Axel Spies BfDI und BNetzA konkretisieren Speicherfristen im TKG mit neuem Leitfaden ZD-Aktuell 2012, 03199

Am 27.9.2012 haben der Bundesdatenschutzbeauftragte (BfDI) *Peter Schaar* und die *BNetzA* einen neuen Leitfaden veröffentlicht. Er umfasst die Speicherung von Daten, die den TK-Verkehr betreffen (z.B. zu Zwecken der Rechnungsstellung oder Beseitigung von Störungen). Die Behörden hoffen damit mehr Rechtssicherheit hinsichtlich der zulässigen Speicherfristen zu schaffen.

Wie datenschutzrechtliche Kontrollen ergaben, haben TK-Anbieter immer wieder Schwierigkeiten mit den Speichervorschriften im TKG: Auf Grund deren Ungenauigkeit sei eine exakte Bestimmung der zulässigen Speicherungsdauer praktisch sehr schwierig und die Folge sei, dass zahlreiche Unternehmen die Gesetze sehr weit auslegen und die Daten teilweise viel zu lange speichern, meint der *BfDI*. An diesem Punkt soll nun der Leitfaden von *BfDI* und *BNetzA* ansetzen und mehr Rechtssicherheit nicht nur für die Unternehmen, sondern zugleich auch für die Betroffenen herstellen. Gem. § 97 Abs. 3 Satz 2 TKG dürfen Informationen über abgehende, entgeltpflichtige Telefonanrufe bis zu sechs Monaten gespeichert werden. Der Leitfaden hält dagegen drei Monate in der Regel für völlig ausreichend.

1. Manchen gehen die Regeln schon jetzt nicht weit genug

Noch immer zu weit gehen die vorgeschlagenen Maßstäbe dem *Arbeitskreis Vorratsdatenspeicherung* (*AK-Vorrat*), einer bundesweiten Lobby-Organisation für Datenschutz: Zunächst sei die Speicherung nicht für Daten aller Art erforderlich. Funkzellen – der Bereich, innerhalb dessen Signale eines Mobilfunknetzes fehlerfrei transportiert werden können – würden z.B. einzig für die Bestimmung eines Ortstarifs gebraucht. Daten zur Störungsbeseitigung sollten nur im Einzelfall, nicht pauschal gespeichert werden. Insgesamt solle für den Verbraucher transparent gemacht werden, wie viele Daten welcher Art wofür gespeichert werden. Problematisch sei auch, dass weder Verbraucher- noch Bürgerrechtsorganisationen in deren Erarbeitung miteinbezogen worden seien. Nach Angaben des *AK-Vorrat* ist zu den zulässigen Speicherfristen von Standortfunkzellen derzeit eine Klage gegen verschiedene Mobilfunkanbieter vor dem *AG Düsseldorf* anhängig.

2. Vorratsdatenspeicherung ausgespart

Dieser Leitfaden gilt ausdrücklich nicht für die Vorratsdatenspeicherung zum Zwecke der Strafverfolgung, bei der auf Anfrage von Sicherheitsbehörden Daten herausgegeben werden können. Er enthält aber eine Anmerkung, dass eine zusätzliche Speicherung der Daten in einem eigens für Behördenauskünfte eingerichteten System als Kopie der betrieblich genutzten Daten „vorläufig toleriert" werde, solange die Daten zeitgleich mit dem jeweiligen System gelöscht würden.

Für diese Daten, die für Strafverfolgungszwecke gespeichert werden, gelten spezielle Regelungen, nämlich das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der RL 2006/24/EG". Dieses hat das *BVerfG* bekanntlich im März 2010 (MMR 2010, 356) für verfassungswidrig erklärt. Die EU hat mittlerweile ein Vertragsverletzungsverfahren wegen Nichtumsetzung der RL 2006/24/EG in der Sache eingeleitet.

Es ist zu bezweifeln, dass der Leitfaden die Rechtsfragen des Speicherns von TK-Daten löst. Bei der jeweiligen Rubrik der „Datenschutzgerechten Auslegung" findet man mehrfach sog. „Escape"-Klauseln, wonach die Daten länger gespeichert werden können, wenn es „nachvollziehbare Gründe" gibt. Manche Datensätze sollen „in der Regel" drei Monate gespeichert werden. Ob diese Klauseln wirklich mehr Rechtssicherheit erzeugen, ist fraglich. Im Zweifel wird sich der TK-Anbieter darauf berufen. Der Leitfaden spricht auch nur von „Löschung" der Daten – nicht von „Anonymisierung." Ein anderes eher technisches Problem ist, wie der TK-Anbieter die gleichzeitige Löschung der Daten in getrennten Datenbanken für die Sicherheitsorgane in den Griff bekommt. Weiß die linke Hand wirklich, was die rechte Hand tut?

3. Schwierigkeiten beim Cloud Computing

Besonders schwierig wird die Anwendung beim immer beliebteren grenzübergreifenden Cloud Computing. Grundsätzlich greift § 97 Abs. 5 TKG als Ermächtigungsgrundlage ein: „Zieht der Diensteanbieter mit der Rechnung Entgelte für Leistungen eines Dritten ein, die dieser im Zusammenhang mit der Erbringung von TK-Diensten erbracht hat, so darf er dem Dritten Bestands- und Verkehrsdaten übermitteln, soweit diese im Einzelfall für die Durchsetzung der Forderungen des Dritten gegenüber seinem Teilnehmer erforderlich sind." Diese Übermittlung führt aber zu Compliance-Problemen: Da die Speicherfristen und Löschungsvorgaben in den EU-Ländern nicht identisch sind, könnte es passieren, dass der Cloud-Anbieter als „Data Processor" die Daten nach deutschem Recht löschen muss, während sie nach dem Recht des Anbieters am Speicherort weiter gespeichert werden müssten. Der TK-Anbieter muss auch sicherstellen, dass in der Cloud die Daten wirklich überall gelöscht sind und es nicht noch Sicherungskopien oder Ähnliches gibt. Das sehen aber andere Behörden in Europa möglicherweise anders: Der *Information Commissioner* in Großbritannien erachtet z.B. in einem Leitfaden Daten als gelöscht, wenn sie sicher archiviert werden. Wörtlich heißt es in diesen Guidelines:

„The *ICO* will be satisfied that information has been 'put beyond use', if not actually deleted, provided that the data controller holding it:

- is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
- does not give any other organisation access to the personal data;
- surrounds the personal data with appropriate technical and organisational security; and
- commits to permanent deletion of the information if, or when, this becomes possible."

Dieses eher großzügige, und von vielen internationalen TK-Anbietern begrüßte Verständnis des Löschens ist wahrscheinlich nicht mit der Intention des Leitfadens vereinbar. Es wäre deshalb wünschenswert, wenn die Diskussion um die Speicherfristen auf EU-Ebene (z.B. über die *Art. 29-Datenschutzgruppe*) weitergeführt und vertieft werden könnte. Die internationale Vernetzung der TK-Anbieter und ihrer Dienstleister (z.B. bei nomadischen Diensten wie internationalem VoIP)

weicht die länderbezogene Speicherungs- und Löschungsverpflichtung ohnehin mehr auf. Daten, die in einer Jurisdiktion gelöscht sind, sind möglicherweise anderswo sehr wohl noch existent und bei Streitigkeiten (z.B. über die sehr weiten Möglichkeiten der E-Discovery in den USA) abrufbar.

■ Vgl. zu E-Discovery *Deutlmoser/Filip*, ZD-Beilage 6/2012, 1 ff.

Dr. Axel Spies
ist Rechtsanwalt bei Bingham McCutchen in Washington DC und Mitherausgeber der Zeitschrift ZD.

Patrick Breyer Korrigierter Leitfaden zur Speicherung von Verkehrsdaten veröffentlicht

ZD-Aktuell 2012, 03218

Die Speicherung von Verkehrsdaten zieht vielfältige staatliche Einsichtnahmen einschließlich massenhafter Funkzellenabfragen und Fälle falschen Verdachts der Ermittlungsbehörden, aber auch Abmahnwellen gegen Internetnutzer durch Rechteinhaber nach sich. Im September 2012 haben die *BNetzA* und der *Bundesdatenschutzbeauftragte* (*BfDI*) einen Leitfaden zu der Frage veröffentlicht, wie lange die TK-Anbieter welche Daten über die Telefon-, Handy-, Internet- und E-Mail-Nutzung ihrer Kunden speichern dürfen. Hintergrund war eine Anzeige des *AK-Vorrat* bei der *BNetzA*, der zufolge die Speicherpraxis der Anbieter gegen die §§ 96 ff. TKG verstößt und ordnungswidrig sei.

Trotz Aufforderung haben *BNetzA* und *BfDI* an der Ausarbeitung ihres „Leitfadens" über die zulässige Speicherdauer nur die TK-Industrie, nicht aber unabhängige Verbraucher- und Datenschützer beteiligt. Dementsprechend zu Gunsten der Anbieter verzerrt, gibt der veröffentlichte Leitfaden die Rechtslage wieder. Um die Rechtslage korrekt darzustellen, habe ich den Leitfaden korrigiert und in korrigierter Fassung im Internet veröffentlicht. Der wichtigste Korrekturbedarf bestand in den folgenden Punkten:

■ Unzulässigkeit siebentägiger Vorratsspeicherung aller Verbindungs- und Standortdaten

Der *BfDI* hält eine siebentägige Vorratsspeicherung jeglicher Verkehrsdaten für zulässig, um Störungen zu erkennen (§ 100 TKG) und Daten wiederherstellen zu können (Backup). Danach soll es z.B. zulässig sein, permanent und ohne Anlass den Standort von Handynutzern und den E-Mail-Verkehr aller Nutzer zu protokollieren. Tatsächlich erlaubt § 100 TKG eine solche Vorratsdatenspeicherung nicht (s. Erwägungsgrund 29 der RL 2002/58/EG; ausf. *Breyer*, MMR 2011, 573). Der *BfDI* beruft sich zu Unrecht auf die Entscheidung des *BGH* (MMR 2011, 341 m. Anm. *Karg*), die nur Internetverbindungen betrifft und die Zulässigkeit deren siebentägiger Vorratsspeicherung offen gelassen hat. Das *OLG Frankfurt/M.* hat nach der Zurückverweisung vergleichsweise eine Löschung „in einem Zeitrahmen von 6–24 Stunden" vorgeschlagen. Eine rechtskräftige Entscheidung steht aus.

■ Unzulässigkeit einmonatiger Protokollierung kostenfreier Verbindungen

Der *BfDI* hält es für zulässig, dass einzelne Anbieter die Daten kostenfreier und pauschal abgegoltener Verbindungen nur einmal im Monat ausfiltern und löschen (§ 97 Abs. 3 TKG). Tatsächlich fordert das geltende Datenschutzrecht von jedem Anbieter die möglichst datensparsame Einrichtung seiner Systeme (vgl. § 3a BDSG und *BVerfG* MMR 2007, 308, Rdnr. 29), sodass die Daten kostenfreier und pauschal abgegoltener Verbindungen spätestens mit Verbindungsende zu löschen sind (z.B. durch „Online-Billing").

■ Recht auf Löschung mit Entgeltermittlung

Der *BfDI* hält es für zulässig, die Daten kostenpflichtiger Verbindungen drei Monate lang zu Nachweiszwecken zu speichern, selbst wenn der Kunde eine Löschung der Daten verlangt. Tatsächlich ist eine Datenspeicherung zu Nachweiszwecken im Fall eines Löschungswunschs nicht erforderlich, weil der Anbieter in diesem Fall nicht nachweispflichtig ist (§ 45i Abs. 2 Satz 2 TKG).

■ Unzulässigkeit dreimonatiger Speicherung zur Abrechnung mit anderen Anbietern

Für Verbindungen, die nicht ausschließlich über das Netz des eigenen Anbieters vermittelt werden, muss der Anbieter oftmals einem anderen Anbieter ein zeitanhängiges Zusammenschaltungs- oder Terminierungsentgelt zahlen. Aus diesem Grund müssen solche Verbindungen, auch wenn sie für den Kunden kostenfrei sind (z.B. Flatrates), protokolliert werden (§ 97 Abs. 4 TKG). Der *BfDI* verkennt jedoch, dass zur Abrechnung zwischen