Schleswig-Holsteinischer Landtag
Umdruck 16/1267

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

ULD • Postfach 71 16 • 24171 Kiel

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Dr. Johann Bizer
Durchwahl: 988-1286

Aktenzeichen:
LD7-61.03/02.114

Kiel, den 4.10.2006

Schleswig-Holsteinischer Landtag
Europaausschuss
Vorsitzende Frau Astrid Höfs, MdL

Innen- und Rechtsausschuss
Vorsitzender Herr Werner Kalinka, MdL

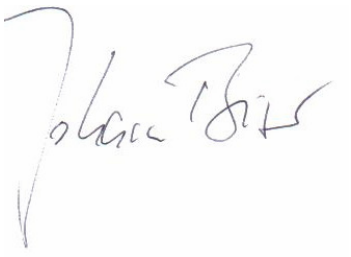
Postfach 7121
24171 Kiel

Vorratsdatenspeicherung von Telefon- und Internetverbindungen
Stellungnahme zur Umsetzung der EG-Richtlinie 2006/24/EG vom 15. März 2006
über die Vorratsdatenspeicherung von Daten

Sehr geehrte Frau Höfs, sehr geehrter Herr Kalinka,

anliegend übersende ich Ihnen die am 1. März 2006 vom Innen- und Rechtsausschuss des Schleswig-Holsteinischen Landtages erbetene Stellungnahme zur Umsetzung der oben genannten EG-Richtlinie zur Vorratsdatenspeicherung.

Mit freundlichen Grüßen



Dr. Johann Bizer
Stellvertretender Landesbeauftragter für den Datenschutz Schleswig-Holstein

Vorratsdatenspeicherung

1. Nach der EG-Richtlinie 2006/24/EG vom 15. März 2006 über die Vorratsspeicherung von Daten tragen die Mitgliedstaaten dafür Sorge, dass die Anbieter öffentlich zugänglicher elektronischer Kommunikations*dienste* und Betreiber öffentlich zugänglicher Kommunikations*netze* die „im Zuge der Bereitstellung" ihrer Dienste erfassten Verkehrsdaten über den betrieblichen Bedarf hinaus auf Vorrat speichern (Art. 3 Abs. 1). Die Verpflichtung zur Vorratsdatenspeicherung gilt also nicht für Kommunikationsdienste und –netze, die für geschlossene, d.h. für fest definierte Benutzergruppen angeboten werden (Corporate Networks etc.).

2. Erfasst sind von der EG-Richtlinie 2006/24/EG *Verkehrs- und Standortdaten* elektronischer Kommunikationsdienste. Hierzu gehören Telefondienste, SMS, E-Mail, Internet-Telefonie sowie der Zugang zum Internet (Art. 5). Nicht erfasst sind von der Speicherpflicht die Inhalte elektronischer Nachrichten sowie die Informationen, die aus dem Internet abgerufen worden sind (Art. 1 Abs. 2). Die Vorratsdatenspeicherung soll die Feststellung „des Teilnehmers oder registrierten Benutzers" ermöglichen (Art. 1 Abs. 2). Sichergestellt werden soll, dass Daten „zum Zweck der Ermittlung, Feststellung und Verfolgung von schweren Straftaten" nach dem Recht der Mitgliedstaaten zur Verfügung stehen (Art. 1 Abs. 1).

3. Gespeichert werden sollen nach der EG-Richtlinie 2006/24/EG Verkehrsdaten nach der *Quelle der Nachricht*, insbesondere nach Name und Anschrift des Teilnehmers, die zur *Identifizierung des Adressaten* erforderlichen Informationen (Rufnummer, Benutzerkennung), *Datum, Uhrzeit und Dauer* der Nachrichtenübermittlung, *Art der Nachrichtenübermittlung* (Telefon, Internet etc.), *Endeinrichtung der Benutzer* (Rufnummer, IMSI/IMEI, DSL-Teilnehmeranschluss) sowie der Standort des mobilen Gerätes.

4. Die EG-Richtlinie 2006/24/EG lässt eine *Speicherdauer* von mindestens 6 Monaten bis maximal 2 Jahren zu (Art. 6). Die Regierungskoalition hat am 9. Februar 2006 im Deutschen Bundestag angekündigt, von der Vorratsspeicherung für einen Zeitraum von 6 Monaten Gebrauch zu machen (BT-Drs. 16/545, S. 4; BT-Prot. 16/19, S. 1430B).

5. Die *Umsetzung* der EG-Richtlinie 2006/24/EG muss bis zum 15. September 2007 erfolgt sein (Art. 15 Abs. 1). Deutschland kann aufgrund einer entsprechenden Erklärung die Anwendung für die Dienste Internetzugang, Internet-Telefonie und E-Mail bis zum 15. März 2009 aufschieben (Art. 15 Abs. 3). Ein Gesetzentwurf der Bundesregierung liegt noch nicht vor.
   Die folgende Bewertung setzt eine Umsetzung der EG-Richtlinie in das nationale Recht der Bundesrepublik voraus:

6. Die Verpflichtung zur Vorratsdatenspeicherung verstößt gegen das national durch Art. 10 GG sowie europarechtlich durch Art. 8 EMRK geschützte Fernmeldegeheimnis. Sie verstößt gegen das Verbot der Speicherung „nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken" (BVerfGE 65, 1, 47). Dieses *Verbot der Vorratsdatenspeicherung* hat das

Bundesverfassungsgericht für den Bereich der Telekommunikation (BVerfGE 100, 313, 360) wiederholt und jüngst in der Entscheidung zur Einschränkung der Rasterfahndung noch einmal wiederholt (BVerfG, Beschluss vom 4. April 2006, NJW 2006, 1939). Die Zwecke der Vorratsdatenspeicherung sind unbestimmt, weil die Verkehrs- und Standortdaten aller Teilnehmer und Netze öffentlicher elektronischer Kommunikationsdienste pauschal und *ohne jeden konkreten Anhaltspunkt* für eine konkrete Straftat der betroffenen Personen gespeichert werden.

7. Die Einbeziehung *aller Kommunikationsteilnehmer* qualifiziert die Vorratsdatenspeicherung als eine Maßnahme mit einer außerordentlich hohen Eingriffsintensität (vgl. BVerfG, Beschluss vom 4. April 2006). Das Bundesverfassungsgericht hat bei Maßnahmen mit einer hohen Streubreite auf die gesamtgesellschaftliche Bedeutung des Schutzes der Vertraulichkeit der Telekommunikation verwiesen. Es gefährdet die Unbefangenheit der Nutzung der Telekommunikation und in der Folge die Qualität der Kommunikation einer Gesellschaft, wenn die Maßnahmen dazu beitragen, dass die Risiken des Missbrauches und ein Gefühl des Überwachtwerdens entstehen (BVerfGE 107, 299, 328). Für die Vorratsdatenspeicherung gilt dies erst recht, weil es sich um einen Grundrechtseingriff mit maximaler Streubreite handelt, durch den alle Teilnehmer und Nutzer der elektronischen Kommunikation erfasst werden.

8. Die Vorratsdatenspeicherung ist unverhältnismäßig und damit verfassungswidrig, weil sie die Speicherung von Verkehrs- und Standortdaten aller Kommunikationsteilnehmer *ohne jeden Verdacht* anordnet. Nach dem Grundsatz der Verhältnismäßigkeit dürfen intensive Grundrechtseingriffe erst von bestimmten Verdachts- oder Gefahrenstufen an vorgesehen werden (vgl. BVerfGE 100, 313, 383 f.; 109, 279, 350 ff.). Grundrechtseingreifende Maßnahmen „ins Blaue hinein“ sind unzulässig (vgl. BVerfGE 112, 284, 297, Beschluss vom 4. April 2006). Verfassungswidrig sind Maßnahmen, bei denen die Betroffenen keinerlei Nähe zu der abzuwehrenden Gefahr aufweisen (Beschluss vom 4. April 2006). Dies ist bei der Vorratsdatenspeicherung aber der Fall, weil sie ausnahmslos alle Teilnehmer öffentlicher elektronischer Kommunikationsdienste ohne jede begrenzende Anforderungen an die Wahrscheinlichkeit eines Gefahreneintritts erfasst.

9. Die Vorratsdatenspeicherung ist verfassungswidrig, weil sie nicht erforderlich ist. Ein milderes und geeignetes Mittel wäre eine gesetzliche Regelung eines so genannten *Quick Freeze* Mit einer solchen Regelung können die Strafverfolgungsbehörden ermächtigt werden, in einem konkreten Verdachtsfall die zeitlich begrenzte Speicherung bestimmter Kommunikationsbeziehungen anzuordnen. Auf diese Weise wird die Speicherung auf konkrete Anlässe verfassungskonform beschränkt, ohne eine wirksame Strafverfolgung zu behindern. Vorschläge in diese Richtung sind von den Datenschutzbeauftragten des Bundes und der Länder bereits mehrfach unterbreitet worden. Der Gesetzgeber hat mit § 16 b Wertpapierhandelsgesetz eine solche Regelung u.a. zur Bekämpfung des Insiderhandels an Börsen bereits erlassen.

10. Die Vorratsdatenspeicherung ist unverhältnismäßig, weil angesichts dieser Alternative der *Aufwand* in keinem Verhältnis zu ihrem Ertrag steht. Erfasst werden von der Vorratsdatenspeicherung alle Teilnehmer und Nutzer der elektronischen Kommunikation, ohne einen konkreten Anlass geboten zu haben. Es handelt sich für einen Zeitraum von 6 Monaten um mehrere Milliarden Datensätze. Nach Feststellungen des Bundesverfassungsgerichts waren es 2002 alleine bei der Deutschen Telekom und nur bezogen auf die Sprachtelefonie *täglich* 216 Mio. Datensätze (BVerfGE 107, 299,

327). Hinzu kommen die Datensätze der anderen Telefonanbieter sowie die Verkehrsdaten der Internetanbieter. Nach Feststellungen des Industrieverbandes BITKOM würde die Erfassung der Verkehrsdaten eines größeren Internetproviders eine Datenmenge von 20.– bis 40.000 Terabytes pro Jahr umfassen. Eine Menge von 40.000 Terabytes entspricht ungefähr rund 40 km gefüllter Aktenordner. Zudem verdoppelt sich laut BITKOM der Internetverkehr in Deutschland alle 14 Monate (Bitkom, Stellungnahme vom 14. 9. 2004, S. 6). Nach einer unveröffentlichten Untersuchung des Bundeskriminalamtes wurden für den Zeitraum vom 1. April bis zum 30. September 2005 insgesamt jedoch nur 381 Fälle gemeldet, in denen eine längere Speicherdauer den Ermittler nach eigenen Angaben geholfen hätten. Nur 2 Fälle betrafen Straftaten aus dem Bereich der organisierten oder terroristischen Kriminalität nach § 129 a, § 129 b StPO (BKA, Mindestspeicherungsfristen für Telekommunikationsverbindungsdaten, 15.11.2005).

11. Die Vorratsdatenspeicherung begegnet auch wegen der *Dauer der Speicherung von 6 Monaten* erheblichen verfassungsrechtlichen Vorbehalten. Nach schwedischen und britischen Erkenntnissen beziehen sich die Datenabfragen der Sicherheitsbehörden zu 80 bis 85% auf einen Zeitraum der letzten drei Monate, nicht aber auf längere Zeiträume (Gutachten des Wiss. Dienstes des Deutschen Bundestages vom 3. August 2006, S. 13). Diese Aussage stützt sich auf eine von dem Industrieverband BITKOM in Auftrag gegebene Studie, wonach in den Staaten, die bereits eine Vorratsdatenspeicherung erlassen haben, von den Sicherheitsbehörden Daten in der Regel nur aus Zeiträumen angefragt werden, die bis zu 3 Monate zurückliegen.[1] Eine Vorratsdatenspeicherung über einen Zeitraum von 6 Monaten ist demnach nicht erforderlich. Diese Erkenntnis zeigt gleichzeitig, dass die der Vorratsdatenspeicherung zugrunde liegenden rechtstatsächlichen Annahmen offensichtlich noch einer unabhängigen Überprüfung und Bewertung bedürfen.

12. Die Vorratsdatenspeicherung begegnet verfassungsrechtlichen Bedenken, weil die massenhaften Speicherung von Verkehrs- und Standortdaten das *Risiko eines Datenmissbrauches* deutlich erhöht. Der Grundsatz der Erforderlichkeit, der auch Grundlage des Gebotes der Datensparsamkeit und –vermeidung ist, beschränkt die Datenspeicherung auf das nach Art, Umfang und Dauer für die Abwicklung der betrieblichen Zwecke notwendige Maß. Durch die Verpflichtung zur Löschung der Verkehrs- und Standortdaten werden gleichzeitig Gesetzesverstöße präventiv verhindert. Die Verpflichtung zur Vorratsdatenspeicherung bewirkt demgegenüber eine deutliche Risikoerhöhung, weil nun Verkehrs- und Standortdaten über längere Zeiträume entgegen den gesetzlichen Regelungen bspw. für die Auswertung für Kundenprofile zur Verfügung stehen. Der aktuelle italienische Telefonskandal - dort konnte durch interne Sicherheitsmaßnahmen nicht wirksam verhindert werden, dass ehemalige Mitarbeiter über längere Zeiträume zahlreiche Telefongespräche gezielt abhören konnten - belegt die erhebliche Verletzlichkeit der Telekommunikation gegen interne, aber auch externe Angriffe und damit die Risiken eines unzureichenden Datenschutzmanagements. Besorgnis erregend ist, dass die Angriffe nicht durch interne Sicherheitsmaßnahmen, sondern erst durch Hinweise eines Tatbeteiligten aufgedeckt werden konnten. Der Gesetzgeber hat bislang nicht zu erkennen gegeben, durch welche zusätzlichen Maßnahmen er zum Schutz der auf Vorrat gespeicherten Daten ein wirksames präventives Datenschutzmanagement gewährleisten will.

---

[1] http://www.bitkom.org/files/documents/Studie_VDS_final_lang.pdf, S. 8.

13. Die Vorratsdatenspeicherung wird auch nicht dadurch verfassungsmäßig, dass die Speicherung der Verkehrs- und Standortdaten durch die Dienstanbieter und die Herausgabe der Daten erst im Einzelfall durch eine richterliche Anordnung erfolgt. Ein solches *zweistufiges Verfahren* ändert zum einen nichts an der Eingriffsqualität der Verpflichtung zur Vorratsdatenspeicherung, die ausnahmslos alle Kommunikationsteilnehmer ohne einen konkreten Anlass erfasst. Zum anderen will die Regierungskoalitionen die Rechtsgrundlagen, auf die sich eine Auskunft auf Verkehrs- und Standortdaten im Ermittlungsverfahren stützen würde (§§ 100 g, h StPO), tatbestandlich offensichtlich nicht einschränken (BT-Drs. 16/545, S. 4).

14. Unter verfassungsrechtlichen Gesichtspunkten ist eine *Einschränkung der §§ 100 g, h StPO* dringend geboten. Von dieser Regelung sind – entgegen der EG-Richtlinie zur Vorratsdatenspeicherung - auch Delikte unterhalb der Schwelle schwerer Straftaten erfasst, soweit nur der Verdacht besteht, dass sie mit Hilfe von Telekommunikation begangen worden sind. Eine Einschränkung ist auch deswegen geboten, weil in der Rechtswirklichkeit über §§ 100 g, h StPO nicht nur die Kommunikationsdaten von Beschuldigten, sondern auch von gänzlich Unbeteiligten und Unverdächtigen wie potentiellen Zeugen beauskunftet werden (bspw. Funkzellenabfrage). Da mit der Vorratsdatenspeicherung die elektronischen Kommunikationsakte aller Teilnehmer über einen Zeitraum von 6 Monaten erfasst werden, bedarf die Regelung über die Beauskunftung aus den Verkehrs- und Standortdaten erheblicher tatbestandlicher Einschränkungen.

15. Die Vorratsdatenspeicherung wird insbesondere auch dadurch verfassungswidrig, dass die Herausgabe von Verkehrs- und Standortdaten Betroffener an die *Nachrichtendienste* wie das Bundesamt für Verfassungsschutz auch ohne einen konkreten Straftatenverdacht bzw. ohne eine konkrete Gefahrenlage unter den Voraussetzungen des § 3 Abs. 1 des Artikel 10-Gesetzes möglich ist (vgl. § 8 Abs. 8 f. BVerfSchG, § 8 Abs. 3 a BND-Gesetz, § 10 Abs. 3 MAG-Gesetz). Derartige Daten werden offensichtlich auch Nachrichtendiensten anderer Staaten zur Verfügung gestellt. Durch die Vorratsdatenspeicherung wird – so ist zu erwarten - die Proliferation derartiger Daten zunehmen. Die Rechtsgrundlagen der Nachrichtendienste zeigen, dass die Annahme, die Herausgabe von auf Vorrat gespeicherten Daten beträfe nur eindeutige Fälle der Verfolgung konkreter Straftaten, ein unvollständiges Bild vermittelt.

16. Die Vorratsdatenspeicherung verletzt das Recht der Betroffenen auf eine „offene, rückhaltlose und vertrauensvolle Kommunikation“ mit besonderen *Vertrauenspersonen* wie mit seinem Arzt, seinem Strafverteidiger oder seinem Seelsorger (vgl. bspw. BVerfGE 110, 226, 260). Verfassungsrechtlich geschützt ist insbesondere, ob und mit welcher Vertrauensperson der Betroffene in Kontakt getreten ist. Die Vorratsdatenspeicherung gefährdet bereits die Kontaktaufnahme, aber auch die Unbefangenheit der Kommunikation mit einer Vertrauensperson.

17. Die Vorratsdatenspeicherung gefährdet und verletzt die *Unabhängigkeit des Abgeordnetenmandats* (Art. 24 LV; Art. 46, 47 GG) sowie die Persönlichkeitsrechte der Abgeordneten (siehe auch Gutachten des Wiss. Dienstes des Landtages vom 28. Februar 2006, LT-Umdruck 16/620). Durch die Verpflichtung zur Vorratsdatenspeicherung werden die Kommunikationsbeziehungen des Abgeordneten erfasst, wenn und soweit er öffentliche Kommunikationsdienste und –netze nutzt. Bereits diese Speicherung der Verkehrs- und Standortdaten vermag die Abgeordneten in ihrer Aufgabe und

Funktion zu beeinträchtigen, die Regierung zu kontrollieren. Die Unabhängigkeit des Abgeordnetenmandats wird aber auch dadurch gefährdet, dass sich Bürgerinnen und Bürger davon abhalten lassen, mit ihren Abgeordneten in Kontakt zu treten. Eine Regelung, die die Kommunikationsdaten der Abgeordneten lediglich einem Verwertungsverbot unterwirft, wird der Unabhängigkeit des Abgeordnetenmandats schon deswegen nicht gerecht, weil die Vorratsdatenspeicherung anlasslos erfolgt und damit die Schutzregelungen zur Aufhebung der Immunität des einzelnen Abgeordneten praktisch unterläuft.

18. Die EG-Richtlinie zur Vorratsdatenspeicherung ist zudem erheblichen europarechtlichen Bedenken ausgesetzt, weil sie auf einer *falschen Rechtsgrundlage* erlassen worden ist. Die Richtlinie stützt sich auf Art. 95 EGV mit der Begründung, sie diene der Angleichung von Rechts- und Verwaltungsvorschriften zur Verbesserung des Binnenmarktes. Art. 95 EGV ist jedoch keine ausreichende Rechtsgrundlage für eine Maßnahme, die als Rahmenbeschluss der justiziellen Zusammenarbeit in der sog. „dritten Säule“ hätten beschlossen werden müssen. Dieser Meinung war ursprünglich auch die Kommission, weil die Vorratsdatenspeicherung schließlich ausschließlich für Zwecke der Strafverfolgung erfolgen sollte (Siehe Art. 1 Abs. 1). Die Kommission änderte ihre Meinung jedoch erst als die erforderliche Einstimmigkeit im Rat für einen solchen Rahmenbeschluss nicht erreicht werden konnte (siehe auch Gutachten des Wiss. Dienstes des Dt. Bundestages, a.a.O., S. 8). Nach der jüngsten Entscheidung des EuGH vom 30. Mai 2006 sind die europarechtlichen Zweifel erheblich gestiegen, denn das Gericht hat die ebenfalls auf Art. 95 ermöglichte Weitergabe von Flugdaten in die USA, die ebenfalls aus justiziellen Gründen erfolgte, wegen der falschen Wahl der Rechtsgrundlage für nichtig erklärt (NJW 2006, 88). Der Deutsche Bundestag teilt die Bedenken, dass Art. 95 die falsche Rechtsgrundlage für die Verpflichtung zur Vorratsspeicherung ist (BT-Drs. 16/545, S. 3).