Kleine Anfrage mit Antwort

Wortlaut der Kleinen Anfrage

der Abgeordneten Ralf Briese und Helge Limburg (GRÜNE), eingegangen am 22.10.2010

Wie weiter mit der Vorratsdatenspeicherung?

Das Bundesverfassungsgericht hat in seinem Urteil vom 2. März 2010 zur umstrittenen Vorratsdatenspeicherung erklärt, dass die §§ 113 a und 113 b des Telekommunikationsgesetzes in der Fassung des Artikels 2 Nr. 6 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 gegen Artikel 10 Abs. 1 des Grundgesetzes verstoßen und deshalb nichtig sind. Die Regelungen entsprechen nicht dem allgemeinen Verhältnismäßigkeitsgrundsatz. Das Gericht führt zudem sinngemäß aus, dass ein diffuses Gefühl allgemeiner Überwachung entstehen könne, wenn Kommunikationsdaten in Form von Zeit, Ort und Zielpersonen mit einer derartigen Tiefe und Dauer über einen langen Zeitraum anlasslos gespeichert würden. Weiterhin sei auch die Datensicherung nach dem Stand der Technik nicht gewährleistet. Daher seien entsprechende vorgehaltene Daten bei den Kommunikationsanbietern zu löschen.

Seit dem Urteil und der anschließenden Löschung der Datenbestände fordern verschiedene Innenminister aus den Ländern eine neue Regelung zur Vorratsdatenspeicherung, weil angebliche oder tatsächliche Schutzlücken bei der Strafverfolgung und der Gefahrenabwehr entstanden seien. Hier stellt sich die Frage, inwieweit die betroffenen Schutz- und Sicherheitsinstitutionen der Länder die Vorratsdaten in der Vergangenheit zu welchen Zwecken genutzt haben und wo nunmehr die konkreten Schutzlücken entstanden sind.

Die EU-Kommission will derweil die umstrittene Richtlinie zur Vorratsdatenspeicherung kritisch evaluieren, weil mehrere EU-Staaten aus verfassungsrechtlichen Bedenken die Richtlinie bisher gar nicht umgesetzt haben. Andere nationale Verfassungsgerichte von EU-Mitgliedstaaten haben die Richtlinie als komplett unvereinbar mit dem jeweiligen nationalen Recht eingestuft. Die zuständige EU-Kommissarin Reding hat daher angekündigt, die Richtlinie auf den Prüfstand zu stellen, um eine Balance zwischen der Terrorismusbekämpfung und der Achtung der Privatsphäre zu finden.

Wir fragen die Landesregierung:

1. Wie oft haben niedersächsische Sicherheitsbehörden (Polizei, Staatsanwaltschaft, Verfassungsschutz) seit Inkrafttreten des Gesetzes über die Vorratsdatenspeicherung auf entsprechende Vorratsdaten zurückgegriffen?
2. Welche und wie viele Straftaten konnten dadurch aufgeklärt oder verhindert werden?
3. Hat sich durch die Vorratsdatenspeicherung bzw. den Rückgriff auf die Daten bei Verdacht einer Straftat die Aufklärungsquote in Niedersachsen signifikant verändert?
4. Wie oft wurde durch abschlägigen richterlichen Beschluss ein Zugriff auf die Vorratsdaten verweigert?
5. Welche Delikte können aufgrund des in der Einleitung zitierten Urteils des Bundesverfassungsgerichtes derzeit nicht mehr oder nur unter erschwerten Bedingungen in Niedersachsen verfolgt werden?
6. Wie wird mit bereits erhobenen Daten nach § 113 TKG bei den Behörden aufgrund der nunmehr verfassungswidrigen Paragraphen aus dem Telekommunikationsgesetz umgegangen?
7. Gibt es insbesondere Beweisverwertungsprobleme im weiteren Strafverfahren durch bereits erhobene Daten, deren Grundlage zur Erhebung nunmehr verfassungswidrig ist?

8. Warum fordert die Landesregierung eine schnelle Wiedereinführung einer Vorratsdatenspeicherung, obwohl die EU-Kommission eine Überarbeitung der entsprechenden Richtlinie angekündigt hat?
9. Hat die Landesregierung Alternativen zur umstrittenen anlasslosen Vorratsdatenspeicherung geprüft? Und wenn ja, wie sehen diese aus?
10. Wie bewertet die Landesregierung die Position der Bundesjustizministerin, als milderes Mittel zur Vorratsdatenspeicherung das sogenannte Quick-Freeze-Verfahren einzuführen?
11. Welche Kommunikationsdaten sollen nach Ansicht der Landesregierung zukünftig wieder anlasslos gespeichert werden, und wie lange sollen diese Daten gespeichert werden?
12. Ist es mittelstandsfreundlich, wenn niedersächsische Telekommunikationsunternehmen zur Speicherung zusätzlicher Datensätze gesetzlich verpflichtet werden, ohne dafür eine entsprechende Kostenerstattung zu bekommen?
13. Wie hoch schätzt die Landesregierung die zukünftigen Zusatzkosten bei niedersächsischen Telekommunikationsunternehmen ein, wenn die Vorratsdatenspeicherung wieder eingeführt wird, aber die durch die höchstrichterliche Rechtsprechung geforderte Datensicherung qualitativ verbessert werden muss?

(An die Staatskanzlei übersandt am 28.10.2010 - II/721 - 808)

Antwort der Landesregierung

Niedersächsisches Justizministerium Hannover, den 29.11.2010
- 4103 I - 404.201 -

Die moderne Kommunikationstechnik hat mittlerweile in nahezu allen Lebensbereichen Einzug gehalten und beeinflusst die Gestaltung unseres Privat- und Berufslebens maßgeblich. Dies gilt selbstverständlich auch für diejenigen, die Informationstechnologien für kriminelle Zwecke nutzen bzw. missbrauchen. Die Veränderungen der Kommunikationslandschaft führen insbesondere auch zu neuen Kriminalitätsformen. Exemplarisch sei an dieser Stelle insbesondere das sogenannte Phishing, das zielgerichtete Ausspähen und Manipulieren von Bankdaten zum Zwecke des Zugriffs auf Konten von Bürgerinnen und Bürgern, genannt. Ein persönlicher Täter-Opfer-Kontakt bzw. ein persönlicher Kontakt zwischen den häufig arbeitsteilig agierenden Mittätern ist in vielen Fällen überhaupt nicht mehr erforderlich.

Klassische polizeiliche Ermittlungsansätze, wie beispielsweise Fingerabdrücke, DNA-Profile oder „Phantomskizzen“ ergeben sich dann nicht mehr und laufen zwangsläufig ins Leere.

Mit dem Urteil des Bundesverfassungsgerichts vom 2. März 2010 fallen die als sogenannte Vorratsdaten gespeicherten Telekommunikationsverkehrsdaten ersatzlos weg. Das Bundesverfassungsgericht hat entschieden, dass eine Speicherpflicht - auch im vorgesehenen Umfang - nicht schlechterdings verfassungswidrig sei, es bei den angegriffenen Vorschriften jedoch an einer entsprechenden Ausgestaltung fehle. So gewährleisteten die angegriffenen Vorschriften u. a. weder eine hinreichende Datensicherheit noch eine Begrenzung der Verwendungszwecke der Daten.

In der Folge sei die Regelung deswegen verfassungswidrig und nichtig.

Die Entscheidung des Bundesverfassungsgerichts hat die Strafverfolgung vor erhebliche Probleme gestellt. Einerseits sind die Strafverfolgungsbehörden an ihren verfassungsrechtlichen Auftrag gebunden, im Interesse des Gemeinwohls eine effektive Strafverfolgung sicherzustellen. Andererseits sind durch den Wegfall der Vorratsdaten erhebliche Schutzlücken entstanden.

Staatsanwaltschaft und Polizei können bei ihren Ermittlungen nur noch auf diejenigen Verbindungsdaten zurückgreifen, die die Unternehmen gemäß § 96 TKG für ihre betrieblichen Zwecke, also in der Regel zu Abrechnungszwecken, speichern. Der wesentliche Unterschied zur vorsorglichen Datenspeicherung nach § 113 a TKG besteht darin, dass die Unternehmen jetzt nicht mehr verpflichtet sind, überhaupt Daten zu speichern. Sie haben lediglich das Recht dazu (§ 96 Abs. 1 TKG). Die betrieblichen Zwecke, für die die Speicherung erfolgt, unterschieden sich zudem nicht nur von Unternehmen zu Unternehmen, sondern auch von Vertrag zu Vertrag. Sie richten sich beispielsweise nach der Vertragsgestaltung (z. B. Flatrate oder Einzelverbindungsnachweis) oder danach, welche Daten das Unternehmen für seine Verwaltung und Geschäftspolitik benötigt. Ob und welche Daten daher auf der Grundlage eines richterlichen Beschlusses z. B. nach § 100 g Abs. 1 StPO erlangt werden können, ist damit letztlich nur noch von Zufälligkeiten abhängig.

Insbesondere für die Strafverfolgung und für die Abwehr erheblicher Gefahren im Bereich des Terrorismus und der organisierten Kriminalität sowie in Deliktsfeldern wie der Kinderpornografie ist die Vorhaltung von Telekommunikationsverkehrsdaten über einen gewissen Mindestzeitraum von essenzieller Bedeutung. Gerade konspirativ vorgehende Tätergruppen bedienen sich zunehmend der neuen Informations-/Kommunikationstechnologien. So wird beispielsweise der groß angelegte „Drogendeal“, bei dem Rauschgift im Kilobereich aus dem Ausland eingeführt wird, heute vor dem eigentlichen Übergabetermin detailliert via E-Mail-Verkehr abgestimmt. Die Weitergabe von kinderpornografischen Schriften erfolgt nicht mehr wie früher in dunklen Hinterhöfen, sondern über Chatrooms im Internet.

Kann man dann die IP-Adressen der „User“ mangels Speicherung nicht mehr ermitteln, sind dem ungehemmten Handel mit kinderpornografischen Schriften Tür und Tor geöffnet. Dies ist im konkreten Fall gerade deshalb so fatal, weil hinter jedem kinderpornografischen Bild der schreckliche sexuelle Missbrauch eines Kindes steckt.

Für Polizei, Justiz und den Verfassungsschutz ist die gesetzliche Regelung der Speicherpflichten und -fristen zwingend erforderlich. Eine erfolgreiche Ermittlungsführung ist mittlerweile in vielen, gerade die schwere Kriminalität betreffenden Fällen nicht mehr möglich, weil die Verkehrsdaten als wesentliche Ermittlungsansätze nicht (mehr) zur Verfügung stehen. Der in letzter Zeit propagierte Ansatz des sogenannten Quick-Freeze ist keine Alternative (siehe dazu Antwort auf Frage 10).

Das Bundesverfassungsgericht hat entgegen anderslautender Behauptungen die Institution der Vorratsdatenspeicherung nicht an sich für verfassungswidrig erklärt. Im Gegenteil: Das Bundesverfassungsgericht hält eine Neuregelung ausdrücklich für möglich und zulässig. Erforderlich sei jedoch, dass hinreichend anspruchsvoll und normenklar die Voraussetzungen im Hinblick auf die Datensicherheit, die Anlässe und Zwecke der Datenverwendung (d. h. Eingriffsschwellen), die Transparenz (d. h. Erkennbarkeit für den Betroffenen) und den Rechtsschutz des Betroffenen festgelegt werden. Die Richtlinie der EU 2006/24/EG, die die Anbieter von Telekommunikationsdiensten dazu verpflichtet, die in § 113 a TKG erfassten Daten für mindestens sechs Monate und höchstens zwei Jahre zu speichern und für die Verfolgung von schweren Straftaten bereitzuhalten, kann daher verfassungskonform umgesetzt werden. Es ist nicht eine Frage des Könnens, sondern allein eine Frage des Wollens.

Ohne die Speicherung von Vorratsdaten entsteht eine immer größere Lücke im Netz der mit Verfassungsrang ausgewiesenen Strafverfolgung. Der Staat kann es sich auf Dauer nicht leisten, den Schutz der Bevölkerung vor hochkriminellen Tätern zu vernachlässigen. In dem Maße, wie der Staat hier seinen Pflichten nicht nachkommen kann, wird sich die Nutzung neuer Kommunikationstechnologien zu immer ausgefeilteren Straftaten erhöhen.

Polizei, Justiz und Verfassungsschutz fehlen ohne die Vorratsdatenspeicherung ein entscheidendes Instrumentarium zum Schutz der Bürgerinnen und Bürger, die aber zu Recht darauf vertrauen dürfen, dass rechtsfreie Räume weder existieren noch (künstlich) geschaffen werden. Die Rechtspolitik ist deshalb aufgefordert, zügig eine den Vorgaben des Bundesverfassungsgerichts entsprechende Neuregelung der Vorratsdatenspeicherung zu schaffen.

Dies vorangestellt, werden die Fragen namens der Landesregierung wie folgt beantwortet:

Zu 1:

Für die niedersächsische Verfassungsschutzbehörde wurde mit der am 24. Januar 2009 in Kraft getretenen Novellierung des Niedersächsischen Verfassungsschutzgesetzes (NVerfSchG) in § 5 a Abs. 6 NVerfSchG die gesetzliche Möglichkeit geschaffen, Auskunft über Daten, die nach § 113 a des Telekommunikationsgesetzes gespeichert wurden, zu erhalten. Seitdem und bis zur Entscheidung des Bundesverfassungsgerichts vom 2. März 2010 (1 BvR 256/08) hat die niedersächsische Verfassungsschutzbehörde vier Mal von dieser besonderen Auskunftspflicht Gebrauch gemacht.

Für den Bereich der niedersächsischen Polizei sowie der Staatsanwaltschaften gilt Folgendes:

Eine Erfassung der Fälle, in denen in der Zeit vom 1. Januar 2008 bis zum 2. März 2010 im Rahmen von Verkehrsdatenerhebungen gemäß § 100 g Abs. 1 StPO auf nach § 113 a TKG vorsorglich gespeicherte Daten (sogenannte Vorratsdaten) zurückgegriffen wurde, ist nicht erfolgt. Entsprechende Zahlen können daher nicht mitgeteilt werden. Eine retrograde Erhebung dieser Zahlen könnte nur durch eine Auswertung sämtlicher Ermittlungsakten per Hand erfolgen. Eine solche verursacht jedoch einen Aufwand, der angesichts der hohen Belastungen bei Staatsanwaltschaften und Polizeidienststellen im Rahmen einer Kleinen Anfrage nicht zu leisten ist.

Allerdings wurden bei den Staatsanwaltschaften seit 2008 aufgrund der in § 100 g Abs. 4 i. V. m § 100 b Abs. 5 StPO festgelegten Berichtspflicht (jährlich zum 30. Juni des Folgejahres) sämtliche Maßnahmen nach § 100 g StPO erfasst. Danach ergeben sich folgende Zahlen:

Berichtsjahr	2008	2009
Anzahl der Verfahren	766	679
Anzahl der Anordnungen	1 208	1 441

Die Erhebung unterscheidet nicht, ob Daten nach § 113 a TKG oder nach § 96 TKG gefordert waren.

Zu berücksichtigen ist auch, dass das Bundesverfassungsgericht bereits am 11. März 2008 in seiner einstweiligen Anordnung festgestellt hat, dass bestimmte Daten auf Anfragen der Strafverfolgungsbehörden von den Unternehmen nur noch gesichert, aber nicht mehr herausgegeben werden durften, sodass die Daten im laufenden Ermittlungsverfahren (zunächst) nicht zur Verfügung standen. Wegen dieser Anordnung haben die Strafverfolgungsbehörden nicht nur vereinzelt davon abgesehen, entsprechende Anfragen zu stellen.

Zu 2:

Der gesetzliche Auftrag der niedersächsischen Verfassungsschutzbehörde besteht nicht in der Aufklärung oder der Verhinderung von Straftaten, sondern vielmehr in der Sammlung und Auswertung von Informationen über Bestrebungen und Tätigkeiten nach § 3 Abs. 1 Satz 1 NVerfSchG (§ 1 Abs. 1 Nr. 1 NVerfSchG). Zur Erfüllung dieser Aufgabe wurde von den Besonderen Auskunftspflichten nach § 5 a Abs. 6 NVerfSchG Gebrauch gemacht.

Für den Bereich der niedersächsischen Polizei sowie der Staatsanwaltschaften gilt Folgendes:

Aufgrund einer fehlenden Erfassung (siehe Nr. 1) kann hierzu keine Aussage getroffen werden.

Zu 3:

Siehe Antwort zu Frage 2.

Zu 4:

Eine Erfassung der Fälle, in denen Anträge auf Erlass einer Anordnung zur Erhebung von gemäß § 113 a TKG vorsorglich gespeicherten Verkehrsdaten durch das Gericht abgelehnt wurden, wurde statistisch nicht erfasst. Eine retrograde Erhebung durch Auswertung per Hand stellt einen Aufwand dar, der im Rahmen einer Kleinen Anfrage unverhältnismäßig und angesichts der Arbeitsbelastung bei Polizei und Staatsanwaltschaft nicht zumutbar ist.

Zu 5:

Seit dem Urteil des Bundesverfassungsgerichts ist die Aufklärung von Straftaten wesentlich erschwert bzw. unmöglich gemacht worden, in denen elektronische Kommunikationsmittel im Rahmen der Tat und/oder für Vorbereitungshandlungen eingesetzt wurden. Zu nennen sind hier beispielsweise sexueller Missbrauch von Kindern und Straftaten gegen das Leben. Des Weiteren sind Delikte wie Erpressungen, Bedrohungen, insbesondere die Nachstellung (Stalking), bandenmäßig begangene Delikte und/oder Taten, bei denen aufgrund kriminalistischer Erfahrungen im Zusammenhang mit den bisherigen Ermittlungen anzunehmen war, dass mindestens zwei Täter im Rahmen der Tatvorbereitung und/oder Tatnachphase miteinander kommuniziert haben, betroffen. In der Vergangenheit wurden auch in Fällen von Brandstiftungen, Raubdelikten sowie der Ausspähung von Daten entscheidende Ermittlungsansätze durch Erhebung von Telekommunikationsdaten gewonnen.

Die gravierendsten Auswirkungen durch den Wegfall der Vorratsdatenspeicherung sind im Bereich der Straftaten festzustellen, die mittels Telekommunikation und insbesondere über das Internet begangen werden.

Bei der Verfolgung von Internetkriminalität stellt regelmäßig die IP-Adresse des Täters den einzigen Ermittlungsansatz dar. Zur Ermittlung der einer dynamischen IP zuzuordnenden Bestandsdaten müssen die Netzbetreiber auf Verkehrsdaten, die sogenannten Log-Files, zurückgreifen. Nach dem Wegfall der Vorratsdatenspeicherung werden diese Daten - mangels betrieblicher Speichererfordernisse - nicht mehr oder nur noch wenige Tage gespeichert. Eine retrograde Ermittlung des Nutzers einer bestimmten IP ist daher regelmäßig nicht mehr möglich. Der Wegfall der Vorratsdatenspeicherung betrifft daher insbesondere Verfahren wegen Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Schriften gemäß §§ 184 b und 184 c StGB.

Erheblich beeinträchtigt werden auch die Ermittlungen hinsichtlich mittels Telekommunikation begangener Bedrohungen oder Beleidigungen.

Der jeweilige Anrufer kann durch Verkehrsdatenabfragen oft nicht ermittelt werden, weil die Kennung eines eingehenden Anrufs von dem Netzbetreiber entweder überhaupt nicht oder nur für wenige Tage gemäß § 96 Abs. 1 TKG gespeichert wird.

Vergleichbare Probleme ergeben sich bei Ermittlungen wegen des Verdachts der Nachstellung (Stalking) mittels Telefonanrufen oder SMS gemäß § 238 Abs. 1 Nr. 2 StGB. Die Angaben des Opfers zu den bisherigen Kontaktversuchen des Täters werden zum Nachweis der „Beharrlichkeit“ der Nachstellung in der Regel nicht genügen. Aufgrund der entweder nur sehr kurzen Speicherzeiträume hinsichtlich Kennungen eingehender Anrufe und Anrufversuche bzw. der gänzlich unterbleibenden Speicherung dieser Daten wird ein belastbarer objektiver Nachweis der in der Vergangenheit erfolgten beharrlichen Nachstellung oftmals nicht mehr möglich sein.

Auch in Fällen des sogenannten Enkeltricks erweist sich der Wegfall der Vorratsdatenspeicherung regelmäßig als erhebliches Ermittlungshindernis. In diesen Fällen werden von den Tätergruppen zumeist ältere Personen auf ihrem Festnetzanschluss angerufen. Nach Vorspiegelung eines Verwandtschaftsverhältnisses und Schilderung einer akuten Notlage bittet der Anrufer um die kurzfristige Überlassung einer größeren Geldsumme. Die Opfer werden hierbei von den professionellen Tätern derart unter Druck gesetzt, dass sie sich dieser „Bitte“ häufig nicht entziehen können. Dieser Betrag - bei dem es sich in der Regel um sämtliche Ersparnisse des Opfers handelt - wird in der Folge durch einen der Täter bei dem Opfer persönlich abgeholt. Auch in diesen Fällen stellt die Nummer des Anrufers in der ganz überwiegenden Anzahl der Fälle den einzigen Ermittlungsansatz dar. Da die Daten, wenn überhaupt, nur für wenige Tage gespeichert werden, die Strafanzeige durch das Opfer indes oft erst mehrere Tage nach der Tat erfolgt, müssen die Ermittlungen eingestellt werden.

Trotz der verharmlosenden Bezeichnung „Enkeltrick“ handelt es sich hierbei nicht um eine Bagatelltat: Ungeachtet dessen, dass die Täter ihre Opfer regelmäßig finanziell vollständig ruinieren, erfolgt der „Enkeltrick“ nach Erkenntnissen der Strafverfolgungsbehörden durch straff gegliederte Täterorganisationen, die nicht nur bundesweit, sondern europaweit agiert und dem organisierten Verbrechen zuzurechnen ist. Strafrechtlich handelt es sich nicht nur um eine Vielzahl von Fällen des besonders schweren Betruges, der mit Freiheitsstrafe bis zu zehn Jahre bestraft werden kann (§ 263

Abs. 3 Nr. 1 StGB), sondern um ein qualifiziertes Verbrechen, mit einer Mindestfreiheitsstrafe von einem Jahr (§ 263 Abs. 5 StGB).

Im Bereich der Verfolgung der organisierten Kriminalität hat der Wegfall der Vorratsdatenspeicherung insgesamt massive Auswirkungen; denn diese Art der Kriminalität lebt von der schnellen Kommunikation zur gemeinsamen Planung und arbeitsteiligen Begehung schwerer Straftaten. Durch die zum Teil nur kurzen Speicherfristen besteht insbesondere die Gefahr, dass aus der Auswertung retrograder Verkehrsdaten sich erschließende Zusammenhänge zwischen Einzeltaten, z. B. bei Serieneinbrüchen „reisender“ Tätergruppierungen, nicht erkannt und damit auch die hinter den Einzeltätern agierenden hauptverantwortlichen (OK-)Täter nicht mehr identifiziert und verfolgt werden.

Die niedersächsische Polizei hat für den Zeitraum vom 1. Juli 2010 bis zum 10. November 2010 eine interne Erhebung durchgeführt. Diese ergab, dass bei den - für diesen Zeitraum - 454 gemeldeten Straftaten, in denen es aus Ermittlungsgründen erforderlich gewesen wäre, die Verbindungsdaten zu erheben, 409 Taten gar nicht mehr bzw. nur noch unzureichend aufgeklärt werden konnten. Dieser Umstand belegt, dass für eine Vielzahl von Straftaten Verkehrsdaten den einzigen Ermittlungsansatz darstellen und nach Wegfall der sogenannten Vorratsdatenspeicherung nicht mehr bzw. nur wesentlich erschwert aufgeklärt werden können. Nur der Vollständigkeit halber wird darauf hingewiesen, dass Verkehrsdaten im Rahmen eines Strafverfahrens nicht nur belastend, sondern auch entlastend sein können.

Zu 6 und 7:

Da nicht § 113 TKG, sondern § 113 a TKG durch Urteil des BVerfG vom 2. März 2010 für verfassungswidrig erklärt wurde, wird davon ausgegangen, dass sich Frage 6 tatsächlich auf nach § 113 a TKG erhobene Daten bezieht.

Das BVerfG hat in dem Urteil vom 2. März 2010 entschieden, dass die aufgrund der einstweiligen Anordnungen vom 11. März 2008, 28. Oktober 2008 und 15. Oktober 2009 von den Telekommunikationsanbietern erhobenen, indes einstweilen nicht an die ersuchenden Behörden übermittelten Daten unverzüglich zu löschen sind und sie nicht an die ersuchenden Stellen übermittelt werden dürfen.

Der Landesregierung sind keine Fälle bekannt, in denen dieser Anordnung des BVerfG zuwider gehandelt wurde und nach § 113 a TKG erhobene, bisher indes nach Maßgabe der einstweiligen Anordnungen gesicherte Daten an die Strafverfolgungsbehörden übermittelt wurden. Auch sind keine Fälle bekannt, in denen nach der Verkündung des Urteils des BVerfG noch nach § 113 a TKG gespeicherte Daten erhoben wurden.

Nicht angeordnet oder ausgeführt hat das BVerfG indes, wie mit den Vorratsdaten umzugehen ist, die entweder in der Zeit vom 1. Januar 2008 bis zur ersten einstweiligen Anordnung vom 11. März 2008 aufgrund § 113 b TKG oder in der Zeit vom 11. März 2008 bis 2. März 2010 aufgrund der einstweiligen Anordnungen zulässigerweise an die ersuchenden Behörden übermittelt worden sind. In den einstweiligen Anordnungen hatte das BVerfG wiederholt angeordnet, dass Anbieter von Telekommunikationsdiensten verpflichtet seien, gemäß § 100 g Abs. 1 StPO Verkehrsdaten im Sinne des § 113 a TKG an die ersuchende Behörde zu übermitteln, wenn Gegenstand des Ermittlungsverfahrens eine Katalogtat im Sinne des § 100 a Abs. 2 StPO sei und die Voraussetzungen des § 100 a Abs. 1 StPO vorlägen.

Soweit Verfahren bereits rechtskräftig abgeschlossen wurden, in denen die Verurteilung auf nach § 113 b TKG übermittelten Vorratsdaten beruht, scheidet eine Wiederaufnahme des Verfahrens gemäß § 79 Abs. 1 BVerfGG und den §§ 359 ff. StPO aus, weil keine Vorschrift des materiellen Strafrechts betroffen ist. Auch greift das Vollstreckungsverbot nach § 79 Abs. 2 Satz 2 BVerfGG nicht hinsichtlich der rechtskräftigen Strafurteile, sondern nur der noch nicht vollstreckten Beschlüsse nach § 100 g Abs. 1 StPO und § 113 a TKG.

In laufenden Ermittlungs- und Strafverfahren ist hinsichtlich nach § 113 a TKG erhobener und übermittelter Daten von folgender Rechtslage auszugehen:

Zumindest in den Fällen, in denen die betreffenden Verfahren eine im Einzelfall schwerwiegende Straftat aus dem Katalog des § 100 a Abs. 2 StPO zum Gegenstand haben, ist ein Beweisverwertungsverbot hinsichtlich Vorratsdaten, die nach Maßgabe der einstweiligen Anordnungen übermit-

telt wurden, nicht anzunehmen. Da sich die Ermittlungsbehörden in diesen Fällen an die Vorgaben des Bundesverfassungsgerichts in dessen einstweiligen Anordnungen gehalten haben, kann von einer fehlerhaften, vorsätzlichen oder auch nur grob fahrlässigen Vorgehensweise bei der Erlangung der Daten keine Rede sein. Den einstweiligen Anordnungen kommt legitimierende Kraft zu, welche sie nicht mit der Entscheidung in der Hauptsache verlieren (vgl. Maunz/Schmidt-Bleibtreu/Klein/Bethge, BVerfGG, § 32 Rdnr. 8; so auch OLG Hamm, Beschluss vom 13. April 2010 - 3 Ws 156/10 -; Schleswig-Holsteinisches OLG vom 30. März 2010 - 1 Ws 228/10 -).

Bei Ermittlungs- und Strafverfahren wegen des Verdachts einer Katalogtat nach § 100 a Abs. 2 StPO überwiegt zudem das Interesse an einer effektiven Strafverfolgung bei der Aufklärung schwerwiegender Straftaten. In diesen Fällen ist auch für in der Zeit vom 1. Januar 2008 bis 11. März 2008 - und damit vor Erlass der ersten einstweiligen Anordnung - gemäß § 113 a TKG gespeicherten und gemäß § 113 b TKG übermittelten Daten kein Verwertungsverbot anzunehmen.

Höchstrichterliche Rechtsprechung liegt derzeit zu dieser Frage noch nicht vor.

Das OLG Hamm hat jedoch am 13. April 2010 (3 Ws 140/10) entschieden, dass entsprechend erhobene Daten verwandt werden dürfen. Derzeit liegen zwei Verfahren aus Niedersachsen dem Bundesgerichtshof zur Entscheidung vor, in denen die Frage der Verwendung entsprechend erhobener Daten eine Rolle spielt. Die Entscheidungen des Bundesgerichtshofes bleiben abzuwarten.

Für die Übermittlung von nach § 113 a TKG erhobenen Daten an die niedersächsische Verfassungsschutzbehörde ist von folgender Rechtslage auszugehen:

Mit der einstweiligen Anordnung vom 28. Oktober 2008 hat das Bundesverfassungsgericht u. a. auch die Voraussetzungen für eine Übermittlung an die Verfassungsschutzbehörden formuliert. Danach sollte eine Übermittlung von Daten vorläufig hinnehmbar sein, wenn die Voraussetzungen für die Einleitung einer Beschränkungsmaßnahme nach dem Artikel-10-Gesetz (§ 1 Abs. 1 und § 3 des Artikel-10-Gesetzes) vorliegen. Diese Festlegungen des Bundesverfassungsgerichts haben Eingang in die gesetzliche Regelung des § 5 a Abs. 6 NVerfSchG gefunden.

Zu 8:

Hierzu wird zunächst auf die Antwort zu Frage 5 verwiesen.

Es liegen keine Anhaltspunkte dafür vor, dass eine eventuelle Überarbeitung der EU-Richtlinie einer Neuregelung der Vorratsdatenspeicherung in Deutschland entgegenstehen könnte. Selbst wenn die EU-Kommission zu einer Überarbeitung käme, stehen keine weitergehenden Restriktionen zu erwarten als diejenigen, die das Bundesverfassungsgericht vorgegeben hat.

Zu 9 und 10:

Die Niedersächsische Landesregierung setzt sich stets dafür ein, dass Ermittlungsmethoden sowohl effektiv als auch schonend im Hinblick auf die Eingriffe in Grundrechte der Bürgerinnen und Bürger sind. Sinnvolle Alternativen zur vorsorglichen anlasslosen Datenspeicherung, welche vergleichbar effektive Aufklärungsmaßnahmen ermöglichen, gibt es indes nicht. Aus den unter Nr. 5 geschilderten Gründen stellt die - der aktuellen Rechtslage entsprechende - betrieblich veranlasste Datenspeicherung gemäß § 96 Abs. 1 TKG keine wirksame Alternative dar; denn anders als offenbar in den USA sind die Unternehmen ihrerseits zur Datensparsamkeit aufgefordert und dürfen nur solche Daten speichern, die sie für ihre betrieblichen Zwecke benötigen.

Aus diesem Grund kann in Deutschland auch das sogenannte Quick-Freeze-Verfahren die Vorratsdatenspeicherung nicht ersetzen. Mit Quick-Freeze („Schockfrosten“) wird ein Verfahren beschrieben, mit dem Telekommunikations-Verkehrsdaten für Zwecke der Strafverfolgung vorübergehend gesichert werden können. Dieses Verfahren wird standardmäßig in Ländern betrieben, in denen die Unternehmen für ihre eigenen Zwecke umfassend und dauerhaft Daten erfassen und speichern.

Will eine Strafverfolgungsbehörde (Polizei und Staatsanwaltschaft) auf diese Daten zugreifen, benötigt sie einen richterlichen Beschluss. Um zu verhindern, dass die Daten währenddessen gelöscht werden, können die Strafverfolger eine sogenannte Speicheranordnung erlassen. Durch die-

se Anordnung wird die routinemäßige Löschung der Daten unterbunden; die Daten werden gesichert („eingefroren“).

Sobald ein richterlicher Beschluss vorliegt, der die Nutzung der Daten erlaubt, werden sie der Strafverfolgungsbehörde ausgehändigt.

Dieses Vorgehen wird auch als quick freeze oder fast thaw bezeichnet.

Quick-Freeze hindert einzig die automatische Löschung von Daten, deren Erheblichkeit bereits bekannt ist, sofern dies den TKÜ-Unternehmen vorab mitgeteilt worden ist.

Diese Fallgestaltung ist jedoch die Ausnahme. Im Übrigen gilt hier: Daten, die von vornherein nicht gespeichert werden, können zudem auch nicht gesichert werden.

In Bezug auf die übliche Fallgestaltung, nämlich dass strafbare Handlungen erst einige Zeit nach ihrer Begehung entdeckt bzw. erst im Nachhinein bei den Strafverfolgungsbehörden angezeigt werden und folglich erst nach Ablauf einiger Wochen oder Monate die Bedeutung retrograder Daten erkannt wird, ist Quick-Freeze völlig belang- und wirkungslos.

Dass Quick-Freeze keine Alternative zur Vorratsdatenspeicherung ist, hat bereits das Bundesverfassungsgericht im Urteil vom 2. März 2010 (1 BvR 256/08, Rdnr. 208) selbst dargelegt:

„Eine vergleichbar effektive Aufklärungsmöglichkeit liegt insbesondere nicht im sogenannten Quick-Freeze-Verfahren, bei dem an die Stelle der anlasslos-generellen Speicherung der Telekommunikationsdaten eine Speicherung nur im Einzelfall und erst zu dem Zeitpunkt angeordnet wird, zu dem dazu etwa wegen eines bestimmten Tatverdachts konkreter Anlass besteht. Ein solches Verfahren, dass Daten aus der Zeit vor der Anordnung ihrer Speicherung nur erfassen kann, soweit sie noch vorhanden sind, ist nicht ebenso wirksam wie eine kontinuierliche Speicherung, die das Vorhandensein eines vollständigen Datenbestandes für die letzten sechs Monate gewährleistet.“

Gerade bei der Ermittlung des Nutzers einer dynamischen IP sind die hierzu erforderlichen Verkehrsdaten im Zeitpunkt der erstmaligen Kenntnis der Strafverfolgungsbehörden von der Straftat bei dem Telekommunikationsanbieter mangels betrieblicher Erfordernisse („Flatrate“-Verträge) bereits oftmals nicht (mehr) vorhanden, sodass auch das „Einfrieren“ der gewünschten Daten bis zur Erlangung eines richterlichen Beschlusses nicht greift.

Da man nur die Daten einfrieren kann, die man hat, kann Quick-Freeze keine Alternative zur Vorratsdatenspeicherung sein. Quick-Freeze gaukelt letztlich einen Zustand der Sicherheit vor, der weder existiert noch mit Hilfe von Quick-Freeze je erreicht werden kann.

Zu 11:

Aus den unter der Antwort zu Frage 5 dargestellten Gründen erscheint der Polizei, der Justiz und dem Verfassungsschutz eine anlasslose Speicherung der Daten notwendig, die zur zuverlässigen Rekonstruktion zurückliegender Telekommunikationsvorgänge einschließlich der Identifizierung der Kommunikationsteilnehmer, der zeitlichen Bestimmbarkeit der Kommunikation, der Form der Telekommunikation, der bei der Kommunikation verwendeten Anschlüsse und Geräte und des Standortes der Kommunikationsteilnehmer zum Zeitpunkt des Verbindungsaufbaus erforderlich sind.

Danach wären alle, bis zum Urteil des Bundesverfassungsgerichts, bevorrateten Daten im Rahmen einer Neuregelung zu speichern. Im Einzelnen handelt es sich dabei um folgende Daten:

Telefondienste:

– die Rufnummer oder andere Kennung des anrufenden und des angerufenen Anschlusses sowie im Falle von Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,

– den Beginn und das Ende der Verbindung nach Datum und Uhrzeit unter Angabe der zugrundeliegenden Zeitzone,

– in Fällen der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht die Zeitpunkte der Versendung und des Empfangs der Nachricht,

– in Fällen, in denen im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können, Angaben zu dem genutzten Dienst (beispielsweise Sprach-, Fax- oder Datenübertragung; SMS, MMS);

bei mobilen Telefondiensten zudem:

– die internationale Kennung für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss (International Mobile Subscriber Identity = IMSI),

– die internationale Kennung des anrufenden und des angerufenen Endgerätes (International Mobile Equipment Identity = IMEI),

– die Bezeichnung der durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzten Funkzellen (Standortdaten); dabei sind durch die Netzbetreiber auch Daten vorzuhalten, aus denen sich die geografischen Lagen der die jeweilige Funkzelle versorgenden Funkantennen sowie deren Hauptstrahlrichtungen ergeben,

– im Fall im Voraus bezahlter anonymer Dienste (Prepaid-Dienste) auch die erste Aktivierung des Dienstes nach Datum, Uhrzeit und Bezeichnung der Funkzelle;

bei Internet-Telefondiensten zudem:

– die Internetprotokoll-Adresse des anrufenden und des angerufenen Anschlusses;

E-Mail-Dienste:

– bei Versendung einer Nachricht die Kennung des elektronischen Postfachs und die Internetprotokoll-Adresse des Absenders sowie die Kennung des elektronischen Postfachs jedes Empfängers der Nachricht,

– bei Eingang einer Nachricht in einem elektronischen Postfach die Kennung des elektronischen Postfachs des Absenders und des Empfängers der Nachricht sowie die Internetprotokoll-Adresse der absendenden Telekommunikationsanlage,

– bei Zugriff auf das elektronische Postfach dessen Kennung und die Internetprotokoll-Adresse des Abrufenden,

– die Zeitpunkte der Versendung und des Eingangs der Nachricht und des Zugriffs auf das Postfach nach Datum und Uhrzeit unter Angabe der zugrundeliegenden Zeitzone;

Internetzugangsdienste:

– die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,

– eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt (Beispiel: Kennung des DSL-Anschlusses),

– den Beginn und das Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse nach Datum und Uhrzeit unter Angabe der zugrundeliegenden Zeitzone.

Dass dies zulässig wäre, ergibt sich bereits aus der Entscheidung des Bundesverfassungsgerichts.

Nach Ansicht von Staatsanwaltschaft, Polizei und Verfassungsschutz hat sich eine sechsmonatige Speicherfrist für die anlasslos gespeicherten Verkehrsdaten überwiegend bewährt. Die Erfahrungen der Behörden haben gezeigt, dass eine kürzere Speicherfrist gerade für Verfahren im Zusammenhang mit der Terrorismusbekämpfung, lang andauernder, bandenmäßig begangener Umfangsverfahren und insbesondere bei der Bekämpfung der Kinderpornografie nicht ausreichend wäre. Eine Neuregelung der Vorratsdatenspeicherung sollte daher auch im Lichte des Grundrechtsschutzes die Speicherungsdauer erneut - der Mindestspeicherungsdauer in Artikel 6 der Richtlinie 2006/24/EG entsprechend - auf sechs Monate festlegen.

Zu 12:

Zu dieser Frage kann mangels Erkenntnissen zur Höhe der entstehenden Kosten keine Bewertung abgegeben werden. Allerdings gibt es auch in anderen Bereichen wirtschaftlicher Betätigung kostenträchtige, zum Teil jahrelange Speicher- und Aufbewahrungspflichten, z. B. nach Handels- und

Steuerrecht. Die Netzbetreiber erhalten zudem für jede Auskunft gegenüber den Strafverfolgungsbehörden eine Kostenerstattung. Letztendlich kann und darf eine effektive Strafverfolgung nicht daran gemessen werden, ob sie mittelstandsfreundlich ist. Die nachhaltige Kriminalitätsbekämpfung ist selbstverständlich auch im Interesse des Mittelstandes, der hierfür natürlich auch seinen gesamtgesellschaftlichen Beitrag leisten wird.

Zu 13:

Eine belastbare Einschätzung der entstehenden Zusatzkosten für die Telekommunikationsunternehmen kann von hier ebenfalls nicht getroffen werden.

Bernd Busemann

(Ausgegeben am 07.12.2010)