem Verdikt der Nichtigkeit.

II. Landesrechtliche TKÜ-Regelungen: Präventives Lauschen

Ausdrückliche Regelungen zur inhaltlichen Überwachung der Telekommunikation waren bis zum Jahr 2002 in den Polizeigesetzen nicht enthalten. Das ist deswegen bemerkenswert, weil es ein längst bekanntes und praktiziertes Mittel zur Gefahrenabwehr – etwa bei Kidnapping, Geiselnahmen oder allgemein der Verhinderung von Straftaten – ist. Es dürfte nicht ernsthaft bestritten werden, dass die Polizei in bestimmten Gefahrensituationen den Telefonverkehr, den beispielsweise ein Geiselnehmer in einer Bank führt, überwachen dürfen muß. Zweifelhaft ist diesbezüglich aber die Rechtsgrundlage, denn die Vorschriften der Strafprozeßordnung kommen aufgrund des unzweifelhaften Schwerpunkts der polizeilichen Maßnahmen im Bereich der Gefahrenabwehr, etwa zugunsten der Befreiung einer Geisel, nicht in Betracht[78]. Es ist schon deshalb gänzlich unerheblich, dass die Vorschriften der §§ 100 a ff. StPO schon aufgrund des Fehlens ihrer tatbestandlichen Voraussetzungen nicht anzuwenden sind[79]. Richtig ist dagegen, eine gefahrenabwehrrechtliche Regelung der TKÜ zu fordern[80], denn die polizeiliche Generalklausel kommt schon aus Bestimmtheitsgründen als Ermächtigungsgrundlage nicht in Betracht[81]. Auch die Regelungen über den Einsatz besonderer technischer Mittel scheiden aus, da die meisten (Polizei-)Gesetzgeber insoweit schon dem Zitiergebot nicht genügt hätten[82].

Die im Jahr 2002 verabschiedete Regelung des Thüringischen Polizeiaufgabengesetzes[83] (ThürPAG) geht über den Befugnisumfang der bereits seit 1994 geltenden niedersächsischen Norm (§ 33 NGefAG) – bis dahin einzige Befugnis zur TKÜ in einem

76 *Gercke* (o. Fn. 72), S. 71.
77 So auch *Schenke*, AöR 2000, 23 f., der das Telekommunikationsgrundrecht und das Grundrecht auf informationelle Selbstbestimmung in »Idealkonkurrenz« sieht.
78 *Weitemeier*/*Große*, Kriminalistik 1997, 336.
79 Entsprechende Überlegungen stellen – überflüssigerweise – *Weitemeier*/*Große*, Kriminalistik 1997, 337, an.
80 *Schenke*, AöR 2000, 2 ff.; *Weitemeier*/*Große*, Kriminalistik 1997, 335 ff..
81 *Löwer* (o. Fn. 25), Art. 10 Rdnr. 29.
82 So auch *Weitemeier*/*Große*, Kriminalistik 1997, 336.
83 GVBl. 2002, S. 248.

Polizeigesetz – weit hinaus. Nach § 34 a ThürPAG kann die Polizei unter bestimmten Umständen auch die Auskunft über Inhalt und nähere Umstände von Telekommunikationen (wozu auch die Funkzellen von Mobiltelefonen gehören, s.o.) verlangen.

1. Tatbestandliche Voraussetzungen des § 34 a ThürPAG

§ 34 a I S.1 Nr. 2 ThürPAG erlaubt unter Richtervorbehalt (vgl. i. E. § 34 a II ThürPAG) die – auch rückwirkende[84] – Telekommunikationsüberwachung zur Gefahrenabwehr über die für eine Gefahr Verantwortlichen, wenn dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben , Gesundheit oder Freiheit einer Person erforderlich ist. Die Befugnis fügt sich nahtlos in das traditionelle Recht der Gefahrenabwehr ein und begegnet schon aufgrund des mit ihr bezweckten Schutzes hochrangiger Rechtsgüter keinen verfassungsmäßigen Bedenken.

Nähere Betrachtung verlangen hingegen die Voraussetzungen der Nr. 1 und 3 des § 34 a ThürPAG. Hiernach ist die präventive Telekommunikationsüberwachung bereits erlaubt, soweit Tatsachen die Annahme rechtfertigen, dass Personen Straftaten im Sinne des § 100 a StPO begehen wollen. Auch deren Kontakt- und Begleitpersonen können von Maßnahmen der Telekommunikationsüberwachung betroffen sein. § 34 a I S.1 Nr.3 ThürPAG beschränkt letztgenannte Datenerhebungen auf die Gewinnung von Hinweisen bezüglich der angenommenen Straftaten. Auch müssen sie zu deren vorbeugender Bekämpfung zwingend erforderlich sein.

Zweifelhaft ist an dieser Vorschrift aus dem Repertoire der vorbeugenden Verbrechensbekämpfung, dass an die Tatsachen keine näher bezeichneten Anforderungen gestellt werden. Bei diesen Tatsachen muß es sich nur um solche handeln, die sich aus der äußeren Geschehenswelt ergeben, die bloß angenommene »verbrecherische Gesinnung« eines bestimmten Personenkreises darf danach also nicht ausreichen[85]. Gemeint ist mit der Formulierung *eine Indizwirkung bestimmter Tatsachen* für eine künftige Straftatbegehung. Es soll reichen, daß diese Indizien nach der polizeilichen Erfahrung die Straftatbegehung als *möglich* erscheinen lassen[86]. Auch an die zeitliche Nähe der zu erwartenden Straftaten werden keine spezifischen Anforderungen gestellt[87].

Anknüpfungspunkt sind hier polizeiliche Annahmen, die sich z.B. aus kriminalistischen Alltagstheorien ergeben können[88]. Wenn also Personen in einer bestimmten (polizeilich definierten) Weise auffällig geworden sind, und sich das mit allgemeinem

84 Vgl. § 34 a I S.2 ThürPAG.

85 Vgl. dazu ausführlich *Rachor* in: Handbuch des Polizeirechts (Hrsg.: Lisken/Denninger), München 2001, S. 270 f.

86 *Rachor* (o. Fn. 85), S. 271. Große Bedeutung soll dem Umstand zukommen, ob und wie oft bestimmte Personen als Verdächtige in strafrechtliche Ermittlungsverfahren verwickelt waren oder nachgewiesenermaßen schon als Straftäter in Erscheinung getreten sind. Bei strafrechtlich noch nicht in Erscheinung getretenen Personen soll ihr Aufenthalt an bestimmten Orten oder die persönlichen Verbindungen zu polizeibekannten StraftäterInnen diese Indizwirkung besitzen.

87 *Rachor* (o. Fn. 85), S. 272.

88 *Weßlau*, KritV 1997, 243.

Erfahrungswissen und weiteren kriminologischen Erkenntnissen ergänzt, so ist diese tatbestandliche Voraussetzung bereits erfüllt. Es fehlt diesbezüglich also an einem verfahrensrechtlichen *Argumentations- und Rechtfertigungszwang* der Polizei hinsichtlich ihrer Annahmen, wie das etwa bei der Belegung einer *Gefahr* als polizeirechtliche Eingriffsvoraussetzung der Fall ist. *Rachor* geht daher zu Recht davon aus, daß der Polizei mit dem entsprechenden Tatbestandsmerkmal eine »weitgehend unkontrollierte (und damit unkontrollierbare), weil unreflektiert-ungefilterte Definitionsmacht« vermittelt werde[89]. Mit einer mindestens zu fordernden »hinreichend sicheren Faktenlage«[90] sind solche tatbestandlichen Voraussetzungen nicht zu vergleichen. Eine effektive nachträgliche gerichtliche Kontrolle muß bei polizeilichen Maßnahmen auf der Basis von Ermächtigungsnormen entsprechender Ausgestaltung bereits bei der Nachvollziehbarkeit des Sachverhalts scheitern.

Bedenklich ist außerdem, dass die Maßnahmen sich auch gegen Kontakt- und Begleitpersonen richten können. Zwar versucht die neue Legaldefinition in § 34 III S.1 Nr. 3 ThürPAG den Begriff präziser zu fassen. Betroffen sollen nunmehr solche Personen sein, die zu den zuvor Genannten („potentielle Straftäter«) »in näherer persönlicher oder geschäftlicher Beziehung stehen oder zu ihnen über einen längeren Zeitraum eine Verbindung unterhalten oder unter konspirativen Umständen hergestellt haben oder pflegen«. Der thüringische Landesgesetzgeber hat sich damit wortgenau an einschlägiger Rechtsprechung orientiert[91]. Allerdings ist die Begrenzungswirkung einer solchen Formulierung nicht zu überschätzen: Lediglich äußerlich flüchtige oder zufällige Alltagskontakte oder Beziehungen[92] scheiden damit aus dem überwachten Personenkreis aus. Dies bedeutet eine erhebliche Ausweitung des von entsprechenden Datenerhebungen betroffenen Personenkreises über die in § 34 a genannten hinaus. Deswegen steht zu befürchten, dass auch zukünftig planmäßig völlig Unbeteiligte (etwa Familienangehörige, Geschäftspartner und Freunde) von derart intensiven Eingriffen betroffen sein werden. Die Vorschrift unterliegt daher auch unter Verhältnismäßigkeitsgesichtspunkten erheblichen Zweifeln[93].

Nicht zuletzt aus diesem Grund begegnet die Regelung deshalb erheblichen rechtsstaatlichen Bedenken. Darüber hinaus ist festzustellen, dass im undefinierbaren Vorfeldbereich konkreter Gefährdungen auch die polizeirechtliche Unterscheidung von Störern und Nichtstörern ins Wanken gerät[94]. Damit wird ein in der Polizeirechtsdogmatik wichtiger Grundsatz zugunsten einer Polizeiarbeit in den Hintergrund gedrängt, in der Nichtstörer und Unverdächtige ihren spezifischen Schutz verlieren[95].

---

89 *Rachor* (o. Fn. 85), S. 272; zum Begriff der *Definitionsmacht* vgl. *Feest/Blankenburg*, Die Definitionsmacht der Polizei, Düsseldorf 1972, S. 19 f.

90 *Schenke*, AöR 2000, 32.

91 Vgl. *SächsVerfGH*, LKV 1996, 284.

92 *SächsVerfGH*, ebenda. Näher zur Entscheidung zum Sächsischen Polizeigesetz vgl. *Paeffgen*, NJ 1996, 454 ff.; *Bäumler*, NVwZ 1996, 765 ff.; *Habermehl*, SächsVBl. 1996, 201 ff.; *W. R. Schenke*, DVBl. 1996, 1393 ff.; *Götz*, JZ 1996, 969 ff. und *Roggan*, KJ 1997, 80 ff..

93 *Kutscha*, CILIP 72 (2/2002), 65 f.

94 *Schenke*, AöR 2000, 31.

95 Ausführlich *Roggan*, (o. Fn. 7), S. 61 ff.

2. Verstoß gegen Gesetzgebungskompetenzen?

Mitunter wird von Teilen des Schrifttums unter Verweis auf Art. 73 Nr. 7 GG ein Verstoß gegen Gesetzgebungskompetenzen behauptet[96]. In der Tat spricht der Wortlaut der Bestimmung für eine solche Auffassung: Die ausschließliche Gesetzgebungskompetenz über das Postwesen und die Telekommunikation liegt demnach beim Bund. Es wird deshalb angenommen, dass es bei der Überwachung der Telekommunikation ja gerade um die umfassende Nutzung der heutigen technischen Potentiale gehe[97]. Deshalb komme nur eine Gesetzgebungskompetenz des Bundes in Betracht.

In der Tat haben bundesrechtliche Normen erst die Möglichkeit zur heute bekannten Nutzung der Telekommunikation zu polizeilichen und anderen Zwecken geschaffen. Genannt sei hier nur § 88 TKG, dessen Regelungsgehalt an anderer Stelle erläutert wurde[98].

Demgegenüber geht das überwiegende Schrifttum davon aus, dass Art. 73 Nr.7 GG mit dem Begriff der Telekommunikation nur den Signaltransport erfasse, nicht dagegen das Transportierte. Die Kompetenzbestimmung betreffe demnach nur die fernmeldetechnische Seite von Kommunikationsvorgängen[99]. Die Länder könnten durchaus in kompetenzgerechter Weise in das Grundrecht aus Art. 10 GG eingreifen[100].

Letztgenannter Auffassung ist zu folgen. Für das Recht der allgemeinen Gefahrenabwehr liegt die Gesetzgebungskompetenz unzweifelhaft bei den Ländern (Art. 70 I GG). Art. 73 Nr.7 GG kann dem Bund deshalb im Bereich der Überwachung der Telekommunikation keine aus der sonstigen Zuständigkeit zur allgemeinen Gefahrenabwehr herausgenommene Kompetenz verleihen[101]. Partikulares (allgemeines) Gefahrenabwehrrecht bundesrechtlicher Natur kann es nicht geben. Die Vertreter der gegensätzlichen Auffassung müßten deshalb zu dem Ergebnis gelangen, dass Gefahrenabwehr mittels einer Überwachung der Telekommunikation schlechthin ausgeschlossen ist. Dies wäre ein nicht sachgerechtes Ergebnis. Zum Zwecke der Abwehr von qualifizierten Gefahren für hochrangige Rechtsgüter muß die Polizei prinzipiell die Möglichkeit zu entsprechenden Maßnahmen besitzen. Die Einzelheiten können nur im (Landes-)Polizeirecht geregelt werden. An der Bedenklichkeit von Ermächtigungen, die über die polizeiliche Bewältigung der genannten Gefahrenlagen hinausgehen, ändert dies freilich nichts.

---

96 *Weitemeier*/*Große*, Kriminalistik 1997, 338; *Mann*/*Müller*, ZRP 1995, 183; *Randl*, NVwZ 1992, 1072.

97 So *Kutscha*, demnächst in LKV.

98 Siehe oben unter 1.; vgl. auch *Schenke*, AöR 2000, 14.

99 *Stettner* in: GG (Hrsg. Dreier), Stuttgart 1998, Art. 73 Rdnr. 31 n.w.N.; *Paeffgen* (o. Fn. 7), S. 1305; *Schenke*, AöR 2000, 14.

100 AK-GG-*Bizer* (o. Fn. 71), Art. 10 Rdnr. 78; BK-*Badura*, Art. 10 Rdnr. 45, jeweils m.w.N..

101 *Paeffgen* (o. Fn. 7), S. 1305.

III. Gesetzgeberische Perspektive: Datenvorratsspeicherung ?

Es war schon im Jahr 2002 nur eine Frage der Zeit, bis die Unternehmen per Gesetz auch zur planmäßigen Datenvorratshaltung für die Sicherheitsbehörden verpflichtet werden. Der Bundesrat hat einen in diese Richtung weisenden Gesetzentwurf bereits verabschiedet[102], in dem beispielsweise für den Bereich der Teledienste die planmäßige Datenvorratsspeicherung vorgesehen ist (§ 6 a TDDSG-E). Satz 1 der Vorschrift soll lauten:

> *„Die Bundesregierung erläßt für Diensteanbieter durch Rechtsverordnung mit Zustimmung des Bundesrates Vorschriften zur Vorratsspeicherung für die Zwecke der Strafverfolgung und der Gefahrenabwehr und für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes.«*

Auch von europäischer Seite gibt es Bestrebungen, eine umfassende Datenvorratsspeicherung im Bereich der Telekommunikation zu ermöglichen. Ein entsprechender Richtlinienentwurf ist inzwischen vom europäischen Rat, der Kommission und dem Europarat gebilligt worden. Er sieht die Möglichkeit vor, Speicherpflichten für Verbindungsdaten gesetzlich festzulegen. Zwar wird insoweit keine Verpflichtung der Mitgliedstaaten zur Umsetzung statuiert, jedoch steht zu befürchten, dass die entsprechende Änderung von nationalstaatlicher Seite zum Anlaß für entsprechende gesetzgeberische Tätigkeit wird[103].

Eine solche Datenvorratsspeicherung jedoch hat das Bundesverfassungsgericht im Volkszählungsurteil ausdrücklich ausgeschlossen: »Ein Zwang zur Angabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren« [104]. Um gerade eine solche Vorratsdatensammlung aber handelt es sich bei Daten, bei deren Erhebung keineswegs feststeht, ob sie überhaupt jemals zu staatlicher Zweckverfolgung (z.B.: Strafverfolgung) benötigt werden. Die flächendeckende Erfassung der gesamten Bevölkerung hinsichtlich ihres Kommunikationsverhaltens und damit die planmäßig Erfassung von unverdächtigen Bürgern[105] dürfte damit – nicht nur im Bereich der Teledienste – verfassungswidrig sein[106].

Das Fernmeldegeheimnis ist aus vielerlei Hinsicht in Bedrängnis. Von einer Unverletzlichkeit, wie sie Art. 10 I GG (noch) formuliert, kann kaum noch ausgegangen werden. Längst hat die Überwachung der Telekommunikation »einen Zug ins Massen-

---

102 BR-Drucks. 275/02.

103 *Gehrken*, Forum Recht 2002, 99.

104 *BVerfGE* 65, 1 (45).

105 So der schleswig-holsteinische Datenschutzbeauftragte *Bäumler*, siehe unter http://www.heise.de/newsticker/data/ad-26.08.02-000 .

106 Eine ausführliche verfassungsrechtliche Analyse findet sich unter http://www.datenschutzzentrum.de/material/themen/rotekarte/hintergr.htm .

hafte« gewonnen[107]. Inzwischen stellt die Gesamtheit der Eingriffsbefugnisse in Frage, ob das Grundrecht aus Artikel 10 GG nicht bereits in seinem Wesensgehalt (Art. 19 II GG) angetastet wird, die Möglichkeiten zulässiger Begrenzung also (längst?) ausgeschöpft sind. Es ist leider so: Man muß bei jedem Telefonkontakt in Deutschland mit dem Abhören rechnen[108].

107 *Welp* in: Holznagel/Nelles/Sokol, Die neue TKÜV, München 2002, S. 5.
108 Ebenso *Kloepfer* (o. Fn. 4), S. 91.