Bürgerrechte und TKG-Novelle

Datenschutzrechtliche Auswirkungen der Neufassung des Telekommunikationsgesetzes[1]

Jede unnötige Datenspeicherung bringt Missbrauchsrisiken mit sich und gefährdet dadurch die Privatsphäre des Bürgers. Effektiv lassen sich Missbräuche nur vermeiden, indem von vornherein so wenige Daten wie möglich gespeichert werden. Dieses Gebot der Datensparsamkeit verkennt die TKG-Novelle leider in mehreren Punkten, und dem Bundesdatenschutzbeauftragten ist zuzustimmen, wenn er gegenüber der bisherigen Rechtslage „durchgängig nur Verschlechterungen" sieht[2]. Der Beitrag nimmt die einzelnen Neuerungen des Telekommunikationsdatenschutzrechts kritisch unter die Lupe, zeigt weiterhin bestehende Mängel der gesetzlichen Regelungen auf und geht auf die aktuell diskutierte Einführung einer Verkehrsdatenspeicherungspflicht ein.

1 Recht zur Vorratsspeicherung von Verkehrsdaten zur Störungs- und Missbrauchsbekämpfung, § 100 TKG

Telekommunikations-Verkehrsdaten, nach bisherigem Recht Verbindungsdaten genannt, sind Daten über die näheren Umstände von Telekommunikationsvorgängen (vgl. § 3 Nr. 30 TKG). Es handelt sich um hochsensible Daten, da es ihre Speicherung erlaubt, das Telekommunikationsverhalten einzelner Bürger oder der gesamten Bevölkerung nachzuvollziehen und zu überwachen. Anhand von Verkehrsdaten lassen sich etwa Fragen der folgenden Art beantworten: Hat eine Person bestimmte Beratungsgespräche per Telefon geführt? Hat sie bei muslimischen Vereinigungen angerufen oder deren Internetseiten betrachtet? Wer ruft oft bei schweizer oder liechtensteiner Banken an? Hat jemand an Internet-Foren von Globalisierungskritikern teilgenommen? Wer erhält regelmäßig Emails von palästinensischen Menschenrechtsorganisationen? Die Beispiele machen deutlich, welchen Sprengstoff für eine Demokratie die Speicherung von Verkehrsdaten mit anschließender staatlicher Zugriffsmöglichkeit (etwa §§ 100g, 100h StPO) bildet.

Der neue § 100 TKG bringt eine problematische Ausweitung der Datenspeicherungsrechte von TK-Unternehmen mit sich und stellt aus Sicht der Bürgerrechte wohl die wichtigste Änderung des Telekommunikationsdatenschutzrechts im Zuge der TKG-Novelle dar. Bisher durften Verkehrsdaten im Grundsatz nur insoweit gespeichert werden, wie es zur Abrechnung der genutzten Dienste erforderlich war (§ 89 Abs. 2 Nr. 1 Buchst. c TKG a.F., § 7 TDSV). Die Speicherung personenbezogener Daten für Zwecke der Störungs- oder Missbrauchsbekämpfung war nur „im Einzelfall" zulässig (§ 9 TDSV). Die Regelungen der TDSV wurden nunmehr weitgehend in das neue TKG übernommen. Im Vergleich zu § 9 TDSV verzichtet § 100 TKG jedoch auf das Merkmal „im Einzelfall" und erlaubt damit letztlich die vorsorgliche und zeitlich unbegrenzte Speicherung sämtlicher Telekommunikations-Verkehrsdaten unter dem Deckmantel der Störungs- oder Missbrauchsbekämpfung. Es lässt sich nämlich nie ganz ausschließen, dass ein Verkehrsdatum einmal erforderlich sein könnte, um die rechtswidrige Inanspruchnahme von Telekommunikationsdiensten zu unterbinden oder

[1] Telekommunikationsgesetz vom 22.06.2004 (BGBl. I, S. 1190).

[2] Schaar, Protokoll 15/49 der 49. Sitzung des Ausschusses für Wirtschaft und Arbeit, www.bundestag.de/parlament/gremien15/a09/004Anhoerungen/TKG/protokoll49.pdf, 36.

Störungen zu beseitigen. Jedes Datum ist hierzu potenziell geeignet. Deswegen wird sich auch das in § 100 TKG vorausgesetzte Merkmal der Erforderlichkeit der Datenverarbeitung zu den genannten Zwecken stets begründen lassen. Keine nennenswerte Einschränkung liegt auch in der Bestimmung, wonach eine Datenspeicherung zur Missbrauchsbekämpfung nur „bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte“ zulässig sein soll (§ 100 Abs. 3 TKG). Dass Telekommunikationsnetze teilweise missbraucht werden, liegt auf der Hand. Hierfür werden sich stets auch tatsächliche Anhaltspunkte finden und dokumentieren lassen. Entscheidend ist, dass das Gesetz keine einzelfallbezogenen Anhaltspunkte verlangt und nicht voraussetzt, dass der Diensteanbieter von der „rechtswidrigen Inanspruchnahme“ der Telekommunikationsnetze selbst betroffen ist.

In der Praxis berufen sich TK-Unternehmen tatsächlich auf Erfordernisse der Störungs- und Missbrauchsbekämpfung, um die Speicherung höchst sensibler personenbezogener Daten auf Vorrat zu rechtfertigen, obwohl diese für Abrechnungszwecke nicht erforderlich sind und auch zu sonstigen Zwecken nur in den seltensten Ausnahmefällen benötigt werden. Dies hat sich im Fall des Internet-Access-Providers T-Online gezeigt[3]. Dieses Unternehmen speichert die IP-Adressen, die seinen Kunden für die Internetnutzung zugewiesen werden, sechs Monate lang auf Vorrat und ermöglicht es damit ohne jeden Verdacht, das Nutzungsverhalten sämtlicher Kunden im Nachhinein nachzuvollziehen. Ausweislich der Begründung des Regierungsentwurfs[4] soll § 100 TKG genau diese Praxis legalisieren und ausweiten: „Zur Verhinderung von Missbrauch und zur Datensicherheit können hiervon auch IP-Adressen erfasst sein [...]”. Dabei haben gerade Berechnungen von T-Online ergeben, dass nur 0,0004% der insgesamt dort anfallenden Verkehrsdaten später von Strafverfolgungsbehörden angefordert werden[5]. Die Chance, dass ein Verkehrsdatum zur Missbrauchsbekämpfung benötigt wird, beträgt danach lediglich 1:250.000.

Ebenso wie IP-Adressen könnten TK-Unternehmen nach dem neuen TKG auch sämtliche von ihren Kunden gewählten Telefonnummern auf beliebige Zeit hinaus speichern. Auch diese Daten können zur Aufdeckung der rechtswidrigen Inanspruchnahme von Telekommunikationsdiensten oder zur Störungsbeseitigung einmal von Nutzen sein. Wozu Gesetze wie § 100 TKG führen, zeigt das Beispiel der USA, wo einige TK-Unternehmen seit ihrer Gründung noch keine Verkehrsdaten gelöscht haben, diese also auf unbegrenzte Zeit speichern. Eine solche Vorratsdatenspeicherung birgt höchste Datensicherheits- und Missbrauchsrisiken.

§ 100 TKG ist als Vorstufe zu einer Verkehrsdatenspeicherungspflicht anzusehen, wie sie die Sicherheitsbehörden anstreben[6]. Alleine die Tatsache, dass die Vorschrift die Entscheidung hinsichtlich der Vornahme einer Vorratsspeicherung dem Ermessen der Diensteanbieter überlässt, ändert nichts an ihrem Charakter als staatlicher Eingriff in das Grundrecht der betroffenen Nutzer aus Art. 10 GG (Fernmeldegeheimnis). Die Speicherung von Verkehrsdaten durch private Unternehmen führt zwar nicht unmittelbar zu einer staatlichen Kenntnisnahme dieser Daten. Sie bringt aber typischerweise staatliche Zugriffe auf die derart geschaffenen Datenbestände mit sich, etwa im Wege von Auskunftsersuchen zu Strafverfolgungszwecken (§§ 100g, 100h StPO). Eröffnet

[3] Hierzu ausführlich Jonas Breyer, DuD 2003, 491 (491 ff.).

[4] BT-Drs. 15/2316, 122, im Internet abrufbar unter www.bmwa.bund.de/Redaktion/Inhalte/Downloads/TKG-E-entwurf-mit-begruendung,property=pdf.pdf.

[5] Uhe/Herrmann, Überwachung im Internet, http://ig.cs.tu-berlin.de/oldstatic/da/2003-08/UheHerrmann-Diplomarbeit-082003.pdf, 161.

[6] Siehe näher Punkt 7.

sich der Staat einen erweiterten Zugriff auf Kommunikationsdaten, indem er Diensteanbietern eine Vorratsdatenspeicherung erlaubt, so greift er mittelbar in das Grundrecht der Kommunikationsteilnehmer aus Art. 10 GG ein.

Eine Vorratsspeicherung von Verkehrsdaten ist in Anbetracht ihres geringen Nutzens unverhältnismäßig (siehe auch Punkt 7 unten). Die bloße theoretische Eignung eines Datums für Zwecke der Störungsbeseitigung oder Missbrauchsunterbindung kann dessen Speicherung noch nicht legitimieren[7]. Ansonsten wäre praktisch das gesamte Datenschutzrecht sinnlos, weil sich bei keinem Datum ausschließen lässt, dass es einmal benötigt werden könnte. Ließe man diese theoretische Möglichkeit genügen, dann wäre auf dem Gebiet der Telekommunikation selbst die Speicherung von Inhalten gerechtfertigt. Auch anhand von gespeicherten Telekommunikationsinhalten könnte nämlich in einzelnen Fällen nachgewiesen werden, dass ein Nutzer einen Dienst rechtswidrig benutzt hat. Telefonunternehmen dürften dann beispielsweise alle Telefongespräche aufzeichnen, um anhand der Stimme nachweisen zu können, wer einmal rechtswidrig telefoniert haben könnte. Den Diensteanbietern die Speicherung von Verkehrsdaten nur im Einzelfall zu erlauben, ist den Anbietern zumutbar, denn sie können sich gegen eventuelle Störungen, Schäden und gegen Missbrauch versichern und die Versicherungsprämie auf ihre Kunden umlegen.

Damit ist § 100 TKG wegen Verstoßes gegen das Verhältnismäßigkeitsgebot mit Art. 10 GG unvereinbar und nichtig. Eine verfassungskonforme Auslegung der Vorschrift dahin gehend, dass eine Datenspeicherung nur in einzelnen Fällen zulässig sei, ist mit dem klaren Wortlaut des § 100 TKG wie auch mit dem in der Begründung zum Ausdruck kommenden Willen des Gesetzgebers nicht in Einklang zu bringen.

Umgekehrt hätte der Gesetzgeber – auch gegenüber der bisherigen Rechtslage – Anlass gehabt, in § 100 Abs. 3 TKG einschränkend klarzustellen, dass Telekommunikationsunternehmen keine Strafverfolgungsbehörden sind. Ohne richterliche Anordnung dürfen sie auch bei Vorliegen tatsächlicher Anhaltspunkte im Einzelfall nicht auf eigene Faust in das Fernmeldegeheimnis eingreifen, um vermeintliche „rechtswidrige Inanspruchnahmen der Telekommunikationsnetze und -dienste" aufzudecken, zumal sie für derartiges Verhalten ihrer Kunden nicht haften. Eine Ausnahme ist allenfalls für Leistungserschleichungen und Hackerangriffen gerechtfertigt, von denen das jeweilige TK-Unternehmen selbst betroffen ist. In anderen Fällen haben TK-Unternehmen – wie jeder andere Bürger auch – die Strafverfolgungsbehörden einzuschalten. Das Fernmeldegeheimnis muss Vorrang vor rechtsstaatlich bedenklichen Überwachungsambitionen von TK-Unternehmen haben.

Der Wille des Gesetzgebers, die Speicherungsrechte der Diensteanbieter auszuweiten, hat sich demgegenüber in verschiedenen Vorschriften des neuen TKG niedergeschlagen, etwa in § 88 TKG, der Vorschrift über das Fernmeldegeheimnis. Bisher sah § 85 Abs. 3 S. 1 TKG a.F. vor, dass sich Diensteanbieter nur insoweit Kenntnis von Inhalt und den näheren Umständen der Telekommunikation verschaffen dürfen, wie es zur geschäftsmäßigen Erbringung der Telekommunikationsdienste erforderlich ist. § 88 Abs. 3 S. 1 TKG erlaubt Diensteanbietern nunmehr die Kenntnisnahme „für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme". Die Einfügung der Worte

[7] Ähnlich die Erklärung der Datenschutzbeauftragten des Bundes und der Länder vom 25. Juni 2004, www.lda.brandenburg.de/sixcms/detail.php?id=161413&template=aktuell_d1: „Das grundgesetzlich garantierte Fernmeldegeheimnis lässt eine Speicherung von Daten über die Nutzung öffentlicher Telekommunikationsnetze (insbesondere auch des Internets) außer für betriebliche Zwecke nur zu, wenn ein konkreter Verdacht für eine Straftat von erheblicher Bedeutung besteht."

„einschließlich des Schutzes ihrer technischen Systeme" könnte so interpretiert werden, dass beliebige Eingriffe in das Fernmeldegeheimnis zulässig sein sollen, wenn sie nur zum (angeblichen) Zweck des Schutzes der technischen Systeme eines Betreibers vorgenommen werden. § 100 TKG enthält jedoch bereits eine differenzierte Regelung über die Zulässigkeit von Eingriffen in das Fernmeldegeheimnis zum Schutz von Telekommunikationsanlagen. Diese Vorschrift geht § 88 Abs. 3 S. 1 TKG als Spezialregelung vor, so dass die verwirrende Generalklausel über den „Schutz technischer Systeme" als rein deklaratorisch und ohne eigenständige Bedeutung anzusehen ist.

Des Weiteren sieht § 92 TKG in Übereinstimmung mit der Vorgängervorschrift des § 3 Abs. 6 TDSV vor, dass Diensteanbieter personenbezogene Daten an ausländische nicht-öffentliche Stellen unter anderem zum Zweck der Missbrauchsbekämpfung übermitteln dürfen. Im Gegensatz zu § 3 Abs. 6 TDSV nimmt § 92 TKG jedoch nicht mehr auf die Regelung der Datenverarbeitung zur Missbrauchsbekämpfung (jetzt § 100 Abs. 3 TKG) Bezug. Die Legalisierung von Datentransfers pauschal „für die Missbrauchsbekämpfung" könnte wiederum so interpretiert werden, dass beliebige Datentransfers in Drittländer zulässig sein sollen, wenn sie nur zur Bekämpfung wie auch immer gearteten „Missbrauchs" vorgenommen werden. § 100 TKG enthält jedoch bereits eine differenzierte Regelung über die Zulässigkeit von Eingriffen in das Fernmeldegeheimnis zum Schutz von Telekommunikationsanlagen vor Missbrauch. Diese Vorschrift geht § 92 TKG daher als Spezialregelung vor, auch wenn der Gesetzestext das – im Gegensatz zur bisherigen Rechtslage – nicht mehr durch einen ausdrücklichen Verweis klarstellt.

2 Recht zur Vorratsspeicherung von Verkehrsdaten zu Abrechnungszwecken, § 97 Abs. 3 und 4 TKG

Das Interesse der Sicherheitsbehörden und der Diensteanbieter an erweiterten Datenspeicherungsrechten hat sich auch im Bereich der Abrechnungsdaten durchgesetzt. § 97 Abs. 3 und 4 TKG regelt die Zulässigkeit der Speicherung von Verkehrsdaten zu Abrechnungszwecken neu und bewirkt verschiedene Veränderungen gegenüber der bisherigen Rechtslage[8].

So können Bürger nur noch die Löschung der von ihnen gewählten Zielrufnummern mit Rechnungsversand verlangen (§ 97 Abs. 4 S. 1 Nr. 2 TKG), nicht mehr aber der übrigen Verkehrsdaten (z.B. Ort und Zeit getätigter Telefonanrufe). Diese dürfen damit für eine Dauer von bis zu sechs Monaten ab Rechnungsversand gespeichert werden (§ 97 Abs. 3 S. 3 TKG), ohne dass der Anschlussinhaber dies untersagen kann. Diese Änderung gegenüber § 7 Abs. 4 S. 1 TDSV lässt sich nicht damit begründen, dass Diensteanbieter die übrigen Verkehrsdaten zum Nachweis der Richtigkeit ihrer Abrechnungen benötigten. Die Diensteanbieter trifft nämlich keine Beweislast, soweit ihre Kunden die Speicherung von Verkehrsdaten untersagt haben (§ 16 Abs. 2 TKV). Damit gestattet § 97 Abs. 4 S. 1 TKG die Speicherung hochsensibler Daten (wer hat wann und von wo aus telefoniert?) ohne Grund; die Änderung wird dementsprechend in der Begründung nicht gerechtfertigt oder auch nur angesprochen.

Weiterhin ist bekannt, dass eine nicht unerhebliche Zahl von Menschen von ihrem gesetzlichen Wahlrecht hinsichtlich der Speicherungsdauer von Abrechnungsdaten (§

[8] Kritisch dazu die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 21.11.2003, www.bfd.bund.de/information/DS-Konferenzen/66_67_ent1.html.

97 Abs. 4 S. 1 TKG) keinen Gebrauch macht. Das gilt vor allem für Altkunden der Deutschen Telekom AG, die ihren Telefonanschluss zu einer Zeit angemeldet haben, zu der es noch kein Wahlrecht gab. Es handelt sich also beispielsweise um Senioren. Anders als bisher soll für den Fall, dass der Kunde keinen Gebrauch von seinem Wahlrecht macht, nicht mehr eine um drei Stellen gekürzte Speicherung der gewählten Zielrufnummern erfolgen (so noch § 7 Abs. 3 TDSV) sondern deren vollständige Speicherung vorgenommen werden (§ 97 Abs. 4 S. 2 Hs. 2 TKG). Mit dieser Änderung macht sich der Staat die technische Unbedarftheit der Kunden, die ihr Wahlrecht nicht ausüben, zunutze. Es ist anzunehmen, dass Kriminelle stets die vollständige Löschung von Zielrufnummern mit Rechnungsversand verlangen und die Änderung daher nur zulasten unbedarfter Bürger geht. Zur Prüfung der Richtigkeit von Abrechnungen ist die Angabe der letzten drei Stellen der gewählten Rufnummern nicht erforderlich, weil die Verbindungskosten von diesen drei Stellen nicht abhängen.

Eine weitere datenschutzrechtliche Verschlechterung durch das neue TKG liegt darin, dass der Kunde künftig nur die Möglichkeit hat, entweder die um drei Stellen gekürzte Speicherung von Zielrufnummern oder deren Löschung mit Versand der Rechnung zu verlangen (§ 97 Abs. 4 S. 1 TKG). Bisher konnte beides kombiniert werden, so dass die Zielrufnummern zunächst um drei Ziffern zu kürzen und mit Rechnungsversand dann vollständig zu löschen waren. Auch die Abschaffung dieser Möglichkeit ist sachlich nicht gerechtfertigt.

Darüber hinaus ist – anders als bisher (§ 7 Abs. 3 S. 3 TDSV) – nicht mehr ausdrücklich festgelegt, dass die Speicherung von Verkehrsdaten über das Verbindungsende hinaus (§ 97 Abs. 3 S. 3 TKG) nur zu Nachweiszwecken für die Richtigkeit der berechneten Entgelte erfolgen darf. Diese Änderung könnte so interpretiert werden, dass die sechsmonatige Speicherung sämtlicher Verkehrsdaten zulässig sei, auch derjenigen, deren Speicherung nicht geeignet ist, die Richtigkeit der berechneten Entgelte nachzuweisen (z.B. IP-Adressen). Einer solchen Interpretation steht jedoch § 97 Abs. 3 S. 2 TKG entgegen, der ausdrücklich vorsieht, dass nicht für die Berechnung des Entgelts erforderliche Daten unverzüglich zu löschen sind. Angesichts dessen kann sich § 97 Abs. 3 S. 3 TKG – entsprechend der bisherigen Rechtslage – nur auf die Verkehrsdaten beziehen, deren Speicherung für die Berechnung des Entgelts erforderlich ist.

Insgesamt wird bei der Diskussion um die Aufbewahrungsdauer von Verkehrsdaten verkannt, dass die Speicherung solcher Daten über das Ende einer Verbindung hinaus an sich nicht erforderlich ist. Bis zur Einführung des digitalen Telefonnetzes Anfang der 90er Jahre sind die damalige Bundespost und die Bürger ohne eine Speicherung von Verkehrsdaten ausgekommen. Es genügte damals und es würde auch heute noch genügen, nach dem Ende einer jeden Verbindung die angefallenen Kosten zu ermitteln und diese dem Kundenkonto zu belasten. Technisch ist dies allen Anbietern möglich und wird verbreitet bereits heute praktiziert. Ein solches Verfahren geht nicht zulasten der Anbieter, weil der Kunde die Beweislast hinsichtlich der Richtigkeit der Abrechnung trägt, wenn er die sofortige Löschung seiner Daten wählt (§ 16 Abs. 2 TKV). Zwar kann der Kunde bei sofortiger Löschung der Verkehrsdaten die Richtigkeit der Abrechnung des Anbieters im Nachhinein nicht mehr nachprüfen. Es sollte aber jedem Bürger überlassen bleiben, ob ihm diese Überprüfungsmöglichkeit wichtiger ist als seine Privatsphäre. Immerhin ist es sehr unwahrscheinlich, dass Abrechnungssysteme falsch arbeiten, und bis Anfang der 90er Jahre ist man, wie bereits erwähnt, problemlos auch ohne die Speicherung von Verkehrsdaten ausgekommen. Zudem verhindert auch die Aufbewahrung von Verkehrsdaten nicht, dass das Abrechnungssystem bereits bei der Erfassung der einzelnen Verbindungen fehlerhaft arbeitet. Angesichts dessen gibt es

keine Notwendigkeit, die Löschung von Verkehrsdaten frühestens mit Versand der Rechnung vorzusehen. Die TKG-Novelle hätte Kunden vielmehr das Recht einräumen sollen, die sofortige Löschung sämtlicher Verkehrsdaten nach dem Ende jeder Verbindung verlangen zu können. Wenn das Gesetz dies anders handhabt, so lässt sich das nur mit dem Interesse der Sicherheitsbehörden an einer möglichst lückenlosen Aufzeichnung des Kommunikationsverhaltens der Bevölkerung erklären. Dieses Interesse rechtfertigt jedoch keine Vorratsspeicherung ansonsten nicht benötigter Daten, zumal ernsthaften Kriminellen ohnehin Mittel und Wege zur Verfügung stehen, um sich der Überwachung ihrer Telekommunikation zu entziehen (z.B. durch Nutzung von Prepaid-Mobiltelefonkarten, die auf den Namen einer anderen Person angemeldet sind).

Zu kritisieren ist auch die Bemessung der maximal zulässigen Aufbewahrungsdauer. Dass zur Abrechnung benötigte Verkehrsdaten bis zu sechs Monate lang gespeichert werden dürfen (§ 97 Abs. 3 S. 3 TKG, ebenso § 7 Abs. 3 S. 3 TDSV), dient offenbar dem Zweck, die Überwachung der Telekommunikation durch die Sicherheitsbehörden zu erleichtern. Eine angemessene Frist stellen sechs Wochen nach Rechnungsversand dar, wie es noch die TKV 1995 vorsah. Innerhalb von sechs Wochen hat jedermann die Möglichkeit, Einwendungen zu erheben.

3 Koppelungsverbot, § 95 Abs. 5 TKG

Geändert wurde des Weiteren das sogenannte „Koppelungsverbot“. Nach bisheriger Rechtslage durfte die Erbringung von Telekommunikationsdiensten nicht von der Angabe personenbezogener Daten abhängig gemacht werden, die nicht erforderlich sind, um diese Dienste zu erbringen (§ 3 Abs. 2 TDSV). Diese Regelung verwirklichte das grundlegende Recht der Bürger auf informationelle Selbstbestimmung, wenn sie es Diensteanbietern verbat, einen Dienst nur unter der Voraussetzung anzubieten, dass der Kunde in die Erhebung oder Nutzung personenbezogener Daten zu anderen Zwecken einwilligt. In solchen Fällen kann von einer Freiwilligkeit der Einwilligung des Kunden nämlich keine Rede sein.

§ 95 Abs. 5 TKG sieht demgegenüber nur noch die folgende Regelung vor: „Die Erbringung von Telekommunikationsdiensten darf nicht von einer Einwilligung des Teilnehmers in eine Verwendung seiner Daten für andere Zwecke abhängig gemacht werden, wenn dem Teilnehmer ein anderer Zugang zu diesen Telekommunikationsdiensten nicht oder in nicht zumutbarer Weise möglich ist.“ Die Vorschrift greift also nur noch ein, wenn der Kunde beweist, dass er keine anderweitige Zugangsmöglichkeit hat. Auch wenn mit dieser Fassung eine Vereinheitlichung mit dem TDDSG angestrebt wurde[9], so ist kein Grund ersichtlich oder in der Begründung angegeben, der eine Vereinheitlichung auf dem niedrigeren Niveau des TDDSG rechtfertigt. Umgekehrt wäre eine Anpassung des TDDSG in Betracht gekommen. Schon bisher konnten Telekommunikationsanbieter um die freiwillige Angabe von Daten bitten und den Kunden dafür besondere Vergünstigungen (z.B. Rabatte) in Aussicht stellen. Dieser Mechanismus ist markt- und interessengerechter als eine einseitige Regelung der Frage durch die AGB des Anbieters.

Der Wortlaut des § 95 Abs. 5 TKG ist nicht eindeutig: Man könnte die Regelung so auslegen, dass sie es genügen lässt, wenn dem Kunden am Markt auch nur ein Dienst

[9] In diese Richtung die Begründung des Regierungsentwurfs, BT-Drs. 15/2316, 89, im Internet abrufbar unter www.bmwa.bund.de/Redaktion/Inhalte/Downloads/TKG-E-entwurf-mit-begruendung,property=pdf.pdf.

zur Verfügung steht, der keine Einwilligung in die Zweckentfremdung personenbezogener Daten fordert. Als Folge wäre zu befürchten, dass sich Anbieter in ihren vorgedruckten AGB die Einwilligung in die Erhebung und Verwendung persönlicher Daten zu anderen Zwecken als der Erbringung der Telekommunikationsdienste routinemäßig erteilen lassen. Beispielsweise könnte die Deutsche Telekom AG die Bereitstellung eines Telefonanschlusses von der Angabe der persönlichen Interessen oder des eigenen Gehalts abhängig machen.

Allerdings formuliert § 95 Abs. 5 TKG nicht, dass ein anderer Zugang zu „Telekommunikationsdiensten dieser Art“ zur Verfügung stehen muss. Erforderlich ist vielmehr ein anderer, zumutbarer Zugang zu „diesen“, also zu den jeweils angebotenen, Telekommunikationsdiensten eines Anbieters. In dieser Auslegung muss jeder Anbieter mindestens eine Zugangsmöglichkeit zu jedem seiner Dienste anbieten, die keine Angabe unnötiger personenbezogener Daten voraussetzt. Weil sich das Angebot verschiedener Diensteanbieter oftmals hinsichtlich der einzelnen Leistungsmerkmale unterscheidet, sichert nur diese Auslegung das Recht auf informationelle Selbstbestimmung der Kunden. Sie ist daher vorzugswürdig.

4 Identifizierungspflicht, § 111 TKG

§ 111 TKG zufolge soll die Bereitstellung von Rufnummern nur noch nach Erhebung von Name, Anschrift und Geburtsdatum des Anschlussinhabers zulässig sein. Das neue TKG führt damit eine allgemeine Identifizierungspflicht mit anschließender Vorratsdatenspeicherung von Telekommunikations-Bestandsdaten ein (§§ 111, 112 TKG). Abgesehen von Sondergebieten wie dem Bereich finanzieller Transaktionen (Geldwäschegesetz) ist eine staatlich angeordnete Identifizierungspflicht im deutschen Recht bisher einmalig. In Verbindung mit den breiten staatlichen Zugriffsrechten auf die erfassten Kundendaten (§§ 112, 113 TKG) stellt § 111 TKG einen einzigartigen Präzedenzfall vorsorglicher staatlicher Überwachung der Bürger dar. Angesichts der vielfältigen Umgehungsmöglichkeiten steht die Schwere des mit § 111 TKG verbundenen Grundrechtseingriffs außer Verhältnis zu dem möglichen Nutzen der Vorschrift[10]. Eine Vorratsspeicherung von Telekommunikations-Bestandsdaten nur zu staatlichen Zwecken ist daher mit dem Grundrecht auf informationelle Selbstbestimmung unvereinbar. Dies hat den Gesetzgeber jedoch nicht davon abgehalten, eine derartige Vorratsspeicherungspflicht einzuführen. Im Laufe des Gesetzgebungsverfahrens hatte der Bundestag zwar beschlossen, die Identifizierungspflicht des § 111 TKG nicht auf Prepaid-Produkte, also auf vorausbezahlte Mobiltelefonkarten, zu erstrecken[11]. Diese Einschränkung konnte sich im Vermittlungsausschuss jedoch nicht durchsetzen und wurde wieder fallen gelassen. Stattdessen wurde in § 111 Abs. 1 S. 1 TKG klargestellt, dass die dort genannten personenbezogenen Daten auch dann zu erheben sind, wenn dies „für betriebliche Zwecke nicht erforderlich“ ist.

5 Ausweitung des Zugriffs auf Bestandsdaten, §§ 112, 113 TKG

§ 112 TKG zufolge haben Anbieter von Telekommunikationsdiensten für die Öffentlichkeit Bestandsdaten in eine besondere Datenbank einzustellen. Auf diese

[10] Vgl. im Einzelnen Breyer, RDV 2003, 218 (220 ff.).

[11] § 109 Abs. 4 TKG-E i.d.F. der Beschlussempfehlung des Wirtschaftsausschusses, BT-Drs. 15/2674.

Datenbank darf eine Vielzahl öffentlicher Stellen im Wege eines Online-Abrufverfahrens zugreifen, und zwar jeweils „zur Erfüllung ihrer gesetzlichen Aufgaben“[12]. Die TKG-Novelle hat die Liste der zugriffsberechtigten Behörden erweitert um Einrichtungen, die Notrufe bearbeiten, die Bundesanstalt für Finanzdienstleistungsaufsicht und die für die Verfolgung und Ahndung von Schwarzarbeit zuständigen Behörden (§ 112 TKG).

Im Jahr 2002 sind etwa 2 Mio. Zugriffe auf Bestandsdaten im Wege des automatischen Abrufverfahrens erfolgt[13]; seit dem Jahr 2000 hat sich die Anzahl der Zugriffe jedes Jahr um 50% erhöht[14]. Da jede Abfrage eine Vielzahl von Datensätzen umfassen kann, ist die Wahrscheinlichkeit, dass an einem beliebigen Tag auf die Bestandsdaten eines beliebigen Bürgers zugegriffen wird, hoch. Diese Wahrscheinlichkeit wird weiter erhöht durch § 112 Abs. 1 S. 4 Nr. 2 TKG, der die Verwendung von Jokerzeichen bei Online-Abfragen erlaubt. Die ursprünglich vom Bundestag beschlossene Begrenzung der Abfragemöglichkeit auf jeweils 20 Datensätze wurde im Vermittlungsverfahren wieder fallen gelassen. Die Behörden dürfen daher nach § 112 Abs. 1 S. 4 Nr. 2 TKG beispielsweise den Namen, die Adresse und das Geburtsdatum aller Anschlussinhaber, die in einer bestimmten Straße wohnen, abrufen, also praktisch eine Rasterung von Haushalten vornehmen. Diese Befugnis greift in besonderem Maße in die Rechte der Betroffenen ein. Mit dem Parlamentsvorbehalt für derart grundrechtswesentliche Fragen ist es unvereinbar, dass die Grenzen dieser Befugnis erst in einer Rechtsverordnung geregelt werden sollen (§ 112 Abs. 3 S. 1 Nr. 3 TKG). Die Verordnung bedarf der Zustimmung des Bundesrats (§ 112 Abs. 3 S. 1 TKG).

Auf Passwörter und andere Codes, mittels derer auf Mobiltelefone, Mailboxen, Anrufbeantworter u.ä. zugegriffen werden kann, haben Staatsanwaltschaft, Polizei, Verfassungsschutzämter und Nachrichtendienste nun weitgehend uneingeschränkten Zugriff (§ 113 Abs. 1 S. 2 TKG). Diensteanbieter müssen derartige Codes auf Anfrage herausgeben, wenn sie über diese verfügen. § 113 Abs. 1 S. 2 TKG bildet allerdings keine gesetzliche Grundlage für Eingriffe in Art. 10 GG, wie sie mit der Kenntnisnahme von Telekommunikationsinhalten und -umständen verbunden sind (vgl. § 113 Abs. 1 S. 3 TKG). Es obliegt daher den zugriffsberechtigten Behörden, Zugriffscodes nur insoweit einzusetzen, wie kein Eingriff in das Fernmeldegeheimnis erfolgt.

Fraglich ist, welche üblicherweise zugriffsgeschützten Informationen dem Fernmeldegeheimnis unterliegen. Zweck des Fernmeldegeheimnisses ist es, die Beteiligten so zu stellen, wie sie ohne die Inanspruchnahme der Fernmeldetechnik, also bei unmittelbarer Kommunikation in beiderseitiger Gegenwart der Kommunizierenden, stünden[15]. Inhalt und nähere Umstände eines Kommunikationsvorgangs sind daher von Art. 10 GG insoweit geschützt, wie sie während der Übermittlungsphase wahrgenommen oder gespeichert wurden. Möglichkeiten der Kenntnisnahme, die auch im Fall einer räumlich-unmittelbaren Kommunikation gegeben wären, bleiben von Art. 10 GG demgegenüber unberührt.

Die vom Fernmeldegeheimnis geschützte Übermittlungsphase endet mit der Kenntnisnahme einer Nachricht durch den Adressaten. Nicht vom Fernmeldegeheimnis

---

[12] Zur verfassungsrechtlichen Problematik der §§ 112, 113 TKG vgl. Breyer, RDV 2003, 218 (220 ff.); Simitis, Spiros: Schriftliche Stellungnahme zur öffentlichen Anhörung des Ausschusses für Wirtschaft und Arbeit am 09.02.2004 in Berlin zum Entwurf eines Telekommunikationsgesetzes (TKG), in: Ausschussdrucksache 15(9)961, www.bundestag.de/gremien15/a09/004Anhoerungen/TKG/materialeingeladene.pdf, 222 (224 ff.).

[13] BfD, 19. Tätigkeitsbericht (2001-2002), 79, www.bfd.bund.de/information/19tb0102.pdf.

[14] BfD, 19. Tätigkeitsbericht (2001-2002), 79, www.bfd.bund.de/information/19tb0102.pdf.

[15] BVerfGE 100, 313 (363).

geschützt sind daher etwa Daten, die der Benutzer eines Mobiltelefons oder eines anderen Endgeräts in dieses eingespeichert hat (z.B. elektronisches Adressbuch, gelesene SMS). In der Kenntnisnahme solcher Daten durch den Staat realisiert sich kein fernmeldespezifisches Übermittlungsrisiko; die Speicherung von Daten auf einem Mobiltelefon durch den Benutzer ist nicht anders anzusehen als die Aufzeichnung von Informationen auf einem Blatt Papier. Anders verhält es sich etwa mit Daten, die ein Telekommunikationsunternehmen für den Kunden speichert, z.B. in elektronischen Mailboxen oder Anrufbeantwortern (Voiceboxen). Solche Informationen werden noch während der Übermittlungsphase gespeichert, nämlich bevor der Kunde sie zur Kenntnis genommen hat. Im Unterschied zur räumlich-unmittelbaren Kommunikation gelangen die Daten auch nicht in den Machtbereich des Kunden, sondern sind bei dem Telekommunikationsunternehmen einem erleichterten staatlichen Zugriff ausgesetzt. Solche, bei Telekommunikationsunternehmen gespeicherte Daten unterliegen daher dem Fernmeldegeheimnis[16] und dürfen von staatlichen Behörden nur aufgrund von Vorschriften zur Kenntnis genommen werden, die zu Eingriffen in Art. 10 GG ermächtigen.

6 Kosten der Telekommunikationsüberwachung

Die Entwicklung der Telekommunikationsüberwachung wird vielfach kritisiert. Die Zahl der Telekommunikationsüberwachungsanordnungen nach § 100a StPO steigt von Jahr zu Jahr rapide und verdoppelt sich etwa alle vier Jahre. Eine Untersuchung des Max-Planck-Instituts für ausländisches und internationales Strafrecht hat ergeben, dass es nur in 17% der untersuchten Verfahren zu Erfolgen der Telekommunikationsüberwachung in bezug auf den Anlass der Überwachungsmaßnahme kam[17]. Ganz ähnlich wird es sich im Bereich des staatlichen Zugriffs auf Bestands- und Verbindungsdaten verhalten, wobei hier keinerlei Statistiken oder Effizienzuntersuchungen vorliegen.

Das richtige Mittel, um diese – auch im internationalen Vergleich – nicht zu rechtfertigende ständige Ausweitung der Telekommunikationsüberwachung einzudämmen, liegt in der Einführung einer staatlichen Erstattung der Überwachungskosten. Im Ausland wird dieser Weg teilweise bereits beschritten, zumal die Verfassungsgerichte der Länder Österreich und Frankreich bereits entschieden haben, dass die Belastung der TK-Unternehmen – und mittelbar ihrer Kunden – mit den Überwachungskosten verfassungswidrig ist[18]. Zugriffe auf Inhalt und Umstände der Telekommunikation dienen der Strafverfolgung und Gefahrenabwehr, mithin also der Allgemeinheit. Es ist mit dem Gebot der Lastengleichheit (Art. 3 Abs. 1 GG) unvereinbar, wenn die Kosten dieser Maßnahmen nur den Telekommunikationsnutzern auferlegt werden. Dass intensive Telekommunikationsnutzer über die von ihnen entrichteten Entgelte die Hauptlast der Kosten tragen müssen, ist willkürlich, da ihr Verhalten keine besonderen Gefahren für die Allgemeinheit schafft und da sie auch nicht besonders von staatlichen Überwachungsmaßnahmen profitieren. Überdies werden durch die Kostentragungspflicht der TK-Unternehmen die wirklichen Kosten der

[16] Ebenso die Begründung des Regierungsentwurfs, BT-Drs. 15/2316, 97.

[17] Albrecht/Arnold/Demko/Braun, Rechtswirklichkeit und Effizienz der Telekommunikationsüberwachung, 455 ff.

[18] Österr. Verfassungsgerichtshof, G 37/02-16 u.a. vom 27.02.2003, www.vfgh.gv.at/presse/G37-16-02.pdf; Franz. Verfassungsgerichtshof, zitiert bei EuroISPA, Internet Service Providers' Association (Europe): Stellungnahme zur Cybercrime-Anhörung der Kommission, http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/PublicHearingPresentations/EuroISPA.html.

Telekommunikationsüberwachung verschleiert und der Haushaltskontrolle des Parlaments entzogen.

Es ist daher lediglich eine Frage der Zeit, bis auch das Bundesverfassungsgericht den bisherigen Ausschluss der Kostenerstattung in Deutschland (vgl. §§ 110 Abs. 1 S. 1 Nr. 1, 111 Abs. 1 S. 5, 112 Abs. 5 TKG) für verfassungswidrig erklären wird[19]. Im Laufe des Gesetzgebungsverfahrens hat nun auch der Bundesrat Zweifel daran geäußert, ob die Regelungen des TKG zur Kostentragung Bestand haben können[20], insbesondere bezüglich der Pflicht zur unentgeltlichen Vorhaltung von Überwachungseinrichtungen nach § 110 Abs. 1 S. 1 Nr. 1 TKG. Gleichwohl sieht die Neufassung des TKG nach wie vor nur eine Kostenerstattung für einzelne Überwachungsmaßnahmen vor (§ 110 Abs. 9 S. 1 TKG). Die Rechtsverordnung nach § 110 Abs. 9 TKG bedarf zudem der Zustimmung des Bundesrats, im dem traditionell die Interessen der Sicherheitsbehörden stark vertreten sind. Diese haben kein Interesse an einer staatlichen Kostenerstattung, weil die finanziellen Implikationen der Telekommunikationsüberwachung ansonsten zu deren Einschränkung führen könnten.

7 Vorratsspeicherungspflicht

In seiner Stellungnahme zum Regierungsentwurf forderte der Bundesrat, allen Anbietern von Telekommunikationsdiensten auf eigene Kosten eine sechsmonatige Aufbewahrung sämtlicher erhobener Verkehrsdaten vorzuschreiben (Vorratsspeicherungspflicht)[21]. Die Aufbewahrung sollte alleine für den Fall erfolgen, dass die Daten einmal von Sicherheitsbehörden und Nachrichtendiensten benötigt werden. Dieser Vorschlag ist im weiteren Gesetzgebungsverfahren von allen Bundestagsfraktionen abgelehnt worden und hat sich auch im Vermittlungsverfahren nicht durchsetzen können. Gleichwohl ist nicht zu erwarten, dass die Sicherheitsbehörden ihr seit 1997 in regelmäßigen Zeitabständen immer wieder verfolgtes Vorhaben aufgeben werden. Derzeit wird auf EU-Ebene ein vergleichbarer Vorschlag beraten[22]. Als EU-Rahmenbeschluss kann diese Vorlage nur mit der Stimme der Bundesregierung beschlossen werden. Die Zustimmung des Europäischen Parlaments ist dagegen nicht erforderlich (Art. 34 EU).

Im Fall einer Vorratsspeicherung von Verkehrsdaten könnte jederzeit und verdachtslos nachvollzogen werden, wer wann mit wem telefoniert hat, wer welche Internetseiten betrachtet hat oder wer wem Emails oder SMS geschickt hat. Da eine Vorratsspeicherung sogar Mobiltelefon-Positionsdaten erfassen würde, ließen sich auch die Bewegungen von Handybesitzern auf Monate oder Jahre hinaus lückenlos nachverfolgen. Dass ein derartiges Generalabbild des Verhaltens der Bevölkerung die Kriminalitätsraten merklich senken könnte, ist nicht zu erwarten. Ernsthafte Kriminelle oder gar Terroristen würden Umgehungsmöglichkeiten wie z.B. ausländische Prepaid-Karten nutzen, so dass den Sicherheitsbehörden letztlich nur in Einzelfällen geholfen wäre, die insgesamt nicht ins Gewicht fallen. Damit stellt eine derartige

[19] Vgl. schon die zutreffenden Ausführungen in BVerfGE 92, 91 – Feuerwehrabgabe.

[20] BR-Drs. 755/03, 35.

[21] BR-Drs. 755/03, 33 f.

[22] 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, Ratsdokument Nr. 8958/04 vom 28.04.2004, http://register.consilium.eu.int/pdf/de/04/st08/st08958.de04.pdf.

Vorratsspeicherung einen grob unverhältnismäßigen Eingriff in Art. 10 GG und in das Recht auf informationelle Selbstbestimmung der Betroffenen dar[23].

Insoweit kann schon auf die Stellungnahme der CDU/FDP-Bundesregierung zum ersten Telekommunikationsgesetz verwiesen werden[24]: „*Die Forderung des Bundesrates, neben den ‚Höchstfristen' auch ‚Mindestfristen' für die Speicherung von personenbezogenen Daten der an der Telekommunikation Beteiligten vorzusehen sowie neben den Interessen der Unternehmen und Betroffenen auch diejenigen der in Absatz 6 Nr. 1 genannten Stellen einzubeziehen, wird abgelehnt. Damit würde den in § 86 Abs. 1 Satz 2 normierten Grundsätzen der Verhältnismäßigkeit, Erforderlichkeit und Zweckbindung beim Erlaß von Datenschutzvorschriften widersprochen. Die Verarbeitung von Telekommunikationsdaten ist regelmäßig auf den betrieblich erforderlichen Zweck der Abwicklung der jeweiligen vertraglich vereinbarten Telekommunikationsdienstleistung beschränkt. Das Anliegen des Bundesrates würde vom Ergebnis her auf eine mangels aktuellen Bedarfs unzulässige Vorratsspeicherung von Daten hinauslaufen.*"

Aus Sicht der Wirtschaft ist zu beachten, dass sich alle Wirtschaftsverbände in der Vergangenheit geschlossen gegen eine Vorratsspeicherungspflicht von Verkehrsdaten ausgesprochen haben. Eine solche Regelung hätte angesichts der zu speichernden Datenberge nicht vertretbare Kostenimplikationen. In der Begründung seines Vorschlags übersieht der Bundesrat, dass die Hauptsache der Kosten nicht für die Speicherung der Daten sondern für deren Aufbereitung, Verwaltung und Herausgabe an Behörden anfällt. Überträgt man britische Berechnungen auf Deutschland, so drohen der Industrie insgesamt Mehrkosten in Höhe von 200 Mio. Euro pro Jahr. Der Branchenverband VATM rechnet für die deutsche Wirtschaft gar mit jährlichen Kosten von 500 Mio. Euro[25]. Eine solche Kostenbelastung der betroffenen Unternehmen würde Markteintrittsschwellen erhöhen, deutsche Unternehmen im internationalen Wettbewerb benachteiligen und Arbeitsplätze vernichten. All dies kann nicht im Interesse der Bundesrepublik sein.

Angesichts der vielen Stimmen, die sich gegen eine Vorratsdatenspeicherungspflicht aussprechen, ist zu hoffen, dass derartigen Plänen weiterhin entschieden entgegen getreten wird.

Patrick Breyer Fassung vom 04.08.2004

---

[23] Die Unverhältnismäßigkeit einer verdachtslosen Vorratsspeicherung von Verkehrsdaten bekräftigen u.a.: Artikel-29-Gruppe der EU, Stellungnahme 5/2002, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp64_de.pdf; BITKOM, Stellungnahme zur Gesetzesinitiative des Bundesrates vom 31.05.2002 (BR-Drs. 275/02), 12.08.2002, www.bitkom.org/files/documents/Position_BITKOM_Vorratsdatenspeicherung_u.a._12.08.2002.pdf, 10; Datenschutzbeauftragte des Bundes und der Länder, Entschließung zur systematischen verdachtslosen Datenspeicherung in der Telekommunikation und im Internet, www.datenschutz-berlin.de/doc/de/konf/64/internet.htm; Empfehlung des Europäischen Parlaments zu der Strategie zur Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität (2001/2070(COS)) vom 06.09.2001, Dokument Nr. A5-0284/2001; Europäische Datenschutzbeauftragte, www.fipr.org/press/020911DataCommissioners.html.

[24] Gegenäußerung der Bundesregierung, BT-Drs. 13/4438, 39.

[25] Capital: Bundesinnenminister bereitet neues Gesetz zur Terrorabwehr vor, Meldung vom 26.05.2004, www.capital.de/heft/presse/257165.html.

Dieser Beitrag ist in der RDV (Recht der Datenverarbeitung) 2004, S. 147-153 erschienen.