Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassungsgemäß

Pressemitteilung Nr. 11/2010 vom 2. März 2010

Urteil vom 02. März 2010
1 BvR 256/08

Die Verfassungsbeschwerden richten sich gegen §§ 113a, 113b TKG und gegen § 100g StPO, soweit dieser die Erhebung von nach § 113a TKG gespeicherten Daten zulässt. Eingeführt wurden die Vorschriften durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21. Dezember 2007.

§ 113a TKG regelt, dass öffentlich zugängliche Telekommunikationsdiensteanbieter verpflichtet sind, praktisch sämtliche Verkehrsdaten von Telefondiensten (Festnetz, Mobilfunk, Fax, SMS, MMS), E Mail Diensten und Internetdiensten vorsorglich anlasslos zu speichern. Die Speicherungspflicht erstreckt sich im Wesentlichen auf alle Angaben, die erforderlich sind, um zu rekonstruieren, wer wann wie lange mit wem von wo aus kommuniziert hat oder zu kommunizieren versucht hat. Nicht zu speichern ist demgegenüber der Inhalt der Kommunikation, und damit auch, welche Internetseiten von den Nutzern aufgerufen werden. Nach Ablauf der Speicherungspflicht von sechs Monaten sind die Daten innerhalb eines Monats zu löschen.

§ 113b TKG regelt die möglichen Zwecke, für die diese Daten verwendet werden dürfen. Die Vorschrift versteht sich dabei als Scharniernorm: Sie enthält selbst keine Ermächtigung zur Datenabfrage, sondern bezeichnet nur grobmaschig allgemein mögliche Nutzungszwecke, die durch fachrechtliche Regelungen des Bundes und der Länder konkretisiert werden sollen. In Satz 1 Halbsatz 1 werden dabei die möglichen Zwecke der *unmittelbaren* Nutzung der Daten aufgelistet: Die Verfolgung von Straftaten, die Abwehr von erheblichen Gefahren für die öffentliche Sicherheit und die Erfüllung von nachrichtendienstlichen Aufgaben. Halbsatz 2 erlaubt darüber hinaus die *mittelbare* Nutzung der Daten für Auskünfte nach § 113 Abs. 1 TKG in Form eines Auskunftsanspruchs gegenüber den Diensteanbietern zur Identifizierung von IP Adressen. Behörden können danach, wenn sie etwa durch Anzeige oder durch eigene Ermittlungen eine IP Adresse schon kennen, Auskunft verlangen, welchem Anschlussnehmer diese Adresse zugeordnet war. Der Gesetzgeber erlaubt dies unabhängig von näher begrenzenden Maßgaben zur Verfolgung von Straftaten und Ordnungswidrigkeiten sowie zur Gefahrenabwehr; ein Richtervorbehalt ist insoweit ebenso wenig vorgesehen wie Benachrichtigungspflichten.

§ 100g StPO regelt - in Konkretisierung des § 113b Satz 1 Halbsatz 1 Nr. 1 TKG - die unmittelbare Verwendung der vorsorglich gespeicherten Daten für die Strafverfolgung. Insgesamt betrachtet ist die Vorschrift dabei weiter und regelt den Zugriff auf Telekommunikationsverkehrsdaten überhaupt. Sie erlaubt also auch und ursprünglich nur den Zugriff auf Verbindungsdaten, die aus anderen Gründen (etwa zur Geschäftsabwicklung) bei den Diensteanbietern gespeichert sind. Der Gesetzgeber hat sich entschieden, insoweit nicht zwischen der Nutzung der nach § 113a TKG vorsorglich gespeicherten Daten und anderer Verkehrsdaten zu unterscheiden. Er erlaubt die Nutzung auch der Vorratsdaten unabhängig von einem abschließenden Straftatenkatalog für die Verfolgung von Straftaten mit erheblicher Bedeutung sowie darüber hinaus nach Maßgabe einer einzelfallbezogenen Verhältnismäßigkeitsprüfung auch allgemein zur Verfolgung von Straftaten, die mittels Telekommunikation begangen wurden. Erforderlich ist eine vorherige richterliche Entscheidung; auch kennt die Strafprozessordnung insoweit Benachrichtigungspflichten und nachträglichen Rechtsschutz.

Die angegriffenen Vorschriften verstehen sich als Umsetzung der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsdatenspeicherung aus dem Jahre 2006. Nach dieser Richtlinie sind Anbieter von Telekommunikationsdiensten dazu zu verpflichten, die in § 113a TKG erfassten Daten für mindestens sechs Monate und höchstens zwei Jahre zu speichern und für die Verfolgung von schweren Straftaten bereitzuhalten. Keine näheren Regelungen enthält die Richtlinie zur Verwendung der Daten; auch die Maßnahmen zum Datenschutz werden im Wesentlichen den Mitgliedstaaten überlassen.

Aufgrund der einstweiligen Anordnungen des Ersten Senats des Bundesverfassungsgerichts (Pressemitteilungen Nr. 37/2008 vom 19. März 2008 und Nr. 92/2008 vom 6. November 2008) durften die nach § 113a TKG gespeicherten Daten zu Strafverfolgungszwecken nach § 113b Satz 1 Nr. 1 TKG zunächst nur gemäß den in der einstweiligen Anordnung vorgesehenen Maßgaben und die nach § 113a TKG auf Vorrat gespeicherten Daten für die Gefahrenabwehr (§ 113b Satz 1 Nr. 2 TKG) von den Telekommunikationsdiensteanbietern nur unter einschränkenden Bedingungen an die ersuchende Behörde übermittelt werden.

Die Beschwerdeführer sehen durch die Vorratsdatenspeicherung vor allem das Telekommunikationsgeheimnis und das Recht auf informationelle Selbstbestimmung verletzt. Sie halten die anlasslose Speicherung aller Telekommunikationsverbindungen für unverhältnismäßig. Insbesondere machen sie geltend, dass sich aus den gespeicherten Daten Persönlichkeits- und Bewegungsprofile erstellen ließen. Eine Beschwerdeführerin, die einen Internetanonymisierungsdienst anbietet, rügt, die mit der Speicherung verbundenen Kosten beeinträchtigten die Anbieter von Telekommunikationsdiensten unverhältnismäßig in ihrer Berufsfreiheit.

Der Erste Senat des Bundesverfassungsgerichts hat entschieden, dass die Regelungen des TKG und der StPO über die Vorratsdatenspeicherung mit Art. 10 Abs. 1 GG nicht vereinbar sind. Zwar ist eine Speicherungspflicht in dem vorgesehenen Umfang nicht von vornherein schlechthin verfassungswidrig. Es fehlt aber an einer dem Verhältnismäßigkeitsgrundsatz entsprechenden Ausgestaltung. Die angegriffenen Vorschriften gewährleisten weder eine hinreichende Datensicherheit, noch eine hinreichende Begrenzung der Verwendungszwecke der Daten. Auch genügen sie nicht in jeder Hinsicht den verfassungsrechtlichen Transparenz und Rechtsschutzanforderungen. Die Regelung ist damit insgesamt verfassungswidrig und nichtig.

Der Entscheidung liegen im Wesentlichen folgende Erwägungen zu Grunde:

Zur Zulässigkeit:

Die Verfassungsbeschwerden sind nicht unzulässig, soweit die angegriffenen Vorschriften in Umsetzung der Richtlinie 2006/24/EG ergangen sind. Die Beschwerdeführer erstreben, ohne dass sie dies angesichts ihrer unmittelbar gegen das Umsetzungsgesetz gerichteten Verfassungsbeschwerden vor den Fachgerichten geltend machen konnten, eine Vorlage durch das Bundesverfassungsgericht an den Europäischen Gerichtshof, damit dieser im Wege der Vorabentscheidung nach Art. 267 AEUV (vormals Art. 234 EGV) die Richtlinie für nichtig erkläre und so den Weg frei mache für eine Überprüfung der angegriffenen Vorschriften am Maßstab der deutschen Grundrechte. Jedenfalls auf diesem Weg ist eine Prüfung der angegriffenen Vorschriften am Maßstab der Grundrechte des Grundgesetzes nach dem Begehren der Beschwerdeführer nicht von vornherein ausgeschlossen.

Zur Begründetheit:

1. Kein Vorabentscheidungsverfahren vor dem Europäischen Gerichtshof

Eine Vorlage an den Europäischen Gerichtshof kommt nicht in Betracht, da es auf einen möglichen Vorrang des Gemeinschaftsrechts nicht ankommt. Die Wirksamkeit der Richtlinie 2006/24/EG und ein sich hieraus möglicherweise ergebender Vorrang des Gemeinschaftsrechts vor deutschen Grundrechten sind nicht entscheidungserheblich. Der Inhalt der Richtlinie belässt der Bundesrepublik Deutschland einen weiten Entscheidungsspielraum. Ihre Regelungen sind im Wesentlichen auf die Speicherungspflicht und deren Umfang beschränkt und regeln nicht den Zugang zu den Daten oder

deren Verwendung durch die Behörden der Mitgliedstaaten. Mit diesem Inhalt kann die Richtlinie ohne Verstoß gegen die Grundrechte des Grundgesetzes umgesetzt werden. Das Grundgesetz verbietet eine solche Speicherung nicht unter allen Umständen.

2. Schutzbereich des Art. 10 Abs. 1 GG

Die angegriffenen Vorschriften greifen auch soweit es um die Speicherung der Internetzugangsdaten und um die Ermächtigung zu Auskünften nach § 113b Satz 1 Halbsatz 2 TKG geht in den Schutzbereich des Art. 10 Abs. 1 GG (Telekommunikationsgeheimnis) ein. Dass die Speicherung durch private Diensteanbieter erfolgt, steht dem nicht entgegen, da diese allein als Hilfspersonen für die Aufgabenerfüllung durch staatliche Behörden in Anspruch genommen werden.

3. Möglichkeit einer anlasslosen Speicherung von Telekommunikationsverkehrsdaten

Eine sechsmonatige anlasslose Speicherung von Telekommunikationsverkehrsdaten für qualifizierte Verwendungen im Rahmen der Strafverfolgung, der Gefahrenabwehr und der Aufgaben der Nachrichtendienste, wie sie die §§ 113a, 113b TKG anordnen, ist mit Art. 10 GG nicht schlechthin unvereinbar. Bei einer Ausgestaltung, die dem besonderen Gewicht des hierin liegenden Eingriffs hinreichend Rechnung trägt, unterfällt eine anlasslose Speicherung der Telekommunikationsverkehrsdaten nicht schon als solche dem strikten Verbot einer Speicherung von Daten auf Vorrat im Sinne der Rechtsprechung des Bundesverfassungsgerichts. Eingebunden in eine dem Eingriff adäquate gesetzliche Ausgestaltung kann sie den Verhältnismäßigkeitsanforderungen genügen.

Allerdings handelt es sich bei einer solchen Speicherung um einen besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt. Auch wenn sich die Speicherung nicht auf die Kommunikationsinhalte erstreckt, lassen sich aus diesen Daten bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen. Adressaten, Daten, Uhrzeit und Ort von Telefongesprächen erlauben, wenn sie über einen längeren Zeitraum beobachtet werden, in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen. Je nach Nutzung der Telekommunikation kann eine solche Speicherung die Erstellung aussagekräftiger Persönlichkeits und Bewegungsprofile praktisch jeden Bürgers ermöglichen. Auch steigt das Risiko von Bürgern, weiteren Ermittlungen ausgesetzt zu werden, ohne selbst hierzu Anlass gegeben zu haben. Darüber hinaus verschärfen die Missbrauchsmöglichkeiten, die mit einer solchen Datensammlung verbunden sind, deren belastende Wirkung. Zumal die Speicherung und Datenverwendung nicht bemerkt werden, ist die anlasslose Speicherung von Telekommunikationsverkehrsdaten geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann.

Dennoch kann eine solche Speicherung unter bestimmten Maßgaben mit Art. 10 Abs. 1 GG vereinbar sein. Maßgeblich dafür ist zunächst, dass die vorgesehene Speicherung der Telekommunikationsverkehrsdaten nicht direkt durch den Staat, sondern durch eine Verpflichtung der privaten Diensteanbieter verwirklicht wird. Die Daten werden damit bei der Speicherung selbst noch nicht zusammengeführt, sondern bleiben verteilt auf viele Einzelunternehmen und stehen dem Staat unmittelbar als Gesamtheit nicht zur Verfügung. Eine Speicherung der Telekommunikationsverkehrsdaten für sechs Monate stellt sich auch nicht als eine Maßnahme dar, die auf eine Totalerfassung der Kommunikation oder Aktivitäten der Bürger insgesamt angelegt wäre. Sie knüpft vielmehr in noch begrenzt bleibender Weise an die besondere Bedeutung der Telekommunikation in der modernen Welt an und reagiert auf das spezifische Gefahrenpotential, das sich mit dieser verbindet. Eine Rekonstruktion gerade der Telekommunikationsverbindungen ist daher für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung.

Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt voraus, dass diese eine Ausnahme bleibt. Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur

verfassungsrechtlichen Identität der Bundesrepublik Deutschland, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss. Durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wird der Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer.

4. Verhältnismäßigkeit der gesetzlichen Ausgestaltung der Regelung (Maßstäbe)

Angesichts des besonderen Gewichts einer vorsorglichen Telekommunikationsverkehrsdatenspeicherung ist diese nur dann mit Art. 10 Abs. 1 GG vereinbar, wenn ihre Ausgestaltung besonderen verfassungsrechtlichen Anforderungen entspricht. Es bedarf insoweit hinreichend anspruchsvoller und normenklarer Regelungen zur Datensicherheit, zur Begrenzung der Datenverwendung, zur Transparenz und zum Rechtsschutz.

Anforderungen an die Datensicherheit:

Angesichts des Umfangs und der potentiellen Aussagekraft der mit einer solchen Speicherung geschaffenen Datenbestände ist die Datensicherheit für die Verhältnismäßigkeit der angegriffenen Vorschriften von großer Bedeutung. Erforderlich sind gesetzliche Regelungen, die ein besonders hohes Maß an Sicherheit jedenfalls dem Grunde nach normenklar und verbindlich vorgeben. Dabei steht es dem Gesetzgeber frei, die technische Konkretisierung des vorgegebenen Maßstabs einer Aufsichtsbehörde anzuvertrauen. Der Gesetzgeber hat dabei jedoch sicherzustellen, dass die Entscheidung über Art und Maß der zu treffenden Schutzvorkehrungen nicht letztlich unkontrolliert in den Händen der jeweiligen Telekommunikationsanbieter liegt.

Anforderungen an die unmittelbare Datenverwendung:

Angesichts des Gewichts der Datenspeicherung kommt eine Verwendung der Daten nur für überragend wichtige Aufgaben des Rechtsgüterschutzes in Betracht.

Für die Strafverfolgung folgt hieraus, dass ein Abruf der Daten zumindest den durch bestimmte Tatsachen begründeten Verdacht einer auch im Einzelfall schwerwiegenden Straftat voraussetzt. Welche Straftatbestände hiervon umfasst sein sollen, hat der Gesetzgeber abschließend mit der Verpflichtung zur Datenspeicherung festzulegen.

Für die Gefahrenabwehr ergibt sich aus dem Verhältnismäßigkeitsgrundsatz, dass ein Abruf der vorsorglich gespeicherten Telekommunikationsverkehrsdaten nur bei Vorliegen einer durch bestimmte Tatsachen hinreichend belegten, konkreten Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr zugelassen werden darf. Diese Anforderungen gelten, da es auch insoweit um eine Form der Gefahrenprävention geht, gleichermaßen für die Verwendung der Daten durch die Nachrichtendienste. Eine Verwendung der Daten von Seiten der Nachrichtendienste dürfte damit freilich in vielen Fällen ausscheiden. Dies liegt jedoch in der Art ihrer Aufgaben als Vorfeldaufklärung und begründet keinen verfassungsrechtlich hinnehmbaren Anlass, die sich aus dem Verhältnismäßigkeitsgrundsatz ergebenden Voraussetzungen für einen Eingriff der hier vorliegenden Art abzumildern.

Verfassungsrechtlich geboten ist als Ausfluss des Verhältnismäßigkeitsgrundsatzes überdies, zumindest für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen ein grundsätzliches Übermittlungsverbot vorzusehen. Zu denken ist hier etwa an Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit anderen Verschwiegenheitsverpflichtungen unterliegen.

Anforderungen an die Transparenz der Datenübermittlung:

Der Gesetzgeber muss die diffuse Bedrohlichkeit, die die als solche nicht spürbare Datenspeicherung und verwendung für die Bürger erhalten können, durch wirksame Transparenzregeln auffangen. Hierzu zählt der Grundsatz der Offenheit der Erhebung und Nutzung von personenbezogenen Daten. Eine Verwendung der Daten ohne Wissen des Betroffenen ist verfassungsrechtlich nur dann zulässig, wenn andernfalls der Zweck der Untersuchung, dem der Datenabruf dient, vereitelt wird. Für die Gefahrenabwehr und die Wahrnehmung der Aufgaben der Nachrichtendienste darf der Gesetzgeber dies grundsätzlich annehmen. Demgegenüber kommt im Rahmen der Strafverfolgung auch eine offene Erhebung und Nutzung der Daten in Betracht. Eine heimliche Verwendung der Daten darf hier nur vorgesehen werden, wenn sie im Einzelfall erforderlich und richterlich angeordnet ist. Soweit die Verwendung der Daten heimlich erfolgt, hat der Gesetzgeber die Pflicht einer zumindest nachträglichen Benachrichtigung vorzusehen. Diese muss gewährleisten, dass diejenigen, auf die sich eine Datenabfrage unmittelbar bezogen hat, wenigstens im Nachhinein grundsätzlich in Kenntnis zu setzen sind. Ausnahmen hiervon bedürfen der richterlichen Kontrolle.

Anforderungen an den Rechtsschutz und an Sanktionen:

Eine Übermittlung und Nutzung der gespeicherten Daten ist grundsätzlich unter Richtervorbehalt zu stellen. Sofern ein Betroffener vor Durchführung der Maßnahme keine Gelegenheit hatte, sich vor den Gerichten gegen die Verwendung seiner Telekommunikationsverkehrsdaten zur Wehr zu setzen, ist ihm eine gerichtliche Kontrolle nachträglich zu eröffnen.

Eine verhältnismäßige Ausgestaltung setzt weiterhin wirksame Sanktionen bei Rechtsverletzungen voraus. Würden auch schwere Verletzungen des Telekommunikationsgeheimnisses im Ergebnis sanktionslos bleiben mit der Folge, dass der Schutz des Persönlichkeitsrechts angesichts der immateriellen Natur dieses Rechts verkümmern würde, widerspräche dies der Verpflichtung der staatlichen Gewalt, dem Einzelnen die Entfaltung seiner Persönlichkeit zu ermöglichen und ihn vor Persönlichkeitsrechtsgefährdungen durch Dritte zu schützen. Der Gesetzgeber hat diesbezüglich allerdings einen weiten Gestaltungsspielraum. Insoweit darf er auch berücksichtigen, dass bei schweren Verletzungen des Persönlichkeitsrechts bereits nach geltender Rechtslage sowohl Verwertungsverbote auf der Grundlage einer Abwägung als auch eine Haftung für immaterielle Schäden begründet sein können, und somit zunächst beobachten, ob der besonderen Schwere der Persönlichkeitsverletzung, die in der unberechtigten Erlangung oder Verwendung der hier in Frage stehenden Daten regelmäßig liegt, möglicherweise schon auf der Grundlage des geltenden Rechts hinreichend Rechnung getragen wird.

Anforderungen an die mittelbare Nutzung der Daten zur Identifizierung von IP-Adressen:

Weniger strenge verfassungsrechtliche Maßgaben gelten für eine nur mittelbare Verwendung der vorsorglich gespeicherten Daten in Form von behördlichen Auskunftsansprüchen gegenüber den Diensteanbietern hinsichtlich der Anschlussinhaber bestimmter, bereits bekannter IP Adressen. Von Bedeutung ist hierfür zum einen, dass dabei die Behörden selbst keine Kenntnis der vorsorglich zu speichernden Daten erhalten. Die Behörden rufen im Rahmen solcher Auskunftsansprüche nicht die vorsorglich anlasslos gespeicherten Daten selbst ab, sondern erhalten lediglich personenbezogene Auskünfte über den Inhaber eines bestimmten Anschlusses, der von den Diensteanbietern unter Rückgriff auf diese Daten ermittelt wurde. Systematische Ausforschungen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits und Bewegungsprofilen lassen sich allein auf Grundlage solcher Auskünfte nicht verwirklichen. Maßgeblich ist zum anderen, dass für solche Auskünfte nur ein von vornherein feststehender kleiner Ausschnitt der Daten verwendet wird, deren Speicherung für sich genommen geringeres Eingriffsgewicht hat und damit unter deutlich geringeren Voraussetzungen angeordnet werden könnte.

Allerdings hat auch die Begründung von behördlichen Auskunftsansprüchen zur Identifizierung von IP Adressen erhebliches Gewicht. Mit ihr wirkt der Gesetzgeber auf die Kommunikationsbedingungen im Internet ein und begrenzt den Umfang ihrer Anonymität. Auf ihrer Grundlage kann in Verbindung mit der systematischen Speicherung der Internetzugangsdaten hinsichtlich zuvor ermittelter IP Adressen die Identität von Internetnutzern in weitem Umfang ermittelt werden.

Innerhalb des ihm dabei zustehenden Gestaltungsspielraums darf der Gesetzgeber solche Auskünfte auch unabhängig von begrenzenden Straftaten oder Rechtsgüterkatalogen für die Verfolgung von Straftaten, für die Gefahrenabwehr und die Aufgabenwahrnehmung der Nachrichtendienste auf der Grundlage der allgemeinen fachrechtlichen Eingriffsermächtigungen zulassen. Hinsichtlich der Eingriffsschwellen ist allerdings sicherzustellen, dass eine Auskunft nicht ins Blaue hinein eingeholt wird, sondern nur aufgrund eines hinreichenden Anfangsverdachts oder einer konkreten Gefahr auf einzelfallbezogener Tatsachenbasis erfolgen darf. Ein Richtervorbehalt muss für solche Auskünfte nicht vorgesehen werden; die Betreffenden müssen von der Einholung einer solchen Auskunft aber benachrichtigt werden. Auch können solche Auskünfte nicht allgemein und uneingeschränkt zur Verfolgung oder Verhinderung jedweder Ordnungswidrigkeiten zugelassen werden. Die Aufhebung der Anonymität im Internet bedarf zumindest einer Rechtsgutbeeinträchtigung, der von der Rechtsordnung auch sonst ein hervorgehobenes Gewicht beigemessen wird. Dies schließt entsprechende Auskünfte zur Verfolgung oder Verhinderung von Ordnungswidrigkeiten nicht vollständig aus. Es muss sich insoweit aber um auch im Einzelfall besonders gewichtige Ordnungswidrigkeiten handeln, die der Gesetzgeber ausdrücklich benennen muss.

Verantwortlichkeit für die Ausgestaltung der Regelungen:

Die verfassungsrechtlich gebotene Gewährleistung der Datensicherheit sowie einer den Verhältnismäßigkeitsanforderungen genügenden normenklaren Begrenzung der Datenverwendung ist ein untrennbarer Bestandteil der Anordnung der Speicherungsverpflichtung und obliegt deshalb gemäß Art. 73 Abs. 1 Nr. 7 GG dem Bundesgesetzgeber. Hierzu gehören neben den Regelungen zur Sicherheit der gespeicherten Daten auch die Regelungen zur Sicherheit der Übermittlung der Daten sowie hierbei die Gewährleistung des Schutzes der Vertrauensbeziehungen. Dem Bund obliegt darüber hinaus auch die Sicherstellung einer den verfassungsrechtlichen Anforderungen entsprechenden, hinreichend präzisen Begrenzung der Verwendungszwecke der Daten, die mit der Speicherung verfolgt werden. Demgegenüber richtet sich die Verantwortung für die Schaffung der Abrufregelungen selbst sowie für die Ausgestaltung der Transparenz und Rechtsschutzbestimmungen nach den jeweiligen Sachkompetenzen. Im Bereich der Gefahrenabwehr und der Aufgaben der Nachrichtendienste liegt die Zuständigkeit damit weithin bei den Ländern.

5. Zu den Bestimmungen im Einzelnen (Anwendung der Maßstäbe)

Die angegriffenen Vorschriften genügen diesen Anforderungen nicht. Zwar ist § 113a TKG nicht schon deshalb verfassungswidrig, weil die Reichweite der Speicherungspflicht von vornherein unverhältnismäßig wäre. Jedoch entsprechen die Regelungen zur Datensicherheit, zu den Zwecken und zur Transparenz der Datenverwendung sowie zum Rechtsschutz nicht den verfassungsrechtlichen Anforderungen. Damit fehlt es an einer dem Verhältnismäßigkeitsgrundsatz entsprechenden Ausgestaltung der Regelung insgesamt. §§ 113a, 113b TKG und § 100g StPO, soweit dieser den Abruf der nach § 113a TKG zu speichernden Daten erlaubt, sind deshalb mit Art. 10 Abs. 1 GG nicht vereinbar.

Datensicherheit:

Es fehlt schon an der gebotenen Gewährleistung eines besonders hohen Standards hinsichtlich der Datensicherheit. Das Gesetz verweist im Wesentlichen nur auf die im Bereich der Telekommunikation allgemein erforderliche Sorgfalt (§ 113a Abs. 10 TKG) und relativiert dabei die Sicherheitsanforderungen in unbestimmt bleibender Weise um allgemeine

Wirtschaftlichkeitserwägungen im Einzelfall (§ 109 Abs. 2 Satz 4 TKG). Dabei bleibt die nähere Konkretisierung der Maßnahmen den einzelnen Telekommunikationsdienstleistern überlassen, die ihrerseits die Dienste unter den Bedingungen von Konkurrenz und Kostendruck anbieten müssen. Den Speicherungspflichtigen sind insoweit weder die von den Sachverständigen im vorliegenden Verfahren nahegelegten Instrumente zur Gewährleistung der Datensicherheit (getrennte Speicherung, asymmetrische Verschlüsselung, Vier-Augen-Prinzip verbunden mit fortschrittlichen Verfahren zur Authentifizierung für den Zugang zu den Schlüsseln, revisionssichere Protokollierung von Zugriff und Löschung) durchsetzbar vorgegeben, noch ist ein vergleichbares Sicherheitsniveau anderweitig garantiert. Auch fehlt es an einem ausgeglichenen Sanktionensystem, das Verstößen gegen die Datensicherheit kein geringeres Gewicht beimisst als Verstößen gegen die Speicherungspflichten selbst.

Unmittelbare Verwendung der Daten zur Strafverfolgung:

Mit den aus dem Verhältnismäßigkeitsgrundsatz entwickelten Maßstäben unvereinbar sind auch die Regelungen zur Verwendung der Daten für die Strafverfolgung. § 100g Abs. 1 Satz 1 Nr. 1 StPO stellt nicht sicher, dass allgemein und auch im Einzelfall nur schwerwiegende Straftaten Anlass für eine Erhebung der entsprechenden Daten sein dürfen, sondern lässt unabhängig von einem abschließenden Katalog generell Straftaten von erheblicher Bedeutung genügen. Erst recht bleibt § 100g Abs. 1 Satz 1 Nr. 2, Satz 2 StPO hinter den verfassungsrechtlichen Maßgaben zurück, indem er unabhängig von deren Schwere jede mittels Telekommunikation begangene Straftat nach Maßgabe einer allgemeinen Abwägung im Rahmen einer Verhältnismäßigkeitsprüfung als möglichen Auslöser einer Datenabfrage ausreichen lässt. Mit dieser Regelung werden die nach § 113a TKG gespeicherten Daten praktisch in Bezug auf alle Straftatbestände nutzbar. Ihre Verwendung verliert damit angesichts der fortschreitenden Bedeutung der Telekommunikation im Lebensalltag ihren Ausnahmecharakter. Der Gesetzgeber beschränkt sich hier nicht mehr auf die Verwendung der Daten für die Verfolgung schwerer Straftaten, sondern geht hierüber und damit auch über die europarechtlich vorgegebene Zielsetzung der Datenspeicherung weit hinaus.

Nicht den verfassungsrechtlichen Anforderungen entspricht § 100g StPO auch insoweit, als er einen Datenabruf nicht nur für richterlich zu bestätigende Einzelfälle, sondern grundsätzlich auch ohne Wissen des Betroffenen zulässt (§ 100g Abs. 1 Satz 1 StPO).

Demgegenüber sind die gerichtliche Kontrolle der Datenabfrage und Datennutzung sowie die Regelung der Benachrichtigungspflichten im Wesentlichen in einer den verfassungsrechtlichen Anforderungen entsprechenden Weise gewährleistet. Die Erhebung der nach § 113a TKG gespeicherten Daten bedarf gemäß § 100g Abs. 2 Satz 1, § 100b Abs. 1 Satz 1 StPO der Anordnung durch den Richter. Des Weiteren bestehen gemäß § 101 StPO differenzierte Benachrichtigungspflichten sowie die Möglichkeit, nachträglich eine gerichtliche Überprüfung der Rechtmäßigkeit der Maßnahme herbeizuführen. Dass diese Vorschriften einen effektiven Rechtsschutz insgesamt nicht gewährleisten, ist nicht ersichtlich. Verfassungsrechtlich zu beanstanden ist hingegen das Fehlen einer richterlichen Kontrolle für das Absehen von einer Benachrichtigung gemäß § 101 Abs. 4 StPO. Unmittelbare Verwendung der Daten für die Gefahrenabwehr und für die Aufgaben der Nachrichtendienste:

§ 113b Satz 1 Nr. 2 und 3 TKG genügt den Anforderungen an eine hinreichende Begrenzung der Verwendungszwecke schon seiner Anlage nach nicht. Der Bundesgesetzgeber begnügt sich hier damit, in lediglich generalisierender Weise die Aufgabenfelder zu umreißen, für die ein Datenabruf nach Maßgabe späterer Gesetzgebung, insbesondere auch der Länder, möglich sein soll. Damit kommt er seiner Verantwortung für die verfassungsrechtlich gebotene Begrenzung der Verwendungszwecke nicht nach. Vielmehr schafft der Bundesgesetzgeber durch die Pflicht der Diensteanbieter zur vorsorglichen Speicherung aller Telekommunikationsverkehrsdaten, verbunden gleichzeitig mit der Freigabe dieser Daten für die Verwendung durch die Polizei und die Nachrichtendienste im Rahmen annähernd deren gesamter Aufgabenstellung, ein für vielfältige und unbegrenzte Verwendungen offenen Datenpool, auf den nur durch grobe Zielsetzungen beschränkt jeweils aufgrund eigener Entscheidungen der Gesetzgeber in Bund und Ländern zugegriffen werden kann. Die Bereitstellung eines solchen seiner Zwecksetzung nach offenen Datenpools hebt den

notwendigen Zusammenhang zwischen Speicherung und Speicherungszweck auf und ist mit der Verfassung nicht vereinbar.

Die Ausgestaltung der Verwendung der nach § 113a TKG gespeicherten Daten ist auch insoweit unverhältnismäßig, als für die Übermittlung keinerlei Schutz von Vertrauensbeziehungen vorgesehen ist. Zumindest für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen ist ein solcher Schutz grundsätzlich geboten.

Mittelbare Nutzung der Daten für Auskünfte der Diensteanbieter:

Nicht in jeder Hinsicht genügt auch § 113b Satz 1 Halbsatz 2 TKG den verfassungsrechtlichen Anforderungen. Zwar begegnet es keinen Bedenken, dass nach dieser Vorschrift Auskünfte unabhängig von einem Straftaten oder Rechtsgüterkatalog zulässig sind. Nicht mit der Verfassung zu vereinbaren ist demgegenüber, dass solche Auskünfte ohne weitere Begrenzung auch allgemein für die Verfolgung von Ordnungswidrigkeiten ermöglicht werden. Auch fehlt es an Benachrichtigungspflichten im Anschluss an solche Auskünfte.

6. Vereinbarkeit mit Art. 12 GG

Demgegenüber sind die angegriffenen Vorschriften hinsichtlich Art. 12 Abs. 1 GG, soweit in diesem Verfahren hierüber zu entscheiden ist, keinen verfassungsrechtlichen Bedenken ausgesetzt. Die Auferlegung der Speicherungspflicht wirkt gegenüber den betroffenen Diensteanbietern typischerweise nicht übermäßig belastend. Unverhältnismäßig ist die Speicherungspflicht insbesondere nicht in Bezug auf die finanziellen Lasten, die den Unternehmen durch die Speicherungspflicht nach § 113a TKG und die hieran knüpfenden Folgeverpflichtungen wie die Gewährleistung von Datensicherheit erwachsen. Der Gesetzgeber ist innerhalb seines insoweit weiten Gestaltungsspielraums nicht darauf beschränkt, Private nur dann in Dienst zu nehmen, wenn ihre berufliche Tätigkeit unmittelbar Gefahren auslösen kann oder sie hinsichtlich dieser Gefahren unmittelbar ein Verschulden trifft. Vielmehr reicht insoweit eine hinreichende Sach und Verantwortungsnähe zwischen der beruflichen Tätigkeit und der auferlegten Verpflichtung. Gegen die den Speicherungspflichtigen erwachsenden Kostenlasten bestehen danach keine grundsätzlichen Bedenken. Der Gesetzgeber verlagert auf diese Weise die mit der Speicherung verbundenen Kosten entsprechend der Privatisierung des Telekommunikationssektors insgesamt in den Markt. So wie die Telekommunikationsunternehmen die neuen Chancen der Telekommunikationstechnik zur Gewinnerzielung nutzen können, müssen sie auch die Kosten für die Einhegung der neuen Sicherheitsrisiken, die mit der Telekommunikation verbunden sind, übernehmen und in ihren Preisen verarbeiten.

7. Nichtigkeit der angegriffenen Vorschriften

Der Verstoß gegen das Grundrecht auf Schutz des Telekommunikationsgeheimnisses nach Art. 10 Abs. 1 GG führt zur Nichtigkeit der §§ 113a und 113b TKG sowie von § 100g Abs. 1 Satz 1 StPO, soweit danach Verkehrsdaten gemäß § 113a TKG erhoben werden dürfen. Die angegriffenen Normen sind daher unter Feststellung der Grundrechtsverletzung für nichtig zu erklären (vgl. § 95 Abs. 1 Satz 1 und § 95 Abs. 3 Satz 1 BVerfGG).

Die Entscheidung ist hinsichtlich der europarechtlichen Fragen, der formellen Verfassungsmäßigkeit und der grundsätzlichen Vereinbarkeit der vorsorglichen Telekommunikationsverkehrsdatenspeicherung mit der Verfassung im Ergebnis einstimmig ergangen. Hinsichtlich der Beurteilung der §§ 113a und 113b TKG als verfassungswidrig ist sie im Ergebnis mit 7:1 Stimmen und hinsichtlich weiterer materiellrechtlicher Fragen, soweit aus den Sondervoten ersichtlich, mit 6:2 Stimmen ergangen.

Dass die Vorschriften gemäß § 95 Abs. 3 Satz 1 BVerfGG für nichtig und nicht nur für unvereinbar mit dem Grundgesetz zu erklären sind, hat der Senat mit 4:4 Stimmen entschieden. Demzufolge können

die Vorschriften auch nicht in eingeschränktem Umfang übergangsweise weiter angewendet werden, sondern verbleibt es bei der gesetzlichen Regelfolge der Nichtigerklärung.

Sondervotum des Richters Schluckebier:

1. In der Speicherung der Verkehrsdaten für die Dauer von sechs Monaten bei den Diensteanbietern liegt kein Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG von solchem Gewicht, dass er als "besonders schwer" und damit gleichermaßen klassifiziert werden könnte wie ein unmittelbarer Zugriff durch die öffentliche Gewalt auf Kommunikationsinhalte. Die Verkehrsdaten verbleiben in der Sphäre der privaten Diensteanbieter, bei denen sie aus betriebstechnischen Gründen anfallen und von denen der einzelne Telekommunikationsteilnehmer aufgrund der vertraglichen Bindung erwarten kann, dass diese sie in ihrer Sphäre strikt vertraulich behandeln und schützen. Wird die nach dem Stand der Technik mögliche Datensicherheit gewährleistet, so fehlt deshalb auch eine objektivierbare Grundlage für die Annahme eines speicherungsbedingten Einschüchterungseffekts beim Bürger. Die Speicherung erstreckt sich nicht auf den Inhalt der Telekommunikation. Bei der Gewichtung des Eingriffs muss deshalb eine wahrnehmbare Distanz zu solchen besonders schweren Eingriffen gewahrt bleiben, wie sie bei der akustischen Wohnraumüberwachung, der inhaltlichen Telekommunikationsüberwachung oder der sogenannten Online-Durchsuchung informationstechnischer Systeme durch unmittelbaren Zugriff staatlicher Organe vorliegen, und bei denen in besonderem Maße das Risiko besteht, dass der absolut geschützte Kernbereich privater Lebensgestaltung betroffen wird. Besonders eingriffsintensiv ist danach nicht bereits die Speicherung der Verkehrsdaten beim Diensteanbieter, sondern erst der Abruf und die Nutzung der Verkehrsdaten durch staatliche Stellen im Einzelfall nach den dafür bestehenden Rechtsgrundlagen; diese wie auch die richterliche Anordnung der Verkehrsdatenerhebung unterliegen ihrerseits den strikten Anforderungen der Verhältnismäßigkeit.

2. Die angegriffenen Regelungen sind im Grundsatz nicht unangemessen, den Betroffenen zumutbar und damit verhältnismäßig im engeren Sinne. Der Gesetzgeber hat sich mit der Pflicht zur Speicherung der Telekommunikationsverkehrsdaten für die Dauer von sechs Monaten, einer Verwendungszweckregelung und der strafprozessrechtlichen Erhebungsregelung in dem ihm von Verfassungs wegen zukommenden Gestaltungsrahmen gehalten. Die Schutzpflicht des Staates gegenüber seinen Bürgern schließt die Aufgabe ein, geeignete Maßnahmen zu ergreifen, um die Verletzung von Rechtsgütern zu verhindern oder sie aufzuklären und die Verantwortung für Rechtsgutsverletzungen zuzuweisen. In diesem Sinne zählt die Gewährleistung des Schutzes der Bürger und ihrer Grundrechte sowie der Grundlagen des Gemeinwesens und die Verhinderung wie die Aufklärung bedeutsamer Straftaten zugleich zu den Voraussetzungen eines friedlichen Zusammenlebens und des unbeschwerten Gebrauchs der Grundrechte durch den Bürger. Effektive Aufklärung von Straftaten und wirksame Gefahrenabwehr sind daher nicht per se eine Bedrohung für die Freiheit der Bürger.

In dem Spannungsverhältnis zwischen der Pflicht des Staates zum Rechtsgüterschutz und dem Interesse des Einzelnen an der Wahrung seiner von der Verfassung verbürgten Rechte ist es zunächst Aufgabe des Gesetzgebers, in abstrakter Weise einen Ausgleich der widerstreitenden Interessen zu erreichen. Ihm kommt dabei ein Einschätzungs- und Gestaltungsspielraum zu. Ziel des Gesetzgebers war es hier, den unabweisbaren Bedürfnissen einer wirksamen, rechtsstaatlichen Strafrechtspflege angesichts einer grundlegenden Veränderung der Kommunikationsmöglichkeiten und des Kommunikationsverhaltens der Menschen in den letzten Jahren Rechnung zu tragen. Dieses Ziel setzt grundsätzlich die Ermittelbarkeit der zur Aufklärung erforderlichen Tatsachen voraus. Dabei ist der Gesetzgeber davon ausgegangen, dass gerade Telekommunikationsverkehrsdaten aufgrund der technischen Entwicklung hin zu Flatrates oftmals entweder überhaupt nicht gespeichert werden oder bereits wieder gelöscht sind, bevor eine richterliche Anordnung zur Auskunftserteilung erwirkt werden kann oder auch nur die für einen entsprechenden Antrag erforderlichen Informationen ermittelt sind. Die Tatsache, dass elektronische oder digitale Kommunikationsmittel in nahezu alle Lebensbereiche vorgedrungen sind und deshalb in bestimmten Bereichen die Strafverfolgung und auch die Gefahrenabwehr erschweren, berücksichtigt die Senatsmehrheit zwar bei der Prüfung der Geeignetheit und Erforderlichkeit der Verkehrsdatenspeicherung, gewichtet sie aber bei der

Verhältnismäßigkeitsprüfung im engeren Sinne unter dem Aspekt der Angemessenheit und Zumutbarkeit nicht in dem gebotenen Maße.

Die Senatsmehrheit schränkt damit zugleich den Einschätzungs- und Gestaltungsspielraum des Gesetzgebers, auf dem Felde der Straftatenaufklärung und der Gefahrenabwehr zum Schutz der Menschen angemessene und zumutbare Regelungen zu treffen, im praktischen Ergebnis nahezu vollständig ein. Dadurch trägt sie auch dem Gebot verfassungsrichterlicher Zurückhaltung ("judicial self-restraint") gegenüber konzeptionellen Entscheidungen des demokratisch legitimierten Gesetzgebers nicht hinreichend Rechnung. Das Urteil gibt eine Speicherdauer von sechs Monaten also dem durch die EG-Richtlinie geforderten Mindestmaß als an der Obergrenze liegend und verfassungsrechtlich allenfalls rechtfertigungsfähig vor, schreibt dem Gesetzgeber regelungstechnisch vor, dass die Verwendungszweckregelung zugleich die Zugriffsvoraussetzungen enthalten muss, beschränkt ihn auf eine Katalogtatentechnik im Strafrecht, schließt die Möglichkeit der Nutzung der Verkehrsdaten auch zur Aufklärung von mittels Telekommunikationsmitteln begangenen schwer aufklärbaren Straftaten aus und erweitert die Benachrichtigungspflichten in bestimmter Art. Danach bleibt dem Gesetzgeber kein nennenswerter Spielraum mehr für eine Ausgestaltung in eigener politischer Verantwortung.

Der Senat verwehrt dem Gesetzgeber insbesondere die Abrufbarkeit der nach § 113a TKG gespeicherten Verkehrsdaten für die Aufklärung von Straftaten, die nicht im derzeitigen Katalog des § 100a Abs. 2 StPO bezeichnet, aber im Einzelfall von erheblicher Bedeutung sind, sowie von solchen Taten, die mittels Telekommunikation begangen sind (§ 100g Abs. 1 Satz 1 Nr. 1 und 2 StPO). Hinsichtlich der letztgenannten Taten wird nicht genügend gewichtet, dass der Gesetzgeber hier von erheblichen Aufklärungsschwierigkeiten ausgeht. Da es Sache des Gesetzgebers ist, eine wirksame Strafverfolgung zu gewährleisten und keine beträchtlichen Schutzlücken entstehen zu lassen, kann es ihm nicht versagt sein, auch bei Straftaten, die zwar nicht besonders schwer sind, aber Rechtsgüter von Gewicht schädigen den Zugriff auf die Verkehrsdaten zu eröffnen, weil nach seiner Einschätzung nur so das Entstehen faktisch weitgehend rechtsfreier Räume und ein weitgehendes Leerlaufen der Aufklärung ausgeschlossen werden kann. Hinzu kommt, dass sich der Gesetzgeber bei der Gestaltung der strafprozessualen Zugriffsbefugnis an Kriterien orientiert hat, die der Senat in seinem Urteil vom 12. März 2003 (BVerfGE 107, 299) zur Herausgabe von Verbindungsdaten der Telekommunikation gebilligt hat.

3. Im Rechtsfolgenausspruch hätte es auch auf der Grundlage der verfassungsrechtlichen Würdigung der Senatsmehrheit unter Rückgriff auf eine ständige Rechtsprechung des Bundesverfassungsgerichts nahe gelegen, dem Gesetzgeber eine Frist für eine Neuregelung zu setzen und die bestehenden Vorschriften in Anlehnung an die Maßgaben der vom Senat erlassenen einstweiligen Anordnungen für vorübergehend weiter anwendbar zu erklären, um nachhaltige Defizite insbesondere bei der Aufklärung von Straftaten, aber auch bei der Gefahrenabwehr zu vermeiden.

Sondervotum Richter Eichberger:

Das Sondervotum schließt sich der Kritik des Richters Schluckebier an der Beurteilung der Eingriffsintensität der Speicherung der Telekommunikationsverkehrsdaten als Eingriff in Art. 10 Abs. 1 GG im Wesentlichen an. Die den §§ 113a, 113b TKG zugrunde liegende gesetzgeberische Konzeption einer gestuften legislativen Verantwortung für die Speicherungsanordnung auf der einen Seite und den Datenabruf auf der anderen Seite steht im Grundsatz mit der Verfassung in Einklang. Dies gilt insbesondere für die in § 100g StPO geregelte Verwendung der nach § 113a TKG gespeicherten Daten zu Zwecken der Strafverfolgung. Der Gesetzgeber ist nicht gezwungen die Verhältnismäßigkeit der Abrufregelung ausschließlich an dem größtmöglichen Eingriff eines umfassenden, letztlich auf ein Bewegungs- oder Sozialprofil des betroffenen Bürgers abzielenden Datenabrufs zu messen, sondern darf berücksichtigen, dass eine Vielzahl von Datenabfragen weitaus geringeres Gewicht haben, über deren Zumutbarkeit im Einzelfall der hierzu berufene Richter zu entscheiden hat.