# Ende des Datenschutzes bei der Kommunikation?

## Vorratsspeicherung von Nutzungs- und Verbindungsdaten geplant

*Rainer W. Gerling, Fürstenfeldbruck*

**Artikel 10 Abs. 1 GG: Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.**

## 1 Vorgeschichte

Das Land Niedersachsen brachte in der 775. Sitzung des Bundesrates vom 26.04.2002 einen „Entwurf eines Gesetzes zur Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Missbrauchs von Kindern und der Vollstreckung freiheitsentziehender Sanktionen“ (BT-Drs. 275/02[1]) ein. Der Entwurf wurde federführend an den Rechtsausschuss verwiesen und stand dann erneut auf der Tagesordnung der 776. Sitzung am 31.5.2002. Der Rechtsausschuss empfahl, mit Änderungen den Gesetzentwurf in den Bundestag einzubringen (BT-Drs. 275/1/02[2]). Der Bundesrat stimmte dieser Empfehlung zu[3].

Damit ist abermals ein Gesetzgebungsverfahren in Gang gekommen, das die eigentlichen Maßnahmen hinter einem unverfänglichen Titel verbirgt. Erinnerungen an die Änderungen im Sozialgesetzbuch X durch den Artikel 4 des „1. Gesetzes zur Änderung des Medizinproduktegesetzes“ vom 6. August 1998[4] werden wach. Unter diesem unverfänglichen Titel wurde damals § 68 Abs. 1. Satz 1 des SGB X neu gefasst und Übermittlungsregeln an Strafverfolgungsbehörden eingeführt. Der aktuelle Gesetzentwurf bringt (obwohl der Titel es nicht sofort vermuten lässt) die Vorratsspeicherung von Verbindungsdaten im Telekommunikationsbereich bzw. der Bestands-, Nutzungs- und Abrechnungsdaten im Teledienstebereich.

In der Begründung heißt es u.a.: *„Der Zugriff auf Telekommunikationsverbindungsdaten läuft praktisch leer, wenn diese bereits gelöscht sind. Erforderlich sind daher Regelungen für eine Vorratsspeicherung dieser Daten, wie sie in § 100g Abs. 1 Satz 3 Halbsatz 2 StPO sowie in Artikel 1a und 1b vorgeschlagen werden. ... Es müssen Regelungen geschaffen werden, wonach die Unternehmen im Einzelfall verpflichtet werden können, Telekommunikationsverbindungsdaten für Strafverfolgungszwecke aufzuzeichnen. „*

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein meint dazu in einer ersten Stellungnahme[5]: *„Die Verfechter des Gesetzesvorschlages scheuen sich nicht einmal, ihr Vorhaben ausdrücklich als “Vorratsspeicherung” zu bezeichnen. In der Rechtsprechung des Bundesverfassungsgerichts steht die “Vorratsspeicherung” seit fast 20 Jahren als Synonym für eine verfassungswidrige staatliche Sammelwut, bei der Daten, die vielleicht irgendeinmal für staatliche Zwecke nützlich sein könnten, gespeichert werden.“*

## 2 Änderungen der StPO

Die zeitliche Befristung der §§ 100g und 100h der StPO bis zum 31. Dezember 2004 soll aufgehoben werden. Außerdem wird im § 100g Abs. 1 Satz 1 der Verweis auf § 100a Satz 1 StPO gestrichen. *„Der Anwendungsbereich der Ermittlungs- und Fahndungsmöglichkeiten darf nicht dadurch eingeengt werden, dass auf den Straftatenkatalog in § 100a StPO Bezug genommen wird, da die nach § 100g StPO mögliche Nutzung von Verbindungs- und Standortdaten mit einem deutlich geringeren Eingriff in das Fernmeldegeheimnis verbunden ist als die Überwachung und Aufzeichnung des Inhalts der Telekommunikation nach § 100a StPO.“* heißt es in der Begründung. Die derzeitige Fassung des § 100g StPO beschränkt die Auskunft über Telekommunikationsverbindungsdaten auf Straftaten von erheblicher Bedeutung, insbesondere auf die in § 100a Satz 1 StPO genannten Straftaten. § 100a regelt dagegen die Überwachung und Aufzeichnung (Abhören) der Telekommunikation. Die Auskunft über Telekommunikationsverbindungsdaten soll allgemeiner eingesetzt werden können, als das Abhören von Telekommunikation.

Darüber hinaus sollen die Telekommunikationsdaten nicht nur unverzüglich sondern auch unentgeltlich zur Verfügung gestellt werden.

Außerdem soll der Einsatz von IMSI-Catchern[6] erleichtert werden.

## 3 Änderung des TKG

Der § 89 Abs. 1 des Telekommunikationsgesetzes soll die folgende Fas-

**INHALT:**



[1] http://www.parlamentsspiegel.de (Zum Redaktionsschluss galt leider: Aus technischen Gründen ist der Zugriff auf die Parlamentspapiere zur Zeit nicht möglich!)

[2] http://www.dud.de/dud/documents/ermittlungsg-e-020515.pdf

[3] http://www.bundesrat.de/pr/ pr118_02.html

[4] BGBl I. S. 2005

[5] http://www.datenschutzzentrum.de/material/themen/presse/kommunik.htm

[6] D.Fox, Gateway: IMSI-Catcher DuD 21, 539 (1997); überarbeitete Fassung http://www.datenschutz-und-datensicherheit.de/jhrg21/imsicatc.htm.

sung (Einfügungen sind unterstrichen) erhalten:

**§ 89 Datenschutz, Vorratsspeicherung**

(1) Die Bundesregierung erläßt für Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, durch Rechtsverordnung mit Zustimmung des Bundesrates Vorschriften zum Schutze personenbezogener Daten der an der Telekommunikation Beteiligten, welche die Erhebung, Verarbeitung und Nutzung dieser Daten regeln, sowie Vorschriften zur Vorratsspeicherung für 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. Die Vorschriften haben dem Grundsatz der Verhältnismäßigkeit, insbesondere der Beschränkung der Erhebung, Verarbeitung und Nutzung auf das Erforderliche, sowie dem Grundsatz der Zweckbindung Rechnung zu tragen. Dabei sind Mindest- und Höchstfristen für die Speicherung festzulegen und insgesamt die berechtigten Interessen des jeweiligen Unternehmens und der Betroffenen sowie die Erfordernisse effektiver Strafverfolgung und Gefahrenabwehr sowie der effektiven Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes zu berücksichtigen. Einzelangaben über juristische Personen, die dem Fernmeldegeheimnis unterliegen, stehen den personenbezogenen Daten gleich.

Hier soll die Exekutive ermächtigt werden über eine Verordnung (mit Zustimmung des Bundesrates) Mindestspeicherfristen festzulegen. Damit entfällt für diesen schweren Grundrechtseingriff der Parlamentsvorbehalt. Außerdem ist die Ermächtigung nahezu allumfassend; so sollen neben effektiver Strafverfolgung und Gefahrenabwehr auch die gesetzlichen Aufgaben des Verfassungsschutzes, des BND, des MAD und des Zollkriminalamtes als Begründung ausreichen.

Obwohl keine Mindestspeicherfrist genannt wird, darf wohl von mindestens sechs Monaten ausgegangen werden. Die entstehenden Datenberge werden erhebliche Kosten verursachen.

Es muss auch die Frage erlaubt sein, was mit diesen Daten auswertetechnisch geschehen soll. Eine der Lehren des 11. September ist sicherlich auch, dass umfangreiches Datenmaterial allein keinen Ermittlungserfolg garantiert. Die Daten müssen nach vorgegebenen Kriterien ausgewertet und in den richtigen Zusammenhang gestellt werden. Das hierzu notwendige Personal und Computerequipment ist bei staatlichen Stellen wohl eher nicht vorhanden, und in Zeiten von Haushaltsknappheit auch nicht einfach aufbaubar.

## 4 Änderung des TDDSG

In das gerade erst novellierte Teledienstedatenschutzgesetz[7] soll der folgende § 6a eingefügt werden:

**§ 6a Vorratsspeicherung**

Die Bundesregierung erlässt für Diensteanbieter durch Rechtsverordnung mit Zustimmung des Bundesrates Vorschriften zur Vorratsspeicherung für die 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. Dabei sind Mindestfristen für die Speicherung von Bestands-, Nutzungs- und Abrechnungsdaten festzulegen und insgesamt die berechtigten Interessen der Diensteanbieter, der Betroffenen und die Erfordernisse effektiver Strafverfolgung und Gefahrenabwehr sowie der effektiven Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes zu berücksichtigen.

Die Mindestspeicherfristen für Nutzungsdaten treten auch hier eine gewaltige Speicherlawine los: alle Abrufe von Web-Seiten, alle Nutzungen eines Proxies müssen dann gespeichert werden. Damit würde in Deutschland die Internetnutzung für staatliche Stellen transparent und nachvollziehbar. Datensparsamkeit und Datenvermeidung stehen dann nur noch als Lippenbekenntnis im BDSG, im Internet gelten diese Prinzipien dann nicht mehr. Der Verwendungszweck ist mit der gleichen Formulierung wie im TKG-E soweit gefasst, das nahezu alles darunter fällt.

## 5 Speicheranordnung im WpHG

Dem Wertpapierhandelsgesetz kommt die zweifelhafte Ehre zu, als erstes Gesetz neue Vorschriften zur Speicherung von Verbindungsdaten zum Zwecke der Strafverfolgung zu haben, nachdem der Bundesrat am 31.5.2002 dem Vierten Finanzmarktförderungsgesetz zugestimmt hat[8] und es damit in Kraft treten kann. In das Wertpapierhandelsgesetz (WpHG) soll zur Durchsetzung der Verbote der Insidergeschäfte und der Kurs- und Marktpreismanipulation durch Einfügung des § 16b von einem Unternehmen die Aufbewahrung von Verbindungsdaten über den Zeitpunkt der Abrechnung hinaus verlangt werden können. Bizer meint dazu[9]: *„Die Speicheranordnung ist gegenüber der Mindestspeicherpflicht ein milderes Mittel, weil auf eine flächendeckende Vorhaltung von Verbindungsdaten verzichtet wird und sich die verlängerte Speicherung auf anlassbezogene Einzelfälle beschränkt."*

**§ 16b Aufbewahrung von Verbindungsdaten**

(1) Hat die Bundesanstalt Anhaltspunkte für einen Verstoß gegen § 14 oder § 20a, kann sie von den Wertpapierdienstleistungsunternehmen sowie von Unternehmen, die an einer inländischen Börse zur Teilnahme am Handel zugelassen sind, und von Emittenten von Insiderpapieren sowie von mit diesen verbundenen Unternehmen, die ihren Sitz im Inland haben oder deren Wertpapiere an einer inländischen Börse zum Handel zugelassen sind, die Aufbewahrung von Verbindungsdaten der Teilnehmer an der Telekommunikation verlangen.

(2) Die Frist zur Aufbewahrung beträgt vom Tage des Zugangs der Aufforderung an höchstens sechs Monate. Ist die Aufbewahrung zur Prüfung der Anhaltspunkte eines Verstoßes gegen ein Verbot nach § 14 oder § 20a nicht mehr erforderlich, hat die Bundesanstalt den Aufbewahrungspflichtigen hiervon unverzüglich in Kenntnis zu setzen und ihm mitzuteilen, dass eine Aufbewahrungspflicht nicht mehr besteht.

[7] Elektronischer Geschäftsverkehr Gesetz vom 14 Dezember 2001. BGBl I, 3721

[8] http://www.bundesrat.de/pr/pr97_02.html

[9] J. Bizer, Speicheranordnung für Verbindungsdaten DuD, 26, 363 (2002).

## 6 Fazit

Nachdem die Gesetzesinitiative des Bundesrates weitgehend unbemerkt geschehen konnte, sind nun alle aufgefordert ihren Einfluss geltend zu machen, um dieses Gesetzesvorhaben zu verhindern. Nach Art. 76 Abs. 3 Grundgesetz muss die Bundesregierung diesen Gesetzesvorschlag zusammen mit einer Stellungnahme binnen sechs Wochen an den Bundestag weiter leiten. Mit einer abschließenden Behandlung des Vorschlages im Bundestag vor der Sommerpause ist allerdings nicht mehr zu rechnen. Für Unternehmen (insbesondere natürlich Telekommunikationsdienstleister) dürften durch die Mindestspeicherfristen und durch die Zugriffstechnik für die Bedarfsträger erhebliche Kosten entstehen, zumal der Staat für sich in Anspruch nimmt, die Verbindungsdaten unentgeltlich zu erhalten.

Während über Tariftreuegesetz und Verbraucherinformationsgesetz ausführlich berichtet wurde, haben Tagespresse und Fernsehnachrichten dieses viel brisantere Thema offensichtlich nicht beachtet. □

# Akkreditierte Prüfstellen für das Datenschutz-Gütesiegel

Das schleswig-holsteinische Datenschutzrecht bietet Herstellern und Vertriebsfirmen von IT-Produkten – die zur Nutzung durch die Verwaltung des Bundeslandes geeignet sind – die Möglichkeit, ihr Produkt mit einem Gütesiegel auszeichnen zu lassen. Dadurch wird vom Unabhängigen Landeszentrum für Datenschutz (ULD) bestätigt, dass die Produkte mit den Vorschriften über den Datenschutz und die Datensicherheit im Einklang stehen. Nach dem Landesdatenschutzgesetz sollen Behörden vorrangig Produkte mit einem derartigen Gütesiegel einsetzen. Das Gütesiegel kann aber auch ein verlässliches Auswahlkriterium für die private Wirtschaft sein und den dort tätigen Datenschutzbeauftragten die Arbeit erleichtern.

Interessierte Hersteller und Vertriebsfirmen können jetzt unter sieben anerkannten Prüfstellen aus dem gesamten Bundesgebiet auswählen und einen privaten Begutachtungsvertrag abschließen. Die erfolgreiche Begutachtung ist Voraussetzung für die Erteilung des Gütesiegels. Das Siegel selbst wird vom ULD (als eine Körperschaft des öffentlichen Rechts) auf Antrag erteilt, nachdem das Gutachten auf Schlüssigkeit und Nachvollziehbarkeit geprüft wurde. □



Weitere Informationen:

*www.datenschutzzentrum.de/guetesiegel/*