Schleswig-Holsteinischer Landtag
Umdruck 15/4788

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

ULD • Postfach 71 16 • 24171 Kiel

Vorsitzende
des Innen- und Rechtsausschusses
Frau Monika Schwalm
Landeshaus

24105 Kiel

Holstenstr. 98
D-24103 Kiel
Tel.: 0431/988-1200
Fax: 0431/988-1223

Ansprechpartner/in:
Herr Bizer
Durchwahl: 988-1286

Aktenzeichen:
LD7-74.03/99.036

Kiel, 11. August 2004

Bekämpfung der Internetkriminalität - Vorschlag der CDU-Fraktion zur Speicheranordnung für Verbindungsdaten
LT-Drucksache 15/3373
Ihr Schreiben vom 08.06.2004

Sehr geehrte Frau Schwalm,

mit Schreiben vom 8. Juni 2004 haben Sie mich gebeten, zu der oben genannten Initiative der CDU Stellung zu nehmen. Diese Gelegenheit nehme ich gerne wahr. Gegenstand der Initiative der CDU-Fraktion ist zum einen die Schaffung der gesetzlichen Voraussetzungen für die kurzfristige Speicheranordnung durch Ermittlungsbeamte („quick freeze“). Zum anderen wird mit der Initiative eine Erweiterung des Anlasstatenkataloges für die Telekommunikationsüberwachung angestrebt.

Die Schaffung einer gesetzlichen Befugnis, mit der Ermittlungsbeamte den Anbietern von Telekommunikationsdienstleistungen kurzfristig untersagen können, bereits gespeicherte Verbindungsdaten zu löschen, kann eine sinnvolle Ergänzung zu den bereits bestehenden gesetzlichen Regelungen sein. Allerdings darf eine solche Befugnis nur in gesetzlich genau eingegrenzten Fällen zum Tragen kommen. Zudem sind ausreichende verfahrensrechtliche Sicherungen vorzusehen. Vor einer Neuregelung ist die Wirksamkeit der bislang getroffenen Regelungen belastbar zu überprüfen.

1. Auskunft über Verbindungsdaten und Löschungspflichten

Hintergrund des Vorschlages ist die Bedeutung der im Rahmen der Telekommunikation anfallenden Verbindungsdaten für die Ermittlung und Aufklärung von Straftaten. Beispiele sind die Ermittlung einer Zielrufnummer, mit der ein Verdächtiger telefoniert hat, oder die IP-Nummer eines Internetnutzers. Als Rechtsgrundlage derartiger Ermittlungen für Zwecke der Strafverfolgung ist §§ 100g, 100h StPO einschlägig. Danach sind die Anbieter geschäftsmäßiger Telekommunikation unter im Einzelnen bestimmten Voraussetzungen verpflichtet, Auskunft über die bei ihnen gespeicherten Verbindungsdaten zu erteilen. Die Auskunft ist u.a. an den Verdacht bestimmter Straftaten geknüpft, muss die Verbindungsdaten einer bezeichneten Person betreffen und setzt eine richterliche Anordnung voraus.

Faktisch ist die Herausgabepflicht allerdings begrenzt, weil die Anbieter der Telekommunikation nur solche Verbindungsdaten herausgeben können, die sie in ihren Systemen zum Zeitpunkt der Herausgabeanordnung auch gespeichert haben. Nach § 96 Abs. 2 TKG 2004 (BGBl. I S. 1190) sind die Verkehrsdaten – diese Bezeichnung verwendet das neue TK-Recht in Anlehnung an das Europäische Recht für den bislang gebräuchlichen Begriff der Verbindungsdaten – „nach Beendigung der Verbindung zu löschen“, soweit sie nicht zum Aufbau weiterer Verbindungen oder im TKG ausdrücklich genannter Zwecke noch verarbeitet werden dürfen.

Wichtigster Ausnahmefall von dieser Löschungsverpflichtung ist die Verarbeitung der Verkehrsdaten, um die Entgelte abzurechnen. Die hierfür erforderlichen Daten dürfen nach § 97 Abs. 3 Satz 3 TKG höchstens sechs Monate nach Versendung der Rechnung gespeichert werden. Im Unterschied zur bisherigen Rechtslage, wonach die Zielrufnummer im Regelfall um die letzten drei Ziffern gekürzt gespeichert wurde (§ 7 Abs. 3 Satz 3 TDSV 1996 – nun außer Kraft), wird nach neuer Rechtslage die Zielrufnummer vom Dienstanbieter ungekürzt gespeichert (§ 97 Abs. 4 Satz 2 TKG 2004). Etwas anderes gilt nur, wenn ein Teilnehmer von seinem Wahlrecht auf Löschung Gebrauch macht und sich für eine vollständige Löschung der Zielnummern entscheidet. Dieses ist jedoch nach der gesetzlichen Regelung nicht der Normalfall.

Zusammenfassend ist also festzuhalten, dass Verbindungsdaten nach geltender Rechtslage von den Anbietern der Telekommunikation im Regelfall bis zu 6 Monate gespeichert werden dürfen, wobei die Zielrufnummer nach neuer Rechtslage im Regelfall ungekürzt gespeichert wird. In diesem Umfang können die Ermittlungsbehörden die Verbindungsdaten unter den Voraussetzungen der §§ 100 g, h StPO herausverlangen.

2. Zur Forderung nach einer Vorratsdatenspeicherung

Nach Einschätzung der Telekommunikationsanbieter gehört die Auskunft nach § 100 g, h StPO mittlerweile zu den Standardmaßnahmen der polizeilichen Ermittlungstätigkeit. Die auf §§ 100 g, h StPO gestützten Anordnungen übersteigt die Zahl der nach § 100 a StPO erlassenen Anordnungen nach einhelligen Angaben der TK-Wirtschaft um ein Vielfaches. Allerdings wird keine Statistik über die Anordnungen nach §§ 100 g, h StPO geführt, so dass die tatsächliche Höhe der Anordnungen im Dunkeln bleibt.

Trotz der praktisch großen Bedeutung der Auskunftsverlangen nach §§ 100 g, h StPO wird in unregelmäßigen Abständen die Forderung erhoben, die im TK-Datenschutzrecht vorgesehene Höchstspeicherfrist in eine Mindestspeicherpflicht zu verändern. Auf diese Weise sollen die Anbieter der Telekommunikation verpflichtet werden, die Verbindungsdaten für eine bestimmte Mindestspeicherfrist auf Vorrat zu speichern, damit sie gegebenenfalls an die Ermittlungsbehörden herausgeben werden können.

2.1 Deutschland

In Deutschland hat sich zuletzt der Gesetzgeber in diesem Frühsommer nach einem Vermittlungsverfahren trotz gegenteiliger Vorschläge aus dem Bundesrat (BR-Drs. 15/2316, S. 120) und einer zögerlichen Haltung der rot-grünen Bundesregierung (BT-Drs. 15/2345, S. 7) *gegen* eine Verpflichtung zur Vorratsdatenspeicherung von Verbindungsdaten entschieden.

Trotz gegenteiliger Stimmen aus einzelnen CDU bzw. CSU regierten Bundesländern hatte sich insbesondere die CDU/CSU-Bundestagsfraktion in einem Entschließungsantrag vom 13. Januar 2004 gegen eine Vorratsdatenspeicherung ausgesprochen:

„Eine generelle und undifferenzierte Vorratsdatenspeicherung von Verkehrsdaten ist aus Datenschutzgründen (Grundsatz der Datenvermeidung und Datensparsamkeit sowie der Beschränkung der Weiterverwendung auf wenige begründbare und nachvollziehbare Einzelfälle) bedenklich und würde darüber hinaus zu einer unverhältnismäßigen finanziellen Belastung der Telekommunikationsunternehmen führen.“

Auch die FDP-Fraktion im Deutschen Bundestag hatte sich in einer eigenen Entschließung vom 10. März 2003 BT-Drs. 15/2686, S. 8) deutlich gegen eine Verpflichtung zur Vorratsdatenspeicherung ausgesprochen

„Die Vorschläge des Bundesrates, eine Pflicht zur Vorratsdatenspeicherung von Verkehrsdaten von sechs Monaten einzuführen, ist <sind> strikt abzulehnen. Ein solcher Vorschlag widerspricht dem liberalen Rechtsstaatsverständnis …“

Hervorzuheben ist, dass sich gegen die Verpflichtung zur Vorratsdatenspeicherung nicht nur die Datenschutzbeauftragten in zahlreichen Stellungnahmen und öffentlichen Äußerungen, sondern bspw. auch die Branchenverbände der Informationswirtschaft sowie zahlreiche Firmen ausgesprochen haben. Nur beispielhaft ist die Stellungnahme von BITKOM zu nennen, der eine Mindestspeicherpflicht nachdrücklich abgelehnt hat.
„Durch diese Maßnahme ist nur eine geringe Stärkung der staatlichen Strafverfolgung und Gefahrenabwehr zu erwarten. Dies wird aber durch schwere Eingriffe in das Grundrecht der Bürger auf informationelle Selbstbestimmung wie auch in die Wirtschaftstätigkeit der betroffenen IT-Unternehmen erkauft …“ (BT-Drs. 15(9)949.

2.2 Europa

Während die nationale Debatte durch die Verabschiedung des Telekommunikationsgesetzes vorerst beendet scheint, wird sie derzeit auf europäischer Ebene erneut diskutiert. Ausgangspunk ist der Entwurf für einen Rahmenbeschluss über die Vorratsdatenspeicherung von Daten, der von den Mitgliedstaaten Frankreich, Irland, Schweden und Großbritannien am 28. April 2004 vorgelegt worden ist (Dok. 8958/04). In diesem Dokument wird in Art. 4 eine Frist von mindestens 12 und höchstens 36 Monaten vorgeschlagen, wobei den Mitgliedstaaten auch die Möglichkeit eingeräumt wird, längere Fristen festzulegen. Derzeit führt die Europäische Kommission bis zum 15. September 2004 eine öffentliche Konsultation zu diesem Thema durch.

Eindeutig gegen diese Vorschläge hat sich bereits der Bundesverband der Deutschen Industrie (BDI) in seiner Stellungnahme vom 7. Juli 2004 ausgesprochen. Insbesondere für den Bereich des Internet zieht der BDI wegen der zahlreichen Umgehungsmöglichkeiten eine Eignung der Vorratsdatenspeicherung in Frage. Vor allem macht der BDI auf die ungeheuren Datenmengen aufmerksam, die eine Verpflichtung zur Vorratsdatenspeicherung nach sich zieht.

Bereits bei größeren Festnetz- und Mobilfunkunternehmen im Bereich der klassischen leitungsvermittelten Telefonie ist zu erwarten, dass pro Jahr um die fünfhundert Milliarden zusätzlich zu speichernde Datensätze mit einem Datenvolumen von ca. 8 Terabyte (1 Terabyte = 1 Mio. Megabytes) entstehen. (…)

Falls alle erdenklichen Verkehrsdaten gespeichert werden müssten, die potenziell im Rahmenbeschluss erfasst werden, würde im Netz eines größeren Internet Service Providers (ISPs) bereits bei heutigem Verkehrsaufkommen eine insgesamt kaum mehr vorstellbare Datenmenge pro Jahr von rund 20 – 40.000 Terabyte anfallen (40.000 Terabyte entspräche rund 4 Mio. km gefüllter Aktenordner). Derzeit ist davon auszugehen, dass sich der Internetverkehr in Deutschland alle 14 Monate verdoppelt (…)

Bei einem Datenvolumen von 20 – 40.000 Terabyte würde ein einmaliger Suchlauf bei einem Einsatz der vorhandenen Technik ohne zusätzliche Investitionen ca. 50 -100 Jahre dauern.

Bereits diese Dimensionen verdeutlichen, dass eine Verpflichtung zur Vorratsdatenspeicherung nicht nur aus verfassungsrechtlichen Gründen wegen einer Speicherung für noch nicht konkret bestimmte Zwecke verfassungswidrig ist, sondern dass sich die Unverhältnismäßigkeit dieser Maßnahme auch dem Missverhältnis von Aufwand und möglichem Ertrag ergibt. Bei Suchlaufzeiten von mehreren Jahren für einen Datensatz kann eine Verpflichtung zur Vorratsdatenspeicherung kein wirksames und damit verfassungsmäßiges Mittel sein.

3. Quick freeze

Vor diesem Hintergrund werden seit einigen Jahren Konzepte des „quick freeze“ als ein milderes Mittel zur Vorratsdatenspeicherung diskutiert. Die Bezeichnungen sind unterschiedlich, teilweise wird auch von „anlassbezogener Speicherung“ oder einer „Speicheranordnung“ gesprochen. Ihnen ist gemeinsam, dass auf Anordnung der Ermittlungsbehörden die routinemäßige Löschung eines Datenbestandes durch den TK-Dienstanbieter blockiert („eingefroren“) wird, um dann auf eine nachträgliche richterliche Anordnung „aufgetaut“ und den Ermittlungsbehörden bereit gestellt werden zu können.

Bereits im Gesetzgebungsverfahren zum TKG wurden derartige Vorschläge bspw. von der Deutschen Telekom AG als milderes Mittel gegenüber einer Vorratsdatenspeicherung in die Diskussion gebracht (BT-Drs. 15(9)949, S. 163). Auch der BDI hat als Vorteil einer anlassbezogenen Speicherung hervorgehoben, dass „nicht riesige Datenmengen gespeichert und den Ermittlungsbehörden zur Verfügung gestellt werden müssen“, sondern die Daten bestimmter verdächtiger Personen ohne größeren Aufwand zur Verfügung gestellt werden könnten (Stellungnahme vom 7. Juli 2004, S. 5).

In der Tat kann sich die Befugnis zur Anordnung eines „quick freeze“ von Verbindungsdaten gegenüber der Vorratsdatenspeicherung als weniger eingriffsintensives Mittel darstellen, weil auf eine flächendeckende Vorhaltung von Verbindungsdaten verzichtet wird und sich die verlängerte Speicherung auf anlassbezogene Einzelfälle beschränkt. Die Ermittlungsbeamten hätten auf diese Weise die Möglichkeit, die schnelle Löschung von Verbindungsdaten, soweit sie ohnehin aus Abrechnungszwecken oder aus technischen Gründen gespeichert sind, zu verhindern, ohne unmittelbar selbst an die Daten zu gelangen. Zudem würde mit einer solchen Regelung zumindest in Deutschland kein Neuland betreten werden. § 16 b Abs. 1 des Wertpapierhandelsgesetzes sieht bereits heute ein solches Verfahren vor, wenngleich für einen sehr engen Anwendungsbereich.

Allerdings sollte der Gesetzgeber nicht voreilig handeln: Zum einen ist die Regelung des § 16 b Wertpapierhandelsgesetz zwar seit Mitte 2002 in Kraft, es sind aber bislang keine Erfahrungsberichte über seine Anwendung bekannt. Entsprechendes gilt im Übrigen auch für die Erfahrungen aus der Anwendung des erst in diesem Sommer in Kraft getretenen TKG, das die Regelkürzung der Rufnummern zu einer regelmäßigen Vollspeicherung verändert hat. Zudem fehlt es dem Gesetzgeber an einer verlässlichen Datenbasis über die Zahl und den Erfolg der Anordnungen nach § 100 g, h StPO. Schließlich sind wirksame Möglichkeiten zu entwickeln, damit die „Freeze“-Anordnung nicht zum Regelfall und damit zu einer routinemäßigen Maßnahme der Ermittlungsbehörden wird. Immerhin stellen derartige Anordnungen Eingriffe in das Fernmeldegeheimnis nicht nur des Beschuldigten dar, sondern auch in die Rechte aller weiteren Kontaktpersonen sowie sonstiger an der Telekommunikation beteiligter Dritter, die im Wege dieser heimlichen Überwachungsmaßnahme in das Fadenkreuz der Fahnder geraten.

Im Fall einer derartigen Gesetzgebung wäre im Übrigen verfahrensrechtlich sicherzustellen, dass nicht die Anordnung zur Herausgabe der Verbindungsdaten führt, sondern lediglich eine sofortige, datenschutzrechtlich an sich gebotene Löschung dieser Daten zeitlich begrenzt unterbleibt. Über die Herausgabe der Daten ist anschließend im bereits geregelten Verfahren nach §§ 100g und 100h StPO zu entscheiden, welches nicht umgangen werden darf. Deshalb muss vorgesehen werden, dass die Anordnung nur für eine begrenzte Zeitdauer wirksam ist, damit der Vorgang unverzüglich einer richterlichen Entscheidung und Überprüfung zugeführt wird. Auch ist die Möglichkeit zur Anordnung auf eng begrenzte Fälle zu beschränken, die keinesfalls über den Anwendungsbereich der §§ 100 g, h StPO hinausgehen dürfen und auf die Fälle schwerer Kriminalität zu beschränken sind. Aus diesem Grund kommt auch eine Anordnungsbefugnis außerhalb des strafrechtlichen Ermittlungsverfahrens nicht in Betracht.

4. Ausweitung des Straftatenkataloges

Die Überwachung der Telekommunikation einzelner Verdächtiger – also nicht nur der Verbindungsdaten, sondern auch der Gesprächsinhalte – darf gemäß §§ 100a ff. StPO nur unter bestimmten Voraussetzungen und aufgrund eines richterlichen Beschlusses erfolgen. Zu diesen Voraussetzungen gehört, dass die Telekommunikationsüberwachung nur aus Anlass des Verdachts bestimmter in einem Katalog enthaltener besonders schwerer Delikte erfolgen darf.

Eine Erweiterung des sog. Anlasstatenkataloges – etwa auf die Fälle der Verbreitung von Kinderpornografie – kann sinnvoll und notwendig sein. Eine Diskussion, die sich nur auf die Ausdehnung des Anlasstatenkatalogs bezieht, greift jedoch zu kurz. Der Anlasstatenkatalog ist in der Vergangenheit stetig erweitert worden, ohne dass ausreichend über eine – dringend notwendige – Neujustierung des Rechts der Telekommunikationsüberwachung diskutiert wurde.

Das Bundesverfassungsgericht hat immer wieder betont, dass die Telekommunikationsüberwachung eine Ermittlungsmethode ist, die besonders schwer in die Grundrechte eingreift und daher nur in Ausnahmefällen - als ultima ratio - Anwendung finden darf. Dennoch hat die Zahl der in den letzten Jahrzehnten überwachten Telefonanschlüsse dramatisch zugenommen. Dies belegen die jährlich von der Bundesregierung veröffentlichten Zahlen mehr als deutlich. Die Zahl der Anordnungen betrug bspw. im Jahr 1995 noch 3.667, im Jahr 2000 bereits 15.741, 2001 21.806 Anordnungen und schließlich 2003 sogar 26.177 Anordnungen (zuletzt BT-Drs. 15/2107, S. 12). Die Telefonüberwachung steht mit anderen Worten in der Gefahr zu einem „Massengeschäft“ zu werden, nachdem diese Ermittlungsmethode – die ursprünglich nur für Tötungsdelikte und schwerwiegende Staatsschutzdelikte vorgesehen war – seit dem Jahr 1968 durch knapp 20 Änderungen stetig erweitert wurde.

Wenn also - wie in dem Gesetzesvorschlag - die Erweiterung des Anlasstatenkatalogs diskutiert werden soll, muss gleichzeitig auch geprüft werden, ob dieser – in Bezug auf andere Delikte – nicht auch reduziert werden kann. Grundrechtlich geboten ist an dieser Stelle eine ständige Evaluation und Neubewertung der Anlasstaten. Insbesondere ist auf Tatbestände zu verzichten, die über Jahre in der Praxis der TK-Überwachung keine nennenswerte Rolle spielen (Siehe die Aufstellung zuletzt

in BT-Drs. 15/2107, S. 12 f.). Schließlich sollte auch die Bedeutung der TK-Überwachung zur Aufklärung einzelner Deliktsgruppen nicht überschätzt werden: Der Straftatbestand des § 184 b Abs. 3 StGB, der die gewerbsmäßige Verbreitung, Erwerb und Besitz kinderpornographischer Schriften unter Strafe stellt, ist bspw. im Jahr 2003 lediglich in einem einzigen Verfahren zur Anwendung gekommen (BT-Drs. 15/2107, S. 14).

Eine grundsätzliche Neuregelung der Vorschriften zur Telekommunikationsüberwachung muss über eine bloße Anpassung des Anlasstatenkataloges deutlich hinausgehen, notwendig ist eine vollständige Überarbeitung der einschlägigen Vorschriften. Dies zeigt sich nicht zuletzt vor dem Hintergrund der Entscheidung des Bundesverfassungsgerichts vom 3.März 2004 zum Großen Lauschangriff. Das Bundesverfassungsgericht hat in seinem Urteil heraus gearbeitet, dass sich die Schutzbedürftigkeit der Kommunikation nicht nur an räumlichen Sphären festmacht, sondern vor allem aus dem Schutz der Gespräche ergibt und damit der zwischenmenschlichen Kommunikation gilt.[1] Aus diesem Grund sind die zentralen Aussagen der Entscheidung auch auf den Bereich der Telekommunikationsüberwachung zu übertragen und wirken sich auf das grundrechtlich gebotene Schutzkonzept aus. Der durch das Bundesverfassungsgericht geforderte Schutz des Kernbereichs persönlich vertraulicher Kommunikation und der Schutz der Kommunikation mit Berufsgeheimnisträgern ist auch im Bereich der Telekommunikationsüberwachung bislang nur unzureichend geregelt. Der Gesetzgeber ist daher aufgefordert, umfassende Erhebungs- und Verwertungsverbote zum Schutz des Kernbereichs privater Lebensgestaltung zu schaffen. Vorzugswürdig ist dabei eine „vor die Klammer gezogene“ Regelung, die für sämtliche heimlichen Ermittlungsmethoden gilt.

Schließlich ist auch auf die Ergebnisse der im Jahr 2003 veröffentlichten Studie des Max-Planck-Instituts hinzuweisen, die auf der Grundlage einer Aktenanalyse zu dem ernüchternden Resultat gekommen ist, dass unmittelbar auf eine TK-Überwachung nur 28% der „erfolgreichen“ Fälle zurückgeführt werden konnten. Die Studie resümiert trocken, dass ein statistisch signifikanter Zusammenhang zwischen dem Erfolg der Überwachungsmaßnahmen und der Katalogstraftat, die den Anlass der TK-Überwachung bildete, nicht feststellbar sei (Albrecht/Dorsch/Krüpe, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation, Baden-Baden 2003, S. 456.).

Mit freundlichen Grüßen

gez.
Dr. Helmut Bäumler

---

[1] Vgl. hierzu Stellungnahme des ULD zum Referentenentwurf des BMJ zum Großen Lauschangriff , http://www.datenschutzzentrum.de/material/themen/lausch/lsch_st4.htm