

## **4. Internet, Telekommunikation, Teledienst**

### **4.1 Terrabyte von Telefondaten sollen auf Vorrat gespeichert werden**

Im letzten Jahresbericht hatte ich über die Verabschiedung der Richtlinie zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten (RL 2006/24/EG) und meine datenschutzrechtlichen und verfassungsrechtlichen Bedenken berichtet (vgl. 28. JB, Ziff. 3.2). Die Richtlinie ist am 3. Mai 2006 in Kraft getreten. Noch im Mai 2006 haben die Länder Irland und Slowakei Klage vor dem Europäischen Gerichtshof in Luxemburg gegen die Richtlinie erhoben. Sie sind der Auffassung, dass die Regelung nur in einem so genannten Rahmenbeschluss, nicht aber in einer Richtlinie hätte getroffen werden können. Eine Entscheidung des Europäischen Gerichtshofs steht noch aus und wird wohl erst nach Ablauf der Umsetzungsfrist in nationales Recht am 15. September 2007 ergehen. Auch nach einem Gutachten des wissenschaftlichen Dienstes des Deutschen Bundestages bestehen erhebliche Bedenken, ob die Richtlinie mit dem Europarecht und den dort verankerten Grundrechten vereinbar ist.

Das Bundesministerium der Justiz hat Ende November 2006 einen Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vorgelegt. Die Speicherungspflicht für Verkehrsdaten, die den Telekommunikationsunternehmen ohne Kostenerstattung auferlegt wird, wird durch die neuen §§ 110 a und 110 b Telekommunikationsgesetz (E-TKG) geregelt.

Nach § 110 a E-TKG soll eine Speicherung nur für die von der Richtlinie vorgegebene Mindestdauer von sechs Monaten erfolgen. Gespeichert werden sollen die Rufnummern des Anrufers und Angerufenen, Beginn und Ende der Verbindung, der genutzte Dienst, sowie zusätzlich bei Mobilfunkgeräten die Kennungen der Mobilfunkkarten bzw. des anrufenden oder angerufenen Endgeräts und die Funkzelle, bei Internettelefonie zusätzlich die Internetprotokoll-Adressen. Bei elektronischer Internetkommunikation (Web, E-Mail) sollen die Adresse von Empfänger und Absender, die Internetprotokoll-Adressen und Beginn und Ende der Nutzung des Dienstes gespeichert werden, bei Internetzugangsdiensten eine eindeutige Kennung des Anschlusses, über den die Internetnutzung läuft, Beginn und Ende der Internetnutzung und die zugewiesene Internetprotokoll-Adresse. Zu speichern sind auch Anrufversuche. Daten, die Aufschluss über den Inhalt der Kommunikation geben, dürfen nicht gespeichert werden.

Die Verwendung der gespeicherten Daten beschränkt § 110 b Abs. 1 Satz 1 E-TKG derzeit auf die Verfolgung von Straftaten. Eine Ausweitung auf Zwecke der Gefahrenabwehr oder andere Zwecke im Laufe des Gesetzgebungsverfahrens ist damit nicht ausgeschlossen. Obwohl weiterhin grundsätzlich verfassungsrechtliche Bedenken bestehen, werde ich mich im Arbeitskreis Justiz der Landesbeauftragten für den Datenschutz des Bundes und der Länder mit dem Referentenentwurf näher auseinandersetzen.

## **4.2 Urteil des Bundesverfassungsgerichts zum IMSI-Catcher**

Mit Beschluss vom 22. August 2006 (2 BvR 1345/03) hat das Bundesverfassungsgericht die Ermittlung der Gerätenummer eines Mobilfunkgeräts (IMEI: International Mobile Equipment Identity) und Kartenummer einer SIM-Karte (IMSI: International Mobile Subscriber Identity) sowie des Standorts von Mobiltelefonen durch den so genannten IMSI-Catcher nach § 100 i StPO für verfassungsgemäß erklärt.

Grundlage des IMSI-Catcher ist, dass jedes Mobiltelefon wie auch jede SIM-Karte mit einer weltweit nur einmal vergebenen Nummer versehen ist, über die der Mobilfunkteilnehmer ermittelt werden kann. Voraussetzung für den Einsatz der technischen Anlage eines so genannten IMSI-Catcher ist die ungefähre Kenntnis des Standorts des gesuchten Mobiltelefons. Der IMSI-Catcher macht sich zunutze, dass sich alle Mobiltelefone im empfangsbereiten Zustand in kurzen Abständen bei der für sie gerade "zuständigen" Basisstation des Mobilfunknetzes anmelden. Das gesamte Mobilfunknetz ist entsprechend einem Raster in einzelne Zellen aufgeteilt. Im Rahmen dieser ständigen Positionsangabe werden unter anderem die IMSI und die IMEI an die Basisstation gesendet. Die Erfassung der IMSI und IMEI erfolgt dadurch, dass innerhalb einer solchen Funkzelle der IMSI-Catcher die Basisstation des Mobilfunknetzes simuliert. Sämtliche eingeschalteten Mobiltelefone, die sich im Einzugsbereich des IMSI-Catcher befinden, senden nunmehr ihre Daten an diesen. Durch eine verstärkte Sendeleistung des IMSI-Catcher ist diese simulierte Funkzelle erheblich kleiner als die reguläre Funkzelle. Befinden sich in der simulierten Funkzelle mehrere Mobilfunkteilnehmer, sind zur Bestimmung des gesuchten Mobiltelefons mehrere Messungen erforderlich. Dabei werden an verschiedenen Orten Messungen durchgeführt und nach einem statistischen Auswerteprozess in Form von Schnittmengen die jeweiligen IMSI/IMEI ermittelt oder zumindest eingegrenzt. Auf diese Weise lässt sich der Standort des gesuchten Gerätes sehr genau ermitteln.

Das Bundesverfassungsgericht hat festgehalten, dass die Erhebung dieser Daten nicht unter den Schutz des Fernmeldegeheimnisses (Art. 10 GG) fällt. Die Feststellung einer Geräte- oder Kartenummer eines im Bereich einer simulierten Funkzelle befindlichen Mobiltelefons durch den Einsatz eines IMSI-Catcher ist unabhängig von einem tatsächlich stattfindenden oder zumindest versuchten Kommunikationsvorgang zwischen Menschen. Es fehlt an einem menschlich veranlassten Informationsaustausch, der sich auf Kommunikationsinhalte bezieht. Es "kommunizieren" ausschließlich technische Geräte miteinander. Die bloße technische Eignung eines Mobilfunkgeräts, als Kommunikationsmittel zu dienen sowie die von dem Gerät ausgehenden technischen Signale zur Gewährleistung der Kommunikationsbereitschaft stellen noch keine Kommunikation dar. Das Bundesverfassungsgericht prüfte und bejahte zwar auch einen Eingriff in das Recht auf informationelle Selbstbestimmung, sah diesen Eingriff jedoch durch die gesetzliche Regelung in § 100 i StPO als gerechtfertigt an und verneinte insbesondere einen unverhältnismäßigen Eingriff.

### **4.3 Urteil des Bundesverfassungsgerichts zur Handy- und PC Überwachung**

Das Bundesverfassungsgericht hat mit Urteil vom 2. März 2006 (2 BvR 2099/04) das Recht auf informationelle Selbstbestimmung gestärkt. Dem Verfahren lag die Verfassungsbeschwerde einer Richterin zugrunde, deren Wohnung wegen des Verdachts der Verletzung von Dienstgeheimnissen durchsucht worden war. Dabei war u. a. auf die auf ihrem Computer gespeicherten Daten sowie den Einzelverbindungs nachweis ihres Mobilfunktelefons zugegriffen worden. Die Durchsuchung erbrachte keine strafrechtlich verwertbaren Anhaltspunkte.

Das Verfassungsgericht hielt fest, dass die im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Telekommunikationsverbindungsdaten nach Abschluss des Übertragungsvorgangs nicht mehr durch das Fernmeldegeheimnis (Art 10 Abs. 1 GG) geschützt sind. Denn anders als bei dem Kommunikationsprozess, bei dem der Teilnehmer keinen Einfluss auf die Entstehung oder Speicherung der Verbindungsdaten durch Nachrichtenermittler besitzt, kann der Teilnehmer nach Abschluss des Vorgangs den Zugriff auf die sich in seiner Sphäre befindlichen Daten durch vielfältige technische Vorkehrungen verhindern.

Die in der Herrschaftssphäre des Teilnehmers gespeicherten personenbezogenen Verbindungsdaten unterliegen jedoch dem Schutz durch das Recht auf informationelle Selbstbestimmung (Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG) und gegebenenfalls durch das Recht auf Unverletzlichkeit der Wohnung (Artikel 13 Abs. 1 GG). Ein Eingriff bedarf danach jeweils im konkreten Fall einer Rechtfertigung nach dem Grundsatz der Verhältnismäßigkeit. Die Verhältnismäßigkeitsprüfung muss dem Umstand Rechnung tragen, dass es sich um Daten handelt, die außerhalb der Sphäre des Betroffenen unter dem besonderen Schutz des Fernmeldegeheimnisses stehen und denen im Herrschaftsbereich des Betroffenen ein ergänzender Schutz durch das Recht auf informationelle Selbstbestimmung zuteil wird. Der Maßnahme können im Einzelfall daher die Geringfügigkeit der zu ermittelnden Straftat, eine geringe Beweisbedeutung sowie die Unbestimmtheit des Auffindungsverdachts entgegenstehen. Die Durchsuchungsanordnung muss zudem auf den tatsächlich erforderlichen Umfang begrenzt werden, etwa durch eine zeitliche Eingrenzung oder die Beschränkung auf bestimmte Kommunikationsmittel.