

HRRS-Nummer: HRRS 2005 Nr. 718

Bearbeiter: Stephan Schlegel

Zitiervorschlag: BVerfG HRRS 2005 Nr. 718, Rn. X

BVerfG 1 BvR 668/04 (Erster Senat) - Urteil vom 27. Juli 2005

Präventive polizeiliche Telekommunikationsüberwachung; Zitiergebot (Anwendung in Änderungsgesetzen; Nichtigkeit; kein Verweis auf Gesetzgebungsverfahren; Gesetze vor dieser Entscheidung); konkurrierende Gesetzgebung im Strafverfahrensrecht (abschließende Regelung; Vorbeugung von Straftaten; bewusste Lücke; Vorfeld; Vorsorge für die Verfolgung von Straftaten); Anforderungen an die Bestimmtheit und Eingriffsnormen (Normenklarheit; Unsicherheit; Begriff der Straftaten von erheblicher Bedeutung); Richtervorbehalt; Unterrichtung von Überwachungsmaßnahmen; Schutzbereich des Fernmeldegeheimnisses (Spezialität; alle mittels Fernmeldetechnik ausgetauschte Informationen; Umstände; Datenverarbeitung); Verhältnismäßigkeit; Kernbereich der Lebensgestaltung (hinreichende Vorkehrungen zum Schutz; Erhebung; Löschung); Zulässigkeit der Verfassungsbeschwerde gegen Gesetze.

Art. 10 GG; Art. 1 Abs. 1 GG; Art. 19 Abs. 1 Satz 2 GG; Art. 74 Abs. 1 Nr. 1 GG; Art. 2 Abs. 1 GG; § 33a Abs. 1 Nr. 2 und 3 NdsSOG; § 100a StPO; § 100g StPO; § 100h StPO; § 484 Abs. 4 StPO

Leitsätze

1. Führt die Änderung eines Gesetzes zu neuen Grundrechtseinschränkungen, ist das betroffene Grundrecht im Änderungsgesetz auch dann gemäß Art. 19 Abs. 1 Satz 2 GG zu benennen, wenn das geänderte Gesetz bereits eine Zitervorschrift im Sinne dieser Bestimmung enthält. (BVerfG)
2. Der Bundesgesetzgeber hat abschließend von seiner Gesetzgebungsbefugnis aus Art. 74 Abs. 1 Nr. 1 GG Gebrauch gemacht, die Verfolgung von Straftaten durch Maßnahmen der Telekommunikationsüberwachung zu regeln. Die Länder sind deshalb nicht befugt, die Polizei zur Telekommunikationsüberwachung zum Zwecke der Vorsorge für die Verfolgung von Straftaten zu ermächtigen. (BVerfG)
3. Zu den Anforderungen an die Bestimmtheit und Verhältnismäßigkeit von gesetzlichen Ermächtigungen zur Verhütung und zur Vorsorge für die Verfolgung von Straftaten durch Maßnahmen der Telekommunikationsüberwachung. (BVerfG)
4. Aus Gründen der Rechtssicherheit führt die Nichtbeachtung des Zitiergebots erst bei solchen grundrechtseinschränkenden Änderungsgesetzen zur Nichtigkeit, die nach dem Zeitpunkt der Verkündung dieser Entscheidung beschlossen werden. (Bearbeiter)
5. Das allgemein aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG folgende Recht auf informationelle Selbstbestimmung tritt hinter die speziellere Gewährleistung aus Art. 10 GG zurück, soweit die Schutzbereiche sich überschneiden (vgl. BVerfGE 100, 313, 358; 110, 33, 53). Das Gleiche gilt für die Gewährleistung der freien Meinungsäußerung aus Art. 5 Abs. 1 GG, soweit der Eingriff in der staatlichen Wahrnehmung und gegebenenfalls Verarbeitung der mit Mitteln der Telekommunikation geäußerten Meinungen liegt. (Bearbeiter)
6. Der Schutz des Fernmeldegeheimnisses umfasst Kommunikationsinhalt und die Kommunikationsumstände. Dabei bezieht sich der Grundrechtsschutz auf alle mittels der Fernmeldetechnik ausgetauschten Informationen (vgl. BVerfGE 100, 313, 358; 110, 33, 52 f.). In den Schutzbereich fällt auch die Erlangung der Kenntnis, ob, wann, wie oft und zwischen welchen Personen Telekommunikation stattgefunden hat oder versucht worden ist (vgl. BVerfGE 85, 386, 396; 107, 299, 312 f.). Dies umfasst auch den sich daran anschließenden Informations- und Datenverarbeitungsprozess in dem Gebrauch von den erlangten Kenntnissen gemacht wird (vgl. BVerfGE 100, 313, 359; 110, 33, 68 f.). (Bearbeiter)
7. Die Vorsorge für die spätere Verfolgung von Straftaten ist kompetenzmäßig dem "gerichtlichen Verfahren" im Sinne des Art. 74 Abs. 1 Nr. 1 GG zuzuordnen, da sie die Sicherung von Beweisen für ein künftiges Strafverfahren bezweckt. (Bearbeiter)

8. Für Ermächtigungen zu Überwachungsmaßnahmen verlangt das Bestimmtheitsgebot zwar nicht, dass die konkrete Maßnahme vorhersehbar ist, wohl aber, dass die betroffene Person grundsätzlich erkennen kann, bei welchen Anlässen und unter welchen Voraussetzungen ein Verhalten mit dem Risiko der Überwachung verbunden ist. (Bearbeiter)

9. Sieht der Gesetzgeber in der Situation der Vorfeldermittlung, die durch eine hohe Ambivalenz der potenziellen Bedeutung einzelner Verhaltensumstände geprägt ist, Grundrechtseingriffe vor, so hat er die den Anlass bildenden Straftaten sowie die Anforderungen an Tatsachen, die auf die künftige Begehung hindeuten, so bestimmt zu umschreiben, dass das besonders hohe Risiko einer Fehlprognose gleichwohl verfassungsrechtlich noch hinnehmbar ist. Die Norm muss 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 (vgl. BVerfGE 110, 33, 56). (Bearbeiter)

10. Grundsätzlich können zwar ausfüllungsbedürftige materielle Normen rechtsstaatlich eher tragbar sein, wenn durch ein formalisiertes, gerichtlich kontrolliertes Verfahren dafür gesorgt wird, dass die wesentlichen Entscheidungsfaktoren geprüft und auslegungsbedürftige Rechtsbegriffe angemessen angewandt werden. Das aber setzt voraus, dass der Richter Anhaltspunkte im Gesetz vorfindet. (Bearbeiter)

11. Verfassungsrechtlich hinzunehmen ist das Risiko, dass bei präventiven Abhörmaßnahmen auch Kommunikation aus dem Kernbereich privater Lebensgestaltung erfasst wird, allenfalls bei einem besonders hohen Rang des gefährdeten Rechtsguts und einer durch konkrete Anhaltspunkte gekennzeichneten Lage, die auf einen unmittelbaren Bezug zur zukünftigen Begehung der Straftat schließen lässt. Hinzu müssen Vorkehrungen kommen, die sichern, dass die Kommunikationsinhalte des höchstpersönlichen Bereichs nicht gespeichert und verwertet werden dürfen, sondern unverzüglich gelöscht werden, wenn es ausnahmsweise zu ihrer Erhebung gekommen ist. (Bearbeiter)

Entscheidungstenor

§ 33a Absatz 1 Nummer 2 und 3 des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung (Nds.SOG) in der Fassung von Artikel 1 des Gesetzes zur Änderung des Niedersächsischen Gefahrenabwehrgesetzes vom 11. Dezember 2003 (Niedersächsisches Gesetz- und Verordnungsblatt Seite 414) und in der Fassung der Bekanntmachung vom 19. Januar 2005 (Niedersächsisches Gesetz- und Verordnungsblatt Seite 9) ist mit Artikel 10 des Grundgesetzes unvereinbar und nichtig.

Das Land Niedersachsen hat dem Beschwerdeführer seine notwendigen Auslagen zu erstatten.

Gründe

A

Die Verfassungsbeschwerde richtet sich unmittelbar gegen § 33a Abs. 1 Nr. 2 und 3 des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung (Nds.SOG) und damit gegen die Ermächtigung der Polizei, personenbezogene Daten durch Überwachung und Aufzeichnung der Telekommunikation zur Vorsorge für die Verfolgung oder zur Verhütung einer Straftat von erheblicher Bedeutung zu erheben. 1

I.

Im Jahre 1994 wurde die Polizei in Niedersachsen ergänzend zu ihrer bisherigen Aufgabe der Gefahrenabwehr ermächtigt, Vorbereitungen zu treffen, um künftige Gefahren abwehren zu können, sowie im Rahmen der Gefahrenabwehr auch für die Verfolgung von Straftaten vorzusorgen und Straftaten zu verhüten (§ 1 Abs. 1 Satz 2 und 3 des Niedersächsischen Gefahrenabwehrgesetzes - NGefAG - in der Fassung des Gesetzes zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung vom 18. Februar 1994 <Nds.GVBI S. 71>). Der Aufgabenzuwachs war verbunden mit einem Ausbau der polizeilichen Befugnisse, darunter auch der Schaffung des Rechts zur Aufzeichnung von Fernmeldedaten sowie zum verdeckten Einsatz technischer Mittel, und zwar auch in der Wohnung. 2

Ende 1997 wurde das Niedersächsische Gefahrenabwehrgesetz durch das Gesetz zur Änderung datenschutz-, gefahrenabwehr- und verwaltungsverfahrenrechtlicher Vorschriften vom 28. November 1997 (Nds.GVBI S. 489) erneut 3

novelliert. Seitdem ist das heimliche Abhören in Wohnungen auch zur Abwehr der Gefahr zulässig, jemand könne eine Straftat von erheblicher Bedeutung begehen (§ 35 Abs. 2 Nr. 2 des Gefahrenabwehrgesetzes). Nach den Ereignissen des 11. September 2001 wurde das Niedersächsische Gefahrenabwehrgesetz erneut geändert, und die polizeilichen Befugnisse wurden weiter ausgebaut.

Durch Art. 1 des Gesetzes zur Änderung des Niedersächsischen Gefahrenabwehrgesetzes vom 11. Dezember 2003 (Nds.GVBI S. 414) erhielt das Gesetz, das unter dem 19. Januar 2005 (Nds.GVBI S. 9) neu bekannt gemacht worden ist, wieder die frühere Bezeichnung "Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung (Nds.SOG)". Durch das Änderungsgesetz wurde die vom Beschwerdeführer hinsichtlich ihres Absatzes 1 Nummer 2 und 3 als verfassungswidrig gerügte neue Vorschrift des § 33a Nds.SOG geschaffen. 4

§ 33a Nds.SOG lautet wie folgt: 5

Datenerhebung durch Überwachung der Telekommunikation 6

(1) Die Polizei kann personenbezogene Daten durch Überwachung und Aufzeichnung der Telekommunikation erheben 7

1. zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person 8

über die in den §§ 6 und 7 genannten Personen, wenn die Aufklärung des Sachverhalts auf andere Weise nicht möglich erscheint, sowie unter den Voraussetzungen des § 8 über die dort genannten Personen, wenn dies für die Aufklärung des Sachverhalts unerlässlich ist, 9

2. über Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie Straftaten von erheblicher Bedeutung begehen werden, wenn die Vorsorge für die Verfolgung oder die Verhütung dieser Straftaten auf andere Weise nicht möglich erscheint, sowie 10

3. über Kontakt- und Begleitpersonen der in Nummer 2 genannten Personen, wenn dies zur Vorsorge für die Verfolgung oder zur Verhütung einer Straftat nach Nummer 2 unerlässlich ist. 11

(2) Eine Datenerhebung nach Absatz 1 kann sich auf 12

1. die Inhalte der Telekommunikation einschließlich der innerhalb des Telekommunikationsnetzes in Datenspeichern abgelegten Inhalte, 13

2. die Telekommunikationsverbindungsdaten (§ 33 Abs. 1) oder 14

3. die Standortkennung einer aktiv geschalteten Mobilfunkendeinrichtung 15

beziehen. Die Datenerhebung darf nur an Telekommunikationsanschlüssen der in Absatz 1 genannten Personen erfolgen. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. 16

(3) Die Datenerhebung nach Absatz 1 bedarf der Anordnung durch das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die in Absatz 1 bezeichneten Voraussetzungen vorliegen. In der Anordnung sind neben der Person, gegen die sich die Datenerhebung richtet, Art und Umfang der zu erhebenden Daten sowie die betroffenen Telekommunikationsanschlüsse zu bezeichnen. Für das Verfahren gilt § 19 Abs. 4 entsprechend. 17

(4) Bei Gefahr im Verzuge kann die Polizei die Anordnung treffen. Die Zulässigkeit der polizeilichen Anordnung ist schriftlich zu begründen. Die Entscheidung trifft die Behördenleitung. Diese kann ihre Anordnungsbefugnis auf Dienststellenleiterinnen oder Dienststellenleiter sowie Bedienstete des höheren Dienstes übertragen. Die richterliche Bestätigung der Anordnung ist unverzüglich zu beantragen. 18

(5) Aufgrund der Anordnung hat jeder, der geschäftsmäßig Telekommunikationsdienstleistungen erbringt oder daran mitwirkt, der Polizei die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen. 19

Für die Telekommunikationsüberwachung haben insbesondere die folgenden weiteren Normen Bedeutung: 20

§ 30	21
Grundsätze der Datenerhebung	22
(1) bis (3) ...	23
(4) Über die Erhebung personenbezogener Daten mit besonderen Mitteln oder Methoden ist die betroffene Person zu unterrichten. Die betroffene Person ist mit der Unterrichtung auf die Rechtsgrundlage der Datenverarbeitung und das Auskunftsrecht nach § 16 des Niedersächsischen Datenschutzgesetzes hinzuweisen. Die Unterrichtung erfolgt, sobald dies möglich ist, ohne die Maßnahme zu gefährden.	24
(5) Die Unterrichtung nach Absatz 4 unterbleibt,	25
1. solange Zwecke der Verfolgung einer Straftat oder Ordnungswidrigkeit entgegenstehen,	26
2. wenn zur Durchführung der Unterrichtung in unverhältnismäßiger Weise weitere Daten über die betroffene Person erhoben werden müssten oder	27
3. solange durch das Bekanntwerden der Datenerhebung Leib, Leben, Freiheit oder ähnlich schutzwürdige Belange einer Person oder die weitere Verwendung einer Vertrauensperson (§ 36 Abs. 1) oder der weitere Einsatz einer Verdeckten Ermittlerin oder eines Verdeckten Ermittlers (§ 36a) gefährdet werden.	28
Ist nach Satz 1 Nr. 3 eine Unterrichtung auch nach Ablauf von fünf Jahren nicht erfolgt, so ist dies der Landesbeauftragten oder dem Landesbeauftragten für den Datenschutz mitzuteilen.	29
(6) Die Datenerhebung nach den §§ 33a bis 36a darf sich nicht gegen Personen richten, die in Strafverfahren aus beruflichen Gründen zur Verweigerung des Zeugnisses berechtigt sind (§§ 53 und 53a der Strafprozessordnung, § 12 Abs. 3 und § 23 Abs. 4 des Bundesdatenschutzgesetzes), soweit Sachverhalte betroffen sind, auf die sich ihr Zeugnisverweigerungsrecht bezieht, es sei denn, die Datenerhebung ist zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich. Die Polizei darf solche Personen nicht von sich aus als Vertrauenspersonen (§ 36 Abs. 1 Satz 1) in Anspruch nehmen.	30
§ 31	31
Datenerhebung	32
(1) Die Polizei kann über jede Person Daten erheben, soweit dies zur Abwehr einer Gefahr oder zur Wahrnehmung einer Aufgabe nach § 1 Abs. 4 oder 5 erforderlich ist. Satz 1 gilt entsprechend, wenn Verwaltungsbehörden zur Abwehr einer Gefahr tätig werden.	33
(2) und (3)...	34
§ 38	35
Speicherung, Veränderung und Nutzung personenbezogener Daten, Zweckbindung	36
(1) Die Verwaltungsbehörden und die Polizei können die von ihnen im Rahmen der Aufgabenerfüllung nach diesem Gesetz rechtmäßig erhobenen personenbezogenen Daten speichern, verändern und nutzen, wenn dies zu dem Zweck erforderlich ist, zu dem sie erhoben worden sind. Erlangen die in Satz 1 genannten Stellen rechtmäßig Kenntnis von personenbezogenen Daten, ohne sie erhoben zu haben, so dürfen sie diese Daten zu einem der Gefahrenabwehr dienenden Zweck speichern, verändern oder nutzen. Die Zweckbestimmung ist bei der Speicherung festzulegen. Können die zur Zweckerreichung nicht erforderlichen Daten nicht oder nur mit unverhältnismäßigem Aufwand gelöscht werden, so dürfen diese Daten gemeinsam mit den Daten nach den Sätzen 1 und 2 gespeichert, aber nur nach Maßgabe des § 39 Abs. 5 verändert und genutzt werden.	37
(2) Die mit besonderen Mitteln oder Methoden erhobenen personenbezogenen Daten sind zu kennzeichnen.	38
(3) und (4)...	39

§ 39	40
Speicherung, Veränderung und Nutzung personenbezogener Daten zu anderen Zwecken	41
(1) Die Speicherung, Veränderung oder Nutzung von personenbezogenen Daten zu anderen als den in § 38 Abs. 1 genannten Zwecken ist nur zulässig, wenn	42
1. die Daten zur Erfüllung eines anderen Zwecks der Gefahrenabwehr erforderlich sind und sie auch zu diesem Zweck mit dem Mittel oder der Methode hätten erhoben werden dürfen, mit denen sie erhoben worden sind,	43
2. bis 4. ...	44
(2) bis (4)...	45
(5) Die Speicherung, Veränderung oder Nutzung personenbezogener Daten über unvermeidbar betroffene Dritte und über Personen, die mit einer ausgeschriebenen Person angetroffen worden sind (§ 37 Abs. 2), ist nur zulässig, wenn dies zur Vorsorge für die Verfolgung oder zur Verhütung von Straftaten von erheblicher Bedeutung erforderlich ist. Satz 1 ist auch auf die Veränderung und Nutzung von Daten anzuwenden, die nach § 38 Abs. 1 Satz 4 gespeichert worden sind.	46
(6)...	47
Einzelne Tatbestandsmerkmale des § 33a Abs. 1 Nr. 2 und 3 Nds.SOG definiert § 2 Nds.SOG wie folgt:	48
10. Straftat von erheblicher Bedeutung:	49
a) ein Verbrechen, mit Ausnahme einer Straftat nach den §§ 154 und 155 des Strafgesetzbuchs,	50
b) ein Vergehen nach den §§ 85, 86, 86a, 87 bis 89, 98, 99, 129, 130, 174, 174a, 174b und 176 des Strafgesetzbuchs, ein in § 138 Abs. 1 des Strafgesetzbuchs genanntes Vergehen und ein nach dem geschützten Rechtsgut und der Strafandrohung vergleichbares Vergehen,	51
c) ein banden- oder gewerbsmäßig begangenes Vergehen,	52
d) die Teilnahme an einer solchen Straftat;	53
11. Kontakt- oder Begleitperson:	54
eine Person, die mit einer anderen Person, von der Tatsachen die Annahme rechtfertigen, dass diese eine Straftat von erheblicher Bedeutung begehen wird, in einer Weise in Verbindung steht, die erwarten lässt, dass durch sie Hinweise über die angenommene Straftat gewonnen werden können.	55
II.	
Der Beschwerdeführer rügt die Verletzung seiner Grundrechte aus Art. 10 Abs. 1, Art. 5 Abs. 1 und Art. 2 Abs. 1 GG.	56
1. Zur Zulässigkeit der Verfassungsbeschwerde legt er dar, er wende sich zwar unmittelbar gegen eine gesetzliche Vorschrift, die noch eines Vollzugsakts bedürfe. Vorliegend bestehe aber die Besonderheit, dass die angegriffene Norm eine Verletzung seines Fernmeldegeheimnisses und anderer Grundrechte erlaube, die ihm unbekannt bleibe. Er habe keine Gelegenheit, vor, während oder nach Durchführung des Grundrechtseingriffs eine gerichtliche Kontrolle herbeizuführen. Auch werde er mit einiger Wahrscheinlichkeit durch Maßnahmen, die auf der angegriffenen Rechtsnorm beruhen, in seinen Grundrechten berührt. Die Voraussetzungen des § 33a Abs. 1 Nr. 2 Nds.SOG seien so weit gefasst und unbestimmt, dass er jederzeit damit rechnen müsse, zum dort genannten Personenkreis gezählt und überwacht zu werden. Gegenwärtig betroffen sei er auch durch § 33a Abs. 1 Nr. 3 Nds.SOG, der eine vorbeugende heimliche Überwachung der Telekommunikation von Kontaktpersonen zulasse. Er besitze einen großen Freundes- und Bekanntenkreis, in dem auch vertrauliche Telefongespräche geführt würden. Er könne nicht ausschließen, dass sich unter seinen Bekannten Personen im Sinne von § 33a Abs. 1 Nr. 2 Nds.SOG befänden und er von der Polizei zu deren Kontaktpersonen gezählt werde.	57

2. Der Beschwerdeführer sieht durch die angegriffenen Regelungen das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG verletzt. § 33a Abs. 1 Nr. 2 Nds.SOG führe dazu, dass seine Telefongespräche heimlich abgehört und aufgezeichnet werden könnten, ohne dass gegen ihn der Verdacht einer Straftat bestehe oder von ihm eine Gefahr im polizeirechtlichen Sinne ausgehe. Die einschränkenden Voraussetzungen für eine Überwachung nach § 33a Abs. 1 Nr. 2 Nds.SOG genügten dem Grundrechtsschutz nicht. Der Begriff der Tatsachen, welche die Annahme künftiger Begehung schwerer Straftaten rechtfertigten, sei so allgemein gehalten und unbestimmt, dass er die Anwendung der Norm nicht wirksam einzugrenzen vermöge. Auch die Einschränkung, nach der "die Vorsorge für die Verfolgung oder die Verhütung dieser Straftaten auf andere Weise nicht möglich" erscheinen dürfe, lasse der Polizei einen äußerst weiten Beurteilungsbereich. Schon wegen des Risikos, dass andere Maßnahmen von den Betroffenen bemerkt werden könnten, werde der Polizei die heimliche Telefonüberwachung regelmäßig als einzig mögliches Mittel der Vorbeugung erscheinen. Schließlich rechtfertige auch die Begrenzung der befürchteten künftigen Straftaten auf solche "von erheblicher Bedeutung" nicht den Grundrechtseingriff. Welche Straftaten unter diesen Begriff fielen, sei in § 2 Nr. 10 Nds.SOG zwar bestimmt. Diese Norm enthalte aber unter Buchstabe b eine unzulässige Allgemeinklausel, nach der auch ein nach dem geschützten Rechtsgut und der Strafandrohung vergleichbares Vergehen eine Straftat von erheblicher Bedeutung darstellen könne. Im Übrigen fielen auch nicht besonders schwerwiegende Taten unter die Legaldefinition. 58

Auch § 33a Abs. 1 Nr. 3 Nds.SOG bewirke eine Verletzung seines Grundrechts aus Art. 10 Abs. 1 GG. Die Voraussetzung, dass die Überwachung einer Kontakt- oder Begleitperson "zur Vorsorge für die Verfolgung oder zur Verhütung einer Straftat nach Nummer 2 unerlässlich" sein müsse, berücksichtige die Bedeutung des Grundrechts nicht gebührend. Die Voraussetzung sei schon dann erfüllt, wenn die Polizei der Auffassung sei, andere Möglichkeiten als die Überwachung des Personenumfelds des künftigen Straftäters stünden nicht zur Verfügung. Dies könne häufig der Fall sein, weil der Eingriff bereits ohne jeden konkreten Verdacht möglich sei. 59

Darüber hinaus verletzen die angegriffenen Vorschriften sein Grundrecht auf freie Meinungsäußerung (Art. 5 Abs. 1 GG) und beeinträchtigen ihn in der freien Entfaltung seiner Persönlichkeit (Art. 2 Abs. 1 GG). Er sei durch diese Normen ständig der Gefahr ausgesetzt, dass seine Telekommunikation heimlich von der Exekutive überwacht werde. Dieses beständige Wissen verhindere eine unbefangene Meinungsäußerung auch in privaten Telefongesprächen und betreffe damit den Kern seiner Privatsphäre. 60

Ergänzend führt der Beschwerdeführer aus, das Gesetz verstoße gegen Art. 19 Abs. 4 GG, weil die Überwachung ihm nicht mitgeteilt werde und es in der Folge unmöglich sei, während oder nach der Überwachung deren gerichtliche Kontrolle herbeizuführen. Der Richtervorbehalt könne dieses rechtsstaatliche Defizit nicht ausgleichen. Schließlich verstießen die Normen gegen das Zitiergebot des Art. 19 Abs. 1 Satz 2 GG und die in Art. 74 Abs. 1 Nr. 1 GG geregelte Gesetzgebungszuständigkeit auf dem Gebiet der Strafrechtspflege. 61

III.

Zur Verfassungsbeschwerde haben Stellung genommen: das Bundesministerium des Innern namens der Bundesregierung, die Niedersächsische Staatskanzlei, der Bundesbeauftragte für den Datenschutz, der Landesbeauftragte für den Datenschutz Niedersachsen, der Hessische Datenschutzbeauftragte, der Landesbeauftragte für den Datenschutz Rheinland-Pfalz, das Unabhängige Landeszentrum für den Datenschutz Schleswig-Holstein sowie der Thüringer Landesbeauftragte für den Datenschutz. 62

1. Nach Auffassung der Bundesregierung ist die Vorsorge für die Verfolgung künftig zu begehender Straftaten der konkurrierenden Gesetzgebung zuzuordnen, von der der Bundesgesetzgeber für den Bereich der Telekommunikationsüberwachung abschließend Gebrauch gemacht habe. Dem Land Niedersachsen stehe insoweit keine Gesetzgebungsbefugnis zu. 63

a) Die Regelung sei dem Strafverfahrensrecht (Art. 74 Abs. 1 Nr. 1 GG) zuzurechnen, da sie letztlich die Sicherung von Beweisen für ein künftiges Strafverfahren bezwecke. Der Bundesgesetzgeber habe in der Vergangenheit für eine Reihe von Maßnahmen zur Verfolgungsvorsorge von der Ermächtigung des Art. 74 Abs. 1 Nr. 1 GG Gebrauch gemacht. Beispielsweise erlaube § 81b StPO die erkennungsdienstliche Behandlung eines Beschuldigten und damit die vorsorgliche Bereitstellung von sächlichen Hilfsmitteln für die Erforschung und Aufklärung künftiger Straftaten. § 81g StPO ermögliche das Erstellen und Speichern von DNA-Identifizierungsmustern für Zwecke künftiger Strafverfahren. Derzeit prüfe der Bundesgesetzgeber im Hinblick auf verschiedene Ermittlungsmaßnahmen die Möglichkeiten ihres Einsatzes im Vorfeld von Straftaten. Der Umstand, dass eine Tat noch nicht begangen sei, stehe der Zuordnung zum Strafverfahren nicht entgegen. Der zur Gesetzgebungskompetenz des Landes gehörenden Gefahrenabwehr könnten allenfalls solche Maßnahmen zugeordnet werden, die primär auf die Verhinderung der Straftat gerichtet seien und bei denen die Vorsorge für die Verfolgung nur als ein bei dieser Gelegenheit anfallendes Nebenprodukt erscheine. 64

b) Die Regelungen der Strafprozessordnung über die Verfolgung von Straftaten mittels Überwachung von Telekommunikationsanlagen seien abschließend. Der Bundesgesetzgeber habe die Überwachung der Telekommunikation zu Zwecken der Strafverfolgung in den §§ 100a, 100b, 100h und 100i StPO nach Umfang, Zuständigkeit und Zweck, vor allem jedoch hinsichtlich der Voraussetzungen umfassend geregelt. Wegen der besonderen Bedeutung des Fernmeldegeheimnisses seien die Überwachung und Aufzeichnung der Telekommunikation von besonderen, hohen Voraussetzungen abhängig gemacht worden. So seien zur Begrenzung der Streubreite entsprechender Maßnahmen sowohl die Echtzeitüberwachung von Telekommunikation (§§ 100a, 100b StPO) als auch die Abfrage von Verbindungsdaten (§§ 100g, 100h StPO) vom Vorliegen eines erhöhten Grads des Anfangsverdachts abhängig. Ferner seien die genannten Maßnahmen nur zur Aufklärung von im Gesetz ausdrücklich bestimmten besonders schweren Straftaten beziehungsweise von Straftaten von erheblicher Bedeutung oder solchen zulässig, die mittels Telekommunikation begangen werden und bei denen daher die Maßnahme zur Aufklärung besonders geeignet erscheine. Dem kriminalistischen Erfordernis eines unter Umständen frühzeitigen Einsatzes der Telekommunikationsüberwachung sei dadurch Rechnung getragen worden, dass die Maßnahmen unter bestimmten Voraussetzungen bereits im Vorbereitungsstadium der genannten Straftaten zulässig seien (unter Hinweis auf § 100a Satz 1, § 100g Abs. 1 Satz 1 StPO). 65

2. Die Niedersächsische Staatskanzlei hält die Verfassungsbeschwerde für unbegründet. 66

a) Das Land habe im Rahmen seiner Gesetzgebungskompetenz gehandelt. Die präventive Telekommunikationsüberwachung falle weder unter die ausschließliche Gesetzgebungszuständigkeit des Bundes nach Art. 73 Nr. 7 GG noch betreffe sie die konkurrierende Gesetzgebung für das gerichtliche Verfahren nach Art. 74 Abs. 1 Nr. 1 GG. Die Verhütung von Straftaten und die Vorsorge für die Verfolgung von Straftaten seien nicht dem Strafverfahren zuzuordnen. Die Verhütung von Straftaten sei Bestandteil der Gefahrenabwehr oder, soweit die Tatbegehung noch nicht hinreichend wahrscheinlich sei, des Vorfelds der Gefahrenabwehr. 67

Soweit die Telekommunikationsüberwachung nach § 33a Nds.SOG der Vorsorge für die Verfolgung von Straftaten diene, sei sie ebenfalls nicht Teil des Strafverfahrens. Die Zuordnung zur Bundeskompetenz setze voraus, dass der Zusammenhang zwischen den geregelten Maßnahmen der Verfolgungsvorsorge und einem künftigen Strafverfahren hinreichend eng und konkret sei. Bei den hier in Rede stehenden Regelungen sei der Zusammenhang jedoch lose. Es würden zwar auch Daten über eine bestimmte Person und im Hinblick auf die mögliche Begehung einer bestimmten Straftat erhoben, die Datenerhebung geschehe aber nicht im Rahmen oder aus Anlass eines laufenden oder abgeschlossenen Strafverfahrens. Durch die Telekommunikationsüberwachung könnten Daten unterschiedlichster Art gewonnen werden, die möglicherweise auch nicht direkt als Beweis in einem Strafverfahren dienen sollten, sondern erst zu weiteren Beweismitteln führen müssten. 68

Maßnahmen mit dem Ziel der Straftatenverhütung ließen sich häufig nicht von Maßnahmen mit dem Ziel der Verfolgungsvorsorge trennen. Eine einheitliche Regelung beider Aspekte sei unerlässlich und gehöre wegen des hauptsächlichen Ziels der Verhinderung von Straftaten zur Gesetzgebungskompetenz des Landes. Es bestehe eine deutliche Nähe der Verfolgungsvorsorge durch Telekommunikationsüberwachung nach § 33a Nds.SOG zur Straftatenverhütung, die Gegenstand der Gesetzgebungskompetenz des Landes sei. Prägend sei die gleichermaßen bestehende Eingriffsvoraussetzung der auf Tatsachen gestützten Annahme, dass jemand eine Straftat begehen werde. Damit werde die primäre Aufgabe der Polizei angesprochen, die Begehung einer Straftat im Vorfeld zu verhindern und dafür zu sorgen, dass ein Schaden erst gar nicht eintrete. Fraglich sei, ob es in dieser Situation überhaupt Maßnahmen geben werde, die ausschließlich dem Ziel der Verfolgungsvorsorge dienten. 69

b) Die angegriffenen Regelungen seien auch materiell rechtmäßig. Sie ermöglichten zwar umfassende und schwerwiegende Eingriffe in das Grundrecht aus Art. 10 Abs. 1 GG, die jedoch von dem Gesetzesvorbehalt des Art. 10 Abs. 2 Satz 1 GG gedeckt seien. Die Normen seien insbesondere hinreichend bestimmt, entsprächen in ihrer Ausgestaltung dem Grundsatz der Verhältnismäßigkeit und enthielten Verfahrensvorkehrungen, die der Schwere und Heimlichkeit des Eingriffs in das Grundrecht aus Art. 10 Abs. 1 GG Rechnung trügen. Die Regelung ausfüllungsbedürftiger Tatbestandsmerkmale genüge den Bestimmtheitsanforderungen, weil sich der Bedeutungsgehalt des § 33a Abs. 1 Nr. 2 und 3 Nds.SOG mit juristischen Methoden ermitteln und auf den Einzelfall anwenden lasse. Die Verhältnismäßigkeit der Überwachung der Telekommunikation zur vorbeugenden Bekämpfung von Straftaten ergebe sich aus dem mit der Bekämpfung von Straftaten verfolgten legitimen und hochrangigen Zweck. Die Maßnahmen seien so ausgestaltet, dass sie das Bedürfnis nach Schutz und Sicherheit einerseits und nach Freiheit andererseits in einen angemessenen Ausgleich brächten. 70

Die Regelungen für die Telekommunikationsüberwachung würden ferner den verfahrensrechtlichen Anforderungen aus Art. 10 in Verbindung mit Art. 19 Abs. 4 GG gerecht. Sie sähen für die Verarbeitung der durch Maßnahmen der 71

Telekommunikationsüberwachung gewonnenen Daten Begrenzungen vor, die verfassungsrechtlichen Anforderungen genügen. So sei in § 33a Abs. 3 Nds.SOG für alle Maßnahmen der Telekommunikationsüberwachung ein Richtervorbehalt vorgesehen. Darüber hinaus sei der Betroffene nach § 30 Abs. 4 Nds.SOG über die Datenerhebung zu unterrichten, sobald dies ohne Gefährdung der Maßnahme möglich sei. Außerdem unterliege die Telekommunikationsüberwachung der parlamentarischen Kontrolle nach § 37a Nds.SOG.

3. Der Bundesbeauftragte für den Datenschutz und die Datenschutzbeauftragten der Länder, die sich im Verfahren geäußert haben, halten die Verfassungsbeschwerde für begründet. Sie führen hierfür im Wesentlichen folgende Gründe an: 72

§ 33a Abs. 1 Nr. 2 und 3 Nds.SOG ermögliche Regelungen zur Initiativmittlung, für die dem Land die Gesetzgebungskompetenz fehle. Die gemäß Art. 74 Abs. 1 Nr. 1 GG für den Bund bestehende Regelungsbefugnis sei - weil es bei der angegriffenen Regelung im Kern um die Bekämpfung von Straftaten gehe - mit der Strafprozessordnung sowie anderen einschlägigen Gesetzen in abschließender Weise ausgeschöpft worden. Zudem stehe dem Bundesgesetzgeber nach Art. 73 Nr. 7 GG die alleinige Befugnis zu, Einschränkungen der Telekommunikation gesetzlich zu regeln. 73

Verfassungsrechtliche Bedenken bestünden ferner unter den Aspekten der Bestimmtheit und der Klarheit der tatbestandlichen Voraussetzungen des § 33a Abs. 1 Nr. 2 Nds.SOG. Ansatzpunkt der Telekommunikationsüberwachung sei zwar die auf Tatsachen beruhende Einschätzung, dass künftig Straftaten begangen würden. Diese Einschätzung bleibe aber bloße Prognose. Nicht gefordert werde eine Plausibilität dieser Prognose etwa durch die Anforderung, dass bereits Straftaten von dem betroffenen Personenkreis begangen worden seien oder ein dahingehender Verdacht bestehe. Die Prognose beziehe sich stattdessen auf ein in der Zukunft liegendes ungewisses Ereignis. Welcher Wahrscheinlichkeitsgrad gefordert werde, bleibe völlig offen. Gleichfalls würden keine einschränkende Anforderungen an die Qualität der zu Grunde zu legenden Tatsachen gestellt. Die vom Gesetz geforderten Tatsachen müssten unter Berücksichtigung kriminalistischer Erfahrung bewertet und oft mit Zusatzinformationen verknüpft werden, damit die Annahme möglich erscheine, eine Person werde künftig Straftaten von erheblicher Bedeutung begehen. Es handele sich letztlich nur um Anhaltspunkte für die Notwendigkeit einer Verdachtsgewinnung oder Verdachtskonkretisierung. 74

Für den Betroffenen sei die Maßnahme nicht vorhersehbar. Er könne insbesondere nicht erkennen, ob die Behörde sein Verhalten als verdächtig oder neutral einstufe. Die weitere Voraussetzung, dass die Vorsorge für die Verfolgung oder die Verhütung bestimmter Straftaten auf andere Weise nicht möglich erscheine, enthalte keine wirksame zusätzliche Schranke. Der Begriff der Vorsorge für die Verfolgung sei so weit und umfassend, dass er alle Datenerhebungen in Bezug auf die ins Auge gefassten, in irgendeiner Weise verdächtigen Personen umfasse. In noch stärkerem Maße würden die Bestimmtheitsbedenken für den in § 33a Abs. 1 Nr. 3 Nds.SOG genannten Personenkreis der Kontakt- oder Begleitpersonen gelten. 75

Die angegriffenen Regelungen seien unverhältnismäßig. Die Erforderlichkeit der präventiven Telekommunikationsüberwachung sei - abgesehen von der nicht angegriffenen Ermächtigung zur Gefahrenabwehr in § 33a Abs. 1 Nr. 1 Nds.SOG - nicht nachgewiesen. Auch sei abzusehen, dass die gesetzgeberischen Ziele, vor allem das der Bekämpfung der Organisierten Kriminalität und des Terrorismus, nicht erreicht würden. Im Übrigen fehlten Normen zum Schutz des unantastbaren Kernbereichs der Persönlichkeit, insbesondere Überwachungsverbote in Bezug auf Gespräche zwischen engsten Familienangehörigen und sonstigen engen Vertrauten. Der Gesetzgeber habe ferner seine Pflicht verletzt, Verwertungsverbote und Löschungsgebote hinsichtlich solcher Daten zu normieren, die unter Beeinträchtigung dieses geschützten Kernbereichs erhoben worden seien. Verfassungsrechtliche Bedenken bestünden auch hinsichtlich der in § 33a Abs. 3 Satz 2 und 3 Nds.SOG normierten maximalen Zeitspannen der Geltungsdauer der Überwachungsmaßnahmen. Schließlich sei die Regelung des § 30 Abs. 4 Nds.SOG mit dem Gebot effektiven Rechtsschutzes gemäß Art. 19 Abs. 4 GG nicht vereinbar. 76

IV.

In der mündlichen Verhandlung haben sich geäußert: der Beschwerdeführer, die Bundesregierung, die Niedersächsische Landesregierung, der Bundesbeauftragte für den Datenschutz, der Landesbeauftragte für den Datenschutz Niedersachsen, die Bundesrechtsanwaltskammer sowie der Leitende Kriminaldirektor Bruckert als sachverständige Auskunftsperson. 77

B.

Die Verfassungsbeschwerde ist zulässig. Der Beschwerdeführer ist durch die angegriffenen Vorschriften unmittelbar (I.) sowie selbst und gegenwärtig (II.) in seinen Grundrechten betroffen (vgl. BVerfGE 100, 313 <354>; 109, 279 <305 ff.>). 78

I.

Eine Verfassungsbeschwerde kann sich ausnahmsweise unmittelbar gegen ein vollziehungsbedürftiges Gesetz richten, wenn der Beschwerdeführer den Rechtsweg nicht beschreiten kann, weil er keine Kenntnis von der Maßnahme erlangt (vgl. BVerfGE 30, 1 <16 f.>; 67, 157 <169 f.>; 100, 313 <354>; 109, 279 <306 f.>). Gleiches gilt, soweit eine nachträgliche Bekanntgabe zwar vorgesehen ist, von ihr aber aufgrund weitreichender Ausnahmetatbestände auch langfristig abgesehen werden kann. Unter diesen Umständen ist effektiver fachgerichtlicher Rechtsschutz ebenfalls nicht gewährleistet (vgl. BVerfGE 109, 279 <307>; Landesverfassungsgericht Mecklenburg-Vorpommern, LKV 2000, S. 345 <346>). 79

Die Datenerhebung durch Überwachung der Telekommunikation gemäß § 33a Nds.SOG erfolgt heimlich. Der Betroffene erfährt weder vor noch während der Durchführung von der Maßnahme, so dass zu diesem Zeitpunkt kein fachgerichtlicher Rechtsschutz in Anspruch genommen werden kann. Der Umstand, dass § 30 Abs. 4 Nds.SOG eine Unterrichtung vorsieht, sobald dies ohne Gefährdung der Maßnahme möglich ist, steht der Zulässigkeit der Verfassungsbeschwerde nicht entgegen. Eine zeitnahe Kenntnis von der Maßnahme und eine daran anknüpfende Möglichkeit zur Überprüfung im gerichtlichen Verfahren sind nicht gewährleistet, weil § 30 Abs. 5 Nds.SOG umfangreiche Ausnahmetatbestände enthält. Nach dieser Vorschrift unterbleibt die Benachrichtigung, solange Zwecke der Verfolgung einer Straftat oder Ordnungswidrigkeit entgegenstehen (Nr. 1), wenn zur Durchführung der Unterrichtung in unverhältnismäßiger Weise weitere Daten über die betroffene Person erhoben werden müssten (Nr. 2) oder solange durch das Bekanntwerden der Datenerhebung Leib, Leben, Freiheit oder ähnlich schutzwürdige Belange einer Person oder die weitere Verwendung einer Vertrauensperson oder der weitere Einsatz einer Verdeckten Ermittlerin oder eines Verdeckten Ermittlers gefährdet werden (Nr. 3). Insbesondere durch Nummer 3 kann die Mitteilung an die Betroffenen auf unabsehbare Zeit ausgeschlossen sein. 80

II.

Der Beschwerdeführer ist durch die angegriffenen Vorschriften auch selbst und gegenwärtig betroffen. 81

Erfolgt die konkrete Beeinträchtigung - wie hier - zwar erst durch die Vollziehung des angegriffenen Gesetzes, erlangt der Betroffene jedoch in der Regel keine Kenntnis von den Vollzugsakten, reicht es für die Möglichkeit der eigenen und gegenwärtigen Betroffenheit aus, wenn der Beschwerdeführer darlegt, dass er mit einiger Wahrscheinlichkeit durch die auf den angegriffenen Rechtsnormen beruhenden Maßnahmen in seinen Grundrechten berührt wird (vgl. BVerfGE 67, 157 <169 f.>; 100, 313 <354>; 109, 279 <307 f.>). Der geforderte Grad der Wahrscheinlichkeit wird davon beeinflusst, welche Möglichkeit der Beschwerdeführer hat, seine Betroffenheit darzulegen. So ist bedeutsam, ob die Maßnahme auf einen tatbestandlich eng umgrenzten Personenkreis zielt oder ob sie eine große Streubreite hat und Dritte auch zufällig erfassen kann. Darlegungen, durch die sich der Beschwerdeführer selbst einer Straftat bezichtigen müsste, dürfen zum Beleg der eigenen gegenwärtigen Betroffenheit nicht verlangt werden (vgl. BVerfGE 109, 279 <308>). 82

Im Hinblick darauf genügen die Darlegungen des Beschwerdeführers zum Nachweis seiner persönlichen und gegenwärtigen Betroffenheit. Betroffener einer Überwachung ist jeder, in dessen Persönlichkeitsrechte durch die Maßnahme eingegriffen wird, auch wenn er nicht Zielperson der Anordnung ist (vgl. BVerfGE 109, 279 <308>). Die Möglichkeit, Objekt einer Maßnahme der Telekommunikationsüberwachung aufgrund der angegriffenen Regelung zu werden, besteht praktisch für jedermann. Sie kann nicht nur den möglichen Straftäter selbst oder dessen Kontakt- und Begleitpersonen erfassen, sondern auch Personen, die mit den Adressaten der Maßnahme über Telekommunikationseinrichtungen in Verbindung stehen. 83

C.

Die angegriffenen Regelungen des § 33a Abs. 1 Nr. 2 und 3 Nds.SOG sind mit dem Grundgesetz unvereinbar und deshalb nichtig. 84

I.

Maßstab der verfassungsrechtlichen Prüfung ist im Hinblick auf die geltend gemachte Freiheitseinschränkung Art. 10 GG. Das allgemein aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG folgende Recht auf informationelle Selbstbestimmung tritt hinter die speziellere Gewährleistung aus Art. 10 GG zurück, soweit die Schutzbereiche sich 85

überschneiden (vgl. BVerfGE 100, 313 <358>; 110, 33 <53>). Das Gleiche gilt für die Gewährleistung der freien Meinungsäußerung aus Art. 5 Abs. 1 GG, soweit der Eingriff in der staatlichen Wahrnehmung und gegebenenfalls Verarbeitung der mit Mitteln der Telekommunikation geäußerten Meinungen liegt. Darauf aber beschränkt sich die Rüge des Beschwerdeführers.

II.

Die Regelungen des § 33a Abs. 1 Nr. 2 und 3 Nds.SOG ermächtigen zu Eingriffen in das Grundrecht des Art. 10 Abs. 1 GG (1). Die Beschränkungen des Fernmeldegeheimnisses durch die angegriffenen Normen genügen den verfassungsrechtlichen Anforderungen nicht; denn sie sind in formeller Hinsicht verfassungswidrig (2) und verstoßen auch gegen materielles Verfassungsrecht (3). 86

1. a) Der Schutz des Fernmeldegeheimnisses umfasst den Kommunikationsinhalt und die Kommunikationsumstände. Die öffentliche Gewalt soll grundsätzlich nicht die Möglichkeit haben, sich Kenntnis vom Inhalt der über Fernmeldeanlagen abgewickelten mündlichen oder schriftlichen Information zu verschaffen. Dabei bezieht sich der Grundrechtsschutz auf alle mittels der Fernmeldetechnik ausgetauschten Informationen (vgl. BVerfGE 100, 313 <358>; 106, 28 <37>; 107, 299 <313>; 110, 33 <52 f.>). In den Schutzbereich fällt auch die Erlangung der Kenntnis, ob, wann, wie oft und zwischen welchen Personen Telekommunikation stattgefunden hat oder versucht worden ist (vgl. BVerfGE 67, 157 <172>; 85, 386 <396>; 100, 313 <358>; 107, 299 <312 f.>). Die freie Kommunikation, die Art. 10 GG sichert, leidet, wenn zu befürchten ist, dass der Staat entsprechende Kenntnisse verwertet (vgl. BVerfGE 65, 1 <42 f.>; 93, 181 <188>; 100, 313 <359>). Daher erstreckt sich die Schutzwirkung des Art. 10 GG auch auf den Informations- und Datenverarbeitungsprozess, der sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließt und in dem Gebrauch von den erlangten Kenntnissen gemacht wird (vgl. BVerfGE 100, 313 <359>; 110, 33 <68 f.>). 87

b) Ein Eingriff in das Fernmeldegeheimnis liegt vor. Aufgrund der angegriffenen Normen können sich staatliche Stellen ohne Zustimmung der Beteiligten Kenntnis von dem Inhalt und den Umständen eines fernmeldetechnisch vermittelten Kommunikationsvorgangs verschaffen (vgl. BVerfGE 100, 313 <366>; 107, 299 <313>). Nach § 33a Abs. 2 Nds.SOG können Inhalte der Telekommunikation - auch soweit sie innerhalb des Telekommunikationsnetzes in Datenspeichern abgelegt sind - ebenso erfasst werden wie die Verbindungsdaten und die Standortkennung von Mobilfunkendeinrichtungen. Die Vielzahl der im Rahmen der modernen Telekommunikation erfassbaren Daten führt zu einer besonderen Intensität der mit den verschiedenen Überwachungsmaßnahmen verbundenen Eingriffe in das Fernmeldegeheimnis (vgl. BVerfGE 107, 299 <318 f.> - zu Verbindungsdaten). 88

Zusätzliche Eingriffe in den Schutzbereich des Art. 10 GG können dadurch begründet werden, dass die erhobenen Daten unter den Voraussetzungen der §§ 38 ff. Nds.SOG auch zu anderen Zwecken als dem ursprünglichen Erhebungszweck verarbeitet und übermittelt werden können (vgl. BVerfGE 110, 33 <68 f.>). 89

2. Die Regelungen des § 33a Abs. 1 Nr. 2 und 3 Nds.SOG sind formell verfassungswidrig. Der niedersächsische Gesetzgeber hat gegen das Zitiergebot des Art. 19 Abs. 1 Satz 2 GG verstoßen (a). Darüber hinaus hat er seine Gesetzgebungskompetenz überschritten, soweit nach § 33a Abs. 1 Nr. 2 und 3 Nds.SOG die Telekommunikationsüberwachung zur Vorsorge für die Verfolgung von Straftaten vorgesehen ist (b). 90

a) Im Gesetz zur Änderung des Niedersächsischen Gefahrenabwehrgesetzes vom 11. Dezember 2003 (Nds.GVBI S. 414) fehlt der nach Art. 19 Abs. 1 Satz 2 GG erforderliche Hinweis auf die Einschränkung des Art. 10 Abs. 1 GG. 91

aa) Nach Art. 19 Abs. 1 Satz 2 GG muss ein Gesetz dasjenige Grundrecht unter Angabe seines Artikels benennen, das durch dieses Gesetz oder aufgrund dieses Gesetzes eingeschränkt wird. Das Grundrecht auf Wahrung des Fernmeldegeheimnisses wird durch Art. 10 Abs. 1 GG geschützt und steht nach Art. 10 Abs. 2 Satz 1 GG unter einem ausdrücklichen Gesetzesvorbehalt. Das Zitiergebot findet Anwendung auf Grundrechte, die aufgrund ausdrücklicher Ermächtigung vom Gesetzgeber eingeschränkt werden dürfen (vgl. BVerfGE 64, 72 <79 f.>), also auch auf das Fernmeldegeheimnis. Die Verletzung des Zitiergebots bewirkt die Verfassungswidrigkeit des Gesetzes (vgl. BVerfGE 5, 13 <15 f.>). 92

Das Zitiergebot erfüllt eine Warn- und Besinnungsfunktion (vgl. BVerfGE 64, 72 <79 f.>). Durch die Benennung des Eingriffs im Gesetzeswortlaut soll gesichert werden, dass der Gesetzgeber nur Eingriffe vornimmt, die ihm als solche bewusst sind und über deren Auswirkungen auf die betroffenen Grundrechte er sich Rechenschaft ablegt (vgl. BVerfGE 5, 13 <16>; 85, 386 <404>). Die ausdrückliche Benennung erleichtert es auch, die Notwendigkeit und das Ausmaß des beabsichtigten Grundrechtseingriffs in öffentlicher Debatte zu klären. Diese Warn- und Besinnungsfunktion betrifft nicht nur eine erstmalige Grundrechtseinschränkung, sondern wird bei jeder Veränderung der Eingriffsvoraussetzungen bedeutsam, die zu neuen Grundrechtseinschränkungen führt. 93

Der gesetzliche Hinweis auf die Grundrechtseinschränkung war vorliegend nicht entbehrlich. Zwar enthielt bereits § 10 NGefAG einen Hinweis auf die Einschränkung des Art. 10 Abs. 1 GG, der auch im Niedersächsischen Gesetz über die öffentliche Sicherheit und Ordnung unverändert fortgilt. Die Benennung des eingeschränkten Grundrechts im fortgeltenden Gesetz reichte aber nicht aus, da mit § 33a Nds.SOG eine deutlich erweiterte Eingriffsgrundlage für eine präventive Telekommunikationsüberwachung durch die Polizei geschaffen wurde (vgl. LTDrucks 15/240, S. 15). 94

Das Zitiererfordernis entfällt nicht im Hinblick auf den Hinweis in der Gesetzesbegründung (LTDrucks 15/240, S. 15), der Gesetzgeber sei sich der Einschränkung des Fernmeldegeheimnisses durch § 33a Nds.SOG bewusst gewesen und davon ausgegangen, dass dem Zitiergebot durch die bestehende Regelung des § 10 NGefAG (jetzt § 10 Nds.SOG) entsprochen werde. Ein bloßer Hinweis in der Gesetzesbegründung genügt dem Formerfordernis des Art. 19 Abs. 1 Satz 2 GG nicht. Im Übrigen ist die im Gesetzentwurf ursprünglich vorgesehene Regelung später nach Befassung des Landtagsausschusses für Inneres und Sport deutlich verschärft und die Zitierproblematik ist in den Gesetzesmaterialien nicht erneut thematisiert worden. 95

bb) Allerdings bleibt die Nichtbeachtung des Zitiergebots für die Wirksamkeit des angegriffenen Gesetzes ohne Konsequenzen. Das Bundesverfassungsgericht hatte bisher nicht geklärt, ob es in den Fällen, in denen das ändernde Gesetz zu neuen Grundrechtseinschränkungen führt oder ermächtigt, den Anforderungen des Art. 19 Abs. 1 Satz 2 GG genügt, wenn das geänderte Gesetz bereits eine Zitiervorschrift im Sinne dieser Bestimmung enthält. In der Folge hat sich hierzu eine unterschiedliche Praxis in der Gesetzgebung herausgebildet. Aus Gründen der Rechtssicherheit führt die Nichtbeachtung des Zitiergebots erst bei solchen grundrechtseinschränkenden Änderungsgesetzen zur Nichtigkeit, die nach dem Zeitpunkt der Verkündung dieser Entscheidung beschlossen werden. 96

b) Das Land Niedersachsen hatte nur für einen Teil der angegriffenen Regelungen eine Gesetzgebungskompetenz. 97

Nach Art. 70 Abs. 1 GG verfügen die Länder über das Recht der Gesetzgebung, soweit die Gesetzgebungsbefugnis nicht dem Bund zugewiesen ist. Zwar ist die präventive Telekommunikationsüberwachung nicht der ausschließlichen Kompetenz des Bundes nach Art. 73 Nr. 7 GG zuzuordnen (aa) und stellt die Verhütung von Straftaten eine landesrechtliche Aufgabe der Gefahrenabwehr dar (bb). § 33a Abs. 1 Nr. 2 und 3 Nds.SOG ist aber mit den Vorschriften des Grundgesetzes zur Gesetzgebungsbefugnis insofern nicht vereinbar, als die Telekommunikationsüberwachung auch zur Vorsorge für die Verfolgung von Straftaten ermöglicht wird. Dieser Sachbereich ist der konkurrierenden Gesetzgebung gemäß Art. 72, Art. 74 Abs. 1 Nr. 1 GG zuzuordnen. Jedenfalls für den Bereich der Telekommunikationsüberwachung hat der Bundesgesetzgeber von seiner Regelungsbefugnis abschließend Gebrauch gemacht (cc). 98

aa) Eine Zuständigkeit des Bundes für Maßnahmen im Bereich der Telekommunikationsüberwachung folgt nicht aus Art. 73 Nr. 7 GG. Die ausschließliche Zuweisung der Gesetzgebungsbefugnis für die Telekommunikation betrifft die technische Seite der Errichtung einer Telekommunikationsinfrastruktur und der Informationsübermittlung, nicht aber Regelungen, die auf die übermittelten Inhalte oder die Art der Nutzung der Telekommunikation ausgerichtet sind. Bei den Regelungen über die Telekommunikationsüberwachung in § 33a Nds.SOG geht es nicht vorrangig um technische Fragen der Datenübermittlung, sondern um den Zugriff auf Informationen. Überwachungsmaßnahmen umfassen zwar Tätigkeiten, mit denen die Übertragungstechnik in Anspruch genommen wird; auch sind sie darauf angewiesen, dass die Ausstattung der Telekommunikationsnetze eine Überwachung technisch zulässt. Vorschriften, die die Telekommunikationsüberwachung zum Zwecke der Erlangung von Informationen für Aufgaben des Straf- oder Polizeirechts ermöglichen, werden jedoch maßgebend durch den jeweiligen Zweck der Überwachungsmaßnahmen und die daran ausgerichteten Eingriffsvoraussetzungen geprägt. Sie sind auch kompetenzmäßig dem Bereich zuzurechnen, für dessen Zwecke die Überwachung erfolgen soll, hier dem der Straftatenverhütung oder -verfolgung. 99

bb) Die Verhütung einer Straftat liegt in der Gesetzgebungskompetenz der Länder für die Gefahrenabwehr, und zwar auch dann, wenn sie vorbeugend für den Zeitraum vor dem Beginn einer konkreten Straftat vorgesehen wird. Wie weit der Gesetzgeber eine derartige Maßnahme in das Vorfeld künftiger Rechtsgutverletzung verlegen darf, ist eine Frage des materiellen Rechts, berührt aber nicht die Gesetzgebungskompetenz des Landes. 100

Dem Landesgesetzgeber ging es bei der Neuregelung um die vorbeugende polizeiliche Tätigkeit im Vorfeldbereich der Rechtsgutgefährdung. Dies kam im ursprünglichen Gesetzentwurf vom 17. Juni 2003 (LTDrucks 15/240, S. 4) dadurch zum Ausdruck, dass die Telekommunikationsüberwachung nach § 33a Abs. 1 Nr. 2 und 3 der vorgesehenen Regelung "zur vorbeugenden Bekämpfung besonders schwerwiegender Straftaten" möglich sein sollte. Demgegenüber schlug der Landtagsausschuss für Inneres und Sport die Gesetz gewordene Fassung vor. In seinem schriftlichen Bericht (LTDrucks 15/776, S. 6) heißt es, die Eingriffsvoraussetzungen des Entwurfs von § 33a Abs. 1 Nr. 1 bis 3 sollten an die 101

des § 34 Abs. 1 Satz 1 Nr. 1 bis 3 NGefAG angepasst werden. Die "sonstigen Änderungen in Absatz 1" seien redaktioneller Natur und dienen "der sprachlichen Anpassung" an die parallele Regelung in dem schon bestehenden § 34 Abs. 1 Satz 1 NGefAG.

Für die vorbeugende Bekämpfung von Straftaten besteht keine konkurrierende Gesetzgebungskompetenz des Bundes nach Art. 74 Abs. 1 Nr. 1 GG (gerichtliches Verfahren unter Einschluss des Strafverfahrens). Das Tatbestandsmerkmal der Verhütung von Straftaten erfasst Maßnahmen, die drohende Rechtsgutverletzungen von vornherein und in einem Stadium verhindern sollen, in dem es noch nicht zu strafwürdigem Unrecht gekommen ist. Derartige Maßnahmen sind allenfalls insoweit der Bundeskompetenz zuzuordnen, als sie zu einem von ihr erfassten Sachbereich in einem notwendigen Zusammenhang stehen, insbesondere für den wirksamen Vollzug der Bundesregelung erforderlich sind (vgl. BVerfGE 109, 190 <215>). Das ist bei den hier zu beurteilenden Bestimmungen des niedersächsischen Gesetzes nicht der Fall. 102

cc) Die Telekommunikationsüberwachung ist allerdings nicht auf die vorbeugende Bekämpfung von Straftaten beschränkt, sondern sieht in § 33a Abs. 1 Nr. 2 und 3 Nds.SOG die "Vorsorge für die Verfolgung von Straftaten" als eigenständiges Tatbestandsmerkmal vor. Die Vorsorge für die Verfolgung noch gar nicht begangener, sondern in ungewisser Zukunft bevorstehender Straftaten gehört zum gerichtlichen Verfahren. Von der in Art. 74 Abs. 1 Nr. 1 GG normierten konkurrierenden Gesetzgebung zur Strafverfolgung hat der Bundesgesetzgeber im Bereich der Telekommunikationsüberwachung abschließend Gebrauch gemacht, so dass die Länder gemäß Art. 72 Abs. 1 GG von der Gesetzgebung ausgeschlossen sind. 103

(1) Das niedersächsische Recht hat die Verfolgungsvorsorge als eigenständige Aufgabe mit der Befugnis zur Telekommunikationsüberwachung geregelt. Das Gesetz trennt ausdrücklich zwischen der Vorsorge für die Verfolgung und der Verhütung einer Straftat. Danach können die Maßnahmen gemäß § 33a Abs. 2 Satz 1 Nr. 1 bis 3 Nds.SOG auch ergriffen werden, wenn die Verhütung einer Straftat nicht oder nicht mehr im Raum steht. 104

(2) Die Vorsorge für die spätere Verfolgung von Straftaten ist kompetenzmäßig dem "gerichtlichen Verfahren" im Sinne des Art. 74 Abs. 1 Nr. 1 GG zuzuordnen. Die gesetzliche Ermächtigung bezweckt die Sicherung von Beweisen für ein künftiges Strafverfahren. 105

Allerdings fehlt es im Zeitpunkt der Überwachungsmaßnahme, anders als für die Strafverfolgung im herkömmlichen Sinne, an einer bereits begangenen Straftat. Die Verfolgungsvorsorge erfolgt in zeitlicher Hinsicht präventiv, betrifft aber gegenständlich das repressiv ausgerichtete Strafverfahren. Die Daten werden zu dem Zweck der Verfolgung einer in der Zukunft möglicherweise verwirklichten konkreten Straftat und damit letztlich nur zur Verwertung in einem künftigen Strafverfahren, also zur Strafverfolgung, erhoben. Dabei knüpft die Ermächtigung zur Erhebung personenbezogener Daten in § 33a Abs. 1 Nr. 2 und 3 Nds.SOG an das erwartete Handeln von Personen an, bei denen Tatsachen die Annahme rechtfertigen, dass sie Straftaten von erheblicher Bedeutung begehen werden. Eine Verwertung der erhobenen Daten für diesen Zweck kommt erst in Betracht, wenn tatsächlich eine Straftat begangen wurde und daraus strafprozessuale Konsequenzen gezogen werden. Die der Verfolgungsvorsorge zugeordneten Daten und Informationen sind insofern dazu bestimmt, in ungewisser Zukunft in ein Ermittlungs- und Hauptverfahren einzufließen. Es geht - jenseits eines konkreten Anfangsverdachts (vgl. LTDruks 15/240, S. 16) - um die Beweisbeschaffung zur Verwendung in künftigen Strafverfahren, nicht um eine präventive Datenerhebung zur Verhütung von Straftaten. Eine solche Verfolgungsvorsorge gehört zum gerichtlichen Verfahren im Sinne des Art. 74 Abs. 1 Nr. 1 GG. 106

Sowohl im gerichtlichen Hauptverfahren als auch im vorgelagerten Ermittlungsverfahren geht es um die Aufklärung eines konkreten Straftatverdachts gegen einen konkreten Beschuldigten. Dies bedeutet indes nicht, dass erst nach Vorliegen eines Anfangsverdachts die Zuordnung zum gerichtlichen Verfahren erfolgen kann (so aber Gärditz, Strafprozess und Prävention, 2003, S. 328, 331, 359, 429). Art. 74 Abs. 1 Nr. 1 GG enthält keine Einschränkungen dahingehend, dass vorsorgende Maßnahmen, die sich auf die Durchführung künftiger Strafverfahren beziehen, von der Zuweisung zur konkurrierenden Gesetzgebungskompetenz nicht erfasst sein sollen (vgl. BVerfG, 3. Kammer des Zweiten Senats, BVerfGE 103, 21 <30>). Die Ungewissheit, ob die zur Strafverfolgung vorsorglich gespeicherten Daten für diesen Zweck später benötigt werden, kann sich bei der Beurteilung der Rechtmäßigkeit der Maßnahme auswirken, steht aber der Zuordnung der Regelungen zur Gesetzgebungskompetenz für das gerichtliche Verfahren nicht entgegen. 107

(3) Der Bundesgesetzgeber hat von seiner konkurrierenden Gesetzgebungskompetenz im Sinne von Art. 72 Abs. 1 GG in abschließender Weise Gebrauch gemacht. 108

(a) Inwieweit bundesgesetzliche Regelungen erschöpfend sind, kann nicht allgemein, sondern nur anhand der einschlägigen Bestimmungen und des jeweiligen Sachbereichs festgestellt werden (vgl. BVerfGE 109, 190 <229>). Es 109

ist in erster Linie auf das Bundesgesetz selbst, sodann auf den hinter dem Gesetz stehenden Regelungszweck, ferner auf die Gesetzgebungsgeschichte und die Gesetzesmaterialien abzustellen (vgl. BVerfGE 98, 265 <300 f.>). Der Bund macht von seiner Kompetenz nicht nur dann Gebrauch, wenn er eine Regelung getroffen hat. Vielmehr kann auch das absichtsvolle Unterlassen eine Sperrwirkung für die Länder erzeugen (vgl. BVerfGE 32, 319 <327 f.>; 98, 265 <300>). Zu einem erkennbar gewordenen Willen des Bundesgesetzgebers, zusätzliche Regelungen auszuschließen, darf sich ein Landesgesetzgeber nicht in Widerspruch setzen, selbst wenn er das Bundesgesetz für unzureichend hält (vgl. BVerfGE 32, 319 <327>; 36, 193 <211 f.>; 36, 314 <320>; 85, 134 <147>; 98, 265 <300>; 109, 190 <230>).

Der Eintritt einer Sperrwirkung zu Lasten der Länder setzt voraus, dass der Gebrauch der Kompetenz durch den Bund bei Gesamtwürdigung des Normenkomplexes hinreichend erkennbar ist. Hat der Bund einen Sachbereich in diesem Sinne abschließend geregelt, ist die Gesetzgebung den Ländern unabhängig davon versperrt, ob die landesrechtlichen Regelungen den bundesrechtlichen Bestimmungen widerstreiten oder sie nur ergänzen. Die rechtsetzenden Organe sind verpflichtet, ihre Regelungen so aufeinander abzustimmen, dass die Rechtsordnung nicht widersprüchlich wird. Konzeptionelle Entscheidungen des Bundesgesetzgebers dürfen durch die Landesgesetzgeber nicht verfälscht werden (vgl. BVerfGE 98, 265 <300 f.>). 110

(b) Der Bundesgesetzgeber hat mit der Regelung der Telekommunikationsüberwachung in der Strafprozessordnung eine abschließende Regelung getroffen. Die bestehenden Vorschriften lassen insbesondere eine konzeptionelle Entscheidung gegen zusätzliche, in das erweiterte Vorfeld einer Straftat verlagerte Maßnahmen erkennen. Dieser Entscheidung widersprechen die angegriffenen Regelungen. 111

Die Gesetzesmaterialien zu den in der Strafprozessordnung geregelten Telekommunikationsüberwachungsmaßnahmen enthalten zwar keine ausdrücklichen Festlegungen zur Frage der abschließenden Regelung für den Bereich der Telekommunikationsüberwachung. Der abschließende Charakter ergibt sich jedoch bei Betrachtung der bestehenden strafprozessualen Vorschriften. 112

(aa) Der Bundesgesetzgeber hat die Überwachung der Telekommunikation zu Zwecken der Strafverfolgung in den §§ 100a, 100b, 100g, 100h und 100i StPO nach Umfang, Zuständigkeit und Zweck sowie hinsichtlich der für die jeweilige Maßnahme erforderlichen Voraussetzungen umfassend geregelt. Dabei kann aus dem Umstand, dass die genannten Vorschriften an eine konkret begangene oder konkret vorbereitete Tat anknüpfen, also gerade keine Datenermittlung im Vorfeld der Begehung einer Straftat betreffen, nicht geschlossen werden, der Bundesgesetzgeber habe Raum für weitere landesgesetzliche Eingriffsnormen belassen wollen. Der Bundesgesetzgeber war sich - wie die bestehenden Vorschriften in anderen Bereichen zeigen (etwa die §§ 81b, 81g StPO) - durchaus der kompetenzrechtlichen Möglichkeit bewusst, im Bereich der Strafverfolgung auch präventive Regelungen zu treffen. 113

Der Verzicht des Bundesgesetzgebers darauf, die Telekommunikationsüberwachung im Vorfeldbereich noch weiter auszudehnen, ist eine bewusste Entscheidung. Anhaltspunkte dafür, dass der Bundesgesetzgeber insofern Parallelregelungen durch die Länder und damit Überschneidungen hätte in Kauf nehmen wollen, sind nicht erkennbar. Seine Entscheidung über die zur Strafverfolgung einsetzbaren Maßnahmen und ihre tatbestandlichen Voraussetzungen müssen die Länder respektieren (vgl. BVerfGE 98, 265 <300 f.>). 114

Der Gesetzgeber hat die tatbestandlichen Voraussetzungen der Telekommunikationsüberwachung im Interesse rechtsstaatlicher Bestimmtheit und Verhältnismäßigkeit und unter Berücksichtigung der Vorgaben der verfassungsgerichtlichen Rechtsprechung möglichst genau zu regeln versucht und an den Verdacht von Straftaten oder ihrer Vorbereitung angeknüpft. Sowohl die Echtzeitüberwachung der Telekommunikation nach den §§ 100a und 100b StPO als auch die Abfrage von Verbindungsdaten nach den §§ 100g und 100h StPO sind - unter anderem zur Begrenzung der großen Streubreite entsprechender Maßnahmen - vom Vorliegen enger gefasster Kriterien für einen Anfangsverdacht abhängig. Die Überwachung der Telekommunikationsinhalte ist nur zulässig zur Aufklärung im Gesetz ausdrücklich bestimmter besonders schwerer Straftaten (§ 100a Satz 1 StPO). Dem Erfordernis eines frühzeitigen Einsatzes der Telekommunikationsüberwachung hat der Bundesgesetzgeber dadurch Rechnung getragen, dass er die Maßnahmen unter bestimmten Voraussetzungen bereits im Vorbereitungsstadium zulässt (§ 100a Satz 1, § 100g Abs. 1 Satz 1 StPO: "durch eine Straftat vorbereitet"). Diese gezielten Eingrenzungen könnten hinfällig werden, wenn die Länder vergleichbare Maßnahmen zur Telekommunikationsüberwachung ebenfalls mit dem Ziel der Sicherung späterer Strafverfolgung unter anderen, etwa geringeren, Voraussetzungen normieren könnten. Damit entstünde das Risiko widersprüchlicher Regelungen oder von Überschneidungen unterschiedlicher Normen. 115

Das zeigt beispielhaft der Vergleich von § 100a StPO und § 33a Abs. 1 Nds.SOG. So sind in den Fällen des Versuchs oder der Vorbereitung einer Straftat - die von § 100a StPO erfasst werden - im Regelfall zugleich die tatbestandlichen Voraussetzungen des weiter gefassten § 33a Abs. 1 Nr. 2 Nds.SOG erfüllt. Das Niedersächsische Gesetz über die 116

öffentliche Sicherheit und Ordnung bietet keine Anhaltspunkte für eine restriktive Auslegung und enthält keine Vorkehrung zur Verhinderung von Überschneidungen. Der in § 100a StPO enthaltene Straftatenkatalog ist nicht nur anders zusammengesetzt als der durch § 33a Abs. 1 Nds.SOG in Bezug genommene (§ 2 Nr. 10 Nds.SOG), sondern auch wesentlich enger gefasst. Nach § 33a Abs. 1 Nr. 2 und 3 Nds.SOG werden Vorfeldmaßnahmen möglich, die nach der Strafprozessordnung gerade ausgeschlossen sein sollen. Darüber hinaus fordert § 33a Abs. 1 Nr. 2 und 3 Nds.SOG anders als § 100a StPO nicht den Verdacht einer Straftat, ihres Versuchs oder der Vorbereitung, sondern begnügt sich mit Tatsachen, die die Annahme rechtfertigen, dass die Person künftig Straftaten begehen wird.

Wären beide Regelungssysteme parallel anwendbar, könnten die Unterschiede in den tatbestandlichen Voraussetzungen zu Unklarheiten führen. Denn die Polizeibehörden als Behörden der Gefahrenabwehr einerseits und der Strafverfolgung andererseits dürften auf beide Ermächtigungen zurückgreifen. Auch formalrechtlich bestehen Unterschiede. So ist nach § 100b Abs. 1 Satz 2 StPO bei Gefahr im Verzug eine Entscheidung durch die Staatsanwaltschaft vorgesehen, in § 33a Abs. 4 Nds.SOG demgegenüber - dem Charakter des Polizeirechts entsprechend - eine Entscheidung durch die Polizei selbst. 117

Wäre die polizeirechtliche Regelung im Hinblick auf die Verfolgungsvorsorge parallel zu der strafprozessualen anwendbar, wäre die Telekommunikationsüberwachung im Vorfeld der Vorbereitung, des Versuchs oder der Ausführung unter geringeren rechtsstaatlichen Anforderungen möglich als dann, wenn der Täter schon konkret zur Rechtsgutverletzung angesetzt hat. Ein solches Konzept wäre in sich widersprüchlich. Es ist nicht erkennbar, dass der Bundesgesetzgeber einen solchen Widerspruch hat in Kauf nehmen wollen. 118

(bb) § 484 Abs. 4 StPO steht der Annahme einer abschließenden bundesgesetzlichen Regelung nicht entgegen. Nach dieser Norm richtet sich die Verwendung personenbezogener Daten, die für Zwecke künftiger Strafverfahren in Dateien der Polizei gespeichert sind oder werden - mit Ausnahme der Verwendung für Zwecke eines Strafverfahrens - nach den Polizeigesetzen. Anhaltspunkte dafür, dass der Bundesgesetzgeber damit die präventive Datenerhebung zum Zwecke späterer Strafverfolgung durch die Polizeibehörden voraussetzen und von seiner Kompetenz zur Regelung dieses Bereichs gerade nicht abschließend Gebrauch machen wollte, bieten weder die Gesetzesbegründung zu § 484 Abs. 4 StPO (BTDrucks 14/1484, S. 33) noch der Sinn dieser Regelung. 119

3. Die angegriffenen Normen sind auch in materieller Hinsicht nicht mit der Verfassung vereinbar. Sie sind nicht hinreichend bestimmt (a) und genügen nicht den Anforderungen, die der Verhältnismäßigkeitsgrundsatz an die Angemessenheit eines grundrechtsbeschränkenden Gesetzes im Sinne des Art. 10 Abs. 1 Satz 2 GG stellt (b). Ferner fehlen im Gesetz Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung (c). 120

a) § 33a Abs. 1 Nr. 2 und 3 Nds.SOG entsprechen nicht dem rechtsstaatlichen Gebot der Normenbestimmtheit und Normenklarheit. 121

aa) Grundlage des Bestimmtheitsgebots ist vorliegend Art. 10 GG selbst (vgl. BVerfGE 110, 33 <52 ff.>). Das Gebot soll sicherstellen, dass der betroffene Bürger sich auf mögliche belastende Maßnahmen einstellen kann, dass die gesetzesausführende Verwaltung für ihr Verhalten steuernde und begrenzende Handlungsmaßstäbe vorfindet und dass die Gerichte die Rechtskontrolle durchführen können (vgl. BVerfGE 110, 33 <52 ff.>). Der Anlass, der Zweck und die Grenzen des Eingriffs müssen in der Ermächtigung bereichsspezifisch, präzise und normenklar festgelegt werden (vgl. BVerfGE 100, 313 <359 f., 372>; 110, 33 <53>). 122

(1) Anhand der gesetzlichen Regelung muss der Betroffene die Rechtslage so erkennen können, dass er sein Verhalten danach ausrichten vermag. Die Anforderungen an die Bestimmtheit und Klarheit der Norm erhöhen sich, wenn die Unsicherheit bei der Beurteilung der Gesetzeslage die Betätigung von Grundrechten erschwert (vgl. BVerfGE 83, 130 <145>; 86, 288 <311>; 108, 52 <75>; 110, 33 <53>). Für Ermächtigungen zu Überwachungsmaßnahmen verlangt das Bestimmtheitsgebot zwar nicht, dass die konkrete Maßnahme vorhersehbar ist, wohl aber, dass die betroffene Person grundsätzlich erkennen kann, bei welchen Anlässen und unter welchen Voraussetzungen ein Verhalten mit dem Risiko der Überwachung verbunden ist. Hinreichend bestimmte Voraussetzungen des staatlichen Eingriffs - und damit der ihn begrenzenden Maßstäbe - kommen auch Personen zugute, denen die konkreten Handlungsvoraussetzungen nicht bekannt sein können, weil sie den Anlass nicht geschaffen haben und eher zufällig betroffen sind. 123

(2) Die Anforderungen an die Bestimmtheit und Klarheit der Norm dienen ferner dazu, die Verwaltung zu binden und ihr Verhalten nach Inhalt, Zweck und Ausmaß zu begrenzen (vgl. BVerfGE 56, 1 <12>; 110, 33 <54>). Dies setzt voraus, dass hinreichend klare Maßstäbe bereitgestellt werden. Die Entscheidung über die Grenzen der Freiheit des Bürgers darf nicht einseitig in das Ermessen der Verwaltung gestellt sein (vgl. BVerfGE 78, 214 <226>). Dem Gesetz kommt im Hinblick auf den Handlungsspielraum der Exekutive eine begrenzende Funktion zu, die rechtmäßiges Handeln des 124

Staates sichern und dadurch auch die Freiheit der Bürger schützen soll. Dieser Aspekt der Bindung der Verwaltung ist bei einer Überwachungsmaßnahme besonders wichtig, da der Betroffene von ihr nichts weiß und daher keine Möglichkeit hat, in einem vorgeschalteten Verfahren Einfluss auf das eingreifende Verhalten der Verwaltung zu nehmen. Der Schutz durch begrenzende Maßstäbe erhält zusätzlich besondere Bedeutung dadurch, dass auch betroffene Dritte - hier die anderen Telekommunikationsteilnehmer, gegebenenfalls auch Kontakt- und Begleitpersonen - mit einer staatlichen Überwachung nicht rechnen und sich deshalb vor einem Einblick in ihren Privatbereich nicht schützen können (vgl. BVerfGE 110, 33 <54>).

(3) Darüber hinaus sollen die Normenbestimmtheit und die Normenklarheit die Gerichte in die Lage versetzen, die Verwaltung anhand rechtlicher Maßstäbe zu kontrollieren. Das gilt auch, wenn das Gericht schon vor Ergreifen der Maßnahme oder bei ihrem weiteren Vollzug zur Kontrolle der Verwaltung eingeschaltet wird (vgl. BVerfGE 110, 33 <54 f.>). 125

bb) Bei der Vorsorge für die Verfolgung künftiger Straftaten oder bei ihrer Verhütung kann nicht an dieselben Kriterien angeknüpft werden, die für die Gefahrenabwehr oder die Verfolgung begangener Straftaten entwickelt worden sind. Maßnahmen der Gefahrenabwehr, die in die Freiheitsrechte der Bürger eingreifen, setzen eine konkrete Gefahrenlage voraus. Die Strafverfolgung knüpft an den Verdacht einer schon verwirklichten Straftat an. Solche Bezüge fehlen, soweit die Aufgabe darin besteht, im Vorfeld der Gefahrenabwehr und Strafverfolgung Vorsorge im Hinblick auf in der Zukunft eventuell zu erwartende Straftaten zu treffen. Deshalb müssen hier die Bestimmtheitsanforderungen spezifisch an dieser Vorfeldsituation ausgerichtet werden. 126

Bei der Vorverlagerung des Eingriffs in eine Phase, in der sich die Konturen eines Straftatbestandes noch nicht abzeichnen, besteht das Risiko, dass der Eingriff an ein nur durch relativ diffuse Anhaltspunkte für mögliche Straftaten gekennzeichnetes, in der Bedeutung der beobachteten Einzelheiten noch schwer fassbares und unterschiedlich deutbares Geschehen anknüpft. Sachverhaltsfeststellung und Prognose sind mit vorgreiflichen Einschätzungen über das weitere Geschehen, ebenso wie über die erst noch bevorstehende strafrechtliche Relevanz der festgestellten Tatsachen verknüpft (vgl. BVerfGE 110, 33 <59>). Da der Eingriff sich auf mögliche zukünftige Aktivitäten bezieht, kann er sich häufig nur auf Tatsachen stützen, bei denen noch offen ist, ob sie sich zu einer Rechtsgutverletzung weiterentwickeln (vgl. BVerfGE 110, 33 <59>). Die Situation der Vorfeldermittlung ist insofern durch eine hohe Ambivalenz der potenziellen Bedeutung einzelner Verhaltensumstände geprägt. Die Indizien oder einzelne beobachtete Tätigkeiten können in harmlosen, strafrechtlich unerheblichen Zusammenhängen verbleiben; sie können aber auch der Beginn eines Vorgangs sein, der zur Straftat führt. 127

Sieht der Gesetzgeber in solchen Situationen Grundrechtseingriffe vor, so hat er die den Anlass bildenden Straftaten sowie die Anforderungen an Tatsachen, die auf die künftige Begehung hindeuten, so bestimmt zu umschreiben, dass das im Bereich der Vorfeldermittlung besonders hohe Risiko einer Fehlprognose gleichwohl verfassungsrechtlich noch hinnehmbar ist. Die Norm muss 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 (vgl. BVerfGE 110, 33 <56>). 128

cc) § 33a Abs. 1 Nr. 2 und 3 Nds.SOG genügt diesen Anforderungen nicht. 129

Die Regelungen verlangen keinen konkreten, in der Entwicklung begriffenen Vorgang oder dessen Planung (vgl. dazu BVerfGE 110, 33 <56, 57, 58>), aber auch keine konkreten Vorbereitungshandlungen, wie sie etwa in § 23a Abs. 2 und 3 des Zollfahndungsdienstgesetzes (ZFdG) in der Fassung des Gesetzes zur Neuregelung der präventiven Telekommunikations- und Postüberwachung durch das Zollkriminalamt und zur Änderung der Investitionszulagengesetze 2005 und 1999 vom 21. Dezember 2004 (BGBl I S. 3603) umschrieben sind. Es genügt die auf Tatsachen gegründete, nicht näher konkretisierte Möglichkeit, dass jemand irgendwann in Zukunft Straftaten von erheblicher Bedeutung begehen wird. 130

Eine derart weite Ermächtigung wird dem Bestimmtheitsgebot nicht gerecht. Dies betrifft sowohl die Anknüpfung an Tatsachen, die die Annahme der Begehung von Straftaten erheblicher Bedeutung rechtfertigen (§ 33a Abs. 1 Nr. 2 in Verbindung mit § 2 Nr. 10 Nds.SOG), als auch den Begriff der Kontakt- und Begleitpersonen (§ 33a Abs. 1 Nr. 3 Nds.SOG). Das Erfordernis richterlicher Anordnung der Maßnahme beseitigt die Bestimmtheitsdefizite nicht. 131

(1) (a) Der in § 33a Abs. 1 Nr. 2 Nds.SOG verwendete Begriff der "Tatsache" ist isoliert betrachtet allerdings hinreichend bestimmt (vgl. BVerfGE 110, 33 <61>). Er nimmt eine Abgrenzung zu bloßen Vermutungen und allgemeinen Erfahrungssätzen vor, die für sich allein gerade nicht ausreichen sollen. Dennoch genügt das Tatbestandsmerkmal in seiner Bezugnahme auf eine künftige Straftatenbegehung den Bestimmtheitsanforderungen 132

nicht.

Es sind vielfältige Anknüpfungen denkbar, die nach hypothetischem Kausalverlauf in der Straftatenbegehung eines potenziellen Täters (so die Begriffswahl bei J. Ipsen, NdsVBl 2003, S. 281 <285>) münden können. Weder hinsichtlich möglicher Indikatoren und des Grads der Wahrscheinlichkeit eines solchen Ablaufs noch in zeitlicher Hinsicht sieht das Gesetz Beschränkungen vor. Die im Vorfeld künftiger Straftaten bestehenden Schwierigkeiten der Abgrenzung eines harmlosen von dem in eine Straftatenbegehung mündenden Verhaltens werden in der Ermächtigung nicht durch einschränkende Tatbestandsmerkmale bewältigt. Die Bestimmung der Voraussetzungen und Grenzen des Eingriffs obliegt vielmehr der Polizei. Sie entscheidet ohne nähere gesetzliche Vorgaben über die Grenzen der Freiheit des Bürgers und muss sich die Maßstäbe dafür selbst zurechtlegen. Sie wird insoweit gewissermaßen tatbestandsergänzend tätig. Die Schaffung eingriffsbeschränkender Maßstäbe ist aber Aufgabe des Gesetzgebers. 133

(b) Die Unbestimmtheit und das damit einhergehende Risiko der Fehlprognose werden nicht durch die Ausrichtung auf "Straftaten von erheblicher Bedeutung" vermindert. Dieses Tatbestandsmerkmal bietet keine Anhaltspunkte dafür, wann ein Verhalten auf die künftige Begehung solcher Straftaten hindeutet. Die vom Gesetz in Bezug genommenen Straftatbestände sind in diesem Stadium, in dem der künftige Geschehensablauf noch offen ist, ohnehin nur wenig geeignet, den maßgeblichen Sachverhalt so einzugrenzen, dass er Indizien für eine zukünftige Straftatenbegehung bietet. Darüber hinaus ist die Bezugnahme auf die Begehung von "Straftaten von erheblicher Bedeutung" selbst nicht hinreichend bestimmt. 134

Der Begriff der Straftat von erheblicher Bedeutung ist in § 2 Nr. 10 Nds.SOG legal definiert und hinreichend bestimmt, soweit konkrete Straftatbestände benannt sind. Die zusätzliche Einbeziehung aller Vergehen, die mit einem der ausdrücklich genannten "nach dem geschützten Rechtsgut und der Strafandrohung" vergleichbar sind (Buchstabe b), genügt den Bestimmtheitsanforderungen jedoch nicht. Insbesondere wird nicht deutlich, wie aus der Bezugnahme auf das Rechtsgut einerseits und den Strafrahmen andererseits eine Vergleichbarkeit hinsichtlich der Erheblichkeit der weiteren Straftaten erschlossen werden soll. 135

(2) Nicht hinreichend bestimmt ist ferner die Regelung in § 33a Abs. 1 Nr. 3 Nds.SOG, die zur Überwachung der Telekommunikation bei Kontakt- und Begleitpersonen ermächtigt, soweit dies unerlässlich ist. 136

Die Bezugnahme in § 33a Abs. 1 Nr. 3 Nds.SOG auf den in Nummer 2 genannten Personenkreis bewirkt, dass die dort bestehenden Bestimmtheitsdefizite es auch erschweren, die Tatbestandsvoraussetzungen für Überwachungsmaßnahmen gegenüber Kontakt- oder Begleitpersonen einzugrenzen. Hinzu kommen Unklarheiten, die mit dem Begriff der Kontakt- und Begleitperson selbst verbunden sind. Die Legaldefinition in § 2 Nr. 11 Nds.SOG meint nicht etwa potenzielle Tatbeteiligte, sondern jede Person, "die mit einer anderen Person, von der Tatsachen die Annahme rechtfertigen, dass diese eine Straftat von erheblicher Bedeutung begehen wird, in einer Weise in Verbindung steht, die erwarten lässt, dass durch sie Hinweise über die angenommene Straftat gewonnen werden können". Zu der Unsicherheit, wer als potenzieller Straftäter in Betracht kommt, tritt des Weiteren also die Unklarheit, wer mit ihm schon im Vorfeld künftiger Straftaten so in Verbindung steht, dass Hinweise über die angenommene Straftat gewonnen werden können. 137

Eine restriktive Auslegung des Begriffs der Kontakt- und Begleitperson vermag dieses Bestimmtheitsdefizit im Bereich der Vorfeldaktivitäten nicht hinreichend zu beseitigen. Zwar gibt es Versuche, den Begriff durch eine nähere Qualifizierung des Kontakts zwischen dem Straftäter und der anderen Person zu konkretisieren. So wird etwa gefordert, dass entweder nähere persönliche oder geschäftliche Beziehungen zu der eigentlichen Zielperson bestehen müssen oder der Kontakt über einen längeren Zeitraum unterhalten oder aber unter konspirativen Umständen hergestellt oder gepflegt wird, während äußerlich flüchtige oder zufällige Alltagskontakte nicht ausreichen sollen (vgl. Verfassungsgerichtshof des Freistaates Sachsen, LKV 1996, S. 273 <284> zu § 39 Abs. 1 Nr. 3 SächsPolG). Geht es um die Anknüpfung an zukünftiges Verhalten eines nur potenziellen Straftäters, fällt es allerdings schwer, derartige Kontakte auf bestimmte Straftaten zu beziehen. Im Übrigen ist es in rechtsstaatlicher Hinsicht bedenklich, im Wesentlichen darauf zu vertrauen, dass eine unbestimmte Eingriffsermächtigung durch Auslegung seitens der Behörde, deren Verhalten gerade beschränkt werden soll, in gebotener Weise eingeengt wird. Hier muss der Gesetzgeber selbst Verantwortung übernehmen, der ausweislich der Gesetzesbegründung (vgl. LTDrucks 15/240, S. 18) konkretisierende Einengungen aber gerade nicht beabsichtigt hat. Vielmehr soll die Erhebung von Daten schon dann in Betracht kommen, wenn diese "von Relevanz für den Kontakt und demnach für die Verhinderung der betreffenden Straftaten sind". 138

Das Bestimmtheitsdefizit wird auch nicht durch die Anforderungen in § 33a Abs. 1 Nr. 3 Nds.SOG behoben, dass die Datenerhebung bei der Kontakt- und Begleitperson zur Vorsorge für die Verfolgung oder zur Verhütung einer Straftat "unerlässlich" sein muss. Es fehlt ein handhabbarer Maßstab für die Prüfung, ob eine Überwachungsmaßnahme zur 139

Vorsorge für die Verfolgung oder die Verhütung einer Straftat eines anderen unerlässlich ist, wenn es sich um ein Verhalten im Vorfeld der Begehung einer künftigen Straftat handelt und damit regelmäßig noch nicht absehbar ist, ob bei späteren Maßnahmen der Verhütung oder Verfolgung andere hinreichende Aufklärungsmöglichkeiten bestehen werden.

(3) Das Erfordernis einer richterlichen Anordnung der Überwachungsmaßnahme nach § 33a Abs. 3 Nds.SOG gleicht 140 die Bestimmtheitsdefizite nicht aus. Grundsätzlich können zwar ausfüllungsbedürftige materielle Normen rechtsstaatlich eher tragbar sein, wenn durch ein formalisiertes, gerichtlich kontrolliertes Verfahren dafür gesorgt wird, dass die wesentlichen Entscheidungsfaktoren geprüft und auslegungsbedürftige Rechtsbegriffe angemessen angewandt werden (vgl. BVerfGE 110, 33 <67 f.>). Das aber setzt voraus, dass der Richter Anhaltspunkte im Gesetz vorfindet. Die vorliegend angegriffenen Normen bieten dem Richter ebenso wenig einen Maßstab für die Prognoseentscheidung wie der Polizei selbst. Seine Prüfung des behördlichen Antrags trägt ohne tatbestandliche Konkretisierung die Unwägbarkeiten der Vorfeldermittlung in gleicher Weise wie die Behördenentscheidung in sich.

b) Die Ermächtigung zur Überwachung der Telekommunikation zwecks Vorsorge für die Verfolgung und die Verhütung 141 der in Bezug genommenen Straftaten genügt darüber hinaus auch nicht den Anforderungen der Verhältnismäßigkeit im engeren Sinne.

aa) Einbußen an grundrechtlich geschützter Freiheit dürfen nicht in unangemessenem Verhältnis zu den Zwecken 142 stehen, denen die Grundrechtsbeschränkung dient. Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person führen zwar dazu, dass der Einzelne Einschränkungen seiner Grundrechte hinzunehmen hat, wenn überwiegende Allgemeininteressen dies rechtfertigen. Der Gesetzgeber muss aber zwischen Allgemein- und Individualinteressen einen angemessenen Ausgleich herstellen. Dabei spielt auf grundrechtlicher Seite eine Rolle, unter welchen Voraussetzungen welche und wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind. Maßgebend sind also insbesondere die Gestaltung der Einschreitschwellen, die Zahl der Betroffenen und die Intensität der Beeinträchtigungen. Im Bereich der Telekommunikationsüberwachung ist von Bedeutung, ob die Betroffenen als Personen anonym bleiben, welche Informationen erfasst werden können und welche Nachteile den Grundrechtsträgern aufgrund der Überwachungsmaßnahme drohen oder von ihnen nicht ohne Grund befürchtet werden. Auf Seiten der mit dem Eingriff verfolgten Zwecke ist das Gewicht der Ziele und Belange maßgeblich, denen die Telekommunikationsüberwachung dient. Es hängt unter anderem davon ab, wie bedeutsam die Rechtsgüter sind, die mit Hilfe der Maßnahme geschützt werden sollen, und wie wahrscheinlich der Eintritt einer Rechtsgutverletzung ist (vgl. BVerfGE 100, 313 <375 f.>).

bb) Die Überwachung der Telekommunikation auf der Grundlage des § 33a Abs. 1 Nr. 2 und 3 Nds.SOG ermöglicht 143 einen schwerwiegenden Eingriff in das Fernmeldegeheimnis.

(1) Nach § 33a Abs. 2 Nr. 1 bis 3 Nds.SOG können Kommunikationsinhalte, Verbindungsdaten und Standortkennung 144 Gegenstand der Datenerhebung sein. Ziel sämtlicher Maßnahmen ist die Erhebung auf konkrete Personen bezogener Daten. Diese lassen Einblicke insbesondere in das Kommunikationsverhalten, das soziale Umfeld sowie persönliche Angelegenheiten und Gewohnheiten zu. Zudem wird die Freiheit der Bürger mittelbar beeinträchtigt, weil die Furcht vor Überwachung unbefangene Telekommunikation verhindern kann.

Der Zugriff auf den Inhalt der Telekommunikation (§ 33a Abs. 2 Nr. 1 Nds.SOG) ermöglicht die Erfassung der 145 Gespräche. Erfasst werden die übermittelten Informationen, die ausgesprochenen Gedanken sowie die Art der Interaktionen am Telefon. Möglich wird der Zugriff auf Bilder und Zeichen sowie auf Inhalte, die aufgrund neuer Kommunikationsformen (vgl. LTDrucks 15/240, S. 18) wie etwa E-Mail über das Internet ausgetauscht werden. Die Erhebung der Verbindungsdaten der Telekommunikation (§ 33a Abs. 2 Nr. 2 Nds.SOG) und die Standortkennung (§ 33a Abs. 2 Nr. 3 Nds.SOG) betreffen zunächst zwar nur die technische Abwicklung des Telekommunikationsvorgangs. Der Eingriff wiegt aber ebenfalls schwer. Verbindungsdaten lassen erhebliche Rückschlüsse auf das Kommunikationsverhalten zu (vgl. BVerfGE 107, 299 <318 ff.>). Die Standortkennung eingeschalteter Mobilfunkendeinrichtungen kann zur Erstellung eines Bewegungsbildes führen, über das gegebenenfalls auf Gewohnheiten der betroffenen Personen oder auf Abweichungen hiervon geschlossen werden kann.

(2) Grundrechtlich bedeutsam ist ferner die große Streubreite der Eingriffe. Das Abhören und die Aufzeichnung der 146 Gesprächsinhalte und die Erhebung der Verbindungsdaten können eine große Zahl von Personen treffen. Erfasst sind nicht nur die potenziellen Straftäter, sondern alle, mit denen diese in dem betreffenden Zeitraum Telekommunikationsverbindungen nutzen. Dazu können Personen gehören, die in keiner Beziehung zu einer möglicherweise zu verhütenden oder später zu verfolgenden Straftat stehen, wie etwa Kontakt- und Begleitpersonen (§ 33a Abs. 1 Nr. 3 Nds.SOG) oder gänzlich unbeteiligte Dritte (§ 33a Abs. 2 Satz 3 Nds.SOG).

(3) Zur Intensivierung des Eingriffs trägt außerdem bei, dass die Betroffenen den Überwachungsmaßnahmen in einer Situation vermeintlicher Vertraulichkeit ausgesetzt werden (vgl. BVerfGE 34, 238 <247>; 107, 299 <321>). Ahnungslosigkeit besteht insbesondere bei Kontakt- und Begleitpersonen oder sonstigen Dritten, von denen nicht angenommen wird, dass sie selbst die in Zukunft erwarteten Straftaten begehen werden. 147

Eingriffe dieser Art bergen darüber hinaus hohe Risiken für die Rechte der Betroffenen auch deshalb in sich, weil diese gegen die Maßnahmen frühestens dann mit rechtlichen Mitteln vorgehen können, wenn sie bereits vollzogen sind, und dies auch nur, wenn sie darüber informiert werden oder auf andere Weise Kenntnis erlangen (vgl. BVerfGE 107, 299 <321>). Bei Maßnahmen der Vorfeldermittlung ist aufgrund der Ungewissheit, ob und wann Straftaten begangen werden, regelmäßig mit einer längeren Zeitdauer bis zur Unterrichtung zu rechnen als bei sonstigen Überwachungsmaßnahmen. Dies wird durch die in § 30 Abs. 4 Satz 3 und Abs. 5 Nds.SOG enthaltenen großzügigen Regelungen über die Zurückstellung der Benachrichtigung verdeutlicht. Durch eine erst spät erfolgende Mitteilung wird auch die in Art. 19 Abs. 4 GG enthaltene Garantie effektiven Rechtsschutzes berührt. Kann gegen einen Eingriff nicht in angemessener Zeit Rechtsschutz begehrt und können seine Folgen dadurch gegebenenfalls nicht zügig beseitigt werden, erhöht dies zusätzlich die Schwere der Grundrechtsbeeinträchtigung. 148

(4) Die Eingriffsschwere wird noch weiter durch die Möglichkeit der Behörden verstärkt, die erhobenen Daten - wie in § 38 Abs. 1 Satz 2 Nds.SOG vorgesehen - allgemein zu Zwecken der Gefahrenabwehr und nach § 39 Nds.SOG zu weiteren Zwecken zu speichern, zu verändern oder zu nutzen. Die Verwertung in anderen Zusammenhängen ist ein eigenständiger Eingriff (vgl. BVerfGE 110, 33 <68 f.>). 149

Die Datenerhebung im Vorfeld der Begehung von Straftaten kann wegen der fehlenden Begrenzung auf eine konkret in der Verwirklichung begriffene oder schon begangene Straftat vielfältig nutzbare Informationen ergeben. Die Bindung an den Zweck, den das zur Kenntnisnahme ermächtigende Gesetz festgelegt hat (zum Grundsatz der Zweckbindung siehe BVerfGE 100, 313 <360 f.>), wird bei der weiteren Verwertung der erlangten Informationen praktisch kaum durchzuführen sein. Die Möglichkeit der Verwendung der erhobenen Daten zu unbestimmten oder noch nicht bestimmbar Zwecken erhöht damit die Schwere des Eingriffs schon in der Phase der Erhebung. 150

cc) Die vorgesehenen Eingriffe in das Grundrecht aus Art. 10 Abs. 1 GG sind nicht verhältnismäßig im engeren Sinne. Die durch die Polizei zu schützenden Gemeinwohlbelange sind nicht auf derart gewichtige begrenzt, dass sie solche schweren Eingriffe rechtfertigen können. 151

(1) Die Datenerhebung dient einem legitimen öffentlichen Zweck, nämlich der Verhütung und Verfolgung von Straftaten von erheblicher Bedeutung. Das Gewicht dieses Belangs ist insbesondere von dem durch die Norm geschützten Rechtsgut und der Intensität seiner Gefährdung abhängig. Dabei hat die der Sicherung des Rechtsfriedens dienende Verfolgung neben der Verhütung einer Straftat ein eigenständiges Gewicht (vgl. BVerfGE 107, 104 <118>). 152

Soweit eine Ermächtigung zur Telekommunikationsüberwachung der Verfolgung schon begangener Straftaten dient, muss sie sich auf eine hinreichende Tatsachenbasis, insbesondere einen konkreten Tatverdacht, und, soweit Dritte betroffen sind, hinreichend sichere tatsächliche Anhaltspunkte für deren Beziehung zu dem Tatverdächtigen gründen (so zum Nachrichtenmittler BVerfGE 107, 299 <321>). Die praktischen Möglichkeiten, solche Anhaltspunkte zu ermitteln, sind im Hinblick auf künftig lediglich erwartete Straftaten grundsätzlich schwächer. Leidet die Ermächtigung zudem - wie § 33a Abs. 1 Nr. 2 und 3 Nds.SOG - an dem Mangel hinreichender Normenbestimmtheit und Normenklarheit hinsichtlich der geforderten Tatsachenbasis (siehe oben C II 3 a), wirkt sich dies auch auf die Verhältnismäßigkeit im engeren Sinne aus (vgl. BVerfGE 110, 33 <55>). In solchen Fällen lassen sich das den Eingriff rechtfertigende Schutzgut und die Art seiner Gefährdung dem Gesetz nicht in einer Weise entnehmen, die eine nachvollziehbare Abwägung mit der Schwere des Eingriffs erlaubt. 153

Je ungenauer die Ziele einer Ermächtigung und die Anforderungen an die tatsächlichen Voraussetzungen einer Maßnahme gesetzlich umschrieben sind, umso größer ist das Risiko unangemessener Maßnahmen im Einzelfall. Da bei der Abwägung der Rang des Schutzguts und die Einschätzung der Intensität der ihm drohenden Gefahr bedeutsam sind, bedarf es hinreichender Anhaltspunkte für die genaue Bestimmung des gefährdeten Guts, aber auch hinreichender tatsächlicher Grundlagen für die Annahme einer dieses Schutzgut gefährdenden Handlung (vgl. BVerfGE 110, 33 <55>; siehe ferner BVerfGE 100, 313 <392>). Unklarheiten über das konkret gefährdete Rechtsgut und die dieses möglicherweise gefährdende Handlung bergen das Risiko in sich, dass die rechtsstaatliche Begrenzungsfunktion des Abwägungsgebots verfehlt wird. 154

Für die Strafverfolgung und die Gefahrenabwehr hat die Rechtsprechung Abwägungsgrundsätze entwickelt, die auch im Vorfeldbereich bedeutsam sind. Je gewichtiger das gefährdete Rechtsgut ist und je weitreichender es durch die 155

jeweiligen Handlungen beeinträchtigt würde oder beeinträchtigt worden ist, desto geringere Anforderungen dürfen an den Grad der Wahrscheinlichkeit gestellt werden, mit der auf eine drohende oder erfolgte Verletzung geschlossen werden kann, und desto weniger fundierend dürfen gegebenenfalls die Tatsachen sein, die auf die Gefährdung oder Verletzung des Rechtsguts schließen lassen (vgl. BVerfGE 100, 313 <392>; siehe auch BVerfGE 110, 33 <55, 60>). Allerdings muss stets gewährleistet bleiben, dass Annahmen und Schlussfolgerungen einen konkret umrissenen Ausgangspunkt im Tatsächlichen haben. Bei einem geringen Gewicht des gefährdeten Rechtsguts steigen die Anforderungen an die Prognosesicherheit sowohl hinsichtlich des Grads der Gefährdung als auch hinsichtlich ihrer Intensität.

Im Bereich der Vorfeldermittlung wird der Grad der Wahrscheinlichkeit der Rechtsgutverletzung aufgrund der fehlenden Nähe der bekannten Tatsachen zu einer konkreten Straftat regelmäßig geringer sein als bei Maßnahmen zur Gefahrenabwehr oder zur Verfolgung konkreter Straftaten. Knüpft das Gesetz nicht einmal an Planungs- oder sonstige Vorbereitungshandlungen an - wie in der früheren Regelung des § 39 Abs. 2 AWG oder jetzt in § 23a Abs. 2 und 3 ZFdG -, sondern begnügt es sich mit nicht näher eingegrenzten Tatsachen, die die Annahme einer künftigen Straftat rechtfertigen, steigen die Anforderungen an das Gewicht des Schutzguts und die Gefährlichkeit der erwarteten Verletzungshandlung weiter. Der schwere Eingriff in das Telekommunikationsgeheimnis kann bei einer derart weiten und offenen Umschreibung der Voraussetzungen der Vorsorge für die Verfolgung und der Verhütung künftiger Straftaten nur dann als angemessen bewertet werden, wenn der zu schützende Gemeinwohlbelang allgemein sowie im konkreten Fall überragend wichtig ist. 156

(2) Den Anforderungen an den Rang des geschützten Rechtsguts und an die tatsächlichen Anhaltspunkte seiner Gefährdung ist der Gesetzgeber nicht gerecht geworden. 157

(a) Das vom Gesetzgeber gewählte Tatbestandsmerkmal der "Straftaten von erheblicher Bedeutung" trägt den Anforderungen an das besondere Gewicht des zu verfolgenden Rechtsguts nicht Rechnung. Den in § 2 Nr. 10 Nds.SOG aufgeführten Straftaten ist schon kein auf die Besonderheiten der Telekommunikationsüberwachung im Vorfeld zugeschnittenes gesetzgeberisches Konzept zu entnehmen, das sich auf den Schutz besonders hochrangiger Rechtsgüter bezieht und beschränkt. Dieser Mangel setzt sich fort, soweit § 2 Nr. 10 Nds.SOG in Buchstabe b nicht näher aufgeführte Vergehen einbezieht, die nach dem geschützten Rechtsgut und der Strafandrohung den enumerativ aufgezählten Vergehen vergleichbar sind. 158

Der Grund für die nicht an den besonderen Anforderungen einer Telekommunikationsüberwachung orientierte Auswahl der Straftaten und für das Fehlen eines darauf bezogenen Konzepts erschließt sich bei Betrachtung der Entstehungsgeschichte der Vorschriften zur präventiven Telekommunikationsüberwachung. Die Bezugnahme auf die allgemeine Definition der "Straftaten von erheblicher Bedeutung" war in dem ursprünglichen Gesetzentwurf (LTDruks 15/240, S. 14) nicht enthalten, sondern erfolgte auf Empfehlung des Landtagsausschusses für Inneres und Sport (LTDruks 15/599, S. 9 f.). Dadurch wurde der im Niedersächsischen Gefahrenabwehrgesetz in der Fassung der Bekanntmachung vom 20. Februar 1998 (Nds.GVBl S. 101) enthaltene Katalog des § 2 Nr. 10 in Bezug genommen, der überall dort maßgebend ist, wo der Begriff der Straftaten von erheblicher Bedeutung im Polizeigesetz genutzt wird. Eine Begründung dafür, dass die angeführten Straftaten auch den besonderen Anforderungen einer Telekommunikationsüberwachung gerecht werden, lässt sich den Gesetzesmaterialien nicht entnehmen. Die fehlende Ausrichtung des Katalogs auf die Telekommunikationsüberwachung dürfte beispielsweise erklärlich machen, dass das Verbreiten oder das öffentliche Verwenden eines Kennzeichens einer verfassungswidrigen Organisation (§ 86a StGB) in dem Katalog enthalten ist, obwohl nicht erkennbar ist, inwieweit eine Telekommunikationsüberwachung ein erforderliches und angemessenes Mittel zur Verhütung oder Verfolgung dieser öffentlich begangenen Straftat sein kann. 159

Es ist ausgeschlossen, den in Bezug genommenen Straftatenkatalog einengend so auszulegen, dass nur Strafrechtsnormen zum Schutz überragend wichtiger Rechtsgüter als Anlass für eine Telekommunikationsüberwachung ausreichen. Das Defizit an Normenklarheit würde dadurch verschärft. Auch kann der Begriff der Straftaten von erheblicher Bedeutung nicht als ein zusätzliches, die Bezugnahme auf die Straftatbestände des Katalogs ergänzend beschränkendes Merkmal ausgelegt werden, etwa dahingehend, dass die Straftat nicht nur allgemein, sondern auch im konkreten Fall, etwa aufgrund des Grads der Bedrohung für die Allgemeinheit, besonderes Gewicht haben muss (dazu vgl. BVerfGE 107, 299 <322>). Dem Wortlaut des § 33a Abs. 1 Nr. 2 in Verbindung mit § 2 Nr. 10 Nds.SOG nach handelt es sich um einen Oberbegriff für die aufgezählten Straftaten, nicht aber um ein zusätzliches Tatbestandsmerkmal. Ebenfalls ist es ausgeschlossen, Einengungen mit Rücksicht darauf vorzunehmen, dass die Regelung im Zusammenhang mit der Bekämpfung der Organisierten Kriminalität und des Terrorismus geschaffen worden ist (vgl. LTDruks 15/240, S. 16; zur Problematik vgl. BVerfGE 109, 279 <338 ff.>). Dieses gesetzgeberische Ziel hat im Wortlaut der Ermächtigung oder in der Typik der aufgeführten Delikte keinen Ausdruck gefunden. 160

(b) § 33a Abs. 1 Nr. 2 und 3 Nds.SOG wird den Anforderungen an die nähere Umschreibung der für die Prognose und die Abwägung nutzbaren Tatsachen ebenfalls nicht gerecht. Die oben (C II 3 a) erfolgte Prüfung des Bestimmtheitsgebots hat ergeben, dass der Ermächtigung Einengungen hinsichtlich der Anhaltspunkte für die Begehung zukünftiger Straftaten, für die Intensität der Gefährdung oder für den Grad der Wahrscheinlichkeit eines auf eine Straftat hindeutenden Ablaufs nicht zu entnehmen sind. Auch wird kein Maßstab für die Abwägung im Einzelfall vorgegeben, ob die tatsächlichen Anhaltspunkte angesichts des Gewichts des gefährdeten Rechtsguts ausreichen. 161

(c) Die oben (C II 3 a cc <2>) sowohl im Hinblick auf den potenziellen Straftäter selbst als auch auf den Begriff der Kontakt- und Begleitperson aufgeführten Bestimmtheitsmängel wirken sich auch auf die Prüfung der Angemessenheit der Maßnahme nach § 33a Abs. 1 Nr. 3 Nds.SOG aus. Nicht normiert ist insbesondere, welcher Art die Hinweise sind, die durch die Kontakt- und Begleitperson über die Straftat gewonnen werden können, oder welche Anforderungen erfüllt sein müssen, damit eine an der künftigen Tat voraussichtlich unbeteiligte Person beim Telekommunikationsverkehr überwacht werden kann. Der Norm fehlen Anhaltspunkte für die abwägende Prüfung, ob die Schwere der zu erwartenden Straftat eine Telekommunikationsüberwachung dieses Personenkreises rechtfertigt. 162

(d) Die Mängel bei der Beachtung des Grundsatzes der Verhältnismäßigkeit im engeren Sinne werden nicht durch andere Regelungen des Gesetzes beseitigt. Sie werden vielmehr dadurch vertieft, dass auf die verfahrensgegenständliche Telekommunikationsüberwachung andere Normen des Gesetzes anwendbar sind, die in gleicher oder leicht veränderter Fassung auch schon vor der Schaffung der neuen Ermächtigung galten und nicht auf die Besonderheit der Überwachung im Vorfeldbereich abgestimmt sind. 163

Dies gilt beispielsweise für die schon erwähnte Möglichkeit der Polizei zur Zurückstellung der Unterrichtung des Betroffenen nach § 30 Abs. 4 und 5 Nds.SOG (siehe oben C II 3 b bb <3>). Infolge der Ausrichtung der Überwachung auf eine künftige Straftat kann die Zurückstellung lange dauern. Die Regelung, dass der Datenschutzbeauftragte in den Fällen des § 30 Abs. 5 Satz 1 Nr. 3 Nds.SOG informiert wird, wenn die Unterrichtung nach Ablauf von fünf Jahren nicht erfolgt ist (§ 30 Abs. 5 Satz 2 Nds.SOG), lässt erkennen, dass der Gesetzgeber mit der Möglichkeit längerer Zeiträume bis zur Benachrichtigung rechnet. Durch die Zurückstellung oder sogar das Unterbleiben der Unterrichtung wird die Möglichkeit nachträglichen Rechtsschutzes im Vergleich zu dem bei der Gefahrenabwehr und Strafverfolgung gewährten Rechtsschutz deutlich verringert, obwohl die Risiken einer Fehlprognose und damit einer tatsächlich nicht hinreichend fundierten Telekommunikationsüberwachung im Vorfeld von Straftaten größer sind als bei der Gefahrenabwehr und der Strafverfolgung (zu den Grundsätzen für die Unterrichtung vgl. BVerfGE 100, 313 <361 f.>; 109, 279 <363 f.>). 164

Die Gefährdung effektiven Rechtsschutzes und damit die Intensität des Eingriffs werden zudem dadurch verstärkt, dass die Unterrichtung nach § 30 Abs. 5 Satz 1 Nr. 1 Nds.SOG stets zurückgestellt werden kann, solange Zwecke der Verfolgung irgendeiner Straftat - also nicht der Straftat, auf deren Verhütung sich die Telekommunikationsüberwachung bezieht - oder irgendeiner Ordnungswidrigkeit entgegenstehen. Nach dem Wortlaut der Regelung muss die Straftat oder Ordnungswidrigkeit nicht einmal vom Betroffenen selbst begangen worden sein. Auch die in § 30 Abs. 5 Satz 1 Nr. 3 Nds.SOG enthaltenen Gründe für das Unterbleiben der Unterrichtung gefährden den effektiven Rechtsschutz. Nach dieser Norm unterbleibt die Unterrichtung, solange durch das Bekanntwerden der Datenerhebung Leib, Leben, Freiheit oder ähnliche schutzwürdige Belange einer Person oder die weitere Verwendung einer Vertrauensperson oder der weitere Einsatz einer Verdeckten Ermittlerin oder eines Verdeckten Ermittlers gefährdet werden. Die so umschriebene Zielsetzung rechtfertigt eine Zurückstellung der Benachrichtigung und damit die Verweigerung von Rechtsschutz nicht in jeder Hinsicht (vgl. dazu mit Bezug auf § 101 Abs. 1 StPO BVerfGE 109, 279 <366 f.>). 165

c) Die Ermächtigung zur Überwachung der Telekommunikation zwecks Vorsorge für die Verhütung und Verfolgung der in Bezug genommenen Straftaten lässt es ferner an hinreichenden Vorkehrungen dafür fehlen, dass Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung unterbleiben. 166

Es kann nicht ausgeschlossen werden, dass bei der Erfassung der Kommunikationsinhalte (§ 33a Abs. 2 Nr. 1 Nds.SOG) personenbezogene Daten betroffen sind, die sich auf den Kernbereich höchstpersönlicher Lebensgestaltung (zu ihm vgl. BVerfGE 109, 279 <311 ff.>) beziehen. Ob eine personenbezogene Kommunikation diesem Kernbereich zuzuordnen ist, hängt davon ab, in welcher Art und Intensität sie aus sich heraus die Sphäre anderer oder Belange der Gemeinschaft berührt (vgl. BVerfGE 80, 367 <374>; 109, 279 <314>). Nicht zu diesem Kernbereich gehören Kommunikationsinhalte, die in unmittelbarem Bezug zu konkreten strafbaren Handlungen stehen, wie etwa Angaben über die Planung bevorstehender oder Berichte über begangene Straftaten (vgl. BVerfGE 80, 367 <375>; 109, 279 <319>). 167

Art. 10 Abs. 1 GG gewährleistet die freie Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit 168

verborgenen Austausch von Kommunikation und schützt damit zugleich die Würde des Menschen (vgl. BVerfGE 67, 157 <171>; 110, 33 <53>). Der Schutz ist allerdings anders ausgestaltet als der des Grundrechts der Unverletzlichkeit der Wohnung nach Art. 13 GG. Aufgrund des besonders engen Bezugs dieses Grundrechts zur Menschenwürde gewährt Art. 13 GG einen absoluten Schutz des Verhaltens in den Wohnräumen, soweit es sich als individuelle Entfaltung im Kernbereich privater Lebensgestaltung darstellt (vgl. BVerfGE 109, 279 <313 f.>). Für sie benötigt jeder Mensch ein räumliches Substrat, in dem er für sich sein und sich nach selbst gesetzten Maßstäben frei entfalten, also die Wohnung bei Bedarf als "letztes Refugium" zur Wahrung seiner Menschenwürde nutzen kann (vgl. BVerfGE 109, 279 <314>).

Die Bürger sind zur höchstpersönlichen Kommunikation nicht in gleicher Weise auf Telekommunikation angewiesen wie auf eine Wohnung. Dementsprechend normiert Art. 10 Abs. 1 GG anders als Art. 13 GG keine spezifischen Eingriffsvoraussetzungen, sondern verweist nur implizit auf die allgemeinen rechtsstaatlichen Anforderungen. Die nach Art. 1 Abs. 1 GG stets garantierte Unantastbarkeit der Menschenwürde fordert auch im Gewährleistungsbereich des Art. 10 Abs. 1 GG Vorkehrungen zum Schutz individueller Entfaltung im Kernbereich privater Lebensgestaltung. Bestehen im konkreten Fall tatsächliche Anhaltspunkte für die Annahme, dass eine Telekommunikationsüberwachung Inhalte erfasst, die zu diesem Kernbereich zählen, ist sie nicht zu rechtfertigen und muss unterbleiben. 169

Da bei der Anordnung einer Telekommunikationsüberwachung oder bei ihrer Durchführung aber nicht sicher vorhersehbar ist, welchen Inhalt die Gespräche haben werden, ist das Risiko nicht auszuschließen, dass die Abhörmaßnahme Kommunikation aus dem Kernbereich privater Lebensgestaltung erfasst. Verfassungsrechtlich hinzunehmen ist dieses Risiko allenfalls bei einem besonders hohen Rang des gefährdeten Rechtsguts und einer durch konkrete Anhaltspunkte gekennzeichneten Lage, die auf einen unmittelbaren Bezug zur zukünftigen Begehung der Straftat schließen lässt. Hinzu müssen Vorkehrungen kommen, die sichern, dass die Kommunikationsinhalte des höchstpersönlichen Bereichs nicht gespeichert und verwertet werden dürfen, sondern unverzüglich gelöscht werden, wenn es ausnahmsweise zu ihrer Erhebung gekommen ist. An derartigen Regelungen aber fehlt es im Gesetz. 170

III.

Die Regelungen des § 33a Abs. 1 Nr. 2 und 3 Nds.SOG sind danach mit Art. 10 GG unvereinbar und nichtig. Hinreichende Möglichkeiten einer einengenden Auslegung zur Vermeidung des Verfassungsverstoßes bestehen nicht. Eine Rechtfertigung, die Normen auch nur teilweise weiterhin anzuwenden, ist nicht erkennbar. 171

Die Kostenentscheidung folgt aus § 34a Abs. 2 BVerfGG. 172