

## Anforderungen der Industrie an die Diskussion über eine europaweit verpflichtende Speicherung von Kommunikationsdaten („Vorratsdatenspeicherung“)

### HINTERGRUND:

Seit gut einem Jahr wird in einer kontrovers geführten Diskussion die Frage erörtert, ob und in welchem Umfang die Telekommunikationsunternehmen und Internetdiensteanbieter verpflichtet werden sollen, Verkehrs- und Standortdaten sowie Teilnehmer- und Nutzerdaten zur Verwendung für die Strafverfolgungsbehörden zu speichern. Unter dem Eindruck der Terroranschläge vom 11. März 2004 in Madrid haben Frankreich, Großbritannien, Irland und Schweden im April 2004 einen gemeinsamen Vorschlag für einen EU-Rahmenbeschluss zur Vorratsspeicherung von Kommunikationsdaten vorgelegt<sup>1</sup>. In der Folge der Bombenanschläge in London vom Juli 2005 haben sich die Justiz- und Innenminister der Europäischen Union nun darauf verständigt, bis Oktober 2005 eine Einigung über die Regelungen zur Speicherung von Kommunikationsdaten und deren Austausch zwischen den Mitgliedstaaten zu erzielen<sup>2</sup>.

Sowohl das Europäische Parlament als auch die Kommission haben neben allgemeinen inhaltlichen Kritikpunkten vor allem an der Regelungskompetenz des Rates (im Rahmen der sog. „Dritten Säule“; auf Grundlage von Artt. 31 Abs. 1 c, 34 Abs.2 b EUV) Zweifel geäußert. Die Europäische Kommission arbeitet derzeit an einem Richtlinienentwurf, welcher sich auf Art. 95 EGV stützen soll. Bislang konnte über die Rechtsgrundlage zwischen den Institutionen noch keine Einigung erreicht werden.

Vor dem Hintergrund der parallelen Diskussion über verschiedene Rechtsakte in unterschiedlichen Legislativverfahren stellt das vorliegende Papier einen Beitrag sowohl für die laufenden Arbeiten im Ministerrat als auch in der Kommission dar.

### GRUNDSATZPOSITION:

Die Industrie unterstützt ausdrücklich das Streben nach sachgerechten Lösungen zur grenzüberschreitenden Bekämpfung der organisierten Kriminalität und des Terrorismus. Innere Sicherheit dient dem Allgemeinwohl und ist damit auch gleichzeitig ein Gewinn für jeden Industriestandort. Seitens der Industrie bestehen aber erhebliche Zweifel, ob der Nutzen der geplanten Regelungen in angemessenem

---

<sup>1</sup> Ratsdokument 8958 / 2004: Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus.

<sup>2</sup> Presseerklärung des JI-Rates vom 13. Juli 2005: [http://ue.eu.int/ueDocs/cms\\_Data/docs/pressData/de/jha/85817.pdf](http://ue.eu.int/ueDocs/cms_Data/docs/pressData/de/jha/85817.pdf) .

Verhältnis zu den Belastungen für die betroffenen Unternehmen und den Eingriffen in die Freiheitsrechte der Bürger steht.

Die Industrie weist darauf hin, dass die Europäische Union sich mit einer Akzeptanzkrise und mit Vertrauensverlust konfrontiert sieht, weil die Politik nicht in der Lage war und ist, den Bürgern und der Industrie den Nutzen der Europäischen Aktivitäten zu erklären. Die Bedenken und das Unbehagen, das sich mit der Vorratsdatenspeicherung verbindet, resultieren auch aus der Tatsache, dass eine sorgfältige und sachgerechte Rechtsfolgenabschätzung fehlt und so der Eindruck entsteht, dass weder die Bedenken der Verbraucher noch die der Industrie ernsthaft berücksichtigt wurden.

Der derzeit in Rat und Kommission diskutierte Umfang geht sowohl hinsichtlich der Datentypen als auch hinsichtlich der Speicherdauer weit über das hinaus, was deutsche Bedarfsträger in Expertengesprächen und in einer „Anforderungsliste“ als für Ermittlungszwecke ausreichend bezeichnet haben. Die Europäische Vereinigung der Polizei (EuroCOP) hat die Entwürfe des Rates sogar mit der Begründung abgelehnt, dass es zu lange dauern würde, die nach den Entwürfen zu erwartenden enormen Datensätze zu durchsuchen, und dass zudem zahlreiche Umgehungsmöglichkeiten die Effektivität einer Vorratsdatenspeicherung insgesamt in Frage stellen (<http://www.enn.ie/news.html?code=9611167>). Eine Studie im Auftrag des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) belegt außerdem, dass Bedarfsträger Daten, die älter als drei Monate sind, nur äußerst selten abfragen ([http://www.bitkom.org/Default\\_28861.aspx](http://www.bitkom.org/Default_28861.aspx)).

Vor diesem Hintergrund muss eine Speicherverpflichtung jedenfalls auf ein Mindestmaß beschränkt sein. Sie darf nicht über solche Datentypen hinausgehen, die bereits jetzt systemseitig erfasst und als Datensatz zur zentralen Verarbeitung zusammengeführt werden. Zudem darf sie eine Speicherfrist von sechs Monaten nicht überschreiten.

Auf jeden Fall müssen die Staaten zu 100 % alle Investitions- und Betriebskosten tragen, die den Unternehmen durch die Umsetzung etwaiger Speicherpflichten entstehen. Schon aus diesem Grund liegt es im Interesse der Staaten selbst, jede vorgeschlagene Regelung hinsichtlich der Speicherdauer, vor allem aber auch hinsichtlich der Datentypen, detailliert daraufhin zu überprüfen, ob sie tatsächlich erforderlich ist oder sich eher als ineffektiver Kostentreiber darstellt.

#### EMPFEHLUNGEN DER INDUSTRIE IM EINZELNEN:

##### 1. Einigung über die Rechtsgrundlage

Unstimmigkeiten zwischen den EU-Institutionen über die Zuständigkeit führen zu Rechtsunsicherheiten bei den Betroffenen und unter Umständen auch zu Fehlinvestitionen. Daher sind die EU-Institutionen – auch mit Blick auf Ihre Glaubwürdigkeit – aufgefordert, ihren Streit über die richtige Rechtsgrundlage zeitnah zu lösen und erst dann auf einer gesicherten Basis die inhaltliche Diskussion fortzusetzen.

## 2. Durchführung einer Rechtsfolgenabschätzung (impact assessment)

Die Kommission hat sich verpflichtet, eine solide „Rechtsfolgenabschätzung“ durchzuführen, bevor sie konkrete Regelungen verabschiedet. Dies ist das einzig verlässliche Mittel, um sowohl die Folgen für die Industrie und die Verbraucher abzuschätzen als auch den Nutzen für die polizeiliche und justizielle Zusammenarbeit zu evaluieren. Diese Vorarbeiten wurden bisher aber nicht durchgeführt; insbesondere haben die Strafverfolgungsbehörden die Notwendigkeit einer Vorratsdatenspeicherung bzw. eine vermeintlich mangelnde Effektivität der gegenwärtigen Auskunft- und Speicherpraxis nach wie vor nicht plausibel dargelegt. Diese Analyse muss dringend nachgeholt werden, wenn das Versprechen nach „besserer Rechtssetzung“ und „Rechtsfolgenabschätzung“ im Bereich der Vorratsdatenspeicherung nicht nur eine Worthülse bleiben soll.

Zu berücksichtigen sind an dieser Stelle auch fundamentale Grundrechtsvorgaben der Mitgliedstaaten. In Deutschland setzt die Rechtsprechung des Bundesverfassungsgerichtes einer pauschalen Vorratsdatenspeicherung Grenzen. Erst jüngst hat das höchste deutsche Gericht die herausragende Bedeutung des Fernmeldegeheimnisses sowie des Rechts auf informationelle Selbstbestimmung hervorgehoben und klargestellt, dass diese Bürgerrechte nur unter sehr engen Voraussetzungen eingeschränkt werden dürfen<sup>3</sup>.

## 3. Persönlicher Anwendungsbereich (Verpflichteter): Beschränkung auf den jeweiligen Diensteanbieter

Die Vorschläge müssen explizit klarstellen, dass eine Speicherpflicht nur dem Unternehmen auferlegt werden kann und darf, das den jeweiligen Dienst anbietet. Nur dieses Unternehmen hat die konkrete Nutzerbeziehung und damit die Berechtigung und Hoheitsgewalt hinsichtlich der zu speichernden Daten. Daher sind Forderungen, Informationen über den Empfänger von Daten bzw. über den Angerufenen bereitzustellen, vom Diensteanbieter des Versenders bzw. des Anrufenden in der Regel nicht umsetzbar und müssen aus den Vorschlägen gestrichen werden.

## 4. Sachlicher Anwendungsbereich (Datentypen): Beschränkung auf ein Mindestmaß

Die Einführung einer Pflicht zu umfassender Datenspeicherung kann insbesondere bei bestimmten Datentypen, die bislang nicht gespeichert werden (dürfen) und daher erst gar nicht erhoben werden, aufgrund der dazu erforderlichen aufwändigen technischen Netzaufrüstungen zu enormen Investitions- und Betriebskosten führen. Insoweit ist eine klare Einschränkung notwendig. Nur ein eng umgrenzter Anwendungsbereich kann zu einer angemessenen und sachgerechten Lösung führen. Maßstab hierfür muss der tatsächliche, durch die Mitgliedstaaten ermittelte und konkret nachgewiesene Bedarf der Sicherheitsbehörden sein.

Rat und Kommission haben betont, dass nur solche Daten gespeichert werden sollen, die ohne zusätzlichen Aufwand erfasst werden können. Offenbar soll es nur darum gehen, bereits systemseitig erfasste Daten länger „festzuhalten“, damit der Aufwand für die Unternehmen überschaubar bleibt. Diesem Ansatz werden die in Rat und Kommission diskutierten Datentypen aber nicht gerecht. Viele der Datentypen werden in den Netzen derzeit nicht aufgezeichnet und erst recht nicht verarbeitet, z. B. weil sie nicht abrechnungsrelevant oder für die Erbringung des Dienstes nicht

---

<sup>3</sup> BVerfG, 1 BvR 668/04 vom 27.7.2005.

erforderlich sind und ihre Speicherung daher nach derzeitigem Datenschutzrecht verboten ist. Somit geht es hier nicht darum, bereits erfasste Daten länger „festzuhalten“, sondern es bedürfte umfangreicher Aufrüstungen der Hard- und Software, um diese Daten überhaupt erst im Netz zu generieren und verfügbar zu machen.

Die deutsche Industrie spricht sich daher für folgende Einschränkungen aus. Auch Expertengespräche mit deutschen Bedarfsträgern haben ergeben, dass die deutschen Bedarfsträger die im Folgenden genannten Datentypen für eine effektive Straftatenverhütung und –verfolgung nicht für erforderlich halten (siehe die in der Ratsarbeitsgruppe vorgelegte deutsche „Anforderungsliste“):

#### Für alle Kommunikationsbereiche:

- Keine Speicherung nicht erfolgreicher Verbindungsversuche

Begründung: Die Speicherung dieser – nicht abrechnungsrelevanten – Daten ist nach derzeitigem Datenschutzrecht verboten. Die Daten werden daher im Netz überhaupt nicht aufgezeichnet und verarbeitet. Um die Daten im Netz verfügbar zu machen, müssten die Unternehmen sämtliche Vermittlungsstellen grundlegend umrüsten. Investitionskosten der Industrie im dreistelligen Millionenbereich allein für diesen Datentyp wären die Folge. Die Bedarfsträger konnten die Notwendigkeit dieser Informationen angesichts dieser erheblichen Aufwendungen der Industrie bisher nicht darlegen.

- Keine Speicherung der genutzten Kommunikationsart (z. B. Sprache, Fax etc.)

Begründung: Diese Information wird im Netz nur dort erfasst, wo sie abrechnungsrelevant ist (z. B. bei SMS). In den meisten Fällen (z. B. ob eine Verbindung für Sprache oder Faxübertragung genutzt wurde) sind die Daten im Netz überhaupt nicht vorhanden. Auch hier wären umfangreiche Aufrüstungen erforderlich, um die Daten überhaupt im Netz verfügbar zu machen.

#### Im Mobilfunkbereich:

- Keine Speicherung der Funkzellen(Cell-)ID während und am Ende eines Gespräches

Begründung: Auch diese – nicht abrechnungsrelevanten – Daten werden derzeit vom Netz überhaupt nicht aufgezeichnet und verarbeitet. Ihre Erfassung wäre erst nach immensen technischen Aufrüstungen möglich. Einen entsprechenden Mehrwert haben die Bedarfsträger nicht nachgewiesen, denn auch mit der Speicherung der Cell-ID lediglich zu Beginn eines jeden Gespräches lässt sich ein Bewegungsprofil erstellen. Dabei ist es auch nicht gerechtfertigt, die Unternehmen dazu zu verpflichten, mit jedem Datensatz ein „Data Mapping“, also eine nähere räumliche Beschreibung der Funkzelle, bereitzustellen. Vielmehr ist es völlig ausreichend, wenn die Bedarfsträger diese Information einer vorab übermittelten Liste entnehmen können.

- Keine Speicherung der IMEI (Gerätenummer)

Begründung: Der Mehrwert einer IMEI-Speicherung neben der Rufnummer zur klaren Identifizierung eines Teilnehmers ist fraglich und nicht belegt. Aus diesem Grund sind auch die deutschen Bedarfsträger in den Expertengesprächen davon abgerückt, eine verbindliche Speicherung der IMEI zu fordern.

### Im Internetbereich:

- Keine Speicherung der Verbindungsdaten der genutzten Internet-Dienste  
Begründung: Die Verbindungsdaten der genutzten Internet-Dienste (z. B.: Wer hat wessen Internetseite aufgerufen oder wem eine E-Mail geschickt?) sind für die meisten Dienste nicht verfügbar. Technische Voraussetzungen für ihre Erfassung, Speicherung und Auswertung müssten erst geschaffen werden und hätten einen unvorstellbaren Anstieg des zu speichernden Datenvolumens zur Folge. Dies gilt selbst bei einer Einschränkung auf die beiden Dienste E-Mail und Voice over IP (Sprachübermittlung über das Internet).

Eine Speicherung der aufgerufenen Internetseiten birgt das zusätzliche Problem, dass sie einer Inhaltsüberwachung gleichkommt, denn man erfährt daraus, welchen Inhalt sich der Nutzer angesehen hat. Dies widerspricht der ausdrücklichen Erklärung der EU-Organe, eine Inhaltsüberwachung ausschließen zu wollen.

Da die Bedarfsträger zudem bisher immer unterstrichen haben, dass die Internet-Zugangsdaten (wer wann mit welcher IP-Adresse am Internetverkehr teilnahm) die wichtigsten ermittlungsrelevanten Informationsquellen darstellen, sollte eine Datenliste aus all diesen Gründen auch auf diesen Datentyp beschränkt bleiben.

- Keine Speicherung der MAC oder einer anderen Gerätenummer  
Begründung: Die Gerätenummer der Netzwerkkarte eines Rechners (MAC) wird, im Gegensatz etwa zu einer IP-Adresse, an den Diensteanbieter überhaupt nicht übertragen. Wollte man dies ändern, müsste man die Internet-Protokolle reformieren und die gesamte Infrastruktur entsprechend aufrüsten. Der Mehrwert einer MAC neben einer IP-Adresse zur klaren Identifizierung eines Teilnehmers ist dabei fraglich und von den Sicherheitsbehörden nicht belegt.

#### 5. Keine Speicherfrist über sechs Monate

Ein an den Erfordernissen der Bedarfsträger orientierter und bezüglich der Kosten angemessener Rechtsrahmen verlangt eine restriktive Regelung der Speicherfristen. Gezielte Untersuchungen in diesem Bereich (siehe die oben erwähnte Studie, erhältlich unter [http://www.bitkom.org/Default\\_28861.aspx](http://www.bitkom.org/Default_28861.aspx)) haben ergeben, dass keine Speicherzeiten von über sechs Monaten notwendig sind. Eine darüber hinausgehende Speicherdauer wäre deshalb klar unverhältnismäßig.

#### 6. Umfassende Kostentragung durch Staaten erforderlich

Sicherheitspolitik ist eine originäre Staatsaufgabe, die der Staat grundsätzlich aus den Mitteln des öffentlichen Haushaltes zu bestreiten hat. Deshalb muss der Staat auch die Kosten einer Vorratsdatenspeicherung tragen. Eine gesetzliche Regelung auf EU-Ebene muss daher die Mitgliedstaaten verpflichten, die Unternehmen für ihre Aufwendungen zu entschädigen. Dabei reicht auch die Aufforderung nach einer „angemessenen“ Entschädigung nicht aus. Vielmehr bedarf es einer eindeutigen Formulierung, die ausdrücklich eine vollständige, hundertprozentige Erstattung sowohl der Investitions- als auch Betriebskosten vorschreibt. Unzureichende und uneinheitliche Entschädigungsregimes innerhalb der EU würden sonst zu Wettbewerbsverzerrungen führen, langfristig

tragfähige Wettbewerbsstrukturen gefährden und die Schaffung eines einheitlichen europäischen Binnenmarktes verhindern. Dies gilt umso mehr, als einige Mitgliedstaaten weit reichende Kosten-erstattungen etabliert oder angekündigt haben, andere hingegen nicht.

7. Unternehmen nicht zusätzlich mit Erstellung von Statistiken belasten

Eine mögliche Datenspeicherungspflicht würde die betroffenen Unternehmen auch bei Vornahme der notwendigen – oben beschriebenen – Einschränkungen bereits erheblich belasten. Die Unternehmen müssten zahlreiche betriebliche Abläufe anpassen, was mit erheblichen Investitionen und jährlichen Betriebskosten verbunden wäre. Zusätzliche Verpflichtungen – wie etwa die ebenfalls diskutierte Pflicht, Statistiken über Auskunftersuchen zu führen – darf es daher nicht geben. Solche und ähnliche Aufgaben können von den zuständigen Stellen (Strafverfolgungsbehörden) ebenso gut vorgenommen werden. Nur diese können ohnehin auch darlegen, in wie vielen Fällen die Anfragen tatsächlich zu einem Ermittlungserfolg geführt haben; diese Information ist notwendig, um die Effektivität einer möglichen Speicherungspflicht beurteilen können. Hier fehlt es an jeglicher Rechtfertigung dafür, Private zur Wahrnehmung staatlicher Aufgaben heranzuziehen.

Eine nachträgliche Überprüfung kann schließlich auch nur bedingt Fehleinschätzungen im Hinblick auf Effektivität und damit Verhältnismäßigkeit einer möglichen Datenspeicherungspflicht korrigieren, denn die Anfangsinvestitionen sind zu diesem Zeitpunkt bereits getätigt.

Berlin, 4. August 2005

Ansprechpartner:

Bundesverband der Deutschen Industrie e.V. (BDI)  
Christiane Eichele, Abteilung Energiepolitik / Telekommunikationspolitik  
Breite Straße 29, 10178 Berlin  
Tel.: +49 - 30 - 2028 1419  
Fax: +49 - 30 - 2028 2419  
E-Mail: C.Eichele@bdi-online.de

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM)  
Dr. Volker Kitz LL.M. (NYU), Bereichsleiter Telekommunikations- und Medienpolitik  
Albrechtstraße 10, 10117 Berlin  
Tel.: +49 - 30 - 27576 221  
Fax: +49 - 30 - 27576 222  
E-Mail: V.Kitz@bitkom.org

Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e.V. (VATM)  
Harald Geywitz, Leiter Büro Berlin  
Albrechtstraße 12, 10117 Berlin  
Tel.: +49 - 30 - 50 56 15 38  
Fax: +49 - 30 - 50 56 15 39  
E-Mail: berlin@vatm.de