Dr. Jürgen-Peter Graf
Richter am Bundesgerichtshof

76133 Karlsruhe
Herrenstraße 45a
Telefon: 0721-159-0
www.internet-strafrecht.de

Stellungnahme zur öffentlichen Anhörung
des Rechtsausschusses des Deutschen Bundestages
am 21. September 2007 in Berlin

zum Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG
(BT-Drs. 16/5846)

Regelung der Vorratsdatenspeicherung

I. Allgemeines

Mit der vorgeschlagenen Einführung der §§ 113a und 113b TKG soll die Richtlinie zur Vorratsdatenspeicherung RL 2006/24 EG der Europäischen Union in nationales Recht umgesetzt werden. Gegenstand dieser Stellungnahme ist nicht die Vereinbarkeit der Richtlinie mit Gemeinschaftsrecht, sondern die Frage der Vereinbarkeit mit deutschem Verfassungsrecht, weiterhin die Frage der Notwendigkeit einer Vorratsdatenspeicherung sowie Ausführungen zur möglichen Praxistauglichkeit der Vorschriften.

Die vorgesehene Verpflichtung zur verdachtsunabhängigen Speicherung von Verkehrsdaten tangiert im Wesentlichen das Fernmeldegeheimnis (Art. 10 GG) sowie das aus dem allgemeinen Persönlichkeitsrecht folgende Recht auf informationelle Selbstbestimmung. Daneben kollidiert eine solche Speicherung, ohne dass diese beispielsweise durch den Verdacht von Straftaten unmittelbar veranlasst ist, ganz allgemein mit den Grundbegriffen des Datenschutzes, welche für Verkehrsdaten ausdrücklich in §§ 96, 97 TKG ihre Ausprägung gefunden haben. Weiterhin ist mit der Speicherverpflichtung für Telekommunikationsanbieter auch ein Eingriff in deren Berufsausübungsfreiheit gemäß Art. 12 GG gegeben.

Die vorgenannten Eingriffe sind nur dann gerechtfertigt und zulässig, wenn Gründe des Gemeinwohls eine solche Einschränkung erfordern und gleichzeit die Grundsätze der Verhältnismäßigkeit gewahrt sind. Das Bundesverfassungsgericht hat insoweit bereits mehrfach ausgeführt, zuletzt in seinem Urteil vom 2. März 2006 - 2 BvR 2099/04, dass eine wirksame Strafverfolgung ein legitimer Zweck zur Einschränkung des Rechts auf informationelle Selbstbestimmung ist. In gleicher Weise gilt dies auch für Einschränkungen des Schutzes des Fernmeldegeheimnisses sowie der Berufsausübungsfreiheit.

Die mit der Vorratsspeicherung verfolgten Zwecke ergeben sich aus § 113b TKG-E. Diese Vorschrift regelt die Voraussetzungen, bei deren Vorliegen gespeicherte Daten von den Telekommunikationsdienstleistern herausgegeben

werden dürfen – und nur dann! Die "Verfolgung von Straftaten" ist dabei der an erster Stelle genannte Zweck, daneben die Abwehr von erheblichen Gefahren für die öffentliche Sicherheit sowie allgemein die Erfüllung der gesetzlichen Aufgaben der Geheimdienste von Bund und Ländern.

Hinsichtlich der unter Nr. 1 genannten „Verfolgung von Straftaten“ wird diese Voraussetzung für ein Herausgabeverlangen noch genauer konkretisiert durch § 100g Abs. 1 StPO-E, wonach nur bei Straftaten von im Einzelfall erheblicher Bedeutung, insbesondere den im Katalog des § 100a Abs. 2 StPO-E genannten Straftaten, oder bei mittels Telekommunikation begangenen Straftaten, gespeicherte Verkehrsdaten herausgegeben werden dürfen. Unter Berücksichtigung einer solchermaßen konkretisierten Anforderungsschwelle erweisen sich die durch die Pflicht zur Vorratsdatenspeicherung erfolgenden Grundrechtseingriffe als hinnehmbar im Verhältnis zu dem beabsichtigten Zweck und den auf diese Weise verfolgten Gemeinwohlbelangen. Sofern die Bekämpfung erheblicher Straftaten auf andere Weise nicht gewährleistet werden kann, ist daher auch der Verhältnismäßigkeitsgrundsatz nicht tangiert. - Dies gilt auch für die erleichterten Voraussetzungen einer Herausgabeverpflichtung bei Straftaten, welche mittels Telekommunikation begangen sind. Solche Straftaten sind bei der derzeitigen Rechtslage praktisch nicht aufzuklären. Straftätern handeln daher insoweit ohne oder allenfalls mit geringem Risiko. Gemäß § 96 Abs. 2 i.V.m. § 97 Abs. 3 TKG dürfen Daten über vom User hergestellte Internet-Verbindungen bei Flatrate-Verträgen nach dem Ende der jeweiligen Verbindungs.Session allenfalls nur noch unter großen Ausnahmevoraussetzungen gespeichert werden. Daher gibt es beispielsweise im Bereich der Verbreitung von Kinderpornografie keine weiteren Ermittlungsmöglichkeiten mehr, sobald die Verkehrsdaten durch die Provider gelöscht sind. Zwar kann im Regelfall in solchen Fällen die Zuordnung einer zu einem bestimmten Tag und einer bestimmten Uhrzeit festgestellten IP-Nummer den zugehörigen Teilnehmeranschluss eindeutig identifizieren, jedoch nur, sofern entsprechende Daten beim Provider (noch) vorhanden sind, welcher die IP vergeben hat. Sofern der betreffende Provider jedoch entsprechend den Datenschutzbestimmungen nach dem Ende der Verbindung diese Daten gelöscht hat, wird ein Straftäter - soweit es keine anderen Identifizierungsmerkmale gibt - regelmäßig nicht mehr zu

ermitteln sein. Dies gilt in besonderer Weise für sog. Chat-Rooms, welche durch die Nutzer zumeist anonymisiert betreten werden und die sowohl für die Kommunikation unter Tätern, als auch zur Anbahnung von Kontakten gegenüber ahnungslosen Minderjährigen benutzt werden.

In gleicher Weise gilt dies für allgemein kriminelle Handlungen, welche unter Benutzung des Internets begangen werden. Beispielsweise werden Betrügereien bei Internet-Auktionen von den Geschädigten oftmals erst nach zwei oder mehr Wochen entdeckt, wenn sie die ersteigerten und - wie üblich - per Vorkasse bezahlten Waren und Gegenstände nicht oder nur in beschädigtem Zustand erhalten haben. Bis dann die betrügerische Absicht durch den Geschädigten tatsächlich erkannt wird, vergehen meist noch weitere Wochen; daher bleibt eine dann erstattete Anzeige vielfach erfolglos. Sofern nämlich der Täter sich nicht nur den Auktionscount erschlichen, sondern auch noch den Zugriff auf ein ihm nicht gehörendes Konto sich ermöglicht hat, bliebe als einziger Ermittlungsansatz die Identifizierung des Anschlussinhabers über die - beim Auktionshaus regelmäßig gespeicherte - IP; diese ist jedoch – nachdem zwei oder mehr Wochen vergangen sind – in aller Regel bereits gelöscht. Schließlich sind derzeit meist auch die Fälle der Begehung von Straftaten mit durch Phishing erlangten Accountdaten oder mittels sog. Trojaner auf fremden Rechnern verschaffter Zugangsdaten zu Bezahldiensten nicht aufzuklären, weil die hierfür verwendeten IP-Nummern infolge Löschung nicht mehr Anschlussinhabern zuzuordnen sind und diese Taten nicht unmittelbar nach Tatbegehung entdeckt werden.
Angesichts dessen erscheint es nicht verwunderlich, dass geschädigte Bürger den Eindruck einer Rechtsverweigerung empfinden, wenn sie darauf hingewiesen werden, dass aus Datenschutzgründen der Telekommunikationsdienstleister verpflichtet war, diese Daten entweder umgehend oder innerhalb einer vorgegebenen Frist zu löschen, weshalb die zu ihrem Nachteil begangene Tat nicht (mehr) aufklärbar sei.

Umgekehrt erscheint der infolge der allgemeinen Datenspeicherung vorgenommene Eingriff nicht so schwerwiegend, so lange die Daten sich noch im

Bereich des Telekommunikationsdienstleisters befinden (der sie ohnehin kennt), und soweit diese auch nur dann an Behörden herausgegeben werden dürfen, sofern die Voraussetzungen für eine Herausgabe erfüllt sind.

Eine ausreichende Alternative zur Speicherung von Verkehrsdaten ist nicht gegeben, was die Bekämpfung und Aufklärung von Straftaten betrifft. Die teilweise genannte Möglichkeit des "Einfrierens von Daten" beim Provider auf Ersuchen der Ermittlungsbehörden wird einerseits oftmals zu spät kommen und muss andererseits auf jeden Fall erfolglos bleiben, sofern der Telekommunikationsdienstleister seiner aus §§ 96, 97 TKG erwachsenen Verpflichtung nachkommt und die Daten unmittelbar nach dem Ende der Telekommunikationsverbindung löscht. Diese Möglichkeit wäre allenfalls eine sinnvolle Alternative, soweit der Täter von den Ermittlungsbehörden "auf frischer Tat" ertappt wird und es diesen gelingt, den Provider "zum Einfrieren der Daten" zu veranlassen, so lange der Täter die Internetverbindung noch aufrecht erhält.

In gleicher Weise gilt dies auch für die Speicherung von Verkehrsdaten im Fernmelde-, Mobilfunk- und anderen Kommunikationsbereichen, wie beispielsweise dem E-Mail-Verkehr. Nicht selten können Täter nur dadurch überführt werden, dass ihnen nachgewiesen wird, dass sie zu einem bestimmten Zeitpunkt mit dem Opfer oder einer anderen Person telefoniert haben oder/und sich dabei an einem bestimmten Ort befunden haben. Dies gilt nicht nur für den Bereich der Betäubungsmitteldelikte, sondern auch für schwerwiegende Straftaten wie Raubüberfälle, Erpressung, Geiselnahme bis hin zu Tötungsdelikten.

Nach alledem ist festzustellen, dass eine allgemeine Vorratsdatenspeicherung von Verkehrsdaten ein taugliches und für eine wirksame Strafverfolgung notwendiges Instrument ist, um Straftaten aufzuklären und Täter zu überführen.

Die vorgesehene Speicherdauer von sechs Monaten ist im internationalen Vergleich eher kurz, nach meiner persönlichen Erfahrung aber ausreichend, um den damit verfolgten Zweck zu erfüllen.

II. Zu den einzelnen Bestimmungen

In § 113a TKG-E ist sorgfältig geregelt, von welchem Anbieter welche Daten abzuspeichern sind. Mit dem gleichzeitigen Verbot, den Inhalt einer Kommunikation sowie Daten über aufgerufene Internetseiten nicht zu speichern (§ 113 Abs. 8 TKG-E), werden schwerwiegendere Eingriffe in die Rechte der Betroffenen verboten und bleibt der Verhältnismäßigkeitsgrundsatz gewahrt.

Mit der Verpflichtung, die Qualität und den Schutz der gespeicherten Daten durch den Verpflichteten sicher zu stellen (§ 113a Abs. 10 TKG-E) hat der Gesetzgeber in ausreichender Weise Vorsorge getragen, dass Daten nicht in die Hände Nichtberechtigter fallen.

Mit der Löschungsverpflichtung in § 113a Abs. 11 TKG-E wird schließlich sichergestellt, dass gespeicherte Daten nach dem Ende der Speicherfrist zügig einer Löschung zugeführt werden.

Die durch den Gesetzgeber in § 113b Satz 1 Nr. 1 TKG-E i.V.m. § 101g Abs. 1 Satz 1 StPO-E vorgenommene Einschränkung, wonach gespeicherte Daten nur zur Aufklärung von Straftaten herausgegeben werden dürfen, welche auch im Einzelfall von erheblicher Bedeutung sind, ist eine Begrenzung für die Herausgabeverpflichtung getroffen, welche sowohl die Interessen der Strafbekämpfung als auch des Datenschutzes berücksichtigt. Dass bei Straftaten, welche mittels Telekommunikation begangen sind, gespeicherte Daten auch dann herausgegeben werden müssen, wenn die Straftaten nicht von erheblicher Bedeutung sind, aber die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos wäre, erscheint sogar erforderlich, weil in diesen Fällen die Aufklärung der benutzten Telekommunikation in aller Regel der einzige Weg ist, um auch die Straftat selbst aufklären zu können.