# Daten auf Vorrat

**Am 28. April 2011 wurden jene Gesetzesvorlagen, mit denen die Richtlinie zur Vorratsdatenspeicherung umgesetzt wurde, im Nationalrat beschlossen.**

Die Verpflichtungen der Anbieter von öffentlichen Kommunikationsdiensten wurden mit einer Novelle des Telekommunikationsgesetzes 2003 festgelegt, und die Zugriffsmöglichkeiten der Strafverfolgungs- und Sicherheitsbehörden mit Änderungen der Strafprozessordnung 1975 und des Sicherheitspolizeigesetzes verankert.

Die darin enthaltenen Bestimmungen über die Vorratsdatenspeicherung (für die Dauer von sechs Monaten) und die Beauskunftungen nach Maßgabe von StPO und SPG treten am 1. April 2012 in Kraft. Bis zu diesem Zeitpunkt erlaubt es das TKG 2003 den Anbietern nur, so genannte „Billingdaten" zu speichern, die sie aus Betriebsnotwendigkeit und insbesondere zu Verrechnungszwecken benötigen. Welche Daten davon umfasst sind (fraglich scheint dies insbesondere bei Standortdaten), und wie lange sie bei den jeweiligen Anbietern verfügbar sind (etwa Angaben zu einem Teilnehmer, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war), hängt ausschließlich von den Gegebenheiten beim Anbieter ab und ist der um Auskunft ersuchenden Stelle nicht bekannt.

Die Tatsache, dass die anfragende Stelle nicht weiß, ob sie (noch) aus „Billingdaten" Auskunft verlangen kann, oder der Anbieter für die Auskunftserteilung auf Vorratsdaten (als solche sind sie ab ihrer Erzeugung oder Verarbeitung beim Anbieter zu speichern) zugreifen muss, kann im Bereich der Auskunftsersuchen nach der StPO wegen der unterschiedlichen Voraussetzungen für die Zulässigkeit der Anfrage zu Problemen führen (siehe dazu unten). Wie schon bisher enthält das TKG 2003 die Verpflichtung der Anbieter, Teilnehmerverzeichnisse ihrer Kunden (insbesondere Namen und Telefonnummern) herauszugeben und diese Stammdaten sowohl im Bereich der StPO als auch für die Aufgabenerfüllung nach dem SPG zu beauskunften.

Darüber hinaus enthält der neue § 99 Abs. 5 TKG 2003 die Speicherverpflichtung bestimmter „Zugangsdaten", die die Zuordnung eines Kommunikationsvorgangs zu einem bestimmten Teilnehmer ermöglichen sollen. Diese Daten sind unterhalb der Grenze der schweren Straftat an Strafverfolgungsbehörden nach der StPO bzw. an die Sicherheitsbehörden nach Maßgabe des SPG zu beauskunften.

Schließlich zählt § 102a TKG 2003 taxativ die von den Betreibern als Vorratsdaten sowohl im Bereich der Telefonie als auch im Bereich der Internetkommunikation für sechs Monate zu speichernden Daten auf (Stammdaten, Standortdaten und Verkehrsdaten wie etwa Beginn und Dauer jedes Kommunikationsvorgangs, E-Mail-Adressen und Art der genutzten Dienste sowie Teilnehmerkennungen zu IP-Adressen), deren Beauskunftung aber nur für Zwecke der Verfolgung schwerer Straftaten nach Maßgabe der StPO erfolgen darf.

**Auskunft im Dienste der Strafrechtspflege** (§§ 99 Abs. 5 Z 1 und 2 sowie § 102a ff TKG 2003 iVm §§ 76a und 134 ff StPO): Durch eine komplizierte Verweiskette normiert der Gesetzgeber, welche Daten nach welchen Bestimmungen der StPO für Zwecke der Strafverfolgung zu beauskunften sind: In je-

## VORRATSDATENSPEICHERUNG

### EU-Richtlinie

Mit der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung vom 15. März 2006 werden Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste verpflichtet, alle Verbindungsdaten ihrer Kunden mindestens sechs Monate lang zu speichern und die Daten den Behörden für die Ermittlung, Feststellung und Verfolgung schwerer Straftaten zur Verfügung zu stellen. Die Richtlinie gilt für Stamm-, Verkehrs- und Standortdaten von juristischen und natürlichen Personen sowie für alle damit in Zusammenhang stehende Daten, die zur Feststellung des Teilnehmers oder registrierten Benutzers erforderlich sind, nicht aber für den Inhalt elektronischer Nachrichtenübermittlungen.

Jene Daten sind auf Vorrat zu speichern, die benötigt werden, um etwa die Quelle einer Nachricht (wie Rufnummer, Name und Anschrift des Teilnehmers, Benutzerkennung oder IP-Adresse) rückverfolgen zu können, Adressaten einer Nachricht zu identifizieren, die Art der Nachrichtenübermittlung (in Anspruch genommener Telefon- oder Internetdienst) sowie Datum, Uhrzeit und Dauer der Nachrichtenübermittlung und den Standort mobiler Geräte bestimmen zu können. Hinsichtlich des Zugangs zu den Vorratsdaten sieht die Richtlinie lediglich vor, dass von den Mitgliedstaaten Maßnahmen zu erlassen sind, um sicherzustellen, dass die Daten „nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden".

Aufgrund der mit ihr verbundenen Grundrechtseingriffe war die Richtlinie zur Vorratsdatenspeicherung umstritten. In mehreren Mitgliedstaaten wurden die Höchstgerichte mit der Prüfung der Umsetzungsgesetze befasst; das deutsche Bundesverfassungsgericht erklärte die Umsetzung für verfassungsrechtswidrig.

Gegen Österreich wurde unter anderem wegen nicht fristgerechter Umsetzung ein Vertragsverletzungsverfahren eingeleitet. Die Richtlinie wäre von den Mitgliedstaaten grundsätzlich bis 15. September 2007 bzw. betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail bis 15. März 2009 umzusetzen gewesen.

Mit Urteil vom 20. Juli 2010 verurteilte der Europäische Gerichtshof die Republik Österreich wegen „Nicht-Umsetzung", wenngleich vorerst ohne Strafzahlungen.

nen Fällen, in denen nur die in § 76a Abs. 2 StPO genannten Zugangsdaten gebraucht werden, bedarf es einer staatsanwaltschaftlichen Anordnung; bei Gefahr im Verzug ist auch die Kriminalpolizei ermächtigt, diese Daten einzuholen (§ 99 Abs. 2 StPO). Unabhängig von der Schwere des Delikts kann der Staatanwalt nach § 76a Abs. 2 StPO im Bereich der Internetkommunikation Auskunft über jene aufgezählten Zugangsdaten verlangen, die unter Umständen die Identifizierung des Absenders einer Nachricht ermöglichen.

Werden darüber hinausgehende Daten benötigt und liegen die Voraussetzungen des § 135 Abs. 2 Z 1 bis 4 StPO vor, so ist eine Auskunft über Daten einer Nachrichtenübermittlung (§ 134 Z 2 StPO) mit gerichtlicher Bewilligung einzuholen. Dies setzt aber voraus, dass die benötigten Daten gemäß § 99 Abs. 5 TKG 2003 aus betriebsnotwendigen Gründen noch vorhanden sind. Andernfalls muss bei Vorliegen der Voraussetzungen die Auskunft über Vorratsdaten gemäß §§ 102a und b TKG 2003 iVm §§ 134 Z 2a und 135 Abs. 2a StPO eingeholt werden. Dies ist etwa zur Aufklärung einer vorsätzlichen Straftat mit einer Strafdrohung von mehr als einem Jahr möglich, wenn Daten des Beschuldigten oder der Aufenthaltsort eines flüchtigen oder abwesenden Beschuldigten ermittelt werden können. Neben der gerichtlichen Bewilligung bedarf die Beauskunftung von Vorratsdaten als zusätzliche formelle Voraussetzung die vorhergehende Befassung des Rechtsschutzbeauftragten der Justiz gemäß § 147 Abs. 1 Z 2a StPO. Da das um Auskunft ersuchende Organ im Zeitpunkt des Auskunftsverlangens, insbesondere bei noch nicht lange zurückliegenden Kommunikationsvorgängen mangels Bekanntgabe entsprechender Richtwerte zum Speicherzeitraum von „Billingdaten“ von Seiten der Anbieter nicht wissen kann, in welcher Form das benötigte Datum vorhanden ist, könnten Auskunftsverlangen ins Leere gehen. Die Auskunft nach „älteren“ Standortdaten sollte daher im Zweifelsfall nicht als Auskunft über Daten einer Nachrichtenübermittlung nach § 134 Z 2 StPO, sondern nach Einbindung des Rechtsschutzbeauftragte beim BMJ direkt als Auskunft von Vorratsdaten nach § 134 Z 2a StPO eingeholt werden.

**Beauskunftung für sicherheitspolizeiliche Zwecke** (§ 99 Abs. 5 Z 3 und 4 iVm § 53 Abs. 3a und 3b SPG): Durch die neu geschaffenen Regelungen erhalten auch die Sicherheitsbehörden Zugriff sowohl auf „Billingdaten“ als auch auf Vorratsdaten in dem Umfang, der durch das SPG vorgegeben ist.

In diesem Sinn legt das TKG 2003 hinsichtlich der Auskunft über Standortdaten ausdrücklich fest, dass für die Feststellung des aktuellen Standorts einer Endeinrichtung, insbesondere für die erste allgemeine Hilfeleistung, eine Auswertung des letzten bekannten Standorts der Endeinrichtung auch unter Zuhilfenahme von Vorratsdaten zulässig ist (§ 99 Abs. 5 Z 3 TKG).

Was die Rückverfolgung der Quelle einer Nachricht anhand der zugewiesenen IP-Adresse bei Internetnutzung anlangt, ist ein Zugriff auf solche Zugangsdaten für die im SPG aufgezählten Zwecke zulässig, wenn sie längstens drei Monate vor der Anfrage gespeichert wurden – unabhängig davon, ob sie als Billingdaten noch vorhanden sind. Die Abfrage der Stammdaten im Bereich der Telefonie (§ 90 Abs. 7 TKG 2003, § 53 Abs. 3a Z 1 SPG) ist für jede Art der Aufgabenerfüllung nach dem SPG zulässig. Voraussetzung für die Beauskunftung von IP-Adressen (§ 53 Abs. 3a Z 2 und 3 SPG) ist das Vorliegen der sicherheitspolizeilichen Aufgabenstellungen der ersten allgemeinen Hilfeleistung, der Abwehr gefährlicher Angriffe oder krimineller Verbindungen und, dass der Inhalt der ermittlungsrelevanten Nachricht (z. B. eine Droh-E-Mail) den Sicherheitsbehörden (etwa durch den Bedrohten) bekannt ist. Und schließlich regelt § 53 Abs. 3a Z 4 SPG nunmehr in einer eigenen Ziffer die Zulässigkeit der so genannten „punktuellen Rufdatenrückerfassung“, das ist die Auskunft über Namen, Anschrift und Telefonnummer des Anrufers durch Bezeichnung eines möglichst genauen Zeitraums und der angerufenen Nummer für Zwecke der erstem allgemeinen Hilfeleistung und zur Abwehr gefährlicher Angriffe.

**Bei Gefahr im Verzug ist auch die Kriminalpolizei ermächtigt, bestimmte Zugangsdaten einzuholen.**

Die Beauskunftung von Standortdaten und der IMSI-Nummer des von einem gefährdeten Menschen mitgeführten Endgeräts zur Hilfeleistung und Gefahrenabwehr regelt wie bisher § 53 Abs. 3b SPG. Die Verantwortung der rechtlichen Zulässigkeit von Auskunftsbegehren nach Abs. 3a und 3b obliegt den Sicherheitsbehörden. Dies umfasst im Falle des Abs. 3b auch eine entsprechende schriftliche Dokumentation, die dem Betreiber unverzüglich, spätestens innerhalb von 24 Stunden nachzureichen ist.

Neu ist in diesem Zusammenhang die Verpflichtung der Sicherheitsbehörden, Betroffene ehest möglich und nachweislich und unter Angabe von Rechtsgrundlage, Datum und Uhrzeit über eine erfolgte Beauskunftung zu einer IP-Adresse oder zu Standortdaten zu informieren, wenn dabei Vorratsdaten verwendet wurden. Diese Information kann aufgeschoben werden, solange durch sie der Ermittlungszweck gefährdet wäre. Sie kann sogar unterbleiben, wenn der Betroffene bereits nachweislich von der Beauskunftung Kenntnis erlangt hat oder die Information des Betroffenen faktisch unmöglich ist.

Die Einhaltung dieser Informationsverpflichtung prüft der Rechtsschutzbeauftragte beim Bundesministerium für Inneres. Auch über das Unterbleiben bzw den Aufschub der Information des Betroffenen und die dafür geltend gemachten Gründe ist der Rechtsschutzbeauftragte in Kenntnis zu setzen.

**Durchlaufstelle.** Bis zum In-Kraft-Treten der neuen Regelungen mit 1. April 2012 ist geplant, zur technischen Abwicklung eine so genannte „Durchlaufstelle“ zu errichten, über die Abfragen in verschlüsselter Weise abgewickelt und protokolliert werden. Der Vertraulichkeit und dem Schutz der Daten einer Nachrichtenübermittlung Rechnung tragend, ist die Einführung eines neuen Straftatbestands in § 301 Abs. 3 StGB geplant, der die Veröffentlichung von Auskünften einer Nachrichtenübermittlung unter Strafe stellt. *Verena Weiss/ Lisa Pühringer*

FOTO: EGON WEISSHEIMER