CyLaw-Report XIII

CyLaw-Report XIII: „Polizeirechtliche Telekommunikations-überwachung“

Entscheidung des BVerfG vom 27.07.2005 – 1 BvR 668/04

Das FÖR[1] an der Technischen Universität Darmstadt (Prof. Dr. Viola Schmid, LL.M. (Harvard)) ist verantwortlich für das SicAri-Teilprojekt[*] "Cyberlaw“[2]. Mit den CyLaw-Reports soll das rechtswissenschaftliche Diskursangebot L.O.S. (Legal Open Source), das bisher nur Rechtsquellen (SicAri-Cyberlaw) enthält, um Rechtsprechung ergänzt werden. Die CyLaw-Reports-Idee ist es, auch Nicht-Juristen an grundlegender und/oder aktueller Cyberlaw-Rechtsprechung und juristischer Methodik fokusssiert teilhaben zu lassen. Fragestellungen, die spezielles juristisches Wissen voraussetzen werden mit dem Kürzel „FEX“ (Für Experten) gekennzeichnet. Hintergrundwissen wird unter der Überschrift „FÖR-Glossar“ ergänzt. Aus Gründen der Präsentationsstrategie wird zwischen „clear cases“, die eine relativ einfache rechtliche Prüfung erfordern, und „hard cases“, die eine vertiefte Diskussion erfordern, unterschieden. In keinem Falle ist mit den CyLaw-Reports die Übernahme von Haftung verbunden.

Die Entscheidung des BVerfG wurde ausgewählt, weil sie zum einen formell die grundgesetzlichen Konturen einer landesrechtlichen Telekommunikationsüberwachung und zum anderen materiell den Schutz unbeobachteter Lebensgestaltung verdeutlicht.

[*] Die Arbeiten am CyLaw-Report werden im Rahmen des Projektes SicAri vom Bundesministerium für Bildung und Forschung gefördert.

Prof. Dr. Viola Schmid, LL.M. (Harvard) - **schmid@jus.tu-darmstadt.de**

CyLaw-Report XIII

Gliederung:

Prof. Dr. Viola Schmid, LL.M. (Harvard) - **schmid@jus.tu-darmstadt.de**

A. Polizeirechtliche Telekommunikationsüberwachung

I. Sachverhalt

Der Sachverhalt entspricht dem Urteil des Bundesverfassungsgerichts vom 27.07.2005.[3]

Bürger B lebt in Niedersachsen. Der niedersächsische Gesetzgeber führt Im Jahr 2003 eine neue Regelung in das Niedersächsische Gesetz über die öffentliche Sicherheit und Ordnung (Nds.SOG) ein, die eine polizeirechtliche Telekommunikationsüberwachung ermöglicht. Darüber ist Bürger B sehr besorgt. Er befürchtet, dass auch seine Telekommunikation abgehört werden könnte. Ausreichend für eine Abhörmaßnahme ist bereits der Verdacht, jemand werde in Zukunft eine Straftat begehen. B sieht daher die Gefahr, dass er schon aufgrund eines belanglosen Verhaltens verdächtigt und abgehört werden könnte. Auch Kontaktpersonen von Verdächtigen können abgehört werden. Da B viele Freunde und Bekannte hat, fürchtet er, für eine Vielzahl an Personen als Kontaktperson zu gelten. B meint, einen solchen Dauerverdacht nicht hinnehmen zu müssen. Er hält die Regelungen des § 33a Abs. 1 Nr. 2 und 3 Nds.SOG für verfassungswidrig, weil

- dem Land Niedersachsen keine Gesetzgebungskompetenz für solche Regelungen zugestanden habe,
- ein Verstoß gegen das Zitiergebot vorliege,
- die Regelungen nicht dem Bestimmtheitsgebot genügten,
- die Regelungen nicht verhältnismäßig seien und
- noch nicht einmal der Kernbereich höchstpersönlicher Lebensgestaltung geschützt sei.

II. Rechtsgrundlage

Rechtgrundlage für eine polizeirechtliche Telekommunikationsüberwachung, wie sie der B befürchtet, könnte entweder

- § 33a Abs. 1 Nr. 2 Nds.SOG sein, wenn B selbst verdächtig würde, eine Straftat begehen zu wollen, oder
- § 33a Abs. 1 Nr. 3 i.V.m.[4] Nr. 2 Nds.SOG, wenn B als Kontaktperson eines Dritten abgehört werden soll.

§ 33a Nds.SOG [Datenerhebung durch Überwachung der Telekommunikation]
(1) Die Polizei kann personenbezogene Daten durch Überwachung und Aufzeichnung der Telekommunikation erheben
1. zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person 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
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
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.
(2) Eine Datenerhebung nach Absatz 1 kann sich auf
1. die Inhalte der Telekommunikation einschließlich der innerhalb des Telekommunikationsnetzes in Datenspeichern abgelegten Inhalte,
2. die Telekommunikationsverbindungsdaten (§ 33 Abs. 1) oder
3. die Standortkennung einer aktiv geschalteten Mobilfunkendeinrichtung
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.
(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.
(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.
(…)

III. Verfassungsmäßigkeit der Rechtgrundlage

B fragt nach der Verfassungsmäßigkeit dieser Rechtsgrundlagen.

FEX: Verfassungsmäßigkeit eines Gesetzes

I. Formelle Verfassungsmäßigkeit
1. Gesetzgebungskompetenz
2. Verfahren
   z.B. Zustimmungs- oder Einspruchsgesetz
3. Form
   z.B. a) Art. 79 GG bei verfassungsändernden Gesetzen
   b) Art. 19 Abs. 1 S. 2 GG - Zitiergebot
   c) Art. 19 Abs. 1 S. 1 GG - Verbot des Einzelfallgesetzes

II. Materielle Verfassungsmäßigkeit
1. Vereinbarkeit mit den Grundprinzipien des Art. 20 GG
   Insbesondere mit dem Rechtsstaatsprinzip (Art. 20 Abs. 3 GG):
   a) Bestimmtheitsgrundsatz
   b) Vertrauensschutz, z.B. bei Rückwirkung des Gesetzes
2. Vereinbarkeit mit den Grundrechten

1. Formelle Verfassungsmäßigkeit

§ 33a Abs. 1 Nr. 2 und Nr. 3 Nds.SOG müssten formell verfassungsmäßig sein. Hier werden nur die Argumentationen geprüft, auf die auch das BVerfG eingegangen ist.

a. Gesetzgebungskompetenz

Das Land Niedersachsen müsste für die geregelte Materie die Gesetzgebungskompetenz haben. Die Länder haben die Gesetzgebungskompetenz immer dann, wenn nicht das Grundgesetz dem Bund die Gesetzgebungsbefugnis verleiht (Art. 70 Abs. 1 GG).

Art. 70 GG [Gesetzgebung des Bundes und der Länder]
(1) Die Länder haben das Recht der Gesetzgebung, soweit dieses Grundgesetz nicht dem Bunde Gesetzgebungsbefugnisse verleiht.
(…)

aa) Kompetenz für die Verhütung von Straftaten

Polizeirechtliche Regelungen liegen grundsätzlich in der Gesetzgebungszuständigkeit der Länder. Polizeirechtliche Regelungen dienen zunächst der **präventiven Gefahrenabwehr** und hierfür haben die Länder die Gesetzgebungskompetenz, da dieser Bereich nicht dem Bund zugewiesen ist. § 33a Abs. 1 Nr. 2 und Nr. 3 Nds.SOG dienen der Verhütung von Straftaten, wie sich aus dem Wortlaut der Normen ergibt. Das Land Niedersachsen hatte daher die erforderliche Gesetzgebungskompetenz – soweit es um die Verhütung von Straftaten geht.

BVerfG:
„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.“[5]

bb) Kompetenz für die Verfolgung von Straftaten

Nach dem Wortlaut der Normen (§ 33a Abs. 1 Nr. 2 und 3 Nds.SOG) sollen diese aber auch zur **„Vorsorge für die Verfolgung von Straftaten“** dienen. Diese Aufgabenzuweisung im **repressiven Bereich** ist nach Ansicht des BVerfG kompetenzrechtlich als eigenständige Aufgabenzuweisung anzusehen.

BVerfG:
„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.“[6]

Die Vorsorge für die Verfolgung von Straftaten könnte inhaltlich zum gerichtlichen Verfahren (Art. 74 Abs. 1 Nr. 1 GG) gehören und somit Gegenstand der konkurrierenden Gesetzgebung (Art. 74 GG) sein.

Art. 74 GG [Gegenstände der konkurrierenden Gesetzgebung]
(1) Die konkurrierende Gesetzgebung erstreckt sich auf folgende Gebiete:
1. das bürgerliche Recht, das Strafrecht und den Strafvollzug, die Gerichtsverfassung, **das gerichtliche Verfahren**, die Rechtsanwaltschaft, das Notariat und die Rechtsberatung;
(…)

Die Vorsorge für die Verfolgung noch gar nicht begangener Straftaten gehört nach Auffassung des BVerfG zum gerichtlichen Verfahren. Inhaltlich geht es nicht mehr um Gefahrenabwehr, sondern um die Sicherung von Beweisen für ein künftiges Strafverfahren.

BVerfG:
„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 - 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.“[7]

Im Rahmen der konkurrierenden Gesetzgebung haben die Länder nur dann die Gesetzgebungskompetenz, wenn nicht der Bundesgesetzgeber von seiner Kompetenz Gebrauch gemacht hat (Art. 72 Abs. 1 GG).

Art. 72 GG [Konkurrierende Gesetzgebung]
(1) Im Bereich der konkurrierenden Gesetzgebung haben die Länder die Befugnis zur Gesetzgebung, solange und soweit der Bund von seiner Gesetzgebungszuständigkeit nicht durch Gesetz Gebrauch gemacht hat.
(…)

Hat der Bundesgesetzgeber eine Materie umfassend und aus seiner Sicht abschließend geregelt, steht den Landesgesetzgebern keine Gesetzgebungskompetenz für diesen Bereich mehr zu (Sperrwirkung). Vorliegend hat der Bundesgesetzgeber mit

den Vorschriften zur Telekommunikationsüberwachung in der Strafprozessordnung eine gesetzliche Regelung getroffen.

BVerfG:
„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").“[8]

Daneben ist nach Ansicht des BVerfG für eine polizeirechtliche Telekommunikationsüberwachung der Länder kein Raum. Dafür sprechen nach Auffassung des BVerfG folgende Argumente:

- Der Bundesgesetzgeber hat sich bewusst gegen eine Ermächtigung zu Telekommunikationsüberwachungsmaßnahmen im Vorfeldbereich entschieden.

  BVerfG:
  „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.“[9]

- Zwischen den bundesrechtlichen Regelungen der StPO und den landesgesetzlichen Regelungen im Nds.SOG bestehen starke Widersprüche.

  BVerfG:
  „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 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."[10]

- Die parallele Anwendbarkeit dieser beiden Regelungssysteme würde zu Unklarheiten führen, da die Behörden auf beide – einander widersprechende – Regelungen zurückgreifen könnten.

BVerfG:
„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. 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."[11]

Somit hatte das Land Niedersachsen nach Auffassung des BVerfG teilweise – nämlich soweit es um die **Vorsorge zur Verfolgung von Straftaten** geht – keine Gesetzgebungskompetenz. **§ 33a Abs. 1 Nr. 2 und 3 Nds.SOG sind insoweit nichtig**.

b. Zitiergebot

Im Übrigen – also im Bereich der präventiven Gefahrenabwehr – könnte der niedersächsische Gesetzgeber gegen das Zitiergebot (Art. 19 Abs. 1 S. 2 GG) verstoßen haben.

Art. 19 GG [Einschränkung von Grundrechten]
(1) Soweit nach diesem Grundgesetz ein Grundrecht durch Gesetz oder auf Grund eines Gesetzes eingeschränkt werden kann, muss das Gesetz allgemein und nicht nur für den Einzelfall gelten. **Außerdem muss das Gesetz das Grundrecht unter Angabe des Artikels nennen.**
(…)

aa) Geltungsbereich des Zitiergebots

Es müsste eine Grundrechtsbeschränkung vorliegen (Art. 19 Abs. 1 S. 2 GG). Die Überwachung der Telekommunikation stellt einen Eingriff in das Fernmeldegeheimnis dar (Art. 10 Abs. 1 GG).

Art. 10 GG [Brief-, Post- und Fernmeldegeheimnis]
(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.
(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. (…)

Der Geltungsbereich des Fernmeldegeheimnisses umfasst sowohl den Kommunikationsinhalt als auch die Kommunikationsumstände.

BVerfG:
„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. In den Schutzbereich fällt auch die Erlangung der Kenntnis, ob, wann, wie oft und zwischen welchen Personen Telekommunikation stattgefunden hat oder versucht worden ist). Die freie Kommunikation, die Art. 10 GG sichert, leidet, wenn zu befürchten ist, dass der Staat entsprechende Kenntnisse verwertet. 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.“[12]

Die in § 33a Nds.SOG geregelte Telekommunikationsüberwachung kann sich auf die Kommunikationsinhalte und auf die Kommunikationsumstände beziehen (§ 33a Abs. 2 Nds.SOG).

§ 33a Nds.SOG [Datenerhebung durch Überwachung der Telekommunikation]
(2) Eine Datenerhebung nach Absatz 1 kann sich auf
1. die **Inhalte der Telekommunikation** einschließlich der innerhalb des Telekommunikationsnetzes in Datenspeichern abgelegten Inhalte,
2. die **Telekommunikationsverbindungsdaten** (§ 33 Abs. 1) oder
3. die Standortkennung einer aktiv geschalteten Mobilfunkendeinrichtung

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.

Art. 10 Abs. 1 GG wird somit durch § 33a Abs. 1 Nr. 2 und Nr. 3 Nds.SOG eingeschränkt. Der niedersächsische Gesetzgeber musste das Zitiergebot beachten.

BVerfG:
„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, also auch auf das Fernmeldegeheimnis.“[13]

bb) Ausnahme vom Zitiergebot

Das Gesetz, das die Regelungen des § 33a Abs.1 Nr. 2 und Nr. 3 Nds.SOG einführte, benennt Art. 10 Abs. 1 GG als eingeschränktes Grundrecht nicht. Allerdings enthielt das niedersächsische Gefahrenabwehrgesetz als Vorgängerregelung des Nds.SOG einen Hinweis auf die Einschränkung des Fernmeldegeheimnisses, der auch nach der Einführung von § 33a Abs. 1 Nr. 2 und Nr. 3 Nds.SOG fortgalt. Dadurch könnte eine nochmalige Nennung der eingeschränkten Grundrechte entbehrlich sein. Durch einen solchen Verzicht auf das Zitiergebot würde aber nach Auffassung des BVerfG dessen Funktion nicht erfüllt werden. Das Zitiergebot hat eine Warn- und Besinnungsfunktion. Dem Gesetzgeber soll dadurch vor Augen geführt werden, dass er mit der angestrebten Regelung in Grundrechte eingreift und er soll sich die Auswirkungen der Norm auf die eingeschränkten Grundrechte verdeutlichen.

BVerfG:
„Das Zitiergebot erfüllt eine Warn- und Besinnungsfunktion. 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. Die ausdrückliche Benennung erleichert es auch, die Notwendigkeit und das Ausmaß des beabsichtigten Grundrechtseingriffs in öffentlicher Debatte zu klären.“[14]

Dies gilt nach dem BVerfG zumindest dann, wenn - wie dies hier der Fall war - die neue Eingriffsgrundlage wesentlich weitere Befugnisse enthält als die Vorgängernorm.

BVerfG:
„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.“[15]

Nach Ansicht des BVerfG wurde somit das Zitiergebot nicht beachtet.

c. Ergebnis

Damit verstoßen § 33a Abs. 1 Nr. 2 und Nr. 3 Nds.SOG nach Ansicht des BVerfG gegen das Zitiergebot. Mit dem BVerfG wird weiter auch die materielle Verfassungsmäßigkeit geprüft.[16]

2. Materielle Verfassungsmäßigkeit

a. Bestimmtheitsgrundsatz

§ 33a Abs. 1 Nr. 2 und Nr. 3 Nds.SOG müssten dem rechtsstaatlichen Gebot der Normenbestimmtheit und der Normenklarheit gerecht werden. Der Bestimmtheitsgrundsatz dient mehreren Zielen:

- Zum einen soll sich der Normadressat auf mögliche belastende Maßnahmen einstellen und sein Verhalten danach ausrichten können.
- Zum anderen soll die Verwaltung bei der Ausführung der Gesetze steuernde und begrenzende Handlungsmaßstäbe vorfinden.
- Schließlich soll den Gerichten die rechtliche Kontrolle der Verwaltung ermöglicht werden.

Gesetzliche Regelungen müssen daher in ihren Voraussetzungen und ihren Rechtsfolgen mindestens so klar und bestimmt sein, dass sich ihre Bedeutung dem Normadressaten erschließt.

BVerfG:
„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 Voraussetzunge 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.“[17]

Bei der präventiven Telekommunikationsüberwachung geht es um die Verhinderung von zukünftigen Straftaten. Ein Einschreiten findet daher hauptsächlich auf der Basis von Prognosen darüber statt, was in Zukunft vermutlich oder wahrscheinlich geschehen wird. Für derartige Prognoseentscheidungen stellt der Bestimmtheitsgrundsatz nach Ansicht des BVerfG große Herausforderungen:

BVerfG:
„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. 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. Die Situation der Vorfeldermittlung ist insofern durch eine hohe Ambivalenz der potentiellen 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.“[18]

Diesen Herausforderungen genügt der Gesetzgeber der präventiven Telekommunikationsüberwachung nur, wenn er den besonders strikten Voraussetzungen der repressiven Strafverfolgung genügt.

BVerfG:
„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.“[19]

Diese BVerfG-Rechtsprechung zu einer strikten Anwendung des Bestimmtheitsgrundsatzes stimmt mit der Anforderung an die „konkrete Gefahr“ bei der Rasterfahndung überein (vergleiche CyLaw Report XII).

Zu prüfen ist, ob § 33a Abs. 1 Nr. 2 und Nr. 3 Nds.SOG diesem strikten Bestimmtheitsgrundsatz genügen.

- Der Begriff **„Tatsachen“** in § 33a Abs. 1 Nr. 2 Nds.SOG könnte nach diesen Maßstäben nicht ausreichend bestimmt sein.

  Im Sinne des B wurde argumentiert:
  „[Es] würden keine einschränkenden 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.“ [20]

  Der Begriff „Tatsache“ allein ist nach Auffassung des BverfG hinreichend bestimmt:

  BVerfG:
  „Der in § 33a Abs. 1 Nr. 2 Nds.SOG verwendete Begriff der "Tatsache" ist isoliert betrachtet allerdings hinreichend bestimmt. Er nimmt eine Abgrenzung zu bloßen Vermutungen und allgemeinen Erfahrungssätzen vor, die für sich allein gerade nicht ausreichen sollen.“[21]

- Die Anforderung von **„Tatsachen, die die Annahme rechtfertigen, dass sie [die zu überwachenden Personen] Straftaten von erheblicher Bedeutung begehen werden“** (§ 33a Abs. 1 Nr. 2 Nds.SOG) qualifiziert das BVerfG aber als zu unbestimmt. Es ist eine Vielzahl von Anknüpfungen denkbar, die hypothetisch in einer Straftatbegehung enden könnten. Der Gesetzgeber hätte hier nach An-

sicht des BVerfG eine nähere Eingrenzung und Beschreibung treffen müssen, um ein Mindestmaß an Klarheit, Vorhersehbarkeit und Berechenbarkeit zu erreichen:

> **BVerfG:**
> „Weder hinsichtlich möglicher Indikatoren und des Grades an 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 Straftatbegehung mündenden Verhaltens werden in der Ermächtigung nicht durch einschränkende Tatbestandmerkmale 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.“[22]

- Der Begriff **„Straftat von erheblicher Bedeutung“** (§ 33a Abs. 1 Nr. 2 Nds.SOG) könnte ebenfalls zu unbestimmt sein. Der Begriff ist in § 2 Nr. 10 Nds.SOG legal definiert.

> **§ 2 Nds.SOG [Begriffsbestimmungen]**
> Im Sinne dieses Gesetzes ist
> (…)
> 10. Straftat von erheblicher Bedeutung:
> a) ein Verbrechen, mit Ausnahme einer Straftat nach den §§ 154 und 155 des Strafgesetzbuches,
> b) ein Vergehen nach den §§ 85, 86, 86a, 87 bis 89, 98, 99, 129, 130, 174, 174a, 174b und 176 des Strafgesetzbuches, ein in § 138 Abs. 1 des Strafgesetzbuches genanntes Vergehen und ein nach dem geschützten Rechtsgut und der Strafandrohung vergleichbares Vergehen,
> c) ein banden- oder gewerbsmäßig begangenes Vergehen,
> d) die Teilnahme an einer solchen Straftat;
> (…)

Soweit dort bestimmte Straftatbestände aufgezählt werden, ist dies hinreichend bestimmt. Allerdings werden auch „nach dem geschützten Rechtsgut und der Strafandrohung vergleichbare Vergehen“ als Straftaten von erheblicher Bedeutung definiert. Hier fehlt es nach Ansicht des BVerfG an der Wahrung des Bestimmtheitsgrundsatzes.

BVerfG:
„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.“[23]

Der Begriff „Straftat von erheblicher Bedeutung“ ist nach Auffassung des BVerfG nicht hineichend bestimmt.

- Der Begriff der **„Kontakt- oder Begleitperson“** (§ 33a Abs. 1 Nr. 3 Nds.SOG) könnte zu unbestimmt sein. Der Begriff wird durch § 2 Nr. 11 Nds.SOG definiert:

§ 2 Nds.SOG [Begriffsbestimmungen]
Im Sinne dieses Gesetzes ist
(…)
11. Kontakt- oder Begleitperson:
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.

Nach Auffassung des BVerfG ist der Begriff der „Kontakt- oder Begleitpersonperson“ zu unbestimmt. Dies ergibt sich zum einen daraus,

- dass der Personenkreis, dessen Kontakt- und Begleitpersonen überwacht werden können, bereits nicht hinreichend bestimmt ist (wie soeben dargestellt). Zum anderen
- grenzt der Begriff der „Kontakt- und Begleitperson“ selbst den zu überwachenden Personenkreis nach Auffassung des BVerfG nicht ausreichend ein.

BVerfG:
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. 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. 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 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".[24]

Die Grenzziehung zwischen bedeutungslosem Alltagskontakt und telekommunikationsüberwachungsrechtlich relevantem Kontakt ist nach Ansicht des BVerfG Aufgabe des Gesetzgebers. Da sich aus der gesetzlichen Definition keinerlei Anhaltspunkte für die Abgrenzung von bedeutungslosem und bedeutsamem Kontakt ergeben, ist der Begriff „Kontakt- und Begleitperson“ zu unbestimmt.

- Auch der Begriff **„zur Vorsorge für die Verfolgung oder zur Verhütung einer Straftat […] unerlässlich“** genügt nach Ansicht des BVerfG dem Bestimmtheitsgrundsatz nicht.

> **BVerfG:**
> „Es fehlt ein handhabbarer Maßstab für die Prüfung, ob eine Überwachungsmaßnahme zur 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.“[25]

§ 33a Abs. 1 Nr. 2 und 3 Nds.SOG verstoßen nach Ansicht des BVerfG gegen den Bestimmtheitsgrundsatz. Daran ändert nach Ansicht des BVerfG auch das Erfordernis einer richterlichen Anordnung nichts – denn auch der anordnende Richter muss im Gesetz Anhaltspunkte für seine Entscheidung vorfinden:

> **BVerfG:**
> „Das Erfordernis einer richterlichen Anordnung der Überwachungsmaßnahme nach § 33a Abs. 3 Nds.SOG gleicht 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. 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."[26]

Auch wenn sich aus dem Verstoß gegen das Bestimmtheitsgebot bereits die Verfassungswidrigkeit der Norm ergibt, wird hier im Einklang mit dem BVerfG auch noch die Vereinbarkeit der Regelung mit den Grundrechten geprüft. Dabei ist die Ermächtigung zur Telekommunikationsüberwachung insbesondere auf

- die Vereinbarkeit mit dem Fernmeldegeheimnis (Art. 10 Abs. 1 GG) und
- die Vereinbarkeit mit der Menschenwürde (Art. 1 Abs.1 GG)

zu prüfen.

b. Vereinbarkeit mit dem Fernmeldegeheimnis

aa) Recht

Die Überwachung der Telekommunikation unterfällt dem Geltungsbereich des Fernemeldegeheimnisses (Art. 10 Abs. 1 GG).

Art. 10 GG [Brief-, Post- und Fernmeldegeheimnis]
(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.
(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

Geschützt werden sowohl Kommunikationsinhalt wie Kommunikationsumstände (siehe oben unter A III 1 b aa).

Soweit auch das Recht auf informationelle Selbstbestimmung aus Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG betroffen ist, überschneiden sich die Geltungsbereiche der beiden Grundrechte: Da es vorliegend um Telekommunikationsüberwachung geht, ist das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG nach vom BVerfG vertretener Auffassung die speziellere Regelung. Das Recht auf informationelle Selbstbestimmung tritt dahinter zurück.

BVerfG:
„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. 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."[27]

bb) Eingriff

Eine gesetzliche Regelung, die eine Überwachung von Telekommunikationsinhalten und Kommunikationsumständen ermöglicht, greift in das Fernmeldegeheimnis ein.

BVerfG:
„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. 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."[28]

Weitere Eingriffe in das Fernmeldegeheimnis können sich nach Auffassung des BVerfG daraus ergeben, dass die erhobenen Daten zu weiteren Zwecken verarbeitet und gespeichert werden können (§§ 38 f.Nds.SOG).

§ 38 Nds.SOG [Speicherung, Veränderung und Nutzung personenbezogener Daten, Zweckbindung]
(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.
(…)

§ 39 Nds.SOG [Speicherung, Veränderung und Nutzung personenbezogener Daten zu anderen Zwecken]
(1) Die Speicherung, Veränderung oder Nutzung von personenbezogenen Daten zu anderen als den in § 38 Abs. 1 genannten Zwecken ist nur zulässig, wenn
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,(…)
(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.
(…)

cc) Rechtfertigung

Die in das Fernmeldegeheimnis eingreifende Regelung müsste verhältnismäßig sein.

Geeignetheit	Eingriff muss geeignet sein, um den Schutz des Rechtsguts, das die Eingriffsrechtfertigung bildet (Rechtfertigungsrechtsgut) zu bewirken – Tauglichkeit des Mittels für den Zweck.
Erforderlichkeit	Es darf keine Maßnahme geben, die für den Schutz des Rechtfertigungsrechtsguts genauso geeignet und weniger eingreifend ist.
Verhältnismäßigkeit im engeren Sinne	Die Schwere des Eingriffs in das Eingriffsrechtsgut darf nicht außer Verhältnis zur Qualität des Schutzes des Rechtfertigungsrechtsguts stehen – Grundrechtseingriff darf in seiner Intensität nicht außer Verhältnis zum angestrebten Ziel stehen.

(1) Geeignetheit

Die Reglung könnte als geeignet angesehen werden. Eine Telekommunikationsüberwachung kann zu Erkenntnissen über bevorstehende Straftaten führen und so Straftaten verhindern.

(2) Erforderlichkeit

Die Regelung könnte auch als erforderlich angesehen werden. Nach dem Tatbestand der Normen ist Voraussetzung, dass die Datenorganisation[29] auf andere Weise nicht möglich erscheint (§ 33 a Abs. 1 Nr. 2 Nds.SOG „nicht möglich erscheint“ und § 33 a Abs. 1 Nr. 3 Nds.SOG „unerlässlich). Es ist demzufolge keine weniger einschneidende Maßnahme ersichtlich, die der Polizei derart genaue Informationen vom Verdächtigen selbst oder aus seinem direkten Umfeld vermitteln kann.

(3) Verhältnismäßigkeit im engeren Sinne

Die gesetzliche Reglung muss verhältnismäßig im engeren Sinne sein:

BVerfG:
„Einbußen an grundrechtlich geschützter Freiheit dürfen nicht in unangemessenem Verhältnis zu den Zwecken 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 Rechtsgutsverletzung ist.“[30]

Danach sind insbesondere die folgenden Argumente gegeneinander abzuwägen und in einen angemessenen Ausgleich zu bringen:

- **Intensität des Grundrechtseingriffs (Eingriffsrechtsgut), die durch die Schwere (Qualität und Quantität) wie die Unbestimmtheit charakterisiert wird und die**

➢ **Qualität der Förderung des Rechtfertigungsrechtsguts, die durch die Bedeutung und die Wahrscheinlichkeit der Gefährdung des Rechtsguts charakterisiert wird.**

Danach ergibt sich für die polizeirechtliche Telekommunikationsüberwachung, wie sie § 33a Abs. 1 Nr. 2 und Nr. 3 Nds.SOG vorsieht, folgendes Bild:

➢ **Qualität des Grundrechtseingriffs**

Die Überwachung der Telekommunikation stellt einen schwerwiegenden Eingriff in das Fernmeldegeheimnis dar. Die Telekommunikationsüberwachung erfasst eine Vielzahl von Daten, da Kommunikationsinhalte, Verbindungsdaten und Standortkennung Gegenstand der Überwachungsmaßnahme sein können.

BVerfG:
„Der Zugriff auf den Inhalt der Telekommunikation (§ 33a Abs. 2 Nr. 1 Nds.SOG) ermöglicht die Erfassung der 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 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. 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.“[31]

Die Eingriffsintensität wird nach Ansicht des BVerfG dadurch erhöht, dass die Betroffenen in einer Situation vermeintlicher Vertraulichkeit überwacht werden.

BVerfG:
„Zur Intensivierung des Eingriffs trägt außerdem bei, dass die Betroffenen den Überwachungsmaßnahmen in einer Situation vermeintlicher Vertraulichkeit ausgesetzt werden. 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.“[32]

Das Nds.SOG ermöglicht außerdem, dass die im Rahmen der Telekommunikationsüberwachung erhobenen Daten auch noch zu anderen Zwecken verarbeitet und übermittelt werden können.

BVerfG:
„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. 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, wird bei der weiteren Verwertung der erlangten Informationen praktisch kaum durchzuführen sein. Die Möglichkeit der Verwendung der erhobenen Daten zu unbestimmten oder noch nicht bestimmbaren Zwecken erhöht damit die Schwere des Eingriffs schon in der Phase der Erhebung.“[33]

Ein weiteres Argument für die Schwere des Eingriffs ist, dass die rechtliche Kontrolle nur bei Benachrichtigung der Betroffenen und stets nur im Nachhinein möglich ist.

BVerfG:
„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. 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.“[34]

- **Quantität der Grundrechtseingriffe**

Eine Telekommunikationsüberwachungsmaßnahme betrifft eine Vielzahl von Personen. Die Streubreite der Maßnahme ist sehr groß, insbesondere können auch unbeteiligte Dritte von der Maßnahme betroffen sein.

BVerfG:
„Grundrechtlich bedeutsam ist ferner die große Streubreite der Eingriffe. Das Abhören und die Aufzeichnung der 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).“[35]

- **Unbestimmtheit des Grundrechtseingriffs**

Die einzelnen tatbestandlichen Voraussetzungen für die Durchführung einer Überwachungsmaßnahme sind nicht ausreichend klar eingegrenzt. Dies wirkt sich nach Auffassung des BVerfG auch im Rahmen der Verhältnismäßigkeitsprüfung aus.

BVerfG:
„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. 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, wirkt sich dies auch auf die Verhältnismäßigkeit im engeren Sinne aus. 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.“[36]

Die Argumente zur Schwere des Grundrechtseingriffs sind mit den Argumenten zur Qualität der Förderung des Rechtfertigungsrechtsguts abzuwägen.

- **Qualität des Rechtfertigungsrechtsguts**

Die Verhütung von Straftaten ist ein legitimer öffentlicher Zweck, dessen Gewicht von der Intensität der Gefahr und vom bedrohten Rechtsgut abhängt.

BVerfG:
„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.“[37]

Je weiter im Vorfeld ermittelt wird, desto geringer ist regelmäßig die Wahrscheinlichkeit des Eintritts einer Rechtsgutsverletzung.

BVerfG:
„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..“[38]

Im vorliegenden Fall verneint das BVerfG die überragende Bedeutung der Rechtfertigungsrechtsgüter auch deshalb, weil

- weder sie

BVerfG:
„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.“[39]

- noch die Qualität ihrer Gefährdung ausreichend bestimmt konturiert sind.

BVerfG:
„§ 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 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.“[40]

Nach Auffassung des BVerfG ist der Eingriff in das Fernmeldegeheimnis somit unverhältnismäßig.

c. Vereinbarkeit mit der Menschenwürde (Art. 1 Abs. 1 GG)

aa) Recht

Zusätzlich könnte auch der Geltungsbereich des Grundrechts der Menschenwürde (Art. 1 Abs. 1 S. 1 GG) eröffnet sein.

Art. 1 GG [Schutz der Menschenwürde]
(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.
(…)

Auch das Fernmeldegeheimnis dient dem Schutz der Menschenwürde.

BVerfG:
„Art. 10 Abs. 1 GG gewährleistet die freie Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch von Kommunikation und schützt damit zugleich die Würde des Menschen."[41]

Nach Auffassung des BVerfG kommt dem Grundrecht der Menschenwürde (Art. 1 Abs. 1 S. 1 GG) neben dem Fernmeldegeheimnis aber eigenständiges Gewicht zu, soweit es um den Schutz des Kernbereichs höchstpersönlicher Lebensgestaltung geht.

BVerfG:
„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."[42]

FEX: Anders als beim Recht auf informationelle Selbstbestimmung bejaht das BVerfG bei der Menschenwürde eine Grundrechtskonkurrenz mit dem Fernmeldegeheimnis. Der Geltungsbereich von Art. 1 Abs. 1 GG ist daher eröffnet.

bb) Eingriff

§ 33a Abs. 1 Nr. 2 und 3 Nds.SOG enthalten keine Regeln zum Schutz dieser höchstpersönlichen Sphäre. Die Normen, die zur Durchführung von Telekommunika-

tionsüberwachungsmaßnahmen ermächtigen, müssen nach vom BVerfG vertretener Auffassung selbst Vorkehrungen treffen, dass Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung unterbleiben.

BVefG:
„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.“[43]

Nach Ansicht des BVerfG greifen die Regelungen des § 33a Abs. 1 Nr. 2 und Nr. 3 Nds.SOG damit in das Grundrecht der Menschenwürde ein.

cc) Rechtfertigung

Wenn ein Eingriff in die Menschenwürde bejaht wird, fehlt immer eine Rechtfertigung. Die Menschenwürde ist schrankenlos gewährleistet.

d. Ergebnis

§ 33a Abs. 1 Nr. 2 und Nr. 3 Nds.SOG sind somit auch materiell verfassungswidrig, da die Reglungen gegen das Bestimmtheitsgebot, sowie gegen das Fernmeldegeheimnis und die Menschenwürde verstoßen. § 33a Abs. 1 Nr. 2 und Nr. 3 Nds.SOG sind daher nichtig.

B. Schlussfolgerungen aus der Entscheidung des BVerfG

- Die Bundesländer haben keine Gesetzgebungskompetenz für eine polizeirechtliche Telekommunikationsüberwachung zur Vorsorge für die Verfolgung von Straftaten.
- Dem Zitiergebot wird nicht durch die Nennung des eingeschränkten Grundrechts in einer fortgeltenden Vorgängerregelung genügt, wenn die Eingriffbefugnisse wesentlich erweitert werden.
- § 33a Abs. 1 Nr. 2 und Nr. 3 Nds.SOG genügten nicht dem verfassungsrechtlichen Bestimmtheitsgebot.
- Die Normen gewährleisten nicht den Schutz des Kernbereichs höchstpersönlicher Lebensgestaltung und sind daher mit der Menschenwürde (Art. 1 Abs. 1 GG) unvereinbar.

C. FEX: Rechtslage in Hessen

Auch das Hessische Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) [44]sieht eine polizeirechtliche Telekommunikationsüberwachung vor:

§ 15a HSOG [Datenerhebung durch Telekommunikationsüberwachung]
(1) Die Polizeibehörden können von einem Dienstanbieter, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, verlangen, dass er die Kenntnisnahme des Inhalts der Telekommunikation ermöglicht und die näheren Umstände der Telekommunikation einschließlich des Standorts aktiv geschalteter nicht ortsfester Telekommunikationsanlagen übermittelt, wenn dies **zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich** ist.
(2) Unter den Voraussetzungen des Abs. 1 können die Polizeibehörden auch Auskunft über die Telekommunikation in einem zurückliegenden oder einem zukünftigen Zeitraum sowie über Inhalte verlangen, die innerhalb des Telekommunikationsnetzes in Speichereinrichtungen abgelegt sind.
(3) Die Polizeibehörden können technische Mittel zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes und zur Ermittlung der Geräte- und Kartennummern einsetzen, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist.
(4) Die Maßnahmen bedürfen außer bei Gefahr im Verzug der richterlichen Anordnung. Für das Verfahren gilt § 39 Abs. 1 mit der Maßgabe, dass das Amtsgericht zuständig ist, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Die Anordnung muss Namen und Anschrift der Person, gegen die sie sich richtet, oder die Rufnummer o-

der eine andere Kennung ihres Telekommunikationsanschlusses oder ihres Telekommunikationsgeräts enthalten. § 15 Abs. 5 Satz 3 und 5 bis 9 gilt entsprechend.
(5) Soweit sich bei Gelegenheit der Auswertung Tatsachen ergeben, die einen anderen Sachverhalt betreffen, dürfen die durch die Maßnahme erlangten personenbezogenen Daten nur verarbeitet werden, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist. Bundesrechtliche Übermittlungspflichten bleiben unberührt.
(6) § 17 Abs. 1 und 3 des Artikel 10-Gesetzes vom 26. Juni 2001 (BGBl. I S. 1254, 2298), zuletzt geändert durch Gesetz vom 22. Dezember 2003 (BGBl. I S. 2836), gilt entsprechend.

Der Hessische Gesetzgeber sieht die Regelung auch nach dem Urteil des BVerfG zur polizeirechtlichen Telekommunikationsüberwachung als rechtmäßig an, da die Norm hohe Eingriffvoraussetzungen vorsähe (gegenwärtige Gefahr für Leib, Leben oder Freiheit der Person).[45] Jedenfalls wird in Hessen – anders als in Niedersachsen – der Kernbereich höchstpersönlicher Lebensgestaltung dergestalt geschützt, dass die Speicherung insoweit unzulässig ist (§ 27 Abs. 2 S. 1 Nr. 1 i.V.m. Abs. 6 S. 1 Nr. 2 HSOG)

§ 27 HSOG [Berichtigung, Löschung und Sperrung von Daten]
(2) Automatisiert gespeicherte personenbezogene Daten **sind zu löschen** und die dazugehörigen Unterlagen sind zu vernichten, **wenn**
1. **ihre Speicherung unzulässig ist**,
(…)
Ist eine Löschung in den Fällen des Satz 1 Nr. 1 und 2 wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich, kann an die Stelle der Löschung die Sperrung treten.
(…)
(6) Löschung und Vernichtung unterbleiben, wenn
(…)
2. die betroffene Person über eine verdeckte Datenerhebung noch nicht unterrichtet worden ist, es sei denn, dass die Datenerhebung den Kernbereich privater Lebensgestaltung betroffen hat,
(…)

beziehungsweise ein Verwertungsverbot besteht (§ 15 Abs, 4 S. 2 HSOG).

§ 15 Abs. 4 S. 2 HSOG [Datenerhebung durch Observation und Einsatz technischer Mittel]
Erkenntnisse aus dem Kernbereich privater Lebensgestaltung unterliegen einem Verwertungsverbot. (…)

Inwieweit die hessische Regelung insoweit der BVerfG-Rechtsprechung genügt, die im Kernbereich höchstpersönlicher Lebensgestaltung ein Erhebungsverbot[46] erwägt, bedarf weiterer Prüfung.

---

[1] Informationen zu FÖR (Fachgebiet Öffentliches Recht) finden Sie unter http://www.bwl.tu-darmstadt.de/jus4/?FG=jus.
[2] Cyberlaw (in einer öffentlich-rechtlichen Betrachtung) ist ein Oberbegriff für Medien-, Telekommunikations-, Computer-, Internet-, Informations-, Datensicherheits- und Datenschutzrechte, die sich mit den Themen des Cyberspace und der Cyberworld befassen.
[3] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04.
[4] in Verbindung mit.
[5] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 94.
[6] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 98.
[7] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 100.
[8] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 109.
[9] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 108.
[10] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 110.
[11] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 111 f.
[12] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 81.
[13] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 86.
[14] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 87.
[15] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 88.
[16] FEX: Dies führt nach Ansicht des BVerfG allerdings nicht zur Nichtigkeit des Gesetzes, da die Frage, ob das Zitiergebot durch eine bereits existierende und in Zukunft fortgeltende Zitiervorschrift erfüllt ist, bisher nicht vom BVerfG geklärt worden war.

BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 90:
„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."

[17] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 117.
[18] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 121.
[19] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 122.
[20] Argumente des Bundesdatenschutzbeauftragten und der Datenschutzbeauftragten der Länder; BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 68.
[21] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 126.
[22] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 127.
[23] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 129.
[24] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 131 f.
[25] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 133.
[26] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 134.
[27] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 79.
[28] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 82.
[29] FÖR-Glossar: Unter „Datenorganisation" versteht FÖR die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten (§ 3 Abs. 2 BDSG).
[30] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 136.
[31] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 139.
[32] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 141.
[33] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 143 f.

[34] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 142.
[35] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 140.
[36] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 147.
[37] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 146.
[38] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 150.
[39] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 152.
[40] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 155.
[41] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 162.
[42] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 163.
[43] BVerfG, Urteil vom 27.07.2005, Az: 1 BvR 668/04, Rn. 164.
[44]

[45] Vergleiche die „Stellungnahme des Hessischen Landtags zum 33. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten“, Drucks 16/4751, S. 12.
[46] FEX: Problematisch ist hier, ob auf § 15 angesichts der Spezialregelung in § 15 a HSOG zurückgegriffen werden kann. Der Gesetzgeber hat in § 15a Abs. 4 S. 4 HSOG auf andere Bestimmungen des § 15 HSOG verwiesen – nicht aber auf § 15 Abs. 4 S. 2 HSOG. Eine verfassungskonforme Auslegung indiziert nach hier vertretener Ansicht eine systematische Auslegung, die diesen Rückgriff erlaubt. Wenn die Polizei technische Mittel – zu denen auch die Datenerhebung durch Telekommunikationsüberwachung gehört – einsetzt (§ 15 Abs. 1 Nr. 2 HSOG), dann muss zumindest ein Verwertungsverbot hinsichtlich der Daten aus dem Kernbereich privater Lebensgestaltung zugrundegelegt werden.