Lothar Binding
Mitglied des Deutschen Bundestages

Berliner Büro
Platz der Republik 1
11011 Berlin
Tel: (030) 227 -73144
Fax: (030) 227 -76435
eMail Berlin:
lothar.binding@bundestag.de

Bürgerbüro Heidelberg/Weinheim
Bergheimer Straße 88
69115 Heidelberg
Tel: (06221) 18 29 28
Fax: (06221) 61 60 40

eMail Heidelberg und Weinheim:
lothar.binding@wk.bundestag.de
Homepage: www.lothar-binding.de

Lothar Binding, MdB * Platz der Republik 1 * 11011 Berlin

Herrn
Alex Müller
(per Mail)

Berlin, den 22. Juni 2007

Vorratsdatenspeicherung

Sehr geehrter Herr Müller,

vielen Dank für Ihr Schreiben, das ich gerne auch im Namen von Gert Weisskirchen beantworte. Mein Fraktionskollege hat Ihr Schreiben an mich weitergeleitet, weil Ihr Wohnort in meinem Wahlkreis liegt. Ihre grundsätzliche Sorge vor der Speicherung von Daten teile ich. Dazu finden Sie auch Hinweise auf meiner website zu den Themen RFID und biometrische Daten auf Ausweisdokumenten.

Präzise Kenntnisse sind für meine eigene Einschätzung der Sachlage dringend notwendig. Meine Ausführungen stützen sich daher auf Informationen der Arbeitsgruppe Rechtspolitik der SPD- Fraktion im Deutschen Bundestag sowie auf eigene Recherchen. Auf diesen Grundlagen mache ich mir ein Bild von den Argumenten der Befürworter und Gegner der Vorratsdatenspeicherung.

Für eine wirksame Verfolgung und Bekämpfung von Straftaten sei der verdeckte Zugriff auf Telekommunikationsverkehrsdaten unbedingt erforderlich, argumentieren die Befürworter der Vorratsdatenspeicherung. Deshalb müsse man diese Daten über einen gewissen Zeitraum speichern. Dies belegen Berichte aus den Bundesländern und anderer EU-Mitgliedstaaten. Terrorismus und Kriminalität nehmen keine Rücksicht auf Landesgrenzen; deshalb sei eine europaweit einheitliche und abgestimmte Strafverfolgung von besonderer Bedeutung. Die Ermittlungsbehörden erhoffen sich vom Zugriff auf die sog. Verkehrs- und Standortdaten Erleichterungen bei der Verbrechensbekämpfung. Dabei handelt es sich um Daten, die entstehen, wenn man telefoniert, ein Fax verschickt, im Internet surft, sich mit anderen in einem Chatroom unterhält oder eine E- Mail verschickt. Sie enthalten Informationen über IP-Adressen, Datum, Uhrzeit und Dauer der Verbindung und die dabei übertragene Datenmenge.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betonte hingegen in einer Pressemitteilung vom März 2007, dass die Vorratsdatenspeicherung in Widerspruch

zum deutschen Verfassungsrecht und zur Rechtsprechung des Bundesverfassungsgerichtes stehe. Zudem beeinträchtige sie „die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich“.

Die Frage nach der Erlaubnis zur Speicherung personenbezogener Daten und deren Verwendung berührt wichtige Aspekte unseres Staatsverständnisses. Eine der fundamentalen Aufgaben unseres demokratischen Gemeinwesens ist der grundgesetzlich verankerte Schutz der Menschenrechte. Sie bilden die Richtschnur für das gesamte staatliche Handeln und setzen ihm klare Grenzen. Gleichzeitig setzt sich der Rechtsstaat aber auch die Aufgabe, seine Bürger zu schützen, ihr Hab und Gut zu verteidigen und sie vor Angriffen auf ihr leibliches Wohl zu bewahren.

Beide Aufgaben haben ihre normative Berechtigung. Zum Dilemma werden sie in einer Entscheidungssituation, in der die Verfolgung eines Ziels nur auf Kosten des anderen gelingen kann. Ein Staat, der nicht in der Lage ist, seine Bürger vor terroristischen Angriffen und Organisierter Kriminalität zu schützen, hat schwerwiegende Defizite aufzuweisen. Wo der Schutz der Bürger allerdings nur durch die Außerkraftsetzung der Menschen- und Bürgerrechte gelingt, steht der Staat vor ernsthaften Legitimationsproblemen.

Die Balance zwischen diesen beiden Zielvorgaben zu finden, ist schwierig und erfordert eine genaue Prüfung der politischen und rechtlichen Aspekte dieses Sachverhaltes. Nicht immer komme ich bei politischen Entscheidungen dabei zu einer Position, die für beide Seiten eine *win- win*- Situation darstellt und meine volle Zustimmung hat. Gelegentlich muss ich zwischen Zielen abwägen, die in einem Spannungsverhältnis zueinander stehen – und bisweilen lassen sich für juristisch komplexe und politisch sensible Probleme keine einfachen Lösungen finden, die alle Seiten zufriedenstellen.

Der rasante Übergang ins Informationszeitalter bietet Ermittlungsbehörden neue Möglichkeiten, Gesetzesverstöße aufzuspüren, zu verfolgen und zu ahnden. Allerdings muss man dabei auf Ausgewogenheit und Verhältnismäßigkeit der Mittel achten. Denn nicht alles, was technisch machbar ist, ist meines Erachtens auch politisch sinnvoll und rechtlich zulässig. Wo Daten, die den Kernbereich der privaten Lebensgestaltung betreffen, gespeichert werden sollen, stößt das Strafverfolgungsinteresse des Staates an seine Grenze. Diese Daten müssen durch ein absolutes Verwertungsverbot geschützt werden.

Auf europäischer Ebene beschäftigt die Auseinandersetzung mit der Rechtmäßigkeit der Richtlinie und der Zuständigkeit der EU mittlerweile den Europäischen Gerichtshof. Er verhandelt eine Nichtigkeitsklage, die allerdings keine aufschiebende Wirkung für die Umsetzung der Richtlinie in innerstaatliches Recht hat. Die Gruppe für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, die sog. Artikel 29-Datenschutzgruppe der Europäischen Union, hat eine treffende Formulierung für dieses Dilemma gefunden:

> „Die Aufbewahrung von Verkehrsdaten ist ein Eingriff in das unverletzliche Grundrecht auf Achtung des Brief-, Post- und Fernmeldegeheimnisses. Eingriffe in dieses Grundrecht müssen einem zwingenden Bedarf entspringen, sie sollten nur in Ausnahmefällen gestattet werden und angemessenen Schutzmaßnahmen unterworfen sein. Der Terrorismus stellt unsere Gesellschaft vor eine reale und drängende Herausforderung. Die Regierungen müssen auf diese Herausforderung in einer Form reagieren, die dem Bedürfnis der Bürger, in Frieden und Sicherheit zu leben, wirkungsvoll nachkommt, ohne die Menschenrechte des Einzelnen, darunter das Recht

> auf Privatsphäre und Datenschutz, auszuhöhlen, denn diese Rechte gehören zu den Eckpfeilern unserer demokratischen Gesellschaft.“[1]

Die Anfänge der aktuell diskutierten Richtlinie reichen in eine Zeit zurück, die durch terroristische Anschläge, wie die in Madrid am 11. März 2004, geprägt waren. Der Europäische Rat hat darauf reagiert und am 25. März 2004 eine Erklärung zum Kampf gegen den Terrorismus verabschiedet. Der EU- Ministerrat wurde beauftragt, Maßnahmen für die Erarbeitung von Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten durch Diensteanbieter zu prüfen. Potentielle Gefahren rechtzeitig erkennen und verdächtige Personen aus dem Verkehr ziehen – so lautete das Vorhaben für jene, die Verantwortung für unsere Sicherheit übernehmen.

Zur Ratstagung am 29. und 30. April 2004 legten Frankreich, Großbritannien, Irland und Schweden einen gemeinsamen Vorschlag für einen Rahmenbeschluss zur Vorratsdaten-speicherung vorgelegt. Am 7. Juni 2005 sprach sich das Europäische Parlament aus Datenschutzgründen gegen diese Initiative aus und forderte ihren Rückzug. Unter dem Eindruck der U- Bahn-Anschläge vom 7. Juli 2005 in London erklärten die EU- Justiz- und Innenminister auf ihrem Sondergipfel am 13. Juli 2005 ihre Absicht, trotz der Ablehnung durch das EP über einen Rahmenbeschluss-Vorschlag noch im Jahre 2005 eine Einigung erzielen zu wollen.

Am 21. September 2005 legte die EU-Kommission einen eigenen Entwurf für eine Richtlinie vor. Die Justizminister einigten sich im EU-Ministerrat am 2. Dezember 2005 auf einen Kompromiss und überarbeiteten den Richtlinienvorschlag der Kommission. Anders als der ursprüngliche Vorschlag enthält dieser Ratskompromiss Spielraum für die Mitgliedstaaten hinsichtlich der Speicherdauer der Daten von Telefon- sowie Internetverbindungen. Am 14. Dezember 2005 stimmte das Europäische Parlament mit deutlicher Mehrheit für diesen Richtlinienkompromissvorschlag. Bei der Sitzung des Ministerrates am 1. und 2. Februar 2006 stand diese Richtlinie in ihrer Kompromissfassung auf der Tagesordnung.

Bundesregierung und Bundestag arbeiteten bei der Meinungsbildung und Entscheidungsfindung im Vorfeld dieser Abstimmung im Ministerrat in einem mehrstufigen Verfahren zusammen. Schon anlässlich der Verabschiedung der Novelle des Telekommunikationsgesetzes hatten sich Bundestag und Bundesrat ausführlich mit der Thematik der Vorratsdatenspeicherung von Telekommunikationsdiensten befasst. Der Bundestag hatte in der aktuellen Debatte um eine europäische Richtlinie einen sog. Parlamentsvorbehalt verhängt, demzufolge die Bundesregierung auf europäischer Ebene keine Entscheidung gegen den Willen des Bundestages treffen durfte. Der federführende Rechtsausschuss hatte mit den Stimmen der Fraktionen von SPD, CDU/CSU und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion der FDP empfohlen, den europäischen Rahmenbeschluss zur Kenntnis zu nehmen und eine eigene Entschließung anzunehmen. Damit wurde die Bundesregierung aufgefordert, bei Beratungen und Abstimmungen auf europäischer Ebene die vom Bundestag eingenommene Position zu beachten, die dieser bei der Beratung des Telekommunikationsgesetzes formuliert hatte.

Bundesjustizministerin Zypries hat diesen Parlamentsvorbehalt berücksichtigt: Sie hat bei der Sitzung der EU-Justizminister im Dezember 2005 der dort erörterten Kompromissfassung zur

[1] Artikel 29- Datenschutzgruppe, 1868/05/DE. In ähnlicher Weise argumentiert auch der Europäische Datenschutzbeauftragte.

neuen EU-Richtlinie und zur Änderung der bestehenden Richtlinie 2002/58/EG nur unter dem Vorbehalt einer erneuten Konsultation der Gremien des Deutschen Bundestages zugestimmt.[2]

Die Regierungsfraktionen haben schließlich in ihrem Antrag „Speicherung mit Augenmaß – Effektive Strafverfolgung und Grundrechtswahrung“ (Bundestagsdrucksache 16/545) ihren Vorbehalt aufgegeben und es der Regierung ermöglicht, am 1. und 2. Februar 2006 im Ministerrat bei der Ratssitzung in Brüssel dem Richtlinienvorschlag in der Kompromissfassung zuzustimmen. Denn dieser Vorschlag enthält alle wichtigen Forderungen Deutschlands, die im Vorfeld der Abstimmung formuliert worden waren.

Die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates ist am 3. Mai 2006 in Kraft getreten. Sie muss für Verkehrsdaten aus den Bereichen der Festnetz- und Mobilfunktelefonie bis zum 15. September 2007 in nationales Recht umgesetzt sein, für Verkehrsdaten aus dem Internetbereich ist ein Aufschub bis 15. März 2009 zulässig. Um die europäische Richtlinie in geltendes nationales Recht zu überführen, bedarf es eines sog. Umsetzungsgesetzes. Geplant ist, die Umsetzung der Richtlinie mit Urteilen des Bundesverfassungsgerichtes zu Datenschutz und Klarstellungen in der Strafprozessordnung zu verbinden und ein „harmonisches Gesamtsystem strafprozessualen heimlichen Ermittlungsmethoden“ zu schaffen. Die Bundesregierung hat dazu einen Gesetzentwurf zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vorgelegt. Das bietet die Möglichkeit, die bei den Verhandlungen auf europäischer Ebene vorgebrachten Schwerpunkte im nationalen Umsetzungsgesetz zu bekräftigen.

Der Entwurf wird am 6. Juli in erster Lesung im Bundestag eingebracht und anschließend an die beteiligten Ausschüsse zur weiteren Beratung überwiesen. Es handelt sich um den federführenden Rechtsausschuss sowie die mitberatenden Ausschüsse für Inneres und Ernährung, Landwirtschaft und Verbraucherschutz. Wir haben uns gemeinsam mit unserem Koalitionspartner dafür eingesetzt, dass bei der Umsetzung der Richtlinie in nationales Recht keine Regelungen zu Speicherungsdauer und erfassten Datenarten getroffen werden, die über die Mindestanforderungen der Richtlinie hinausgehen. Diese Selbstbindung hatten wir auch im Koalitionsvertrag festgeschrieben.

Die wesentlichen Eckpunkte des EU- Kompromisses sind:

- Es ist eine Mindestspeicherfrist von 6 Monaten vorgesehen, eine Verlängerung der Frist auf bis zu 24 Monate liegt im Ermessen der einzelnen Mitgliedstaaten. Der Bundestag hat bekräftigt, dass nicht über die Mindestspeicherdauer von sechs Monaten hinausgegangen werden soll. Der von der Richtlinie vorgegebene Spielraum von bis zu 24 Monaten wird also nicht ausgeschöpft werden. Auch heute schon können Unternehmen nach dem Telekommunikationsgesetz Daten bis zu sechs Monate lange aufbewahren, um sie zur Rechnungslegung verwenden zu können. Was sich allerdings ändert, ist folgendes: aus der Erlaubnis für Unternehmen zur Speicherung von Daten wird durch die europäische Richtlinie eine Verpflichtung. In der Praxis bedeutet dies, dass die Unternehmen, die schon heute in der Regel drei Monate speichern, diesen Zeitraum um lediglich drei Monate verlängern müssen.

[2] Die Richtlinie 2002/58/EG regelt die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

- Speicherzweck und Datenabfrage sind auf Zwecke der Strafverfolgung, d.h. die Ermittlung, Aufdeckung und Verfolgung von Straftaten von erheblicher Bedeutung sowie von mittels Telekommunikation begangener Straftaten beschränkt. Für diese Daten muss ein tatsächlicher Bedarf vorliegen, und die Speicherung darf keinen unverhältnismäßigen Aufwand verursachen. Für letztgenannte Fallgruppe ist dies jedoch nur dann zulässig, wenn die Erforschung des Sachverhalts auf andere Weise ausgeschlossen ist; zudem muss die Datenerhebung in angemessenem Verhältnis zur Bedeutung der Sache stehen. Das deutsche Recht sieht schon heute vor, dass Behörden bei Vorliegen der genannten gesetzlichen Voraussetzungen, wie bei der Verbreitung von kinderpornographischer oder fremdenfeindlicher Inhalte im Internet, Auskünfte von Telekommunikationsunternehmen einfordern können. Dazu benötigen sie einen richterlichen Beschluss und müssen bestimmte Verfahrensvorschriften einhalten. Meiner Ansicht nach muss sichergestellt werden, dass mit der Vorratsdatenspeicherung nur solche schwerwiegenden Taten verfolgt werden, für deren Aufklärung die Telekommunikationsüberwachung besonders unerlässlich ist. Sie darf nicht zu einem „normalen“ Instrument der Strafverfolgung werden.

- Standort- und Verbindungsdaten, wie Telefonnummern von Handys und Festnetzgeräten, werden nur für den Beginn des Mobilfunkverkehrs, nicht auch für das Ende gespeichert, um die Speicherkosten zu senken. Erfolglose Anrufversuche werden nicht aufgezeichnet. Es werden lediglich Internet-Einwahldaten, d.h. die IP- Adresse und der Zeitpunkt, sowie Verkehrsdaten zu Emails und Internettelefonie aufgezeichnet. Inhalte der vom Nutzer aufgerufenen Seiten und der Kommunikation werden ausdrücklich nicht protokolliert. Die Neuregelung sieht vor, diese Daten vielen Behörden zum Online-Abruf zur Verfügung zu stellen. Dazu gehören Polizei, Staatsanwaltschaft, Nachrichtendienste, Zoll und der Bundesanstalt für Finanzdienstleistungsaufsicht, kurz BaFin. Allerdings hege ich an dieser Stelle auch deutliche datenschutzrechtliche Bedenken, wenn Nutzer öffentlich zugänglicher E-Mail-Dienste zur Angabe ihres Namens und ihrer Adresse verpflichtet werden.

Effektive Strafverfolgung und Grundrechtsschutz zugleich zu gewährleisten, ist eine Aufgabe, die große Wachsamkeit und Besonnenheit erfordert. Ich vertraue fest darauf, dass meine Kolleginnen und Kollegen, die im federführenden Rechtsausschuss diese Angelegenheit beraten, sich dieser Verantwortung bewusst sind und eine Regelung finden werden, die einen sinnvollen und praktikablen Ausgleich zwischen diesen beiden Zielen schafft.

In der Hoffnung, dass ich Ihre Bedenken konstruktiv reflektieren und Ihnen einen Einblick in meine Überlegungen geben konnte, verbleibe ich

mit freundlichen Grüßen

Lothar Binding

P.S. Da merkwürdigerweise im Zusammenhang mit der Vorratsdatenspeicherung viel Massenpost unterwegs ist, möchte ich Ihnen vorschlagen, sich künftig in diesem Zusammenhang direkt an die Mitglieder des Rechtsausschusses zu wenden. Ein Mitgliederverzeichnis finden Sie auf der Homepage des Deutschen Bundestages.