Antrag

Fraktion der SPD Hannover, den 15.04.2011

Vorratsdatenspeicherung verfassungskonform regeln!

Der Landtag wolle beschließen:

Entschließung

I. Der Landtag stellt fest:

Aufgrund des vom Deutschen Bundestag am 9. November 2007 beschlossenen Gesetzes zur Novelle der Telekommunikationsüberwachung und zur Umsetzung der europäischen Richtlinie 2006/24/EG zur sogenannten Vorratsdatenspeicherung wurden ohne Anlass und vorsorglich Daten sämtlicher Telekommunikationsdienste für die Strafverfolgung gespeichert.

Die Umsetzung der EU-Richtlinie ging über die europäischen Vorgaben hinaus.

Am 2. März 2010 erklärte das Bundesverfassungsgericht dieses Gesetz für verfassungswidrig und somit für nichtig.

Das Bundesverfassungsgericht entschied, dass die Vorratsdatenspeicherung unverhältnismäßig in das Recht auf informationelle Selbstbestimmung und die persönliche Privatsphäre eingreift.

Sämtliche gespeicherten Daten mussten seit dem Urteil gelöscht werden.

Die anlasslose, verdachtsunabhängige Vorratsdatenspeicherung verhindert weder Terrorismus noch Kriminalität mehr als sonst. Die Landesregierung konnte bisher keine Auskunft erteilen, ob die Aufklärungsquote mithilfe gespeicherter Daten höher ist.

Bis zur Entscheidung des Bundesverfassungsgerichts hat die niedersächsische Verfassungsbehörde nur viermal von dieser besonderen Auskunftspflicht Gebrauch gemacht.

Der Wegfall der anlasslosen Vorratsdatenspeicherung führte zu keiner gravierenden Schutzlücke in unserem Rechtssystem, da es diese in Deutschland über einen längeren Zeitraum hinweg nie gegeben hat.

Im Internetzeitalter stehen die Ermittlungsbehörden jedoch vor der Herausforderung, auch zunehmend Straftaten im Netz zu bekämpfen. Angesichts der weiter zunehmenden Internetkriminalität, wie z. B. Kinderpornografie, sind jedoch an die Speicherung von Daten neue Anforderungen zu stellen.

Zwar ist eine bedingungslose anlasslose Speicherung von Daten generell abzulehnen, jedoch in Zeiten der Cyber-Welt auch nicht ganz verzichtbar.

Dies hat das Bundesverfassungsgericht auch berücksichtigt und hält eine Vorratsdatenspeicherung mit Artikel 10 GG für nicht schlechthin unvereinbar.

Es setzt mit seinem Urteil hohe rechtliche Hürden an die Datenspeicherung und fordert den Gesetzgeber auf, einen strengen Maßstab zu entwickeln.

Seit dem Urteil ist ein Jahr vergangen, und ein neues Gesetz unter Berücksichtigung der Grundsätze des Bundesverfassungsgerichtsurteils ist durch die Bundesregierung nicht eingebracht worden.

Der Rechtsunsicherheit muss nunmehr ein Ende gesetzt werden.

II. Der Landtag fordert die Landesregierung daher auf,

1. eine Bundesratsinitiative zu starten, die die aufgezeigte Rechtsunsicherheit durch die Neuregelung der Datenspeicherung insbesondere im Bereich der Telekommunikationsüberwachung behebt.

   a) Die Speicherung von Kommunikationsdaten darf maximal sieben Tage erfolgen.

   b) An die Herausgabe der Daten sind sehr hohe Hürden zu stellen.

   c) Der Abruf und die Nutzung der Daten dürfen nur bei Verdacht auf schwerste Straftaten, die in einem Katalog festgelegt werden müssen, erfolgen.

   d) Die Speicherung von IP-Adressen darf maximal 90 Tage erfolgen.

   e) Der Abruf aller Daten steht unter Richtervorbehalt.

   f) Hohe Sicherheitsanforderungen für die Datensicherheit: Die Behörden sind personell und sachlich so auszustatten, dass eine Überprüfung aller Zusagen der Herausgabe von Kommunikationsdaten zum Schutz der Privatsphäre im Rahmen der Aufnahme durch den Dienst möglich ist.

   g) Die von einem Datenabruf Betroffenen sind hierüber umgehend, bei Gefahr im Verzug zumindest im Nachhinein, zu unterrichten.

   h) Die durch die Speicherung der Daten entstandenen und nachgewiesenen Kosten sind dem Dienstanbieter zu erstatten.

   i) Für Berufsgeheimnisträger soll ein absolutes Verwertungsverbot gelten.

2. sich auf Bundesebene dafür einzusetzen, dass die Bundesregierung auf europäischer Ebene auf eine Änderung der Richtlinie 2006/24/EG (betreffend Vorratsdatenspeicherung im Telekommunikationsbereich) hinwirkt.

Begründung

Zu I:

Nach dem Urteil des Bundesverfassungsgerichts ist nach grundrechtsschonenden Alternativen zu suchen, die einerseits - in Umsetzung des Urteils - keine umfangreichen Nutzungsprofile ermöglichen, aber gleichzeitig den Ermittlern bei mittels Internet begangenen Delikten nicht die Hände binden und die Vorgaben der Richtlinie umsetzen.

Die von Bundesjustizministerin Sabine Leutheusser-Schnarrenberger favorisierte Alternative, das sogenannte Quick-Freeze-Verfahren, ist hierfür ungeeignet. Dieses Verfahren sieht den vollständigen Verzicht auf eine verdachtsunabhängige und anlasslose Speicherung von Verkehrsdaten auf Vorrat vor.

Voraussetzung hierbei ist ein hinreichender Verdacht oder Anlass, aufgrund dessen Daten auf „Zuruf“ eingefroren, also gespeichert werden und für die Strafverfolgung und Gefahrenabwehr genutzt werden können. Es kann aber nur das eingefroren werden, was auch vorhanden ist. Bis die Ermittlungen anlaufen, die IP-Adresse des Täters ermittelt wird, dauert es einige Zeit. Da aber nichts gespeichert werden darf, sind alle Daten weg.

Wenn keine Mindestspeicherfrist vorliegt, ist das Quick-Freeze-Verfahren völlig sinnlos.

Diese Möglichkeit, erst bei Verdacht auf Vorliegen einer Straftat die bei den Providern vorhandenen Daten einzufrieren, ist nicht zeitgemäß und daher zur Gewährleistung einer effektiven Strafverfolgung nicht ausreichend und verletzt außerdem rechtsstaatliche Grundsätze.

Zu II:

Die o. g. Forderung ist unter Beachtung der Vorgaben des Bundesverfassungsgerichtsurteils eine grundrechtsschonende Alternative zur Vorratsdatenspeicherung.

Unter Berücksichtigung der vom Bundesverfassungsgericht neu formulierten Hürden für den Zugriff auf die Daten und die Beschränkung bei Telekommunikationsverkehrsdaten auf schwerste Straftaten und die Gefahrenabwehr für Leib und Leben ist es erforderlich, den Umfang der zu speichernden Daten sowie den Kreis der Verpflichteten genau zu definieren.

Aufgrund der unterschiedlichen Informationsgewinnung und der unterschiedlichen Intensität der Eingriffe ist daher zwischen der Speicherung von Kommunikationsdaten und der Speicherung von IP-Adressen zu unterscheiden.

Die Protokollierung von E-Mail- und Telefondaten ist die große Gefahr der Vorratsdatenspeicherung. Denn sie erlaubt die Erstellung von Nutzungsprofilen und mehr. Insbesondere kann hier festgehalten werden, wer wann wem eine E-Mail geschrieben, wer wann wen angerufen oder wer sich wann wo aufgehalten hat (Mobiltelefon). Die langfristige Speicherung dieser Daten würde einen erheblichen Eingriff in die Privatsphäre aller Bürger bedeuten. Deswegen kann die Speicherung dieser Daten nicht von langer Dauer sein.

Mit der Speicherung von IP-Adressen ist es nicht möglich, Nutzungsprofile zu erstellen und Bürger zu überwachen oder Data Mining zu betreiben. Sie ermöglicht festzustellen, welche IP-Adresse zu welcher Uhrzeit wem zugeordnet war. Deswegen stellt die Speicherung von IP-Adressen keine tiefen Grundrechtseingriffe dar. Da jedoch die IP-Adresse oft der einzige Erfolg versprechende Ermittlungsansatz ist, ist sie unverzichtbar und rechtfertigt die Speicherung für einen überschaubaren Zeitraum, und zwar für 90 Tage beim Access-Provider.

Um den Missbrauch von Daten zu vermeiden, sind an die Datensicherheit hohe Anforderungen zu stellen. Voraussetzung hierfür ist, eine gesetzliche Regelung zu schaffen, die jedenfalls dem Grunde nach normenklar und verbindlich die Sicherheitsmaßstäbe vorgibt. Hierbei steht es dem Gesetzgeber frei, die technische Konkretisierung des vorgegebenen Maßstabs einer Aufsichtsbehörde anzuvertrauen. Nur so kann sichergestellt werden, dass die Entscheidung über Art und Maß der zu treffenden Schutzvorkehrungen nicht unkontrolliert in den Händen der jeweiligen Telekommunikationsanbieter liegt.

Ein Abruf der Daten darf nur durch bestimmte Tatsachen begründeter Verdacht einer auch im Einzelfall schwerwiegenden Straftat erfolgen. Der Gesetzgeber hat einen abschließenden Katalog der Straftaten zu erstellen.

Aufgrund des Eingriffs in die Privatsphäre und um den Missbrauch zu vermeiden, ist die Übermittlung und Nutzung der gespeicherten Daten unter Richtervorbehalt zu stellen.

Der Betroffene ist über die Verwendung seiner Daten zu informieren. Sollte der Zweck der Untersuchung, dem der Datenabruf dient, dadurch gefährdet sein, muss zumindest eine nachträgliche Benachrichtigung des Betroffenen erfolgen.

Grundsätzlich ist ein Übermittlungsverbot der Daten für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen, wie etwa Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern telefonische Beratung in seelischen oder sozialen Notlagen anbieten und insoweit anderen Verschwiegenheitsverpflichtungen unterliegen, zu regeln.

Die Entschädigung der Diensteanbieter hat den Effekt, dass damit Datensparsamkeit belohnt wird und der massenhafte Zugriff auf VDS-Daten für die Behörden nicht billiger wird als andere, oft grundrechtsschonendere und volkswirtschaftlich verträglichere „klassische“ Ermittlungen.

Stefan Schostok
Fraktionsvorsitzender

(Ausgegeben am 18.05.2011)