Osnabrücker Jahrbuch
Frieden und Wissenschaft
16 / 2009

Neue Fragen an den Rechtsstaat

Wie begegnen Politik, Recht und Exekutive aktuellen Friedensgefährdungen?

■ OSNABRÜCKER FRIEDENSGESPRÄCHE 2008

■ MUSICA PRO PACE 2008

■ BEITRÄGE ZUR FRIEDENSFORSCHUNG

Herausgegeben vom Oberbürgermeister der
Stadt Osnabrück und dem Präsidenten der
Universität Osnabrück

V&R unipress

Jens-Peter Schneider, Osnabrück

Rechtsstaatliche Sicherheit in der europäischen Informationsgesellschaft am Beispiel der Vorratsdatenspeicherung

I. Einleitung — Terrorismus und Organisierte Kriminalität stellen erhebliche sicherheitspolitische Bedrohungen dar. Bedrohlich können allerdings auch die staatlichen Reaktionen auf diese Bedrohungen sein, wenn sie die rechtsstaatlichen und freiheitsrechtlichen Leitplanken der Sicherheitspolitik nicht hinreichend beachten. Beide Bedrohungen sind für die Bürger oft schwer greifbar, solange sie sich nicht aktuell erkennbar verwirklicht haben. Insbesondere Verluste an rechtsstaatlicher Freiheit und Sicherheit treten schleichend ein. Zudem meinen viele Bürger, dass sie persönlich davon nicht betroffen seien und auch nicht betroffen sein werden.

Die hier erörterte *Vorratsdatenspeicherung* bezieht sich auf die sogenannten Verkehrsdaten aller Telekommunikationsnutzer und damit in der modernen Informationsgesellschaft auf nahezu sämtliche Bürger. Dabei zeichnet sich die Vorratsdatenspeicherung durch verschiedene Eingriffsstufen aus:

- Speicherung der Daten durch die Telekommunikationsdienstleister,
- in der Regel heimlicher Abruf der Daten durch Sicherheitsbehörden,
- Auswertung der Daten und Nutzung derselben zu weiteren Ermittlungs-, Gefahrenabwehr- oder Strafverfolgungsmaßnahmen,
- ggf. Weitergabe an Private, die ihrerseits aufgrund der Daten zivilrechtliche Schritte etwa zur Verfolgung von Urheberrechtsverletzungen einleiten.

Durch die verdachtslose Speicherung der Daten ist zunächst jeder Telekommunikationsnutzer aktuell betroffen. Vor allem aber ist jeder dem Risiko ausgesetzt, aufgrund einer Verkehrsdateninterpretation in einen falschen Verdacht zu geraten und dadurch zum Gegenstand von sich anschließenden, ggf. stark belastenden Eingriffen zu werden. Durch die intensive journalistische und gesellschaftliche Diskussion über die Vorratsdatenspeicherung sind diese Freiheitsbeschränkungen inzwischen auch in Teilen der Bevölkerung präsent und scheinen nach ersten Umfragen in durchaus relevantem Maße das Kommunikationsverhalten in Deutschland zu beeinflussen.[1]

Für die juristische Debatte über die Vorratsdatenspeicherung, die derzeit aufgrund mehrerer Verfassungsbeschwerden vor allem vor dem Bundesverfassungsgericht (BVerfG) geführt wird, ist deren doppelte rechtliche Grundlegung in einer Richtlinie der Europäischen Gemeinschaft (Richtlinie 2006/24/EG)[2] einerseits und in einem deutschen Parlamentsgesetz[3] andererseits von besonderer Bedeutung. Hieraus folgt nämlich eine komplexe Abschichtung und Zuordnung der grundrechtlichen Maßstäbe sowie der gerichtlichen Zuständigkeiten für die Überprüfung der Rechtsgrundlagen der Vorratsdatenspeicherung. Konkret geht es um die rechtsstaatliche Sicherung der *informationellen Selbstbestimmung* bzw. des Fernmeldegeheimnisses einerseits durch das BVerfG am Maßstab des Grundgesetzes (GG) und andererseits durch den Europäischen Gerichtshof (EuGH) am Maßstab europäischer Grundrechte.

Diese komplexen Wechselwirkungen und Ebenenverflechtungen stehen im Zentrum der nachfolgenden Überlegungen. Die Kernfrage lautet dabei, inwieweit die europäische Gewährleistung von Rechtsstaatlichkeit mit der Europäisierung der Sicherheitspolitik Schritt hält oder ihr gegenüber in Rückstand geraten ist bzw. zu geraten droht.

II. Geltung der nationalen Grundrechte außerhalb zwingender Vorgaben der Richtlinie 2006/24/EG — Seit der Entscheidung des 1. Senats vom 13. März 2007 ist bis auf weiteres davon auszugehen, dass die Solange-Grundsätze des BVerfG zur Abschichtung der Wahrnehmung von Prüfungskompetenzen im Grundrechtsbereich zwischen BVerfG und EuGH[4] auch für die verfassungsrechtliche Kontrolle nationaler Umsetzungsakte von EG-Richtlinien gelten. Danach ist das BVerfG »grundsätzlich gehindert, über die Gültigkeit von Gemeinschaftsrecht zu entscheiden, da es sich hier nicht um einen Akt deutscher Staatsgewalt handelt«.[5] Ferner wird »[a]uch eine innerstaatliche Rechtsvorschrift, die eine Richtlinie in deutsches Recht umsetzt, [...] insoweit nicht an den Grundrechten des Grundgesetzes gemessen, als das Gemeinschaftsrecht keinen Umsetzungsspielraum lässt, sondern zwingende Vorgaben macht.«[6] Spielraum-Entscheidungen des Umsetzungsgesetzgebers außerhalb zwingender Richtlinienvorgaben überprüft das BVerfG jedoch am Maßstab der deutschen Grundrechte. Insbesondere hat der Umsetzungsgesetzgeber bei mehreren Umsetzungsoptionen den Verhältnismäßigkeitsgrundsatz zu beachten, also in der Formulierung der EU-Haftbefehlsentscheidung des 2. Senats Umsetzungsspielräume in einer grundrechtsschonenden Weise auszufüllen.[7]

Deshalb ist es von maßgeblicher Bedeutung, dass die Richtlinie 2006/24/EG den Mitgliedstaaten in erheblichem Umfang Umsetzungsspielräume belässt und nur wenige zwingende Mindestvorgaben[8] trifft: Zwingend festgelegt sind die mindestens zu speichernden Datenkategorien und

Datentypen sowie die gemeinschaftsrechtliche Mindestspeicherdauer von 6 Monaten. Beträchtliche und vom deutschen Umsetzungsgesetzgeber in beachtlichem Maße genutzte Umsetzungsspielräume bestehen bezüglich der Speicher- und Verwendungszwecke sowie – ohne dass dies hier aus Raumgründen näher ausgeführt werden kann – hinsichtlich der zugriffsberechtigten Stellen, der Zugriffsvoraussetzungen und -verfahren, der Zweckbindung und der Anforderungen an die Datensicherheit.

Art. 1 I der Richtlinie 2006/24/EG erwähnt als Zweck der Vorratsdatenspeicherung die Gewährleistung, dass Verkehrsdaten zum Zwecke der Ermittlung, Feststellung und Verfolgung von *schweren Straftaten* zur Verfügung stehen. Damit unterliegt die in § 113b des Telekommunikationsgesetzes (TKG) vorgenommene Festlegung weiterer Verwendungszwecke für auf Vorrat gespeicherte Daten zur Gefahrenabwehr und für Geheimdienstzwecke uneingeschränkter verfassungsrechtlicher Kontrolle. Dies gilt partiell sogar für die Verwendung zu Strafverfolgungszwecken. Art. 1 I und Erwägungsgrund 21 der Richtlinie 2006/24/EG legen die Konkretisierung des unbestimmten Rechtsbegriffs der »schweren Straftaten« durch die Formulierung: »wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden«, nämlich ausdrücklich weitgehend in die Hand der Mitgliedstaaten.[9] Gemeinschaftsrechtlich zwingend vorgegeben ist durch verschiedene Bezugnahmen in den Erwägungsgründen 7 bis 10 lediglich,[10] dass die Mitgliedstaaten insbesondere die Organisierte Kriminalität sowie terroristische Akte als schwere Straftaten einzustufen haben.[11] Irrelevant ist es deshalb, dass in anderen strafrechtsbezogenen Gemeinschaftsrechtsakten unter den Begriffen der »schweren Straftaten« bzw. der »serious crimes« auch minder schwere Delikte zu verstehen sind.[12]

Wegen der Unbestimmtheit der beiden Begriffe *Terrorismus* und *Organisierte Kriminalität* ist aber selbst diese Vorgabe weniger klar, als es vordergründig erscheinen mag. Insgesamt führt die Richtlinie 2006/24/EG die betonte Berücksichtigung nationaler Souveränität in Fragen der inneren Sicherheit fort,[13] weshalb nur der gemeineuropäische Begriffskern der beiden Begriffe als zwingende Vorgabe anzusehen ist. Hierfür spricht auch die vom EuGH akzeptierte, binnenmarktbezogene Kompetenzgrundlage der Richtlinie,[14] aufgrund derer das mitgliedstaatliche Strafrecht nur in dem Maße angeglichen werden darf, wie es zur Gewährleistung eines funktionierenden Binnenmarkts erforderlich ist. Zu welchen genauen Zwecken die Daten zu speichern sind, ist jedoch für die Belastung der speichernden Unternehmen weitgehend belanglos.

III. Rechtsstaatliche Kontrolle der zwingenden Richtlinienvorgaben — Zwar belässt die Richtlinie 2006/24/EG den Mitgliedstaaten, wie die

vorstehenden Ausführungen gezeigt haben, im großen Umfang Umsetzungsspielräume. Zwingend vorgegeben sind jedoch insbesondere
– die sechsmonatige Speicherpflicht von Anbietern öffentlicher Telekommunikationsdienste für die in Art. 5 der Richtlinie 2006/24/EG aufgeführten Datenkategorien;
– die Verwendung dieser Daten zur staatlichen Verfolgung schwerer Straftaten in Gestalt der – hier eng zu verstehenden – Organisierten Kriminalität und des Terrorismus.

Die insoweit aus der Solange-Rechtsprechung folgende Sperre für eine Überprüfung der Regelungen zur Vorratsdatenspeicherung an den deutschen Grundrechten entfiele, sofern der EuGH auf eine Vorlage durch das BVerfG oder anderer mitgliedstaatlicher Gerichte im Vorabentscheidungsverfahren gemäß Art. 234 des EG-Vertrages (EGV) die Ungültigkeit der Richtlinie feststellte.

a) Zulässigkeit und Notwendigkeit einer Vorlage an den EuGH durch das BVerfG — Die Frage nach der Ungültigkeit der Richtlinie 2006/24/EG wegen eines Verstoßes gegen das europäische Grundrecht auf Privatheit ist ein zulässiger Vorlagegegenstand gemäß Art. 234 EGV.[15] Eine Gültigkeitsvorlage verlangt nicht, dass das vorlegende nationale Gericht von der Ungültigkeit der Richtlinie abschließend überzeugt ist. Für eine Vorlagebefugnis genügen bereits Zweifel an der primärrechtlichen Rechtmäßigkeit der Richtlinie.[16] Die vom EuGH Anfang 2009 als unbegründet abgewiesene Nichtigkeitsklage Irlands gegen die Richtlinie 2006/24/EG[17] schließt die Zulässigkeit einer Vorlage durch deutsche Gerichte nicht aus, soweit sich diese auf bislang nicht entschiedene rechtliche Gesichtspunkte bezieht.[18] Da sich die irische Klage auf die Wahl der Ermächtigungsgrundlage beschränkte[19] und der EuGH ausdrücklich von einer Prüfung grundrechtlicher Fragen absah,[20] bleibt eine Vorlage wegen Verstößen der Richtlinie gegen Gemeinschaftsgrundrechte weiter zulässig. Die Voraussetzung der Entscheidungserheblichkeit[21] ist erfüllt, weil bei einer Nichtigerklärung der Richtlinie durch den EuGH zwar das deutsche Umsetzungsgesetz nicht automatisch unbeachtlich wird, jedoch eine Überprüfung durch das BVerfG anhand der deutschen Grundrechte hinsichtlich aller Gesetzesregelungen zur Vorratsdatenspeicherung eröffnet wird.[22]

Bislang erfolgt der Grundrechtsschutz gegenüber gemeinschaftsrechtlich zwingend vorgegebenen nationalen Umsetzungsakten primär im Wege einer Vorlage an den EuGH seitens der zuständigen Fachgerichte, also etwa der Verwaltungs- oder Strafgerichte. Diese sind ggf. sogar verfassungsrechtlich verpflichtet, die Prüfungs- und Verwerfungskompetenz des EuGH zu beachten und ein Vorabentscheidungsverfahren gemäß Art. 234 EGV einzuleiten.[23] Nur abstrakt hat das BVerfG in früheren Urteilen auch

die Möglichkeit einer eigenen Vorlage angedeutet,[24] von dieser Option aber bislang noch nie Gebrauch gemacht, sondern die Fachgerichte in die Pflicht genommen. Deshalb stellt sich die Frage, ob das BVerfG in den gegen das Gesetz über die Vorratsdatenspeicherung anhängigen Verfassungsbeschwerdeverfahren erstmals ein Vorabentscheidungsverfahren beim EuGH einleiten soll.

Eine Vorlage durch die Fachgerichte ist in vielen Prozesssituationen unproblematisch und sachgerecht, insbesondere wenn die Fachgerichte bereits mit der Prüfung einer Gemeinschaftsnorm befasst sind. Bei der Vorratsdatenspeicherung besteht jedoch die Ausnahmesituation einer unmittelbar gegen das Gesetz selbst zulässigen Verfassungsbeschwerde. Hier würde eine vom Verfassungsgericht ungeprüfte partielle Abschirmung des deutschen Umsetzungsrechtsakts aus Rücksicht auf die oben genannten zwingenden EG-Vorgaben die grundlegende Grundrechtsbeeinträchtigung durch die Vorratsdatenspeicherung selbst ausblenden.[25] Die einschlägigen Grundrechte sind aber bereits durch die Vorratsdatenspeicherung für sich genommen verletzt. Die Grundrechtsträger trotz der Zulässigkeit einer Gesetzesverfassungsbeschwerde, die sich gerade auf die von der Streuwirkung der anlasslosen Speicherung ausgehende allgemeine Bedeutung der aufgeworfenen Verfassungsfragen gründet, auf den Rechtsweg zu den Fachgerichten zu verweisen, hat diverse Nachteile, die nur durch eine unmittelbare Vorlage der Grundrechtsfragen durch das BVerfG selbst vermieden werden können:

Die andernfalls ›hinkende‹ Grundrechtsprüfung würde den Grundrechtsschutz erheblich und für die Bürger kaum verständlich schwächen.[26] Sie wäre auch alles andere als prozessökonomisch, da die unbeantworteten Grundrechtsfragen dem BVerfG durch ein Fachgericht alsbald erneut vorgelegt werden könnten. Sobald der EuGH aufgrund einer fachgerichtlichen Gültigkeitsvorlage die Richtlinie 2006/24/EG wegen eines Verstoßes gegen Gemeinschaftsgrundrechte für nichtig erklärt hätte, stünde einer konkreten Normenkontrolle nach Art. 100 GG nämlich kein Hindernis mehr entgegen.[27] Im Zusammenhang mit der Vorratsdatenspeicherung kommt hinzu, dass fachgerichtlicher Rechtsschutz keineswegs unproblematisch zu erlangen wäre. Schließlich wirft die Bestimmung der zwingenden Vorgaben der Richtlinie 2006/24/EG angesichts der vorstehend aufgezeigten Unbestimmtheit des Begriffs der »schweren Straftaten« diffizile – nach der strengen EuGH-Rechtsprechung[28] zu einer Vorlage verpflichtende – gemeinschaftsrechtliche Auslegungsfragen auf. Eine Vorlage seitens des BVerfG auf diese Abgrenzungsfrage zu beschränken, wäre aber offenkundig unzweckmäßig.

In der Literatur wird eine Vorlage des BVerfG an den EuGH gleichwohl als »kein wahrscheinliches Szenario« eingestuft.[29] Das BVerfG würde zu

»einer Durchlaufstation auf dem Weg zum EuGH gemacht werden« und »letztlich zu einer Art Vorprüfungsausschuss des EuGH ohne Kompetenz zur eigenständigen Entscheidung«, weshalb es zweifelhaft sei, »ob das BVerfG diesen Schritt, der pointiert als Selbstdegradierung verstanden werden könnte, zu tun bereit wäre«.[30] Eine solche Sichtweise verkennt meines Erachtens das institutionelle Selbstbewusstsein des BVerfG, dessen Rechtsprechung zwar auf eine konfliktvermeidende Abschichtung von Kontrollkompetenzen zwischen BVerfG und EuGH gerichtet ist, aber zugleich das Kooperationsverhältnis beider Gerichte betont. Dieses besteht in einem gleichberechtigten judiziellen Dialog im europäischen Mehrebenensystem, in dem BVerfG und EuGH als jeweils letztentscheidende Hüter der rechtlichen Grundlagen der nationalen Ebene einerseits und der Gemeinschaftsebene andererseits interagieren, ohne dass die Bedeutung und Eigenständigkeit einer der beiden Gerichtsbarkeiten in Frage gestellt würde.[31] Die Nutzung des Vorabentscheidungsverfahrens durch das BVerfG eröffnet eine funktionsfähige Schnittstelle, um den reichen Erfahrungsschatz des BVerfG bei der grundrechtssichernden Begleitung der Sicherheitspolitik auch auf der Gemeinschaftsebene fruchtbar werden zu lassen. Dies gilt umso mehr, weil entsprechende materielle Rechtsfragen aufgrund des bisherigen wirtschaftsrechtlichen Schwerpunkts der EuGH-Rechtsprechung auf europäischer Ebene noch eine entwicklungsbedürftige Materie darstellen und etwa auch in der Fluggastdaten-Entscheidung[32] nicht erörtert werden mussten. Gleichzeitig werden sie jedoch wegen der zunehmenden sicherheitspolitischen Aktivitäten auf europäischer Ebene[33] zukünftig in der Rechtsprechung der Gemeinschaftsgerichte größeres Gewicht erhalten.

Eine Vorlage wäre ein wichtiger Beitrag zur Gewährleistung der Grundrechtskohärenz in Europa. Durch eine Vorlage könnte das BVerfG die deutsche Grundrechtstradition im Bereich der öffentlichen Sicherheit weit besser im Sinne des Art. 6 II des EU-Vertrages (EUV) zu einem Baustein der europäischen Grundrechtsarchitektur werden lassen, als wenn es vom Rande aus beobachtete, wie die deutschen Fachgerichte mit ihrer zwar nicht zu unterschätzenden, aber doch im Vergleich deutlich geringeren Autorität auf diesem Gebiet mit dem EuGH kommunizieren. Das BVerfG sollte dem EuGH nicht aus dem Weg gehen, sondern danach trachten, dessen Grundrechtsprechung über das Instrument einer Vorlage nach Art. 234 EGV aktiv mitzugestalten. Das BVerfG würde sich durch eine Vorlage der langen Reihe anderer ebenso traditions- wie selbstbewusster oberster (Verfassungs-)Gerichte der Mitgliedstaaten wie etwa dem *House of Lords* oder dem dänischen *Hojesteret* anschließen, die – teilweise bereits seit langem – immer wieder Vorlagen an den EuGH richten.[34] Besonders bemerkenswert ist insoweit eine Entscheidung des italienischen Verfas-

sungsgerichts vom April 2008, mit der dieses seine bisherige Zurückhaltung aufgegeben hat und dem EuGH Fragen zur Vorabentscheidung vorgelegt hat.[35] Wie hier vorgeschlagen, ist das italienische Verfassungsgericht nunmehr jedenfalls in der Sondersituation einer Direktklage ohne Vorbefassung der Fachgerichte zu Vorlagen an den EuGH bereit.

b) Verstoß der Richtlinie 2006/24/EG gegen Gemeinschaftsgrundrechte – Mit welchem Ausgang wäre bei einer Gültigkeitsvorlage durch das BVerfG an den EuGH zu rechnen? Entscheidend ist, ob die Richtlinie 2006/24/EG gegen das vom EuGH zumindest im Grundsatz anerkannte Gemeinschaftsgrundrecht auf Datenschutz verstößt.[36] Die Generalanwältin *Juliane Kokott* hat ausdrücklich und unter Hinweis auf die Richtlinie 2006/24/EG Zweifel an der Vereinbarkeit einer verdachtslosen Vorratsdatenspeicherung mit europäischen Grundrechten geäußert, wie sie zuvor bereits von den europäischen Datenschutzbeauftragten und anderen vorgebracht wurden. [37] Allerdings musste die Generalanwältin wegen mangelnder Entscheidungserheblichkeit in der vorliegenden Rechtssache auf eine abschließende Prüfung der Gültigkeit der Richtlinie 2006/24/EG verzichten.

Eingriff in den Schutzbereich — Einschlägig ist insbesondere das Urteil des EuGH in der Rechtssache C-465/00,[38] in dem dieser die europäische Datenschutzrichtlinie 95/46 im Lichte des Grundrechts auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten auslegte. Dieses Gemeinschaftsgrundrecht wird vom EuGH jedenfalls in dieser Entscheidung mit dem *Recht auf Privatheit* gemäß Art. 8 der Europäischen Menschenrechtskonvention (EMRK), wie es in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) entwickelt wurde, gleichgesetzt.[39] Daher erscheint es in besonderem Maße gerechtfertigt, zur nachfolgenden Konkretisierung des Gemeinschaftsgrundrechts die Rechtsprechung des EGMR heranzuziehen.

Dies gilt insbesondere für die Definition des Schutzbereichs und die Eingriffsfeststellung. Für Telekommunikationsüberwachungsmaßnahmen greift der EGMR auf die in Art. 8 EMRK parallel garantierten Rechte auf Achtung des Privatlebens und der Korrespondenz zurück.[40] Dabei wird das Recht auf Privatheit sehr weit verstanden, so dass auch (öffentliche) Kommunikationen mit beruflichem Hintergrund oder im politischen Meinungskampf ggf. in den Schutz einbezogen werden.[41] Ergänzend wäre mit Blick auf die Speicherung von Internetverbindungsdaten noch ein Eingriff in die Informationsfreiheit gemäß Art. 10 I 2 EMRK zu erwägen.

Diskutiert wird teilweise, ob der EuGH bereits die bloße Datenspeicherung als rechtfertigungsbedürftigen Eingriff erachtet. Dies wird gelegentlich unter Hinweis auf die Tz. 74 des ORF-Urteils verneint,[42] wodurch

eventuell die grundrechtlichen Bedenken gegen die erste Stufe der Vorratsdatenspeicherung auf der europäischen Ebene nicht zum Tragen kämen. Der EuGH formuliert dort wie folgt:

> »Zwar kann die bloße Speicherung personenbezogener Daten über die an das Personal gezahlten Gehälter durch einen Arbeitgeber als solche keinen Eingriff in die Privatsphäre begründen, doch stellt die Weitergabe dieser Daten an einen Dritten [...] unabhängig von der späteren Verwendung der übermittelten Informationen [...] einen Eingriff im Sinne von Art. 8 EMRK dar.«

Allerdings ist nach dem Wortlaut nicht eindeutig, ob der Eingriffscharakter generell für Datenspeicherungen vom EuGH verneint werden soll oder nur für den vorliegenden Sonderfall der – grundsätzlich selbstverständlichen – Lohn- und Gehaltsbuchung bzw. -dokumentation durch Arbeitgeber.[43] Die besseren Gründe sprechen für die zweite Variante. Zunächst umschließt der Richtlinienbegriff der Datenverarbeitung, wie der EuGH nur kurz zuvor in der Tz. 64 – und in Übereinstimmung mit der Definition in Art. 2 lit. b) Richtlinie 95/46/EG – festhält, auch die Stufe der Speicherung. Bei einem grundsätzlich anderen Verständnis des Art. 8 EMRK hätte hier zumindest eine kurze Begründung nahegelegen.[44] Vor allem aber widerspräche ein solch genereller Ausschluss der Speicherung als Eingriffstatbestand dem offenkundigen Bemühen des EuGH in diesem Urteil, die Straßburger Vorgaben exakt nachzuzeichnen.[45] In der Rechtsprechung des EGMR wird nämlich die Datenspeicherung seit langem als eingriffsbegründende Maßnahme eingestuft.[46] Bei geheimen Überwachungsmaßnahmen genügt im Übrigen bereits eine gesetzliche Ermächtigung zur Verwirklichung des Eingriffstatbestands, ohne dass es tatsächlich zu Überwachungsmaßnahmen – vorliegend also eine tatsächliche Speicherung von Internetzugangsdaten oder die Weitergabe an Behörden durch die speicherverpflichteten Unternehmen – gekommen sein müsste.[47]

Rechtfertigung des Eingriffs — Nach alledem begründet bereits die schlichte Vorratsdatenspeicherung einen Eingriff in das Gemeinschaftsgrundrecht auf Privatheit und Korrespondenz. Wie bei der Prüfung der deutschen Grundrechte liegt der eigentliche Kern des Problems damit bei der Rechtfertigung der Grundrechtseingriffe. In ständiger Rechtsprechung hat der EGMR für das Recht auf Datenschutz in Konkretisierung von Art. 8 II EMRK Kriterien entwickelt, die vom EuGH im zitierten ORF-Urteil ebenfalls grundsätzlich übernommen worden sind.[48] Danach bedarf es einer gesetzlichen *Ermächtigung*, die für die Betroffenen hinreichend zugänglich ist, Bestimmtheitserfordernissen genügt sowie in einer demo-

kratischen Gesellschaft notwendig ist, also rechtsstaatliche Grundsätze der Verhältnismäßigkeit nicht verletzt. Die diesbezüglichen Maßstäbe weichen nicht signifikant von denen der deutschen Rechtfertigungsprüfung ab. Die nachfolgenden Bemerkungen beschränken sich auf die letztlich ausschlaggebende Prüfung der Angemessenheit bzw. Verhältnismäßigkeit im engeren Sinne, die von der generellen Schutzwürdigkeit von Verkehrsdaten und der mit einer verdachtslosen Vorratsdatenspeicherung verbundenen, besonderen Eingriffsintensität einerseits und dem Gewicht der zur Rechtfertigung herangezogenen Belange der Strafrechtspflege andererseits abhängt.

Verkehrsdaten werden oft als weniger schutzbedürftig als Inhaltsdaten eingestuft. Gleichwohl darf die mit ihrer Speicherung auf Vorrat verbundene Eingriffsintensität nicht unterschätzt werden. Verkehrsdaten haben schon isoliert einen besonders schutzwürdigen Aussagegehalt, da sie erhebliche Rückschlüsse auf das Kommunikations- oder Bewegungsverhalten der Telekommunikationsnutzer zulassen.[49] Verkehrsdaten sind aufgrund ihrer unproblematischen automatischen Auswertbarkeit und relativen Überschaubarkeit für Rasterfahndungsmethoden bzw. strategische Überwachungen durch Nachrichtendienste sogar besonders geeignet und können dadurch Vorteile gegenüber nur mit erheblich größerem Aufwand auswertbaren Inhaltsdaten aufweisen. Sie sind somit ein naheliegendes Instrument zur Identifikation von Ermittlungsansätzen. Insbesondere können sie dazu dienen, soziale, politische oder wirtschaftliche Beziehungsnetzwerke zu rekonstruieren und diese anhand von Häufigkeit oder Dauer der Kommunikation auf ihre Intensität hin zu analysieren. Dabei sind Fehlbeurteilungen selbstverständlich nicht ausgeschlossen, wenn z.B. intensive individuelle Kommunikationsbeziehungen aus einem, etwa familiären oder politischen, sozialen Kontext als Teil einer ganz anderen, etwa kriminellen, Kommunikationsstruktur erscheinen. Die Folgen für die Betroffenen sind offenkundig, sie werden zum Gegenstand staatlicher Ermittlungen mit allen Belastungen, die diese unvermeidlich mit sich bringen.

Zusätzlich erhöht wird die Schutzbedürftigkeit von Verkehrsdaten durch vielfältige Möglichkeiten der Verknüpfung mit anderen, bei den Ermittlungsbehörden oder bei auskunftsberechtigten Privaten vorhandenen Daten beispielsweise zu Inhalten von Internetnutzungen. So versuchen Urheberrechtsinhaber bzw. von ihnen beauftragte Verwertungsgesellschaften die Nutzer von Internettauschbörsen und die von diesen angebotenen oder heruntergeladenen Datenmengen oder gar Dateninhalte zu identifizieren. Eigenständig können sie zwar nur die auf einer Tauschbörse zu einem bestimmten Zeitpunkt aktiven dynamischen *IP*-Adressen speichern. Mittels auf Vorrat gespeicherter Verkehrsdaten lassen sich zunächst die dahinterstehenden Anschlussinhaber ermitteln. Diese selbst und weitere Nutzer

ihres Anschlusses werden dann zum Gegenstand weiterer Ermittlungen bzw. zivilrechtlicher Mahn- und Klageverfahren.

Mit guten Gründen hat daher das BVerfG sogar eine Schutzpflicht des Staates gegen ungerechtfertigte private Verkehrsdatenspeicherungen angenommen, selbst wenn die Speicherung nur wenige Tage andauert.[50] Damit hat das Gericht den *Grundsatz der Datensparsamkeit* als wirksamstes Mittel zur Wahrung der informationellen Selbstbestimmung betont. In der Informationsgesellschaft kann und darf dieser zwar nicht zu einem Gebot der Datenaskese überhöht werden.[51] Mit der verdachtslosen und universellen Vorratsspeicherung sensibler Telekommunikationsverkehrsdaten wird aber umgekehrt die Informationsvorsorge erheblich überspannt.

Besonders belastend wirkt dabei die Verdachtslosigkeit der Vorratsdatenspeicherung. Durch sie werden unter den Bedingungen der modernen Informationsgesellschaft die Träger des Grundrechts auf Telekommunikationsfreiheit zum Objekt staatlich veranlasster Datenspeicherung, ohne dass sie dafür durch ihr Verhalten über die verfassungsrechtlich geschützte Grundrechtsausübung hinaus einen relevanten Anlass geboten haben. Die Speicherung erfolgt vielmehr ›ins Blaue‹ hinein und entfaltet eine ganz außergewöhnliche Streubreite. Beide Aspekte wurden vom BVerfG in seiner bisherigen Rechtsprechung als Kriterien für eine hohe Eingriffsintensität bzw. ein besonderes Maß der Rechtfertigungsbedürftigkeit gewertet.[52] Angesichts einer Mindestspeicherdauer von sechs Monaten kann man auch keinesfalls von einer unverzüglichen, spurenlosen Löschung von Verkehrsdaten unbeteiligter Dritter sprechen.[53]

Bedeutsam für das Maß der Grundrechtsbeeinträchtigung durch die verdachtslose Vorratsdatenspeicherung ist im Übrigen nicht allein das Maß der je individuellen Grundrechtsbetroffenheit, sondern, wie das BVerfG vielfach betont hat, ebenso die von staatlichen Datenverarbeitungsmaßnahmen mit großer Streuwirkung ohne qualifizierte Anwendungshürden ausgehenden Rückwirkungen auf gesamtgesellschaftliche Verhaltensmuster und den demokratischen Diskurs.[54] Zudem sind nicht nur aktuell nachweisbare Rechtsbetroffenheiten, sondern auch nachvollziehbare Befürchtungen relevant,[55] die sich auch auf einen widerrechtlichen Missbrauch gespeicherter Daten durch Private oder staatliche Stellen beziehen können.[56]

Entscheidend ist, ob diese Grundrechtsbelastungen durch die mit der Vorratsdatenspeicherung verfolgten Zwecke aufgewogen werden. Sicherlich kommt der strafrechtlichen Bekämpfung der Organisierten Kriminalität und des Terrorismus bei der notwendigen Zweck-Mittel-Abwägung ein hohes Gewicht zu. Zudem mögen in diesem Bereich telekommunikationsbezogene Ermittlungsmaßnahmen aufgrund der internationalen Verflechtungen in diesen Kriminalitätsformen besondere Bedeutung besitzen.

Gleichwohl rechtfertigen diese Belange nicht die nun eingeführte verdachtslose und universelle Vorratsdatenspeicherung. Das Gewicht der hiermit verbundenen und im Vergleich zur bisherigen Rechtslage zusätzlichen Grundrechtsbeeinträchtigung sowie die Risiken für das demokratisch bedeutsame Kommunikationsverhalten der Bürger wurden bereits ausführlich dargelegt. Diese Beeinträchtigungen werden nicht durch den ›kriminalistischen Mehrwert‹ der Vorratsdatenspeicherung aufgewogen. Dieser dürfte sogar gerade in diesen Kriminalitätsfeldern aufgrund der besonderen kriminellen Energie der Täter und ihres guten Organisationsgrads am geringsten sein. Auch die bisher bestehenden Zugriffsmöglichkeiten auf Verkehrsdaten ermöglichen in der ganz überwiegenden Zahl der Fälle eine kaum weniger effektive Strafverfolgung. Zusätzlichen Gewinn verspricht das Instrument des *Quick-Freeze*, also der kurzfristig möglichen Anordnung der einstweiligen Datenspeicherung aufgrund bestimmter Verdachtsmomente. Da dieses Instrument deutlich weniger grundrechtsbeeinträchtigend wirkt als die verdachtslose und universelle Vorratsdatenspeicherung, muss die mit ihm mögliche partielle Substitution der Vorratsdatenspeicherung bei der Angemessenheitsprüfung Berücksichtigung finden.

Abschließend soll für die Angemessenheitsprüfung an den sicherheitspolitischen Kontext der Vorratsdatenspeicherung erinnert werden. Die Belastungswirkung der Vorratsspeicherung und der an diese anknüpfenden Datenverwendungsbefugnisse sind nicht nur isoliert zu betrachten. Die Vorratsdatenspeicherung ist nämlich bekanntermaßen nur ein Baustein im aktuellen und absehbaren sicherheitspolitischen Instrumentenmix mit automatisierten Kennzeichenerfassungen, *Online*-Durchsuchungen, Rasterfahndungen, Videoüberwachungen öffentlicher Räume, Mautdatennutzung oder Fluggastdatenspeicherung. Auf eine Kontrolle sich wechselseitig verstärkender Rückwirkungen auf die demokratische Offenheit im gesellschaftlichen Diskurs und das rechtsstaatliche Vertrauen der Bürger durch derartige komplexe Instrumentenstrukturen ist der Grundrechtsschutz im europäischen Mehrebenensystem vor allem prozessual nur sehr begrenzt eingestellt. Umso wichtiger ist es im Interesse der Freiheitlichkeit unseres Rechtsstaats, diese im Auge zu behalten.

IV. Fazit — Auf die eingangs gestellte Kernfrage ist nach dem Vorstehenden eine gemischte Antwort zu geben: Bei einer sachgerechten Nutzung des Vorabentscheidungsverfahrens durch das BVerfG sind die verflochtenen Grundrechtsbeeinträchtigungen auf europäischer und mitgliedstaatlicher Ebene durch die Vorratsdatenspeicherung angemessen zu verarbeiten. Dabei bedarf es allerdings noch einer Konsolidierung der datenschutzrechtlichen Rechtsprechung des EuGH, zu der das BVerfG im Rahmen des

judiziellen Dialogs einen wertvollen Beitrag liefern könnte. Schwerer fällt die Verarbeitung des sicherheitspolitischen Instrumentenmix, was aber kein Spezifikum des Mehrebenensystems ist, sondern bereits auf der nationalen Ebene allein zu beobachten ist.

---

1 Siehe hierzu die im Rahmen einer Umfrage des Meinungsforschungsinstituts Forsa unter 1.002 Bundesbürgern am 27./28. Mai 2008 erhobenen Umfrageergebnisse, vgl. http://www. vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf.

2 Richtlinie 2006/24/EG vom 15.3.2006 über die Vorratsspeicherung von Daten. In: Amtsblatt der Europäischen Union (ABl.) 2006 L 105/54 ff.

3 Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007. In: Bundesgesetzblatt (BGBl.) 2007 I, S. 3198 ff.

4 Hierzu näher: Jens-Peter Schneider: Verfassungsgerichtsbarkeit und Europäischer Gerichtshof. In: Wilfried Masing / Johannes Erbguth (Hg.): Verfassungs- und Verwaltungsgerichtsbarkeit im Mehrebenensystem. Stuttgart u.a. 2008, S. 11 ff.

5 Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 118, 79, S. 95 ff. (= Deutsches Verwaltungsblatt (DVBl.) 2007, S. 821, Textziffer 67, 69, 72. Siehe ferner den Beschluss zur Vorratsdatenspeicherung des BVerfG vom 11. März 2008. In: BVerfGE 121, S. 1, hier S. 15.

6 BVerfGE, DVBl. 2007, 821 (Anm. 5), S. 66 ff.

7 BVerfGE 113, 273 (300 ff.) (= Neue Juristische Wochenschrift (NJW) 2005, Tz. 2289 (2291, 2293); s. ferner BVerfGE (Anm. 5), Tz. 70, 79 ff.

8 S. auch Dietrich Westphal: Die Richtlinie zur Vorratsdatenspeicherung von Verkehrsdaten. Brüsseler Stellungnahme zum Verhältnis von Freiheit und Sicherheit in der Post-9/11-Informationsgesellschaft. In: Europarecht (EuR) 2006, S. 706 (S. 709 f.); zu eng: Benjamin Rusteberg. In: Verwaltungsblätter für Baden-Württemberg (VBlBW) 2007, S. 171, hier S. 176 f.

9 S. auch Westphal: Die neue EG-Richtlinie zur Vorratsdatenspeicherung. In: Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2006, S. 555, hier S. 558.

10 Ein entsprechender Hinweis am Ende von Art. 1 I fand sich auch noch im Kommissionsvorschlag: KOM 2005 (438) endgültig, vom 21. Sept. 2005. Seine Streichung hat den Handlungsspielraum der Mitgliedstaaten weder erweitert noch verengt.

11 Siehe auch Peter Gola u.a.: Datenschutz und presserechtliche Bewertung der »Vorratsdatenspeicherung«. In: NJW 2007, S. 2599, hier S. 2601.

12 Vgl. die Gesetzesbegründung der Bundesregierung, in: Deutscher Bundestag, Drucksache 16/5846 vom 27. Juni 2007, S. 52 f.

13 Vgl. dazu auch Spiros Simitis: Übermittlung der Daten von Flugpassagieren in die USA: Dispens vom Datenschutz? In: NJW 2006, S. 2011 f.

14 EuGH, Rechtssache C-301/06. Vgl. DVBl. 2009, S. 371 ff; s. auch die kritischen Bemerkungen in Fussnote 17.

15 Zur Zulässigkeit und zum Prüfungsmaßstab einer Gültigkeitsvorlage s. Uwe Kischel, in: Kay Hailbronner / Heinrich Wilms (Hg.): Recht der Europäischen Union, Art. 234 EGV, Rn. 7, 10.

16 Oliver Dörr / Christofer Lenz: Europäischer Verwaltungsrechtsschutz. Baden-Baden 2006, Rn. 262.

17 EuGH, Rechtssache C-301/06 (Anm. 14); die kompetenzrechtliche Argumentation des EuGH ist sicher gut vertretbar, wenngleich nicht absolut zwingend, da beispielsweise die Frage offenbleibt, ob die Richtlinie 2006/24/EG tatsächlich zur Beseitigung spürbarer Verzerrungen des Wettbewerbs (zu diesem Maßstab s. ferner EuGH, Rs. C-376/98, EuZW 2000, S. 694, Tz. 108; EuGH, Rs. C-380/03, EuZW 2007, S. 46, Tz. 38) beiträgt. Zumindest sind Mindestspeicherpflichten ohne zeitliche Höchstgrenze nur sehr bedingt geeignet, die von Generalanwalt Bot und dem EuGH herangezogenen Wettbewerbsverzerrungen für Telekommunikationsdienstleister zu mindern, da eine Reihe von Ländern bereits heute deutlich längere mehrjährige Speicherfristen mit entsprechenden Kostenfolgen vorsehen, während eine andere Gruppe von Mitgliedstaaten an der Mindestfrist von 6 Monaten festhält.

18 Vgl. zu diesen Anforderungen: Entscheidungen des Europäischen Gerichtshofes (EuGHE) 2000, I-11.369 Tz. 57; Bernhard W. Wegener, in: Christian Calliess / Matthias Ruffert (Hg.): Das Verfassungsrecht der Europäischen Union. 3. Aufl. München 2007, Art. 234 EGV, Tz. 15.
19 Siehe ABl. EU 2006, C 237/5.
20 EuGH, Rs. C-301/06, DVBl. 2009, 371 (Rn. 57).
21 Hierzu: Kischel (Anm. 15), Art. 234 EGV, Rn. 22.
22 Vgl. hierzu allg. BVerfGE 118, 79 sowie DVBl. (Anm. 5), Tz. 72.
23 BVerfGE 118, S. 79 (95 ff.) = DVBl. (Anm. 5), Rn. 67, 69, 72. Siehe ferner den Beschluss zur Vorratsdatenspeicherung des BVerfG vom 11. März 2008 (Anm. 5); zusammenfassend: Jens-Peter Schneider (Anm. 4), S. 11 ff.
24 BVerfGE 37, S. 271, hier S. 282; BVerfGE 52, S. 187, hier S. 200 ff.; hierzu ferner: Franz C. Mayer: Das Bundesverfassungsgericht und die Verpflichtung zur Vorlage an den Europäischen Gerichtshof. In: EuR 2002, S. 239, hier S. 251 ff.
25 Sie wäre nur als Gewichtungsfaktor bei der Angemessenheitsprüfung der deutschen Gestaltungsentscheidungen einzubeziehen: vgl. Beschluss des BVerfG vom 11. März 2008 (Anm. 5), Rn. 155.
26 Siehe die kritischen Stellungnahmen in der aktuellen Literatur: Andreas Gietl: Das Schicksal der Vorratsdatenspeicherung. In: Datenschutz und Datensicherheit (DuD) 2008, S. 317, hier S. 323: »für das Grundrecht wohl die denkbar schlechteste Alternative«; Jenny Valerian: Eile mit Weile – Vorratsdatenspeicherung auf dem Prüfstand. In: Computer und Recht (CR) 2008, S. 282 ff., hier S. 286: »wäre zwar konsequent, aber inhaltlich unbefriedigend«; vgl. auch Wolfgang Bär: Anmerkungen zum Beschluss des BVerfG vom 11.03.2008. In: Mulitimedia und Recht (MMR) 2008, S. 307 ff., hier S. 308: »Eine zu frühe Entscheidung zur Hauptsache könnte daher in der Sache nur unvollständig bleiben«.
27 Abstrakt zu dieser Kombination einer fachgerichtlichen Vorlage einer Richtlinie nach Art. 234 EGV und sich anschließender Vorlage des deutschen Umsetzungsgesetzes nach Art. 100 GG: BVerfGE (Anm 5.), Rn. 72.
28 Zu den Anforderungen des EuGH statt vieler: Ulrich Karpenstein. In: Eberhard Grabitz / Meinhard Hilf (Hg.): Das Recht der Europäischen Union. Loseblatt, Stand der 37. Ergänzungslieferung vom Nov. 2008. München 2009, Bd. 3., Art. 234, Tz. 51 ff. (Stand der Kommentierung: EL 36 vom Juli 2008); Jürgen Schwarze, in: Ders. (Hg.): EU-Kommentar, 2. Aufl., Baden-Baden 2009, Art. 234, Tz. 41 ff.
29 Valerian (Anm. 26), S. 287.
30 Ebd.
31 Vgl. zu dieser Rekonstruktion und Absicherung des immer wieder betonten Kooperationsparadigmas: F. Mayer: Europäische Verfassungsgerichtsbarkeit – Gerichtliche Letztentscheidung im europäischen Mehrebenensystem. In: Armin v. Bogdandy (Hg.): Europäisches Verfassungsrecht, Berlin u.a. 2003, S. 228 (passim, insb. aber S. 273 f., 277).
32 EuGHE 2006, I-4721, Tz. 61, 70 (= NJW 2006, 2029 ff.).
33 Hinzuweisen ist an dieser Stelle nur auf die aktuelle rechtspolitische Diskussion in den EU-Gremien über ein System zur langjährigen Speicherung von Fluggastdaten, vgl. den Artikel: EU skeptisch über Datenspeicherung. In: Frankfurter Allg. Zeitung vom 26. Jan. 2008, S. 8.
34 Vgl. den Überblick bei F. Mayer (Anm. 31), S. 235 ff.
35 Entscheidung Nr. 103/2008 – Legge della Regione Sardegna 11 maggio 2006 / 29 maggio 2007. Zit. nach F. Mayer: Verfassungsgerichtsbarkeit (Anm. 31), in der Neuauflage (i.E.), Fn. 34 des Manuskripts (Stand Februar 2009); zu dieser Entscheidung s. ferner: Filippo Fontanelli / Giuseppe Martinico: Cooperative Antagonists. The Italian Constitutional Court and the Preliminary Reference: Are We Dealing with a Turning Point?; Eric Stein: Working Paper No 5/2008, insbesondere S. 13; M. Dani: Tracking Judicial Dialogue. The Scope for Preliminary Rulings from the Italian Constitutional Court, Jean Monnet Working Paper 10 (2008) (http://www.jeanmonnetprogram.org).
36 EuGHE 2003, I-4989 (Tz. 68 ff.) – ORF; jüngst EuGHE vom 29. Januar 2008, Rs. C-275/06, Tz. 63 ff., sowie die vorherigen Schlussanträge von Generalanwältin Kokott v. 18. Juli 2007 in der Rs. C-275/06, Tz. 50 ff.
37 Generalanwältin Kokott (Anm. 36), Tz. 82 mit Fn. 43; s. auch Westphal (Anm. 9), S. 558 ff.

38 EuGHE 2003, I-4989, Tz. 68 ff. – ORF; s. ferner: EuGHE 1969, 419 – Stauder; 1985, S. 3359 – Adams; ausführlich: Birte Siemen: Datenschutz als europäisches Grundrecht. Berlin 2006; s. a. Marion Albers: Informationelle Selbstbestimmung. Baden-Baden 2005, S. 285 ff.
39 Ähnlich: Matthias Ruffert: Die künftige Rolle des EuGH im europäischen Grundrechtsschutzsystem. In: Europäische Grundrechte-Zeitschrift (EuGRZ) 2004, S. 466, hier S. 470; Birte Siemen: Grundrechtsschutz durch Richtlinien. Die Fälle Österreichischer Rundfunk u.a. und Lindqvist. In: EuR 2004, S. 306, hier S. 314 f.
40 Entscheidung des Europäischen Gerichtshofs für Menschenrechte (EGMR) vom 6. Sept. 1978 (Application no. 5029/71) Tz. 41 – Klass = NJW 1979, 1755; v. 25. Juni 1992 (17/1991/269/340) Tz. 39 – Lüdi = NJW 1992, 3088; v. 16. Feb. 2000 (Application no. 27798/95) Tz. 44 – Amann; v. 29. Juni 2006 (Application no. 54934/00) Tz. 76 ff. – Weber and Saravia; v. 28. Juni 2007 (Application no. 62540/00) Tz. 54, 58 ff. – Association for European Integration and Human Rights.
41 EGMR v. 4. Mai 2000 (Application no. 28341/95) Tz. 42 f. – Rotaru; v. 25. Sept. 2001 (Application no. 44787/98) Tz. 56 – P.G and J.H; 17.7.2003 (Application no. 63737/00) Tz. 36 – Perry.
42 Ruffert (Anm. 39); Gutachten des Wissenschaftlichen Dienstes des Landtages von Schleswig-Holstein v. 27. Feb. 2006 zu den Auswirkungen des Richtlinienvorschlags KOM (2005) 438 endg. (»Vorratsdatenspeicherung«) auf die Rechte der Abgeordneten, S. 26.
43 Die französische und englische Fassung sind ebenfalls nicht eindeutig, deuten aber tendenziell noch stärker die nachfolgend begründete Auslegung an.
44 Insbesondere weil Generalanwalt Tizzano aufgrund seiner Auffassung bezüglich der Unanwendbarkeit des EG-Datenschutzrechts zu diesen Auslegungsfragen überhaupt keine Aussagen trifft: GA Tizzano, EuGHE 2003, I- 4989 Tz. 40 ff.
45 S. hierzu: Ruffert (Anm. 39), S. 471.
46 EGMR v. 26. März 1987 (Application no. 9248/81), Tz. 48 – Leander; v. 4. Mai 2000 (Application no. 28341/95) Tz. 43, 46 – Rotaru; s. auch Rusteberg (Anm. 8).
47 EGMR v. 29. Juni 2006 (Application no. 54934/00) Tz. 78 – Weber and Saravia; v. 28. Juni 2007 (Application no. 62540/00) Tz. 69 – Association for European Integration and Human Rights.
48 EGMR v. 28. Juni 2007 (Application no. 62540/00) Tz. 71 ff. – Association for European Integration and Human Rights; v. 26. März 1987 (Application no. 9248/81), Tz. 50 ff. – Leander; EuGHE 2003, I-4989 Tz. 76 ff. – ORF.
49 BVerfGE 115, S. 166 (190); BVerfGE 100 (313) (= NJW 2000, 55, hier S. 64 ff.; s. auch: Bundesregierung (Anm. 12), S. 31; die gegenteilige Bewertung von isolierten Kontostammdaten (BVerfG, in: NJW 2007, S. 2464, hier S. 2470, Tz. 136, kann also keinesfalls auf die Verkehrsdaten übertragen werden.
50 BVerfG-K, in: NJW 2007, S. 3055 ff.
51 Dazu Hans-Peter Bull: Zweifelsfragen um die informationelle Selbstbestimmung – Datenschutz als Datenaskese? In: NJW 2006, S. 1617 ff.
52 Zu Telekommunikationsüberwachungen bzw. Datenerhebungen ins Blaue hinein: BVerfG, in: NJW 2006, S. 1939, hier S. 1946; BVerfGE 107, S. 299, hier S. 321 f.; BVerfGE 109, S. 279, hier S. 353; zur Problematik der Streubreite u.a.: BVerfG, in: NJW 2005, S. 2603, hier S. 2609 – Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung (NdsSOG).
53 Dies war das zentrale Argument für eine geringe Eingriffsintensität in BVerfG, in: Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2007, S. 351, hier S. 356, Tz. 76.
54 BVerfGE 100, S. 313, hier S. 381.
55 BVerfG, in: NJW 2003, S. 1787, hier S. 1793; E 100, S. 313, hier S. 376.
56 Vgl. BVerfGE 65, S. 1, hier S. 46; S. 85, S. 386, hier S. 397, 400; BVerfG-K, in: NJW 2007, S. 3055, hier S. 3056, Tz. 17.