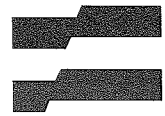
Ministerium für Justiz,
Arbeit und Europa
des Landes Schleswig-Holstein



Ministerium für Justiz, Arbeit und Europa
des Landes Schleswig-Holstein | Postfach 71 45 | 24171 Kiel

Vorsitzenden des
Innen- und Rechtsausschusses des
Schleswig-Holsteinischen Landtages
Herrn Werner Kalinka, MdL
Düsternbrooker Weg 70
24105 Kiel

Ihr Zeichen: /
Ihre Nachricht vom: /
Mein Zeichen: /
Meine Nachricht vom: /

Elisabeth Zimmermann
Elisabeth.Zimmermann@jumi.landsh.de
Telefon: 0431 988-38 06
Telefax: 0431 988-38 04

Schleswig-Holsteinischer Landtag
Umdruck 16/1153

25. August 2006

Vorratsdatenspeicherung von Telefon- und Internetverbindungen

Sehr geehrter Herr Vorsitzender,

am 01. März 2006 hatte der Innen- und Rechtsausschuss des Schleswig-Holsteinischen Landtages das Ministerium für Justiz, Arbeit und Europa gebeten, eine Stellungnahme, basierend auf dem Antrag der Fraktion der FDP, Keine Ausweitung der Vorratsdatenspeicherung von Telefon- und Internetverbindungen, Drucksache 16/472, abzugeben.

Anliegend übersende ich ein Eckpunkte-Papier der Landesregierung zur Umsetzung der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG mit der Bitte um Kenntnisnahme.

Mit freundlichen Grüßen

Uwe Döring
Minister

Anlage: Eckpunktepapier Vorratsdatenspeicherung

Eckpunkte-Papier der Landesregierung zur Umsetzung der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG

Die am 3. Mai 2006 in Kraft getretene (ABl. vom 13. April 2006, L 105/54) und an die Mitgliedstaaten gerichtete (Artikel 17)

> "Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG"

bedarf der Umsetzung in das nationale Recht. Denn im Gegensatz zu Verordnungen, die in allen Mitgliedstaaten der Europäischen Union (EU) unmittelbar und mit der gleichen Wirkung wie das nationale Recht selbst gelten, setzen Richtlinien dem nationalen Gesetzgeber lediglich einen Rahmen und eine Frist, innerhalb derer jeder Mitgliedstaat verpflichtet ist, sein Recht an die Richtlinie anzupassen und damit zur Harmonisierung der nationalen Rechtsordnungen beizutragen. Nach Artikel 249 Abs. 3 EGV ist die Richtlinie für jeden Mitgliedstaat "hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel".

Die Richtlinie muss gemäß Artikel 15 bis spätestens 15. September 2007 in das innerstaatliche Recht umgesetzt werden. Allerdings sind einige Ausnahmen zu beachten. So hat Deutschland z.B. von der Option in Artikel 15 Abs. 3 Gebrauch gemacht, wonach "jeder Mitgliedstaat die Anwendung dieser Richtlinie auf die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail aufschieben [kann]", und zwar bis 15. März 2009.

A. Ziel der Richtlinie

Die Mitgliedstaaten müssen - nach EU-weit einheitlichen Vorgaben - die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste und die Betreiber eines öffentlich zugänglichen Kommunikationsnetzes verpflichten, die in Telefonaten, SMS-Kurzmitteilungen und der Internetnutzung erzeugten Daten (Verkehrs- und Standortdaten sowie alle damit in Zusammenhang stehenden Daten, die zur Fest-

stellung des Teilnehmers oder Benutzers erforderlich sind, Artikel 2 Abs. 2 lit. a) zu erheben und für einen bestimmten Zeitraum zu speichern. Es sollen demnach nicht die Kommunikationsinhalte (Daten, die Aufschluss über den Inhalt einer Kommunikation geben) gespeichert werden (Artikel 5 Abs. 2), sondern vor allem die sog. **Verbindungsdaten**. Ziel ist, mit Hilfe der Informationen über Quelle und Adressaten sowie die Dauer der Verbindung die Gesprächspartner vor allem in Fällen, in denen es um schwere Kriminalitätsformen geht, zurückzuverfolgen, zu identifizieren und zu lokalisieren (Artikel 1).

B. Richtschnur für die Umsetzung der Richtlinie

Die Landesregierung wird sich im Bundesrat bei der Umsetzung der Richtlinie in das innerstaatliche Recht für eine strikte Wahrung des Verhältnismäßigkeitsgrundsatzes sowie für eine interessengerechte Lösung einsetzen, die sowohl sicherheits- und datenschutzrechtliche als auch wirtschafts- und haushaltspolitische Belange berücksichtigt und gegeneinander abwägt.

Bei der Umsetzung der Richtlinie sind vor allem die verfassungsrechtlichen Vorgaben des Bundesverfassungsgerichts zu beachten, insbesondere die Entscheidungen zur "Volkszählung" (BVerfGE 65, 1 ff.), zur "Handy-Überwachung" (E 107, 299 ff.), zum "Lauschangriff" (E 109, 279 ff.), zum niedersächsischen Gefahrenabwehrgesetz (Entscheidung vom 27. Juli 2005, Az: 1 BvR 668/04, NJW 2005, 2603 ff.) sowie aktuell zur "Beschlagnahme von Verbindungsdaten" (Entscheidung vom 2. März 2006, Az: 2 BvR 2099/04).

Die Entscheidungen des Bundesverfassungsgerichts enthalten zwar keine Festlegung auf bestimmte Speicherfristen bzw. auf die (Un-)Zulässigkeit der Speicherung bestimmter Datentypen, umschreiben jedoch das Spannungsverhältnis zwischen Datenschutz- und Verhältnismäßigkeitsgrundsätzen auf der einen und sicherheitspolitischen Bedürfnissen auf der anderen Seite.

Datenschutz/Verhältnismäßigkeit: Das Bundesverfassungsgericht verlangt für die Speicherung von Verbindungsdaten insbesondere unter Hinweis auf das Recht auf informationelle Selbstbestimmung (Artikel 1 Abs. 1 i.V.m. Artikel 2 Abs. 1 GG), das Fernmeldegeheimnis (Artikel 10 Abs. 1 Var. 3 GG), die Berufsfreiheit (Artikel 12 Abs. 1 GG) sowie die Meinungs-, Informations-, Rundfunk- und Pressefreiheit (Artikel 5 Abs. 1 GG) eine bereichsspezifische, präzise und normenklare Begrenzung des Eingriffs sowie eine strikte Wahrung des Verhältnismäßigkeitsgrundsatzes.
Dabei geht es vorrangig nicht um die Grundrechte der Unternehmen der Informations- und Telekommunikationsbranche (IuTK) selbst, sondern um die grundrechtliche

Stellung der Kommunikationspartner, welche das Unternehmen für Zwecke ihrer vertraulichen Kommunikation nutzen. Insoweit sind die Unternehmen "Grundrechtsmittler" ihrer (Fernsprech-)Kunden (vgl. E 107, 299 [313 f.]).

Bereits die **Erhebungen** der Verkehrsdaten der Telekommunikation und der Standortkennung wiegen nach Auffassung des Bundesverfassungsgerichts grundrechtlich schwer. Denn vom **Schutzbereich** des Artikel 10 GG ist neben dem Inhalt der Fernmeldekommunikation auch umfasst, ob, wann und wie oft zwischen welchen Personen oder Endeinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist (vgl. E 67, 157 [172], 85, 386 [396]). Auch insoweit darf der Staat - das hat das Bundesverfassungsgericht in der Handy-Überwachungs-Entscheidung betont - grundsätzlich keine Kenntnis nehmen.

Zweck des Fernmeldegeheimnisses ist, "die Bedingungen einer freien Telekommunikation aufrechtzuerhalten" (E 107, 299 [313]):

> "Die Nutzung des Kommunikationsmediums soll in allem vertraulich möglich sein (vgl. BVerfGE 100, 313 [358]). Mit der grundrechtlichen Verbürgung der Unverletzlichkeit des Fernmeldegeheimnisses soll vermieden werden, dass der Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen deswegen unterbleibt oder nach Form und Inhalt verändert verläuft, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen (vgl. BVerfGE 100, 313 [359])."

Die "Unbefangenheit des Kommunikationsaustauschs" und das "Vertrauen in den Schutz der Unzugänglichkeit der Telekommunikationsanlagen" müssten geschützt werden (E 107, 299 [313], vgl. ferner E 65, 1 [43], 100, 313 [381]).

Da der Grundrechtsschutz auch die Umstände des kommunikativen Kontakts umfasst, und zwar unabhängig davon, ob dieser schon begonnen hat, noch andauert oder schon beendet ist, kann er bereits vor dem konkreten Beginn eines Telefongesprächs beginnen, also wenn der Gesprächskontakt - mit oder ohne Erfolg - aufgebaut werden soll und dadurch Daten anfallen (vgl. E 85, 386 [396]; Bonner Kommentar/*Badura*, Artikel 10, RN 37).
Mehrfach verweist das Bundesverfassungsgericht darauf, dass die Erhebung und Auswertung von Verkehrs- und Standortdaten in zunehmendem Maße Rückschlüsse auf Interessen, Gewohnheiten und Neigungen der Nutzer ermöglichen kann (Erstel-

lung von **Bewegungsbildern** und **Persönlichkeitsprofilen**, siehe etwa E 107, 299 [318 ff.]).

Ein **Eingriff** in Artikel 10 GG liegt (erst dann) vor, wenn der Gesetzgeber Telekommunikationsunternehmen die Pflicht auferlegt, personenbezogene Daten über die näheren Umstände der Telekommunikation auf Vorrat zu speichern und für den Abruf durch staatliche Behörden verfügbar zu halten. Nach dem modernen Eingriffsbegriff schützen die speziellen Grundrechte auch vor **mittelbaren Eingriffen** durch staatliche Maßnahmen, welche die Beeinträchtigung eines grundrechtlich geschützten Verhaltens typischerweise und vorhersehbar zur Folge haben oder die eine besondere Beeinträchtigungsgefahr in sich bergen, die sich jederzeit verwirklichen kann (vgl. E 100, 313 [366]; ferner BVerwGE 119, 123 [126 f.] für eine Pflicht zur generellen Speicherung von Telekommunikations-Bestandsdaten unter dem Aspekt des Grundrechts auf informationelle Selbstbestimmung).

Derartige Eingriffe mögen weniger schwer wiegen als solche, bei denen durch Abhörmaßnahmen auch der Inhalt der Gespräche aufgezeichnet wird. Doch betont das Bundesverfassungsgericht gerade auch die Bedeutung einer staatlichen Kenntnisnahme von den Umständen der Kommunikation. Das in Artikel 10 GG statuierte Fernemeldegeheimnis kompensiere die fehlende Möglichkeit der Beteiligten, durch gemeinsame Wahl des Ortes und der Umstände ihres Kontakts über dessen Vertraulichkeit zu disponieren, und soll stattdessen die Bedingungen einer "Vertraulichkeit auf Distanz" technisch und medial verbürgen (siehe dazu *Gusy*, NStZ 2003, 399 [403]).

Grundrechtlich bedeutsam ist ferner die **große Streubreite** der Eingriffe. Bereits die **Erhebung**, erst recht aber die **Übermittlung** der Verbindungsdaten an die Strafverfolgungsbehörden trifft eine große Zahl von Personen, nämlich alle, zu denen in dem betreffenden Zeitraum Telekommunikationsverbindungen hergestellt worden sind. Erfasst sind nicht nur potenzielle 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.

Das Gewicht ihrer Beeinträchtigung hängt nach Ansicht des Bundesverfassungsgerichts (E 107, 299 [320]) davon ab,

> "ob die Gesprächsteilnehmer als Personen anonym bleiben, welche Umstände der Kommunikation erfasst werden und welche Nachteile den Ge-

sprächsteilnehmern auf Grund der Überwachungsmaßnahmen drohen oder von ihnen nicht ohne jeden Grund befürchtet werden (vgl. E 100, 313 [376])."

Sowohl das Fernmeldegeheimnis als auch das Recht auf informationelle Selbstbestimmung werden jedoch **nicht vorbehaltlos** gewährt. Nach Artikel 10 Abs. 2 S. 1 GG dürfen Beschränkungen des Fernmeldegeheimnisses auf Grund eines Gesetzes angeordnet werden. Das Recht auf informationelle Selbstbestimmung darf durch die verfassungsmäßige Ordnung, also durch jede verfassungsmäßige Rechtsnorm eingeschränkt werden (Artikel 2 Abs. 1 GG). Aus dem Verhältnismäßigkeitsprinzip und den betroffenen Grundrechten selbst folgen jedoch besondere Anforderungen, die dass Bundesverfassungsgericht zu Zwecken des effektiven Grundrechtsschutzes an Gesetze stellt, welche Eingriffe in die Grundrechte erlauben.

Sicherheit: Das Bundesverfassungsgericht hat zwar wiederholt festgestellt, dass eine Erhebung personenbezogener Daten "auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken" verfassungswidrig sei (E 100, 313 [359 f.]; 65, 1 [46]), allerdings hat es eine Vorratsspeicherung von Daten nicht generell verboten. Schon heute dürfen innerhalb bestimmter Grenzen Strafverfolgungsbehörden (§§ 81b Var. 2, 484 StPO) und Gefahrenabwehrbehörden personenbezogene Daten "auf Vorrat" zur zukünftigen Erleichterung ihrer und der Arbeit anderer Behörden speichern, beispielsweise Daten aus dem Bundeszentralregister (§§ 492 ff. StPO; dazu BVerfG StV 1991, 556 [556 f.]). In neuerer Zeit hat das Bundesverfassungsgericht auch die Regelung des § 81g StPO für verfassungsgemäß erklärt, wonach "personenbezogene DNA-Identifizierungsmuster" festgestellt und gespeichert werden dürfen, wobei eine Verwendung der Daten auch zur Gefahrenabwehr und zur Gewährung internationaler Rechtshilfe zulässig ist (vgl. §§ 8 Abs. 6, 14 BKA-Gesetz; dazu E 103, 21 ff., insbesondere 35).

Das Bundesverfassungsgericht hat zudem wiederholt die unabweisbaren Bedürfnisse einer wirksamen Strafverfolgung betont, das öffentliche Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren hervorgehoben und die wirksame Aufklärung gerade schwerer Straftaten als einen wesentlichen Auftrag eines rechtsstaatlichen Gemeinwesens bezeichnet (vgl. E 29, 183 [194], 77, 65 [76], 80, 367 [375], 100, 313 [388 f.]). In der "Handy-Überwachungs-Entscheidung" haben die Karlsruher Richter - unter Hinweis auf den Gesetzesvorbehalt in Artikel 10 Abs. 2 GG - betont, dass die §§ 100g und 100 h StPO einen **legitimen Zweck** verfolgen, nämlich die Aufklärung und Verfolgung schwerer Straftaten (E 107, 299 [316]).

Insbesondere bei der Beschaffung von Beweismitteln für tatbestandsmäßiges Verhalten, zur Bestimmung des Standorts eines Beschuldigten und zur Abklärung, ob und bezüglich welcher Personen eine Telekommunikationsüberwachung Erfolg ver-

sprechend erscheint, ist die Auskunftsanordnung - auch nach Auffassung des Bundesverfassungsgerichts (E 107, 299 [316]) - "ein wirkungsvolles Ermittlungsinstrument". Ihre Eignung unterliegt danach "keinen Zweifeln, wenn Auskunftsverlangen mit dem Ziel angeordnet werden, den Aufenthaltsort eines Beschuldigten in Erfahrung zu bringen".

Um insbesondere die Aufklärung schwerer Straftaten organisierter Kriminalität, bei gewerbsmäßiger Hehlerei, Raub, räuberischer Erpressung, Bandendiebstahl und die von Terrorakten zu ermöglichen oder nachhaltig zu verbessern, ist - auch nach Auffassung der staatsanwaltschaftlichen Praxis in Schleswig-Holstein - die Speicherung eines gewissen Umfangs von Daten ebenso unerlässlich wie eine Speicherfrist, die einen sachgerechten Zeitraum für Ermittlungsansätze eröffnet.

Bei Ermittlungen in Strafverfahren sind die Daten über die Nutzung elektronischer Kommunikationsmittel wichtiges und häufig einziges Beweismittel bzw. liefern wichtige Ermittlungsansätze:

- Telefon: Durch Speicherung der Verbindungsdaten ergeben sich Ermittlungsansätze für geführte Gespräche (z.B. Rückschlüsse von Telefonanschlüssen auf Gesprächsteilnehmer, Zeitraum und -punkt der geführten Gespräche)
- Mobiltelefone: Die Speicherung der Standortdaten zu Beginn eines Gesprächs kann wichtige Hinweise zum Standortbestimmung eines Nutzers liefern, z.B. bei Geiselnahmen)
- Internet: Durch Identifizierung von gespeicherten Benutzernamen und IP-Adressen ergeben sich Ermittlungsansätze zur Identifizierung möglicher weiterer Mittäter (z.B. in Fällen des Verbreitens pornographischer Schriften nach § 184b Abs. 3 StGB).

Bislang sind die Strafverfolgungsbehörden darauf angewiesen, dass die Daten von den Unternehmen überhaupt zu Abrechnungszwecken gespeichert werden und bei der Abfrage noch vorhanden sind (in der Praxis werden die Daten derzeit durchschnittlich für ca. 80 bis 90 Tage gespeichert).

Des Weiteren sind bei der Umsetzung der Richtlinie in das innerstaatliche Recht wirtschafts- und haushaltspolitische Belange zu berücksichtigen.

Wirtschaft/Haushalt: Die Umsetzung der Richtlinie in das innerstaatliche Recht wird für die Informations- und Telekommunikationsbranche Zusatzkosten verursachen, insbesondere aufgrund des erforderlichen zusätzlichen technischen Aufwandes (Vorhalten eines höheren Speichervolumens). Da die Höhe der Zusatzkosten u.a. von den Speicherfristen und den Datentypen, die gespeichert werden müssen, ab-

hängig ist (je länger die Speicherfristen sind und je umfangreicher die Liste der Datentypen ist, die gespeichert werden müssen, umso höhere Kosten entstehen den jeweiligen Anbietern und Betreibern), wird die Landesregierung auch aus diesem Grund im Bundesrat insbesondere darauf hinwirken, die Speicherfristen möglichst kurz zu fassen.

Ferner wird die Landesregierung darauf hinwirken, zusätzliche Belastungen für die öffentlichen Haushalte zu vermeiden.

C. Erarbeitung eines Gesamtkonzepts

Die Landesregierung wird sich im Bundesrat dafür einsetzen, dass sich die Umsetzung der Richtlinie in das innerstaatliche Recht maßgeblich an den Vorgaben des Bundestages orientiert.

Dieser hat die Bundesregierung in seiner Stellungnahme Ende Februar 2006 (BT-Drs. 16/545 und 16/690) aufgefordert, "alsbald" einen Gesetzentwurf zur gebotenen Umsetzung der Richtlinie in das innerstaatliche Recht vorzulegen, "dessen Regelungen sich in das für Mitte 2007 angekündigte 'harmonische Gesamtsystem' der verdeckten strafprozessualen Ermittlungsbefugnisse einfügen" müssen.

Hintergrund: Damit soll die Umsetzung der Richtlinie in das innerstaatliche Recht, insbesondere die Überarbeitung der §§ 100g und 100h StPO, die bereits jetzt den Zugang der Strafverfolgungsbehörden zu den bei den Telekommunikationsunternehmen zu Abrechnungszwecken gespeicherten Daten ermöglichen, mit dem Vorhaben verknüpft werden - entsprechend RN 5911-5916 des Koalitionsvertrages zwischen CDU/CSU und SPD vom 11. November 2005 - "die Regelungen zur Telekommunikationsüberwachung in der Strafprozessordnung zu überarbeiten". Kernpunkte des Vorhabens sind mögliche **Änderungen im Bereich der Telefonüberwachung** aufgrund der Vorgaben des Bundesverfassungsgerichts im Urteil vom 3. März 2004 zur akustischen Wohnraumüberwachung (E 109, 279 ff.), wie z.B. die Notwendigkeit der **Kompensation** der wesentlichen Schwächung des Grundrechtsschutzes aufgrund heimlicher Ermittlungsmethoden durch besondere verfahrensrechtliche Gestaltungen.

Ferner ist in diesem Zusammenhang zu beachten, dass die §§ 100g und 100h StPO zum 1. Januar 2008 außer Kraft treten ("sunset-law"), da insbesondere hinsichtlich der Berücksichtigung der **Zeugnisverweigerungsrechte** für alle heimlichen Ermittlungsmaßnahmen ein Gesamtkonzept erarbeitet werden soll (Art. 2, Art. 4 Satz 2 des Gesetzes zur Änderung der Strafprozessordnung vom 20. Dezember 2001 [BGBl. I S. 3879], geändert durch Art. 1 des Gesetzes zur Verlängerung der Gel-

tungsdauer der §§ 100g, 100h StPO vom 9. Dezember 2004 [BGBl. I S. 3231] und durch Art. 4 des Gesetzes zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004 (akustische Wohnraumüberwachung) vom 24. Juni 2005 [BGBl. I S. 1841]; siehe dazu auch Entschließung des Bundestages vom 21. Oktober 2004, in dem die Bundesregierung aufgefordert wird, dem Bundestag bis zum 30. Juni 2007 einen Erfahrungsbericht über die praktische Umsetzung der §§ 100g und 100h StPO seit deren Einführung vorzulegen, siehe Ergänzung zu BR-Drs. 845/04 B).

Die geplanten Neuregelungen werden zudem durch ein **Gutachten** des Freiburger Max-Planck-Instituts für ausländisches und internationales Strafrecht ("Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100 h StPO"), das 2007 veröffentlicht werden soll, wissenschaftlich vorbereitet bzw. begleitet.

D. Position der Landesregierung zu zentralen Bestimmungen der Richtlinie

Die Landesregierung wird sich im Bundesrat dafür einsetzen, den Eingriff für die Bürgerinnen und Bürger wie auch für die IuTK-Unternehmen so gering wie möglich zu halten. Daher sollte sich die Umsetzung der Richtlinie in das innerstaatliche Recht maßgeblich an den Vorgaben des Bundestages orientieren (Drs. 16/545 und 16/690). Das Gesetz zur gebotenen Umsetzung der Richtlinie müsse insbesondere die folgenden Punkte berücksichtigen:

- Es werden "hinsichtlich der Speicherungsdauer und der erfassten Datenarten keine über die Mindestanforderungen der Richtlinien hinausgehenden Pflichten geregelt; dies gilt insbesondere für die Speicherungsfrist von 6 Monaten und die Beschränkung der Datenabfrage zu Zwecken der Strafverfolgung auf die Ermittlung, Aufdeckung und Verfolgung erheblicher oder mittels Telekommunikation begangener Straftaten",
- mit dem Gesetz ist zugleich sicherzustellen, "dass Daten, die über den Inhalt einer Kommunikation Aufschluss geben, wie bisher nicht gespeichert werden dürfen".

(1) Verpflichtungen der IuTK-Unternehmen

(a) Speicherfristen

Derzeitige Rechtslage

Das Rechtsinstrument der gezielten Vorratsspeicherung von Telekommunikationsdaten zu Strafverfolgungszwecken ist dem deutschen Recht zwar bislang fremd, die Speicherung von Telekommunikationsdaten als solche hingegen nicht. Bereits heute

sieht das Telekommunikationsgesetz (TKG) die Speicherung von Kommunikationsdaten beispielsweise zur Entgeltabrechnung vor.

Das bundesdeutsche Recht enthält im TKG eine allgemeine Speicherungsberechtigung der Unternehmen nur hinsichtlich der sog. Bestandsdaten (Kundendaten, § 95 Abs. 1 S. 1 TKG), während die Speicherung von Telekommunikationsverkehrs- und -standortdaten bislang lediglich als **zeitlich eng beschränkte Befugnis** der Telekommunikationsunternehmen ausgestaltet ist (Artikel 96 ff. TKG).
Auf diese Daten kann auf der Grundlage der §§ 100g und 100h StPO auch bisher schon zugegriffen werden. Der Auskunftsanspruch ist u.a. an einen qualifizierten Verdacht und an Katalogtaten gebunden (§ 100g Abs. 1 S. 1 StPO) und betrifft die Verbindungsdaten des Beschuldigten und des Nachrichtenmittlers (Abs. 1 S. 2 StPO). Für Geistliche, Verteidiger und Abgeordnete statuiert § 100h Abs. 2 ein (weitreichendes) Erhebungs- und Verwertungsverbot. § 100g StPO beschränkt die Informationserhebung nicht auf Verbindungsdaten aus der Vergangenheit, sondern ermöglicht auch die Auskunft über zukünftige Telekommunikationsverbindungen (§ 100g Abs. 1 S. 3 StPO).

Ferner können Telekommunikationsverbindungsdaten nach Maßgabe von

- § 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel-10-Gesetz, G-10),
- § 23a Abs. 8 des Zollfahndungsdienstegesetzes (ZFdG),
- § 8 Abs. 8 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (BVerfSchG),
- § 8 Abs. 3a des Gesetzes über den Bundesnachrichtendienst (BNDG),
- § 10 Abs. 3 des Gesetzes über den militärischen Abschirmdienst (MADG) und
- soweit darin vorgesehen: der Polizeigesetze der Länder

erhoben werden.

Gestaltungsspielraum nach der Richtlinie
Die Mitgliedsstaaten müssen den Telekommunikationsanbietern eine Speicherungsfrist von mindestens 6 und maximal 24 Monaten ab dem Zeitpunkt der Kommunikation für im Einzelnen aufgeführte Datenkategorien auferlegen (Artikel 6).

Position der Landesregierung
Angesichts der besonderen Bedeutung von Telekommunikationsverkehrs- und -standortdaten für eine wirksame Strafverfolgung auf der einen Seite und der notwendigen, aber auch hinreichenden Speicherungsfrist von (einheitlich) 6 Monaten

spricht sich die Landesregierung dafür aus, den Vorgaben des Bundestages grundsätzlich zu folgen.

(b) Datentypen - Kategorien von auf Vorrat zu speichernden Daten

Derzeitige Rechtslage

Die von der Auskunft umfassten Verbindungsdaten sind in § 100g Abs. 3 StPO abschließend aufgezählt: Telekommunikationsverbindungsdaten sind (Nr. 1) im Falle einer Verbindung Berechtigungskennungen, Kartennummern, Standortkennung sowie Rufnummer oder Kennung des anrufenden und angerufenen Anschlusses oder der Endeinrichtung, (Nr. 2) Beginn und Ende der Verbindung nach Datum und Uhrzeit, (Nr. 3) vom Kunden in Anspruch genommene Telekommunikationsdienstleistung, (Nr. 4) Endpunkte festgeschalteter Verbindungen, ihr Beginn und ihr Ende nach Datum und Uhrzeit.

Das Wort "oder" in Abs. 3 Nr. 1 ist nicht i.S.v. "entweder oder" zu verstehen; es kann auch Auskunft über alle dort genannten Verbindungsdaten verlangt werden. Eine Ausdehnung des Auskunftsanspruchs aus § 100g StPO auf Teledienstenutzungsdaten hatte der Gesetzgeber abgelehnt (BT-Drs. 14/7679 S. 7).

Der Gesetzgeber hatte sich dafür entschieden, die **Standortkennung** bei der Telekommunikationsauskunft (TKA) (anders als bei der Telefonüberwachung nach § 100a StPO) nur im Falle einer **Verbindung** zu gestatten: In § 100 g Abs. 3 Nr. 1 StPO wird auch die Standortkennung unter den Begriff der "Telekommunikationsverbindungsdaten" gefasst, allerdings unter der Einschränkung "im Falle einer Verbindung" sowie bezogen auf den "anrufenden und angerufenen Anschluss oder die Endeinrichtung". Verbindungsdaten nach § 100g Abs. 3 Nr. 1 StPO, die über Aktivmeldungen lediglich im Stand-by-Betrieb anfallen, sind damit bisher ausdrücklich ausgeschlossen.

Die in Abs. 3 Nr. 1 genannte **Kennung** erfasst die Gerätekennung (IMEI), die Teilnehmeridentifikationsnummer (IMSI) und die (auch temporäre) IP-Adresse von Computern. Nicht von der TKA erfasst werden hingegen Auskünfte über den Namen einer "hinter einer" IP-Adresse oder E-Mail-Adresse stehenden Person. Solche Daten sind (auch bei temporären IP-Adressen) jedoch Bestandsdaten i.S.d. § 3 Nr. 3 TKG, die nach § 111 TKG abgefragt werden können (vgl. BT-Drs. 14/7008 S. 7).

Nach § 113 Abs. 1 TKG sind die Diensteanbieter verpflichtet, den Strafverfolgungsbehörden **Auskunft über ihre Bestandsdaten** zu geben. Daneben kann die Aus-

kunft nach § 112 TKG über die Regulierungsbehörde im automatisierten Verfahren - hier ausdrücklich unentgeltlich (Abs. 5 S. 3) - erfolgen.

Verpflichtung aus der Richtlinie
Kategorien von auf Vorrat zu speichernden Daten enthält Artikel 5, und zwar jeweils differenziert nach Telefonfestnetz- und Mobilfunkdaten sowie solchen, die beim Internetzugang, beim Internet-E-Mail und bei der Internet-Telefonie anfallen sowie nach Daten, die benötigt werden

- zur Rückverfolgung und Identifizierung der Quelle einer Nachricht,
- zur Identifizierung des Adressaten einer Nachricht,
- zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung,
- zur Bestimmung der Art einer Nachrichtenübermittlung,
- zur Bestimmung der Endeinrichtung oder der vorgeblichen Endeinrichtung von Benutzern sowie
- zur Bestimmung des Standorts mobiler Geräte.

Gestaltungsspielraum nach der Richtlinie
Zur Wahrung der Verhältnismäßigkeit (insbesondere unter Berücksichtigung der Eingriffsintensität in das Grundrecht auf informationelle Selbstbestimmung), aber auch um die Kosten für die Speicherung möglichst niedrig zu halten sind Verkehrsdaten von sog. **erfolglosen Anrufversuchen** (das sind Telefonanrufe, bei denen die Verbindungen erfolgreich aufgebaut wurden, aber unbeantwortet bleiben oder bei denen das Netzwerkmanagement eingegriffen hat, Artikel 2 Abs. 2 lit. f) in die Mindestspeicherungsfrist nur in den Fällen in die Verpflichtung einzubeziehen, in denen die Unternehmen diese Daten ohnehin speichern (Artikel 3 Abs. 2 S. 1 sowie Erwägungsgrund 12).

Nach der Richtlinie ist die Vorratsdatenspeicherung im Zusammenhang mit Anrufen, bei denen **keine Verbindung** zustande kommt, nicht erforderlich (Artikel 3 Abs. 2, S. 2).

Da Artikel 5 Abs. 1 lit. f der Richtlinie für die Bestimmung des Standorts mobiler Geräte nur die Standortkennung (Cell-ID) bei Beginn der **Verbindung** sowie Daten zur geographischen Ortung von Funkzellen durch Bezugnahme auf ihre Standortkennung (Cell-ID) während des Zeitraums, in dem die Vorratsspeicherung der Kommunikationsdaten erfolgt, auf Vorrat gespeichert werden müssen, lässt die Richtlinie die Frage offen, ob auch Verbindungsdaten, die über Aktivmeldungen lediglich im Standby-Betrieb anfallen, gespeichert werden können.

Position der Landesregierung

Die Landesregierung begrüßt, dass die Vorratsdatenspeicherung im Zusammenhang mit Anrufen, bei denen **keine Verbindung** zustande kommt, nicht erforderlich ist. Im Hinblick auf **erfolglose Anrufversuche** wird sich die Landesregierung im Bundesrat dafür einsetzen, an der derzeitigen Rechtslage festzuhalten.

(c) Löschungspflicht

Derzeitige Rechtslage

Die gespeicherten **Verkehrsdaten** dürfen nach § 96 Abs. 2 S. 1 TKG über das Ende der Verbindung hinaus nur verwendet werden, soweit sie zum Aufbau weiterer Verbindungen oder für die in den §§ 97, 99, 100 und 101 TKG genannten Zwecke erforderlich sind, also vor allem für die Entgeltermittlung nach § 97 TKG und den Einzelverbindungsnachweis nach § 99 TKG. In allen anderen Fällen sind nach § 96 Abs. 2 S. 2 TKG die Verkehrsdaten vom Diensteanbieter nach Beendigung der Verbindung unverzüglich, das heißt ohne schuldhaftes Zögern, zu löschen.

Diese Vorgabe des TKG hat das LG Darmstadt in einem erst vor kurzem verkündeten Urteil für die Erfassung und Speicherung von Verbindungsdaten im Zusammenhang mit einem Pauschaltarif (Flat Rate) für das Internet näher konturiert (Az: 25 S 118/2005). Danach müssen die Unternehmen die bei jeder Einwahl neu vergebene Internet-Adresse (IP-Adresse) eines Kunden sofort nach dem Ende der Verbindung löschen. Ferner darf der Internetanbieter nur diejenigen Verbindungsdaten seiner Kunden speichern, die er für die Rechnung benötigt. Das Gericht verbot dem Anbieter, das Volumen der übertragenen Daten zu erheben und zu speichern, weil dies zur Ausstellung von Rechnungen nicht nötig sei (Flat Rate). Dagegen ließ es die Speicherung von Anfangs- und Endzeit der Verbindung zu, weil dafür laut Vertrag unter bestimmten Umständen zusätzliche Kosten in Rechnung gestellt werden können.

Verpflichtung aus der Richtlinie

Alle Daten müssen am Ende der Vorratspeicherungsfrist vernichtet werden, mit Ausnahme jener Daten, die abgerufen und gesichert worden sind (Artikel 7 lit. d).

Position der Landesregierung

Die Landesregierung wird sich im Bundesrat dafür einsetzen, dass technische und organisatorische Vorkehrungen getroffen werden, damit die Datenerhebung und -verarbeitung auf das für den Erhebungszweck erforderliche Maß begrenzt wird.

(d) Sanktionen

Derzeitige Rechtslage

Die Anbieter von Telekommunikationsdiensten sind aufgrund der innerstaatlichen telekommunikationsrechtlichen Bestimmungen in Deutschland (§ 88 TKG) bereits nach geltender Rechtslage verpflichtet, die Daten, die sie für unternehmensinterne Zwecke speichern, vor unbefugtem Zugriff zu schützen. Dies gilt sowohl für Bestands- als auch für Verkehrs- und Standortdaten.

Gestaltungsspielraum nach der Richtlinie
Nach Artikel 7 der Richtlinie stellt jeder Mitgliedstaat sicher, dass die Anbieter und Betreiber "zumindest die folgenden Grundsätze der Datensicherheit einhalten: [...] in Bezug auf die Daten werden geeignete technische und organisatorische Maßnahmen getroffen, um die Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust oder zufällige Änderung, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung zu schützen".
Ferner müssen "geeignete technische und organisatorische Maßnahmen getroffen [werden], um sicherzustellen, dass der Zugang zu den Daten ausschließlich besonders ermächtigten Personen vorbehalten ist". Der vorsätzliche Zugang zu oder die vorsätzliche Übermittlung von auf Vorrat gespeicherten Daten sollen nach Artikel 13 Abs. 2 mit verwaltungs- und strafrechtlichen Sanktionen belegt werden, die "wirksam, verhältnismäßig und abschreckend" sind.
Durch Artikel 9 werden die Mitgliedstaaten verpflichtet, eine oder mehrere unabhängige Kontrollstellen zur Überprüfung der in Artikel 7 niedergelegten Grundsätze einzurichten.

Position der Landesregierung
Die Landesregierung wird im Bundesrat darauf hinwirken, den Missbrauchsmöglichkeiten mit einem hohen technischen Sicherheitsstandard zu begegnen.
Die Landesregierung ist skeptisch, ob darüber hinaus eine Verschärfung der bereits bestehenden verwaltungs- und strafrechtlichen Sanktionsregelungen erforderlich ist (§§ 43, 44 BDSG und § 44 LDSG-SH).

(2) Zugang der Strafverfolgungsbehörden zu den Daten
Der Zugang der Strafverfolgungsbehörden zu den Daten ist nach der Richtlinie **innerstaatlich** zu regeln, wobei der Grundsatz der Verhältnismäßigkeit, das Unionsrecht und das Völkerrecht, insbesondere die Europäische Menschenrechtskonvention, zu beachten sind (Artikel 4).

(a) Zweck der Speicherung

Derzeitige Rechtslage

Die TKA muss zur Untersuchung einer in § 100g Abs. 1 S. 1 StPO bezeichneten Katalogtat erforderlich sein. Das ist zum einen eine Straftat (einschließlich Versuch oder Vorbereitung) von erheblicher Bedeutung, insbesondere eine Katalogtat nach § 100a S. 1 StPO.

Die TKA ist darüber hinaus auch bei Straftaten - die jedoch nicht von erheblicher Bedeutung sein müssen - gestattet, die "mittels einer Endeinrichtung" begangen, versucht oder vorbereitet wurden. Dazu gehören insbesondere beleidigende Telefonanrufe ("Telefonterror") oder E-Mails (siehe BT-Drs. 14/7008 S. 7). Generell keine TKA gibt es bei Ordnungswidrigkeiten (§ 46 Abs. 3 S. 1 OWiG; siehe BT-Drs. 14/7008 S. 7).

Gestaltungsspielraum nach der Richtlinie

Der Zweck der Speicherung wird - ganz allgemein - auf die Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, beschränkt (Artikel 1 Abs. 1). Nach einer "Erklärung des Rates zu Artikel 1" vom 17. Februar 2006 (Dok. 5777/06, ADD 1 REV 1) haben die Mitgliedstaaten "bei der Definition des Begriffs 'schwere Straftat' im einzelstaatlichen Recht [...] die in Artikel 2 Absatz 2 des Rahmenbeschlusses des Rates über den Europäischen Haftbefehl (2002/584/JI) genannten Straftaten sowie Straftaten unter Einsatz von Telekommunikationseinrichtungen angemessen zu berücksichtigen".

Die in Artikel 2 Absatz 2 des Rahmenbeschlusses des Rates über den Europäischen Haftbefehl (2002/584/JI) genannten Straftaten umfassen insgesamt 32 Straftatbestände bzw. Kriminalitätsphänomene:

- Beteiligung an einer kriminellen Vereinigung
- Terrorismus
- Menschenhandel
- sexuelle Ausbeutung von Kindern und Kinderpornographie
- illegaler Handel mit Drogen und psychotropen Stoffen
- illegaler Handel mit Waffen, Munition und Sprengstoffen
- Korruption
- Betrugsdelikte, einschließlich Betrug zum Nachteil der finanziellen Interessen der Europäischen Gemeinschaften im Sinne des Übereinkommens vom 26. Juli 1995 über den Schutz der finanziellen Interessen der Europäischen Gemeinschaften
- Wäsche von Erträgen aus Straftaten

- Geldfälschung, einschließlich der Euro-Fälschung
- Cyberkriminalität
- Umweltkriminalität, einschließlich des illegalen Handels mit bedrohten Tierarten oder mit bedrohten Pflanzen- und Baumarten
- Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt
- vorsätzliche Tötung, schwere Körperverletzung
- illegaler Handel mit Organen und menschlichem Gewebe
- Entführung, Freiheitsberaubung und Geiselnahme
- Rassismus und Fremdenfeindlichkeit
- Diebstahl in organisierter Form oder mit Waffen
- illegaler Handel mit Kulturgütern, einschließlich Antiquitäten und Kunstgegenständen
- Betrug
- Erpressung und Schutzgelderpressung
- Nachahmung und Produktpiraterie
- Fälschung von amtlichen Dokumenten und Handel damit
- Fälschung von Zahlungsmitteln
- illegaler Handel mit Hormonen und anderen Wachstumsförderern
- illegaler Handel mit nuklearen und radioaktiven Substanzen
- Handel mit gestohlenen Kraftfahrzeugen
- Vergewaltigung
- Brandstiftung
- Verbrechen, die in die Zuständigkeit des Internationalen Strafgerichtshofs fallen
- Flugzeug- und Schiffsentführung
- Sabotage

Position der Landesregierung

Aufgrund des schwerwiegenden Eingriffs in das Fernmeldegeheimnis und mit Blick auf den Verhältnismäßigkeitsgrundsatz sowie das Zweckbindungsgebot wird sich die Landesregierung im Bundesrat für eine Begrenzung der Zugangsmöglichkeiten der Ermittlungsbehörden auf Verbindungsdaten einsetzen und auf eine Konkretisierung hinsichtlich der "Schwere" der Straftat hinwirken.

Denn aufgrund des schwerwiegenden Eingriffs in das Fernmeldegeheimnis ist im Rahmen der Rechtsgüterabwägung das "Gewicht des Strafverfolgungsinteresses" insbesondere von der Schwere und der Bedeutung der aufzuklärenden Straftat abhängig. Das Bundesverfassungsgericht hat in der "Handy-Überwachungs-Entscheidung" betont (siehe E 107, 299 [321]; ferner E 100, 313 [392 f.]), dass es

"insofern [...] verfassungsrechtlichen Anforderungen nicht [genügt], dass die Erfassung der Verbindungsdaten allgemein der Strafverfolgung dient. Vorausgesetzt sind vielmehr eine 'Straftat von erheblicher Bedeutung', ein konkreter Tatverdacht und eine hinreichend sichere Tatsachenbasis für die Annahme, dass der durch die Anordnung Betroffene als Nachrichtenmittler tätig wird."

Die derzeitige in § 100g StPO vorgenommene Begrenzung der Erhebung von Verbindungsdaten, insbesondere die Konkretisierung hinsichtlich der "Schwere" der Straftat, ist nach Ansicht des Bundesverfassungsgerichts ausreichend (E 107, 299 [321 f.]). Das Vorliegen einer Katalogtat im Sinne von 100a S. 1 StPO ist danach zwar nicht unbedingte Voraussetzung der Anordnung, aber als bedeutsamer Anwendungsfall für eine Straftat von erheblicher Bedeutung hervorgehoben worden und gebe deshalb einen Anhaltspunkt für die rechtliche Bewertung. Damit werde dem Umstand Rechnung getragen, dass die Offenlegung von Verbindungsdaten ein detailliertes Bild über Kommunikationsvorgänge und Aufenthaltsorte ermöglicht.
Durch die Orientierung an dem Begriff der Straftat von erheblicher Bedeutung und der Angabe von Regelbeispielen werde verdeutlicht, dass derartige Eingriffe nur bei Straftaten gerechtfertigt sind, denen der Gesetzgeber allgemein ein besonderes Gewicht beimisst (E 107, 299 [322]).

Die Landesregierung wird im Bundesrat bei der Erarbeitung eines "harmonischen Gesamtkonzepts" auf eine sorgfältige Prüfung hinwirken, ob und inwieweit der Anwendungsbereich der §§ 100g und 100h StPO modifiziert werden muss.

Die Landesregierung spricht sich dafür aus, im Rahmen der "angemessenen Berücksichtigung" der in Artikel 2 Absatz 2 des Rahmenbeschlusses des Rates über den Europäischen Haftbefehl (2002/584/JI) genannten Straftaten sowie solchen unter Einsatz von Telekommunikationseinrichtungen eine extensive Ausdehnung des Straftatenkatalogs nach §§ 100g Abs. 1 i.V.m. 100a StPO zu vermeiden.

(b) Verdachtsgrad

Derzeitige Rechtslage

Voraussetzung der Erhebung von Verbindungsdaten nach § 100g StPO ist ein konkreter Tatverdacht. Auf Grund bestimmter Tatsachen "muss anzunehmen sein, dass der Beschuldigte mit hinreichender Wahrscheinlichkeit Straftaten von erheblicher Bedeutung begangen hat" (vgl. E 107, 299 [322]).

Position der Landesregierung
An der derzeitigen Rechtslage (Erfordernis eines qualifizierten Verdachts) sollte nach Auffassung der Landesregierung festgehalten werden.

(c) Personenkreis
Derzeitige Rechtslage
§§ 100g Abs. 1 S. 2 i.V.m. 100a S. 2 StPO gestatten die TKA nur bei dem in § 100a genannten Personenkreis (Beschuldigter und Nachrichtenmittler, die allerdings noch nicht identifiziert sein müssen), nicht hingegen beim Zeugen.
Unerlässlich zur Beurteilung, ob diejenige Person, gegen die eine Anordnung erfolgt, als Nachrichtenmittler angesehen werden kann ist eine gesicherte Tatsachenbasis. Insofern verlangen die §§ 100a, 100b Abs. 1 S. 2 StPO, dass gegen andere Personen als den Beschuldigten Maßnahmen nur erfolgen dürfen, wenn auf Grund von bestimmten Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte den Anschluss nutzt. Entsprechend muss § 100g StPO "einengend ausgelegt werden" (E 107, 299 [323]). Bloße Vermutungen genügen danach für die Nachrichtenmittlereigenschaft nicht.

Position der Landesregierung
Die Landesregierung wird sich im Bundesrat dafür einsetzen, an der jetzigen Regelung festzuhalten.

(d) Subsidiaritätsklausel
Derzeitige Rechtslage
Das Auskunftsverlangen ist nachrangig gegenüber anderen Ermittlungsmaßnahmen (§ 100g Abs. 2 StPO). Mit dieser Subsidiaritätsklausel lockert das Gesetz nicht die Anforderungen, die die §§ 100g und 100h StPO an die erzwungene Offenbarung der Verbindungsdaten stellen.

Nach einer Entscheidung des Bundesverfassungsgerichts (vom 4. Februar 2005, Az: 2 BvR 308/04, RN 24) wäre es

> "mit dem sich aus Artikel 10 Abs. 2 GG ergebenden Erfordernis nach einer bereichsspezifischen, präzisen und normenklaren Begrenzung des Eingriffs nicht vereinbar, wenn die Ermittlungsbehörden auf eine andere Zwangsmaßnahme zurückgreifen könnten, an die geringere Anforderungen in Bezug auf das Anordnungsverfahren gestellt sind, um zum gleichen Ziel zu gelan-

gen, nämlich dem unfreiwilligen Offenbaren der durch Artikel 10 Abs. 1 GG geschützten Daten".

§ 100g Abs. 2 StPO könne daher so verstanden werden, dass ein Auskunftsverlangen unzulässig ist, wenn der fragliche Sachverhalt, etwa der Aufenthaltsort des Beschuldigten, durch andere Ermittlungsmaßnahmen, die nicht auf Telekommunikationsverbindungsdaten zugreifen, aufzuklären ist (vgl. auch E 107, 299 [317 f.]).

Position der Landesregierung
Die Landesregierung wird im Bundesrat darauf hinwirken, an der Subsidiaritätsklausel festzuhalten.

(e) Anordnungskompetenz
Derzeitige Rechtslage
Bezüglich der Anordnungskompetenz für die TKA verweist § 100h Abs. 1 S. 3 StPO auf die Regelung für die Telekommunikationsüberwachung (TÜ) nach § 100a in § 100b Abs. 1 StPO. Zuständig ist danach grundsätzlich der Richter, bei Gefahr im Verzug die Staatsanwaltschaft. Die Verweisung nimmt zudem auf § 100b Abs. 1 S. 3 StPO Bezug, wonach die Anordnung der Staatsanwaltschaft außer Kraft tritt, wenn sie nicht binnen drei Tagen vom Richter bestätigt wird.

Position der Landesregierung
Mit Blick auf die durch den Verhältnismäßigkeitsgrundsatz gebotene Abwägung der sich bei Eingriffen in das Fernmeldegeheimnis gegenüberstehenden Rechtspositionen ist es nach Ansicht der Landesregierung für die Umsetzung der Richtlinie in das innerstaatliche Recht unabdingbar, an dem Vorbehalt der richterlichen Entscheidung festzuhalten. Denn dieser zielt auf eine vorbeugende Kontrolle der Maßnahme durch eine persönlich und sachlich unabhängige und neutrale Instanz. Zur richterlichen Einzelentscheidung gehören eine sorgfältige Prüfung der Eingriffsvoraussetzungen und eine umfassende Abwägung zur Feststellung der Angemessenheit des Eingriffs im konkreten Fall. Die richterliche Anordnung des Eingriffs in das Fernmeldegeheimnis muss den Tatvorwurf so beschreiben, dass der äußere Rahmen abgesteckt wird, innerhalb dessen sich der Eingriff halten muss.

Vor dem Hintergrund der Maßgaben des Bundesverfassungsgerichts (siehe grundlegend E 103, 142 [151 ff.]; vgl. auch E 107, 299 [325]) sowie der vielfach in der Literatur geäußerten Kritik an der Effizienz des Richtervorbehalts (siehe etwa Gutachten des Freiburger MPI für ausländisches und internationales Strafrecht "Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b

StPO und anderer verdeckter Ermittlungsmaßnahmen, Freiburg 2003, S. 23 ff.; ferner *Backes/Gusy*, Wirksamkeitsbedingungen von Richtervorbehalten, 2003, passim) wird die Landesregierung im Rahmen der Einbindung der Umsetzung der Richtlinie in ein "harmonisches Gesamtsystem" der verdeckten Ermittlungsmaßnahmen auf eine Prüfung hinwirken, ob die Aufgabe und Pflicht des Ermittlungsrichters, sich im Rahmen einer Einzelfallprüfung eigenverantwortlich ein Urteil zu bilden und nicht etwa die Anträge der Staatsanwaltschaft auf Übermittlung der Verbindungsdaten nach einer nur pauschalen Überprüfung einfach gegenzuzeichnen, einer vergleichbaren Regelung wie in § 100d Abs. 2 und 3 StPO bedarf.

(f) Form und Inhalt der Anordnung

Derzeitige Rechtslage

Die Anordnung bedarf nach § 100h Abs. 1 S. 3 i.V.m. § 100b Abs. 2 S. 1 StPO der Schriftform. Sie muss Art, Umfang und Dauer - den zurückliegenden oder zukünftigen Zeitraum - der TKA bestimmen (§ 100h Abs. 1 S. 3 i.V.m. § 100b Abs. 2 S. 3 StPO). Bedient sich der in der Anordnung bezeichnete Diensteanbieter bei der Durchführung von Telekommunikationsverbindungen - etwa beim Roaming - weiterer Betreiber (quasi als Subunternehmer), so genügt die Anordnung gegen einen Diensteanbieter.

Bezüglich der Individualisierung des Betroffenen enthalten S. 1 und 2 des § 100h Abs. 1 StPO eine differenzierte Regelung. Nach Abs. 1 S. 1 muss die Anordnung der TKA bei Straftaten, die **nicht von erheblicher Bedeutung** sind, Namen und Anschrift des Betroffenen sowie die Rufnummer oder eine andere Kennung seines Anschlusses enthalten. Im Falle einer Straftat von **erheblicher Bedeutung** sind nach Abs. 1 S. 2 zwar geringere Individualisierungsmerkmale erforderlich, dafür gilt aber die strenge Subsidiaritätsklausel. Hier genügt eine räumlich und (i.S.v. kumulativ) zeitlich hinreichend bestimmte Begrenzung. Damit sind vor allem die Fälle gemeint, in denen Name und Anschrift des Betroffenen durch die TKA gerade erst ermittelt werden sollen, wie z.B. bei der **Funkzellenabfrage** (vgl. BGH NStZ 2002, 107 f.), bei der es um Telefonate geht, die ein unbekannter Täter während eines bestimmten Zeitraums aus einer bestimmten Funkzelle geführt hat (BT-Drs. 14/7258 S. 2, 4).

Position der Landesregierung

Die Landesregierung wird im Bundesrat darauf hinwirken, dass bei den zur Individualisierung geforderten Angaben eine Regelung gefunden wird, die den Bedürfnissen der Aufklärung von Straftaten insbesondere in den Fällen gerecht wird, die mittels des **Internet** begangen werden. Sowohl bei Straftaten von erheblicher Bedeutung als auch in anderen Fällen ist der Autor einer Homepage häufig nicht bekannt; ent-

sprechendes gilt für Chats mit strafbaren Äußerungen. Dies hat zur Folge, dass häufig keine hinreichend präzise räumliche und zeitliche Begrenzung möglich ist, zumal der Standort des Providers, auf dem die Homepage gespeichert ist, ebenso wie der Aufenthaltsort des Autors der Homepage, häufig nicht bekannt sind.
Da zudem kaum Angaben gemacht werden können, wann der Autor der Homepage diese erstellt hat, sollte eine Individualisierung ausreichen, soweit sie nach dem jeweiligen Stand der Technik möglich ist.

(g) Schutz bestimmter Personen-/Berufsgruppen

Derzeitige Rechtslage

Auf Empfehlung des Rechtsausschusses (BT-Drs. 14/7679 S. 9) wurden - nur für die TKA, nicht aber für die TÜ - in § 100h Abs. 2 StPO ein Beweiserhebungsverbot und ein weitreichendes Verwertungsverbot statuiert. Danach steht das Zeugnisverweigerungsrecht der Geistlichen, der Verteidiger sowie der Mitglieder gesetzgebender Körperschaften nach § 53 Abs. 1 Nr. 1, 2 und 4 StPO der Anordnung der Auskunft über Telekommunikationsverbindungen, die von dem oder zu dem zur Verweigerung des Zeugnisses Berechtigten hergestellt wurden, entgegen.

Das Erhebungs- und Verwertungsverbot gilt nicht bei dem **Verstrickungsverdacht** der Zeugnisverweigerungsberechtigten (also wenn diese einer Teilnahme, Begünstigung, Strafvereitelung oder Hehlerei verdächtig sind), wobei jedoch z.B. beim Verteidiger besondere Anforderungen an die Verstrickung zu stellen sind. Bei Abgeordneten greift in diesen Fällen der Immunitätsvorbehalt.

Zwar sind die Verbindungsdaten von deren **Berufshelfern** (§ 53a StPO) nicht geschützt. Soweit durch eine derartige TKA aber das Auskunftsverbot bei den privilegierten Berufsgeheimnisträgern umgangen wird, greift auch in diesen Fällen das Erhebungsverbot (vgl. auch § 100c Abs. 6 S. 2 StPO).

Bei den übrigen Berufsgeheimnisträgern ist eine **einschränkende Auslegung** geboten. In der "Handy-Überwachungs-Entscheidung" hat das Bundesverfassungsgericht z.B. die Bedeutung des Artikel 5 Abs. 1 S. 2 GG (Pressefreiheit) auch für die Fälle betont, in denen ein gesetzliches Zeugnisverweigerungsrecht nicht greift (E 107, 299 [334]; vgl. auch E 64, 108 [119 f.]; 77, 65 [81 f.]). Zwar folge aus Artikel 5 GG kein unmittelbar aus der Verfassung herleitbares generelles Zeugnisverweigerungsrecht. Die Karlsruher Richter weisen hingegen auf das Erfordernis hin, im Rahmen der Auslegung und Anwendung der jeweils betroffenen Normen der Ausstrahlungswirkung der Pressefreiheit Rechnung zu tragen. In diesem Sinne sei bei §§ 100g f. StPO die gesetzgeberische Entscheidung hinzunehmen, dass derartige Maßnahmen

auch gegen Journalisten angewandt werden dürfen. Im Rahmen der Verhältnismäßigkeitsprüfung seien aber die Besonderheiten des Einzelfalls zu berücksichtigen.

Position der Landesregierung
Nach Auffassung der Landesregierung war es aufgrund der verfassungsrechtlichen Vorgaben nicht erforderlich und technisch und wirtschaftlich praktisch auch nicht leistbar, in der Richtlinie Beschränkungen zum Schutz der Rechte bestimmter Berufsgeheimnisträger vorzusehen, also die Telekommunikationsverkehrsdaten von Berufsgeheimnisträgern von der Speicherung bei den Diensteanbietern auszunehmen oder nur unter bestimmten - im Einzelfall zu prüfenden - Voraussetzungen zu speichern. Vielmehr sind entsprechende Regelungen im Rahmen der den Zugang der Behörden zu diesen Daten regelnden Bestimmungen zu treffen, insbesondere über die Zeugnisverweigerungsrechte.

Vor dem Hintergrund der erforderlichen Erarbeitung eines Gesamtkonzepts für alle heimlichen Ermittlungsmaßnahmen kommt der Berücksichtigung und der Ausgestaltung der **Zeugnisverweigerungsrechte** nach Auffassung der Landesregierung eine zentrale Bedeutung zu. Denn diese gewährleisten im Einzelfall den Schutz bestimmter Berufsgruppen vor dem Zugriff der Strafverfolgungsbehörden auf die erhobenen und gespeicherten Verbindungsdaten.

Da die Richtlinie das nationale Recht als Grundlage für eine Abrufberechtigung betont und für dessen Gestaltung nur sehr abstrakte Vorgaben macht, wird die Landesregierung im Bundesrat auf eine umfassende Neuregelung der Beweiserhebungs- und -verwertungsverbote hinwirken, **insbesondere** auf eine Prüfung, ob die Beweiserhebungs- und -verwertungsverbote auch auf die Angehörigen nach § 52 StPO, auf Berufshelfer sowie auf alle der in § 53 StPO genannten Berufsgeheimnisträger (also z.B. auch auf Rechtsanwälte, Wirtschaftsprüfer, Steuerberater, Ärzte, Psychotherapeuten, Journalisten sowie Einrichtungen der Schwangerschaftsberatung und der Drogenhilfe) auszudehnen sind (entsprechend § 100c Abs. 6 S. 2 StPO).
Denn für die bisherige differenzierte Behandlung der Berufsgeheimnisträger sind sachliche Gründe nur schwer erkennbar.
Ferner könnte beispielsweise der besondere Schutz der Presse gegen Beschlagnahme und bei Vernehmungen umgangen werden, wenn es den Ermittlungsbehörden "freistünde", jene Ermittlungsmaßnahmen durch heimliche Überwachungsmaßnahmen, die nicht den genannten Regelungen zum Schutz der Presse unterliegen, zu ersetzen (sog. **Umgehungsverbot**, so *Gusy*, NStZ 2003, 399 [402]).

Durch die generelle Einbeziehung **aller** Berufsgeheimnisträger in den Schutz der Beweiserhebungsverbote könnten die strafprozessualen Vorschriften insoweit auch systematisch an die präventiv-polizeilichen Regelungen (in Schleswig-Holstein) angepasst werden. Bereits das geltende Landesrecht enthält bei **offener** Datenerhebung einen ausdrücklichen Schutz der Vertrauensberufe. Die Auskunftsverweigerungsrechte nach den §§ 52 bis 55 StPO sind im Polizeirecht bereits umfassend de lege lata gesichert. Nach § 180 Abs. 2 S. 3 und 4 LVwG ist die bestehende Grenze die Gefahrenabwehr für Gesundheit, Leben oder Freiheit einer Person.

Durch den Gesetzentwurf "zur Anpassung gefahrenabwehrrechtlicher und verwaltungsverfahrensrechtlicher Bestimmungen" (LT-Drs. 16/670) wird dieser besondere Schutz auf alle **verdeckten** Datenerhebungen ausgedehnt und der Heimlichkeit der Maßnahmen angepasst (siehe Begründung S. 50). Eingriffe mit verdeckten Maßnahmen in ein Amts- und Berufsgeheimnis geschütztes Vertrauensverhältnis im Sinne von §§ 53 und 53a StPO sind nach § 186a Abs. 4 Gesetz-E nur insoweit zulässig, als es zur Abwehr einer gegenwärtigen Gefahr für Leben oder Gesundheit erforderlich ist.

(h) Befristung und Vernichtung

Derzeitige Rechtslage

Nach § 100h Abs. 1 S. 3 i.V.m. § 100b Abs. 2 S. 4 und 5 StPO ist die TKA über zukünftige Verbindungsdaten auf höchstens drei Monate zu befristen. Eine Verlängerung ist, wie bei der TÜ, möglich. Die Bezugnahme auf § 100b Abs. 4 StPO regelt die Beendigung und die Mitteilungspflicht gegenüber dem Richter und dem Diensteanbieter. Die nicht mehr benötigten Unterlagen sind nach Abs. 1 S. 3 i.V.m. § 100b Abs. 6 StPO zu vernichten.

Position der Landesregierung

Die Landesregierung wird sich im Bundesrat dafür einsetzen, an dieser Regelung festzuhalten.

(3) Rechtsschutz

Derzeitige Rechtslage

Nach § 101 Abs. 1 S. 1 StPO sind die Beteiligten von den getroffenen Maßnahmen nach §§ 100g und 100h zu **benachrichtigen**, sofern dies u.a. ohne Gefährdung des Untersuchungszwecks geschehen kann.

Nach Durchführung der Maßnahme kann mit der **Beschwerde** (§ 304 Abs. 1 StPO) ggf. die Feststellung ihrer Rechtswidrigkeit beantragt werden. Anders als Entschei-

dungen, die eine Beschlagnahme - auch Postbeschlagnahme - oder die Durchsuchung zum Gegenstand haben, sind jedoch die von dem OLG oder dem Ermittlungsrichter des BGH getroffenen Entscheidungen nach dem Willen des Gesetzgebers (BGH NStZ 2002, 274) und nach dem Wortlaut des § 304 Abs. 4 S. 2, Abs. 5 StPO nicht mit der Beschwerde anfechtbar (BGH 3. 12. 2002, 2 BGs 513/02; s. auch BGH CuR 1998, 738).

Gegen **Eilentscheidungen** der Staatsanwaltschaft ist der Antrag nach § 98 Abs. 2 S. 2 StPO analog gegeben ("richterliche Entscheidung").

Nach höchstrichterlicher Rechtsprechung (BVerfG, NJW 1997, 2163 [2164]) darf die Beschwerde nicht allein deswegen, weil die richterliche Anordnung vollzogen worden sei und die Maßnahme sich deshalb erledigt habe, unter dem Gesichtspunkt **prozessualer Überholung** als unzulässig verworfen werden. Vielmehr habe das Beschwerdegericht - mit Blick auf Artikel 19 Abs. 4 GG - zu prüfen, ob - ungeachtet der eingetretenen Erledigung - ein Rechtsschutzinteresse des Betroffenen besteht.

Artikel 19 Abs. 4 GG enthält ein Grundrecht auf effektiven und möglichst lückenlosen richterlichen Rechtsschutz gegen Akte der öffentlichen Gewalt (ständige Rechtsprechung, siehe etwa BVerfGE 67, 43 [58]). Wenn sich der Eingriff bei einem tiefgehenden Grundrechtseingriff nach dem typischen Verfahrensablauf auf eine Zeitspanne beschränkt, in der der Betroffene die gerichtliche Entscheidung vom Prozessgericht regelmäßig nicht erlangen kann, gebietet Artikel 19 Abs. 4 GG, die Rechtmäßigkeit des Grundrechtseingriffs nachträglich feststellen zu lassen, auch wenn der Eingriff abgeschlossen ist und tatsächlich nicht fortwirkt (E 96, 27 (39 f.); NJW 1998, 2131 f.).
Das Bundesverfassungsgericht hatte dies bisher für die Hausdurchsuchung (Artikel 13 GG) sowie die Ingewahrsamnahme und für die Abschiebungshaft (Artikel 2 Abs. 2 S. 2 GG) bejaht und erstreckt diese Rechtsprechung auch auf § 12 FAG a.F. (E 107, 299 [337 m.w.N]): der vom Gesetzgeber geregelte **einfachgesetzliche Richtervorbehalt sei ein Indiz** für die außerordentliche und der Ingewahrsamnahme, der Hausdurchsuchung und der Abschiebehaft vergleichbaren Eingriffstiefe. Im Übrigen würde in diesen Fällen, da der Betroffene von der Auskunftserteilung nichts erfahre, bei Nichtgewährung nachträglichen Rechtsschutzes das Rechtsschutzgebot "völlig ausgehöhlt werden". Bei **heimlichen** Grundrechtseingriffen sei ein Rechtsschutzinteresse des Betroffenen auf nachträgliche Überprüfung **in der Regel zu bejahen**.

Die Beschwerde des von der TKA **Betroffenen** ist danach namentlich dann zulässig, wenn die richterliche Anordnung willkürlich ermessensfehlerhaft war und ein nachwirkendes Rechtsschutzinteresse dafür besteht, dies festzustellen.

Die Beschwerdebefugnis des **Betreibers** ist allerdings eingeschränkt (BGH, Entscheidung vom 3. Dezember 2002, 2 BGs 513/02; LG Bremen StV 1999, 307 m.w.N.). Die Rechtmäßigkeit der Anordnung kann er nicht angreifen; seine Beschwerdebefugnis kann sich aber auf die Modalitäten der technischen Umsetzung beziehen.

Gestaltungsspielraum nach der Richtlinie
Nach Artikel 13 Abs. 1 stellt jeder Mitgliedstaat sicher, "dass die einzelstaatlichen Maßnahmen zur Umsetzung von Kapitel III der Richtlinie 95/46/EG über Rechtsbehelfe [...] im Hinblick auf die Datenverarbeitung [...] in vollem Umfang umgesetzt werden". Danach müssen die Mitgliedstaaten u.a. sicherstellen, dass jede Person bei der Verletzung der Rechte, die ihr durch die für die betreffende Verarbeitung geltenden einzelstaatlichen Rechtsvorschriften garantiert sind, "bei Gericht einen Rechtsbehelf einlegen kann".

Position der Landesregierung
Die Landesregierung wird im Bundesrat - im Rahmen der Prüfung, ob im Hinblick auf strafprozessuale heimliche Ermittlungsmaßnahmen Änderungsbedarf besteht - darauf hinwirken, den Rechtsschutz der von solchen Maßnahmen Betroffenen u.a. durch Benachrichtigungs-, Kennzeichnungs-, Datenlöschungs- und Dokumentationspflichten zu verbessern. Da die TKA - wie dies bei Eingriffen in das Fernmeldegeheimnis typischerweise der Fall ist - ohne Anhörung des Betroffenen angeordnet und damit ohne Kenntnisnahme heimlich vollzogen wird, sollte insbesondere geprüft werden, ob und inwieweit gesetzliche Klarstellungen zum nachträglichen Rechtsschutz erforderlich sind.

(4) Entschädigungszahlungen
Verfassungsrechtlicher Rahmen
Da die gesetzliche Einführung einer generellen Vorratsspeicherung von Telekommunikationsdaten einerseits zwar nicht final auf eine Einschränkung der Berufsfreiheit zielt, andererseits aber spezifisch an das Angebot von Telekommunikations- und Telediensten anknüpft und diese Tätigkeit regelt, indem geschäftsmäßigen Anbietern von Telekommunikations- und Telediensten die Speicherung von Verkehrs- und Standortdaten im Rahmen ihrer Tätigkeit aufgegeben wird, liegt ein Eingriff in die Freiheit der Berufsausübung vor.

Die Berufsausübungsfreiheit kann jedoch nach Artikel 12 Abs. 1 S. 2 GG durch Gesetz oder auf Grund eines Gesetzes eingeschränkt werden. Hinsichtlich der verfassungsrechtlichen Anforderungen an ein solches Gesetz kann grundsätzlich auf das oben Gesagte verwiesen werden.

Derzeitige Rechtslage
Die konkrete Auskunftserteilung auf Ersuchen der Strafverfolgungsbehörden ist im Regelfall mit Kosten verbunden, insbesondere aus den personellen Aufwendungen für die Recherche nach den gewünschten Daten.
Für Überwachungsmaßnahmen nach §§ 100a, 100b StPO sind Entschädigungen nach dem zum 1. Juli 2004 in Kraft getretenen Justizvergütungs- und -entschädigungsgesetz (JVEG) zu gewähren, § 23 Abs. 1 Nr. 3 JVEG. Die Regelung entspricht dabei der Vorgängernorm in § 17a Abs. 1 Nr. 3 ZSEG.
Das OLG Zweibrücken (in: DuD 1998, 168 f.) hat in einer Entscheidung zu dem alten ZSEG festgestellt, dass die Vorschriften des ZSEG für jene Fälle anzuwenden seien, in denen kostenpflichtige Ermittlungen auf Veranlassung der Staatsanwaltschaft durchgeführt werden. Demnach sind Auskünfte auf der Grundlage des § 161 StPO und der §§ 100g, 100h StPO nach dem ZSEG (jetzt JVEG, § 23 Abs. 1 Nr. 2) zu entschädigen. Einzelheiten über das Verfahren und die Entschädigungshöhe sind dem JVEG zu entnehmen.

Die früher umstrittene Frage nach einer Entschädigung für Auskünfte über **Bestandsdaten** gemäß § 113 Abs. 1 TKG wurde durch den Gesetzgeber in § 113 Abs. 2 TKG geklärt. Demnach hat der zur Auskunft Verpflichtete die in seinem Verantwortungsbereich für die Auskunftserteilung erforderlichen Vorkehrungen (Organisation etc.) auf eigene Kosten zu treffen. Im Falle einer Auskunftserteilung wird dem Verpflichteten durch die anfragende Stelle eine Entschädigung gewährt, deren Umfang sich abweichend von § 23 Abs. 1 Nr. 2 JVEG nach der Rechtsverordnung nach § 110 Abs. 9 TKG bemisst.

Position der Landesregierung
Die Landesregierung begrüßt, dass die im Richtlinienvorschlag der Kommission ursprünglich enthaltene Verpflichtung der Mitgliedstaaten, den Anbietern elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes die **Zusatzkosten** (Investitionen in neue Speichermedien), die ihnen in Erfüllung der ihnen aus der Richtlinie erwachsenden Verpflichtungen nachweislich entstanden sind, zu erstatten, gestrichen wurde. Denn dadurch wären zusätzliche Kosten auf die öffentlichen Haushalte zugekommen. Auch aus diesem Grund begrüßt sie es, dass die Bundesregierung in den Verhandlungen auf EU-Ebene durchgesetzt hat, dass

eine Speicherungsverpflichtung nur diejenigen Datenarten und nur solche Zeiträume erfassen kann, die unbedingt erforderlich sind, um die mit der Vorratsspeicherung verfolgten Ziele zu erreichen, und die zugleich keinen unverhältnismäßig hohen zusätzlichen Aufwand für die betroffenen Unternehmen verursachen.

Da nach der Richtlinie im Rahmen der Umsetzung in das nationale Recht **Entschädigungsregelungen** für die Fälle, in denen Strafverfolgungsbehörden im Einzelfall auf die Daten zugreifen, getroffen werden können, wird die Landesregierung im Bundesrat darauf hinwirken (ebenso wie der Bundestag, Drs. 16/545 und 16/690), dass die Bundesregierung einen Gesetzentwurf für eine angemessene Entschädigung der Telekommunikationsunternehmen für die Inanspruchnahme im Rahmen der Erfüllung hoheitlicher Ermittlungsmaßnahmen im Bereich der Telekommunikation vorlegt.