

## **Stellungnahme des BITKOM**

### **zur Gesetzesinitiative des Bundesrates für ein “Gesetz zur Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Missbrauchs von Kindern und der Vollstreckung freiheitsentziehender Sanktionen“ (Beschluss vom 31. Mai 2002, BRats-Drs. 275/02),**

### **insbesondere zur geplanten Einführung einer Vorratsdatenspeicherung (Änderung des § 89 TKG und Neueinführung eines § 6a TDDSG)**

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) vertritt 1.300 Unternehmen, davon gut 700 als Direktmitglieder mit ca. 120 Mrd. Euro Umsatz und mehr als 700.000 Beschäftigten. Hierzu zählen Produzenten von Endgeräten und Infrastruktursystemen sowie Anbieter von Software, Dienstleistungen, neuen Medien und Content. Mehr als 600 Direktmitglieder gehören dem Mittelstand an. BITKOM setzt sich insbesondere für eine Verbesserung der rechtlichen und politischen Rahmenbedingungen in Deutschland, für eine Modernisierung des Bildungssystems und für die Entwicklung der Informationsgesellschaft ein.

BITKOM nimmt hiermit Stellung zu einer Gesetzesinitiative des Bundesrates vom 31. Mai 2002, die unter dem Titel “Gesetz zur Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Missbrauchs von Kindern und der Vollstreckung freiheitsentziehender Sanktionen“ (BRats-Drs. 275/02) beschlossen wurde. Viele der im Gesetz enthaltenen Änderungsvorschläge stehen allerdings in keinem inneren Zusammenhang mit dem im Titel formulierten Ziel, sondern es handelt sich um weitreichende Verschärfungen des Einsatzes von Überwachungsmaßnahmen bei Telekommunikations- und Telediensten bei der allgemeinen Strafverfolgung und der Gefahrenabwehr. Hierzu zählt insbesondere die geplante Einführung einer Vorratsdatenspeicherung, für die durch die Änderung des § 89 TKG und die Neueinführung eines § 6a TDDSG die gesetzlichen Voraussetzungen geschaffen werden sollen. Es besteht daher der Verdacht, dass hier in der Öffentlichkeit sehr kritisch und kontrovers diskutierte Themen wie die Vorratsdatenspeicherung hinter einem Thema, das kaum zu einer kontroversen Diskussion taugt, versteckt und in dessen Schlepptau möglichst unbemerkt „durchgebracht“ werden sollen. Eine solche Vorgehensweise ist der Bedeutung der hier zu diskutierenden Themen nicht angemessen.

Der Gesetzgeber strebt mit der Novellierung eine Stärkung der staatlichen Stellen bei der Strafverfolgung und der Gefahrenabwehr an. BITKOM unterstützt grundsätzlich das Streben nach einer effektiven Verbrechensbekämpfung, insbesondere im Bereich der Schwerstkriminalität. Doch gerade die geplante Einführung der Vorratsdatenspeicherung stößt auf nachhaltige Bedenken. Durch diese Maßnahme ist nur eine geringe Stärkung der staatlichen

Strafverfolgung und Gefahrenabwehr zu erwarten. Diese wird aber durch schwere Eingriffe in das Grundrecht der Bürger auf informationelle Selbstbestimmung wie auch in die Wirtschaftstätigkeit der betroffenen TK-Unternehmen erkauft. Den Sicherheitsbehörden bleiben auch ohne diese zusätzlichen, stark belastenden Maßnahmen genügend Möglichkeiten, ihre Aufgaben erfolgreich wahrzunehmen. Dem gegenüber würden sich die geplanten Neuregelungen als ein Hemmschuh für die dynamische Weiterentwicklung der Kommunikationsmärkte darstellen: Die zu erwartenden wirtschaftlichen Belastungen der Unternehmen gingen letztlich zu Lasten des Wettbewerbs und der Verbraucher, da einzelne Marktteilnehmer in Anbetracht der hohen Belastung aus dem Wettbewerb ausscheiden würden, andere zur Kostenkompensation ihre Endkundenpreise erheblich anheben müssten. Damit wird die ordnungspolitisch wünschenswerte dynamische Weiterentwicklung der Telekommunikationsdienstleistungen, der neuen Medien und des E-Commerce in Deutschland gefährdet.

Grundsätzlich sollte zudem bei jeder Neuregelung zur Einführung neuer Sicherheitsmaßnahmen im Bereich der Telekommunikations- und Teledienste zunächst ein intensiver Dialog mit den betroffenen Unternehmen und ihren Verbänden gesucht werden, um bei wirklich erforderlichen Maßnahmen nach einer möglichst wenig belastenden und zugleich effektiven Lösung zu suchen. BITKOM steht hierfür als Gesprächspartner jederzeit gerne zur Verfügung.

Im Weiteren nimmt BITKOM zu den einzelnen Vorschlägen des Änderungsgesetzes detailliert Stellung:

## **I. Artikel 1: Änderungen in der Strafprozessordnung**

### **1. Nummer 1: Änderung in § 100a StPO**

Die vorgesehene Erweiterung des Straftatenkatalogs in § 100a StPO auf den Bereich des sexuellen Missbrauchs von Kindern und die Verbreitung kinderpornografischer Schriften wird grundsätzlich als ein Schritt zur Verfolgung eines wichtigen staatlichen Schutzziels erkannt. Hierbei ist allerdings zu beachten, dass inzwischen durch das am 13. Juni 2002 im Bundestag und am 12. Juli 2002 im Bundesrat verabschiedete „Sechste Gesetz zur Änderung des Strafvollzugsgesetzes“ (Bundesrats-Drucksache 539/02) bereits eine Ergänzung des § 100a StPO in diesem Bereich vorgenommen wurde. Hiernach sind Fälle eines schweren sexuellen Missbrauchs von Kindern nach § 176a Abs. 1, 2 oder 4 StGB und eines sexuellen Missbrauchs von Kindern mit Todesfolge nach § 176b StGB sowie die gewerbliche Verbreitung (kinder-)pornografischer Schriften nach § 184 Abs. 4 StGB in den Straftatenkatalog des § 100a StPO aufgenommen. Im Vergleich zu der vorliegenden Gesetzesinitiative des Bundesrates stellt dies zwar insoweit ein Weniger dar, als die minder schweren Begehungsformen des § 176 StGB, § 176a Abs. 3 und des § 184 Abs. 3 StGB nicht mit einbezogen wurden, dies erscheint jedoch gerade aufgrund der deutlich geringeren Schwere dieser Straftaten auch angemessen. Andernfalls wäre die Gleichartigkeit in dem Straftatenkatalog des § 100a StPO, der die schwerwiegenden Eingriffsbefugnisse gerade auf besonders schwere Straftaten beschränken soll, nicht mehr gewahrt. Auch in der jetzt bereits verabschiedeten

Form ist aber gewährleistet, dass die besonders gravierenden Fälle von Kindesmissbrauch und Kinderpornografie unter Verwendung aller zur Verfügung stehenden Ermittlungsmaßnahmen verfolgt werden können. Der in Artikel 1 Nr. 1 der Gesetzesinitiative enthaltene Änderungsantrag sollte daher nicht weiter verfolgt werden.

## **2. Nummer 2: Änderung in § 100c StPO**

Durch die geplante Änderung des § 100c Abs. 1 Nr. 1 StPO wird endgültig der Einsatz des so genannten „IMSI-Catcher“ auch auf Straftaten ausgedehnt, die nicht in den Katalog schwerer Straftaten in § 100a StPO fallen, soweit diese „von erheblicher Bedeutung“ sind. Zwar wurde, wie die Begründung des Gesetzentwurfs ausführt, auch bislang schon gelegentlich in solchen Fällen eine Anwendung des IMSI-Catcher auf § 161 StPO gestützt, doch ist die Neuregelung dennoch mehr als eine „Klarstellung“, weil die Heranziehung des § 161 StPO auch in Fällen nicht so gravierender Straftaten eindeutig umstritten war. Insofern stellt die Neuregelung aus der Sicht des BITKOM eine Verschärfung zur jetzigen Rechtslage dar, die wegen der mit dem Einsatz dieses Gerätes verbundenen Probleme als problematisch angesehen wird. Denn durch das „Vortäuschen“ einer Funkzelle wird nicht nur das jeweilige Observationsziel, sondern werden auch alle sonstigen Mobilfunknutzer im Einsatzgebiet betroffen. Diesen ist für einen bestimmten Zeitraum eine Mobilfunknutzung – einschließlich des Absetzens von Notrufen – nicht möglich. Hierin liegt zugleich ein Eingriff in die Wirtschaftstätigkeit der Telekommunikationsanbieter. Zum Teil dauern die Netzstörungen auch über den eigentlichen Einsatz des IMSI-Catcher an. Genauere Erkenntnisse über das Ausmaß der Störung sind trotz des Angebots der Netzbetreiber, hier weitergehende Untersuchungen durchzuführen, bislang nicht gesammelt worden. Der Verband fordert dazu auf, hier zunächst weitere Klarheit über die genauen technischen Auswirkungen zu sammeln, ehe der Einsatz auf weitere Gebiete der Strafverfolgung ausgedehnt wird. Grundsätzlich wird darauf zu achten sein, dass der Einsatz nur bei Straftaten erfolgt, deren Verfolgung tatsächlich ein solche Dringlichkeit hat, dass auch die mit dem Einsatz verbundenen Eingriffe in die Nutzungsmöglichkeiten anderer Handybesitzer, die Sammlung von Daten auch von unbeteiligten Personen und der Eingriff in die Wirtschaftstätigkeit der Telekommunikations-Anbieter zu rechtfertigen sind. Dies ist am ehesten bei einer Beschränkung des Einsatzes auf die Katalogstraftaten des § 100a StPO zu gewährleisten.

## **3. Nummer 3: Änderungen in § 100g StPO**

### **a) Nummer 3 a) aa) bbb): Änderung in § 100g Abs. 1 StPO**

Die geplante Festschreibung, dass die Auskunftserteilung nach § 100g StPO „unentgeltlich“ zu erfolgen hat, würde zu einer nicht hinnehmbaren und nicht zu rechtfertigenden Benachteiligung der betroffenen Telekommunikations-Anbieter führen. Bislang ist auf die Indienstnahme der Anbieter das Gesetz über die Entschädigung von Zeugen und Sachverständigen (ZSEG) anwendbar. Dies erscheint auch sachgerecht, da die Auskunftserteilung nach §§ 100g und 100h StPO als Wissensmitteilung eines unbeteiligten Dritten ihrem Wesen nach eine typische Zeugenaussage ist. Aus der Sicht des BITKOM sollte

die bisherige Praxis beibehalten werden. Die hierdurch gewährten geringen Entschädigungen decken selbst nicht entfernt den hohen Aufwand, der mit der Auskunftserteilung verbunden ist. Eine noch weitergehende auch kostenmäßige Überlagerung originärer Staatsaufgaben ist nicht zu rechtfertigen. Dies gilt umso mehr, als die entstehenden Kosten im Falle einer Verurteilung dem jeweiligen Straftäter auferlegt werden können, so dass der Staat nur bei letztlich unberechtigten Maßnahmen belastet wäre. Dies erscheint, um eine Ausuferung bei der Nutzung dieser Eingriffsbefugnisse zu verhindern, aber auch gerade geboten.

**b) Nummer 3 b): Änderung in § 100g Abs. 3 Nr. 1 StPO**

Die unter Nr. 3 b) geplante unscheinbare Änderung in § 100g Abs. 3 Nr. 1 durch Streichung der Worte „im Falle einer Verbindung“ bedeutet eine erhebliche Verschärfung der Telekommunikationsüberwachung und hierdurch bedingt auch einen nicht praktikablen Anstieg der Verpflichtungen für die Telekommunikations-Anbieter. Durch die veränderte Definition von Telekommunikationsverbindungsdaten werden nun auch solche Daten erfasst, die nicht nur im Rahmen einer tatsächlichen Telekommunikationsverbindung (Gespräch, Datenabruf etc.) angefallen sind, sondern auch Daten, die im Standby-Modus von eingeschalteten Handys an Mobilfunk-Basisstationen übermittelt werden, also etwa bei der Einbuchung in eine Funkzelle. Hieraus ergeben sich erheblich größere Datenmengen als bislang bei Geltung der Beschränkung auf tatsächliche Kommunikationsverbindungen. Darin liegt ein eklatanter Verstoß gegen die datenschutzrechtlichen Prinzipien der Datenvermeidung und der Datensparsamkeit.

Besonders bedenklich erscheint diese Änderung in Verbindung mit der ebenfalls in diesem Gesetzentwurf beabsichtigten Einführung einer Vorratsdatenspeicherung mit Mindestfristen für die Vorhaltung von „Telekommunikationsverbindungsdaten“ (hierzu unter den Nummern 3 und 4 in dieser Stellungnahme). In der Kombination entstünde dann faktisch eine Verpflichtung der TK-Unternehmen, ein Bewegungsprofil für alle Mobilfunknutzer Deutschland aufzuzeichnen und eine bestimmte Zeit für staatlichen Zugriff vorzuhalten. Treffend wurde hier schon vom Handy als potentieller „elektronischer Fußfessel“ gesprochen. Die Verpflichtung ist gerade auch deshalb bedenklich, weil es sich hier um Daten handelt, die von den TK-Anbietern über die unmittelbare Dienstleistung hinaus (also etwa für die Abrechnung) nicht benötigt werden. Eine Speicherung bedeutet daher einen eklatanten Verstoß gegen das Verbot einer zweckungebundenen Vorratsdatenspeicherung, wie es vom Bundesverfassungsgericht im Volkszählungsurteil aufgestellt wurde. Hier droht die moderne Informationsgesellschaft, in der etwa die Mobilfunknutzung zum Alltag gehört, für staatliche Überwachungsmaßnahmen über Gebühr in Anspruch genommen zu werden. In diesem Maße kann dies jedoch auch mit dem wichtigen und legitimen Ziel einer wirksamen Strafverfolgung nicht mehr gerechtfertigt werden.

Neben den datenschutzrechtlichen Bedenken stehen aber auch massive wirtschaftliche Bedenken. Auf den immensen Aufwand, den die erforderlichen Speicherkapazitäten und Systeme zur Datenverwaltung benötigen würden, wird im Rahmen der Stellungnahme zur Vorratsdatenspeicherung noch ausführlich eingegangen.

**c) Nummer 3 c): Neueinfügung eines § 100g Abs. 4 StPO**

Die als Klarstellung gedachte Ergänzung erscheint, wenn sie tatsächlich nur eine Klarstellung sein sollte, entbehrlich. Es besteht jedoch der Verdacht, dass hier unter dem Vorwand der Klarstellung eine Festschreibung dahingehend erreicht werden soll, dass die in § 100g vorgesehenen Änderungen auch für den Bereich der Teledienste gelten sollen. Dies erscheint aus datenschutzrechtlicher Sicht wegen des hierdurch wesentlich erweiterten Anwendungsbereichs bedenklich.

**4. Nummer 4: Änderungen in § 100 h StPO**

**a) Nummer 4 a): Änderung in § 100h Abs. 1 Satz 2 StPO**

Die Vorschrift bedeutet ebenfalls eine Ausdehnung der Auskunftsbefugnisse. Bedenklich ist hier, wie schon unter Nummer 3 Punkt b), das die Ermittlungsmaßnahmen nicht mehr an einer tatsächlich geführten Telekommunikation, sondern allein an der Aktivschaltung eines Mobiltelefons ansetzen. Dies bedeutet eine neue Dimension der Überwachungsmöglichkeit, die geeignet erscheint, das Vertrauen der Bürger in die Telekommunikation nachhaltig zu erschüttern. Derartige Maßnahmen sollte daher zumindest an hohe Eingriffsvoraussetzungen, vorzugsweise an das Vorliegen einer Katalogstraftat nach § 100a StPO, geknüpft werden.

**b) Nummer 4 b): Streichung des § 100h Abs. 2 StPO**

Die mit der Streichung des Absatz 2 einhergehende Aufhebung des Zeugnisverweigerungsrechts erscheint aus rechtsstaatlicher Sicht bedenklich. Die Existenz dieses Rechtes ist ein äußerst sensibler Punkt im Rahmen einer rechtsstaatlichen Strafverfolgung, so dass auch mit Blick auf die anhaltenden Diskussionen zur Reichweite der Zeugnisverweigerungsrechte hier nicht selektiv an einzelnen Stellen geändert, sondern ein in sich kohärentes und klares System angestrebt werden sollte. Bis dahin sollte eher ein Zuviel an Schutz als ein Zuwenig in Kauf genommen werden.

**5. Nummern 5 und 6: Ergänzungen in §§ 457 und 463 StPO**

Die geplanten Ergänzungen, die einer besseren Auffindung flüchtiger Sexualstraftäter dienen – unabhängig davon, ob sie zu einer Haftstrafe verurteilt wurden oder die Unterbringung in einem psychiatrischen Krankenhaus, einer Entziehungsanstalt oder in Sicherungsverwahrung angeordnet wurde –, erweitern erneut den Kreis der Anwendungsfälle für die stark freiheitsbeschränkende Telekommunikations-Überwachungsmaßnahmen nach §§ 100a, 100b, 100c StPO. Bei grundsätzlichem Verständnis für das Ziel, in solchen Fällen den flüchtigen Tätern möglichst schnell wieder habhaft zu werden, wird doch auch die erneute Einschränkung einer freien Telekommunikation mit Sorge gesehen. Der Gesetzgeber ist grundsätzlich gefordert, bei solchen Erweiterungen die Verhältnismäßigkeit dieser schwerwiegenden Eingriffe zu gewährleisten.

## **II. Artikel 2: Aufhebung der zeitlichen Befristung der Geltung der §§ 100g und 100h StPO**

Durch die Änderung soll die zeitliche Befristung bis zum Jahr 2005, unter der die erst Ende 2001 eingeführten Vorschriften §§ 100g und 100h StPO stehen, nachträglich aufgehoben werden. Für einen solchen Schritt sieht BITKOM zum jetzigen Zeitpunkt keine Notwendigkeit. Die tatsächlichen Gegebenheiten haben sich seit der Einführung der befristeten Vorschriften nicht verändert. Es ist daher nicht erkennbar, wieso nun eine unbefristete Geltung erforderlich sein sollte. Jedenfalls ist nicht nachvollziehbar, warum diese Entscheidung jetzt fallen sollte. Die Befristung von Gesetzen ist ein in anderen Ländern schon länger praktiziertes probates Mittel, um eine Überprüfung gesetzlicher Maßnahmen nach einem bestimmten Zeitraum sicherzustellen. Die alleinige Möglichkeit, Gesetze später zu ändern, – auf die die Begründung jetzt verweist – leidet daran, dass eine Überprüfung dann oft überhaupt nicht stattfindet. Erst die Befristung setzt hier den notwendigen Handlungsdruck. Angesichts der schwerwiegenden Freiheitseingriffe, die die fraglichen Vorschriften mit sich bringen, erscheint es dem Verband geboten, die Befristung zunächst aufrechtzuerhalten, um dann zu einem wesentlich späteren Zeitpunkt aufgrund der gemachten Erfahrungen und der weltpolitischen Entwicklung eine Neueinschätzung zum verbliebenen Gefahrenpotential, vor allem aber auch zur Wirksamkeit der geregelten Maßnahmen vorzunehmen. Die in Artikel 2 vorgesehene Änderung des Gesetzes zur Änderung der Strafprozessordnung vom 20.12.2001 sollte daher nicht weiter verfolgt werden.

## **III. Artikel 3 und 4: Einführung einer Vorratsdatenspeicherung.**

Mit den erst auf Antrag des Bundesrats-Rechtausschusses aufgenommenen Artikeln 3 und 4 der Gesetzesinitiative sollen durch Änderung des § 89 TKG und die Neueinführung eines § 6a TDDSG die gesetzlichen Voraussetzungen für eine Vorratsdatenspeicherung geschaffen werden. Die Bundesregierung soll sowohl für den Telekommunikationssektor als auch für den Bereich der Teledienste ermächtigt werden, mit Zustimmung des Bundesrates Mindestspeicherfristen für die Speicherung von Bestands-, Nutzungs- und Abrechnungsdaten einzuführen und einer Vielzahl staatlicher Stellen Zugriff auf diese Datenbestände zum Zwecke der Strafverfolgung einschließlich der Zollkriminalität, zudem aber auch zum Zwecke der allgemeine Gefahrenabwehr und des Verfassungsschutzes einzuräumen. BITKOM steht der geplanten Einführung einer Vorratsdatenspeicherung aus den im Nachfolgenden näher erläuterten Gründen ausgesprochen kritisch gegenüber:

### **■ Verstoß gegen das Wesentlichkeitsgebot**

Die geplante Einführung einer Vorratsdatenspeicherung stellt einen erheblichen Eingriff in Grundrechte dar, sowohl auf Seiten der betroffenen Nutzer (Recht auf informationelle Selbstbestimmung) als auch auf Seiten der betroffenen Anbieter (Artt. 12 und 14 GG). Angesichts der schwerwiegenden Belastungen erscheint es nicht hinnehmbar, dass durch die jetzt vorgelegte Gesetzesänderung fast alle Einzelfragen zur Ausgestaltung der Vorratsdatenspeicherung allein dem Ordnungsgeber überlassen bleiben sollen. Die vorgeschlagene

gesetzliche Verordnungsermächtigung enthält weder Vorgaben für den Zeitraum der Mindestspeicherfrist noch für den genauen Umfang der zu speichernden Daten, was insbesondere für den Bereich der Teledienste problematisch erscheint. Denn nach dem vorliegenden Text erschiene es auch möglich, in einer Verordnung eine Speicherpflicht für einzelne Seitenaufrufe und möglicherweise sogar einzelne E-Mail-Kontakte einzuführen. Die in § 6a Satz 2 z.B. allein enthaltene Vorgabe, dass „die berechtigten Interessen der Diensteanbieter und der Betroffenen“ – ebenso wie die „Erfordernisse effektiver Strafverfolgung und Gefahrenabwehr sowie der effektiven Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden (usw.)...“ – zu berücksichtigen sind, lässt einen nahezu uneingeschränkten Spielraum für den Ordnungsgeber. Das verfassungsrechtliche Wesentlichkeitsgebot würde jedoch erfordern, dass die entscheidenden Festlegungen für den Umfang und die Ausgestaltung des mit der Vorratsdatenspeicherung verbundenen Freiheitseingriffs vom Parlament selbst und damit bereits in der gesetzlichen Ermächtigung getroffen werden.

### ■ Verstoß gegen grundlegende datenschutzrechtliche Prinzipien

Die geplante Einführung einer Vorratsdatenspeicherung greift in erheblichen Maße in das grundgesetzlich nach Art. 2 Abs. 1 GG (und Art. 8 der Europäischen Grundrechtscharta) geschützte Recht auf informationelle Selbstbestimmung ein. BITKOM sieht in der angestrebten Anhäufung von personenbezogenen Daten eine Gefahr für wichtige datenschutzrechtliche Prinzipien. Es wird sowohl das Gebot der Datensparsamkeit und Datenvermeidung missachtet als auch gegen das Verbot der Vorratsdatenhaltung verstoßen.

Grundgedanke der Datensparsamkeit und Datenvermeidung ist, dass den Rechten des Bürgers dann die geringste Gefahr droht, wenn Daten, die möglicherweise in unbefugte Hände gelangen oder zu ungesetzlichen Zwecken verwendet werden könnten, überhaupt nicht erhoben und gespeichert, jedenfalls aber möglichst schnell wieder gelöscht werden. Damit ist möglichen Missbräuchen besser vorzubeugen als mit noch so guten Schutzvorrichtungen. Die Einführung von Mindestspeicherfristen unabhängig von einer betrieblichen Notwendigkeit und eine mögliche Ausweitung der zu erhebenden Daten steht hierzu im eklatanten Widerspruch. Es sollen hier Datensammlungen allein zum Zwecke einer möglichen Auskunftserteilung an staatliche Behörden betrieben werden. Denn die zu sammelnden Daten werden zum Teil überhaupt nicht für den Geschäftsbetrieb der Netzbetreiber benötigt (z.B. die Daten aus den Einbuchungen von Mobiltelefonen ohne Verbindung oder bei Telediensten die Logfiles mit den Informationen über die aufgerufenen Websites); in der Regel werden die Daten aber vor allem nicht für einen derart langen Zeitraum benötigt, wie sie nun aufgrund von Mindestspeicherfristen vorgehalten werden sollen.

Der Umstand, dass die verlangten Datensammlungen für den Betrieb der Anbieter selbst nicht erforderlich sind, lässt die Datensammlung zu einer klassischen Vorratsdatenhaltung werden. Das Bundesverfassungsgericht hat in seinem „Volkszählungsurteil“ (BVerfGE 65, S. 1 ff.) klargestellt, dass das Sammeln personenbezogener Daten nur in Verbindung mit einem bereichsspezifisch und präzise bestimmten Verwendungszweck zulässig, eine Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbareren Zwecken hingegen unzulässig ist. Genau dies ist aber Ziel der geplanten Verordnungsermächtigungen. Der für die Datensammlung im Gesetzestext angegebene Zweck

(„zum Zwecke der Strafverfolgung und der Gefahrenabwehr und für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes“) erscheint viel zu weit, als dass er eine Zweckbindung, wie es das Verfassungsgerichts-Urteil fordert, darstellen könnte. Dies gilt insbesondere, wenn man den Blick auf den einzelnen Datensammlungsvorgang richtet. Die beliebige Speicherung aller Daten von unbescholtenen Bürgern ohne konkreten Anlass geschieht allein unter dem Generalverdacht, dass dann auch – in verschwindend kleinem Anteil – tatsächlich für die verfolgten Zwecke relevante Daten gespeichert werden. Grund für die Datenerhebung ist also nur, dass davon möglicherweise auch Daten von (potentiellen) Straftätern betroffen sein könnten. Mit dieser Vermutung ließe sich letztlich jedoch jegliche Datensammlung rechtfertigen. Bei der überwältigenden Mehrheit aller Kommunikationsverbindungen geht aber schon der Gesetzgeber selbst davon aus, dass für diese Daten nie ein konkreter Bedarf bestehen wird. In diesen Fällen fehlt es also an einem konkret gegebenen Zweck für die Datenspeicherung, so dass der hier verfolgte Ansatz mit den vom Verfassungsgericht gezogenen Grenzen, die gerade den totalen Überwachungsstaat verhindern sollen, nicht zu vereinbaren ist.

#### ■ **Unverhältnismäßigkeit der drohenden Kostenbelastung für die Anbieter-Unternehmen**

Neben den schweren datenschutzrechtlichen Bedenken kritisiert BITKOM vor allem die hohen und gänzlich unverhältnismäßigen Kostenbelastungen der Betreiber durch die sie treffenden Speicherpflichten. Sie werden zur Speicherung der Bestands-, Abrechnungs- und auch darüber hinausgehenden Nutzungsdaten für einen Zeitraum verpflichtet, in dem sie selbst regelmäßig keinen Bedarf mehr an den angefallenen Daten haben. Dies soll damit im alleinigen Interesse der staatlichen Sicherheitsorgane geschehen.

Die reine Speicherung, insbesondere aber auch die Verwaltung der hierbei anfallenden Datenmengen in datenschutzrechtlich einwandfreier Weise bedeutet einen hohen zusätzlichen Aufwand. Die vorhandene Speicherkapazität müsste hierfür – je nach Länge der erst vom Ordnungsgeber festzusetzenden Mindestspeicherfrist – um ein Mehrfaches der jetzigen Kapazitäten erhöht werden. Daneben müssten aber auch ganz neue Programme entwickelt werden, die in der Lage wären, die enormen Datenbestände zu verwalten, um auf diese Weise überhaupt zu einem späteren Zeitpunkt den Zugang zu den Daten eines bestimmten Teilnehmers gewährleisten zu können. Der Aufwand für die Anpassung und Anschaffung der erforderlichen Soft- und Hardware dürfte für größere Unternehmen im Bereich von mehreren Millionen Euro liegen. Angesichts der augenblicklich besonders harten Wettbewerbssituation in der Telekommunikations- und Teledienstbranche könnten diese Kosten auch nicht ohne Weiteres an die Kunden weitergegeben werden und wären somit letztlich von den Anbietern selbst zu tragen.

Daneben stellt die gesetzliche Vorgabe vor allem aber auch kleinere Anbieter und die Betreiber privater Netze vor kaum zu lösende Herausforderungen. Hierunter fallen etwa private Firmennetze, aber auch die Telekommunikationseinrichtungen in Hotels oder Krankenhäusern. Da auch diese Einrichtungen unter die gesetzliche Definition der „geschäftsmäßigen Anbieter von Telekommunikationsdiensten“ (§ 3 Nr. 5 TKG) fallen, wären auch sie verpflich-

tet, die in ihren Netzen angefallenen Verbindungsdaten entsprechend den Vorgaben für eine bestimmte Zeit vorzuhalten. Hierzu sind sie aufgrund ihrer bisherigen Infrastruktur keinesfalls in der Lage. Die nötigen Investitionen könnten gerade von diesen kleinen Anbietern in aller Regel nicht getragen werden. Im Bereich der Teledienste fehlt es sogar gänzlich an einer begrenzenden Regelung, so dass jeder verpflichtet wäre, der selbst Teledienste anbietet oder hierzu den Zugang vermittelt, egal in welchem Umfang oder mit welcher Zielsetzung. Erfasst würden also etwa auch alle Unternehmen – unabhängig von ihrer Größe – die ihren Mitarbeitern eine private Nutzung des Internets (oder entsprechend ihrer Telekommunikationseinrichtungen) erlauben. Die zusätzlichen Belastungen für die gesamte Wirtschaft wären immens.

Diese geschilderte schwerwiegende Kostenbelastung ist umso weniger akzeptabel, als sie allein im Interesse staatlicher Stellen und der diesen obliegenden Sicherungsaufgaben erfolgt. Die Indienstnahme Privater bei gleichzeitiger Auferlegung der Kostenlast lässt sich grundgesetzlich nicht rechtfertigen. Die schon gegen bisherige Verpflichtungen der Anbieter von Telekommunikations- und Telediensten vorgebrachten Argumente greifen bei der stark ansteigenden Kostenbelastung durch die nun geplante Vorratsdatenspeicherung erst recht. Die Voraussetzungen für das Vorliegen einer Sonderabgabe (besondere Sachnähe, Gruppenverantwortung oder Gruppennützigkeit) sind nicht gegeben. Gerade die nun geplante Datenspeicherung geht weit über das für den betrieblichen Ablauf erforderliche Maß hinaus und fände somit allein im Interesse des Staates statt. Dann sollte dies aber auch aus allgemeinen Steuermitteln finanziert werden.

#### ■ Geringer Nutzen der geplanten Maßnahmen

BITKOM bezweifelt insbesondere, ob die genannten hohen Belastungen in einem vernünftigen Verhältnis zu einem möglichen Sicherheitsgewinn infolge der Vorratsdatenspeicherung stehen. Der Verband kann in dieser Maßnahme nur einen geringen Mehrwert bei der Verbrechensbekämpfung erkennen.

Die überwältigende Mehrheit der großen Menge erfasster Daten stammt von unbescholtenen Bürgern. Die eigentliche Zielgruppe der durch die Neuregelung eingeführten Abfragemöglichkeiten, nämlich terroristische Gruppen und die organisierte Kriminalität, können und werden die Maßnahmen auch ohne große Probleme umgehen können. Die Nutzung von Verschlüsselungstechniken, Anonymizern oder Re-Mailing-Systemen erlaubt es, die Spuren einer Internet-Nutzung zu verwischen. Gleiches gilt für die Nutzung öffentlicher Internet-Terminals (Internet-Cafés, Bibliotheken, Universitäten) oder öffentlicher Telekommunikations-Anlagen, bei denen eine Rückführung gespeicherter Nutzungsdaten auf einen bestimmten Nutzer überhaupt nicht möglich ist. Voraussichtlich werden durch die Einführung einer Vorratsdatenspeicherung also höchstens unvorsichtige, mit geringerer krimineller Energie agierende Straftäter überführt werden können. Nur für diesen Bereich erscheinen die geplanten schweren Freiheitseingriffe jedoch nicht verhältnismäßig.

Ein weiteres Problem wird stets bleiben, einen gespeicherten Kommunikationsvorgang einer bestimmten Person zuzuordnen. Denn selbst bei persönlichen Anschlüssen wird gerade im Nachhinein kein Beweis mehr möglich sein, wer zur fraglichen Zeit den Anschluss tatsächlich

genutzt hat. Bei den Verbindungsdaten steht auch anders als bei der Überwachung von Gesprächsinhalten nicht einmal mehr die persönliche Stimme als Anhaltspunkt für eine nachträgliche Zuordnung zur Verfügung. Unter diesen Umständen erscheint es fraglich, ob durch eine Vorratsdatenspeicherung überhaupt für die Strafverfolgung verwertbare Ergebnisse erlangt werden können.

Der Nutzen der Neuregelung für die Sicherheitsorgane steht also in keinem Verhältnis zu dem massiven Eingriff in das Recht auf informationelle Selbstbestimmung des einzelnen betroffenen Bürgers wie auch zu den erheblichen wirtschaftlichen Belastungen, die die Umsetzung der geforderten Maßnahmen für die verpflichteten Unternehmen mit sich brächte.

#### **IV. Artikel 6: Inkrafttreten**

Entgegen der in der Begründung geäußerten Auffassung verursachen die geplanten Änderungen in der StPO einen erheblichen Anpassungsbedarf bei den betroffenen Telekommunikations- und Teledienste-Anbieter. Es erscheint deshalb erforderlich, zumindest entsprechende Übergangsfristen einzuräumen, in denn die technischen und betrieblichen Voraussetzungen für die neuen Verpflichtungen geschaffen werden können.

Berlin, den 12. August 2002