

Gesetzentwurf

Fraktion der SPD
Fraktion Bündnis 90/Die Grünen

Hannover, den 21.05.2013

Der Landtag wolle das folgende Gesetz beschließen:

**Gesetz
zur Änderung des Niedersächsischen Gesetzes
über die öffentliche Sicherheit und Ordnung
und des Niedersächsischen Verfassungsschutzgesetzes**

Artikel 1

Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung

Das Niedersächsische Gesetz über die öffentliche Sicherheit und Ordnung in der Fassung vom 19. Januar 2005 (Nds. GVBl. S. 9), zuletzt geändert durch Artikel 3 des Gesetzes vom 12. Dezember 2012 (Nds. GVBl. S. 566), wird wie folgt geändert:

1. § 33 wird wie folgt geändert:
 - a) In der Überschrift wird das Wort „Telekommunikationsverbindungsdaten“ durch das Wort „Verkehrsdaten“ ersetzt.
 - b) In Absatz 1 Satz 1 werden die Worte „Telekommunikationsverbindungsdaten im Sinne des § 100 g Abs. 3 der Strafprozessordnung“ durch die Worte „Verkehrsdaten (§ 96 des Telekommunikationsgesetzes)“ ersetzt.
 - c) In Absatz 2 werden das Wort „Telekommunikationsdienstleistungen“ durch das Wort „Telekommunikationsdienste“ und das Wort „Telekommunikationsverbindungsdaten“ durch das Wort „Verkehrsdaten“ ersetzt.
2. § 33 a wird wie folgt geändert:
 - a) In Absatz 2 Satz 1 Nr. 2 werden die Worte „Telekommunikationsverbindungsdaten (§ 33 Abs. 1)“ durch die Worte „Verkehrsdaten (§ 96 des Telekommunikationsgesetzes)“ ersetzt.
 - b) Absatz 7 wird wie folgt geändert:
 - aa) In Satz 1 wird das Wort „Telekommunikationsleistungen“ durch das Wort „Telekommunikationsdienste“ ersetzt.
 - bb) Satz 2 erhält folgende Fassung:

„²Die Polizei hat den Diensteanbietern eine Entschädigung entsprechend § 23 des Justizvergütungs- und -entschädigungsgesetzes zu gewähren.“
 - c) Es wird der folgende Absatz 8 angefügt:

„(8) ¹Diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, haben der Polizei aufgrund eines Auskunftsverlangens nach Absatz 2 Satz 1 Nr. 2 oder 3 die zur Auskunftserteilung erforderlichen Daten unverzüglich zu übermitteln; die Absätze 4 und 5 gelten entsprechend. ²Die Polizei hat den Diensteanbietern eine Entschädigung entsprechend § 23 des Justizvergütungs- und -entschädigungsgesetzes zu gewähren.“

3. § 33 c erhält folgende Fassung:

„§ 33 c
Auskunftsverlangen

(1) ¹Die Polizei kann zur Abwehr einer Gefahr für die öffentliche Sicherheit Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten zu den in den §§ 6 und 7 dieses Gesetzes sowie unter den Voraussetzungen des § 8 dieses Gesetzes zu den dort genannten Personen verlangen. ²Die Datenerhebung darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. ³Auf das Auskunftsverlangen nach Satz 1 findet § 30 Abs. 4 keine Anwendung.

(2) ¹Die Polizei darf auch Auskunft über Daten verlangen, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt werden. ²Die Auskunft darf nur verlangt werden, wenn die Voraussetzungen des § 33 a Abs. 1 und die gesetzlichen Voraussetzungen dafür vorliegen, dass die Polizei zu dem jeweils angestrebten Nutzungszweck, insbesondere zur Sicherstellung von Daten nach § 26 oder zur Durchführung einer Telekommunikationsüberwachung nach § 33 a, Zugriff auf die geschützten Daten und Telekommunikationsvorgänge nehmen darf. ³Die Datenerhebung darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. ⁴§ 33 a Abs. 4 und 5 gilt entsprechend. ⁵Satz 4 findet keine Anwendung, wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird.

(3) ¹Unter den Voraussetzungen des § 33 a Abs. 1 darf die Auskunft nach Absatz 1 auch anhand einer zu bestimmten Zeitpunkten zugewiesenen Internetprotokoll-Adresse verlangt werden. ²§ 33 a Abs. 4 und 5 gilt entsprechend.

(4) ¹Diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, haben der Polizei aufgrund eines Auskunftsverlangens nach den Absätzen 1 bis 3 die zur Auskunftserteilung erforderlichen Daten unverzüglich, vollständig und richtig zu übermitteln. ²Die Polizei hat für die Erteilung von Auskünften nach den Absätzen 1 bis 3 eine Entschädigung entsprechend § 23 des Justizvergütungs- und -entschädigungsgesetzes zu gewähren.“

Artikel 2

Änderung des Niedersächsischen Verfassungsschutzgesetzes

Das Niedersächsische Verfassungsschutzgesetz in der Fassung vom 6. Mai 2009 (Nds. GVBl. S. 154), zuletzt geändert durch Artikel 5 des Gesetzes vom 7. Oktober 2010 (Nds. GVBl. S. 465), wird wie folgt geändert:

1. § 5 a Abs. 6 wird wie folgt geändert:

- a) Satz 1 erhält folgende Fassung:

„¹Diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, sind verpflichtet, der Verfassungsschutzbehörde auf Anordnung Auskünfte zu Verkehrsdaten nach § 96 Abs. 1 Nrn. 1 bis 4 des Telekommunikationsgesetzes (TKG) und sonstigen zum Aufbau und zur Aufrechterhaltung der Telekommunikation notwendigen Verkehrsdaten zu erteilen.“

- b) Es wird der folgende Satz 3 angefügt:

„³Die Verfassungsschutzbehörde hat für die Erteilung von Auskünften nach Satz 1 eine Entschädigung entsprechend § 23 des Justizvergütungs- und -entschädigungsgesetzes zu gewähren.“

2. Nach § 5 b wird der folgende § 5 c eingefügt:

„§ 5 c

Auskunftsverlangen

(1) Soweit dies zur Erfüllung der Aufgaben der Verfassungsschutzbehörde erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 TKG erhobenen Daten verlangt werden (§ 113 Abs. 1 Satz 1 TKG).

(2) ¹Bezieht sich das Auskunftsverlangen nach Absatz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Abs. 1 Satz 2 TKG), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der geschützten Daten vorliegen. ²§ 5 b Abs. 1 bis 4 gilt entsprechend.

(3) ¹Die Auskunft nach Absatz 1 darf auch anhand einer zu bestimmten Zeitpunkten zugewiesene Internetprotokoll-Adresse verlangt werden (§ 113 Abs. 1 Satz 3 TKG). ²§ 5 b Abs. 1 bis 4 gilt entsprechend.

(4) Aufgrund eines Auskunftsverlangens nach Absatz 1 bis 3 hat derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich, vollständig und richtig zu übermitteln.

(5) Die Verfassungsschutzbehörde hat für die Erteilung von Auskünften nach Absatz 1 bis 3 eine Entschädigung entsprechend § 23 des Justizvergütungs- und -entschädigungsgesetzes zu gewähren.

(6) Das Grundrecht des Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird nach Maßgabe des Absatzes 2 eingeschränkt.“

Artikel 3

Einschränkung von Grundrechten

Aufgrund dieses Gesetzes kann das Grundrecht auf Wahrung des Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) eingeschränkt werden.

Artikel 4

Weitere Änderung des Niedersächsischen Gesetzes
über die öffentliche Sicherheit und Ordnung

§ 33 c des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung in der Fassung vom 19. Januar 2005 (Nds. GVBl. S. 9), zuletzt geändert durch Artikel 1 dieses Gesetzes, wird gestrichen.

Artikel 5

Weitere Änderung des Niedersächsischen Verfassungsschutzgesetzes

§ 5 c des Niedersächsischen Verfassungsschutzgesetzes in der Fassung vom 6. Mai 2009 (Nds. GVBl. S. 154), zuletzt geändert durch Artikel 2 dieses Gesetzes, wird gestrichen.

Artikel 6

Inkrafttreten

¹Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft. ²Abweichend von Satz 1 treten die Artikel 4 und 5 am 1. Juli 2015 in Kraft.

Begründung

A. Allgemeiner Teil

I. Anlass, Ziel und Schwerpunkte des Gesetzes

Der Anlass für den vorliegenden Gesetzentwurf ergibt sich aus einem Beschluss des Bundesverfassungsgerichts vom 24. Januar 2012 zu einer gegen die §§ 111 bis 113 TKG gerichteten Verfassungsbeschwerde (1 BvR 1299/05), mit dem das Gericht § 113 Abs. 1 Satz 2 TKG als mit dem Grundgesetz unvereinbar erklärt hat.

Die §§ 95, 111 TKG verpflichten geschäftsmäßige Anbieter von Telekommunikationsdiensten dazu, die von ihnen vergebenen Telekommunikationsnummern und die dazugehörigen persönlichen Daten der Anschlussinhaber (u. a. Telefonnummer, Name, Anschrift, Geburtsdatum, Datum) zu erheben und zu speichern. § 113 TKG regelt ein manuelles Auskunftsverfahren, das Telekommunikationsdiensteanbieter dazu verpflichtet, diese Daten an Sicherheitsbehörden zu übermitteln, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes erforderlich ist. Das Bundesverfassungsgericht hat entschieden, dass § 113 Abs. 1 Satz 1 TKG verfassungskonform dahin gehend auszulegen ist, dass die Vorschrift den Abruf von Bestandsdaten im Sinne von §§ 95, 111 TKG durch Sicherheitsbehörden nur in Verbindung mit qualifizierten fachrechtlichen Rechtsgrundlagen ermöglicht. Bei Materien, die der Regelung der Länder vorbehalten sind, bedürfe es nicht nur einer spezifischen landesrechtlichen Berechtigung für den Abruf der Daten, sondern auch einer landesrechtlichen Rechtsgrundlage, die die Auskunftspflicht privater Telekommunikationsunternehmen eigenständig und normenklar begründe.

Darüber hinaus legt das Bundesverfassungsgericht § 113 Abs. 1 Satz 1 TKG verfassungskonform dahin gehend aus, dass darin keine Rechtsgrundlage für die Zuordnung von dynamischen Internetprotokoll-Adressen gesehen werden könne. Ein Auskunftsanspruch über die Zuordnung dynamischer Internetprotokoll-Adressen bedürfe einer normenklaren Regelung.

Die Regelung des § 113 Abs. 1 Satz 2 TKG, die Auskunftsverlangen über solche Daten betrifft, die als Zugangssicherungs_codes (insbesondere PIN und PUK) den Zugang zu Endgeräten oder Speichereinrichtungen sichern, hat das Bundesverfassungsgericht für unvereinbar mit dem Recht auf informationelle Selbstbestimmung erklärt. Die Vorschrift regelt die Auskunftserteilung über Zugangssicherungs_codes unabhängig von den Voraussetzungen für deren Nutzung. Das Bundesverfassungsgericht führt aus, dass der Staat zwar ein legitimes Interesse daran habe, den betreffenden Behörden die in § 113 Abs. 1 Satz 2 TKG genannten Daten für ihre Aufgabenwahrnehmung zugänglich zu machen. Ein Auskunftsverlangen über Zugangssicherungen sei aber nur dann erforderlich und damit zulässig, wenn auch die gesetzlichen Voraussetzungen für den damit konkret erstrebten Nutzungszweck vorliegen.

Das Bundesverfassungsgericht hat § 113 Abs. 1 Satz 1 TKG gleichwohl übergangsweise bis zum 30. Juni 2013 auch unabhängig von den Maßgaben des Gerichts weiterhin für anwendbar erklärt. § 113 Abs. 1 Satz 2 TKG gilt ebenfalls bis zum 30. Juni 2013 mit der Maßgabe fort, dass die in der Vorschrift genannten Zugangsdaten nur erhoben werden dürfen, wenn die gesetzlichen Voraussetzungen für deren Nutzung gegeben sind.

II. Wesentliches Ergebnis der Gesetzesfolgenabschätzung

Mit der vorgeschlagenen Bestandsdatenabfrage wird der Polizei und der Verfassungsschutzbehörde ein Instrument zur Verfügung gestellt, das sie in verhältnismäßiger Weise in die Lage versetzt, ihren gesetzlichen Auftrag zu erfüllen. Das gilt für die Polizei im Hinblick auf die Gefahrenabwehr insbesondere bei Suizidankündigungen oder Vermisstenfällen ebenso wie für den Verfassungsschutz im Hinblick auf Sammlung und Auswertung von Informationen über verfassungsfeindliche

Bestrebungen und Tätigkeiten. Die vorgesehenen Regelungen können die Grundrechte auf informationelle Selbstbestimmung und auf Wahrung des Fernmeldegeheimnisses einschränken. Der mögliche Grundrechtseingriff ist aber von geringer Tiefe, da lediglich Bestandsdaten abgefragt werden. Er ist zudem im Hinblick auf die schützenden Rechtsgüter gerechtfertigt. Folgen über die Erreichung des Regelungszwecks hinaus sind nicht zu erwarten.

Mehrausgaben aufgrund dieses Gesetzes sind für den Landeshaushalt im Rahmen der Entschädigung der im Einzelfall in Anspruch genommenen Dienstanbieter zu berücksichtigen. Weder für die kommunalen Haushalte noch für die Bürgerinnen und Bürger sind Mehrbelastungen zu erwarten. Die Bestimmungen zur Bestandsdatenabfrage schaffen keine neuen Aufgaben für Polizei und Verfassungsschutz, sondern regeln in verfassungsmäßig gebotener Weise die Befugnisnormen in den entsprechenden (Landes-)Fachgesetzen.

Der für den Abruf von Zugangssicherungs-codes und für den Abruf von Bestandsdaten anhand von dynamischen IP-Adressen durch die Polizei vorgesehene Richtervorbehalt begründet neue Zuständigkeiten für die ordentlichen Gerichte, was für diese eine geringfügige Arbeitsmehrbelastung bedeutet.

III. Voraussichtliche Kosten und haushaltmäßige Auswirkungen

Auswirkungen auf die kommunalen Haushalte ergeben sich nicht. Für den Landeshaushalt sind aufgrund der neu geregelten Entschädigung der Diensteanbieter Mehrbelastungen in Höhe von jährlich 5 000 Euro zu erwarten.

B. Besonderer Teil

Zu Artikel 1 (Nds. SOG):

Zu Nummer 1 (§ 33):

Zu Buchstaben a und b:

§ 33 wird begrifflich an das TKG und die StPO angeglichen. Der Begriff „Telekommunikationsverbindungsdaten“ wurde bis zum 31. Dezember 2007 in § 100 g Abs. 3 der Strafprozessordnung (StPO) definiert. Er basierte auf der Telekommunikations-Datenschutzverordnung aus dem Jahr 2000, die am 26. Juni 2004 außer Kraft trat, als ihre wesentlichen Regelungen Eingang in das Telekommunikationsgesetz (TKG) fanden. Seither definiert das TKG den Begriff „Verkehrsdaten“ (§§ 3 Nr. 30, 96 TKG). Dieser Begriff ersetzt seit dem 1. Januar 2008 auch in der StPO den Begriff „Telekommunikationsverbindungsdaten“.

Zu Buchstabe c:

In Absatz 2 wird zudem das Wort „Telekommunikationsdienstleistungen“ durch das Wort „Telekommunikationsdienste“ ersetzt. Dabei handelt es sich um eine begriffliche Anpassung an § 3 Nr. 24 TKG und die StPO.

Zu Nummer 2 (§ 33 a):

Zu Buchstabe a:

Es handelt sich wie in § 33 um eine sprachliche Angleichung an das TKG und die StPO; siehe auch die Begründung zu Nummer 2.

Zu Buchstabe b:

In Absatz 7 Satz 1 wird das Wort „Telekommunikationsleistungen“ zur begrifflichen Anpassung an das TKG und die StPO durch das Wort „Telekommunikationsdienste“ ersetzt.

Satz 2 erklärt für die Entschädigung der Telekommunikationsunternehmen bei Maßnahmen nach § 33 a die Regelung des § 23 Justizvergütungs- und -entschädigungsgesetz (JVEG) für entsprechend anwendbar. Die Einschränkung „soweit eine telekommunikationsrechtliche Regelung nicht

besteht“ wird gestrichen. Sie bezog sich auf eine Verordnungsermächtigung des Bundes in § 110 Abs. 9 TKG, die zwischenzeitlich aufgehoben wurde. Seit einer Gesetzesänderung im Jahr 2009 ist § 23 JVEG darüber hinaus für die Entschädigung, die Telekommunikationsunternehmen für die Umsetzung von Anordnungen zur Überwachung der Telekommunikation oder die Erteilung von Auskünften erhalten, abschließend.

Zu Buchstabe c:

Der neue Absatz 8 enthält in Satz 1 die bislang in § 33 c geregelte Verpflichtung von Telekommunikationsunternehmen, der Polizei Auskünfte über Verkehrsdaten zu erteilen; der Regelungsgehalt bleibt unverändert. Die Abrufbefugnis der Polizei und die Auskunftspflicht der Telekommunikationsunternehmen in Bezug auf Verkehrsdaten werden durch die Änderung in derselben Vorschrift geregelt.

Aufgrund von Satz 2 wird den betroffenen Telekommunikationsunternehmen der Aufwand für die Auskunftserteilung nach § 23 Justizvergütungs- und -entschädigungsgesetz entschädigt.

Zu Nummer 3 (§ 33 c neu):

Durch den neu gefassten § 33 c erhält die niedersächsische Polizei über den 30. Juni 2013 hinaus die Berechtigung zur Erhebung von Bestandsdaten im Sinne von §§ 95, 111 TKG, auch anhand dynamischer Internetprotokoll-Adressen, und zur Abfrage von Zugangssicherungs-codes bei Telekommunikationsdiensteanbietern.

Bisher fragt die niedersächsische Polizei entsprechende Daten bei Telekommunikationsunternehmen auf der Grundlage von §§ 30, 31 Nds. SOG i. V. m. § 113 Abs. 1 TKG ab.

Der neu gefasste § 33 c setzt die Vorgaben des Bundesverfassungsgerichts für qualifizierte Rechtsgrundlagen zur Erhebung von Bestandsdaten, auch anhand dynamischer Internetprotokoll-Adressen, und zur Abfrage von Zugangssicherungs-codes bei Telekommunikationsdiensteanbietern durch die Polizei um.

Zu Absatz 1:

Absatz 1 Satz 1 regelt die Abrufbefugnis der Polizei für Daten im Sinne von §§ 95, 111 TKG. Voraussetzung für die Erhebung dieser Daten ist, dass sie zur Abwehr einer konkreten Gefahr für die öffentliche Sicherheit erforderlich ist.

Die Polizei ist insbesondere bei Ankündigungen von Amokläufen oder Suiziden über das Telefon oder das Internet häufig auf die Erhebung von Bestandsdaten zu E-Mail-Konten oder Telefonnummern angewiesen, um die Gefährder oder die gefährdeten Personen identifizieren und einschreiten zu können. Umgekehrt kann eine Bestandsdatenabfrage dann, wenn der Name einer vermissten Person oder eines Suizidgefährdeten bekannt ist, zur Ermittlung eines Mobilfunkanschlusses erforderlich sein, um die Ortung eines mitgeführten Mobiltelefons vorbereiten zu können. In Vermisstenfällen kann beispielsweise auch eine Bestandsdatenabfrage der Polizei zu Internet-Chat-Partnern einer vermissten Person dazu führen, dass der oder die Vermisste gefunden wird.

Satz 3 trägt für die Auskunftsverlangen nach Satz 1 der bisherigen Rechtslage Rechnung, nach der für diese Maßnahmen keine Benachrichtigungspflicht besteht. Aufgrund der systematischen Einordnung der Bestandsdatenabfrage als Datenerhebung mit besonderen Mitteln und Methoden (§§ 33 a bis 37) wird für Maßnahmen nach Absatz 2 und 3 künftig eine Benachrichtigungspflicht nach § 30 Abs. 4 eingeführt. Dies geht über die Anforderungen des Bundesverfassungsgerichts hinaus, ist wegen des gegenüber den Auskunftsverlangen nach Absatz 1 größeren Eingriffsgewichts aber sachgerecht.

Zu Absatz 2:

Absatz 2 regelt die Erhebung von Zugangssicherungs-codes (wie Passwörter, PIN und PUK).

Die Erhebung ist an strengere Eingriffsvoraussetzungen und Verfahrensregelungen geknüpft als die „normale“ Bestandsdatenabfrage nach Absatz 1. Sie setzt eine gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person voraus. Darüber hinaus müssen die Voraussetzungen dafür vorliegen, dass die Polizei zu dem jeweils angestrebten Nutzungszweck Gebrauch von den Zugangssi-

cherungscodes machen und auf die durch sie geschützten Daten und Telekommunikationsvorgänge zugreifen darf.

Absatz 2 Satz 4 stellt die Abfrage von Zugangssicherungs_codes durch den Verweis auf § 33 a Abs. 4 und 5 unter Richtervorbehalt. Der Richtervorbehalt trägt verfahrensmäßig dem Umstand Rechnung, dass Zugangssicherungs_codes Daten sind, die Telekommunikationsteilnehmer einsetzen, um ihre Daten besonders zu sichern. Der im Abruf dieser Sicherungs_codes liegende Eingriff in das Recht auf informationelle Selbstbestimmung (Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG) geht daher über ein Auskunftsverlangen zu „normalen“ Bestandsdaten, das einem Blick in das Telefonbuch gleicht, hinaus. Wenngleich das Bundesverfassungsgericht für die Auskunftsverlangen über Zugangssicherungs_codes keinen Richtervorbehalt verlangt, scheint es geboten, Auskunftsverlangen der Polizei zu Zugangssicherungsdaten an eine vorbeugende Kontrolle durch eine unabhängige und neutrale Instanz zu knüpfen. Mit Absatz 2 wird zudem ein Gleichklang mit den auf Bundesebene im Gesetzgebungsverfahren befindlichen Neuregelungen zur Bestandsdatenauskunft geschaffen.

Beispielkonstellationen, in denen die Polizei zur Gefahrenabwehr auf die Abfrage von Zugangssicherungs_codes, vor allem PIN und PUK von Mobiltelefonen bzw. Smartphones, angewiesen ist, sind das Auffinden von zugangsgesicherten Mobiltelefonen oder Smartphones von vermissten oder suizidgefährdeten Personen. Die Polizei muss die Geräte entsperren können, um Informationen über zuletzt getätigte oder eingegangene Anrufe, SMS oder E-Mails zu erhalten und dadurch Hinweise auf den Aufenthaltsort der gefährdeten Person finden zu können.

Absatz 2 Satz 5 erklärt eine richterliche Anordnung in den Fällen für entbehrlich, in denen bereits der angestrebte Nutzungszweck wie beispielsweise eine Telekommunikationsüberwachung nach § 33 a unter Richtervorbehalt steht. Damit wird vermieden, dass der Richter in derselben Angelegenheit zweimal eine Anordnung treffen muss - erst für das Auskunftsverlangen bezüglich des Zugangssicherungs_codes und dann für die Durchführung der Telekommunikationsüberwachung.

Zu Absatz 3:

Absatz 3 Satz 1 enthält die Rechtsgrundlage für Auskunftsverlangen der Polizei über die Zuordnung von dynamischen Internetprotokoll-Adressen. Dabei ist zu berücksichtigen, dass die Telekommunikationsunternehmen nur dann dazu in der Lage sind, entsprechende Auskünfte zu erteilen, wenn sie zuvor die dem Schutz des Telekommunikationsgeheimnisses unterfallenden, nach § 96 TKG gespeicherten Verkehrsdaten auswerten und feststellen, welchem Anschluss die fragliche Nummer zu dem gegebenen Zeitpunkt zugeordnet war. Der Verarbeitungsprozess und damit die Verkehrsdaten sind für die Auskunft verlangenden Behörden zwar nicht einsehbar, dem darin liegenden mittelbaren Eingriff in Artikel 10 Abs. 1 Grundgesetz wird gleichwohl durch Eingriffsvoraussetzungen und Verfahrensregelungen Rechnung getragen.

Voraussetzung für die Abfrage von Bestandsdaten anhand von dynamischen Internetprotokoll-Adressen ist insbesondere eine gegenwärtige Gefahr im Sinne von § 2 Nr. 1 Buchst. b für die Rechtsgüter Leib, Leben oder Freiheit einer Person. Diese Eingriffsschwelle liegt höher als diejenige für Auskunftsverlangen über Bestandsdaten im Sinne des Absatzes 1, die eine Gefahr im Sinne von § 2 Nr. 1 Buchst. a, also eine konkrete Gefahr für die öffentliche Sicherheit im Einzelfall, erfordern.

Absatz 3 Satz 2 verweist darüber hinaus auf § 33 a Abs. 4 und 5 und stellt damit die Bestandsdatenabfrage anhand der Zuordnung von dynamischen Internetprotokoll-Adressen unter Richtervorbehalt.

Die Polizei ist zur Gefahrenabwehr auf die Möglichkeit angewiesen, Bestandsdaten auch anhand dynamischer Internetprotokoll-Adressen abzufragen. Das gilt insbesondere für Suizidankündigungen oder Amokandrohungen über das Internet, aufgrund derer von einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person auszugehen ist. Eine Abfrage von Bestandsdaten über Internetprotokoll-Adressen kann in diesen Fällen erforderlich sein, um die gefährdeten Personen oder Gefahrenverursacher identifizieren und ausfindig machen zu können.

Zu Absatz 4:

Absatz 4 Satz 1 begründet die Verpflichtung von Telekommunikationsunternehmen, Auskunft über die Daten zu erteilen, die die Polizei nach Maßgabe des Absatzes 1 bis 3 abzurufen berechtigt ist. Das Bundesverfassungsgericht hat in seinem Beschluss vom 24. Januar 2012 dargelegt, dass die Kompetenz des Bundes für das Telekommunikationsrecht gemäß Artikel 73 Abs. 1 Nr. 7 GG den Bundesgesetzgeber nicht dazu in die Lage versetzt, private Telekommunikationsunternehmen abschließend zu verpflichten, einem Auskunftsbeghären Folge zu leisten. Die Inpflichtnahme Privater sei untrennbarer Bestandteil des Datenabrufs. In Materien, die der Regelung der Länder vorbehalten sind, muss diese Auskunftsverpflichtung daher in der landesrechtlichen Abrufnorm selbst geregelt werden.

Aufgrund von Satz 2 wird den betroffenen Telekommunikationsunternehmen der Aufwand für die Auskunftserteilung nach § 23 Justizvergütungs- und -entschädigungsgesetz entschädigt. Die Regelung entspricht § 33 a Abs. 7 Satz 2 und Abs. 8 Satz 2.

Zu Artikel 2 (Änderung des NVerfSchG):

Zu Nummer 1 (§ 5 a Abs. 6):

Zu Buchstaben a und b:

Mit der Neufassung des Satzes 1 fällt die bisher statuierte Unentgeltlichkeit einer Auskunftserteilung nach § 5 a Abs. 6 weg. Gleichzeitig wird ein neuer Satz 3 angefügt, der eine Entschädigungspflicht für Telekommunikationsunternehmen für eine Auskunftserteilung über Verkehrsdaten vorsieht. Die Regelung dient der Gleichbehandlung der manuellen Auskunftsverfahren und stellt gleichzeitig eine Angleichung der niedersächsischen Gesetzeslage an die bereits bestehenden Entschädigungsregelungen im Bundesverfassungsschutzgesetz (§ 8 b Abs. 9 BVerfSchG) dar. Die Entschädigung ist in entsprechender Anwendung des § 23 des Justizvergütungs- und -entschädigungsgesetzes zu gewähren.

Gleichzeitig wird mit der Neufassung des § 5 Abs. 6 Satz 1 die Verweisung auf § 113 a des Telekommunikationsgesetzes gestrichen. Diese Streichung dient der redaktionellen Bereinigung des Gesetzes, nachdem das Bundesverfassungsgericht die Vorschrift des § 113 a des Telekommunikationsgesetzes mit seiner Entscheidung vom 2. März 2010 (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08) zur vorsorglichen Speicherung von Telekommunikationsverkehrsdaten für nichtig erklärt hat.

Zu Nummer 2 (§ 5 c):

Mit der Einfügung eines neuen § 5 c wird das Niedersächsische Verfassungsschutzgesetz an die Anforderungen, die das Bundesverfassungsgericht mit Beschluss vom 24. Januar 2012 (1 BvR 1299/05) aufgestellt hat, angepasst. Es wird mit § 5 c eine landesrechtliche Ermächtigungsgrundlage eingefügt, die eine Befugnis zur Abfrage von Bestandsdaten der Niedersächsischen Verfassungsschutzbehörde gegenüber den Telekommunikationsdiensteanbietern eigenständig und normenklar begründet. Daneben werden, der Eingriffsintensität angepasst, Verfahrensvorschriften neu eingeführt. Schließlich enthält § 5 c Abs. 5 eine Entschädigungsregelung für diese Bestandsdatenauskünfte.

Zu Absatz 1 bis 3:

Die Abfrage von Bestandsdaten ist für die Aufgabenerfüllung der Verfassungsschutzbehörde unerlässlich. Sie liefert nicht nur wesentliche Informationen und Daten für die Durchführung von Maßnahmen nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, sondern ermöglicht es, Absender und sonstige Beteiligte an Kommunikationsvorgängen zu identifizieren. Dadurch kann das Erkenntnisbild relevanter Personen vervollständigt und Vernetzungen von Personen und Gruppierungen festgestellt werden.

In der Vergangenheit wurden diese Abfragen auf § 5 NVerfSchG und § 113 des Telekommunikationsgesetzes gestützt.

Die bisher durch § 113 Abs. 1 Satz 1 des Telekommunikationsgesetzes ermöglichte Abfrage von Bestandsdaten im manuellen Auskunftsverfahren kann die Verfassungsschutzbehörde künftig nach § 5 c Abs. 1 durchführen.

Auskunftsverlangen zu Zugangssicherungs-codes, mittels derer der Zugriff auf Endgeräte oder Speichereinrichtungen durch Passwörter, PIN und PUK geschützt ist, können nach § 5 c Abs. 2 eingeholt werden. Gleichzeitig wird in Umsetzung der Rechtsprechung des Bundesverfassungsgerichts die Erhebung der Zugangsdaten an das Vorliegen der jeweiligen Voraussetzungen für deren Nutzung geknüpft. Obwohl vom Bundesverfassungsgericht mit der oben genannten Entscheidung vom 24. Januar 2012 unter Hinweis auf die geringe Eingriffstiefe aller Auskünfte nach § 113 des Telekommunikationsgesetzes nicht gefordert (RdNrn. 177 und 186), wird durch den Verweis auf § 5 b Abs. 1 bis 4 der Sensibilität der Daten durch spezielle Verfahrensregelungen Rechnung getragen. So bedarf das Auskunftsverlangen danach der Anordnung durch die Fachministerin oder den Fachminister und der Zustimmung durch die G 10-Kommission. Für die erhobenen personenbezogenen Daten sowie die Unterrichtungspflicht gegenüber den Betroffenen gelten die Vorschriften des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses entsprechend.

In Absatz 3 wird eine Rechtsgrundlage für Auskunftsverlangen der Verfassungsschutzbehörde über die Zuordnung dynamischer Internetprotokoll-Adressen geschaffen. Dem Eingriff in Artikel 10 Abs. 1 des Grundgesetzes, der bei der für die Auskunft erforderlichen automatisierten Auswertung von Verkehrsdaten beim Telekommunikationsunternehmen entsteht, wird ebenfalls durch den Verweis auf § 5 b Abs. 1 bis 4 mit den dort geregelten speziellen Verfahrensregelungen Rechnung getragen.

Zu Absatz 4:

In Umsetzung der oben genannten Entscheidung des Bundesverfassungsgerichts wird in Absatz 4 die Verpflichtung von Telekommunikationsunternehmen normiert, Auskunft über die Daten zu erteilen, die die Verfassungsschutzbehörde nach Maßgabe des Absatzes 1 bis 3 abzurufen berechtigt ist.

Zu Absatz 5:

In Absatz 5 wird im Hinblick auf eine konsequente Behandlung der im manuellen Verfahren erteilten Auskünfte auch für die Auskunftsverlangen nach Absatz 1 bis 3 eine Regelung über den Anspruch der zur Auskunft verpflichteten Anbieter von Telekommunikationsdiensten auf eine Entschädigung für die Auskunftserteilung geschaffen.

Zu Absatz 6:

Die Bestandsdatenauskunft anhand dynamischer Internetprotokoll-Adressen stellt einen Eingriff in das Fernmeldegeheimnis des Artikels 10 des Grundgesetzes dar. Für derartige Eingriffe gilt das Zitiergebot gemäß Artikel 19 Abs. 1 Satz 2 des Grundgesetzes. Dem Zitiergebot wird mit der Vorschrift entsprochen.

Zu Artikel 3:

Artikel 3 trägt dem Zitiergebot aus Artikel 19 Abs. 1 Satz 2 des Grundgesetzes Rechnung.

Zu den Artikeln 4 und 5:

Die Vorschriften regeln im Zusammenwirken mit Artikel 6 Satz 2 eine Befristung der Bestimmungen zum Auskunftsverlangen im Nds. SOG und im NVerfSchG. Durch die Befristung wird gewährleistet, dass die Erforderlichkeit der Befugnisnorm bewertet und über den Fortbestand der Regelung neu entschieden wird.

Zu Artikel 6:

Die Vorschrift bestimmt das Inkrafttreten.

Für die Fraktion der SPD

Grant Hendrik Tonne
Parlamentarischer Geschäftsführer

Für die Fraktion Bündnis 90/Die Grünen

Anja Piel
Fraktionsvorsitzende