

## **Stellungnahme**

in dem Verfassungsbeschwerdeverfahren  
des Herrn S., 26121 Oldenburg

gegen

§ 33a Abs. 1 Nrn. 2 und 3 des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung (Nds. SOG) in der Fassung der Änderung durch Art. 1 des Gesetzes vom 11. Dezember 2003 (Nds. GVBl S. 414)

### **1 BvR 668/04**

#### **1. Zur bisherigen Entwicklung der polizeilichen Eingriffsbefugnisse im niedersächsischen Polizeirecht**

Um den Stellenwert der in § 33a Nds. SOG getroffenen Regelungen richtig bestimmen zu können, erscheint es notwendig, einleitend vorangehende Entwicklungen im niedersächsischen Polizeirecht aufzuzeigen.

Der mit der Verfassungsbeschwerde angegriffene § 33a Nds. SOG setzt eine Entwicklung in der Gesetzgebung fort, durch die die Polizei in zunehmendem Umfang ermächtigt wird, unabhängig von der Eingriffsschwelle einer konkreten Gefahr bzw. eines Anfangsverdachts bereits im Vorfeld von Gefahren und Straftaten tätig zu werden und dazu insbesondere Informationseingriffe vorzunehmen, die das Recht auf informationelle Selbstbestimmung und andere geschützte Freiheitsrechte berühren.

Bereits Ende der 80-er Jahre zeichnete sich in der politischen Diskussion die Tendenz ab, die Aufgabenfelder der Polizei erheblich auszuweiten. Bis zu diesem Zeitpunkt war es Aufgabe der Polizei, konkrete Gefahren abzuwehren und nach den Vorschriften der Strafprozessordnung Straftaten zu verfolgen. Auf der Grundlage des Vorentwurfs zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes von 1986 (VE MEPolG) wurden der Polizei die Aufgaben, Vorbereitungen zu treffen, um künftige Gefahren abwehren zu können, neu übertragen sowie in diesem Rahmen auch für die Verfolgung von Straftaten vorzusorgen und Straftaten zu verhüten (§ 1 Abs. 2 und 3 des Gesetzes zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung vom 18. Februar 1994, Nds. GVBl. S. 71, das auch die neue Gesetzesbezeichnung „Niedersächsisches Gefahrenabwehrgesetz“ festlegte). Diesen neuen Aufgaben war gemeinsam, dass die polizeiliche Tätigkeit nunmehr bereits im „Vorfeld“ von Gefahren und Straftaten einsetzen konnte, ohne dass auf der Tatbestandsseite eine Verdichtung des Sachverhalts zu einer konkreten Gefahr bzw. einem Anfangsverdacht gegeben sein musste. Die dadurch ausgelöste polizeiliche Tätigkeit besteht im wesentlichen in der Erhebung, der Speicherung

und dem Abgleich von Informationen, die in aller Regel aus personenbezogenen oder personenbeziehbaren Daten bestehen. Diese Datenverarbeitung im Vorfeld geriet bereits damals in eine gefährliche Nähe zu der im sog. Volkszählungsurteil des Bundesverfassungsgerichts (BVerfGE 65, 1) als unzulässig erachteten Vorratshaltung von Daten. Der Aufgabenzuwachs war sachlogisch verbunden mit einem Ausbau der polizeilichen Handlungsformen: Die Polizei erhielt nunmehr den Zugriff auf bisher nur den Verfassungsschutzbehörden vorbehaltene heimliche Ermittlungsmethoden, etwa die verdeckte Anfertigung von Bild- und Tonaufzeichnungen bei nicht dem Versammlungsgesetz unterliegenden Veranstaltungen (§ 27c des Änderungsgesetzes), die Aufzeichnung von Fernmelde-daten (§ 27d), die längerfristige Observation (§ 27e), den verdeckten Einsatz technischer Mittel, auch in einer Wohnung, (§ 27f) und den Einsatz von Vertrauenspersonen (§ 27g). In einer anschließenden Novelle des Nds. Gefahrenabwehrgesetzes durch das Änderungsgesetz vom 20. Mai 1996 (Nds. GVBl. S. 230) wurde die die weitreichenden Vorfeldbefugnisse begrenzende Anknüpfung an Straftaten von erheblicher Bedeutung in § 2 Nr. 9 und der damit verbundene Straftatenkatalog dadurch aufgeweicht, dass auch solche Vergehen einbezogen wurden, die bezogen auf das zu schützende Rechtsgut und die Strafandrohung den im Gesetz aufgezählten Vergehen „vergleichbar“ waren. Unklar blieb, welche Vergehen damit gemeint waren, denn die Strafandrohungen bei den schon bisher genannten Vergehen waren sehr unterschiedlich. Die Einschätzung, ob eine Straftat von erheblicher Bedeutung vorliegt, ging im Ergebnis auf den jeweiligen Dienststellenleiter über und wurde nicht mehr vom Gesetzgeber vorgegeben. Die noch bei den Gesetzesberatungen zur Novelle 1994 überwiegende Meinung, der Katalog stelle eine wesentliche Leitentscheidung dar und nur das Parlament solle den möglichen Rahmen heimlicher Ermittlungen im Vorfeldbereich bestimmen, wurde damit aufgegeben.

Ende 1997 erfolgte eine weitere Änderung des Nds. Gefahrenabwehrgesetzes durch das Gesetz zur Änderung datenschutz-, gefahrenabwehr- und verwaltungsverfahrenrechtlicher Vorschriften vom 28. November 1997 (Nds. GVBl. S. 489). Bis dahin war das heimliche Abhören von Wohnungen nur zulässig, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit unerlässlich ist und Tatsachen die Annahme rechtfertigen, dass die Person, der die Gefahr droht oder von der die Gefahr ausgeht, sich in der Wohnung aufhält. Durch eine neu angefügte Nr. 2 in § 35 Abs. 2 wurde dies dahingehend erweitert, dass das Lauschen in Wohnungen auch zur Abwehr der Gefahr, jemand könne eine Straftat von erheblicher Bedeutung begehen, zugelassen wurde. Neu eingefügt wurde auch die Befugnis, verdeckte Ermittler einzusetzen (§ 36a des Änderungsgesetzes). Dies war bis dahin nur in Ermittlungsverfahren nach der Strafprozessordnung möglich. Weiterhin wurden etwa zwei Drittel aller Bestimmungen, die den Grundrechtsschutz durch verfahrenssichernde Maßnahmen gewährleisten sollten, gestrichen. Dies betraf z.B. externe Anordnungskompetenzen (Richtervorbehalte) und die Pflicht zur Unterrichtung Betroffener nach verdeckten Datenerhebungen. Auch die bisherige öffentliche Berichtspflicht der Landesregierung gegenüber dem Landtag zu Entwicklungen polizeilicher Vorfeldaktivitäten wurde in § 37a durch eine Berichtspflicht gegenüber einem in nicht öffentlicher Sitzung tagenden parlamentarischen Ausschuss ersetzt.

Außerdem wurde die in § 12 Abs. 6 enthaltene Befugnis zu Kontrollen im Straßenverkehr ganz erheblich dadurch erweitert, dass nunmehr verdachts- und ereignisunabhängig zur Vorsorge für die Verfolgung oder zur Verhütung von Straftaten von erheblicher Bedeutung mit internationalem Bezug landesweit jeder Verkehrsteilnehmer angehalten und befragt sowie zur Aushändigung mitgeführter Ausweispapiere und zur Gestattung der Inaugenscheinnahme mitgeführter Sachen veranlasst werden kann. Bei diesen Maßnahmen der sogenannten Schleierfahndung war danach ein Zurechnungszusammenhang zwischen dem Kontrollierten und dem Lagebild, das Anlass für das polizeiliche Tätigwerden gegeben hat, nicht mehr erforderlich, so dass die Schleierfahndung zu Recht als reines Verdachtsschöpfungsinstrument bezeichnet worden ist.

Nach den Ereignissen des 11. Septembers 2001 wurde das Nds. Gefahrenabwehrgesetz erneut novelliert. Die Befugnisse der Polizei wurden im Bereich der Videoüberwachung und durch die Einführung der sog. Rasterfahndung erweitert. Hierdurch wurde zwar die Tätigkeit der Polizei nicht direkt noch weiter in das Vorfeld verlagert, jedoch werden durch die erweiterten Befugnisse in einem immer größer werdenden Umfang völlig unbeteiligte und gesetzestreue Bürgerinnen und Bürger von polizeilichen Maßnahmen betroffen. Die Polizei durfte nunmehr außerdem an öffentlichen Orten Videoaufzeichnungen vornehmen, wenn (nur) Tatsachen die Annahme rechtfertigen, dass dort künftig Straftaten von erheblicher Bedeutung begangen werden, ohne dies auf bestimmte Personen beziehen oder in anderer Weise konkretisieren zu müssen (§ 32 Abs. 3 Satz 2). Auch bei dieser Form der Erhebung und Speicherung personenbezogener oder personenbeziehbarer Daten ergibt sich wieder eine gefährliche Nähe zu der verfassungsrechtlich problematischen Datenerhebung auf Vorrat. Gleiches gilt für die sog. Rasterfahndung nach dem neuen § 45a. Hier werden durch die Polizei Daten von Personen erhoben, unabhängig davon, ob diese eine persönliche „Nähe“ zu der abzuwehrenden Gefahr oder zu den erwarteten Straftaten haben.

In einer vorerst letzten Novelle wurde Ende 2003 dann u.a. die hier angegriffene Bestimmung des § 33a (Datenerhebung durch Überwachung der Telekommunikation), durch die der Polizei die Befugnis gegeben wurde, Telekommunikationsdaten im Vorfeld einer Straftat und ohne Vorliegen einer konkreten Gefahr zu erheben, in das nunmehr wieder in die alte Bezeichnung umbenannte Niedersächsische Gesetz über die öffentliche Sicherheit und Ordnung eingefügt.

Der Niedersächsische Gesetzgeber hat sich somit in den letzten fünfzehn Jahren bei der rechtlichen Konditionierung polizeilicher Eingriffsbefugnisse immer mehr von der Eingriffsschwelle der (konkreten) Gefahr für die öffentliche Sicherheit entfernt. Polizeiliches Eingreifen soll nicht mehr nur der „Unterbrechung bereits laufender Kausalzusammenhänge dienen, welche die hinreichende Wahrscheinlichkeit eines Schadeneintritts begründen“ (Kugelmann: Der polizeiliche Gefahrenbegriff in Gefahr?, DÖV 2003, S. 781, 782), also der klassischen Gefahrenabwehr. Vielmehr sollen die polizeilichen Maßnahmen die Entstehung von Gefahren, insbesondere die Begehung von Straftaten, bereits im Vorfeld verhindern sowie für die Verfolgung künftiger Straftaten Vorsorge treffen und Straftaten verhüten. Dass diese Maßnahmen zu einem großen Teil im Sammeln und Abgleichen von

personenbezogenen oder -beziehbaren Informationen bestehen, ist eine zwangsläufige Folge. Betroffen von derartigen Informationseingriffen sind nicht nur Verantwortliche nach herkömmlichen polizeirechtlichen Kategorien, sondern auch und gerade Nichtverantwortliche. Insofern kommt es in besonderer Weise darauf an, dass die damit verbundenen Eingriffe in das Recht auf informationelle Selbstbestimmung auf der Grundlage hinreichend bestimmter und auch angemessener Tatbestandsvoraussetzungen erfolgen und dass die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit gewahrt bleiben. Durch die Beachtung dieser verfassungsrechtlichen Grundsätze wird verhindert, „dass der Gesetzgeber die eigenen staatlichen Grundlagen gefährdet, indem er in seinem Bemühen, Stärke und Schutzfähigkeit öffentlich darzustellen, über das Ziel hinausschießt und rechtliche Grundlagen und Schutzpositionen der Bürger in unverhältnismäßiger Weise abbaut“ (Kugelman, a.a.O., S. 782).

## **2. Zahlen zur Bedeutung des Zugriffs auf Daten der Telekommunikation**

Der Datenschutz ist bei der repressiven wie präventiven Telekommunikationsüberwachung besonders gefordert, weil sie heimlich erfolgt und eine große Zahl in aller Regel völlig unbeteiligter Dritter, nämlich die Kommunikationspartner der überwachten Person, betroffen ist. Telekommunikationsüberwachung ist dabei nicht mehr nur auf das klassische „Hineinhören“ in Telefonate, also auf die Gesprächsinhalte gerichtet, sondern bezieht gemäß § 33a Abs. 2 Nr. 2 Nds. SOG auch die Telekommunikationsverbindungsdaten ein. Damit werden also Informationen darüber zugänglich, wer mit wem wann wie lange telefoniert, welche SMS-Verbindung gewählt oder welche Verbindung im Internet benutzt hat.

### **2.1 Zahlen zur Telekommunikationsüberwachung nach § 100a StPO**

Zahlen zur „klassischen“ Telefonüberwachung im Sinne des § 100a StPO zeigen in den letzten Jahren eine Entwicklung auf, die Besorgnis erregend ist. Die Gesamtzahl hat sich von 1990 bis 2000 versechsfacht, in absoluten Zahlen von ungefähr 2.500 auf 15.750 im Jahre 2000. Neueste Zahlen der Regulierungsbehörde für Telekommunikation und Post besagen, dass sich die Zahl der Überwachungsmaßnahmen nach § 100a StPO gegenüber 21.874 Fällen im Jahr 2002 auf nunmehr 24.441 Fälle im Jahr 2003 nochmals deutlich erhöht hat. Ausgehend von 4.674 Überwachungsanordnungen im Jahre 1995 ergibt sich somit eine Steigerungsrate von über 400% in weniger als einem Jahrzehnt (vgl. die Pressemitteilung des Bundesbeauftragten für den Datenschutz vom 29. Juni 2004, <http://www.bundesdatenschutzbeauftragter.de>).

Eine Statistik darüber, wie viele Gespräche im Rahmen dieser Überwachungsanordnungen jeweils abgehört worden sind, existiert offensichtlich nicht. Nach den in dem Gutachten des Max-Planck-Instituts Freiburg (Hans-Jörg Albrecht, Claudia Dorsch, Christiane Krüpe, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, Kriminologische Forschungsberichte aus dem MPI, Bd. 115, Freiburg/Br., 2003 bzw. [http://www.iuscrim.mpg.de/verlag/online/Band\\_115.pdf](http://www.iuscrim.mpg.de/verlag/online/Band_115.pdf) – die folgenden Fundstellenhin-

weise beziehen sich auf die Internetveröffentlichung) veröffentlichten Zahlen sind bei 21 %, also in einem Fünftel der Anordnungen, jeweils 1.000 bis 5.000 Gespräche, in weiteren 8 % der Anordnungen jeweils über 5.000 Gespräche abgehört worden. Spitzenreiter bei einer Stichprobe ist eine Anordnung, aufgrund der 30.500 Gespräche abgehört worden sind (Seite 444). Diese Zahlen machen deutlich, dass es eine verkürzte Sichtweise ist, wenn als Betroffener nur der jeweilige Inhaber des Anschlusses gesehen wird, für den eine Telefonüberwachung angeordnet wird. Betroffen und in ihrem Recht auf vertrauliche Kommunikation aus Art. 10 GG sowie in ihrem Recht auf informationelle Selbstbestimmung berührt sind vielmehr neben dem Betroffenen und den ggf. den Anschluss mitnutzenden Familienangehörigen auch alle Gesprächspartner von Telefonaten, die von dem überwachten Anschluss aus oder mit ihm geführt werden. Insofern liegt die Zahl der von einer Telefonüberwachung Betroffenen um ein Vielfaches höher als es die veröffentlichten Zahlen der Anordnungen vermitteln wollen.

Bedeutsam für eine Bewertung ist auch, dass ausweislich des vorgenannten Gutachtens in nur rund 60 % aller Fälle überhaupt Ermittlungserfolge erzielt wurden (Seite 455). Von diesen Erfolgen entfielen lediglich 28 % auf unmittelbare Erkenntnisse, von denen wiederum 69 % der Fälle Selbstbelastungen und 12 % Aussagen Dritter wegen einer Katalogstraftat waren (Seite 456). Bezogen auf die Gesamtzahl der Anordnungen ergibt sich demnach ein unmittelbarer Erfolg für die Straftatenaufklärung in Höhe von nur etwa 13,6 %.

62 % der erfolgreichen Maßnahmen entfielen auf mittelbare Erkenntnisse, von denen wiederum 41 % Hinweise auf Straftaten Dritter ergaben (Seite 455). Bezogen auf die Gesamtzahl der Maßnahmen hat es also in rund 15 % Hinweise auf Straftaten Dritter gegeben.

Selbst wenn man diese unbeabsichtigte und unkalkulierbare Folge der Maßnahmen mit zu den Erfolgen zählt, so bleibt dennoch festzustellen, dass die Überwachungsmaßnahmen insgesamt in lediglich etwa 28,6 % aller Fälle erfolgreich waren.

Letztlich haben nur in 16 % aller Anordnungen die aufgrund der Telefonüberwachung gewonnenen Beweismittel auch Eingang in die Anklageschrift gefunden, so dass bei 84 % der Anordnungen die Erkenntnisse nicht unmittelbar für die Anklage von Bedeutung gewesen sind.

Nach der StPO kann die Dauer der Überwachungsmaßnahme maximal drei Monate betragen. Drei Viertel aller Anordnungsbeschlüsse haben dieses Maximum ausgeschöpft, obwohl tatsächlich in wiederum drei Viertel aller Anordnungen nur über einen Zeitraum von bis zu zwei Monaten abgehört worden ist (Seite 442).

Besonders bedenklich war nach den Erkenntnissen dieser Untersuchung, dass nur 24 % der untersuchten Anordnungsbeschlüsse substantiell begründet waren (Seite 447). In allen anderen Fällen sind Formularbegründungen übernommen worden. Noch bedenklicher ist, dass in 73 % der Fälle die betroffenen Anschlussinhaber in keiner Weise informiert worden sind (Seite 450). Das heißt, dass die gesetzlich vorgegebene Benachrichtigungspflicht in diesen Fällen schlicht unterlassen worden ist. Eine Benachrichtigung der Gesprächspartner von Telefonaten, die von dem fraglichen Anschluss aus oder mit ihm geführt worden sind, ist in keinem Fall erfolgt, obwohl, wie dargelegt, diese in gleicher Weise wie der Anschlussinhaber in ihren Rechten berührt waren.

Die 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. September 2003 in Leipzig hat sich in einer Entschließung eingehend mit den aus der Untersuchung des Max-Planck-Instituts zu ziehenden Folgerungen befasst ([http://www.bfd.bund.de/information/DS-Konferenzen/66dsk\\_ent2.html](http://www.bfd.bund.de/information/DS-Konferenzen/66dsk_ent2.html)).

## **2.2 Zahlen zur Abfrage von Telekommunikationsverbindungsdaten nach §§ 100g und h StPO**

Heute wird an Stelle des Abhörens von Inhalten sehr viel häufiger von der Möglichkeit Gebrauch gemacht, Verbindungsdaten abzufragen, weil die Polizei bzw. die Strafverfolgungsbehörde auf der einen Seite den technischen und personellen Aufwand scheut, der mit einem Hineinhorchen in die Telefongespräche und dem Aufnehmen der Gesprächsinhalte sowie deren Auswertung verbunden ist, und es auf der anderen Seite oft als zielführender oder auch als ausreichend bewertet, Informationen darüber zu bekommen, wer mit wem kommuniziert hat.

Es gibt leider zu der Zahl der Fälle, in denen die Herausgabe von Verbindungsdaten auf der Grundlage der §§ 100g und h StPO verlangt worden ist, und zur Zahl der davon betroffenen Verbindungsdatensätze keine veröffentlichte Statistik. Schon bei der Abfrage von Bestandsdaten nach § 90 TKG ergeben sich nach einer groben Übersicht, die von der RegTP stammt und dem Bundesbeauftragten für den Datenschutz vorliegt, aber Zahlen, die in ihrer Höhe, aber auch in den jährlichen Steigerungsraten alarmierend sind: Danach gab es 2001 1,5 Mio. Anfragen, 2002 2,0 Mio. Anfragen und 2003 2,7 Mio. Anfragen von Sicherheitsbehörden bei Telekommunikationsanbietern. Da die Anfragen nach Bestandsdaten der Telekommunikation vielfach der Vorbereitung von Maßnahmen der Telekommunikationsüberwachung und dabei insbesondere der Abfrage von Verbindungsdaten dienen dürften, ist davon auszugehen, dass die Zahl der von Abfragen der Sicherheitsbehörden erfassten Verbindungsdatensätze noch erheblich höher liegt.

Das Bundesverfassungsgericht hat in seinem Urteil vom 12. März 2003 (1 BvR 330/96 und 1 BvR 348/99) unter Rd.Nr. 94 zu der sogenannten Zielwahlsuche, bei der ermittelt wird, von welchen Anschlüssen aus Telefonate mit dem überwachten Anschluss geführt worden sind, folgende Zahlen festgestellt: „Im Jahre 2002 wurde nach Auskunft der Deutschen Telekom jede der 216 Millionen täglich hergestellten Telefonverbindungen innerhalb der dreitägigen Dauer der Speicherung der jeweiligen Verbindungsdatensätze durchschnittlich zweimal in eine Zielwahlsuche einbezogen.“

Der Leiter der Abteilung „Staatliche Sicherheitssonderauflagen“ der Deutschen Telekom hat nach einem bei heise online am 17. Oktober 2003 erschienenen Bericht beklagt, dass der Hunger der Ermittler nach den heiß begehrten Verbindungsdaten stark zugenommen und verfassungswidrige Auswüchse erreicht habe, so dass die Verhältnismäßigkeit und die Grundrechtsverträglichkeit der Eingriffe nicht mehr gewahrt sei. Allein die Anordnung massenhafter Zielwahlsuchläufe bei Straftaten von allenfalls mittlerer Schwere habe ganz große Ausmaße angenommen. Um nur die häufig verlangten Kontakte zu ausländischen Handy-Nutzern herausgeben zu können, müsste die Telekom ihre 50 Millionen Kunden alle drei Monate komplett durchrastern. Dazu kämen täglich Tausende Abfragen von Verbindungsdaten allgemeiner Natur. Obwohl das Gesetz die Rechtmäßigkeit des Eingriffs

gemäß der Interpretation des Bundesverfassungsgerichts nur bei Straftaten von erheblicher Bedeutung und einem konkreten Tatverdacht erlaube, verstünden ihn die Strafverfolger als allgemeinen Anspruch.

Diese Zahlen und Aussagen belegen, dass die Abfrage von Verbindungsdaten ganz offensichtlich zu einem Standardermittlungsinstrument der Sicherheitsbehörden geworden ist und dass die Zahl der von derartigen Maßnahmen Betroffenen, das sind auch hier wieder sämtliche Kommunikationspartner aller abgefragten Verbindungen, schon jetzt eine Größenordnung erreicht, die herkömmliche Vorstellungen übersteigt und die Frage aufwirft, inwieweit bei der Nutzung der Telekommunikation überhaupt noch eine Vertraulichkeit gegeben ist.

Hierbei ist auch berücksichtigen, dass es außerhalb der StPO noch weitere Zugriffsmöglichkeiten auf die Telekommunikation gibt, nämlich durch das Zollkriminalamt nach dem Außenwirtschaftsgesetz und vor allem auch durch die Behörden des Verfassungsschutzes, deren Befugnisse im Zusammenhang mit den Terrorismusbekämpfungsgesetzen weiter ausgedehnt worden sind.

Wenn neben diesen schon vorhandenen Zugriffsmöglichkeiten nun auch noch die präventive Telekommunikationsüberwachung der Polizei ermöglicht wird, dann entsteht aus meiner Sicht endgültig eine nicht mehr akzeptable Schiefelage zwischen der Verpflichtung des Staates zur Gewährleistung individueller und kollektiver Sicherheit einerseits und seiner Pflicht andererseits, die Freiheitsrechte der Bürgerinnen und Bürger auf vertrauliche Kommunikation aus Art. 10 GG (und ihr Recht auf informationelle Selbstbestimmung) gerade auch gegenüber Informationseingriffen des Staates zu sichern.

### **3. Regelungsbefugnis des Landesgesetzgebers für eine präventive Telekommunikationsüberwachung im Polizeirecht**

Die Zielrichtung von Ermittlungen auf der Grundlage des § 33a Abs. 1 Nr. 2 und 3 Nds. SOG, die kriminalistisch vielfach als Initiativermittlungen bezeichnet werden, ist zumindest im Kern auf die Aufklärung von Straftaten gerichtet. Insoweit heißt es in Ziffer 6.1 der Gemeinsamen Richtlinien der Justizminister/-senatoren und der Innenminister/-senatoren der Länder über die Zusammenarbeit bei der Verfolgung der Organisierten Kriminalität vom 13. November 1990 (JMBl. NW S. 267): „Organisierte Kriminalität wird nur selten von sich aus offenbar, Strafanzeigen in diesem Bereich werden häufig nicht erstattet, u. a. weil die Zeugen Angst haben. Die Aufklärung und wirksame Verfolgung der Organisierten Kriminalität setzt daher voraus, dass Staatsanwaltschaft und Polizei von sich aus im Rahmen ihrer gesetzlichen Befugnisse Informationen gewinnen oder bereits erhobene Informationen zusammenführen, um Ansätze zu weiteren Ermittlungen zu erhalten (Initiativermittlungen)“. Weiter wird in Ziffer 6.4 der Gemeinsamen Richtlinien dargelegt, dass bei Initiativermittlungen die Elemente der Strafverfolgung und der Gefahrenabwehr häufig in Gemengelage vorliegen oder im Verlauf eines Verdichtungs- und Erkenntnisprozesses ineinander übergehen.

Hierdurch wird klargestellt, dass bei Initiativermittlungen zwar auch Elemente der Gefahrenabwehr eine Rolle spielen können, jedoch im Regelfall „die Aufklärung und wirksame

Verfolgung“ (Ziffer 6.1 der Gemeinsamen Richtlinien) im Vordergrund stehen. Jedenfalls ist nicht ersichtlich, dass nach Durchführung der Initiativmittlungen noch Raum für konkrete Gefahrenabwehrmaßnahmen ist, ohne dass nicht zugleich der Anfangsverdacht für Straftaten vorliegt. Auch die Entwurfsbegründung räumt dies ein, wenn dort (LT-Drs. 15/240, S. 18) ausgeführt wird, dass „letztlich auch Anhaltspunkte zur Begründung eines konkreten Anfangsverdacht einer Straftat“ ermittelt werden sollen. In der vom Niedersächsischen Landtag zum Entwurf des Änderungsgesetzes durchgeführten Anhörung ist dazu auf folgende „groteske“ Konsequenz hingewiesen worden: „Die Polizeibehörden müssten geradezu nach Kräften bemüht sein, einen Anfangsverdacht im strafprozessualen Sinne zu verneinen“. Dann nämlich brauchten die strengeren Tatbestandsvoraussetzungen und Verfahrensregelungen der §§ 100a ff. StPO nicht beachtet zu werden, es stünde unter weitaus niedrighschwelligeren Voraussetzungen der weite Anwendungsbereich der polizeirechtlichen Initiativ-TKÜ zur Verfügung, um (letztlich) im Ergebnis ebenfalls Strafverfolgung zu betreiben (Generalstaatsanwalt Range, Vorlage 4 zu LT-Drs. 15/240, S. 11, unter Buchstabe h).

Geht es im Kern aber um die Bekämpfung von Straftaten, so erscheint es naheliegend, dass für Regelungen zur Initiativmittlung, wie sie § 33a Abs. 1 Nr. 2 und 3 Nds. SOG ermöglicht, keine Gesetzgebungskompetenz des Landesgesetzgebers besteht, sondern dass hier die gemäß Art. 74 Abs. 1 Nr. 1 GG für den Bund bestehende Regelungsbefugnis mit der StPO sowie anderen einschlägigen Gesetzen bereits in abschließender Weise ausgeschöpft worden ist.

Zudem hat der Bundesgesetzgeber die ausschließliche Gesetzgebungskompetenz für die Telekommunikation nach Art. 73 Nr. 7 GG und damit auch die alleinige Befugnis, Einschränkungen der Telekommunikation gesetzlich zu regeln (Honnacker / Beinhofer, Kommentar zum Bay. Polizeiaufgabengesetz, 17. Auflage, 1999, Art. 34, Nr. 9 sowie Kutscha, Anhörung im Bay. Landtag am 1.7.2003, Drucksache 14/91(VF), Seiten 15/16).

Der Bundesgesetzgeber hat in der Telekommunikations-Überwachungsverordnung (TKÜV) vom 22. Januar 2002 (BGBl. I S. 458), zuletzt geändert durch Artikel 328 der Verordnung vom 25. November 2003 (BGBl. I S. 2304) nur die Anforderungen an die Gestaltung der technischen Einrichtungen geregelt, die zu stellen sind, um Telekommunikationsüberwachungen nach den Bestimmungen der Strafprozessordnung, des Artikel 10-Gesetzes sowie des Außenwirtschaftsgesetzes durchführen zu können. Regelungen für (sonstige) präventive Telekommunikationsüberwachungen sind nicht getroffen.

Das Gegenargument, die Länder hätten die Kompetenz für die Gefahrenabwehr, ist zwar richtig, jedoch hier nicht einschlägig, da sich die Vorschriften der Telekommunikationsüberwachung darauf stützen, die heutigen technischen Möglichkeiten gezielt zur Überwachung zu nutzen. Deshalb hätte der Bundesgesetzgeber im § 1 TKÜV bestimmen müssen, dass diese Anforderungen auch für (präventive) Überwachungsmaßnahmen der Länder Geltung haben sollen, was aber nicht geschehen ist.

Aufgrund dieses Arguments hat letztlich der Bayerische Landtag im Jahre 2002 auf die Einführung einer präventiven Telekommunikationsüberwachung verzichtet (Kutscha, Protokoll der Anhörung des Ausschusses für Inneres und Sport des Nds. Landtages am 24. September 2003, Seite 24).

In der Gesetzesbegründung wird zur Begründung der Gesetzgebungskompetenz des Landes auf die sog. 1. Rundfunkentscheidung des Bundesverfassungsgerichts vom 28.02.1961 Bezug genommen (BVerfGE 12, 205, 225). Hierbei wird jedoch übersehen, dass diese Entscheidung nicht geeignet ist, in verallgemeinernder Form zur Auslegung von Art. 73 Nr. 7 GG beizutragen. Das Gericht hatte seinerzeit entschieden, dass das Hamburgische Gesetz betreffend den Staatsvertrag über den Norddeutschen Rundfunk vom 10. Juni 1955 (GVBl. I S. 197), soweit es sich auf § 3 Absatz 1 des Staatsvertrages bezieht, mit Artikel 73 Nr. 7 des Grundgesetzes insofern unvereinbar und daher nichtig ist, als § 3 Absatz 1 des Staatsvertrags dem Norddeutschen Rundfunk das ausschließliche Recht vorbehält, sendetechnische Anlagen des Hörrundfunks und des Fernsehrundfunks zu errichten und zu betreiben (BVerfGE 12, 205, Leitsatz 1). In diesem engen Zusammenhang hat das Gericht sodann die für das konkrete Verfahren erforderliche Abgrenzung zwischen Bundes- und Länderkompetenzen vorgenommen:

„Das Post- und Fernmeldewesen im Sinne von Art. 73 Nr. 7 GG umfaßt – wenn man vom Empfang der Rundfunksendungen absieht – nur den sendetechnischen Bereich des Rundfunks unter Ausschluß der sogenannten Studiotechnik.

Art. 73 Nr. 7 GG gibt dem Bund nicht die Befugnis, die Organisation der Veranstaltung und die der Veranstalter von Rundfunksendungen zu regeln.“ (Leitsätze 3 a und 3 b).

Generelle Rückschlüsse für die Regelungszuständigkeit bei der präventiven TKÜ können aus dieser Entscheidung also entgegen der Gesetzesbegründung nicht gezogen werden.

#### **4. Bestimmtheit und Klarheit der tatbestandlichen Voraussetzungen**

Ermächtigungen für Eingriffe in das Grundrecht aus Art. 10 Abs. 1 GG bedürfen, wie das Bundesverfassungsgericht in seinem Beschluss zu der präventiven TKÜ nach § 39 AWG durch das Zollkriminalamt erneut bekräftigt hat, einer gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenbestimmtheit und Normenklarheit entspricht. Die gleichen Anforderungen gelten nach dem Volkszählungsurteil des Bundesverfassungsgerichts auch für Eingriffe in das Recht auf informationelle Selbstbestimmung. Im übrigen hat das Bundesverfassungsgericht auch mit Nachdruck klargestellt, dass auch im Bereich der Straftatenverhütung Eingriffsermächtigungen keinen geringeren rechtsstaatlichen Anforderungen bezogen auf die Normenbestimmtheit und Normenklarheit unterliegen als Ermächtigungen zu Maßnahmen der Gefahrenabwehr und der Strafverfolgung (Beschluss v. 3.3.2004, 1 BvF 3/92, Leitsatz 2).

Eingriffe des Staates bedürfen einer normenbestimmten und normenklaren Rechtsgrundlage, damit der Betroffene die Rechtslage anhand der Gesetzeslage erkennen und sein Verhalten entsprechend ausrichten kann. Hierbei erhöhen sich die Anforderungen an die Bestimmtheit und Klarheit der Norm, wenn es sich um Eingriffe in grundrechtlich gesicherte Positionen handelt (Rd.Nr. 107).

Der Betroffene muss also erkennen können, bei welchen Anlässen und unter welchen Voraussetzungen ein bestimmtes Verhalten dazu führen kann, dass die Verwaltung in seine Grundrechtsposition eingreifen kann (Rd.Nr. 108).

Insoweit bestehen erhebliche Bedenken gegen den in § 33a Abs. 1 Nr. 2 Nds. SOG auf der Tatsachenseite gewählten Anknüpfungspunkt, dass Daten durch Überwachung und Aufzeichnung der Telekommunikation über Personen erhoben werden dürfen, „bei denen Tatsachen die Annahme rechtfertigen, dass sie Straftaten von erheblicher Bedeutung begehen werden.“ Es stellt sich die Frage, welchen Gehalt die Voraussetzung hat, wonach Tatsachen die Annahme einer drohenden Straftat rechtfertigen. Das Kriterium ist personenbezogen und kennzeichnet die Vermutung, dass aufgrund tatsächlicher Erkenntnisse und ihrer kriminalistischen Bewertung eine bestimmte Person Straftaten zu begehen beabsichtigt (Kugelman, DÖV 2003, 781, 785).

Angesichts der Unbestimmtheit der Formulierung ist es dem Betroffenen nicht möglich, etwaige Eingriffe in sein Grundrecht aus Art. 10 GG vorherzusehen. Die vom Gesetz geforderten „Tatsachen“ müssen aus kriminalistischer Erfahrung und Sichtweise gewertet und oft auch mit Zusatzinformationen verknüpft werden, um die Annahme möglich erscheinen zu lassen, eine Person werde künftig Straftaten von erheblicher Bedeutung begehen. Es handelt sich letztlich nur um Anhaltspunkte für die Notwendigkeit einer Verdachtsgewinnung oder Verdachtskonkretisierung, die den Anlass für polizeiliches Eingreifen bieten (Kugelman, DÖV 2003, 781, 785). Die zur Beurteilung der Tatsachen erforderliche kriminalistische Erfahrung und das ggf. erforderliche Zusatzwissen hat der Betroffene nicht. Es ist ihm also nicht möglich zu unterscheiden, ob sein konkretes Verhalten im einen Fall „verdächtig“, im anderen Fall jedoch „neutral“ und damit unverdächtig ist.

Er kann somit weder abschätzen, ob in sein Grundrecht eingegriffen werden kann, noch kann er sein Verhalten entsprechend ausrichten.

In noch erheblicherem Maße gelten diese Bedenken für den in § 33a Abs. 1 Nr. 3 Nds. SOG genannten Personenkreis. In diesen Fällen müsste die Kontakt- oder Begleitperson (§ 2 Nr. 11 Nds. SOG) zum einen den Versuch unternehmen, festzustellen, ob Tatsachen die Annahme rechtfertigen, dass Straftaten von erheblicher Bedeutung begangen werden sollen. Zu den vorstehend geschilderten Schwierigkeiten kommt bei der Beantwortung dieser Frage erschwerend hinzu, dass der Betroffene hier berücksichtigen müsste, dass die Tatsachen und der daraus zu ziehende Schluss nicht in seiner Person sondern der eines Dritten begründet sein müssen.

Zum anderen müsste die Kontakt- oder Begleitperson darüber hinaus beurteilen können, ob sie mit der dritten Person derartig in Verbindung steht, dass durch sie Hinweise auf die angenommene Straftat des Dritten erwartet werden können. Diese Beurteilungen sind schlicht nicht möglich.

Die verfassungsrechtlichen Anforderungen an die Bestimmtheit und Klarheit der Eingriffsnormen dienen darüber hinaus auch dazu, die Exekutive zu binden, indem ihr klare Maßstäbe für die notwendigen Abwägungsentscheidungen gegeben werden. Der Handlungsspielraum der Exekutive wird also durch das Gesetz begrenzt. Hierdurch wird der Bürger vor staatlichem Missbrauch geschützt. Diese Schutzfunktion ist umso wichtiger, wenn der Betroffene von dem Eingriff keine Kenntnis hat und es sich um unbeteiligte Dritte handelt, die mit einer staatlichen Überwachung nicht rechnen müssen und sich deshalb vor einem Einblick in ihren Privatbereich nicht schützen können.

Das verfassungsrechtliche Problem liegt darin, dass diese Regelungen auf eine *petitio principii* hinauslaufen, denn die „Tatsachen“, d.h. Erkenntnisse über tatsächliche Vorgänge, lassen sich eben gerade nur durch die Maßnahmen gewinnen, für deren Anordnung sie die gesetzliche Voraussetzung darstellen (Ipsen, Vorlage 2 zu LT-Drs. 15/240, S. 10), d.h. es handelt sich letztlich bei ihnen nur um Anhaltspunkte für die Notwendigkeit einer Verdachtsgewinnung oder Verdachtskonkretisierung.

Die verfassungsrechtlichen Anforderungen an die Bestimmtheit und Klarheit der Eingriffsnorm geben der Exekutive somit keine klaren Maßstäbe für die notwendigen Abwägungsentscheidungen.

Insoweit weicht die Gesetzeslage in Niedersachsen grundlegend von der Rechtslage ab, die das Bundesverfassungsgericht zu beurteilen hatte, als es entschied, dass Strafverfolgungsbehörden die Verbindungsdaten der Mobiltelefone von Journalisten verdeckt erheben dürfen, um so den Aufenthaltsort der Kontaktperson der Journalisten herauszufinden. Derartige Eingriffe in Art. 5 Abs. 1 S. 1 und Art. 10 GG wurden für zulässig erachtet, wenn die Ermittlungsmaßnahmen eine Straftat von erheblicher Bedeutung, einen konkreten Tatverdacht und eine hinreichend sichere Tatsachenbasis für die Annahme voraussetzt, dass der Betroffene als Nachrichtensmittler tätig werde (Urt. v. 12.3.2003, 1 BvR 330/96 und 1 BvR 348/99, Leitsatz 3).

Die beiden letzten Tatbestandsmerkmale („konkreter Tatverdacht“, bezogen auf § 33a Abs. 1 Nr. 2 und hinsichtlich § 33a Abs. 1 Nr. 3 Nds. SOG „sichere Tatsachenbasis für die Annahme, dass der Betroffene Nachrichtensmittler ist“) sind nach der niedersächsischen Gesetzeslage gerade nicht erforderlich. Die Vorschrift verwendet insoweit weder den präventiv orientierten Begriff der Gefahr noch den repressiv orientierten Begriff des Verdachts einer Straftat.

Das Strafrecht beginnt mit der – vollendeten oder versuchten – Straftat; es verfolgt den Täter. Das Gefahrenabwehrrecht weist insofern Überschneidungen mit dem Strafrecht auf, als Straftaten stets Störungen der öffentlichen Sicherheit sind und, sofern sie bevorstehen, unter anderem mit Mitteln des Polizeirechts verhindert werden können. Die Parallele zum Strafrecht beschränkt sich aber nicht hierauf. Auch bei jeder anderen Störung der öffentlichen Sicherheit (und Ordnung) sind Gefahrenabwehrmaßnahmen möglich, allerdings nur dann, wenn es einen „Täter“, also einen Störer, gibt. Einen Ausnahmefall bildet lediglich die Inanspruchnahme des Nichtstörers gem. § 8 Nds. SOG.

Anders als das Strafprozessrecht ist jedoch das (niedersächsische) Gefahrenabwehrrecht auf die Ermittlung von Gefahren und der hierfür verantwortlichen Personen eigentlich nicht zugeschnitten. Im Bereich der Vorfeldaufgaben, die nach § 1 Abs. 1 S. 3 Nds. SOG der Polizei obliegen, fehlt es nicht nur an einem Störer, es liegt auch noch keine konkrete Gefahr vor, für die ein Verantwortlicher ermittelt werden könnte. Die Vorfeldaufgaben sind also dadurch gekennzeichnet, dass sich die darauf fußenden Maßnahmen nur gegen potentielle Täter/Störer richten können. Angesichts der allgemeinen Unschuldsvermutung begegnet das Präventionsrecht insofern insgesamt verfassungsrechtlich erheblichen Bedenken (Ipsen, Vorlage 2 zu LT-Drs. 15/240, S. 10).

Präventionsmaßnahmen wurden lange Zeit nicht als Grundrechtseingriffe eingeordnet. Die Anerkennung des Eingriffscharakters einer Vielzahl solcher Maßnahmen führte dazu, dass die Exekutive hierfür Eingriffsermächtigungen benötigt, die den rechtsstaatlichen Bestimmtheitsanforderungen genügt (BVerfGE 65, 1, 44 ff, 54).

Je ungenauer die Ziele einer Normierung und die Anforderungen an die tatsächliche Ausgangslage gesetzlich umschrieben sind, umso schwerer fällt die Beurteilung der Eignung und Erforderlichkeit einer Maßnahme. Vor allem begründet die Unbestimmtheit der tatsächlichen Voraussetzungen das Risiko, dass zwischen Gemeinwohlbelangen, zu deren Wahrnehmung in Grundrechte eingegriffen wird, und den Rechtsgütern der von den Eingriffen Betroffenen nicht sachgerecht abgewogen werden kann.

Von maßgeblicher Bedeutung im Zuge der Abwägung ist insbesondere die Einschätzung der Schwere der dem Schutzgut drohenden Gefahr. Diese setzt Klarheit nicht nur über das gefährdete Rechtsgut, sondern auch über die dieses gefährdende Handlung voraus.

Der Bestimmtheitsgrundsatz verlangt, dass die jeweiligen Ermächtigungen handlungsbegrenzende Tatbestandselemente enthalten, die einen Standard an Vorhersehbarkeit und Kontrollierbarkeit vergleichbar dem schaffen, der für die überkommenen Aufgaben der Gefahrenabwehr und der Strafverfolgung rechtsstaatlich geboten ist (BVerfG, Beschluss v. 3.3.2004, 1 BvF 3/92, Rd.Nr. 113).

Dies gilt umso mehr für Überwachungsmaßnahmen im Anwendungsbereich des Art. 10 GG. Sieht der Gesetzgeber solche Maßnahmen auf dem Gebiet der Straftatenverhütung vor, so hat er die den Anlass bildenden Straftaten sowie die Anforderungen an die Verdachtstatsachen so bestimmt zu umschreiben, dass das Risiko einer Fehlprognose in dem Rahmen verbleibt, der auch für Maßnahmen der Strafverfolgung und der Gefahrenbekämpfung als verfassungsrechtlich hinnehmbar erscheint (Rd.Nr. 114).

Wie ausgeführt, werden die angegriffenen Bestimmungen diesen Anforderungen an die Verdachtstatsachen des § 33a Abs. 1 Nr. 2 und 3 Nds. SOG nicht gerecht.

Neben der Erhebung der Inhalte der Telekommunikation gewinnt – nicht zuletzt auch wegen der enormen Kosten und des häufig relativ geringen Erkenntniswertes „klassischer Abhörmaßnahmen“ – die Erforschung der Kommunikationswege, also die Beantwortung der Frage, wer hat wann mit wem wie lange kommuniziert, immer mehr an Bedeutung. Wie bereits dargestellt, wurde dazu im Rahmen der sog. Zielwahlsuche im Jahre 2002 jede der 216 Mio. täglich hergestellten Telefonverbindungen innerhalb der dreitägigen Dauer der Speicherung der jeweiligen Verbindungsdatensätze durchschnittlich zweimal in eine Abfrage einbezogen.

Angesichts der Möglichkeiten der Zielwahlsuche und der vorstehenden Zahlen wird deutlich, dass durch Maßnahmen nach § 33a Abs. 1 Nr. 2 und 3 Nds. SOG aufgrund unscharfer gesetzlicher Voraussetzungen nicht nur in Einzelfällen Personen betroffen sind sondern jeder Anwendungsfall Millionen Betroffener nach sich ziehen kann.

## 5. Erforderlichkeit

Erforderlich ist eine grundrechtseinschränkende Norm, wenn nicht ein anderes, gleich wirksames, aber das Grundrecht nicht oder weniger stark einschränkendes Mittel zur Verfügung steht (Verfassungsgerichtshof Rheinland-Pfalz, Urteil VGH B 2/04 vom 22.6.2004, Seite 16).

Die Erforderlichkeit der präventiven TKÜ ist – abgesehen von § 33a Abs. 1 Nr. 1 Nds. SOG – nicht nachgewiesen. Durch die neuen Befugnisse werden die bisherigen, wohlwogenen Trennungslinien zwischen den Kompetenzen von Verfassungsschutz, Polizei und Justiz „ohne ernsthaft nachgewiesene Notwendigkeit für Polizei und Justiz und ohne den Nachweis eines zusätzlich zu erwartenden Gewinns an Sicherheit für die Bevölkerung“ (Generalstaatsanwalt Range in der Anhörung, Vorlage 4 zu LT-Drs. 15/240, S. 1) verwischt.

Es sind im gesamten Rechtssetzungsverfahren keine Fälle aufgezeigt worden, die nicht bereits durch die bisherigen Regelungen der StPO gelöst werden könnten.

Zur Begründung der Notwendigkeit der präventiven Telekommunikationsüberwachung wird ausgeführt, die Auswerte- und Analysestellen der Kriminalpolizeiinspektionen-Organisierte Kriminalität (KPI-OK) gäben im Rahmen ihrer Tätigkeit regelmäßig Hinweise auf Sachverhalte, die sich oft noch im Planungsstadium und vor einem konkreten Anfangsverdacht einer Straftat nach § 152 Abs. 2 StPO befänden, aber deutliche Anzeichen einer kriminalistischen Relevanz böten, die mit adäquaten und effektiven Ermittlungsmethoden abgearbeitet werden müssten (LT-Drs. 15/240, S. 16, Abs. 1).

Die Eingriffsbefugnisse der Polizei müssten an die Handlungs- und Organisationsformen angepasst werden, die sich gerade im Bereich der Organisierten Kriminalität entwickelt hätten. Die präventive TKÜ sei daher erforderlich, um Sachverhalte weiter abzuklären, kriminelle Strukturen zu erhellen und dadurch letztlich auch Anhaltspunkte zur Begründung eines konkreten Anfangsverdachts einer Straftat zu ermitteln (LT-Drs. 15/240, S. 18, Abs. 2).

Weiterhin wird unter Berufung auf das Urteil des Sächsischen Verfassungsgerichtshofs vom 14.05.1996 (LKV 1996, 273 = NJW 1996, 1953f.) ausgeführt, dass es erforderlich, aber auch zulässig sei, dass die Polizei als Widerpart des Organisierten Verbrechens ihre Fahndungs- und Beobachtungsmethoden der Langfristigkeit und Weiträumigkeit der gegnerischen Strategien anpasse (LT-Drs. 15/240, S. 16, Abs. 2). Dazu gehöre auch, dass die Sicherheitsbehörden in die Organisation eindringen und bereits die frühe Entstehungsphase von Straftaten, die Zusammenhänge, die Arbeitsweisen mafiöser Gebilde und die sie steuernden Personen ergründen. Kriminalitätsbekämpfung und Vorfeldaktivität bestehe im Durchleuchten des kriminellen Umfeldes, im Erkennen von verbrechensbegünstigenden Strukturen und in der Feststellung sich einnistender Verbrechenslogistik sowie dem operativen Vorgehen gegen solche Gebilde, wie etwa der Beseitigung von Tatgelegenheiten und der Auflösung von Organisationen und Szenen (LT-Drs. 15/240, S. 16, Abs. 3).

Jedoch ist auch dann, wenn „die frühe Entstehungsphase von Straftaten, die Zusammenhänge, die Arbeitsweisen mafiöser Gebilde und die sie steuernden Personen“ ergründet werden müssen, wenn „deutliche Anzeichen einer kriminalistischen Relevanz“ vorliegen oder „Sachverhalte weiter abzuklären und kriminelle Strukturen zu erhellen“ sind, in aller Regel zugleich ein strafprozessualer Anfangsverdacht i.S.d. § 152 Abs. 2 StPO gegeben, da die Anforderungen hieran relativ gering sind (Generalstaatsanwalt Range in der Anhörung, Vorlage 4 zu LT-Drs. 15/240, S. 6). Die „Gemeinsamen Richtlinien der Justizminister/-senatoren und der Innenminister/-senatoren der Länder über die Zusammenarbeit bei der Verfolgung der Organisierten Kriminalität“ (MinBl. NW 1990, S. 1721) erläutert den Begriff, die Erscheinungsformen und Indikatoren der Organisierten Kriminalität. Danach versteht man unter Organisierter Kriminalität „die vom Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen, unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken“. Nach dieser Definition wird die Erkenntnisgewinnung über entsprechende Strukturen oder Aktivitäten immer auch den Anfangsverdacht einer Straftat (z.B. nach § 129 StGB) begründen, wodurch gleichzeitig deutlich wird, dass es letztlich im Kern um Maßnahmen zur Strafverfolgung geht. Zur Aufdeckung von Strukturen der Organisierten Kriminalität reichen daher auch aus Sicht von Polizeipraktikern die Befugnisse aus den §§ 100a ff StPO völlig aus (Polizeidirektor Mokros, Vorlage 11 zu LT-Drs. 15/240, S. 3).

Zur weiteren Begründung der präventiven TKÜ wird auf sog. Gemengelagen verwiesen, die z.B. bei erpresserischem Menschenraub oder bei einer Geiselnahme nach den §§ 239a, 239b StGB entstünden. Bei derartigen Situationen habe der Polizeieinsatz gleichzeitig repressiven und präventiven Charakter (LT-Drs. 15/240, S. 17).

Hierbei wird übersehen, dass zwar eine Zuordnung des Eingriffs zum Bereich der Gefahrenabwehr oder Strafverfolgung erforderlich ist, da unterschiedliche Voraussetzungen für den Eingriff bestehen können und unterschiedliche Gerichte für die Überprüfung der Rechtmäßigkeit des Eingriffs zuständig sind. Bei den in der Begründung aufgeführten Gemengelagen wird es jedoch nach der Beendigung der Situation selbstverständlich ein Strafverfahren geben und die etwaigen Aufzeichnungen der Gespräche werden als Beweismittel in das Verfahren eingeführt. Der Einsatz der Polizei ist also in diesen Fällen immer auch auf die Strafverfolgung gerichtet, sodass die Befugnisse der StPO insoweit ausreichend sind (Polizeidirektor Mokros, Vorlage 11 zu LT-Drs. 15/240, S. 3, 4).

Zudem werden die rechtlichen Probleme derartiger Gemengelagen durch § 33a Nds. SOG nicht beseitigt. Bisher konnte die Polizei, sofern die übrigen Voraussetzungen der §§ 100a ff. StPO vorlagen, entsprechende Überwachungsmaßnahmen einleiten. Nunmehr steht sie vor der Frage, ob sie die TKÜ-Maßnahmen wie bisher auf strafprozessualer oder auf gefahrenabwehrrechtlicher Grundlage durchführen soll, die Gemengelage bleibt jedoch unabhängig von der getroffenen Entscheidung erhalten.

Letztlich ausschlaggebend ist jedoch, dass die mit der Verfassungsbeschwerde angegriffenen Bestimmungen des § 33a Abs. 1 Nr. 2 und 3 Nds. SOG für die Lösung der recht-

lichen Probleme bei den in der Begründung genannten Gemengelage des erpresserischen Menschenraubs und Geiselnahme nach den §§ 239a, 239b StGB nicht einschlägig sind. Eine TKÜ-Maßnahme würde hier nämlich im gefahrenabwehrrechtlichen Bereich auf § 33a Abs. 1 Nr. 1 Nds. SOG zu stützen sein, da es um die Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit des Opfers und nicht um die Frage geht, ob eine Person eine Straftat von erheblicher Bedeutung begehen wird (§ 33a Abs. 1 Nr. 2) bzw. um Kontakt- oder Begleitpersonen einer solchen Person (§ 33a Abs. 1 Nr. 3).

Es ist also festzustellen, dass andere, gleich wirksame Mittel – nämlich die der StPO – zur Verfügung stehen, um die angestrebten Zwecke zu erreichen.

Auch die Betrachtung der polizeilichen Praxis bei der Nutzung der Möglichkeiten einer präventiven Telekommunikationsüberwachung belegt nicht die Notwendigkeit der angegriffenen Regelungen.

In Thüringen als dem einzigen Land, in dem zum Zeitpunkt des Inkrafttretens des neuen § 33a Nds. SOG bereits eine präventive Telekommunikationsüberwachung bestand, hat es nach einem Bericht in der taz vom 27. August 2003, der sich auf Angaben aus dem thüringischen Innenministerium bezieht, in dem Zeitraum eines Jahres 13 Anwendungsfälle gegeben, die sich aber alle – ausnahmslos – darauf bezogen, dass mit Hilfe der Abfrage der Verbindungsdaten zu einem aktiv geschalteten Handy Vermisste oder Verletzte gesucht wurden, also Fälle, die nach § 33a Abs. 1 Nr. 1 Nds. SOG zu behandeln und auch aus meiner Sicht datenschutzrechtlich unproblematisch sind.

Die bisherige Praxis in Niedersachsen seit Inkrafttreten des neuen § 33a Nds. SOG entspricht diesen Erfahrungen. In der Zeit vom 1. Januar bis zum 30. Juni 2004 gab es insgesamt fünf Anwendungsfälle des § 33a Nds. SOG, allerdings ausschließlich Fälle nach § 33a Abs. 1 Nr. 1 Nds. SOG. Die Unverzichtbarkeit der präventiven Telekommunikationsüberwachung in den Fällen des Abs. 1 Nr. 2 und 3 zur Bekämpfung der Organisierten Kriminalität und des internationalen Terrorismus hat sich also zumindest in den vergangenen sechs Monaten in Niedersachsen nicht bestätigt. Auch die von einigen Polizeipraktikern in den Anhörungen zum Gesetzentwurf dargestellten Szenarien haben danach ganz offensichtlich nicht die ihnen dort unterstellte Praxisrelevanz.

Ich gehe davon aus, dass sich unter anderem auch aus diesen Gründen der Gesetzgeber in Rheinland-Pfalz bei der Novellierungen des dortigen Polizeigesetzes auf Bestimmungen beschränkt hat, die dem niedersächsischen § 33a Abs. 1 Nr. 1 Nds. SOG entsprechen und von Regelungen entsprechend § 33a Abs. 1 Nr. 2 und 3 Nds. SOG abgesehen hat (§ 31 Abs. 1 des Polizei- und Ordnungsbehördengesetz (POG) in der Fassung vom 10. November 1993, zuletzt geändert durch Artikel 1 des Gesetzes vom 02.03.2004 (GVBl. S. 202 ff.)). Auch in Hessen enthält der Gesetzentwurf der Landesregierung vom 8. Juni 2004 (Drucksache 16/2352) unter Nr. 6 im neu einzufügenden § 15a „Datenerhebung durch Telekommunikationsüberwachung“ nur Regelungen, die die Überwachung an die Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person binden.

In diesem Zusammenhang stellt sich auch die Frage, ob der Straftatenkatalog der angegriffenen Vorschriften vor dem Hintergrund des Beschlusses des Bundesverfassungsgerichts vom 3.3.2004 (1 BvF 3/92, Rd.Nr. 179) verfassungsrechtlichen Vorgaben genügt. Hiernach sind bei einer eventuellen Neuregelung der präventiven Telekommunikationsüberwachung im Außenwirtschaftsgesetz die Grundsätze zu berücksichtigen, die das Gericht in seinen Urteilen vom gleichen Tage (1 BvR 2378/98 und 1 BvR 1084/99) aufgestellt hat. Diese Grundsätze sind auch in anderen Gesetzen, die die präventive Telekommunikationsüberwachung regeln, zu beachten. Ich beziehe dies auch auf die Ausführungen zu den Straftatenkatalogen in den Urteilen 1 BvR 2378/98 und 1 BvR 1084/99.

In Rd.Nr. 228 der letztgenannten Urteile führt das Gericht aus, dass der verfassungsrechtliche Begriff der besonders schweren Straftat nicht mit dem strafprozessualen Begriff einer Straftat von erheblicher Bedeutung gleichgesetzt werden kann. Bezogen auf Art. 13 Abs. 3 GG müsse es sich abstrakt um eine besonders schwere Straftat handeln. Dafür gäbe der Strafrahmen einen maßgebenden Anhaltspunkt. Von der besonderen Schwere einer Straftat im Sinne des Art. 13 Abs. 3 GG ist nur auszugehen, wenn sie der Gesetzgeber jedenfalls mit einer höheren Höchststrafe als fünf Jahre Freiheitsstrafe bewehrt hat (Rd.Nr. 238).

Eine Straftat von erheblicher Bedeutung müsse hingegen mindestens der mittleren Kriminalität zuzurechnen sein, den Rechtsfrieden empfindlich stören und geeignet sein, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen (Rd.Nr. 228).

Bei der Auswahl der in Betracht kommenden Delikte sei der Gesetzgeber (durch Art. 13 Abs. 3 GG) nicht auf solche Straftaten beschränkt worden, die typische Erscheinungsformen der Organisierten Kriminalität darstellen oder im konkreten Einzelfall in diesem Umfeld begangen würden (Rd.Nr. 231). Andererseits könnten Straftaten nicht allein deshalb als besonders schwer angesehen werden, weil sie für die Organisierte Kriminalität typisch sind. In ihrem Umfeld werden sowohl schwere wie auch leichte Straftaten begangen (Rd.Nr. 232).

§ 33a Abs. 1 Nr. 2 und 3 Nds. SOG fordern „Straftaten von erheblicher Bedeutung“. Diese sind in § 2 Nr. 10 Nds. SOG legaldefiniert. Hierbei dürfte § 2 Nr. 10 Buchst. a) noch relativ unproblematisch sein, da er Verbrechen mit Ausnahme von Straftaten nach den §§ 154 und 155 StGB nennt. § 2 Nr. 10 Buchst. b) hingegen zählt eine Reihe von Vergehen nach dem Strafgesetzbuch auf und umfasst darüber hinaus „nach dem Rechtsgut und der Strafandrohung vergleichbare Vergehen“. § 2 Nr. 10 Buchst. c) bestimmt darüber hinaus jedes banden- oder gewerbsmäßig begangene Vergehen zu einer Straftat von erheblicher Bedeutung.

Der Strafrahmen der in § 2 Nr. 10 Buchst. b) genannten Straftaten reicht von „bis zu drei Jahren“ (§§ 85 bis 86a und 174 bis 174b) bis zu „bis zu zehn Jahren“ (§§ 130 und 176). Allerdings ist in allen Bestimmungen mit Ausnahme der §§ 130 Abs. 1, 174 Abs. 1 und 176 auch (nur) eine Geldstrafe möglich.

Es erscheint daher mehr als fraglich, ob sich diese Straftaten mindestens der mittleren Kriminalität zuzurechnen lassen, den Rechtsfrieden empfindlich stören und geeignet sind, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen.

Insbesondere bei den banden- oder gewerbsmäßig begangenen Vergehen des § 2 Nr. 10 Buchst. c) dürften in einer Vielzahl der Fälle derartige Taten nicht geeignet sind, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen, da sich derartige Taten häufig im sog. „Kleinkriminellen-Milieu“ abspielen.

Zudem hat das Bundesverfassungsgericht in seiner Entscheidung 1 BvF 3/92 in Rd.Nr. 142 festgestellt, dass § 39 Abs. Satz 1 Nr. 1 AWG einen abgeschlossenen Straftatenkatalog ergänzt, der allerdings insoweit Bestimmtheitsbedenken begegnet, als er unbestimmte Tatbestandelemente genügen lässt, für deren nähere Bestimmung die Norm keine hinreichenden Anhaltspunkte bietet. So beziehe sich § 39 Abs. 2 Satz 1 Nr. 1 AWG auf § 34 Abs. 2 AWG, der über § 33 AWG auf die Außenwirtschaftsverordnung verweise, die dort normierten Ordnungswidrigkeitentatbestände aber nur genügen lasse, wenn die Maßnahme geeignet sei, die äußere Sicherheit der Bundesrepublik Deutschland, das friedliche Zusammenleben der Völker oder die auswärtigen Beziehungen der Bundesrepublik Deutschland erheblich zu gefährden (Rd.Nr. 147).

Diese letztgenannte Einschränkung der Anwendbarkeit der Ordnungswidrigkeitentatbestände nach der Außenwirtschaftsordnung ist in ihrer Unbestimmtheit vergleichbar der Regelung des § 2 Nr. 10 Buchst. b) Nds. SOG („nach dem Rechtsgut und der Strafdrohung vergleichbare Vergehen“), sodass der Straftatenkatalog, auf den die angegriffenen Vorschriften Bezug nehmen, in weiten Teilen nicht den verfassungsrechtlichen Anforderungen genügt.

## **6. Verhältnismäßigkeit**

Der mit den gefahrenabwehrrechtlichen Regelungen verfolgte gesetzgeberische Zweck ist grundsätzlich ein anderer als der der strafprozessualen Vorschriften. Es geht nicht um die staatliche Sanktionierung einer bereits erfolgten, aber nicht mehr zu verhindernden Rechtsgutsverletzung, sondern darum, das bedrohte Rechtsgut vor der drohenden Verletzung zu schützen (BVerfGE 100, 313, 394). Das Bundesverfassungsgericht hat in dieser Entscheidung aber auch dargelegt, dass auch das gesetzgeberische Anliegen, Gefahren für hochrangige Rechtsgüter abzuwehren, einen legitimen Zweck darstellt (BVerfGE 100, 313, 372).

Das BVerfG hat in diesem Zusammenhang in der Vergangenheit immer den Stellenwert des Verhältnismäßigkeitsprinzips gerade für die informationellen Befugnisse der Sicherheitsbehörden herausgestellt. Es erscheint jedoch fraglich, ob die angegriffenen Regelungen diesem Verhältnismäßigkeitsprinzip Rechnung tragen.

Danach muss die grundrechtseinschränkende Norm geeignet und erforderlich sein, den angestrebten Zweck zu erreichen (Verfassungsgerichtshof Rheinland-Pfalz, a.a.O., S. 16). Geeignet ist sie, wenn mit ihrer Hilfe der angestrebte Zweck gefördert werden kann. Dies muss für die Regelungen in § 33a Abs. 1 Nr. 2 und 3 – wie dargelegt – auch nach den Aussagen von Polizeipraktikern erheblich bezweifelt werden.

Erforderlich ist eine grundrechtseinschränkende Norm, wenn nicht ein anderes, gleich wirksames, aber das Grundrecht nicht oder weniger stark einschränkendes Mittel zur

Verfügung steht. Unter Ziffer 5 habe ich bereits ausführlich zur Erforderlichkeit mit dem Ergebnis Stellung genommen, dass die Erforderlichkeit der angegriffenen Regelungen für die Zweckerreichung nicht gegeben ist.

Des Weiteren muss eine Gesamtabwägung zwischen der Schwere des Eingriffes und dem Gewicht und der Dringlichkeit der ihn rechtfertigenden Gründe mit der Eingriffsbelastung des Betroffenen vorgenommen werden. Diese Abwägung muss zu dem Ergebnis führen, dass der Betroffene nicht übermäßig belastet wird (Verfassungsgerichtshof Rheinland-Pfalz, a.a.O., S. 16).

Dieser Grundsatz der Verhältnismäßigkeit in engeren Sinne verlangt, dass die Grundrechtsbeeinträchtigungen der Betroffenen noch in einem angemessenen und vernünftigen Verhältnis zu dem durch den Eingriff erreichbaren Schutz für bestimmte Rechtsgüter stehen (Verfassungsgerichtshof Rheinland-Pfalz, a.a.O., S. 21).

Im vorliegenden Fall steht dem Eingriff in das Grundrecht aus Art. 10 GG (und somit zugleich dem Eingriff in das Recht auf informationelle Selbstbestimmung) das gesetzgeberische Ziel gegenüber, Organisierte Kriminalität und internationalen Terrorismus erfolgreicher zu bekämpfen sowie Gemengelagen zwischen Gefahrenabwehr und Strafverfolgung zu beseitigen.

Wie oben unter Ziffer 5 ausführlich dargelegt, bieten die Vorschriften des § 33a Abs. 1 Nrn. 2 und 3 Nds. SOG keine über die Möglichkeiten der §§ 100a ff. StPO hinausgehenden Ansatzpunkte für eine Bekämpfung der Organisierten Kriminalität und des internationalen Terrorismus. Das Ziel der Verbesserung der Bekämpfungsmöglichkeiten wird also nicht erreicht.

Gleiches gilt wie ebenfalls unter Ziffer 5 dargelegt für die Beseitigung der Gemengelagen zwischen Gefahrenabwehr und Strafverfolgung.

Der Nichterreichbarkeit der gesetzgeberischen Ziele steht somit ein tiefgreifender Eingriff in grundrechtlich geschützte Positionen der von einer präventiven Telekommunikationsüberwachung Betroffenen gegenüber.

Der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit im engeren Sinne ist somit verletzt.

Dies wird besonders deutlich, wenn der von einer präventiven Telekommunikationsüberwachung Betroffene als Kontakt- oder Begleitperson gemäß § 33a Abs. 1 Nr. 3 Nds. SOG lediglich in mittelbarer Nähe zu den Tatsachen steht, die bei anderen Personen „die Annahme rechtfertigen, dass sie Straftaten von erheblicher Bedeutung begehen werden“ (§ 33a Abs. 1 Nr. 2 Nds. SOG).

Die verfassungsrechtlich gebotene Verhältnismäßigkeit im engeren Sinne ist erst recht nicht mehr gegeben, wenn diese erforderliche Abwägung mit den grundrechtlich geschützten Positionen aus Art. 10 GG (und dem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) der von einer Zielwahlsuche Betroffenen erfolgt. Diese stehen – von den wenigen „Treffern“ abgesehen – in keinerlei Bezug zu den gesetzgeberischen Zielen, wobei auch diese Personen den Schutz des Fernmeldegeheimnis in Anspruch nehmen können, denn vom Schutz des Fernmelde-

geheimnisses sind nicht nur die Kommunikationsinhalte, sondern auch die näheren Umstände der Telekommunikation erfasst. Dazu gehört insbesondere, ob, wann und wie oft zwischen welchen Personen oder Endeinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist (BVerfGE 67, 157, 172; 85, 386, 396). Das Grundrecht aus Art. 10 GG will die Bedingungen einer freien Telekommunikation aufrechterhalten. Die Nutzung des Kommunikationsmediums soll in allem vertraulich möglich sein (BVerfGE 100, 313, 358).

Hierzu führt das Bundesverfassungsgericht in den Rd.Nrn. 95 bis 98 seines Urteils vom 12.3.2003 (1 BvR 330/96 und 1 BvR 348/99) aus, dass sich hinsichtlich der Eignung und Erforderlichkeit der Erfassung von Verbindungsdaten eingehender Gespräche keine Besonderheiten gegenüber der Erfassung der sonstigen Verbindungsdaten ergeben. Bei der Prüfung der Verhältnismäßigkeit im engeren Sinne sei aber ergänzend zu berücksichtigen, dass eine besonders große Zahl von Personen betroffen wird.

Art. 10 GG schütze den Einzelnen vor staatlichen Eingriffen in das Fernmeldegeheimnis und gewährleiste in seinem objektivrechtlichen Gehalt die Vertraulichkeit der Telekommunikation auch in ihrer gesamtgesellschaftlichen Bedeutung.

Der Grundsatz der Verhältnismäßigkeit verlangt danach, dass die Einbußen an grundrechtlich geschützter Freiheit nicht in unangemessenem Verhältnis zu den Gemeinwohlzwecken stehen, denen die Grundrechtseinschränkung dient.

Gerade wegen der Vielzahl und der Unübersehbarkeit der Betroffenen sowohl bei den Kontakt- und Begleitpersonen als auch bei den Betroffenen der Zielwahlsuche wird § 33a Nds. SOG weder hinsichtlich der Nr. 2 noch insbesondere hinsichtlich der Nr. 3 diesen verfassungsrechtlichen Ansprüchen gerecht.

## **7. Konsequenzen aus den Entscheidungen des Bundesverfassungsgerichts vom 3.3.2004 (1 BvR 2378/98 - 1 BvR 1084/99 sowie 1 BvF 3/92)**

Das Bundesverfassungsgericht hat insbesondere in den Verfahren 1 BvR 2378/98 und 1 BvR 1084/99 weiterhin eine Reihe von Verfahrensvorschriften eingefordert, die gemäß Rd.Nr. 179 des Beschlusses 1 BvF 3/92 auch für die präventive Telekommunikationsüberwachung gelten. Deshalb werden nachstehend die Anforderungen einheitlich dargestellt.

Die folgenden Verfahrensvorschriften sind im Nds. SOG nicht enthalten, woraus sich auch insoweit die Verfassungswidrigkeit des § 33a Nds. SOG ergibt.

- Absoluter Schutz des Kernbereichs privater Lebensgestaltung (1 BvR 2378/98, 1 BvR 1084/99, Rd.Nrn. 120/121 und 134-173): Hierzu gibt es im Nds. SOG keine Regelungen.
- Schutz von Gesprächen zwischen dem Überwachten und Personen nach § 53 StPO (1 BvR 2378/98, 1 BvR 1084/99, Rd.Nr. 174): Die Regelung des § 30 Abs. 6 Nds. SOG besagt lediglich, dass sich die Maßnahme nicht gegen den Zeugnisverweigerungsberechtigten richten darf. Wird nicht der Anschluss des

Zeugnisverweigerungsberechtigten, sondern der seines Gesprächspartners überwacht, läuft diese Bestimmung leer.

- Schutz von Gesprächen im engsten Familien- oder Vertrautenkreis (1 BvR 2378/98, 1 BvR 1084/99, Rd.Nr. 175): § 30 Abs. 6 Nds. SOG führt Zeugnisverweigerungsberechtigte nach § 52 StPO nicht auf. Der „Vertrautenkreis“ wird überhaupt nicht erfasst.
- Verwertungsverbot, Abbruch der Überwachung bei Eingriffen in den Kernbereich privater Lebensgestaltung (1 BvR 2378/98, 1 BvR 1084/99, Rd.Nrn. 177 - 180): Hierzu gibt es im Nds. SOG keine Regelungen.
- Zweckänderung (1 BvF 3/92, Rd.Nrn. 153-169): Hier besagt § 39 Abs. 1 Satz 1, Ziff. 1 Nds. SOG, dass die Daten aus der präventiven Telekommunikationsüberwachung nur für einen anderen Zweck genutzt werden dürfen, wenn sie auch für diesen Zweck mit diesem Mittel hätten erhoben werden dürfen. Allerdings ist eine Zweckänderung gemäß Ziff. 2 auch dann zulässig, wenn „die Daten zur Behebung einer Beweisnot unerlässlich sind,“ ohne dass klar ist, welche Anforderungen an den der Beweisnot zugrunde liegenden Sachverhalt zu stellen sind.
- Richtervorbehalt (1 BvR 2378/98, 1 BvR 1084/99, Rd.Nr. 128, 269): Gemäß § 33a Abs. 3 Nds. SOG bedarf die Datenerhebung durch Überwachung der Telekommunikation der Anordnung des zuständigen Amtsgerichts. Allerdings darf die Polizei bei Gefahr im Verzug die Anordnung selbst treffen. Grundsätzlich trifft die Behördenleitung in diesen Fällen die Anordnung, sie kann die Befugnis jedoch auf Dienststellenleiter oder Bedienstete des höheren Dienstes übertragen (§ 33a Abs. 4 Nds. SOG). Wenn man die Zuständigkeit des Amtsgerichts auch in Anbetracht der verfassungsgerichtlichen Entscheidungen noch als ausreichend ansehen kann, so gilt dies jedoch nicht für die polizeiliche Anordnungsbefugnis. Hierin ist keine ausreichende verfahrensrechtliche Absicherung der Überwachungsmaßnahmen zu sehen. Zudem ist nicht ersichtlich, – und auch in den Gesetzesberatungen nicht deutlich geworden – in welchen Fällen dieser weit in das Vorfeld von Straftaten oder konkreten Gefahren liegenden Maßnahme „Gefahr im Verzug“ überhaupt vorstellbar ist. Eine polizeiliche Anordnungsbefugnis bei Gefahr im Verzug ist daher allenfalls in den Fällen des § 33a Abs. 1 Nr. 1 denkbar und akzeptabel.
- Benachrichtigungspflicht (1 BvR 2378/98, 1 BvR 1084/99, Rd.Nr. 289): Nach § 30 Abs. 4 Nds. SOG ist der von einer Maßnahme gemäß § 33a Nds. SOG Betroffene grundsätzlich zu unterrichten. Dies gilt allerdings gemäß Abs. 5 dann nicht, wenn u.a. „die weitere Verwendung einer Vertrauensperson (§ 36 Abs. 1) oder der weitere Einsatz einer Verdeckten Ermittlerin oder eines Verdeckten Ermittlers (§ 36a) gefährdet werden“. Genau dies hat das Bundesverfassungsgericht als mit dem Grundgesetz unvereinbar angesehen.

## **8. Fazit**

Die Verfassungsbeschwerde ist sowohl hinsichtlich § 33a Abs. 1 Nr. 2 als insbesondere auch hinsichtlich § 33a Abs. 1 Nr. 3 Nds. SOG begründet.

## **9. Antrag auf Erlass einer einstweiligen Anordnung**

Der Antragsteller ist schon durch die Regelung in § 33a Abs. 1 Nrn. 2 und Nr. 3 Nds. SOG in seinem Grundrecht aus Art. 10 und seinem Recht auf informationelle Selbstbestimmung selbst und unmittelbar deshalb verletzt, weil die auf Grund der Regelungen getroffenen Vollzugsmaßnahmen ohne seine Kenntnis erfolgen. Angesichts der unbestimmten und sehr weiten Fassung der Tatbestandsvoraussetzungen in Nr. 2 (vgl. dazu oben unter Ziffer 4) und der umfassenden Einbeziehung von Kontakt- und Begleitpersonen in § 33a Abs. 1 Nr. 3 Nds. SOG einerseits sowie andererseits im Hinblick darauf, dass auch diejenigen, gegen die sich die Maßnahmen zwar nicht selbst richten, die aber Kommunikationspartner der Zielpersonen sind, von der Überwachung betroffen sind (vgl. dazu oben unter Ziffer 2), ist die Gefahr naheliegend und gegenwärtig, dass der Antragsteller ebenso wie zahllose andere Bürgerinnen und Bürger bis zur Entscheidung über die Verfassungsbeschwerde in Maßnahmen nach § 33a Abs. 1 Nrn. 2 oder 3 einbezogen und dadurch in ihren Rechten verletzt werden. Dass diese Gefahr beim Antragsteller auf Grund seines Freizeitverhaltens besonders greifbar ist, hat er in seinem Schreiben vom 14. März 2004 an das Gericht geschildert. Der Umstand, dass die niedersächsische Polizei bislang von den gesetzlichen Möglichkeiten keinen Gebrauch gemacht hat (vgl. dazu oben unter Ziffer 5), kann an dieser Beurteilung nichts ändern, weil dieses Verhalten und die polizeiliche Praxis jederzeit und ohne weiteres verändert werden kann.

Da bis zum Inkrafttreten des Änderungsgesetzes vom 11. Dezember 2003 die niedersächsische Polizei ohne das Mittel der präventiven Telekommunikationsüberwachung durchaus erfolgreich hat arbeiten können und mit Ausnahme von Thüringen alle anderen Bundesländer auf den Einsatz dieses Mittels gänzlich verzichten, ist ein Aussetzen des Vollzugs der angegriffenen Gesetzesbestimmungen aus meiner Sicht auch ohne Beeinträchtigung der Aufgabenwahrnehmung der Polizei möglich. Dass die Niedersächsische Landesregierung von sich aus die Anwendung der angegriffenen Gesetzesbestimmungen aussetzen wird, steht nicht zu erwarten, da sie auch im Hinblick auf die Entscheidungen des Bundesverfassungsgerichts zum Großen Lauschangriff bereits öffentlich erklärt hat, dass sie keinerlei Änderungsbedarf erkennen könne (Niedersächsischer Landtag, Stenografischer Bericht, 15. Wahlperiode, 31. Sitzung, 28. April 2004, Seite 3315).

Ich befürworte daher den Erlass einer einstweiligen Anordnung.

Burckhard Nedden